06/01/2005

ORGANIZATIONAL CONTRIBUTIONS TO NUCLEAR POWER PLANT SAFETY†

S. TINA GHOSH[1]* and GEORGE E. APOSTOLAKIS[2]
[1]US Nuclear Regulatory Commission
Office of Nuclear Material Safety and Safeguards
Mail Stop: T-7F27 Washington, DC 20555, USA
[2]Massachusetts Institute of Technology
Department of Nuclear Science and Engineering, and Engineering Systems Division
77 Massachusetts Avenue, Room 24-221, Cambridge, MA 02139-4307, USA
*Corresponding author. E-mail : tinag@alum.mit.edu

Received June 13, 2005

Nuclear power plants (NPP) are complex socio-technological systems that rely on the success of both hardware and human components. Empirical studies of plant operating experience show that human errors are important contributors to accidents and incidents, and that organizational factors play an important role in creating contexts for human errors. Current probabilistic safety assessments (PSA) do not explicitly model the systematic contribution of organizational factors to safety. As some countries, like the United States, are moving towards increased use of risk information in the regulation and operation of nuclear facilities, PSA quality has been identified as an area for improvement. The modeling of human errors, and underlying organizational weaknesses at the root of these errors, are important sources of uncertainty in existing PSAs and areas of on-going research. This paper presents a review of research into the following questions: Is there evidence that organizational factors are important to NPP safety? How do organizations contribute to safety in NPP operations? And how can these organizational contributions be captured more explicitly in PSA? We present a few past incidents that illustrate the potential safety implications of organizational deficiencies, some mechanisms by which organizational factors contribute to NPP risk, and some of the methods proposed in the literature for performing root-cause analyses and including organizational factors in PSA.

KEYWORDS : Organizational Factors, PSA, Human Error

1. INTRODUCTION

Some countries, like the United States, are moving towards increased use of risk information in the regulation and operation of nuclear facilities. The primary reason is to make decisions more rational – e.g., expending safety resources on structures, systems, components, and operational activities commensurate with their respective risk-significance. But decisions are risk-*informed*, meaning traditional safety strategies such as defense-in-depth and safety margins are still employed to some extent, not risk-based, because there are known uncertainties and incompleteness in existing probabilistic safety assessments (PSA).

Nuclear power plants are complex socio-technological systems that rely on the success of both hardware and human components. Weaknesses in modeling human failure events are an important source of uncertainty in existing PSAs [1-4], and human reliability analysis (HRA) is an on-going topic of research[5]. HRA is particularly of concern because analyses of past accidents and incidents at nuclear power plants show that both hardware and human failures are responsible for adverse events. In fact, empirical studies show that human failures dominate compared to hardware failures contributing to an accident or incident[6, 7]. Human actions can contribute to initiating events, and often play an important role in mitigating potential accidents and controlling the evolution of events after initiation of a potential accident sequence. Furthermore, human actions are important in pre-initiator situations because of contributions to latent failures in hardware that are not revealed until the hardware is needed during an incident evolution.

† This journal article was prepared, in part, by an employee of the United States Nuclear Regulatory Commission on her own time apart from her regular duties. NRC has neither approved nor disapproved its technical content.

Modeling human reliability is qualitatively different and more complicated than hardware failures because human failures are not random, but rather highly dependent on context, e.g., the evolution of a particular accident situation, the information available at the time of human action, the training and requisite knowledge of the team carrying out actions, and a variety of performance-shaping factors such as stress, fatigue or environment in which actions must be performed[8]. An important part of the context for human failure events is the operating organization within which people work. Thus a related PSA quality issue is organizational modeling, i.e., capturing the systematic contribution of operating organizations to safety.

Organizations are critical to safety in the nuclear industry. In both of the high-profile accidents at the Chernobyl reactor in 1986 and at the Three-Mile-Island reactor in 1979, detailed root-cause analyses identified organizational failures as important contributors to the accidents. The TMI-2 and Chernobyl accidents raised awareness in the nuclear industry of the importance of safety culture and other organizational issues related to the safe operation of nuclear power plants. Organizational deficiencies continue to be revealed periodically in less severe incidents. Recent incidents in the nuclear industry revealing multiple organizational weaknesses include the 1999 criticality accident at the Tokai-mura uranium processing plant in Japan, the 2002 discovery of severe degradation on the reactor pressure vessel head at the Davis Besse Nuclear Power Station in the United States, and the nuclear fuel damage incident at the Hungarian Paks nuclear power plant in April 2003. We note that the importance of organizational contributions to safe operations is not unique to the nuclear industry; it is important in all high-risk industries. Examples of prominent accidents with organizational root causes in other industries include the Bhopal chemical disaster, and the Challenger and Columbia space shuttle disasters. Empirical studies of operating experience (reported in Refs. [6, 7, 9, 10] demonstrate the importance of organizational culture, structure, and processes (how the organization carries out its work) in achieving safety in technologically complex hazardous operations. For the most part in current PSAs, these organizational effects on safety are not explicitly characterized and quantified but may be implicitly captured to some extent in the uncertainty distributions assigned to component failure and common-cause failure parameters. Hence organizational contribution to safety is a source of uncertainty and potential incompleteness in PSAs.

The questions of interest in this review paper are the following: Do organizations make important contributions to safety in NPP operations? How do organizations contribute to safety in NPP operations? And how can these organizational contributions be captured more explicitly in PSA? We start by recounting a few recent past incidents and analyses of events that illustrate the potential safety implications of organizational deficiencies. Next we present some of the mechanisms for organizational contributions to NPP risk discussed in the literature. In the following section, we review some methods for root-cause analysis that can reveal organizational weaknesses. Then we review examples of how the international community has approached organizational contributions to NPP safety. Finally we review a few methods proposed in the literature for inclusion of organizational factors in PSA, and conclude with some reflections on organizational influences in PSA and practical challenges.

2. ILLUSTRATIVE PAST INCIDENTS AND EVENTS

2.1 Davis Besse RPV Head Degradation Spring 2002

In spring 2002, significant damage was discovered on the reactor pressure vessel (RPV) head at the Davis Besse Nuclease Power Station (DBNPS) during its 13th refueling outage (13 RFO). The RPV head is of course a significant component of the reactor coolant pressure boundary and hence important for safety. The condition was classified as a serious incident, level 3 on the International Nuclear Event Scale (INES).

Vessel Head Penetration (VHP) nozzle leakage had been a problem at Babcock and Wilcox plants, either through axial or circumferential cracks. Davis Besse was suspected to be suffering nozzle leakage prior to 13 RFO. Near the end of 2001, the US regulator, US Nuclear Regulation Commission (USNRC), was preparing to order the DBNPS shut down by December 2001 for a full inspection, but the operating organization provided additional information to the USNRC and obtained approval to postpone a full inspection until the 13th RFO, moved up six weeks to mid-February 2002 [11].

