

A Computer-Aided Technique for Identifying Latent Conditions (CATILaC)

K. Marcinkowski, G. Apostolakis and R. Weil

Department of Nuclear Engineering, Massachusetts Institute of Technology, Cambridge, MA, USA

Abstract: An incident investigation methodology has been developed to better place operating experience into an organisational context. It uses the concept of work processes to suggest the locations of organisational deficiencies that contributed to an event. To guide an analyst through this methodology, a software package has been developed which offers suggestions about where corrective actions and further investigation should be directed after an event. In this paper, the methodology is introduced, the software development is discussed, and a sample event is analysed. Comparisons are made to existing incident analysis methods and areas for future work are outlined. Although the discussion is geared toward nuclear power plant applications, the methodology is applicable to any type of highly proceduralised and structured organisation.

Keywords: Latent conditions; Root-cause analysis; Organisational factors

1. INTRODUCTION

Research and experience have shown that human errors are a product of the context in which they occur. Reason's work on human error (Reason 1990) shifted the incident investigation paradigm from the 'sharp end', or the execution tasks, to management and organisational deficiencies and other latent conditions that combine with system conditions to create contexts conducive to unsafe acts. Latent conditions are weaknesses that exist within a system that create contexts for human error 'beyond the scope of individual psychology' (Reason 1997). These latent conditions can range from poor procedures, inadequate training, unusable equipment, or bad management policies, and are usually the result of high-level organisational problems.

Both active and latent failures can result from latent conditions within an organisation. Reason defines active failures as those 'whose effects are felt almost immediately' and latent failures as those 'whose adverse consequences may lie dormant in the system for a long time' (Reason 1990). The active and latent failures combine to defeat a system's defences and create incidents. A recent examination of nuclear power plant operating experience by Gertman and Hallbert (2000) found that most failures identified in actual events were latent in nature, having no immediate impact on the system. Based on the analysis of 35 events, these authors found that latent errors outnumbered active errors by a ratio of four to one.

Reason modelled the connection between failure events and human error. In doing so, he provided a way for analysts to look beyond the traditional unsafe acts when investigating the causes of what he calls organisational accidents (Reason 1997). However, understanding how unsafe acts and the organisation are connected is not sufficient to make specific improvements within the organisation. Only by understanding the location of the unsafe act within the organisation's structure can corrective actions be directed toward the causes of the latent conditions.

To understand the human contribution's place in the organisation, we turn to the Work Process Analysis Model (WPAM) (Davoudian et al 1994). A work process is a standardised sequence of tasks that coordinates the activities of an organisation to achieve a specific goal. Most often, the tasks within a work process are performed by a series of individuals or groups rather than by a single individual.

The work process concept is best applied to organisations that are structured as machine bureaucracies. A machine bureaucracy has 'highly specialized, routine operating tasks, very formalized procedures in the operating core, large-scale units at the operating level, reliance on the functional basis for grouping tasks, relatively centralized power for decision making, and an elaborate administrative structure with a sharp distinction between line and staff' (Mintzberg 1979). Nuclear power plants and other high-hazard industrial facilities fit easily into this category.

A work process differentiates itself from a procedure in that each of the tasks within the process may have its own specific procedures. Most work processes contain essentially the same sequence of tasks. The general structure of a work process is shown in Fig. 1.

In addition to being consistent as a group, work processes are also consistent throughout an industry. For example, the corrective maintenance work process will be nearly identical from one nuclear power plant to another. Although the procedures that govern the execution of each task within the work process may be different and the group or individual responsible for each task may change from facility to facility, the series of tasks needed to accomplish corrective maintenance will not change substantially. This is useful because once a database of work processes for a particular industry is developed, it can be easily adapted to any facility.

An organisation usually groups work processes into programmes. These programmes do not accomplish work themselves, but serve as the manifestations of high-level policy objectives within the organisation (Weil and Apostolakis 1999). Although work processes are consistent from facility to facility, their placement within programmes, as well as the programmes that exist, can vary greatly. For example, while some plants might have a maintenance programme that contains both preventive and corrective maintenance work processes, other plants might

have corrective maintenance in the corrective action programme and preventive maintenance in its own preventive maintenance programme. Figure 2 illustrates the relationship between programmes, work processes, tasks and procedures.

By combining Reason's work with WPAM, Weil and Apostolakis (1999) were able to develop an incident investigation methodology to identify the contributions that organisational factors make to significant events. When implemented as part of a root cause analysis programme, the methodology can help the analyst assess the latent conditions that led to the human contributions in an incident. Thanks to the work process, the analyst will also know where to direct any corrective actions for identified deficiency.

In this paper, we begin by presenting a brief background on incident analysis and the current state of the art in understanding human error in the context of the organisation. This serves as an introduction to the latent condition identification methodology, which is discussed in detail, as well as the CATILaC (Computer-Aided Technique for Identifying Latent Conditions) software package that was developed as a means of implementing the latent condition identification methodology. After CATILaC is introduced, we demonstrate its capabilities by analysing and discussing a sample event.

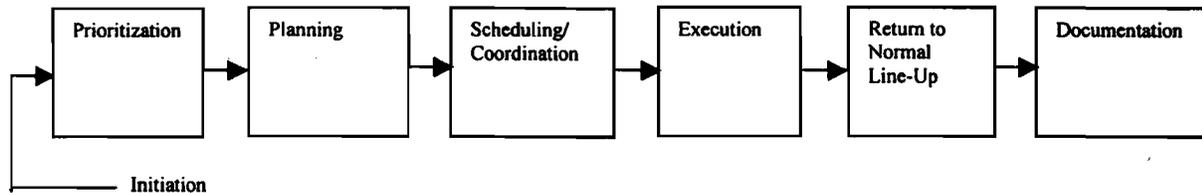


Fig. 1. General work process structure (the corrective maintenance work process).

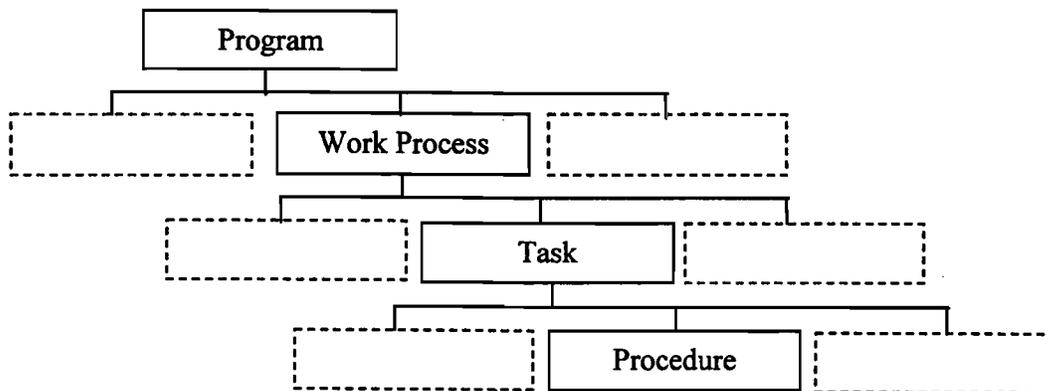


Fig. 2. Hierarchical relationship among programmes, work processes, tasks and procedures.

2. BACKGROUND ON INCIDENT ANALYSIS

The goal of any incident analysis is threefold:

- to understand what happened during the event;
- to discover why and how the event happened;
- to provide corrective action recommendations to prevent recurrence of the event.

