INTERNATIONAL NUCLEAR SAFETY JOURNAL
vol.3 issue 3, 2014, pp.1-7

ISSN 2285 – 8717
ISSN–L 2248 – 8717
http://www.insj.info

NUCLEAR SAFETY CULTURE ATTRIBUTES AND LESSONS TO BE LEARNED FROM PAST ACCIDENTS

Madalina Tronea, Cantemir Ciurea
National Commission for Nuclear Activities, Bucharest, Romania
Corresponding author: madalina.tronea@cncan.ro

Received: *9 September 2014*; accepted: *29 September 2014*

Abstract
The paper presents an overview of the lessons to be learned from past nuclear reactor accidents and their relevance for the development of nuclear safety culture. Although the term "safety culture" emerged after the Chernobyl accident, the factors that contributed to earlier accidents, of which the most notable was the accident of Three Mile Island Unit 2, are also relevant for nuclear safety culture. As regards the Fukushima Daiichi accident from 2011, safety culture was once again brought into discussion. In this paper we will analyze the lessons learned from past nuclear accidents by making use of the 37 attributes of a strong safety culture, promoted by the IAEA.

Keywords
nuclear safety culture, operational experience feedback, reactor accidents

1. Introduction

The concept of "nuclear safety culture" was first introduced after the Chernobyl accident [1] and was given particular emphasis each time a significant event occurred, including after the accident at Fukushima Daiichi. In hindsight, all accidents are judged to have been preventable. The fact that nuclear safety culture is given increased attention after accidents happen shows a reactive approach.

Safety culture is part of the defence-in-depth strategy and plays a major role in preventing nuclear accidents. *Defence-in-depth also includes thoughtful compliance with existing regulatory requirements and the internal imposition of additional requirements when regulations are insufficient for safety.*

This is something that we need internalize in order to have a proactive approach in giving first priority to nuclear safety over competing demands of other nature.

The definition of safety culture used in this paper is that proposed by the International Atomic Energy Agency (IAEA): "the assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, protection and safety issues receive the attention warranted by their significance" [2].

Strictly as a matter of logic and language safety culture is that part of culture that involves safety. Culture includes mental content, norms, institutions, and physical objects (artefacts).

In this paper we try to analyze the main factors that contributed to the accidents at Three Mile Island Unit 2 (TMI-2), Chernobyl Unit 4 and at Fukushima Daiichi from the perspective of the safety culture attributes promoted by the International Atomic Energy Agency (IAEA) [3]. There are 37 attributes, grouped into 5 areas corresponding to safety culture characteristics:

A. Safety is a clearly recognised value;
B. Leadership for safety is clear;
C. Accountability for safety is clear;
D. Safety is integrated into all activities;
E. Safety is learning driven.

Although not explicitly called out by IAEA, the following four traits suggest themselves time and time again in the reflection upon nuclear power accidents:

A. Competence (People being able to do what they have to do);

B. *Compliance (Knowing the rules and doing what they require);*
C. *Integrity (Honesty and the intolerance of falsehood, deceptions, and misrepresentation);*
D. *Transparency (Doing activities in such a way that the essentials are clearly visible.)*

2. Causes that contributed to the TMI-2 accident

The TMI-2 reactor suffered a partial melt down on March 28, 1979. The accident began at about 4.a.m., when the plant experienced a loss-of-feedwater transient, leading to turbine trip and reactor shutdown. *This transient was a result of operator actions that introduced water into the instrument air system while conducting risky evolutions with inadequate supervision, training, and instructions.*

The pressure in the reactor primary coolant system started to increase and the pilot-operated relief valve (PORV) located at the top of the pressurizer opened to relieve pressure. The valve should have closed when the pressure fell to proper levels, but it became stuck open. Instruments in the control room, however, indicated to the plant staff that the valve was closed. As a result, the plant staff was unaware that cooling water was pouring out of the stuck-open valve. Plant staff assumed that as long as the pressurizer water level was high, the core was properly covered with water. *They had ineffective training and instructions as to actions to be taken in case of high pressurizer level indication. Also they had inaccurate cognitive models of reactor coolant system hydraulics due to inadequate training.*

There was no instrument that showed how much water covered the core and the operators did not realize that the plant was experiencing a loss-of-coolant accident. *This instrumentation compensates for inadequate operator knowledge of how pressurized water reactors work.*

The operators took a series of actions that made conditions worse, such as significantly reducing the flow of emergency cooling water that was being pumped into the primary system following the automatic actuation of the emergency cooling system. This lead to a partial core melt.

