ELSEVIER

Reliability Engineering and System Safety **45** (1994) 85–105
1994 Elsevier Science Limited
Printed in Northern Ireland
0951-8320/94/$7.00

Incorporating organizational factors into risk assessment through the analysis of work processes

Keyvan Davoudian, Jya-Syin Wu, & George Apostolakis*

School of Engineering and Applied Science, 38-137 Engineering IV, University of California, Los Angeles, California 90024-1597, USA

It is proposed that the impact of organizational factors on nuclear-power-plant safety can be determined by accounting for the dependence that these factors introduce among probabilistic safety assessment parameters. The work process analysis model (WPAM) is presented as an analytical tool, in which these dependencies are investigated via work processes. In this paper, WPAM is applied to pre-accident conditions within the framework of the maintenance work process.

1 INTRODUCTION AND LITERATURE REVIEW

Industrial experience and research findings have shown that major concerns regarding the safety of nuclear power plants and other complex industrial systems are not so much about the breakdown of hardware components or isolated operator errors as about the insidious and accumulated failures occurring within the organization and management domains.[1–5] The International Nuclear Safety Advisory Group (INSAG) has maintained that the establishment of a safety culture within an organization is one of the fundamental management principles necessary for the safe operation of a nuclear power plant (NPP).[6] Furthermore, Ref. 7 contends that the 'achievement of total system safety, both human and technical, is dependent on the existence of a single safety culture which must be properly defined'. Based on this understanding, then, an ideal organization at a nuclear power plant is one in which a safety culture is formally established in order to govern the actions and the interactions of all individuals who are engaged in activities related to the station's operation. Such a culture helps not only to ensure safe practices at the plant, but also to create an environment of safety consciousness for every individual who works there.

Numerous recent incidents highlight the importance of a plant-wide and, in fact, an industry-wide safety culture. For example, as stated by INSAG, the Chernobyl accident was in large part due to the absence of a widespread safety environment. Indeed, layers of safeguards and safety precautions, ranging from design and safety reviews to operation were breached, one after another, because of an imprudent attitude toward nuclear safety.

The concept of safety culture is further expanded upon in a preliminary study by Wu *et al.*[9] Here, the authors identify four characteristics of a safety culture that are important to the safe operational environment of a nuclear power plant: the safety knowledge acquired by utility and plant personnel; the attitude of plant personnel toward plant operation; the choice of plant performance goals; and the establishment of lines of responsibility and communication. Besides safety culture, however, there are many other organizational factors that may have an impact on safety performance at nuclear power plants. The Nuclear Regulatory Commission (NRC), for example, has explored some of these factors (e.g., communication, decision making, standardization of work, organizational learning, and management involvement).[10] Marcus *et al.*,[11] relying primarily on data that are readily accessible, have conducted empirical studies that investigate the relationship between organizational performance and safety.[11] More recently, the research on the impact of organizational factors on plant risk has resulted in a list of twenty such factors (or dimensions).[12] By themselves, the organizational factors can only help in

* To whom correspondence should be addressed.

locating areas within an organization where 'weak links' may exist. In order to be able to assess the impact of these weaknesses on plant safety, however, structured models are needed that go beyond qualitative analyses.

Having recognized the importance of safety culture and, in general, the significance of the influence of organizational factors on plant safety, the next question one might ask is what is the extent to which such influences are accounted for in current probabilistic safety assessment (PSA) methodology. As pointed out by Bley *et al.*,[13] an issue of debate, in recent years, has been the contention by the nuclear industry that the existing plant-specific data (e.g., failure rates) that are used in PSAs already contain in them the influence of organizational factors. While this may very well be the case, it is important to realize that the state of the art in current PSA methodology is such that organizational dependencies between hardware failures, between human errors, and between hardware failures and human errors are not modelled explicitly. Instead, the current methodology is confined mostly to models of isolated human errors and equipment failures.[14] Therefore, models must be developed that focus primarily on capturing the common-cause effect of organizational factors on parameters such as equipment failure rates. This, in effect, is analogous to the common-cause failure (CCF) analysis of hardware, where the 'basic' failure probabilities are left alone and an additional term (containing the β factor, for example) is introduced to account for the failure of redundant equipment due to a single cause.[15] The bottom line, as stated by Bley *et al.*,[13] is that 'any model that fails to examine the organizational factors is guaranteed to underestimate the overall risk by an undetermined amount'.

The need to account for the common-cause effect of organizational factors has also been recognized in other industries. For example, Bellamy *et al.*[16] state that 'when historical data on failure rates, such as pipework failure rates, is used in QRA (quantified risk assessment), human error is implicitly included as just one of the many contributing factors to the failures. Therefore, differences between hazardous installations in the way they are managed, maintained and operated will not be taken into account in a conventional (hardware) QRA.' Furthermore, referring to offshore platforms, Paté-Cornell & Bea[17] state that 'a large fraction of (the probability of failure) may be attributable to errors and bad decisions rooted in the organization itself, which affect the PRA inputs but are not accounted for explicitly (even though their effects may appear implicitly in performance statistics and expert opinions)'. Also, with regard to the Challenger incident, Vaughan[18] reports that 'intra- and interorganizational relations are characterized by structurally engendered weaknesses that contribute to technical system accidents. Because the sophisticated formulas used to estimate risk in technical systems do not acknowledge the possible organizational contribution to technical failures, risk is always underestimated'.

In attempting to assess the impact of organizational factors on plant safety, two major tasks must be accomplished. First, models of the organization as a whole are needed that shed light on the way(s) in which organizational factors may impact on the safety of the plant. Second, models are needed which allow for the quantification and incorporation of this impact into PSAs. Arguably, the largest obstacle in the way of accomplishing the first task is the fact that, quite frequently, an informal organization is superimposed upon the formal work organization.[4,5,19] In other words, although most of the work in complex organizations is, in one way or another, standardized, individuals within the organization often depart from these standards in their daily routines. This paper focuses on the formal organization, so that the informal organization and its impact on plant safety are beyond the scope of this paper. Admittedly, in order to understand the informal organization, one must first understand the formal environment.

One description of the formal environment of a nuclear power plant is given by Haber *et al.*,[20] who specify five functional areas in order to describe the organizational structure of an NPP. These five functional areas are the strategic apex (top management), middle-level management, technostructure, support staff, and operating core. The authors specify the standardization of work as the prime coordinating mechanism in the NPP organization. This point is debatable, however, as the adherence of personnel to standards is one instance where the informal organization plays a major role. Also, as stated by Llory,[19] it should be kept in mind that 'the entire activity of the members of an organization cannot be formalized and proceduralized in detail'.

Reason's 'types-tokens' model[21,22] of accident causation describes the manner in which the attitudes and practices of different (hierarchical) groups within the organization can help to facilitate and/or proliferate the occurrence of human errors. In this model, types are defined as general classes of organizational failures and tokens as more specific failures related to individual situations. Reason's model provides some direction to the responses to questions such as: where and how within a system are unsafe attitudes translated into unsafe acts that are capable of breaching the defenses of the system? How can one identify organizational failures before they turn into serious accidents? Moreover, the model guides the analyst away from concentrating on what Reason calls 'tokenism', which is 'the tendency to treat human failures at a local level rather than within

the global context of the organization'. As reported by Wreathall and Appignani,[23] in a review of the Licensee Event Reports (LERs) for ten plants, the two nuclear power plants that reported the most inadvertent engineered safety features (ESF) actuations due to testing and maintenance employed discipline or counselling of the workers as the most frequent means of corrective action. In essence, the management at these plants relied on 'punishing the final human link (rather than) searching for root causes'. What may be even more significant (with regard to an overall organizational culture) is that the two plants mentioned were sister plants at a common site. Logically similar to Reason's model, the 'sociotechnical pyramid' developed by Hurst *et al.*, proposes a hierarchical model of accident causation.[24]

The Onion Model[25–27] conceives of the NPP as a series of 'englobing fields' that mutually interact, but keep their own identity at each level. The levels of the field begin with the general environment within which the corporation/utility must work. The Onion Model then proceeds downward and inward through the corporation, plant environment, division/departmental factors, work groups, and, ultimately, to the individual worker. Extending this work, Modarres *et al.* combine the onion model (now called the 'organization field model') with a 'diamond tree' to form an integrated framework that establishes the relationship between organizational factors and NPP safety.[28]

Wu *et al.*[9] maintain that two ways in which current PSA methodology can be improved include the re-assessment of probability distributions of the pertinent parameters to include organizational factors and the assessment of dependencies among these parameters. From the point of view of PSA, the parameters of interest include equipment failure rates, human error rates, component repair times, and the like, all of which appear in the unavailability expressions for NPP components/systems. What is more important is that in the model developed in Ref. 9, one can see clearly that each organizational factor may influence more than one parameter (within one system or among several systems), which causes dependencies to exist among these parameters.

Concentrating on the design phase of an offshore platform, Paté-Cornell and Bea[17,29] develop a PRA model in which the inputs (such as the rate of boat collisions during a time period) can be affected by decisions and errors made during this phase. The errors are further broken down into 'gross errors' (i.e. errors about which there is no controversy or ambiguity) and 'errors of judgment' (i.e. those that involve ambiguous or incomplete informaton), each of which is in turn rated as either a high-severity or a low-severity error. Using this model, the authors then show how (erroneous) decisions made by management can affect the probability of system failure. In the same spirit as the treatment of offshore platforms, Paté-Cornell and Fischbeck perform a PRA for the tiles of the space shuttle orbiter[30] and use the results to articulate several risk-management strategies.[31]

Finally, the model developed by Embrey also allows for both understanding and quantification of the effect of organizational factors on risk.[32] The pattern of accident causation is similar to that of Reason[21] and Hurst *et al.*,[24] that is, it consists of active, latent, and recovery errors which are caused by level-1 error inducing factors (such as poor instructions or procedures) which, in turn, are rooted in level-2 policy deficiencies (e.g. risk management). However, this is only part of a generic model called MACHINE (Model of Accident Causation using Hierarchical Influence Network) which shows that hardware failures and external events, in addition to human errors, can result in accidents.