A number of analysis methods focus on various means of locating the failure source, or sources, and for understanding why an incident occurred. Advances in analysis methods have helped analysts to increase the scope of their incident investigations and have allowed them to identify more far-reaching causes for the incidents that occur.

Initially, analysts used root-cause analysis as a tool to identify the mechanical and ergonomic causes behind a failure. The analyst was interested in identifying the physical reason why a given component did not operate properly or to find human deficiencies that could be corrected through engineering action. This included identification of wear-out modes, various types of failures and stresses, and other signs of damage by examining the failed components, as well as various aspects of human factors engineering such as control room design. Failure modes and effects analysis (FMEA) or fault tree analysis are examples of traditional safety analysis methods that are suitable for obtaining these types of results.

As the importance of human actions to system safety became more widely recognised, root-cause analysis expanded to include the identification of cognitive processes and other factors that affected worker performance. The analyst became interested in understanding the sequence of occurrences that led to the event and the factors that shaped human action during the event. For example, operator action or poor/improper maintenance might be identified as the cause of a particular component failure. Sequence of events analysis is one method used to develop an understanding of how an event developed and the important factors that contributed to its occurrence (Mobley 1999). Sequence of events analysis is a form of event flowcharting (similar to causal factors charting). In it, the analyst uses a prescribed diagram structure to describe the sequence of events leading up to and following the incident. Possible causes of events and explanatory and qualifying observations and details are added to the diagram for completeness. This method has many advantages: it allows for a logical order to be shown, it demands precision in the definition of events, causes, and qualifiers, and allows the analyst an overall view of the event itself and the factors that influenced it.

Incident analysis thinking continued to progress and events began to be viewed as a combination of multiple failures and the overlap of multiple missing barriers.

Reason's work (1990, 1997), introduced this new paradigm for discussing human error. He introduced the important role that latent conditions play in creating events by presenting an accident as the alignment of deficiencies in the many barriers designed to prevent it. In other words, these organisational events result from a combination of active failures in the form of unsafe acts and latent failures, which create inadequate defences. 'No one person's failure was a sufficient cause for an accident' (Johnson and Botting 1999).

As mentioned in the introduction, Reason (1990) highlights the important role that management and organisational structure play in creating what is commonly known as error-forcing contexts, and presents a model for the relationship between human actions and organisational issues. In this model, fallible decisions by top management and deficiencies in line management (types) interact with psychological precursors of unsafe acts and unsafe acts themselves (tokens) to breach the defences of the system, thus creating accidents and incidents. Using this progression, accident analysts no longer need to focus on the active failures, or the individual unsafe acts, but can devote themselves to understanding and eliminating latent conditions caused by management and organisational problems. As Reason says, 'We cannot change the human condition, but we can change the conditions under which people work' (Reason 1997).

In order to take advantage of these broader perspectives, more incident analysis methods were developed to try to pinpoint the managerial and organisational problems that led to events. Some of these new methods, such as improved causal factor charting with root-cause identification (ABS Group, Risk and Reliability Division 1999) do not use Reason's work directly, but still try to pinpoint broader managerial and organisational deficiencies. Other methodologies, such as the Tripod-Beta software package and A Technique for Human Event Analysis (ATHEANA) developed by the US Nuclear Regulatory Commission (NRC 2000), include Reason's methodology essentially unchanged. Tripod-Beta, for example, allows the analyst to associate active and latent failures with the failed barriers that led to an event. ATHEANA 'postulates that unsafe human actions occur within an error-forcing context that can be specifically identified' (NRC 2000).

Tripod-Beta uses Reason's model to make the connection between failed or missing barriers and active or latent failure and the precondition that turns latent failures into active ones (EQE International 1999). These unsafe acts are then connected to general failure types using preconditions and management deficiencies. It employs the idea of identifying latent conditions as a means of better understanding how to prevent future problems, and views events as a combination of hazards and targets which breach the defences inherent in the system.

The ABS root-cause analysis system is a prescriptive methodology for identifying causal factors for an event and for finding the root causes for each of the causal factors. The concepts of latent failures or high-level organisational deficiencies are not introduced into the method; however, many broad classes of potential problems are considered. The method uses 11 major root-cause categories to classify the source of problems: from design and equipment reliability to administrative/management systems and human factors engineering. The analyst uses causal factors charting to develop an understanding of how an event occurred and what factors contributed to its occurrence. The causal factors that are identified are then analysed using the Root Cause Map: a hierarchical categorisation scheme that contains a comprehensive listing of root causes. Each identified root cause on the map also has a list of typical issues, typical corrective action recommendations and examples. Although this method does not specifically consider latent conditions, it does consider the effect that things like management and training have on creating conditions that can lead to failures.

ATHEANA is a major research project on human reliability analysis from the NRC. The technique can be used for retrospective analysis of events. ATHEANA guides the analyst through the process of identifying the key operator actions during the progression of an event. The idea of an error-forcing context, determined by a combination of performance shaping factors and plant conditions, is central to ATHEANA. As such, it provides guidance to the analyst on identifying the plant conditions and performance-shaping factors that led to human failure events, recognising that latent conditions within the system are what led to unsafe acts.

In this work, we continue the advancement of incident analysis techniques by incorporating the work process and Reason's work into a method that can deconstruct an incident into a series of hardware and human failures (similar to causal factors charting) and analyse them to locate latent conditions and organisational issues that led to the event.

3. THE LATENT CONDITION IDENTIFICATION METHODOLOGY

The Latent Condition Identification methodology used as the basis for the CATILaC (Computer-Aided Technique for Identifying Latent Conditions) software tool is an expanded version of the Incident Investigation Methodology developed by Weil and Apostolakis (1999). The goal of the work of Weil and Apostolakis was to outline a methodology for identifying the contribution of organisational factors to specific incidents. The methodology builds on the work of Tuli and Apostolakis (1996) on how to incorporate organisational issues into root-cause analysis.

By combining Reason's work (1990) with the Work Process Analysis Model (WPAM) and narrowing and redefining Jacobs and Haber's (1994) organisational factors, Weil and Apostolakis provide a means for connecting human error contributions to their roots within the organisation. The methodology used as the basis for CATILaC has been essentially unchanged from the original version (Weil and Apostolakis 1999); however, additional steps and further detail have been added to assist an analyst in getting useful results using the technique.

The premise of the methodology is that the front-line failures of hardware components and operators are caused by multiple underlying human contributions. By understanding where within the organisation these underlying human contributions occurred, an analyst can use that information to suggest organisational factors that may have impacted the event. The methodology does not draw specific conclusions with regard to the existence of organisational deficiencies; rather, it suggests possible areas within the organisation that may benefit from further analysis and corrective actions.

The methodology works best when it is tailored to each individual facility that uses it. Therefore, before an incident occurs, the first step is to compile a listing of programmes and work processes at the facility. The list need not be comprehensive, as there are many work processes that do not have an impact on plant performance. However, those work processes that coordinate activities involving the identification, prevention and repair of the problems at the facility should be included.

Because the identification of latent conditions relies heavily on understanding the structure of the organisation, and because no two organisations have exactly the same organisational structure, it is important to tailor the methodology to the structure of the facility at which it will be implemented in order to obtain the most insightful results. While a generic listing of work processes and programmes can be used to analyse events from a variety of facilities, the results will not be as accurate since the locations of the existing deficiencies will not be precisely pinpointed within the organisation. This problem will be discussed in detail later when we demonstrate the methodology on NRC Augmented Inspection Team (AIT) Reports using a generic organisational format.

After this preliminary work is completed and an incident occurs at the facility, analysis can begin in earnest. The following steps are necessary to complete the analysis:

1. Describe the incident.
2. Identify the hardware and operator contributions to the event.
3. Classify the hardware and operator contributions as pre- or post-initiator.