During the 13th RFO at DBNPS, 5 of the 69 nozzles were found to be cracked, and three nozzles had complete through-wall cracking which allowed RCS leakage onto the RPV head. In this case, the boric acid had eaten away approximately 70 pounds of the carbon steel RPV head, covering an area about 20-30 square inches and total 6.63 inch depth of the RPV head in some places. This left only the stainless steel liner (the cladding layer), merely 1/8 inch thick in some places, to withstand the high pressure of the RPV[12, 13].

Some of the significant aspects of this incident include the following: (1) boric acid corrosion of control-drive rod mechanism (CRDM) penetrations into the RPV head was a known possibility yet for years investigations were inadequate to determine whether this was occurring at Davis Besse; (2) the condition had existed for several years at Davis Besse before discovery; (3) there were a number of warning signs from different plant systems, such as excessive clogging of containment air filters and inability to completely clean crud off the RPV head during

previous refueling outages, that were not considered in an integrated and holistic fashion to infer sooner that corrosion was occurring; (4) the licensee originally intended to keep operating for a longer period of time beyond the refueling outage when the degradation was discovered during an inspection of all CRDM nozzles.

The Davis-Besse Root Cause Analysis Team that focused on underlying management and organizational reasons for the RPV head degradation identified the following root causes, contributing causes, and related observations [14]:

Root Causes
1. Less than adequate nuclear safety focus (safety culture problem).
2. Less than adequate implementation of the corrective action program.
   a. Addressing symptoms rather than causes.
   b. Low categorization of symptoms.
   c. Less than adequate cause determinations.
   d. Less than adequate corrective actions.
   e. Less than adequate trending.
3. Less than adequate analyses of safety implications.
4. Less than adequate compliance with Boric Acid Corrosion Control (BACC) Procedure and In-service Test Program.

Contributing Causes
1. Lack of Hazard Analyses.
2. Corrective Action Procedure – has provisions that do not reflect state-of-the-art practice in industry.

Related Observations
1. Design – failed to prevent boric acid leaks.
2. Training – insufficient for boric acid corrosion.
3. Coordination of Boric Acid control activities – RPV head inspection activities and corrective action documents on head not coordinated through BACC coordinator.
4. BACC procedure – does not identify CRDM nozzles as one probable location of leakage.
5. Untimely Corrective Action – condition reports unresolved until significant degradation occurred.
6. Quality Assurance – little evidence of QA involved in this area.
7. Incentives Program – monetary incentive program rewards production more than safety at senior levels of the organization.
8. Policies on Safety – inconsistent and incomplete, and do not provide strong safety focus.
9. Operations Involvement – was minimal in resolution of boric acid issues.
10. Management Observations – management has minimal entries into containment and observation of conditions in the containment.

As this root-cause analysis showed, and other peer and oversight assessments generally agreed [11], organizational problems were at the root of this serious incident.

2.2 Paks Fuel Damage Event in Spring 2003

There was a fuel damage incident in April 2003 at the Paks Nuclear Power Plant, during ex-core cleaning of corrosion deposits from the fuel. This was classified as a serious incident, level 3 on the INES scale. The fuel was cleaned in a pool with circulating water to keep it cool. During cleaning, the cooling of the fuel was insufficient because of deficiencies in the design of the cleaning system: (1) the capacity of the cooling water pump was not large enough for the job; (2) the location of the outlet of the inner vessel at the bottom enabled it to become partially clogged with corrosion deposits; (3) available paths for water that would bypass the fuel elements (and hence not contribute to cooling) were recognized but not addressed effectively; (4) slight mis-alignment of the fuel in the cleaning chamber would reduce cooling flow, yet there was only one fuel guide plate; (5) the time to boiling in the case of insufficient cooling was very small. In addition, there was no effective monitoring system to detect problems in the cleaning chamber and notify personnel in the form of an alarm. To exacerbate this situation, the operational personnel for the cleaning job were not aware of the time pressure to recover in the case of reduced cooling, and had inadequate operating instructions and event recovery procedures. In the incident, water started boiling because of insufficient cooling and it was not discovered immediately. Actions during recovery further exacerbated the fuel damage, because lid removal operation was initially ineffective (one of the ropes broke) which delayed recovery, and the sudden influx of cold water during recovery resulted in thermal shock to the fuel elements resulting in further mechanical degradation (i.e., fuel rods were broken). As a result, 30 fuel elements were severely damaged[15, 16].

The Hungarian Atomic Energy Authority and the International Atomic Energy Agency (IAEA) identified numerous safety management and safety culture weaknesses implicated in this incident [15, 16], including:
- Commitment to safety.
- Conservative decision making – the schedule for design, fabrication, installation, testing and operating of the fuel cleaning system was aggressive (on the scale of a few months), and the sense of urgency contributed to a lack of rigor in the nuclear safety assessment and design review.
- Use of procedures.
- A reporting culture – problems in implementing procedures were not reported, e.g., delays in opening the fuel cleaning tank for earlier batches, and personnel were not aware of commitments in the safety analysis related to the implementation problems.
- Challenging unsafe acts and conditions – no evidence that anyone challenged the design or operation of the

fuel cleaning system even though the analysis showed that boiling could occur in 9 minutes following loss of cooling.
- A learning organization – there were no indications that inter-organizational unit communication was encouraged except through managers, and thus opportunities to share information was reduced which affected the knowledge of personnel in emergency preparedness and radiation protection organizations.

Once again, organizational problems were at the root of this serious incident.

2.3 International Events that Highlight Recurring Organizational Deficiencies

The OECD's Nuclear Energy Agency's (NEA) most recent report on recurring events in the nuclear industry included a section on recurring management and organizational factors that were revealed as root causes in multiple events [10]. These events occurred in the late 1990s in multiple countries. A few examples of events involving disabled safety systems from different countries include the following:

1. Short-term inoperability of all four EDGs at a unit while at full power (in 1999). The hardware cause was that a switch was in the wrong position at each diesel (IRS #7433).
2. Total loss of essential and auxiliary service water service systems (in 1999). The hardware cause was an incorrect line-up of the inlet valves during a periodic test of gate valves associated with the essential and auxiliary service water systems. In this case, the control room detected the problem and effectively directed field personnel to restore service water (IRS #7327).
3. Both core spray pumps in a BWR (in 1995) were rendered inoperable and the condition was not discovered for a week. The hardware cause was the pump motors were not connected; they had been disconnected during a containment leak test and were not reconnected properly (IRS #7303).