Due to the fact that the containment system functioned as design, the radiological consequences outside the plant were minimal. *The containment effectiveness was however degraded by pumping radioactive water to the auxiliary building.*

The operational experience shows that in September 1977 a similar incident occurred at the similar reactor of the Davis-Besse plant, with similar response from operators, but which had no consequences because the reactor was a low power. The incident was investigated by the reactor vendor and plant engineers and by the regulatory authority but no measures have been taken (i.e. no official request for corrective actions), although the generic nature of the problem, as well as its potential consequences have been recognised by several individuals [4, 5]. Various problems with plant equipment and control room design had been reported since the start of the operation of the plant, but they were not corrected. All these have been given due attention only as part of the accident investigations.

The overall conclusion of the Kemeny report [4] was that: "To prevent nuclear accidents as serious as Three Mile Island, fundamental changes will be necessary in the organization, procedures, and practices -- and above all -- in the attitudes of the Nuclear Regulatory Commission and, to the extent that the institutions we investigated are typical, of the nuclear industry." It also noted that "as the evidence accumulated, it became clear that the fundamental problems are people-related problems and not equipment problems" and that "The most serious "mindset" is the preoccupation of everyone with the safety of equipment, resulting in the down-playing of the importance of the human element in nuclear power generation".

The accident causes listed in the Kemeny report include:
- deficiencies in the training of the operators;
- deficiencies in the operating procedures;
- lessons from previous incidents not used to improve training and procedures;
- inadequate use of operating experience;
- lack of attention to the human factors in the design of the control room;
- utility management permitted operation of the plant with a number of poor control room practices.

Other findings of relevance include:

- the licensee did not have sufficient knowledge, expertise, and personnel to operate the plant or maintain it adequately;
- deficiencies in maintenance;
- training of operators and supervisors did not give sufficient emphasis to a fundamental understanding of the reactor;
- reports of operating experience at other plants were screened by technical analysts who did not have nuclear backgrounds;
- there was no group with special responsibility for receiving and acting upon potential safety concerns raised by employees;
- deficiencies in maintaining "as built" drawings and in the purchasing of "safety-related" equipment without quality controls;
- there were not enough utility inspectors to perform the quality assurance inspections;
- independent assessment of general plant operations was minimal.

Each of the above deficiencies were clear departures from the then existing NRC (Nuclear Regulatory Commission) requirements. TMI-2, like all other costly nuclear mishaps can be equally viewed as compliance shortfalls.

The Rogovin report [5] identified similar problems and issued similar conclusions: "The one theme that runs through the conclusions we have reached is that the principal deficiencies in commercial reactor safety today are not hardware problems, they are management problems. We have found, based upon our study of TMI and our interviews with knowledgeable people in the industry, that many nuclear plants are probably operated by management that has failed to make certain that enough properly trained operators and qualified engineers are available on site in responsible positions to diagnose and cope with a potentially serious accident. The NRC, for its part, has virtually ignored the critical areas of operator training, human factors engineering, utility management, and technical qualifications".

The Rogovin report also emphasized the fact that operating experience was available but not used, either because it was not accessible to the licensee, or because of bureaucracy and lack of clear requirements on the use of operational experience feedback. As stated in the Rogovin report, "The accident at Three Mile Island on March 28, 1979, had almost happened before - twice. Virtually identical "transients," as they are called in the industry, occurred in 1974 at a Westinghouse reactor in Beznau, Switzerland, and in 1977 at Toledo Edison's Davis Besse plant in Ohio, a Babcock & Wilcox reactor similar in design to the one at Three Mile Island. Both involved the same failed-open pressurizer relief valve (PORV), and the same misleading indications to operators that the reactor coolant system was full of water. In both cases, operators diagnosed and solved the problem in a matter of minutes before serious damage could be done." [5].