4. Analyse the human contributions to each hardware/operator contributor.
5. Summarise the output: deficient tasks and work processes, suggested organisational factors, dominant contributions, and event consequences.

3.1. Describe the Incident

The first step is the same as in any other incident investigation method: understand what happened during the incident, determine the conditions of the facility prior to the incident, and discover the progression of events that led to the incident. Of special importance is the trigger, or as Weil and Apostolakis call it, the initiator, of the event. The trigger is that failure or action that changed latent failures within the system into active ones. This will be used later in the analysis to identify the latent conditions within the system. The methodology does not provide a great deal of guidance in this area; it is assumed that the analyst will have the resources necessary to carry out his initial investigation.

3.2. Identify Hardware and Operator Contributors

Once the initial investigation is complete, the analyst identifies the hardware and operator contributions to the event. These contributions include hardware failures and operator actions that either initiated or exacerbated the event, as well as latent failures that created a vulnerability to the occurrence of the event (Corcoran 1998). The second category, vulnerabilities, is especially important to the methodology, particularly with respect to hardware contributions, since that is where the latent conditions are often found.

When developing the list of hardware contributions, every component whose unexpected action or lack of action was part of the event should be considered. Those that were not direct contributors (do not fall into initiator, exacerbator, or vulnerability categories) can be eliminated, as can hardware systems that activated as designed due to the failure/activation of another component. Any problems known prior to the incident that were not repaired or were not repaired properly should be included. Those hardware problems that, after analysis, were determined to be new and unexpected and that occurred during the course of the incident as the direct result of other failures will not benefit from continued analysis with the methodology. Of course, all of this discussion is only meant to guide an analyst, not to serve as a series of unbreakable rules. Ultimately, the analyst makes the final decision about what contributors should or should not be analysed further.

This methodology was developed primarily to aid in the analysis of the latent conditions leading to hardware contributions to events, an area that previously had received little focus. However, we acknowledge the

important role that operators play in the progression of events; thus, operator contributions should also be included in the methodology for further analysis.¹

3.3. Classify Contributors as Pre- or Post-Initiator

The next step is the classification of the hardware and operator contributions as pre- or post-trigger. As mentioned earlier, the trigger, or initiator, is the event that turns the latent failures in the system into active failures. Thus, all latent failures and known conditions within the system that became active during the event are classified as pre-trigger. For example, if a safety system fails after the initiating event because maintenance workers had removed all of the oil during the last preventive maintenance period, the failure of the safety system would be classified as pre-trigger. Only those failures that occurred during the course of the event and were not known should be classified as post-trigger. Classifying the contributions in this manner makes it easier to recognise the latent contributions to a particular event.

3.4. Identify and Analyse Human Contributions

It is in this next step that the methodology distinguishes itself from other incident analysis methods. The human contributions to each hardware/operator contribution must be identified and analysed. That is, the human contributions are placed into an organisational context and the organisational factors that influenced their occurrence are identified. Human contributions can range from improper maintenance to not making corrections after a precursor event. In the case of hardware contributions, asking the question 'Why did this hardware contribution happen?' and being able to answer in the form 'Because person A did/did not do X' will usually result in a human contribution to the hardware contribution in question.

Handling operator contributions is more complex, as there may be other human contributions, besides the operator action itself that merit analysis. For example, an error in procedure writing or training could lead to an operator contribution without any sort of unsafe act on the part of the operator. Asking the question, 'Why did the operator respond that way?' and finding an answer in the form, 'Because person B did/did not do Y' is useful for locating additional human contributions to operator contributions.

Each human contribution is placed into the context of the organisation by identifying the programme and work

¹The methodology is most useful for identifying latent conditions that contribute to the error-forcing context. It is not useful in analysing the cognitive aspects of error mechanisms. These error mechanisms are related to decisions that operators make in response to an incident such as detection, situation awareness, response planning and implementation (NRC 2000).

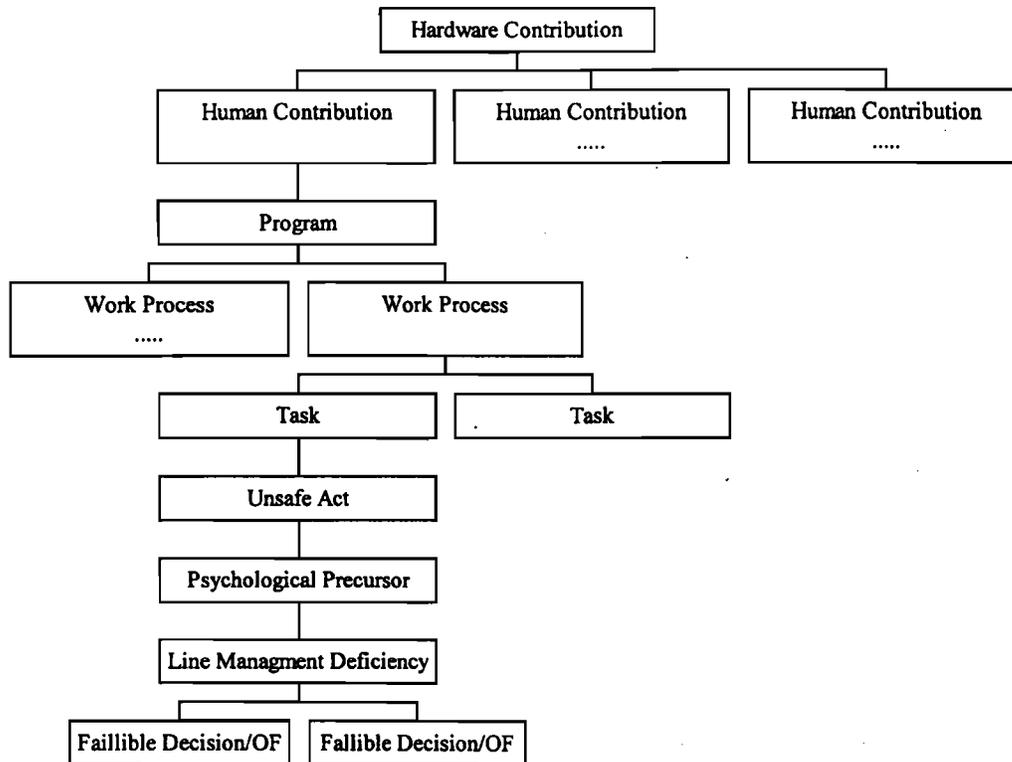


Fig. 3. Linking hardware contributions to organisational issues.

process in which it occurred or which contained a latent condition that led to the contribution.² The task or tasks in which the deficiency existed must also be identified. The listing of programmes and work processes discussed earlier is used here. It is possible that more than one work process could contain deficiencies that led to a single human contribution. By checking for other factors contributing to a human contribution after identifying one potential organisational location, it is possible to identify these other deficient work processes or tasks.

The deficiencies are then analysed using the type/token terminology developed by Reason. Moreover, they are classified as an unsafe act, a psychological precursor, a line management deficiency or a fallible decision. Then, contributors on the same type/token path are investigated. For example, if the deficiency is classified as an unsafe act, there may be a psychological precursor or line management deficiency that can be identified. Doing this will improve the analysis because it enables the analyst to find the contributing factors to each deficiency. For each deficient task, at least one organisational factor should be suggested as a fallible decision potentially contributing to the

existence of the deficiency. In this methodology, we equate organisational factors with fallible decisions. Management policies can be divided into broad categories of organisational issues and poor decisions made by upper management with regard to any of these issues have a far-reaching impact on plant performance. For example, if a problem is linked to the organisational factor of communication, it means that the organisation has been making fallible decisions about its policies or practices for ensuring good communication. The methodology allows the analyst to go a step further and suggest corrective actions to communication policies that are directed at a specific work process or task. The relationship between hardware contributions and fallible decisions/organisational factors is shown in Fig. 3.