Common safety management deficiencies at the root of the analyzed events included:
- Deficiencies in safety culture in general
- Deficiencies in communication
- Deficiencies work practices such as not following procedures, lack of clear work responsibility, improper use of system diagrams
- Deficiencies in procedures, instructions, work orders, administrative orders, and work control
- No common understanding of design basis document review process, lack of design basis information available
- Failure to act appropriately after the identification of a significant deficiency
- Inadequate management oversight
- Heavy workloads and conflicts between personal safety and configuration management
- Insensitivity to shutdown risk activities among multiple organizational units within licensee organization.

2.4 Analysis of events in the US

A few years ago, 48 events at US NPPs were analyzed thoroughly for human performance contributions[17]. In 37 of the 48 events, human errors were included among the root causes, and most events contained multiple human errors as root causes. Table 1 lists the error categories identified for the 270 human errors in these events. While this was not a very large sample of events, the analysis does illustrate what kinds of errors have occurred in operations and gives an indication of the relative prevalence of different kinds of errors. Latent weaknesses in organizational factors contributed to all of these events; the mechanisms for these organizational effects are discussed in the next section.

3. MECHANISMS OF ORGANIZATIONAL RELIABILITY

There are at least three levels of socio-technical analysis for operating organizations: individual, organization, and environment. At the *individual* level, analysis concentrates on the mechanisms by which human operators may err or make unsafe decisions. Human reliability analysis (HRA) techniques concentrate on the individual level of analysis. Analyses at the *organizational* level focus on how the operating organization's structure, processes, culture, and other factors contribute to safety management and reliability. The *environmental* level of analysis focuses on interactions between the operating organization and other external organizations with which the operating organization has relationships, e.g., the regulatory environment, the financial environment in the industry. All three levels of analysis are related – for example, many of the effects of organizational reliability are realized in individuals' acts, and the environment within which the organization operates influences its culture and behavior. This paper is focused on reliability at the organizational level specifically.

There are many mechanisms by which organizations affect NPP safety, as apparent from operating experience:
- Organizational processes (e.g., maintenance practices) can contribute to common-cause failures of multiple redundant components, e.g., through a systematic miscalibration of sensors, or other deficient maintenance practice used on multiple components. This was the case in the event above where all 4 EDGs were inoperable because of a switch mispositioned systematically on all 4 EDGs.
- Organizational processes and factors can contribute to common-cause failures of diverse components, which is particularly troubling since typically these are not modeled in PSAs. For example, in one event presented in Ref. [18], there was strong evidence that a single organizational deficiency, "goal prioritization," resulted

Table 1. Summary of Human Error Categories and Subcategories in 37 Analyzed Operating Events in the US [17]

Category Description	# Errors	% Latent in Category	% of Total Errors	% of Events where Category Present
Operations	***72***	***43%***	***27%***	***54%***
Command and control including resource allocation	18	22%		
Inadequate knowledge or training	23	65%		
Operator action/inaction	16	23%		
Communications	15	60%		
Design and Design Change Work Practices	***70***	***96%***	***26%***	***81%***
Design deficiencies	24	100%		
Design change testing	9	100%		
Inadequate engineering evaluation and review	19	95%		
Ineffective abnormal indications	3	33%		
Configuration management	15	100%		
Maintenance Practices and Maintenance Work Control	***58***	***92%***	***21%***	***76%***
Work package development, QA and use	16	94%		
Inadequate maintenance and maintenance practices	31	90%		
Inadequate technical knowledge	5	100%		
Inadequate post-maintenance testing	6	100%		
Procedures and Procedures Development	***26***	***96%***	***10%***	***38%***
Corrective Action Program	***33***	***100%***	***12%***	***41%***
Failure to respond to industry and internal notices	8	100%		
Failure to follow industry practices	4	100%		
Failure to identify by trending and use problem reports	9	100%		
Failure to correct known deficiencies	12	100%		
Management and Supervision	***11***	***91%***	***4%***	***30%***
Inadequate supervision	9	89%		
Inadequate knowledge of systems and plant operations	1	100%		
Organizational structure	1	100%		

in the main hardware failures in two dissimilar systems, the start-up boiler and the atmospheric dump valve.

- Latent organizational weaknesses are particularly insidious since they can remain hidden in the system for a long time. Examples of latent deficiencies include: inadequate training is not revealed until an incident where that aspect of training was required; procedure deficiency not revealed until a particular step is required; work-arounds may be fine most of the time, but in sporadically challenging situations more formal procedures are needed and not used. Human-error theorist James Reason uses the analogy of Swiss cheese to explain how latent weaknesses can lead to accidents – we can think of the system as Swiss cheese where the holes represent missing barriers/latent weaknesses and solid parts represent working barriers; the solid part of the cheese will prevent complete penetration/failure in most instances, but in the rare cases when all the holes line up, the entire system can be defeated[6]. Latent organizational weaknesses were revealed in the 2003 fuel damage incident, for example, and in all the events in Ref. [17] (see "% latent in category" column in Table 1).
- Organizational culture, in particular safety culture, is a pervasive issue that affects all aspects of operations. This is evident in numerous past incidents and events, such as the 2003 Paks fuel damage incident presented above. In this case, safety culture affected multiple processes within the plant including the design process, normal operations, and emergency recovery operations, and cut across multiple organizational units within the organization. This pervasive weakness was revealed when the system was challenged.

- Many of the mechanisms of organizational contributions to unreliability are not captured (at least not explicitly) in plant PSAs, and hence are sources of uncertainty and incompleteness in PSAs, and may lead the plant to unanalyzed conditions. In addition, initiating events may be caused by plant personnel actions during routine activities (that are heavily influenced by organizational factors); these pre-initiators are likely to be another source of incompleteness in PSAs[19, 20].
- On the positive side, organizations and people are a very important layer of defense in defense-in-depth operations at NPPs. For example, for emerging safety issues, perhaps related to aging-related degradation phenomena or power-uprate related system challenges, people and good organizational processes may be best able to identify these issues before they become a safety problem.
- Similarly, organizations that are well-positioned to handle challenging situations may be better at averting accidents, e.g., through effective recovery actions. A good example of this was in the second example in section 2.3, where control room operators immediately recognized the loss of essential and auxiliary water and effectively implemented recovery actions.

Based on past events, we have insights about specific aspects of organizational reliability that are important in terms of organizational performance, organizational processes and organizational factors, and safety culture.