According to Embrey, the quantification of the influence of organizational factors using MACHINE may be achieved through the use of influence diagram quantification methods. At each level, experts are asked to assign probabilities (or weights) that are conditioned upon the state of (combinations of) factors in the immediately-preceding level. For example, a typical question may be 'What is the probability that the quality of training will be high, given that both task analysis and feedback from operational experience are used in developing training?' Here, training is a level-1 factor and 'task analysis' and 'feedback from operational experience' are level-2 factors. The same procedure is followed until the final probability is calculated. Embrey also points out that the SLIM-MAUD[33,34] methodology can be used to obtain the probabilities. In such an application, the organizational factors would be accounted for through the evaluation of the performance shaping factors (PSFs), i.e. the level-1 factors mentioned above.

As its name implies, the work process analysis model (WPAM) uses nuclear-power-plant work processes as its backbone. Therefore, following an overview of WPAM in Section 2, Section 3 presents a discussion on the role and nature of work processes at NPPs. This is followed by an overview of probabilistic safety assessment methods in Section 4. Section 5 discusses the details of the first part of the WPAM methodology (WPAM-I) within the context of the maintenance work process. Finally, Section 6 contains a summary of the main topics.

2 AN OVERVIEW OF THE WORK PROCESS ANALYSIS MODEL (WPAM)

Figure 1 is an illustration fo the WPAM philosophy; that is, it demonstrates the ways in which organiza-

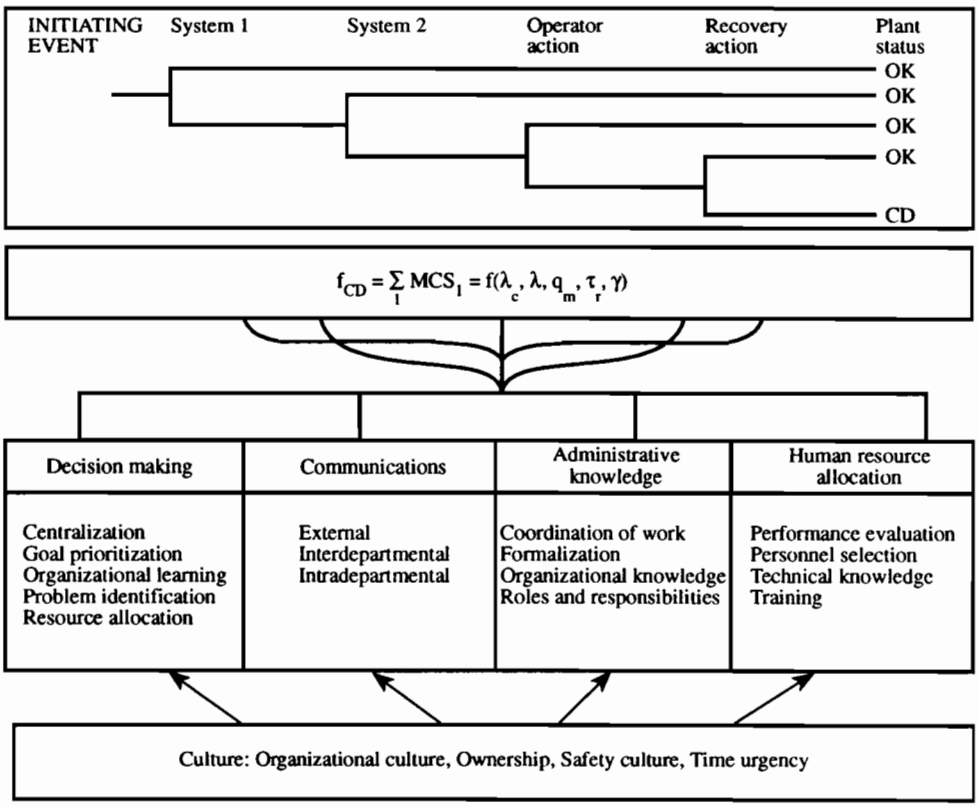

Fig. 1. Incorporation of organizational impact into PSA.

tional factors are viewed to impact on NPP safety. The top portion of the figure contains a simple example of an event tree for a typical accident sequence. As can be seen, the frequency of core damage (f_{CD}) is a function of hardware failure rates (λ), human error probabilities (γ), etc. The bottom portion of the figure consists of two levels of organizational factors: the top level, represented by the overall culture and its constituents, and the second level, represented by factors contained under decision making, communications, administrative knowledge, and human resource allocation. The link between the top and bottom portions of Fig. 1 is achieved by recognizing that any one or more of the organizational factors can influence the quality and efficiency of a given work process. This, in turn, will have an impact on personnel and/or equipment performance, with the effect being manifested in parameters such as λ and γ.

Several notes need to be made at this time. First, it must be pointed out that, in the present study, only pre-accident operations are considered, so that operator actions during a transient, for example, are not analyzed. However, as well be seen later, this does not preclude the analysis of dynamic situations which may have their roots in the routine operation of the plant. Second, the analysis is performed within the framework of the corrective maintenance work process, although, with some modification, the model that is developed can be made applicable to the testing work process (e.g. surveillance testing, in-service testing, etc.) as well. That is, corrective maintenance and testing are related. In fact, quite often, the former is initiated as a result of the latter. Therefore, even though a detailed analysis of testing is not presented in this study, whenever possible the discussion includes elements of both corrective maintenance and testing. The overview of PSA methodology that is presented in Section 4, for instance, contains unavailability expressions for both corrective maintenance and testing. Third, as has been alluded to before, WPAM concentrates on capturing the common-cause effect of organizational factors on NPP safety. In accomplishing this task, however, WPAM goes beyond conventional CCF analyses by considering organizational common-cause failures of not only similar, but also dissimilar systems and/or components. Finally, as may be inferred from the common-cause-analysis nature of WPAM, the methodology goes beyond a mere recalculation of independent event-probabilities; it is the 'common' effect that is of more interest in this analysis. The concepts introduced in Fig. 1 and in the present paragraph will be expanded upon in the sections that follow.

3 WORK PROCESSES AT NUCLEAR POWER PLANTS

3.1 Work processes: a definition

According to Galbraith,[35] two basic elements determine the structure of an organization: the division of labor and the coordination of effort. Through the division of labor, the overall task is decomposed into subtasks which can be performed by individuals or groups of individuals who are specialized in the subtasks. The coordination of effort is the process that integrates the subtasks into a single effort toward the completion of the overall task.

In the NPP environment, the first of these two elements, namely, the division of labor, is realized through the creation of working units which are formed according to their technical (i.e. functional) specialization.[36] These working units may include, for example, operations, maintenance, instrumentation and control, and health physics. Clearly, since the emphasis is being placed on the technical specialty of each working unit, the NPP organization must develop subtask-co-ordinating mechanisms that are specialized enough to meet the requirements of each unit, yet broad enough so that the overall task may be accomplished as smoothly and coherently as possible. This, of course, is the subject of the second element of the structure of an organization.

The coordination of work in an organization consists of a series of information-based decision processes which are developed in order to facilitate the accomplishment of the overall task, and thus, the achievement of organizational goals. In NPP organizations, both formal and informal coordinating mechanisms (e.g. policies, procedures, vertical and horizontal channels, scheduled and unscheduled meetings) are utilized in support of various types of decision-making processes. A careful examination of these processes shows that, for a given working unit, although the goal may be different from one job assignment to the next, the path to achieving that goal basically follows a standardized pattern. In other words, although each job assignment accomplishes a different goal, all job assignments follow a standardized flow path. For example, in the maintenance department, fixing a valve and fixing a pump are two different job assignments. However, they are both carried out by following the same sequence of steps, namely, initiating a work request, having the work request reviewed planning the work, scheduling it, executing it, performing post-maintenance testing, returning the equipment to its normal state, and documenting the work.

Clearly, the execution of an assignment from beginning to end (e.g. from initiating a work request to documenting the work) involves a predictable flow path. The term 'work process' is henceforth used in referring to this flow path (or process). Formally, a work process is defined as a standardized sequence of tasks designed within the operational environment of an organization to achieve a specific goal. Since the steps along each work process follow a set pattern, it is advantageous to develop standardized procedures for each step. This standardization eliminates many of the uncertainties and irregularities along the flow paths. Moreover, it reduces the load on both hierarchical and lateral channels in the organization, so that valuable resources can be saved for decisions that involve more uncertainties or that cannot be anticipated in advance.

Most of the work processes at NPPs are described in (and controlled by) written procedures. The written procedures include an elaborate and step-by-step set of instructions that are carefully documented to guide operators and working crews through predictable job-related situations. For example, the corrective maintenance process control procedure lists in detail the entry conditions which determine its appropriateness for the situation at hand. It then lists step-by-step instructions for the actions to be taken by, along with the responsibilities, of each individual or working unit. Training is usually provided so that individuals will understand their roles and responsibilities in the process.

3.2 An overview of work processes at NPP organizations

The predictable nature of the work processes suggests that a systematic analysis can be conducted to identify the desirable design of a given process and to develop performance measures with respect to the strengths and weaknesses in the process. Furthermore, since the work processes are closely related to plant performance, it is possible to conduct the analysis in such a way so as to facilitate the integration of organizational factors and PSA methodology.