3.5. Output

The output of the methodology is a listing of deficient tasks and work processes as well as potential areas of organisational problems. These results can be very useful in aiding in the development of complete and appropriate corrective actions. In addition, by tracking the recurrence of organisational issues in a number of events at a facility, an analyst can look for pervasive organisational issues or specific work process problems that need to be addressed.

²For certain human actions that do not happen within the context of a work process, e.g., post-trigger recovery actions by operators, the identification of a task or work process is not necessary.

The methodology has the capability to identify the latent conditions that led to events at a facility. The analyst can use these results to develop corrective actions and to assist in managing risk at his facility.

4. THE CATILaC SOFTWARE PACKAGE

Once the Latent Condition Identification Methodology is developed and tested using operating experience, the next step is to computerise the process. There are several reasons for doing this:

- to provide an instructional tool to teach analysts how to use the methodology;
- to provide a way to store and access the analyses that have been completed;
- to create a way to interact between the methodology and a database of work processes.
- to increase the accessibility of the methodology to plant personnel.

The package is needed not only to collect and store the information from incident investigations, but also to guide a novice analyst through the process without being burdensome to advanced users. To meet these objectives, a Computer-Aided Technique for Identification of Latent Conditions (CATILaC) has been developed.

4.1. Software Development

The software was developed using the Microsoft Access database program. This is used as the basis for the package because the software itself is not calculation or graphic intensive; it just needs to accept, store and organise large amounts of data. The program guides the analyst through the incident investigation methodology, from creating and updating the work process database to choosing work processes that correspond to human contributions. It does this in two steps: (1) by providing a work process database for the work processes to be input and displayed; and (2) by guiding the analyst through the input and analysis of the event contributors.

The input and analysis of human contributions is done using a series of forms that both store the data and guide the analyst through the process. The first form is an event information and hardware contribution form that is used to store basic event details such as event name, date, plant operating state and event trigger, and gives the analyst space to list the hardware contributions to the event. On the second form, the analyst inputs the human contributions to each hardware contribution. On the third and final form, the analyst performs the analysis of each human contribution by choosing the programme, work process, and task (from the work process database) that contained deficiencies leading to the contribution. CATILaC stores

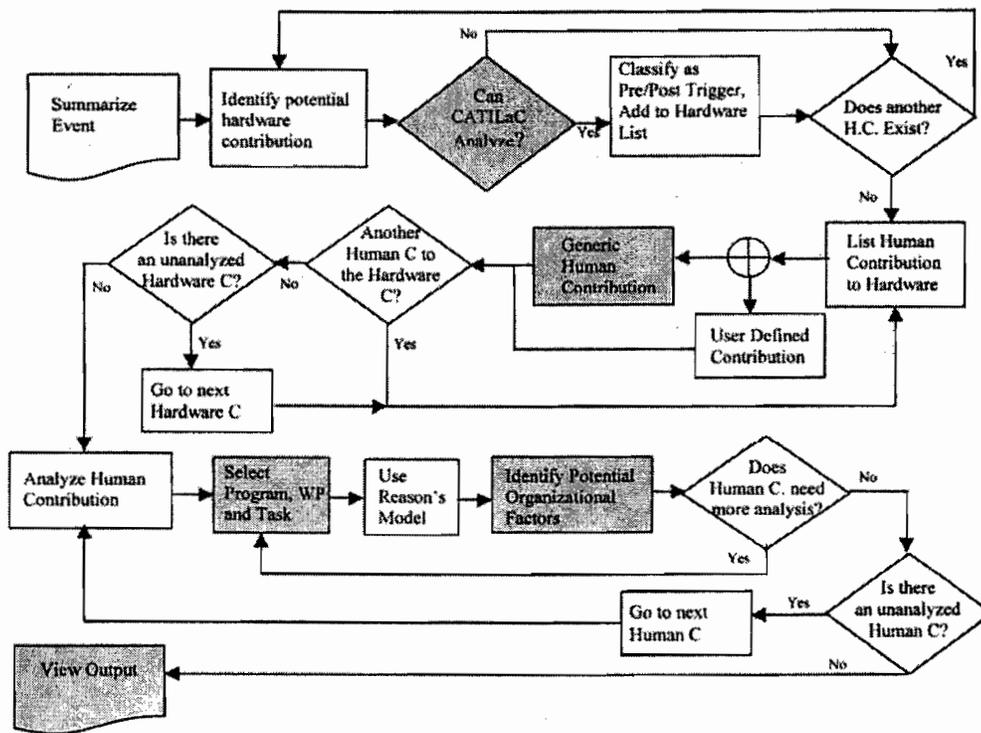


Fig. 4. CATILaC flowchart. The shaded boxes represent the tasks for which guidance is provided in the package. 'C' is used to stand for 'contribution'.

the input data in a series of tables and displays the result of the analysis in various reports. The application itself does not perform any analysis or manipulation of the data that the analyst enters; it merely takes the input information and stores and organises it for easy access later.

The software logic is outlined in Fig. 4. Each row on the flowchart represents the tasks that are carried out on each of the three input forms.

4.2. Guidance

CATILaC provides guidance to assist the analyst in inputting appropriate information in each of the forms. This guidance includes a tool to assist in identifying analysable hardware contributions, multiple examples of human contributions and unsafe acts, and a listing of important organisational factors. The areas for which guidance is provided are shown as shaded boxes in Fig. 4.

The hardware contribution analysis tool was developed because the CATILaC methodology is not useful for all hardware failures across the board. Because the methodology is focused on latent conditions, it is best used on hardware contributors that were known prior to the event, or could have been predicted before the event. Latent failures and those active failures that are a result of known conditions provide the most insight into latent contributions. Using hardware failure categories developed by Kumomoto and Henley (1996), an algorithm was developed to sort potential hardware contributions. The purpose was to assist the analyst in deciding which contributions to include in the analysis.

Since the goal of the incident investigation methodology is to identify and analyse latent conditions leading to incidents, naturally the algorithm must be designed such that hardware failures resulting from identifiable latent conditions are identified. The most common of these hardware failures are those classified as latent. Latent failures are problems within a system that were known prior to the incident (e.g., a faulty seal that was not repaired), or which existed in the system prior to the incident but had not yet been recognised (e.g., a diesel generator fails to start on demand due to a fault introduced during the previous testing cycle). It is these latent failures that can be associated with latent conditions within the organisation. On the other hand, unanticipated spurious occurrences, or random failures, should not be included in the analysis since attempting to identify organisational issues associated with this type of failure does not appear to produce insightful results. It is important to note, however, that declaring a failure to be random is not always an easy distinction. Care must be taken to ensure that all potential human contributions and underlying conditions have been taken into account before classifying a failure as random.

Kumomoto and Henley define several hardware failure

Table 1. Hardware failure classifications, from Kumamoto and Henley (1996)

Failure classification	Category	Definition
Component status	Mechanical	Device unusable due to component failures
	Functional/interface	Device usable but fails due to interfacing devices or lack of signal
Unavailability cause	Primary	Component unusable and repair required due to causes within the design envelope
	Secondary	Component unusable and repair required due to past or present stresses outside of design envelope
	Command	Component unavailable due to signal or noise, no repair needed.
Failure source	Hardware induced	Caused by the failure of another component
	Human induced	Caused directly or indirectly by human action

classification schemes made up of mutually exclusive and exhaustive failure types. These include mechanical/functional/ interface, primary/secondary/command and hardware induced/operator induced. Table 1 defines these classification schemes.