3.1 Organizational Performance

The organization is responsible for managing safety and must carry out important functions, such as effective problem identification and resolution. We depend on organizations to discover latent deficiencies, e.g., in designs or procedures, possess adequate requisite knowledge to carry out its functions, learn effectively from its own experiences and those of others in the industry, and conservatively (from safety standpoint) interpret limited information when faced with uncertainty. In the US regulatory oversight program for NPPs, there are three cross-cutting areas in the reactor oversight process and all of them are related to organizational factors and processes (see next paragraph) to achieve necessary safety performance. The cross-cutting issues are called such because they affect all aspects of safe operations. The cross-cutting areas are[21]:

- Human performance
- Safety-conscious work environment, i.e., management attention to safety and workers' ability to raise safety issues
- Problem identification and resolution, i.e., effectiveness of corrective action programs.

3.2 Organizational Processes and Organizational Factors

The functions above are fulfilled through organizational processes, i.e., the processes by which work is performed. For example, problems could be identified in the systematic evaluation of operating experience (operating experience evaluation process), or through the reporting of events and conditions (condition reporting process). Then they may be resolved through the corrective action program through maintenance processes, or other processes such as re-writing procedures. These processes together are responsible for achieving effective organizational learning and safety management.

Organizational Factors (OFs) describe how the organization is working at the macro level. For example, the OF "communications" refers the exchange of information, both formal and informal, between different departments of units within the plant, between a given department or unit, between the plant and its parent organization, etc. Examples of organizational factors implicated in past NPP events include [18, 22-26]:

- Communication – the exchanges of information, both formal and informal.
- Formalization – the extent to which there are well-identified rules, procedures and/or standardized methods for routine activities and unusual occurrences.
- Goal prioritization – the extent to which plant personnel acknowledge and follow the stated goals of the organization 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 – the extent to which plant personnel use their knowledge to identify potential problems.
- Resource allocation – manner in which the plant distributes its resources (esp. financial). Refers to the actual and perceived distribution.
- Roles and responsibilities – the degree to which work activities are clearly defined and the degree to which plant personnel carry out those work activities.
- Technical knowledge – the depth and breadth of requisite understanding that plant personnel have regarding plant design and systems, and the phenomena and events that bear on their safe and reliable operation.

3.3 Safety Culture

Safety culture is an aspect of organizational culture that deserves special attention. Organizational culture refers to "plant personnel's shared perceptions of the organization. It includes the traditions, values, customs, practices, goals and sociali-zation processes that endure over time and that distinguish an organization from others. It defines the 'personality' of the organization"[18, 23]. While there are still multiple definitions of safety culture in the literature [24], one commonly accepted definition is from the IAEA's International Safety Advisory Group (INSAG) INSAG-4 report: "Safety culture is that

assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance" [27]. Personnel attitudes and motivation for carrying out their work is an important aspect of safety management. As mentioned above, the organization makes important contributions to defense-in-depth – e.g., through human recovery actions, and its ability to erode or defeat multiple layers of defense in defense-in-depth system [9]. Safety culture, as defined in INSAG-4, enco-mpasses both behavior of individuals and organizations and the structural aspects of organizations; as such, safety culture encompasses organizational performance and organizational processes as well. Recent operating experience in the US, Germany, Canada, and Japan have indicated weaknesses in safety culture at a few individual plants [20]. The relationship between safety culture and a reliability measure (such as failure rate) is hypothesized in a Swedish Nuclear Power Inspectorate (SKI) report – e.g., for a particular hardware system, compared to the failure rate at a plant with "normal" safety culture, the same system is likely to have a higher mean failure rate at a plant with "low" safety culture and a lower mean failure rate at a plant with "high" safety culture (see Ref. [28] for details.) Some frequently cited safety culture attributes (some of which coincide with important organizational factors) are [22]:

- Roles/responsibilities/accountabilities
- High priority to safety
- Openness and communications
- Organizational learning
- Top management commitment to safety
- Initial and continuing training
- Employees have a questioning attitude
- Recognizing employee's efforts
- Appreciation of risks
- Self-assessment
- Technical competence.

4. DIAGNOSING POTENTIAL ORGANIZATIONAL DEFICIENCIES: REVIEW OF METHODS FOR EXTENDED ROOT-CAUSE ANALYSES

Analysis of actual events is of course an important way to gain insights into organizational contributions to safety. Root-cause analyses are retrospective analyses to identify the root and contributing causes to an accident or incident. There are several available methods that help analysts identify organizational contributions through root-cause analysis. First we present a few methods that are used in practice in the nuclear industry to analyze significant events in operating experience. Then we present a method proposed in the literature that is targeted towards identifying the latent conditions that exist in organizations and create contexts for human errors.

4.1 Error Cause and Factors Charts, Hazard-Barrier Analysis, Change Analysis

Root-cause analyses after an incident typically begin with interviews of personnel who were involved, reconstruction of the evolution of the incident, and eventual identification of the root and contributing causes. Error Cause and Factors (ECF) charts and analysis are one way to organize the information gained through the investigations, and to identify areas to probe further. The ECF chart displays the sequence of events and conditions leading up the incident initiator and throughout the evolution of the incident. An *event* is defined as "any action or occurrence that happened at a specific point in time relative to the hardware failure or human performance problem under investigation" and is shown as a rectangle; a *condition* is defined as "a state or circumstance that affected the sequence of events in the ECF chart" and is shown as an oval; *significant events* are those that led directly to, or were necessary to bring about, the hardware failure or human performance problem, and are shown as diamonds; *causal factors* are identified in octagons [29, 30]. The purpose of the ECF analysis is to tell the story of the incident and its causes. Fig. 1 shows part of an ECF chart from a RCS overpressurization event.