NPP work processes are designed to affect, either directly or indirectly, the performance of the hardware at the plant. In this study, those work processes whose constituent activities (or tasks) have a direct influence on the operability of the plant hardware are classified as front-line work processes; those whose impact is felt indirectly are classified as supporting work processes (Fig. 2). For example, the corrective maintenance work process is designed to restore a failed or degraded piece of equipment to its normal state. Clearly, this work process qualifies as a front-line work process since it has a direct impact on the operability of the hardware. In general, the front-line work processes include plant operation,

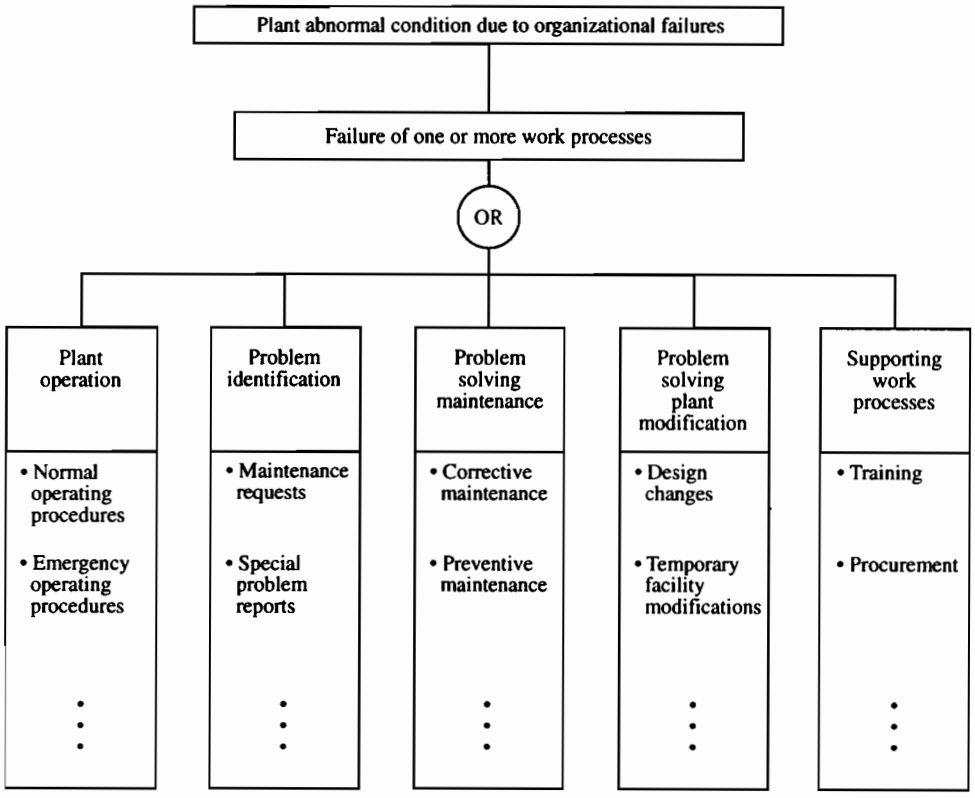

Fig. 2. Front-line and supporting work processes.

problem identification, and problem solving, where the latter is achieved through either maintenance or plant modification. In contrast to front-line processes, there exist other work processes at NPPs that exert their influence in an indirect manner. That is, these work processes act to control the quality of the operations and maintenance crews, rather than that of the actual hardware. Examples of supporting work processes include training and quality control.

In general, work processes are designed so that, in principle, most defects within the system will be caught at some point by the defense mechanisms built into the organizational structure. For example, the maintenance work process at a typical plant normally consists of multiple testing and inspection programs that are devised to identify hardware faults or malfunctions. Once problems are identified, (corrective) maintenance processes are initiated to correct them. At this stage, safety-related maintenance jobs are planned and reviewed by independent individuals according to written procedures. Furthermore, most NPP organizations require that safety-related jobs be performed by teams of two or more workers and under the supervision of quality assurance personnel. This, of course, is to ensure that job assignments are performed correctly and that they meet high safety standards. After a maintenance work has been executed, a post-maintenance test is performed to ensure that the component or system can function properly. Finally, upon completion of the test, the system is returned to its normal line-up and alignment is independently verified. As mentioned above, these steps (or tasks) comprise the maintenance work process and are expanded upon in the next section.

3.3 The maintenance work process

Both corrective maintenance and testing are included in the maintenance program at a given NPP. Basically, testing refers to actions which are taken to meet technical specifications and surveillance requirements. These actions may include some or all of the following: periodic maintenance based on, for example, operating hours or calendar time, predictive maintenance based on monitoring and trending analyses (typically performed by performance engineers), and periodic maintenance based on industrial experience, root cause analyses from previous incidents, or other analyses, such as those performed by system engineers. Corrective maintenance, on the other hand, refers to the repair and/or restoration of equipment or components which have failed or which are found, as a result of testing, to be in a degraded state. The overlap between the two maintenance modes occurs in situations where routine testing of a component or system reveals that remedial actions are

needed that require the initiation of corrective maintenance.

Conceptually, the corrective maintenance work process at a nuclear power generating station follows the control cycle shown in Fig. 3. Plant deficiencies are identified through testing or as a result of a system failure. Once a deficiency is identified, its priority is determined and the maintenance process moves into its planning stage, where the possible causes for the deficiency are diagnosed and the necessary maintenance steps are planned in detail. It is important to keep in mind that, usually, there are more than one maintenance tasks awaiting execution. Of course, this phenomenon is of much higher concern during a refueling outage, when the plant is faced with a large number of maintenance jobs during a rather short period of time. As a result, scheduling and coordination are crucial steps in the maintenance work control cycle. After scheduling and coordinating the specific maintenance tasks, the work is executed, post-maintenance testing is carried out, and the equipment is returned to its normal operating status. The final step of documenting the work is crucial because it allows the organization to analyze and keep track of problem areas.

The testing work process involves steps that are similar to those outlined above. However, there are some differences. Whereas corrective maintenance is usually performed on an as-needed basis, testing is carried out at regular, predetermined intervals, at which time components/systems are tested regardless of their functional status. Since testing is governed by technical specifications (or other such standards), the testing program at NPPs is usually computerized in such a way that the computer links the technical specification requirements to the specific tests that fulfill these requirements. In addition, the computer identifies the procedures that are to be used in each test, stores data on completed tests, and calculates future test schedules. With respect to Fig. 3 then, there is much less prioritization, planning, and scheduling/coordination involved in testing than in corrective maintenance. There are, of course, exceptions. For example, in order to better trend equipment performance, engineers may wish to (manually) reschedule testing so that tests are performed at shorter intervals. Also, for tests having a frequency that is shorter than weekly, the department in charge has the responsibility of developing a weekly test procedure that provides for data collection and review of the more frequent testing. These tests involve, to a certain degree, the same kind of scheduling, execution, verification, and documentation that were discussed within the context of corrective maintenance. However, when, during the performance of tests, faulty or inoperable equipment is found, the process takes a detour so that the equipment can be fixed through the corrective maintenance work process (i.e. Fig. 3).

Each individual plant has its own administrative procedures describing the work control system designed for the organization. The work control procedures standardize the work processes so that all personnel will have the same understanding of the requirements and controls required for performing maintenance work. Although each plant varies with regard to the details of its control system design, all plants follow more or less the same general guidelines. With this in mind, the block diagram of Fig. 4 will now be used to describe a typical corrective

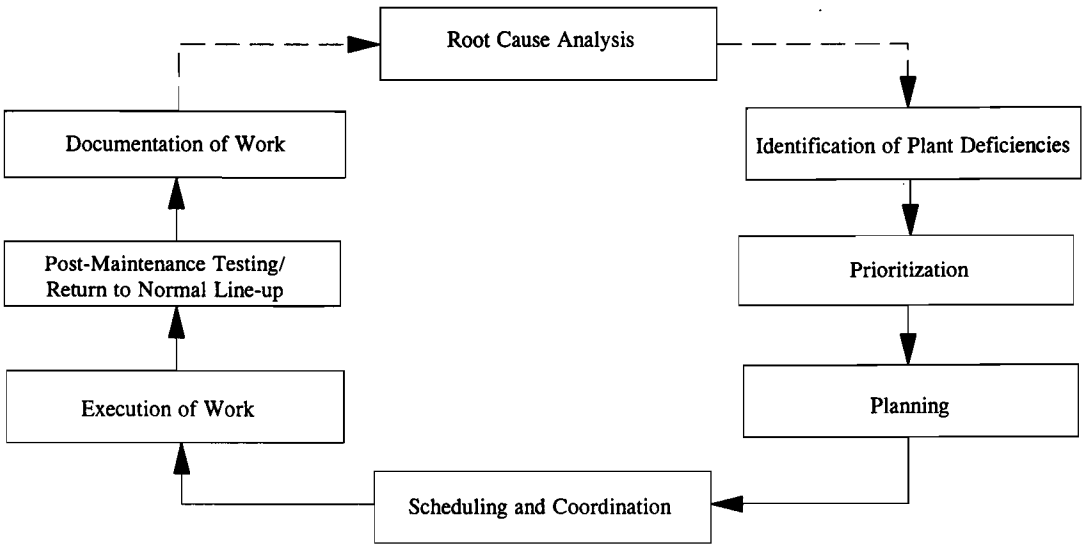

Fig. 3. The control cycle for the corrective maintenance work process.

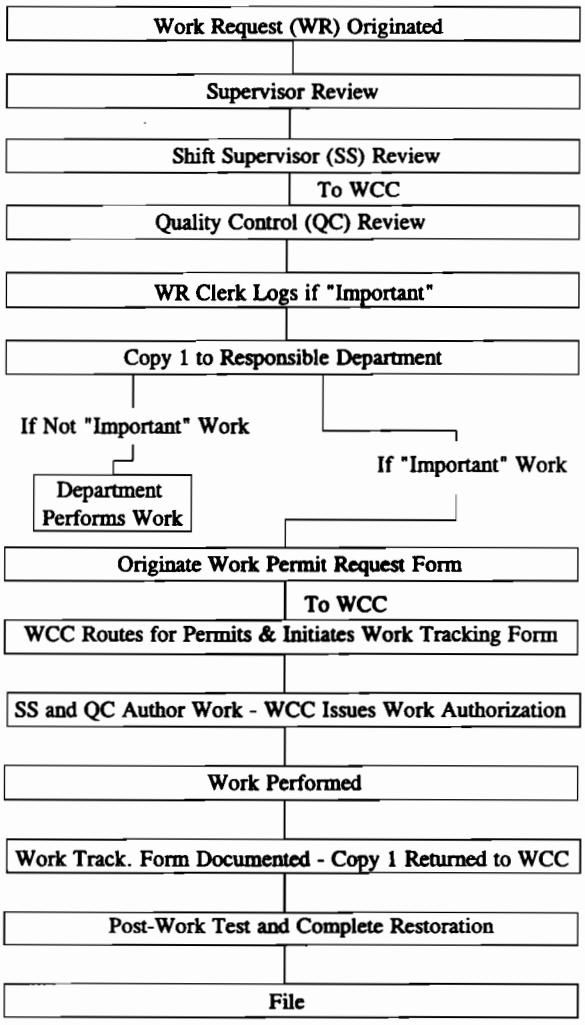

Fig. 4. A sample work flow path for the corrective maintenance work process.

maintenance process, along with the level of coordination which it necessitates among the various departments of a nuclear power plant.