We have made slight modifications to the component status classification, changing the term 'mechanical' to 'mechanical/electrical' in order to better reflect all types of component failures, and the functional and interface failures were combined into a single category. Also, in the failure source classification, the term 'human induced' was modified to 'operator induced' in order to reflect the idea that all failures are in some sense human induced and the only distinction to be made was between those directly caused by an operator and those directly caused by hardware action. For example, maintenance errors would most likely fall into the category of hardware induced. The hardware component failed during the event, but the cause of the failure was due to improperly done or inadequate maintenance work. The distinction that we are seeking is between contributions that began due to hardware failures versus contributions that began due to operator action, keeping in mind that both types of failure have human actions (e.g., maintenance) at their roots. The final change we made was to add another failure source category, 'Maintenance/Testing Induced', to take into account components that would be functional but are out of service for some reason. This type of unavailability is categorised as functional/interface since the device is usable but is out of service. All other terminology was left as it was.

The algorithm asks the analyst to classify a potential hardware contributor as either being mechanical/electrical (M/E) or functional/interface in nature (F/I). If the contributor is F/I, the analyst must decide whether it is

hardware induced or operator induced or maintenance/testing induced. Hardware-induced and maintenance/testing-induced F/I failures should always be included in the analysis. Operator-induced F/I failures should probably be included as well, but require some special treatment in the programme and may be omitted if the facility has a separate operator action analysis programme in place. If the contributor is M/E, the analyst must decide whether it is a primary, secondary or command failure. Primary hardware failures should always be included. However, to make a further distinction between types of secondary and command failures, we introduce two other classifications into the algorithm: pre- versus post-trigger and known versus unknown failures. Pre-trigger secondary failures and known command failures should be included, while post-trigger secondary and unknown command should not be included. Post-trigger secondary failures are those non-latent failures that occur due to a component being subjected to stresses outside its design envelope. In other words, they occur after the event and are usually caused by the primary failures of other components. As such, given the circumstances surrounding the failure, it was an expected response to the unusual events in the system and thus does not require analysis. Unknown command failures are functional failures due to problems with signal or noise within the system that had not been experienced or anticipated before the event. If no cause for the failure can be ascertained, analysis will not be useful; rather the failure should be added to the facility's failure-tracking system.

Using these steps, the output of the algorithm is a decision about whether the potential hardware contribution may merit further analysis. As with any other analytical method, however, the analyst must take care to evaluate the results carefully as to whether or not they make sense. The algorithm is only a tool that can help the analyst obtain better results; it is up to the analyst to make the final decision about which hardware contributions should or should not be included in the analysis.

In addition to the hardware algorithm, we have also provided guidance for the analyst when it comes time to choose the human contributions to the previously input hardware contributions. While the analyst can type any human contributions into the form, he can also select a contribution from a drop-down menu that lists several commonly seen human contributions. The list of examples of generic human contributions was developed after examining several operating events and identifying broad categories of common human issues. In developing this generic listing, it was discovered that many of the same human contributions occur in multiple events at multiple facilities.

The following generic human contributions are included in CATILaC:

- confusion/error in operator action;
- failure to notice/recognise problem;
- incomplete procedures provided;
- known problem not reported;
- management rejects maintenance/design change;
- no action taken after precursor event;
- problem repaired incorrectly/incompletely;
- procedures not followed;
- reported problem not repaired (other reason).

The results of the operating experience review showed that problems involving failure to take action on known problems are most common. Errors (operational or otherwise) caused by procedure problems, failure to use industry operating experience and inadequate responses to precursor events are also commonly seen (Weil and Apostolakis 1999). All of the incidents analysed to date have one, if not more, of these problems, some occurring multiple times in a single incident. Most of the contributions listed fall into one of the three common categories discussed above. For example, errors caused by procedure problems can fall into the categories of incomplete procedures provided or procedures not followed.

Note that human contributions can be either active failures, such as operator actions, or latent failures, such as the failure to report a known problem. The latencies that led to these contributions will be identified during the analysis. The listing of the human contributions to each hardware contribution is straightforward, usually involving maintenance issues. The listing of human contributions to operator contributions is slightly more complex as the operator action itself is sometimes the human contribution, and there may also be other human actions that led to the operator contribution. For example, an operator may not perform correctly because he was not informed about a piece of equipment that was taken out of service. In developing the generic human contribution listing, we have included both of these types of failures.

The list of generic human contributions can be used to provide a basis for inputting more detailed and incident-specific human contributions, or it can be used exclusively in order to track these common problems at a facility. Six events were analysed and the analysis results confirmed the frequent occurrence of these contributions. There were, on average, about five human contributions per event. Presently the sample size is too small to draw any real conclusions; however, as expected, 'reported problem not repaired' occurs most frequently. However, this may only be because 'reported problem not repaired' is a very broad category that contains many possible human contributions such as inadequate management of maintenance backlog, or a planned repair that has not been implemented, or a delay in implementing a repair due to worker or part

availability. With more data, it is possible that this category should be subdivided to reflect these distinctions.

As with the hardware contribution help tool, the sample human contributions are not meant to be the final guidance. The analyst can input his own human contributions at any time. Often, in fact, more detail is appropriate for describing the human contributions. For example, if the analyst were not interested in attempting to look for common contributors or to gather data on frequencies of contributions to specific tasks, it would be more helpful to include a more detailed description of the human contribution. Being generic, the human contributions provided do not provide a large amount of detail concerning the human contribution. Including more detail in the analysis will be helpful in understanding how the human contributions fit into work processes and tasks and how they connect to organisational deficiencies.

To aid in the analysis of the human contributions and to assist the analyst in getting started, a generic set of work processes specific to nuclear power facilities is included in the work process database. We have included the following seven work processes:

- procedure modification;
- root-cause analysis;
- condition reporting;
- operating experience review;
- corrective maintenance ;
- preventive maintenance ;
- design change.

While there is no claim that this list represents a complete database of work processes that exist at a nuclear plant, the listing is complete enough to allow for basic, non-plant-specific analysis. Most of the work processes we have included in the database were developed based on a review of the processes of several nuclear power facilities, but some are based on processes found during the analysis of operating experience.

Because work processes are so crucial to the CATILaC methodology, let us take a moment to discuss their role in the methodology and their limitations. The work process is the tool that CATILaC uses to place human actions properly within the context of the organisation so that underlying organisational factors can be found and corrective actions can be appropriately directed. By knowing which work processes, and which tasks in particular, are susceptible to problems, and which particular organisational factors are deficient, the latent conditions that lead to events can be reduced or eliminated. As has been mentioned before, most work processes follow a generic sequence of tasks in order to accomplish work. The corrective maintenance work process, shown in Fig. 1, exemplifies the general structure. This has the added

benefit of being able to direct corrective actions to a particular task that is common to many work processes, for example, prioritisation, or to particular organisational factors that may be deficient in multiple areas.

While work processes are extremely useful in helping us understand how an organisation accomplishes work, they are limited by only being able to describe organisations that have routine operating tasks and formalised procedures, i.e., machine bureaucracies. Organisations that do not have large operating units or centralised decision-making do not accomplish their work through these types of standardised work processes. As a result, the CATILaC methodology would not be useful for such organisations.