Hazard-Barrier analysis is another RCA technique used that can focus on the organizational and management contributions to an incident. The purpose of a barrier analysis is to identify the physical and management barriers that should exist to prevent the incident under investigation, and which barriers were missing, bypassed

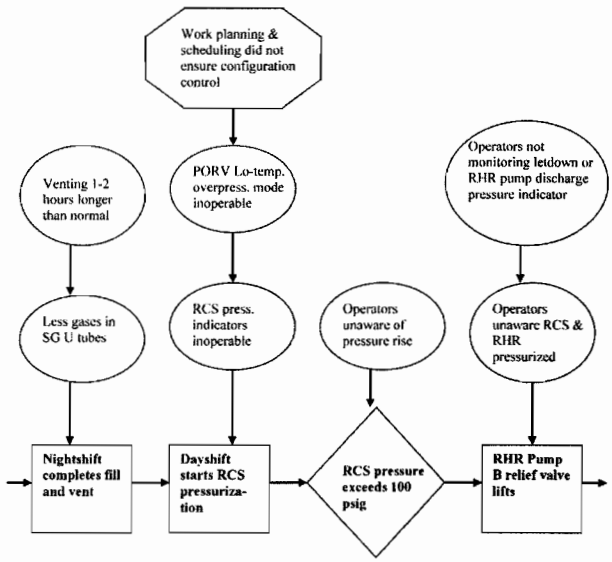

Fig. 1. Example of Partial ECF Chart from RCS Overpressurization Event [29]

Table 2. Example of Partial Hazard-barrier Analysis for RCS Overpressurization Event [29]

Hazard: Pressure		**Target** : Catastrophic failure of system piping	
Physical Barrier	**Performance**	**Why Did it Fail?**	**Effect on Event**
RCS pressure instrument transmitters	Failed	Out of service for maintenance	RCS pressure indicators inoperable so operators could not detect rapid pressure rise
RHR Pump B suction relief valve	Succeeded in stopping uncontrolled pressure rise		Maintained pressure below limits – prevented catastrophic failure of RHR piping
Management Barrier	**Performance**	**Why Did it Fail?**	**Effect on Event**
Startup procedures	Did not control RCS vent evolution	Fill and vent procedure did not specify a time limit for venting gases from reactor head	Night shift extended the RCS vent evolution 1-2 hours longer than normal, reducing the volume of gases remaining in the SG U tubes
Work management (planning and scheduling)	Failed	Work planners overlooked the need for the RCS pressure instruments to be operable before initial pressurization of the RCS	Pressurization was initiated without RCS pressure indications operable
Independent review	Missing	Not performed or required	Failed to identify the RCS pressure instrument isolation

Table 3. Example of Partial Change Analysis for RCS Overpressurization Event [29]

Event Situation	**Event-Free Situation**	**Difference**	**Effect on Event**
RCS pressure instrument transmitters isolated for maintenance	RCS pressure indicators operable	No accurate indications of RCS pressure were available	Operators were unable to monitor RCS pressure
Reduced volume of gases in SG U tubes caused by longer vent times	Greater volume of gases in SG U tubes	Reduced amount of non-condensable gases caused RCS pressure to increase sooner than in previous refill operations	RCS pressure rose sooner than expected and approached 100 psig within 2.5 hours of initiating pressurization
Operators were monitoring the inoperable RCS pressure gauges, but not all available pressure indications (e.g., letdown and RHR discharge pump pressure gauges)	Operators monitored all available pressure indications	Operators did not detect indications of the rapid pressure increases on the letdown and RHR discharge pump pressure gauges	An opportunity to detect the pressure rise and prevent the overpressurization was missed

or failed, and their causal role in the incident. The analysis identifies *hazards*, the potential sources of harm, *targets*, which are personnel and equipment that must be protected, and *barriers* that should prevent the hazards from harming the targets. Examples of management barriers are maintenance, training, supervision, and the design of the human-system interface or procedures. Table 2 shows part of a hazard-barrier analysis for the same RCS overpressurization event analyzed in Fig. 1.

Change analysis is another RCA technique that involves "systematically identifying and analyzing any changes that may have affected the problem under investigation." The goal is to identify changes in the work environment that resulted in unanticipated and unwanted consequences

that affected the incident. Examples of such changes are work activities that were carried out concurrently with the work activity of interest, equipment condition, and management expectations for the work. Table 3 shows an example of change analysis for the same RCS overpressurization event.

All root-causes analysis techniques help the analyst provide structure to the incident investigation, guide the analyst to ask questions during the investigation that will reveal the root and contributing causes of the incident, with the ultimate goal of preventing recurrence.

4.2 CATILaC

The Computer-Aided Technique for Identifying Latent Conditions (CATILaC) is another method proposed in the literature to aid root-cause analysis, specifically to identify latent organizational weaknesses. The method combines elements of Reason's model [6], the WPAM model [31], and research on organizational factors [26]. The CATILaC approach provides a systematic way to guide root-cause analysis (RCA) to: (1) relate hardware failures to the operating organization and latent conditions within the organization; (2) relate latent conditions to organizational factors; (3) facilitate identifying more effective corrective actions to prevent repeat problems; (4) create an easily searchable summary database for the user.

There are three essential features of the method: (1) it takes advantage of the fact that NPPs operate like machine bureaucracies (defined in Ref. [32], based on Max Weber's seminal work in the early 1900s on bureaucratic organizations) that are highly specialized, with routine operating tasks and very formalized procedures in the operating core; and analyze failures in terms of their locations within the organization -- i.e., which program, which work process(es) (WP) within a program, which task within each work process, and so on [31]. Fig. 2 shows

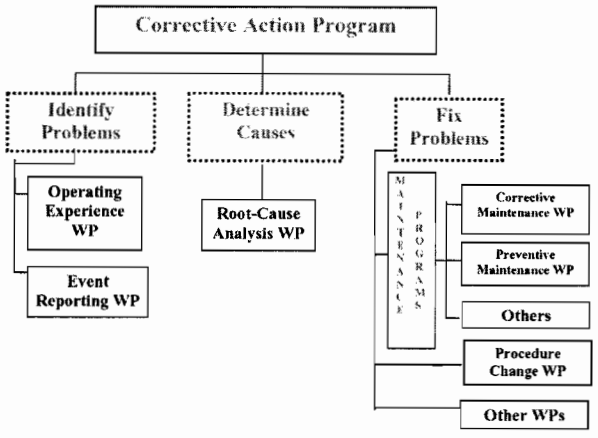

Fig. 2. Example of a Typical Program Found in Nuclear Power Plant Organizations [18]

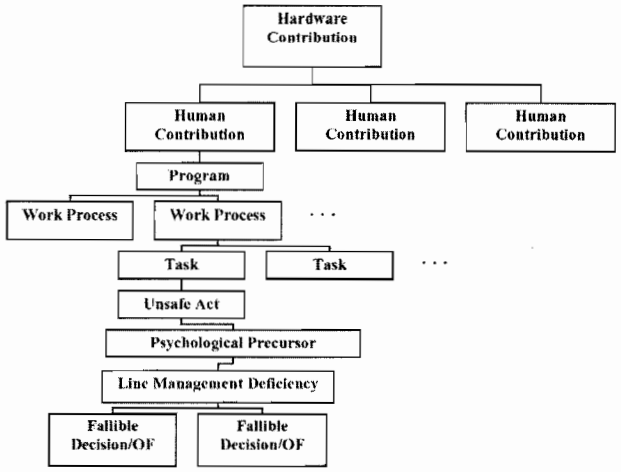

Fig. 3. Extended Root-Cause Analysis Framework Implemented in CATILaC [26]

an example of a typical program (adapted from Ref. [31] and Ref. [18]). A typical work process consists of the following sequential tasks after initiation: (I) Prioritization, (II) Planning, (III) Scheduling/Coordination, (IV) Execution, (V) Return to normal line-up, and (VI) Documentation; (2) it tracks latent conditions in organizational factors (OFs); (3) Recently an augmented version of the approach, A-CATILaC, has been proposed, which adds a dimension to the analysis that focuses more explicitly on the decision - making perspective of *individuals* within the organization [33]. The individual dimension was added because everything that is important can not be captured by looking at macro-factors of the organization as a whole. There may be sub-cultures within the organization and/or individuals' goals and priorities may be in tension with those of the overall organization [34]. These aspects are important to capture, particularly with respect to safety culture.