Before continuing, one point of clarification is deemed necessary. Within the descriptions given below, several references are made to the 'work control center' (WCC). In the plant that was studied, the work control center refers to an area next to the control room which acts as the central nerve for coordinating and authorizing work and for testing in the plant. The WCC is staffed by personnel from the Radiological and Environmental Services (RES), Operations, and Quality Control Departments. A partial list of the functions of the WCC is given below.

(i) Issuing work tracking forms (WTFs), protective tags, jumpers, scaffolding permits, and welding permits.
(ii) Processing and distribution of both new and completed work requests.
(iii) Coordinating the planning, scheduling, and performance of maintenance activities.
(iv) Tracking the status of work in progress.
(v) Determining and scheduling post work testing (PWT) for completed items.
(vi) Providing an interface between the Operations Department and the other various departments.

Maintenance processes are initiated only after problems are identified—see also the flow diagram of Fig. 5. If NPP personnel lack an in-depth understanding of the plant systems, or if the culture at the NPP does not promote a vigilant attitude towards the diagnosis and amelioration of potentially hazardous events, problems may reside within the system for long periods of time without being noticed.

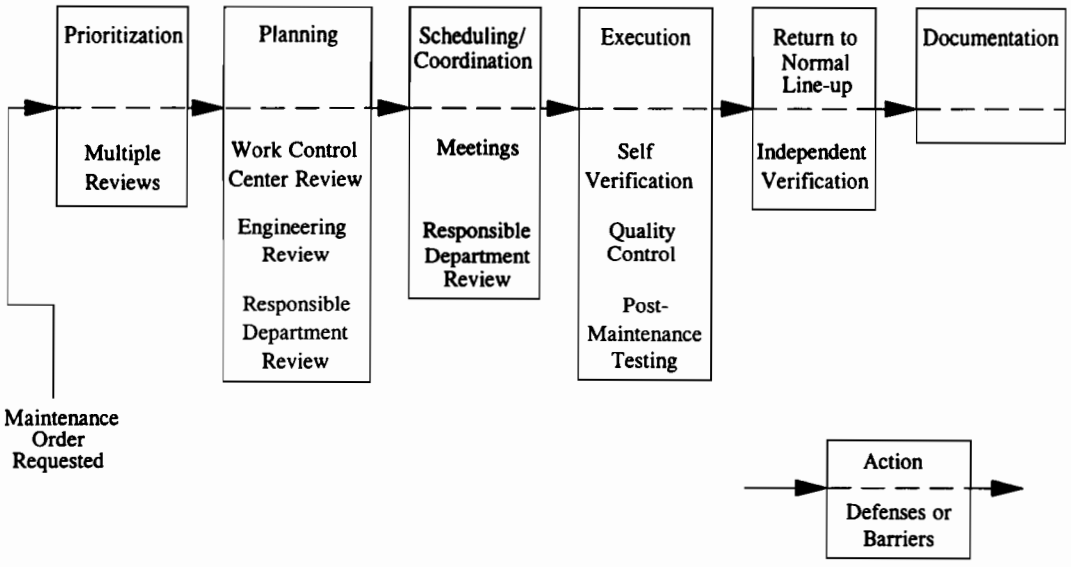

Fig. 5. The flow diagram for the corrective maintenance work process.

Once a problem is identified, a maintenance work request is issued. Each work request is reviewed in three different stages: first, a manager or supervisor, who is either the shift supervisor or another individual who holds a management position (e.g. department superintendents, principal engineers, etc.) conducts a brief and preliminary diagnosis of the problem, suggests a responsible department or group for the maintenance work, and usually assigns a priority ranking to the problem. Second, the shift supervisor or the work control center supervisor reviews the work request to determine and/or confirm the priority of the maintenance work requested, to determine whether it is classified as 'important' work, and to judge, on a preliminary basis, whether procedures require work permits to control various aspects of the work (e.g., radiation work permits, protective tagging, scaffolding permits, weld permits, confined space entry permits, etc.): Third, appointed Quality Control (QC) personnel review the work request to determine whether QC is required. Once a work request has been reviewed, it is entered into the tracking computer and forwarded to the responsible department, which, then, issues work tracking forms.

Issues considered by the shift supervisor when assigning priorities to ('important') maintenance tasks include personnel safety, equipment repair urgency, operability of redundant equipment, licensing commitments, station conditions, repair or replacement parts status, ALARA (as low as reasonably achievable) considerations, and manpower availability.

Once a work request has been reviewed by the work control center, it is forwarded to the responsible department for planning. The main function of planning is to assemble a work package that lists or addresses all issues related to the proper execution of a job. During the preparation of this work package, the planner typically follows the steps listed below.

(i) Confirmation of the problem and definition of the workscope. The planner reviews the original work request and updates the information listed in it by contacting the work request initiator, inspecting the work site, reviewing the maintenance history of the problematic equipment, and reviewing the other maintenance activities that could or should be combined with the current maintenance job.

(ii) Identification of maintenance-related procedures, manufacturer manuals, drawings, maintenance history, test or calibration records, and other reference documents. If there is no approved procedure that can be used for the situation at hand, the planner is responsible for the preparation (and documentation) of a set of special instructions.

(iii) Procurement of the necessary repair parts and materials for the maintenance activity.

(iv) Identification of special tools and equipment, along with any construction or scaffolding that may be necessary for the maintenance activity.

(v) Assessment of manpower and skill requirements for station, non-station utility, and contractor personnel.

(vi) Identification of pre-job ALARA planning and radiation exposure permit requirement.

(vii) Identification of quality control inspection, code, and technical specification requirements.

(viii) Identification of prerequisite system conditions and request for applicable work permit(s) from the operations department.

(ix) Specification of post-installation tests and post-maintenance function tests.

(x) Initiation of the work permit request form.

Planning starts when the responsible department receives the work request. Usually, a planner within the department is assigned as the responsible individual throughout the planning stage of the maintenance process. The planner reviews the work request and initiates a work package. For straightforward jobs, such as changing a light bulb in an indicator, the planner proceeds to complete a checklist of items on the work package.

When maintenance involves a much more complex component, such as a major valve or pump, problems arise that involve more than one department. In these situations, coordination among departments is essential. First, the planner in the responsible department consults with personnel from the operations department and with system engineers from the technical services department regarding the nature and solution of the problem. These discussions usually take the form of direct contact. Verbal communication is used most often, although memos are sometimes issued after some conclusions are reached at the end of the meeting. If there are plant modifications or design changes involved, a plant modification or design change process is initiated. The maintenance process is temporarily halted until the design-change issue has been resolved. It is also not unusual for more than one work request, involving other responsible departments, to be issued as the result of these meetings. The original responsible department is often assigned as the lead department for the co-ordination of this specific maintenance task force.

Scheduling and co-ordination of maintenance activities ensure that maintenance is accomplished in a timely manner. In most organizations, work is scheduled and coordinated by a central department (i.e. the planning department). Computer systems of various levels of sophistication are used for the scheduling and tracking of maintenance activities,

which are scheduled according to the priority of the tasks, items in the plant maintenance backlog, available manpower, expected plant mode, and the status of the available equipment. In the plant studied, concerns over work schedule or other related issues are normally expressed during scheduled daily meetings that are held at various levels of the organization and are attended by personnel from various departments. These meetings also provide a regular channel for lateral inter-departmental communication. When necessary, additional meetings of a smaller scale are scheduled during these daily meetings for further co-ordination of effort.

Once maintenance work on a particular component is scheduled, a field work package, which includes all of the work permits, procedures, drawings, and instructions, is assembled by the responsible department and journeymen are sent out to obtain the necessary materials, equipment, and tools. After the control room operators tag out the required components, the workers from the responsible department can start their field work. Depending on applicable procedures and the components involved, this work may be executed in the presence of health physics and/or QC personnel. At this point, the status of the work request is changed to 'working' and remains this way until the work tracking form is returned to the work control center signaling the completion of the work requested.

Upon completion of the job, the leadman describes his work in the work tracking form. The department supervisor then reviews the form, signs it off, and forwards it to the work control center so that the operations department can be notified and post-maintenance tests can be conducted.

Upon completion of the maintenance work, the work control center supervisor reviews the work package and, based on plant conditions, determines whether post-maintenance testing can be performed. If plant conditions are appropriate, the shift supervisor is notified so that post-maintenance testing can begin. If, however, testing cannot be performed, then the work request is filed as 'APWT', i.e. as waiting post-maintenance testing. In this case, the WCC supervisor reviews the plant work schedule and conditions and schedules the test accordingly.

Post-maintenance testing is performed according to the request in the work plan. If the results of the test are satisfactory, the work request is forwarded to the WCC until all the paperwork is received and the file can be closed. If, on the other hand, the results are not satisfactory, the work request is sent back to the responsible department for 'rework' and the post-maintenance test process is repeated. Once the required testing has been completed satisfactorily, the system is realigned to normal operating conditions and is returned to service.

Upon completion of the maintenance process, the work package is documented. Root cause analyses are conducted on some of the incidents to gain further insights into the events. Depending on plant policy, computer software may be designed to record some of the experiences learned from the maintenance activities. For example, due to concern with common-cause failures, repeated maintenance on the same component, or on components of the same type, usually attracts more attention.

When the work package is received by the work control center, it is forwarded to the nuclear plant reliability data (NPRD) coordinator for review. If the work request is classified as a QA category 1 or 1EH, or if it involves a design modification, then the quality control department reviews the package before sending it to the NPRD coordinator. Furthermore, for a design modification work package, after the NPRD coordinator has reviewed it, it is sent to the technical services department so that its design modification portion can be reviewed and, subsequently, closed. Finally, the work package is sent to the quality control department, where document copies are transmitted to the NPRD co-ordinator and the work request is closed.

Up to this point, the discussion has been focused on NPP work processes and, to some extent, on the organizational factors (e.g. coordination, training, formalization of procedures) that might affect them. In other words, so far, only the bottom portion of Fig. 1 has been considered. To complete the picture, Section 4 presents an overview of probabilistic safety assessment methodology (i.e. the top portion of Fig. 1).