The final feature of CATILaC that will be discussed is the list of organisational factors provided with the programme. The list includes eight factors thought to have a high degree of impact on the organisation. The analyst can modify or change this list as he sees fit.

The provided list is based on the work of Jacobs and Haber (1994). These authors defined 20 common dimensions, or factors, related to organisational performance. They divided their 20 dimensions into five categories: administrative knowledge, communications, culture, decision-making, and human resource allocation. While developing the first version of the incident investigation methodology, Weil and Apostolakis (1999) examined the 20 organisational factors and found a great deal of overlap among them as well as several factors that they considered to have little impact on performance. By combining these insights with the result of a review of operating experience, they reduced the list to six organisational factors: communication, formalisation, goal prioritisation, problem identification, roles and responsibilities, and technical knowledge. In doing this, they hoped to improve the efficiency of analysis and to improve the distinction between the various factors.

Communication factors were combined into a single category, and because culture issues are, by nature, a pervasive problem in all events, they were eliminated from the list. Organisational learning and training-related factors were also eliminated since these areas are work processes in themselves, and the coordination of work was also eliminated since that is the definition of a work process. Weil and Apostolakis also chose to eliminate the factors of centralisation, resource allocation and personnel selection, judging that these areas could be subsumed into other organisational factors.

In compiling the organisational factors to be included in the database, we chose all of the factors originally listed by Weil and Apostolakis (1999). In addition, resource allocation and personnel selection were added to the list because we feel that they can offer increased insight into events being analysed. Personnel selection is an important issue in work processes and is not fully recognised in any of

Table 2. Organisational factors included in CATILaC

Organisational factor	Definition
Communication	Exchange of information, both formal and informal (includes external, interdepartmental and intradepartmental)
Formalisation	There are well-identified rules, procedures and/or standardised methods for routine activities and unusual occurrences
Goal prioritisation	Plant personnel acknowledge and follow the stated goals of the organisation and the appropriateness of those goals
Personnel selection	Plant personnel are identified with the requisite knowledge, experience, skills and abilities to perform a given job
Problem identification	Plant personnel use their knowledge to identify potential problems
Resource allocation	Manner in which the plant distributed its resources (esp. financial). Refers to the actual and perceived distribution
Roles and responsibilities	Work activities are clearly defined and plant personnel carry out those work activities
Technical knowledge	Depth and breadth of requisite understanding that plant personnel have regarding plant design and systems, and the phenomena and events that bear on their safety and reliable operation

the six original factors. Resource allocation may be a crucial factor impacting plant decisions to carry out or postpone corrective maintenance work. Weil and Apostolakis (1999) felt that this factor was present in goal prioritisation; however, further examination has shown that there is a distinction between personnel accepting and agreeing with goals (goal prioritisation) and the distribution of financial and human resources (resource allocation) that is very important in understanding an event. Although goal prioritisation and resource allocation often go hand-in-hand, making a distinction between the two factors can provide greater insight into appropriate corrective actions. The organisational factors included in CATILaC are listed in Table 2.

5. EVENT ANALYSIS

5.1. Testing the Method

To fine-tune the procedures as well as to provide data to test the usability of the software, several events were analysed using the latent condition identification methodology and the CATILaC software package. The information used in the analyses is from NRC AIT reports. These reports are issued by the NRC in response to significant events at a nuclear plant. NRC investigators are sent out to evaluate the utility's RCA and to provide their own comments and conclusions about why and how the event occurred and how the plant succeeded or did not succeed in responding to the event. Everything from the pending

corrective maintenance on crucial equipment to the suitability of the emergency response is evaluated by the AIT.

Accident reports usually have many weaknesses, including inconsistencies, excessive cross-referencing and ambiguities. It is impossible for them to contain all relevant information and the reader is limited by the scope of the analysis chosen by the authors (Johnson and Botting 1999). Of particular importance is that AITs are not geared toward organisational issues, nor do they make reference to work processes or programmes in which deficiencies were found. The reason that AITs are used here for this preliminary testing and analysis is that they represent the best, most detailed source of information on events at nuclear power plants. The team uses a high degree of detail, which is particularly helpful in the analysis because it reduces the need to infer organisational issues. Keeping these limitations in mind, a sample event will now be discussed to demonstrate the CATILaC methodology.

It is also important to note that we have used the generic work process database to complete the analysis. Without plant specific information, the results are sometimes no more than educated guesses. As mentioned in the description of the methodology, tailoring CATILaC to the facility at which it will be used is crucial to obtain valid and useful results.

5.2. Sample Event Analysis

The event described here is a simplified version of a flooding event that occurred at a US nuclear facility. To demonstrate the method without burdening the reader with excessive nuclear power plant technical details some of the hardware contributors that occurred in the actual event have been eliminated or simplified.

The plant was shut down and was preparing to begin operation when the event occurred. The event did not pose any risk to the public and its safety consequences were minimal; however, it resulted in a delayed start-up of the plant, a costly clean-up operation and increased regulatory attention on the utility.

Smoke from cutting and grinding maintenance work in one of the plant buildings actuated the plant's fire protection system. When the fire protection system was actuated due to detection of smoke, the sprinklers did not activate, but the normally dry sprinkler headers filled with water. The activation of the main fire water pumps in response to the pressure drop caused by the actuation of the system resulted in a water hammer, or pressure wave, which ruptured an isolation valve in the plant's fire protection system.

Maintenance procedures for the cutting and grinding activities did not provide appropriate guidance to prevent system actuation. A similar event had occurred five months

prior to the flooding event when maintenance activities caused pre-action of the fire safety system and water hammer without pipe rupture. The corrective actions from that event, including any procedure changes, had not been implemented.

The pipe rupture led to the flooding of a stairwell of the reactor building with approximately 163,000 gallons of water. Due to an improperly closed watertight door, water from the stairwell flowed into the adjacent residual heat removal (RHR) pump room, flooding it with 19 feet of water. Plant workers were aware that extra care was required to ensure that the door was completely closed and that the latching rods were fully inserted into their receptacles. If a worker turned the closing mechanism too quickly, the rods would bounce out of the receptacles into the retracted position. Although these problems were well known among plant personnel, no formal documentation of the problem existed. Also contributing to the incident was the fact that the door position was recorded, but the door was not alarmed. This made it very difficult to be sure that it was closed properly.

The flooding situation was exacerbated due to a problem with the closing mechanism of the cross-connect valve that connected the RHR pump room to the adjoining low-pressure core spray (LPCS) pump room. When the valve failed to close as designed, it caused flooding in the adjacent room as well. However, the adjacent room flooding was not as severe as in the RHR pump room since the LPCS pump motor was not submerged. See Fig. 5 for a schematic of the flooded region.

[insert fig. 5 near here]

It was known prior to the event that the cross-connect valve was degraded since it had failed to close during testing. A work request on that valve was made over six months before the event, but no corrective actions or compensatory measures had been taken. In addition, neither the maintenance rule nor the in-service testing

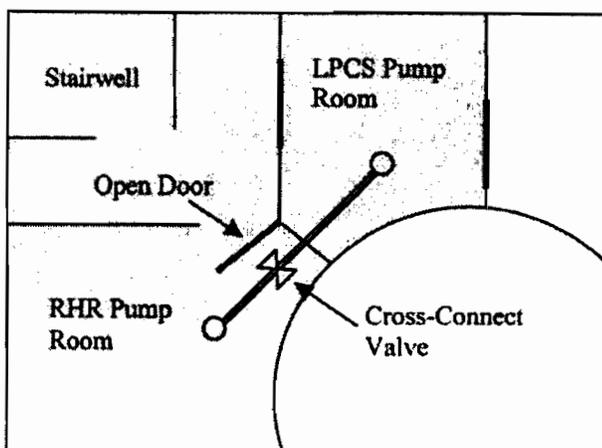


Fig. 5. Schematic of flooded region in sample event.

programme covered the valve. In an attempt to eliminate unnecessary maintenance activities the plant had also taken the valve off the 60-month maintenance list. The last preventive maintenance had occurred over three years before the event.