A-CATILaC is a Microsoft® Access database program that guides the analyst to make consecutive inputs according to Fig. 3. Each analysis starts with a list of hardware contributions identified. Then for each hardware contribution, the analyst identifies the program within the operating organization, then the work process within the program, then the task within the WP where the hardware contribution originated. For each task, the analyst identifies the unsafe act committed by the responsible person. Then for each unsafe act, psychological precursors and OFs can be identified [18]. Lastly, the analyst is guided to probe reasons for the unsafe act from the perspective of the individual decision-maker, in terms of the *information* and *incentives* motivating him at the time of the decision (these concepts are based loosely on IAEA's model for organizational management of safety culture [35]). Examples of information deficiencies include: (1) an inadequate work order if the company as a whole had the information to

make the right decision but the individual did not; (2) inadequate company knowledge; or (3) inadequate knowledge at the level of the industry as a whole; as new hardware degradation mechanisms are observed with aging, for example, there may be *surprises* for the entire industry, not just an individual or operating company. Examples of deficiencies in incentives include: (1) work load management; (2) work practices and norms; and/or (3) reward system within the organization. Evaluating incentives is a way to probe the more amorphous *safety culture* issue. For example, if the leadership of the operating organization has set improper norms, this may be revealed in individuals' unsafe decisions. Findings from all event analyses are stored in a searchable database. This allows trending, identification of OFs implicated in multiple events, and identification of which OFs are most important to various WPs/tasks within WPs and programs (see Ref. [18] and Ref. [26] for further details).

5. APPROACHES USED TO ADDRESS ORGANIZATIONAL ASPECTS OF NPP SAFETY

As mentioned above, the importance of organizational aspects of NPP safety has been recognized internationally for a while. International and national agencies have taken different approaches to addressing organizational safety management. Here we present two examples – the IAEA's on-going services for safety culture and operational safety management, and the US regulator's approach to addressing the organizational weaknesses revealed in the 2002 Davis Besse incident.

5.1 IAEA

The IAEA's approach to enabling effective safety management is to offer a series of services and guidance for evaluating and improving organizational aspects of NPP safety. The Operational Safety Review Team (OSART) is one example. It is comprised of international experts who provide in-depth reviews of NPP operational safety performance upon request [36]. The scope of reviews include: management, organization and administration; training and qualification; operations; maintenance; technical support; radiation protection; chemistry; emergency planning and preparedness; construction, commissioning, etc. The IAEA also has a Peer Review of Operational Safety Performance Experience (PROSPER) program to promote organizational learning processes and practices at individual NPPs, i.e., learning from plant and industry operating experience [36]. The IAEA also offers a Safety Culture Assessment Review Team (SCART). The SCART provides external peer reviews of an operating organization's safety culture. SCART missions are:

"· Assisting key staff at the operating organization or advising on ways in which improvements to safety culture might be achieved
· Identifying good safety culture practices, which are unique and worth bringing to the attention of other operating organizations
· Providing opportunities to experts from Member States to broaden their experience and knowledge of safety culture [37]."

Similarly, the Safety Culture Enhancement Program (SCEP) assists countries in enhancing the safety culture of nuclear installations[37].

INSAG has published a series of guidance documents to help nations and NPP operating organizations recognize and implement important aspects of safety culture [27, 38, 39]. Other international advisory groups have published similar guidance documents, for example, Germany's International Committee on Nuclear Technology's (ILK) recent statement on the regulator's management of the licensee self-assessments of safety culture [40].

5.2 Davis Besse Restart Conditions

After the 2002 Davis Besse incident, the US Nuclear Regulatory Commission (USNRC) specified conditions that the operating organization had to meet before restarting the reactor. Because deficiencies in safety culture and corrective action programs were implicated in the organization's root-cause analysis, the USNRC specified restart requirements for the plant programs. The following were identified for scrutiny under the topic of "Adequacy of Safety Significant Programs": (a) Corrective Action Program; (b) Operating Experience Program; (c) Quality Audits and Self-Assessments of Programs; (d) Boric Acid Corrosion Management Program; (e) RCS Unidentified Leakage Monitoring Program; (f) In-Service Inspection Program; (g) Modification Control Program; (h) Radiation Protection Program; (i) Process for Ensuring Completeness and Accuracy of Required Records and Submittals to the NRC. The following were scrutinized under "Adequacy of Organizational Effectiveness and Human Performance": (a) Adequacy of Corrective Action Plan in the Organizational Effectiveness and Human Performance Area; (b) Effectiveness of Corrective Actions in the Organizational Effectiveness and Human Performance Area. Each of these areas were investigated in depth, and the plant was not allowed to restart until the operating organization could demonstrate that performance in each of these areas was adequate.

6. METHODS FOR MODELING AND INCLUDING ORGANIZATIONAL FACTORS IN PSA

Methods for the explicit inclusion of organizational effects in PSA are not yet well-developed or tested. Several methods have been proposed in the literature, but not many are commonly used in actual PSAs. Several of the proposed

approaches in the literature have been geared to other hazardous industries – aerospace systems, off-shore oil drilling platforms, and medical procedures. These methods could be useful for nuclear industry applications as well. One example is an approach developed for analyzing organizational influences in major rail accidents. The MACHINE (Model of Accident Causation using Hierarchical Influence Network) model is used to capture the effect of organizational and management factors in the PSA for rail systems (see Ref. [41] for details). Another example is the System-Action-Management (SAM) approach, which is similar to WPAM approach discussed below, in that it connects organizational and management factors to PSA by modifying the frequency of the PSA's minimal cut sets (MCS), through the use of expert elicitation methods to quantify the effects on the MCS (see Ref. [42] for details).