4 PROBABILISTIC SAFETY ASSESSMENT

4.1 An overview of PSA methodology

In PSA methodology, event tree analysis is used to delineate all possible events following the occurrence of an initiating event (IE). As shown in Fig. 6, an event tree is a logic model which shows the relationships among events occurring at a plant. This tool helps analysts and decision makers to investigate plant risk systematically and in an integrated fashion as accident scenarios stemming from a group of initiating events of similar physical characteristics, instead of viewing them as isolated incidents.

Basically, an event tree consists of three parts: initiating events, barriers, and the end-states. Initiating events are those events which may set off accident sequences. Over the years, systems analyses and experience have resulted in a generic list of potential accident-initiating events.[14]

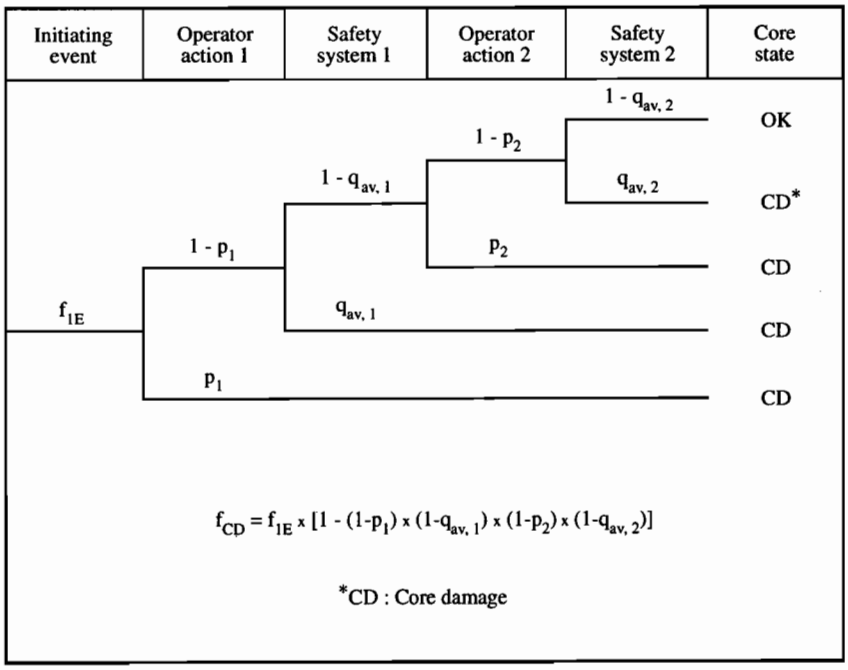

Fig. 6. A simplified event tree.

As shown in Fig. 6, barriers are safeguards which are placed in the path of potential accident sequences and consist of operator actions and safety system responses. For a certain accident sequence, human operators are counted upon to perform their actions correctly. However, since humans are not infallible, human error probabilities (HEPs) are derived so that the impact of human errors on the progression and/or the consequences of the accident can be quantified. By the same token, NPPs rely on their safety systems to impede the progression of an accident as quickly and efficiently as possible. The extent to which this may be possible, however, depends on safety-system availabilities at the specific plant and is the subject of further discussion in this section.

Finally, the end-state on an event tree shows the consequences of an accident sequence based on whether the sequence was stopped by any of the barriers and, if it was, according to the point at which it was stopped. For example, typical end-states for an event tree which analyzes the frequency of core damage include: core OK (OK), core vulnerable (CV), or core damage (CD).

For the event tree of Fig. 6, two operator actions and two different safety systems are shown. In this simplified example, damage of the reactor core can be prevented only if both operator actions are carried out correctly and both plant safety systems function accordingly. The estimated frequency of core damage for this specific initiating event is, thus

$$f_{CD} = f_{IE} * [1 - (1 - p_i)(1 - q_{av,i})(1 - p_2)(1 - q_{av,2})] \quad (1)$$

where

$f_{CD} \equiv$ frequency of core damage (caused by this specific initiating event),

$f_{IE} \equiv$ frequency of the initiating event,

$p_i \equiv$ probability of error of the ith operator action conditioned on its prior events, and

$q_{av,i} \equiv$ average unavailability of the ith safety system conditioned on its prior events.

To correctly estimate the risk, the impact of the quality of organization and management on plant safety should be reflected in the parameters f_{IE}, p_i, and $q_{av,i}$. Generally, the sources of data for f_{IE} include the Reactor Safety Study (RSS),[37] plant-specific data, data gathered through operational experience of the industry as a whole, and PSAs performed for other NPPs which may be similar to the NPP being analyzed. As for p_i, several models have been proposed which assign HEPs to certain tasks or groups of tasks (e.g., Swain and Guttmann[38] and Apostolakis *et al.*[39]). Lastly, the quantification of $q_{av,i}$ employs a combination of the above sources as it contains terms which require data on both system and human reliability. It is noted again that the extent to which the above-mentioned sources and parameters already include the impact of organizational factors is an issue of on-going debate.

As mentioned earlier, the current analysis does not involve an explicit treatment of the dynamics of a given accident sequence. Therefore, considering eqn (1), attention will be focused on the system unavailability term $q_{av,i}$; operator error probabilities and initiating event frequencies fall outside the scope

of this analysis. Before investigating the influence of organizational factors, it is important to identify the basic parameters that are used to calculate the unavailability.

4.2 System unavailability

The engineered safety systems in nuclear power plants are installed for emergencies and are normally on stand-by. To ensure their operability, they are tested at periodic intervals and, if necessary, repaired on an as-needed basis. The pointwise (time-dependent) system unavailability, $q(t)$, is defined as the probability that the system is down at time t. To avoid the need for the detailed information that is required for the calculation of the time-dependent unavailability, the average unavailability over a time interval of interest $(0, T)$, q_{av}, is defined as

$$q_{av} \equiv (1/T)\int_0^T q(t)\,dt \tag{2}$$

In the present analysis, the analytical approach of Apostolakis and Chu[40] along with that of the Reactor Safety Study[37] are followed with some modification in modeling the average unavailabilities of both a single-component system and a one-out-of-two redundant system. For the latter, although the analysis presented below is specific to cases where sequential testing is performed, analogous results can be found for staggered-testing schemes by making the appropriate modifications to the expressions derived in the above-mentioned references. Also, as was pointed out earlier, the unavailability expressions that are discussed below contain the contributions of both testing and corrective maintenance to component/system unavailability.

4.2.1 Average unavailability of single-component systems

The average unavailability of a single standby component that is periodically tested can be approximated by

$$q_{av} = (\tau_r/\tau) + \gamma + Q + (1/2)\lambda\tau + f\tau_m \tag{3}$$

where

τ = interval between tests,
τ_r = duration of test,
γ = probability of failure due to testing/maintenance,
Q = probability of failure on demand,
λ = failure rate (the failure distribution is assumed to be exponential),
f = frequency of (corrective) maintenance,
τ_m = average duration of (corrective) maintenance.

The various contributions to the average unavailability are:

(τ_r/τ) = test contribution (the component has been assumed to be disabled during testing),
γ = human error contribution (testing and/or maintenance)
Q = contribution from failure due to demand stresses,
$(1/2)\lambda\tau$ = contribution from 'random' failures (such as those due to environmental stresses) occurring between tests while the component is on standby,
$f\tau_m$ = contribution from corrective (unscheduled) maintenance.

It is noted that the presence of both terms Q and $(1/2)\lambda\tau$ is usually unnecessary. However, both are included to keep the analysis as general as possible.

4.2.2 Average unavailability of one-out-of-two systems

The average unavailability of a one-out-of-two system under a sequential testing scheme can be represented by the sum of four terms

$$q_{av} = q_R + q_C + q_D + q_{TM} \tag{4}$$

where q_R represents the 'random' independent failure contribution, q_C represents the dependent (due to random shocks) failure contribution, q_D represents the demand failure contribution, and q_{TM} represents the test and maintenance contribution. Of interest in the present study is the test and maintenance contribution q_{TM}, which is further calculated as:[40]

$$q_{TM} = \gamma_0[\gamma_1 + (1-\gamma_1)Q + (2-\gamma_1)(\lambda_R + \lambda_C)(\tau/2) + (2\tau_r/\tau) + (2f\tau_m)] \tag{5}$$

where

λ_C = occurrence rate of 'shocks' that fail both components (i.e. common cause failures),
λ_R = random failure rate,
γ_0 = probability of failure of one component due to a test or maintenance error, and
γ_1 = conditional probability of the second component failure given that the first fails due to test or maintenance error.

Some terms in this expression of system unavailability can be readily interpreted, for example,

$\gamma_0\gamma_1$ = contribution of dependent (test/maintenance) errors on both components,
$\gamma_0 Q$ = one component down due to human error and the other fails on demand,
$2\gamma_0 f\tau_m$ = one component down due to human error and the other down due to (unscheduled) maintenance.

4.2.3 Influence of organizational factors on system unavailability—candidate parameter groups (CPGs)

In this analysis, the goal is to identify all possible paths through which human errors due to organizational deficiencies can affect the PSA event tree (refer to Fig. 1). However, even within the exclusive context of the maintenance work process, this is not a simple task, since these errors could influence both the

frequency of initiating events and the availability of safety systems.

Although this study is focused on the influence of organizational factors on system unavailability, it is important to recognize that uncorrected errors during maintenance could lead to an increase in the frequency of initiating events. The Mihama-2 incident in Japan, for instance, is a good case in point, where the initiating event turned out to be a small LOCA.[41] This incident started when inexperienced engineers installed the antivibration bars into the wrong slots in the steam generators. Since the bars did not fit properly this way, the engineers sawed about 40 cm off each bar. The result of this error was that some of the tubes were never secured by the antivibration bars, and one eventually ruptured and caused a steam generator tube rupture, which is in the range of a small LOCA. Better procedures and a higher level of technical knowledge (including a better training or qualification program) promoted at the organizational level, for example, might have helped to reduce the chance of occurrence of this incident.

With regard to system (average) unavailabilities, an analysis of the terms of eqns (3) and (5) provides some insight into the potential dependencies between system unavailabilities, human errors, and the organization and management of an NPP. First, it is important to recognize that the parameters of q_{av} must be viewed as potentially dependent variables. The sources of data of these error rates or failure rates are affected by common factors, e.g. the quality of procedures, the quality of plant operation, and the quality of maintenance. These are, in turn, determined by an overall factor, namely, plant management. In the case of a single component, the quality of maintenance may simultaneously affect τ_m, the length of time spent on maintenance; γ_0, the probability of failure due to testing and maintenance errors; Q the probability of component failure on demand; λ, the component failure rate; and f, the frequency with which corrective actions must be carried out.