Similar to the "mindset" mentioned in the Kemeny report, the Rogovin report highlights "complacency": "On top of all this, we found that before March 28, 1979, an attitude of complacency pervaded both the industry and the NRC, an attitude that the engineered design safeguards built into today's plants were more than adequate, that an accident like that at Three Mile Island would not occur-in the peculiar jargon of the industry, that such an accident was not a "credible event"[5]. *Ironically this would have been true in the case of TMI-2 but for the dysfunctional unnecessary action of the operators. Such behaviour was considered doubly incredible.*

The "mindset" and complacency and refusal to consider an accident as credible were also factor in the Chernobyl and Fukushima accidents. *This mindset was noticed also in the case of the Davis-Besse 2002 near miss, where a LOCA (Loss of Coolant Accident) through the reactor vessel head failure had been excluded from the PRA (Probabilistic Risk Assessment).*

3. Causes that contributed to the Chernobyl-4 accident

The accident at Chernobyl Unit 4 happened on April 26, 1986. The reactor crew was performing a test to determine how long turbines would spin and supply power to the main circulating pumps following a loss of main electrical power supply. A series of operator decisions and actions brought the reactor in an unstable condition. An attempt to emergency shutdown the reactor from this state leads to a

power excursion, due to a peculiarity of the design of the control rods. A steam explosion followed, destroying the reactor.

The peculiarity of the design of the control rods and its effect had been known before the accident, but no measures have been taken to correct it. "The existence of the positive scram effect was first acknowledged by Soviet experts at the Conference on Nuclear Power Performance and Safety in Vienna in 1987. The SCSSINP Commission report states that this phenomenon had been known of at the time of the accident and that it had first been identified at the Ignalina RBMK plant in the Lithuanian Republic in 1983. Although the Chief Design Engineer for RBMK reactors promulgated this information to other RBMK plants, and stated that design changes would be made to correct the problem, he made no such changes, and the procedural measures he recommended for inclusion in plant operating instructions were not adopted. Apparently, there was a widespread view that the conditions under which the positive scram effect would be important would never occur. However, they did appear in almost every detail in the course of the actions leading to the accident" [6]. "INSAG notes the observations made at the Ignalina plant in 1983, when the possibility of positive reactivity insertion on shutdown became evident, and the event at the Leningrad nuclear power plant in 1975 which, in retrospect, indicated that events excited by local reactivity feedback could cause damage to the reactor. These two events pointed to the existence of design problems. Although the events had the semblance of potential precursors to an accident, apparently no thorough analysis was performed. It is a matter of great concern that this important information was not adequately reviewed and, where it was disseminated to designers, operators and regulators, its significance was not fully understood and it was essentially ignored" [6].

Such failures to analyse nuclear power mishaps effectively persists to this day. The authors could find no publicly available examples of competent thorough root cause analyses of nuclear power mishaps.

Moreover, the INSAG-7 publication [6] reveals, based on the report by the SCSSINP Commission (USSR State Committee for the Supervision of Safety in Industry and Nuclear Power), that regulations that had come into force more than 10 years before the accident have not been enforced at Chernobyl NPP. *Failure to comply with existing requirements continues to be an unidentified harmful factor of most, if not all, nuclear power mishaps.*

The INSAG publication also mentions the operator's lax attitudes towards nuclear safety: e.g. "disabling of reactor protection seems to have been regarded rather lightly both in the operating procedures and by the operators", "when the reactor power could not be restored to the intended level of 700 MW(th), the operating staff did not stop and think, but on the spot they modified the test conditions to match their view at that moment of the prevailing conditions. The INSAG report emphasizes both the fact that the reactor was operated in unstable and unanalyzed conditions and the fact that the reactor's safety analysis report did not identify the violations of the regulations and the design deficiencies (this information is based on the SCSSINP Commission report that is annexed to the INSAG report). *This sounds ominously similar to the operator performance at TMI-2.*