We present three proposed methods – one that explicitly includes the influence of organizational factors on component unreliabilities in the PSA, one that connects organizational factors to the frequency of minimal cut sets in the PSA, and one that incorporates dynamic modeling of NPP programmatic processes to connect programmatic performance to plant risk.

6.1 The Omega Factor

The omega factor approach focuses on explicitly including organizational influences on reliability at the component level. The motivation for developing the approach came from a previous study that had found that plant maintenance practices could explain a significant part of the differences between generic PSAs and plant-specific PSAs; i.e., one plant's increased component unavailability compared to generic industry average was found to be due in large part to an idiosyncrasy in the plant's maintenance program. "The form of dependence is through increase or decrease in failure probabilities of multiple components due to changes in their common organizational influences. In other words, under the influence of a poor organization, failure rates of components will probably be higher" [43].

The PSA component reliability parameters (e.g., component failure rate) are divided into two parts – the rate of inherent failures, and the rate of failures due to adverse organizational factors:

$$\lambda_T = \lambda_I + \lambda_O \tag{1}$$

where λ_I = "inherent" failure rate and λ_O = rate of failure due to organizational factors. A parameter ω is introduced that is a measure of the relative contribution of organizational factors and is defined as:

$$\omega = \frac{\lambda_O}{\lambda_I} \tag{2}$$

Similarly, the authors suggest that a factor can be introduced for other PSA parameters, e.g., the average maintenance duration, τ, can be re-written as:

$$\tau_T = (\omega_M + 1)\tau_I \tag{3}$$

There are two ways to estimate ω – directly from data, or from the probability, P, that a worker will be adversely influenced by organizational factors (ω is a function of P). P in turn can be estimated through analysis of operating data (where it exists) for specific mechanisms of influence, or can be calculated. In the authors' analysis of 10 years of licensee event reports for containment spray pumps from several different plants, organizational factors (such as procedure or training weaknesses) were responsible for the majority of events (75%). (See Ref. [43] for further details.)

6.2 The Work Process Analysis Model II

WPAM-II is another method proposed in the literature to capture organizational effects in PSA. The goal of WPAM-II is to connect organization factors (OFs), work processes, and PSA parameters to help quantify the effect of OFs on plant safety [31]. One key idea is that dissimilar components and subsystems can become coupled through the organization, leading to potential common-cause failures that are not modeled in the PSA [18]. Another key idea is that some organizational factors will figure more prominently in particular work processes and/or components /subsystems; not all OFs are equally important across functions, processes, and components. So more specifically, the goal is to identify and quantify the common-cause effect of organizational factors that cause PSA "candidate parameter groups" (CPG) to become coupled, hence leading to underestimation of plant risk, if assumed independent. WPAM-II re-calculates probabilities for minimal cut sets (MCS) by considering these organizational dependencies among the basic events comprising the MCS.

This is accomplished through several steps. First, a basic-event vector is defined that identifies for each basic event the relevant:

(1) Work Process (WP) (as defined above).
(2) Candidate Parameter Group (CPG). The six CPGs are (i) failure to restore equipment to normal configuration after test/maintenance, (ii) miscalibration of equipment, (iii) unavailability due to maintenance, (iv) failure to function on demand, (v) common cause failure due to factors other than human errors, and (vi) available time for recovery.
(3) Working Unit (WU), which identifies four working units which may interact with plant equipment. These can be (i) operations, (ii) maintenance—mechanical, (iii) maintenance—electrical, or (iv) instrumentation and control.
(4) the System/Component Identification (ID). This is the

identification that exists in the basic-event description in the PSA, which includes the type of failure (e.g., human error, pump failure), failure mode (e.g., miscalibration, failure on demand), and the component/system identification (e.g., pump No. 2 in loop A) [31].

Then for each of these four dimensions, a correlation matrix is created to quantify the degree of dependence among possible values. So for example, for the work process dimension, the correlation $R_{WP} = 1$ if two basic events involve the same WP, and $R_{WP} = 0$ otherwise. As another example, for the six possible candidate groups, correlation assignments range from 0.01 to 1.0 as follows: $R_{CPG} = 1.0$ for human actions represented by similar candidate groups; 0.5 for human actions represented by dissimilar candidate groups; 0.1 for hardware-related problems represented by similar candidate groups or for one human action and one hardware problem; and 0.01 for hardware-related problems represented by dissimilar candidate groups.

The MCS frequencies are modified to reflect the rated correlation:

$$f_{mcs}=f_{ie}*p_1*p_{2/1} \quad (4)$$

where f_{mcs} is the core damage frequency contributed by the MCS; f_{ie} is the initiating event frequency; p_1 is the probabilities of the basic events that are modeled by candidate parameter groups; and the Success Likelihood Index (SLI) method [44] is used to calculate $p_{2/1}$. For each CPG_j, the OFs are weighted $W_{OF,j}$ according to importance. The weights W_j were obtained from expert elicitation (in the 1994 study).

A case study using this approach based on preliminary estimates showed that the common-cause effect of organizational factors on basic-event probabilities could lead overall to a core damage frequency twice as large as the original estimate that did not consider common-cause effects due to OFs (see Ref. [31] for details).

6.3 Dynamical Systems Modeling of NPP Programmatic Performance

The US industry (Electric Power Research Institute, EPRI) recently sponsored an exploratory study into the dynamic modeling of NPP programmatic processes to connect programmatic performance to plant risk[45]. The authors of the study note that the plant design is relatively static, and the changes and dynamic features of operations are mainly due to plant programs and processes, and that age related failure mechanisms also spur changes in plant programmatic factors. The industry developed a multilevel process model as a management tool, called the Standard Nuclear Process Model (SNPM). The SNPM defines five core processes, (1) plant operations, (2) plant configuration control, (3) work management, (4) equipment reliability, and (5) materials and services; and three enabling processes that impact the plant directly, (6) support services, (7) loss prevention, and (8) training. These processes are further decomposed into subprocesses that describe in more detail the necessary functions that comprise each process. One of the main goals of this work is to quantitatively describe the effect of programmatic factors on plant risk. In the preliminary work, the authors developed a quantitative dynamic model that matched the qualitative relationships among these eight processes and plant risk that have been assumed in the past by other experts and methods. This is a potentially useful method to track risk implications of organizational and management factors; the ability of empirical verification is limited at the time, because the necessary data is not collected at NPPs. Future empirical verification (based on real operating experience) would lend more confidence on the accuracy and utility of the method.