For example, it is clear that, if an error by a maintenance worker is not corrected at any point along the work process and has to wait to be corrected during post-maintenance testing, then the unavailability of the system will increase through an increase in the value of τ_m (i.e. the system may have to remain disabled until the maintenance work, or some portion of it, is repeated, and the system is tested again). Similarly, if the quality of procedures and/or training is poor, or if organizational barriers are either nonexistent or inadequate, then an error in maintenance may go unnoticed. This can lead directly to the failure of the system, and is accounted for by γ. Lastly, although a system may be operable at the time post-maintenance testing is performed, subsequent failures may occur sooner than originally anticipated due to minor, yet important steps being left out of the maintenance work process (e.g. lubrication). This effect manifests itself as an increase in the failure rate.

The qualitative discussion presented in this section has shown that dependencies among parameters can have a significant effect on the availability of plant equipment. Clearly, ignoring these dependencies is very likely to lead to an underestimation of plant risk.[42] In the present study, the dependence that is introduced by organizational factors (OFs) is evaluated by recalculating basic-event probabilities while accounting for the dependencies among the parameters that represent each basic event. As such, the parameters (i.e. λ_R, γ, etc.) take center stage in the procedure that has been devised to incorporate the impact of organizational factors into basic-event probabilities. This procedure will be discussed in more detail in subsequent sections, where the above-mentioned parameters are referred to as 'candidate parameter groups' (CPGs), i.e. groups of parameters that are candidates for re-assessment with regard to the OFs.

As has been stated already, the predictable nature of the work processes suggests that a systematic analysis can be conducted to identify the desirable characteristics of a given process and to develop performance measures with respect to the strengths and weaknesses in the process. Furthermore, since work processes are closely related to plant performance, it is possible to conduct the analysis in such a way so as to facilitate the integration of organizational factors and PSA methodology. In order to address these issues, the work process analysis model has been divided into two parts. WPAM-I consists of a mostly qualitative analysis of a given work process, including an assessment of the importance of the role of organizational factors in the overall quality and efficiency of the work process. WPAM-II, on the other hand, consists of a quantitative analysis for each dominant accident sequence, whereby the effect of organizational factors on a work process, and thus, on the candidate parameter groups is measured and then incorporated into PSA results. WPAM-I is discussed in this paper and WPAM-II is discussed in a subsequent paper.[43] Needless to say, the existence of a PSA for the plant under analysis is crucial for the successful application of WPAM.

5 WORK PROCESS ANALYSIS MODEL-I (WPAM-I)

5.1 The structure of WPAM-I

The total number of work processes at a nuclear power plant may be large; however, some work processes are more critical to the safe and reliable

operation of the plant than others. Therefore, WPAM-I starts by identifying the front-line and supporting work processes (see Fig. 2). This is generally accomplished by reviewing plant documents, conducting interviews with senior managers, and consulting documents from the Nuclear Regulatory Commission (NRC), the Institute of Nuclear Power Operations (INPO), and the Electric Power Research Institute (EPRI).

For each work process, WPAM-I proceeds by asking the following basic question: how can the accumulation of organizational failures lead to an unsafe plant condition? In other words, how can unsafe attitudes or unsafe decisions made in the work processes defeat the defenses and barriers of the organization and be translated into noticeable unsafe events of either hardware failures or human errors? In answering these questions, WPAM-I utilizes a three-step procedure to investigate systematically, within each work process, the types of failures that might occur, the breaches of the defenses and barriers of the system that are supposed to intercept these failures, the organizational causes that may bring about these failures and breaches, the modes and consequences of these failures and breaches, and the relative importance of the pertinent organizational factors for each task within a given work process. This process is similar to a failure modes, effects, and criticality analysis (FMECA) that addresses organizational factors. The three-step procedure is as follows:

(i) conduct a task analysis of each work process,
(ii) define the organizational factors matrix for each work process,
(iii) determine the relative importance of the organizational factors for each task.

5.1.1 Task analysis

The first step of WPAM-I is to conduct a task analysis. This analysis focuses on understanding the following three elements of the work processes under investigation (in this case, the corrective maintenance work process).

(i) Tasks (e.g. planning, execution, etc.) that are involved in the work process and the plant personnel involved in each. A typical task involves two sequential steps: the actions taken to achieve a specific goal, followed by the defenses or barriers designed to capture errors that might have been made during the action step. For example, for the task entitled 'planning' in the corrective maintenance process, the action step involves the planner assembling the work package, and the defenses include the various reviews performed by the responsible departments.
(ii) Actions involved in each task and their failure modes. In the terminology of Reason's model,[21,22] these failures are called unsafe acts and are taken to be the manifestations of organizational failures. For instance, when a planner assembles the work package, the unsafe actions may include 'incorrect procedures identified' or 'wrong drawings referenced'. Both of these failure modes would lead to unsatisfactory planning.
(iii) The defenses or barries involved in each task and their failure modes. Defenses or barriers are built into the system to capture potential unsafe acts. For example, the purpose of the engineering and health physics reviews of the work package after it has been assembled is to identify any errors that may have been made in the planning stage, before maintenance activities are scheduled.

The products of the task analysis are a flow diagram, a cross-reference table, and a design/implementation checklist. The flow diagram identifies the most important tasks in the process and their sequential relationship. The cross-reference table specifies the departments, the personnel, the actions, and the defenses involved in each task. Finally, the checklist contains a series of questions aimed at comparing the design and the implementation of tasks in a given work process. Figure 5 shows the flow diagram for the corrective maintenance work process, and Table 1 shows the cross-reference table for the same work process. An example of a checklist for scheduling and co-ordination of maintenance work is presented in Fig. 7.

5.1.2 Organizational factors matrix

The second step of WPAM-I is to define the organizational factors matrix for each key work process, which shows the organizational factors that might impact the safe performance of each task in the work process. For the plant being studied, the matrix specifies task-specific organizational factors by collecting related procedures/documents on the work process of interest, by conducting interviews with plant personnel, and by collecting information on plant operating experience (e.g. through Licensee Event Reports). Table 2 shows the organizational factors matrix for the corrective maintenance work process. As can be seen, the horizontal axis contains the tasks involved in the work process; the organizational factors (or dimensions) listed on the vertical axis are taken from Ref. 12 and are defined in Table 3. The following observations are made with regard to the organizational factors matrix.

First, the organizational factors matrix supports the hypothesis that the relationship between organizational failures and unsafe acts is a 'many-to-many mapping' in a nuclear-power-plant organization.[21] In effect, this implies that backtracking from unsafe acts

Table 1. The cross-reference table for the corrective maintenance work process

Task	Action/Barriers	Department	Personnel
Prioritization	Prioritization	Work Control Center (WCC)	WCC Supervisor
	Reviews	WCC/Operations	Shift Supervisor
Planning	Planning	Maintenance/I & C	Planner
	WCC Review	WCC	WCC Supervisor
	Engineering Reviews	Engineering	System Engineer
	Responsible Dept. Review	Maintenance/I & C	Mech./Elec./I & C Engineer
Scheduling/Coordination	Scheduling/Coordination	Planning Dept.	Scheduler
	Meetings	Various Depts.	Variable
	Responsible Dept. Review	Various Depts. (Operations for system tagging)	(Operations for Work Authorization)
Execution	Execution	Maintenance/I & C	Mech./Elec./I & C
	Self Verification	Maintenance/I & C	Mech./Elec./I & C
	QC	Quality Control/ Quality Assurance	QC/QA Engineer
	Post-Maintenance Testing	Maintenance/I & C/WCC	Mech./Elec./I & C
Return to Normal Line-Up	Return to Normal Line-Up	Operations	Control Room Operator
	2nd Verification	Operations	Control Room Operator
Documentation	Documentation	WCC (Nuclear Plant Reliability Data)	Clerk

may not be sufficient to identify the nature of the unsafe attitude existing in the organization since, as can be seen from Table 2, one organizational failure is capable of causing many unsafe acts, and one unsafe act can be caused by a number of organizational failures. Second, the organizational factors matrix is useful for diagnosing organizational weakness at the plant; it helps to localize the problem areas and to guide the direction of the analysis. For example, the matrix indicates that, in the corrective maintenance process, the organizational factors that affect planning include intra-, inter-, and external communications, formalization, technical knowledge, etc. The analyst can then use appropriate instruments to evaluate the quality of maintenance planning activities with respect to the above factors and to identify the organizational weaknesses relevant to maintenance planning.

5.1.3 Determination of relative importance weights

Since each task in a given work process can be influenced by more than one organizational factor, it is deemed necessary (for the purposes of prioritizing investigative and/or corrective actions and for use in WPAM-II) to rank the pertinent factors according to their importance to (i.e. their level or degree of influence on) the tasks of the work process under analysis. The analytic hierarchy process (AHP)[44] is a computer interactive tool that has been developed to aid in setting priorities.

In each AHP session, the weights are obtained by asking experts to assign relative weights to the pertinent organizational factors two at a time (i.e. perform a pairwise comparison). Once all of the factors have been exhausted, AHP calculates relative importance weights for the factors with respect to the given task. Also, the weights are renormalized so that they add up to one. Moreover, in order to ensure that the expert is being consistent, AHP computes two measures of consistency, λ_{max} and CR. The rigorous mathematical definitions of these measures will not be discussed here. However, suffice it to say that the closer λ_{max} is to the number of activities (in this case, the number of organizational factors), the more consistent the result is. Also, a consistency ratio (CR) of 0·10 or less is considered acceptable. A final, yet important note is that AHP requires that the factors being weighed be mutually exclusive (i.e. that there be no overlap among them). In WPAM (especially in WPAM-II), this assumption is of utmost importance because it ensures that the weaknesses or strengths of the organization will not be disregarded or double counted. However, this is only an assumption since, at this point, it cannot be claimed that the set of dimensions being used in this analysis meets this requirement. For example, it is obvious that safety culture is one of the underlying factors that influence many of the other factors, such as communication or formalization. Nevertheless, AHP is used in the WPAM framework while further research continues to be conducted on this issue. Should this research be unable to produce organizational factors without any overlap among them, it is believed that WPAM can still produce meaningful results as long as a reasonably mutually exclusive set of factors is used;

DESIGN/IMPLEMENTATION CHECKLIST EXAMPLE

Design Checklist:

1. Is there a central organization (planning department and work control center) in charge of coordinating planned work?
2. What is the organizational relationship of the planning department and work control center to other departments in the working core; i.e., operations, maintenance, and instrumentation and control departments?
3. What are the barriers built into the system to correct errors made in the scheduling or coordination of maintenance work? And what are their functions?
4. What is the standard process for the scheduling and coordination of a maintenance work?