Six minutes after the fire pumps activated, it was verified that an actual fire did not exist and control room operators isolated the fire protection system in the affected areas, and 12 minutes after the activation the fire pumps were turned off. Water was drained from the stairwell and pump rooms using portable pumps and hoses after repeated chemistry analysis assured that there was no radioactive contamination.

5.2.1. Hardware and Operator Contributions

Hardware:

1. The valve ruptured due to a water hammer caused by actuation of the fire protection system due to smoke from maintenance activities.
2. The watertight door between the stairwell and the RHR C pump room was not closed properly, thus allowing water into the RHR C pump room.
3. The sump isolation valve failed to close as designed, thus allowing water to enter the LPCS pump room.

Operator:

There were no active operator actions that contributed to the event.

5.2.2. Classification of Constituents as Pre- or Post-Trigger

The trigger of the event was the cutting and grinding maintenance activities. The fire protection system pipe rupture due to water hammer was a post-trigger constituent since, although the problem was known, the rupture itself did not occur until the fire system was actuated. The watertight door closing problems and the sump isolation valve failure to close were both pre-trigger. These components were in a damaged state before the incident and had they been undamaged the incident could have been avoided or mitigated.

5.2.3. Identification and Analysis of Human Contributions to Hardware Contributions

5.2.3.1. Fire Pipe Valve

The problem of water hammer in the fire protection system after actuation and the potential for actuation due to cutting or grinding maintenance activities had already been exhibited in a prior event at the plant. Despite this event precursor, no corrective actions had been taken to reduce the possibility of water hammer if the fire protection system actuated without fire. In addition, the procedure that governed cutting and grinding work had not been modified

to include more detail about how to prevent fire system actuation. Although the maintenance workers followed the procedure before the event, the current procedure at the time provided inadequate guidance to have prevented the event.

The lack of corrective actions taken after the precursor water hammer event reflects a potential problem in the corrective maintenance work process (Fig. 1). The previous event had apparently been documented in the plant's corrective actions process, but the corrective actions had not yet been implemented. Based on this information, it appears that the deficient task may be prioritisation. This reflects a fallible decision on the part of management not to give the modification of this system a higher priority and may reflect an organisational problem with resource allocation. While the plant most likely has a policy for correcting even low-priority corrective actions within a certain period of time, there is only a limited amount of resources that can be divided among the many corrective action tasks. As a result, certain corrective actions may not be implemented as quickly as necessary. This may reflect a problem with the organisational factor of resource allocation.

Management's problem with prioritisation tasks may also have influenced the failure to make changes to the procedures governing work with ignition sources after the precursor event occurred. This seems to reflect a deficiency in either the maintenance work process (whichever maintenance work process was responsible for coordinating the cutting and grinding activity, either corrective or preventive) in properly documenting the problems they encountered during the maintenance work. The planners should have included a warning in the work package about the previous incident and advised the crew on how to avoid actuating the fire protection system while cutting and grinding. Alternatively, the procedure writers should have modified the procedure to include better guidance. Both of these deficiencies are unsafe acts that were most likely a result of the fact that the planner/procedure writer may not have been aware of the previous incident. This can be linked to the line management deficiency of not sharing important operating information with plant staff, which might have been caused by poor documentation on the part of the maintenance staff. This suggests a problem with communication. If the problem occurred because the organisation has ill-defined guidance for incorporating operating experience events into procedures and work packages, a deficiency in formalisation could exist as well. The problems in this area fall into the broad category of organisational learning issues.

5.2.3.2. Stair/RHR Door

As mentioned in the event description, the closing problem with the watertight door between the stairwell and the

RHR pump was common knowledge prior to the incident. Plant staff was aware of the problem and knew that the door required extra attention; however, the problem was never officially reported. The corresponding programme is corrective action, and the pertinent work process is the condition reporting work process. The human contribution did not occur in any of the tasks within this work process, but rather in the initiation of the process.

Since no one ever came forward to initiate the condition reporting process, the condition was never officially reported for repair. Line management may have caused this problem by not encouraging the use of the condition reporting system for all noted deficiencies; however, the AIT does not go into sufficient detail to say for certain if this is true. This line management deficiency is connected to the organisational factor of problem identification. This may reflect a problem with the plant's safety culture. Specifically, problem identification may be an issue since the problem with the door was never reported to management. This is related to the 'questioning attitude' recommended by the International Nuclear Safety Advisory Group in its definition of safety culture (INSAG 1991). However, safety culture is too far reaching an issue to be of use when cited in an incident report (Weil and Apostolakis 1999). In this event, the specific problem was that plant personnel did not use their knowledge to identify a potential problem to management. They were either not aware or not interested in the overall management policy of supporting plant safety through the use of the condition reporting process to identify problems in the plant.

5.2.3.3. Sump Valve

As with the fire pipe rupture, plant personnel knew that the sump valve was not functioning properly and made a report about the problem. However, as before, the problem was not repaired. Making it even more difficult to correct this problem was the fact that this sump valve, as well as all sump cross-connect valves in the plant, had been removed from the preventive maintenance programme. Management had decided that performing any regularly scheduled maintenance on these valves was unnecessary.

This reflects a problem with the preventive maintenance work process. However, the way in which items are added or removed from the preventive maintenance programme is not clear in the work process. Since we do not really know at what point in the process, if it is part of the process at all, or for what exact reasons the valves were removed, we cannot name a task within the modification process. Considering the valves unnecessary and removing them from the maintenance schedule was a fallible decision on the part of plant management. A potential organisational factor leading to these fallible decisions is resource allocation. We have chosen to cite resource allocation as

opposed to goal prioritisation because, based on the description of management's decision to remove the valves from the schedule, it seems that their decision was based on a need to save money rather than a need to accomplish another pressing task. Because of this distinction, resource allocation is the appropriate factor to cite. However, since the cited organisational factors are not meant as definitive answers, it is possible that upon further investigation deficiencies in goal prioritisation may also have contributed to the problem. By examining the planning and scheduling task of the preventive maintenance work process more carefully, the analyst can devise appropriate corrective actions in this area.

A problem was discovered with the closing mechanism of the valve six months before the incident and the valve was tagged with a work request reflecting this deficiency. However, no corrective action was performed and no compensatory measures were taken in response to this work request. This demonstrates a deficiency in the corrective action programme in the corrective maintenance work process. The task where the human contribution occurred was prioritisation. Based on the fact that the valve had already been removed from the preventive maintenance schedule, we can assume that plant management felt the valve was not crucial to plant performance (another fallible decision). This failure may reflect a continuing problem with resource allocation, similar to the problem with the delay in implementing corrective actions for the water hammer precursor.

5.2.4. Output

1. Possible managerial and organisational deficiencies:
 - resource allocation in the prioritisation task of the corrective maintenance work process and in the preventive maintenance work process;
 - communication and formalisation in the documentation task of the corrective maintenance work process;
 - problem identification in the initiation of the condition reporting work process (perhaps associated with problems with safety culture).
2. Dominant contributors:
 - Most issues involved in the incident stemmed from management not implementing corrective actions to fix known and reported problems. The dominant contributors were deficiencies in resource allocation in the corrective action programme and problems with initiation of the condition reporting process.
3. Consequences:
 - Consequences of this event included delayed start-up of the plant, expensive repair and clean-up operations, and increased regulatory oversight.