The INSAG report concludes that "the accident can be said to have flowed from deficient safety culture, not only at the Chernobyl plant, but throughout the Soviet design, operating and regulatory organizations for nuclear power that existed at the time" [6]. It lists the following broad contributors to the accident:

- "a plant which fell well short of the safety standards in effect when it was designed, and even incorporated unsafe features;
- inadequate safety analysis;
- insufficient attention to independent safety review;
- operating procedures not founded satisfactorily in safety analysis;
- inadequate and ineffective exchange of important safety information both between operators and between operators and designers;
- inadequate understanding by operators of the safety aspects of their plant;
- insufficient respect on the part of the operators for the formal requirements of operational and test procedures;
- an insufficiently effective regulatory regime that was unable to counter pressures for production;

- a general lack of safety culture in nuclear matters, at the national level as well as locally" [6].

4. Causes that contributed to the Fukushima Daiichi accident

The manifestation of the Fukushima Daiichi accident started on March 11, 2011, when, following a major earthquake, a 15-metre tsunami, significantly exceeding the design basis for the plant, disabled the power supply to the Fukushima Daiichi Units 1-4. *The actual event started decades before and eluded copious opportunities to have prevented it.*

A total loss of power supply event is known as station blackout. Without power supply, cooling was lost and this lead to reactor core melts in Units 1 - 3. Hydrogen explosions occurred in Units 1, 3 and 4. Unit 4 had not been operating, but was affected by a hydrogen explosion due to gas back-flow from unit 3.

The National Diet of Japan independent investigation commission (NAIIC) report concluded that "The TEPCO Fukushima Nuclear Power Plant accident was the result of collusion between the government, the regulators and TEPCO, and the lack of governance by said parties. They effectively betrayed the nation's right to be safe from nuclear accidents. Therefore, we conclude that the accident was clearly "manmade." We believe that the root causes were the organizational and regulatory systems that supported faulty rationales for decisions and actions, rather than issues relating to the competency of any specific individual" [7].

It is interesting that the NAIIC did not ask about the harmful factors that resulted in those "root causes." Nor did NAIIC ask about any other harmful factors that could equally well be called root causes, such as the ineffective relationships between TEPCO, Japanese regulatory authorities, and international nuclear organisations.

This NAIIC conclusion is due to the fact that the accident could have been prevented or its consequences significantly reduced if proper risk assessment was performed and if design upgrades and severe accident management measures would have been implemented. The investigation revealed that the regulatory authorities and TEPCO had been sharing information on the possibility of the station blackout scenario and on its potential consequences starting with 2006. They also shared an awareness of the risk of potential reactor core damage from a breakdown of seawater pumps if the magnitude of a tsunami striking the plant turned out to be greater than the assessment made by the Japan Society of Civil Engineers and used in the design features protecting the site. However no corrective actions were taken. As explained in the NAIIC report, "The reason why TEPCO overlooked the significant risk of a tsunami lies within its risk management mindset - in which the interpretation of issues was often stretched to suit its own agenda. In a sound risk management structure, the management considers and implements countermeasures for risk events that have an undeniable probability, even if details have yet to be scientifically confirmed. Rather than considering the known facts and quickly implementing counter measures, TEPCO resorted to delaying tactics, such as presenting alternative scientific studies and lobbying." [7]

These tactics are not unique to Japan. They could be observed also in how the licensee of Davis-Besse handled the reactor vessel head nozzle cracking issue before the 2002 near miss.

The investigation also revealed that the severe accident management measures in place at Fukushima Daiichi were practically ineffective. These measures addressed only severe accidents initiated by internal events and disregarded the possibility that a severe accident is initiated by an external event such as an earthquake or a tsunami, even if such events were frequent in Japan. The NAIIC report concluded "that there were organizational problems within TEPCO. Had there been a higher level of knowledge, training, and equipment inspection related to severe accidents, and had there been specific instructions given to the on-site workers concerning the state of emergency within the necessary time frame, a more effective accident response would have been possible" [7].