Implementation Checklist (Normative):

1. Where is the work control center located?
2. What is the information transfer mechanism used in the work tracking system?

Implementation Checklist (Behavioral):

1. How many items are on the maintenance backlog?
2. How many items on the maintenance backlog are of PRIORITY 1?
3. How many equipment deficiency tags are on the main control panels?
4. Does the plan-of-the-day schedule reflect the ongoing work?
5. Does scheduling reflect prioritization of work with respect to safety impact?
6. What is the management philosophy in scheduling; i.e., which type of work is usually assigned higher priority?
7. Does the shift superintendent need to review most of the work packages?
8. Are technicians often allowed to "negotiate" with the shift superintendent regarding assigned work?
9. Does the planning department communicate well with other departments?
10. Does the daily meeting on scheduling and coordination show conflicts among departments regarding scheduled work?

Fig. 7. A sample design/implementation checklist for scheduling and coordination of maintenance work.

the examples given later utilize a subset of factors that are deemed to be reasonably mutually exclusive.

The matrix shown in Table 4 represents an AHP session for the task entitled 'prioritization'. For simplicity, only four organizational factors (inter-departmental communication, formalization, technical knowledge, and time urgency) are considered. As is evident, the diagonal of the matrix is predetermined and consists of 1·0s. That is, in the pairwise comparison, technical knowledge, for example, is as

Table 2. The organizational factors matrix for the corrective maintenance work process

	Prioritization		Planning			Execution				
	Prioritization	Reviews	Planning	Reviews	Scheduling/ coordination	Execution	QC	Post-Maint. testing	Return to normal line-up	Documentation
Centralization	×	×	×	×	×	×	×	×	×	×
Communication-External			×							
Communication-Interdepartmental	×		×		×	×				
Communication-Intradepartmental	×	×	×	×	×	×	×	×	×	
Coordination of Work			×		×	×				
Formalization	×		×		×	×	×	×	×	×
Goal Prioritization	×				×					
Organizational Culture	×	×	×	×		×	×	×		
Organizational Knowledge	×	×	×	×	×	×	×			
Organizational Learning	×	×	×	×				×		
Ownership				×		×	×			
Performance Evaluation						×	×			
Personnel Selection	×	×	×	×	×	×	×	×	×	
Problem Identification		×	×	×		×	×	×	×	
Resource Allocation	×				×					
Roles-Responsibilities	×	×	×	×	×	×	×	×	×	×
Safety Culture	×	×		×		×	×			×
Technical Knowledge	×	×	×	×	×	×	×	×	×	
Time Urgency	×	×	×	×	×	×		×		
Training						×	×	×	×	×

Table 3. Definitions of the organizational factors

Organizational factor	Definition
Centralization	Centralization refers to the extent to which decision-making and/or authority is localized in one area or among certain people or groups.
Communication-External	External communication refers to the exchange of information, both formal and informal, between the plant, its parent organization, and external organizations (e.g., NRC, state, and public).
Communication-Interdepartmental	Interdepartmental communication refers to the exchange of information, both formal and informal, between the different departments or units within the plant. It includes both the top-down and bottom-up communication networks.
Communication-Intradepartmental	Intradepartmental communication refers to the exchange of information, both formal and informal, within a given department or unit in the plant. It includes both the top-down and bottom-up communication networks.
Coordination of Work	Coordination of work refers to the planning, integration, and implementation of the work activities of individuals and groups.
Formalization	Formalization refers to the extent to which there are well-identified rules, procedures, and/or standardized methods for routine activities as well as unusual occurrences.
Goal Prioritization	Goal prioritization refers to the extent to which plant personnel understand, accept, and agree with the purpose and relevance of goals.
Organizational Culture	Organizational culture refers to plant personnel's shared perceptions of the organization. It includes the traditions, values, customs, practices, goals, and socialization processes that endure over time and that distinguish an organization from others. It defines the 'personality' of the organization.
Organizational Learning	Organizational learning refers to the degree to which plant personnel and the organization use knowledge gained from past experiences to improve future performance.
Organizational Knowledge	Organizational knowledge refers to the understanding plant personnel have regarding the interactions of organizational subsystems and the way in which work is actually accomplished within the plant.
Ownership	Ownership refers to the degree to which plant personnel take personal responsibility for their actions and the consequences of the actions. It also includes commitment to and pride in the organization.
Performance Evaluation	Performance evaluation refers to the degree to which plant personnel are provided with fair assessments of their work-related behaviors. It includes regular feedback with an emphasis on improvement of future performance.
Personnel Selection	Personnel selection refers to the degree to which plant personnel are identified with the requisite knowledges, experiences, skills, and abilities to perform a given job.
Problem Identification	Problem identification refers to the extent to which the organization encourages plant personnel to draw upon knowledge, experience, and current information to identify problems.
Resource Allocation	Resource allocation refers to the manner in which the plant distributes its financial resource. It includes both the actual distribution of resources as well as individual perceptions of this distribution.
Roles-Responsibilities	Roles and responsibilities refers to the degree to which plant personnel and departmental work activities are clearly defined and carried out.
Safety Culture	Safety culture refers to the characteristics of the work environment, such as the norms, rules, and common understandings, that influence plant personnel's perceptions of the importance that the organization places on safety. It includes the degree to which a critical, questioning attitude exists that is directed toward plant improvement.
Technical Knowledge	Technical knowledge refers to the depth and breadth of requisite understanding plant personnel have regarding plant design and systems, and of phenomena and events that bear on plant safety.
Time Urgency	Time urgency refers to the degree to which plant personnel perceive schedule pressures while completing various tasks.
Training	Training refers to the degree to which plant personnel are provided with the requisite knowledges and skills to perform tasks safely and effectively. It also refers to plant personnel perceptions regarding the general usefulness of the training programs.

important (or unimportant) as itself. In fact, for this example, only six numbers (out of a total of sixteen) need to be provided. This is due to the fact that the matrix is symmetrical, so that the portion below the diagonal consists of comparisons that are the reverse of those considered in the upper half. Therefore, the numbers in the lower half are just the reciprocals of their upper-half counterparts.

In the matrix, 'formalization', for example, has received a weight of negative 3·0 as compared to

Table 4. AHP results for the task 'prioritization'

	Interdept. communication	Formalization	Technical knowledge	Time (urgency)
Interdept. communication	1·0	−3·0	−2·0	−2·0
Formalization	—	1·0	1·0	1·0
Technical knowledge	—	—	1·0	1·0
Time (urgency)	—	—	—	1·0
Weights	0·128	0·312	0·280	0·280

$\lambda_{max} = 4{\cdot}021$.
CR = 0·008.

interdepartmental communication. In the language of AHP, this means that the former is three times as important to the task of prioritization than the latter; the assignment of a positive 3·0 would have signified that formalization is only 1/3 as important as interdepartmental communication. The last row in the matrix contains the results of the AHP session for the task 'prioritization'. As can be seen, formalization is the most important factor, while interdepartmental communication is the least important; technical knowledge and time urgency are of equal (and moderate) importance. Finally, it is noted that $\lambda_{max} = 4{\cdot}021$, which is a satisfactory result since the number of factors considered in this example is 4. Also, CR = 0·008, which is well below the upper limit of 0·10. Therefore, the expert has been consistent in his comparison of, and assignment of numbers to, the factors involved. In the next section, the applications of the products of WPAM-I are discussed.

5.2 The applications of WPAM-I

The primary application of WPAM-I is to provide input to WPAM-II, which is a quantification model developed to include organizational factors into the risk assessment of nuclear power plants. In addition, WPAM-I can provide useful qualitative information that may help to systematize diagnostic evaluations of the work processes.

As described in the details of WPAM-II, the products of WPAM-I (i.e. the work process flow diagram, the cross-reference table, and the organizational factors matrix) are used to identify the minimal cut sets (MCS) that possess the highest degree of organizational dependence. Due to the large number of MCS in a typical PSA, this 'screening' will significantly reduce the amount of quantification that will be needed in WPAM-II. In addition, a modification introduced into the AHP process will facilitate the identification of the organizational factors that have the highest impact on the minimal-cut-set frequencies.

As for the evaluation of work processes at nuclear power plants, the products of WPAM-I are useful in at last two ways:

(1) Before the field inspection, the process flow diagram, the cross-reference table, and the design/implementation checklist developed in WPAM-I for each work process can be used to provide the inspector with a basic knowledge of the operation of the organization (i.e., how the organization is *supposed* to operate). Based on this information, the inspector can identify the strengths and weaknesses in the design of a given work process at the plant. For example, the inspector may want to find out whether all of the actions and barriers that have been identified as being essential are actually existent at the plant.

(2) During the field inspection, the design/implementation checklist developed in WPAM-I can provide some basic indicators which the inspector can use to evaluate the quality and efficiency of task performance at the plant. For example, the inspector may want to look into the number of jobs in the maintenance backlog that involve requests of priority 1. Or, from an ergonomics point of view, he may want to determine the advantages/disadvantages of the physical location and arrangement of the work control center with respect to the control room. Here, the AHP results could be used to prioritize the inspection of the various tasks within a given work process.

All in all, the products of WPAM-I help the inspector to identify: (before the actual field inspection) the areas which he would like to investigate and, once at the plant, a systematic way in which he may want to conduct this investigation. Also, as part of the final WPAM package, the products of WPAM-I can aid in the management of risk and in the allocation of resources by utilities and plant managers.