7. CONCLUSIONS

Based on operating experience, there is no doubt that organizational aspects of NPP operating bodies generally affect safety. Numerous analyses have identified more specifically what aspects of the organization are important to safety in terms of organizational performance, organizational processes and factors, and safety culture. There is also no doubt that many of these organizational influences are not explicitly captured in probabilistic safety assessments. Some of the influences are captured implicitly in PSAs, for example, through component unavailability rates derived from operating experience, and uncertainty distributions on modeled human error rates. But some of the influences are likely to be part of PSA incompleteness. It is not clear to what extent the incompleteness affects the PSA results.

The current approach internationally is to address organizational factors, usually under the umbrella of safety culture or safety management, outside the realm of operational and regulatory decision-making based directly on PSA. The implicit assumption is that safety culture is clearly a pervasive and important aspect of operations[1], but one whose effect on risk may be difficult to quantify. While there are some methods proposed in the literature to incorporate the effects of organizational factors into PSA, there is no consensus on the appropriate way to do so, and it is not yet clear whether this can be done successfully [47]; further empirical verification is needed.

There are various challenges to including the influence of organizational factors on PSA. One challenge is that organizations are not static but rather fundamentally

[1] Some authors [46] argue that operations cannot be separated from safety attitudes and one should talk about a "quality culture" rather than "safety culture."

dynamic in nature. The organization is constantly changing, e.g., there may be changes in management, organizational structure, and/or organizational processes. In addition, most organizations go through a complacency-vigilance cycle (as described in Ref. [6]), where safety vigilance is heightened after an incident but slowly relaxed as more time has elapsed since the incident until the complacency may lead to the next incident. Because of this dynamism, a PSA that adequately captures today's OFs may be inadequate to describe tomorrow's organizational influence (while hardware states are also dynamic, change is usually more gradual and/or targeted surveillance activities are designed to detect adverse changes before a safety concern emerges [48]). Another challenge is that since many organizational influences are latent, weaknesses may not be recognized for a long time. Along the same lines, signals of potential organizational weaknesses may be weak and difficult to interpret. Lastly, at this time, there is a general lack of data (or analysis to interpret existing data) to tie organizational influences systematically to PSA.

The most important outcome is achieving safety effectively and efficiently, and ultimately the strategy for where to address OFs, within and/or outside PSA, will depend on requirements and limitations yet to be determined. If it is discovered that the potential incompleteness in PSAs due to OFs is significant, e.g., it is difficult to use PSA results for risk prioritization without consideration of OFs, a concerted effort should be expended for rigorous inclusion of organizational influences in PSA. If analysts find that it is nearly impossible to capture organizational influences in PSA (because of ambiguities and uncertainties), traditional defense-in-depth strategies and extra-PSA evaluations of OFs should continue. If both of these turn out to be true, i.e., OFs exert a significant influence on PSAs and it is nearly impossible to adequately capture the influence of OFs on PSA, additional strategies should be developed to augment the use of PSA results for prioritization.

REFERENCES

[1] A. Kolaczkowski, J. Forester, E. Lois, and S. Cooper, *Good Practices for Implementing Human Reliability Analysis (HRA)*, NUREG-1792, US Nuclear Regulatory Commission (April 2005).

[2] USNRC, *An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities*, Draft Regulatory Guide 1.200/DG-1122, US Nuclear Regulatory Commission (December 2003).

[3] USNRC, *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis*, Regulatory Guide 1.174, US Nuclear Regulatory Commission (November 2002).

[4] NEA Committee on the Safety of Nuclear Installations, *Critical Operator Actions: Human Reliability Modeling and Data Issues*, NEA/CSNI/R(98)1, Organization for Economic Cooperation and Development (1998).

[5] O. Sträter, Guest Editor, Special issue on "Human Reliability Analysis: Data Issues and Errors of Commission," *Reliability Engineering and System Safety*, **83**, 127 (2004).

[6] J. Reason, *Managing the Risks of Organizational Accidents*, Ashgate, Brookfield, USA (1997).

[7] D. I. Gertman, B. P. Hallbert, D. Prawdzik, and H. S. Blackman, "Human Performance Characterization in the Reactor Oversight Process," *Proceedings of the 6th International Conference on Probabilistic Safety Assessment and Management (PSAM 6)*, San Juan, PR (2002).

[8] USNRC, *Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis* (ATHEANA), NUREG-1624, US Nuclear Regulatory Commission (May 2000).

[9] NEA Committee of the Safety of Nuclear Installations, *Identification and Assessment of Organisational Factors Related to the Safety to NPPs*, NEA/CSNI/R(98)17/VOL1, Organization for Economic Cooperation and Development (February 1999).

[10] NEA Committee of the Safety of Nuclear Installations, *CSNI Technical Opinion Paper No. 3: Recurring Events*, NEA No. 4388, Organization for Economic Cooperation and Development (2003).

[11] USNRC, *Davis Besse Reactor Vessel Head Degradation Lessons-Learned Task Force Report*, US Nuclear Regulatory Commission (September 2002).

[12] USNRC, NRC *Update on Davis-Besse Reactor Vessel Head Damage*, US Nuclear Regulatory Commission (October 2002).

[13] FirstEnergy Nuclear Operating Company(FENOC)/DBNPS, *Root Cause Analysis Report: Significant Degradation of the Reactor Pressure Vessel Head*, CR 2002-0891, (April 2002).

[14] FENOC, *Root Cause Analysis Report: Failure to Identify Significant Degradation of the Reactor Pressure Vessel Head* (August 2002).

[15] Hungarian Atomic Energy Authority, *Report to the Chairman of the Hungarian Atomic Energy Commission on the Authority's investigation of the incident at Paks Nuclear Power Plant on 10 April 2003*, Event ID: 1120 (2003).

[16] International Atomic Energy Agency (IAEA), *Report of the Expert Mission To Assess the Results of the Hungarian Energy Authorities Investigation of the 10 April 2003 Fuel Cleaning Incident at Paks NPP* (2003).

[17] D. I. Gertman, B. P. Hallbert, M. W. Parrish, M. B. Sattison, D. Brownson, J. P. Tortorelli *Review of Findings for Human Performance Contribution to Risk in Operating Events*, NUREG/CR-6753, US Nuclear Regulatory Commission (March 2002).

[18] R. Weil and G. Apostolakis, "Identification of Important Organizational Factors Using Operating Experience," in: B. Wilpert and N. Itoigawa (Eds.), *Safety Culture in Nuclear Power Operations*, Taylor & Francis, New York (2001).

[19] ACRS, Letter from D. A. Powers, Chairman, ACRS, to R. A. Meserve, Chairman, US Nuclear Regulatory Commission, "Subject: SECY-00-0053, NRC Program on Human Performance in Nuclear Power Plant Safety," May 23 (2000).

[20] ACRS, Letter from D. A. Powers, Chairman, ACRS, to