5.3. Discussion

As has been seen in other events (Weil and Apostolakis 1999), the flooding event was caused by a combination of hardware failures and organisational deficiencies. In the sample event, unrepaired faults in the system combined with poor procedures and lack of attention to precursor events to result in the extent of flooding that occurred. Using CATILaC, however, the analysis can go much beyond that. Not only are the broad organisational issues recognised, but also the line management deficiencies and unsafe acts that contributed to the event. Most important is that specific tasks within work processes have been identified as being deficient and corrective actions can be developed to repair the organisational deficiencies affecting those tasks.

Broad deficiencies in safety culture at the plant appear to be responsible for these problems. By making improvements to the way corrective actions are prioritised and corrected and perhaps by reducing the backlog of pending corrective actions, the plant could overcome these difficulties.

6. CONCLUSIONS

We have developed an incident investigation methodology to identify latent conditions that have led to abnormal events and to suggest potential organisational deficiencies that may exist in a system. The process involves the identification of hardware contributors to the event and the human contributions to them. Each human contribution is associated with one or more deficient work processes and these deficient work processes are analysed using Reason's type-token methodology to identify organisational deficiencies.

Although it incorporates much of the current thinking in event analysis, the method separates itself from other incident investigation techniques because it uses work processes as a tool for placing the human contributions to an event into the context of the organisation. The methodology is especially suited to identify latent conditions in highly structured organisations, which lend themselves to work process analysis. By taking advantage of the predictable way that work gets accomplished in such organisations and the centralised upper management structure, the analyst is able to pinpoint the locations of deficiencies within the organisation. If an organisation is not a machine bureaucracy, the methodology becomes less useful. In that case, another analysis technique, such as Tripod-Beta, which identifies latent conditions but does not depend on the structure of the organisation, could be used to produce insightful results.

In addition to the methodology, we have developed a software package, CATILaC, to assist the analyst in

applying the methodology and storing the results. The software offers the analyst several useful tools such as a work process database, a hardware contribution selection tool, and a list of common human contributions to operational events. CATILaC provides a tool to store and organise event information, but it is up to the analyst to implement the methodology and to draw conclusions about causes of human contributions and organisational issues that may have created latent conditions within the system. While this offers a great deal of flexibility, it also forces the analyst to have a great deal of analysis and insight available concerning the event, the organisational structure, and the plant's operating history during the process. The value of tools such as CATILaC is not that they can provide this information to the analyst, but, rather, that they assist the analyst in asking the proper questions in order to locate the deficiencies in organisational factors and work processes that contributed to an incident.

Since CATILaC is designed to be a computerised analysis aid, we believe that there are ways to assist the analyst even more in locating these organisational deficiencies. For example, if a large set of events were analysed using the methodology, it is possible that the results could be used to draw general conclusions about the way that events occur and the factors that cause them. We used this technique to some extent in the development of the generic list of human contributions that is provided; however, many more events would need to be analysed before this data could be used to assist the user in the analysis of the human contributions.

One idea is to develop a correlation between particular tasks within work processes and commonly deficient organisational processes. Then, once the analyst selects the work process and task in which a deficiency exists, he or she could be presented with a list of potential organisational influences. This could even be expanded to include potential unsafe acts, if enough data were available. Based on the events that have been analysed so far, it appears that certain tasks within some work processes seem to reflect common organisational deficiencies. For example, the prioritisation task in the corrective maintenance work process is often deficient. As always, however, these additional tools do not serve to automate the methodology. Rather, they just provide additional information to the analyst, who has the responsibility to question that information and to use it as he or she sees fit.

As has been mentioned, the output of this methodology is a list of latent conditions that played a role in a particular event and that could affect plant performance in the future. Specifically, organisational factors are used to identify latent problems within the organisation itself that may have played a role in an event but still remain undetected. Through the methodology, these organisational factors are linked to a programme, work process and task in which

deficiencies in the area of that factor contributed to the event.

These results can be used to direct efforts to improve performance. Management can examine the findings from a CATILaC analysis and identify specific areas at which corrective actions should be directed. Because the results identify potential areas of vulnerability, they can be used in a manner similar to probabilistic risk assessment (PRA), that is, as a tool to identify options for the management of risk within an organisation.

Using results from CATILaC to direct corrective actions to specific tasks and work processes can be an effective way of improving plant performance. The next logical step in this work would be to develop a way to measure the effectiveness of these corrective actions. Currently, no metrics exist for measuring the effect of corrective actions on organisational issues. Improvements in this area could help to quantify the degree to which the results can be used to improve the way the organisation accomplishes work.

Acknowledgements

This work was funded in part by the University Research Consortium, a joint venture between the Idaho National Engineering and Environmental Laboratory (INEEL) and MIT. We thank David Gertman of INEEL for his support. We also thank EQE International for making the Tripod-Beta software package available to us.

References

- ABS Group, Risk and Reliability Division (1999). Root cause analysis handbook: a guide to effective incident investigation. Government Institutes, Rockville, MD.
- Corcoran WR (1998). Root cause analysis: part of every engineer's toolkit. Presentation to the Massachusetts Institute of Technology American Nuclear Society Branch, November 1998.
- Davoudian K, Wu J-S, Apostolakis G (1994). Incorporating organizational factors into risk assessment through the analysis of work processes. *Reliability Engineering and System Safety* 45:85-105.
- EQE International (1999). TRIPOD BETA version 2 software user manual. EQE International, Aberdeen.
- Gertman D, Hallbert B (2000). Quantitative analysis of risk associated with human performance. Presentation to the Human Factors Subcommittee of the Advisory Committee on Reactor Safeguards, 15 March 2000. Nuclear Regulatory Commission, Washington, DC.
- INSAG (1991). Safety culture, Safety series no. 75-INSAG-4. International Atomic Energy Agency, Vienna.
- Jacobs R, Haber S (1994). Organizational processes and nuclear power plant safety. *Reliability Engineering and System Safety* 45:75-83.
- Johnson CW, Borring RM (1999). Using Reason's model of organisational accidents in formalising accident reports. *Cognition, Technology & Work*; 1:107-118.
- Kumamoto H, Henley EJ (1996). Probabilistic risk assessment and management for engineers and scientists. IEEE Press, Piscataway, NJ.
- Mintzberg H (1979). The structure of organizations. Prentice-Hall, Englewood Cliffs, NJ.
- Mobley KR (1999). Root cause failure analysis. Newnes, Boston, MA.

NRC (2000). Technical basis and implementation guidelines for a technique for human event analysis (ATHEANA). Report NUREG-1624, Rev 1, US Nuclear Regulatory Commission, Washington, DC.

Reason J (1990). Human error. Cambridge University Press, Cambridge, UK.

Reason J (1997). Managing the risks of organizational accidents. Ashgate, Aldershot, UK.

Tuli RW, Apostolakis G (1996). Incorporating organizational issues into root-cause analysis. Trans IChemE 74B:3-16.

Weil R, Apostolakis G (1999). Identification of important organization factors using operating experience. In Proceedings of the third international conference on human factor research in nuclear power operations, Mihama, Japan.

Correspondence and offprint requests to: G. Apostolakis, Department of Nuclear Engineering, Room 24-221, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA. E-mail: apostola@mit.edu