6 SUMMARY

It has been recognized by both the nuclear and the non-nuclear industries that organizational factors in

general, and safety culture in particular, play a major role in the level of safety that can be realistically achieved by any organization. Furthermore, many have conceded that current PSA methodology is not capable of accounting for the common-cause effects of organizational factors on risk. To address the issue, then, researchers have identified numerous organizational factors which are believed to present potential causes of human and hardware failure at nuclear power plants. The extent to which this may be the case has been the subject of a handful of studies on the incorporation of organizational factors into PSAs. The work process analysis model has been introduced as one such analytical tool.

The WPAM methodology is predicated on the observation that the day-to-day operation of nuclear power plants is governed by several front-line and supporting work processes. The research on work processes has shown that these processes standardize NPP operations while conforming to the defense-in-depth philosophy. This was shown through an in-depth analysis of the corrective maintenance work process. Furthermore, it was demonstrated that the impact of organizational factors on NPP safety may be captured through the use of work processes (and the personnel, hardware, etc., involved in them) as a bridge between the organizational factors and PSA parameters. WPAM-I, the first part of WPAM, was introduced as the first step of this integration process.

The major products of WPAM-I are the work process flow diagram, the cross-reference table, the organizational factors matrix, and the design/implementation checklist. These are used as input to WPAM-II, which involves the quantitative analysis of the impact of organizational factors on risk.

ACKNOWLEDGMENTS

This work was sponsored in part by the U.S. Nuclear Regulatory Commission under Contract NCR-04-90-369. The authors thank the technical project monitor, Carl Johnson of the NRC; Professors David Okrent and Ike Grusky of UCLA; Dr Sonja Haber of Brookhaven National Laboratory; Professor Rick Jacobs of Pennsylvania State University; and Dr Doug Orvis of the Accident Prevention Group, Inc., for many stimulating discussions.

Although this paper is based on research funded in part by the US Nuclear Regulatory Commission, it presents the opinions of the authors, and does not necessarily reflect the regulatory requirements or policies of the USNRC.

REFERENCES

1. Rasmussen, J. Human error and the problem of causality in analysis of accidents, *Ergonomics*, **33** (1990) 1185–99.
2. Perrow, C. *Normal Accidents: Living with High-Risk Technologies*. Basic Books Inc., NY, USA 1984.
3. Joksimovich, V., Orvis, D. D. & Moieni, P. Safety culture assurance via integrated risk management programs. In *Proceedings of the Probabilistic Safety Assessment International Topical Meeting*. American Nuclear Society, IL, USA 1993, pp. 220–26.
4. Hurst, N. W. Immediate and underlying causes of vessel failures: Implications for including management and organizational factors in quantified risk assessment. Paper presented at IChemE Symposium Series No. 124. Institution of Chemical Engineers, Rugby, UK.
5. Winsor, D. A. Communication failures contributing to the challenger accident: An example for technical communicators. *IEEE Transactions on Professional Communication*, **31** (1988) 101–7.
6. INSAG. Basic Safety Principles for Nuclear Power Plants, Safety Series. No. 75-INSG-3. International Nuclear Safety Advisory Group, International Atomic Energy Agency, Vienna, Austria, 1988.
7. IIASA. Working Paper—The Influence of Organization and Management on the Safety of NPPs and Other Complex Industrial Systems. International Institute of Applied Systems Analysis (IIASA), WP-91-28, July 1991.
8. Reason, J. The Chernobyl errors, *Bull. British Psychological Soc.* **40** (1987).
9. Wu, J. S., Apostolakis, G. E. & Okrent, D. On the inclusion of organizational and managerial influences in probabilistic safety assessments of nuclear power plants. *The Analysis, Communication, and Perception of Risk*, B. J. Garrick & W. C. Gekler (eds). Plenum Press, NY, USA, 1991, pp. 429–39.
10. FY 1991 Organization Factors Research and Applications Progress Report. US Nuclear Regulatory Commission Policy Issue, SECY-92-00, Jan. 8, 1992.
11. Marcus, A. A., Nichols, M. L., Bromiley, P., Olson, J., Osborn, R. N., Scott, W., Pelto, P. & Thurber, J. Organization and Safety in Nuclear Power Plants. US Nuclear Regulatory Commission Report, NUREG/CR-5437, 1990.
12. Jacobs, R. & Haber, S. Organizational processes and nuclear power plant safety. *Reliability Engineering and System Safety*, **45** (1994) 75–83.
13. Bley, D., Kaplan, S. & Johnson, D. The strengths and limitations of PSA: Where we stand. *Reliability Engineering and System Safety*, **38** (1992) 3–26.
14. PRA Procedures Guide. US Nuclear Regulatory Commission, NUREG/CR-2300, Washington, DC, 1983.
15. Mosleh, A. Common cause failures: An analysis methodology and examples. *Reliability Engineering and System Safety*, **34** (1991) 249–92.
16. Bellamy, L. J., Geyer, T. A. W., Wright, M. S. & Hurst, N. W. The development in the UK of techniques to take account of management, organisational and human factors in the modification of risk estimates. Paper presented at the American Institute of Chemical Engineers Spring National Meeting, Orlando, FL, March 18–22, 1990.
17. Paté-Cornell, M. E. & Bea, R. G. Management Errors and System Reliability: A probabilistic approach and application to offshore platforms, *Risk Analysis*, **12** (1992) 1–18.
18. Vaughan, D. Autonomy, Interdependence, and Social Control: NASA and the Space Shuttle Challenger. *Administrative Science Quarterly*, **35** (1990) 225–57.
19. Llory, M. A. Human reliability and human factors in complex organizations: epistemological and critical

analysis—Practical avenues to action. *Reliability Engineering and System Safety*, **38** (1992) 109–17.
20. Haber, S., O'Brien, J., Metlay, D. & Crouch, D. *Influence of Organizational Factors on Performance Reliability*. Vol. 1. NUREG/CR-5538, BNL-NUREG-52301, 1991.
21. Reason, J. Types, tokens and indicators. In *Proceedings of the Human Factors Society 34th Annual Meeting*. The Human Factors Society, Santa Monica, CA 1990, pp. 885–9.
22. Reason, J. *Human Error*. Cambridge University Press, Cambridge, UK, 1990.
23. Wreathall, J. & Appignani, P. One search for measures of maintenance effectiveness in safety. In *Proceedings of the International Conference on Probabilistic Safety Assessment and Management (PSAM)*. Elsevier Science Publishing Co., Inc., NY, USA 1991, pp. 31–35.
24. Hurst, N. W., Bellamy, L. J., Geyer, T. A. W. & Astley, J. A. A classification scheme for pipework failures to include human and sociotechnical errors and their contribution to pipework failure frequencies. *Journal of Hazardous Materials*, **26** (1991) 159–86.
25. Wreathall, J. Organizational factors relevant to safety. Paper presented at the 2nd Annual Information Exchange Meeting on NRC Organizational Factors Research, State College, PA., May 22–24, 1991.
26. Wreathall, J., Schurman, D. L., Modarres, M., Anderson, N. S., Roush, M. L. & Mosleh, A. Performance Indicators Integration Project—A Summary of Frameworks. NUREG/CR-5610, US Nuclear Regulatory Commission, Washington, DC, 1990.
27. Anderson, N. S., Schurman, D. L. & Wreathall, J. A structure of influences of management and organizational factors on unsafe acts at the job performer level. In *Proceedings of the Human Factors Society 34th Annual Meeting*. The Human Factors Society, Santa Monica, CA, 1990, pp. 881–4.
28. Modarres, M., Mosleh, A. & Wreathall, J. A framework for assessing influence of organization on plant safety. *Reliability Engineering and System Safety*, **38** (1992) 157–71.
29. Paté-Cornell, M. E. Organizational aspects of engineering system safety: The case of offshore platforms. *Science*, **250** (1990) 1210–17.
30. Paté-Cornell, M. E. & Fischbeck, P. S. Probabilistic risk analysis and risk-based priority scale for the tiles of the space shuttle. *Reliability Engineering and System Safety*, **40** (1993) 221–38.
31. Paté-Cornell, M. E. & Fischbeck, P. S. PRA as a management tool: Organizational factors and risk-based priorities for the maintenance of the tiles of the space shuttle orbiter. *Reliability Engineering and System Safety*, **40** (1993) 239–57.
32. Embrey, D. E. Incorporating management and organisational factors into probabilistic safety assessment. *Reliability Engineering and System Safety*, **38** (1992) 199–208.
33. Embrey, D. E., Humphreys, P. C., Rosa, E. A., Kirwan, B. & Rea, K. SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment. NUREG/CR-3518, US Nuclear Regulatory commission, Washington, DC, 1984.
34. Embrey, D. E. SLIM-MAUD: A computer-based technique for human reliability assessment. In *Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Safety Methods and Applications* 1985.
35. Galbraith, J. R. *Designing Complex Organizations*. Addison-Wesley, NY, USA, 1973.
36. Haber, S. B., O'Brien, J. N. & Ryan, T. G. Model development for the determination of the influence of management on plant risk. In *Proceedings of the* 1988 *IEEE Fourth Conference on Human Factors and Power Plants*. Institute of Electrical and Electronic Engineers, NY, USA, 1988, pp. 349–52.
37. US Nuclear Regulatory Commission, Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants. WASH-1400, Washington, DC, USA 1975.
38. Swain, A.D. & Guttmann, H. E. Handbook of Human Reliability Analysis With Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278, US Nuclear Regulatory Commission, Washington, DC, USA, 1983.
39. Apostolakis, G. E., Bier, V. M. & Mosleh, A. A critique of recent models for human error rate assessment. *Reliability Engineering and System Safety*, **22** (1988) 201–17.
40. Apostolakis, G. & Chu, T. L. The unavailability of systems under periodic test and maintenance. *Nuclear Technology*, **50** (1980) 5–15.
41. 'Improper Placement Led to AVB Flaw, says MITI'. *Nuclear News*, Aug. 1991 p. 94.
42. Apostolakis, G. & Kaplan, S. Pitfalls in risk calculations. *Reliability Engineering*, **2** (1981) 135–45.
43. Davoudian, K., Wui, J.-S. & Apostolakis, G. The work process analysis model (WPAM). *Reliability Engineering and System Safety*, **45** (1994) 107–25.
44. Saaty, T. L. *The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation*. McGraw-Hill NY, USA, 1980.