A comprehensive description of the causes of the Fukushima Daiichi accident and of the lessons learned in provided in the reports issued by the Institute of Nuclear Power Operations (INPO) [8, 9]. One of the most significant operational lessons from the Fukushima Daiichi

accident is that "When periodic reviews or new information indicates the potential for conditions that could significantly reduce safety margins or exceed current design assumptions, a timely, formal, and comprehensive assessment of the potential for substantial consequences should be conducted" [9]. *However, INPO did not indicate the need to identify the early better cheaper more risk-informed, more compliant opportunities, to pre-identify such conditions. Thus the nuclear community may miss the opportunity to see its own blind spots.*

TEPCO's own analysis of the root causes of the Fukushima Daiichi accident [10] revealed the following:

- lack of safety awareness and failure to ensure defence-in-depth against unexpected natural events;
- a large tsunami exceeding the design basis was seen as not credible in spite of little knowledge regarding such tsunamis;
- lack of flexibility in thinking in taking feasible cost-effective measures within a short period of time;
- past scandals in the nuclear sector have not been viewed as a sign of deteriorating safety culture;
- preparations to respond to simultaneous occurrence of severe accidents at multiple units were insufficient;
- inability to analyze the situation, to identify and estimate the status of the plant;
- training was merely formal because of the assumption that no severe accidents would occur.

Like in the case of TMI-2 and Chernobyl-4 accidents, a number of factors came into play in order to cause a severe accident, this time affecting multiple units on a site.

One of the lessons learned outlined in the INPO report is that "Behaviours prior to and during the Fukushima Daiichi event revealed the need to strengthen several aspects of nuclear safety culture. It would be beneficial for all nuclear operating organizations to examine their own practices and behaviours in light of this event and use case studies or other approaches to heighten awareness of safety culture principles and attributes" [9]. The report acknowledges that "An important nuclear safety culture principle is cultivating a questioning attitude and challenging assumptions. In retrospect, TEPCO would have benefited from additional questioning and challenging of the assumption that a large tsunami capable of flooding the plant could not occur. Additionally, questioning and challenging of assumptions may have helped maintain core cooling during the Fukushima event when communications were difficult and reliable information on plant parameters was unavailable" [9].

5. Conclusions

Studying the three most prominent nuclear power reactor accidents, we can see some recurring themes related to safety culture:

- a mindset that considers severe accidents as incredible;
- failure to make effective use of operational experience feedback;
- incomplete safety and risk assessment or failure to take into account into plant emergency operating procedures and severe accident management guidelines;
- insufficient attention provided to training;
- insufficient understanding of plant behaviour under accident conditions;
- lack of a questioning attitude in all organizations with influence on the plant operation;
- *lack of commitment to full intelligent business-like compliance with existing regulatory requirements;*
- *lack of commitment to addressing those cases in which the regulatory requirements are known to be insufficient.*

In an attempt to link these with the safety culture attributes promoted by the IAEA [3], we note that the main attributes that could be directly linked with attitudes and actions that could have prevented the major accidents addressed in this paper are the following:

- E.1. A questioning attitude prevails at all organizational levels
- E.2. Open reporting of deviations and errors is encouraged
- E.3. Internal and external assessments, including self-assessments, are used
- E.4. Organizational and operating experience (both internal and external to the facility) are used
- E.5. Learning is facilitated through the ability to recognize and diagnose deviations, to formulate and implement solu-

tions and to monitor the effects of corrective actions
- E.6. Safety performance indicators are tracked, trended, evaluated and acted upon
- E.7. There is systematic development of individual competences

The above attributes belong to the characteristics of a "learning organization", where "safety is learning driven" (characteristic E in the IAEA system of characteristics and attributes of a strong safety culture).

Based on this, it appears that indicators related to an organization's capability to learn are good candidates for use in a regulatory oversight process that aims to address safety culture. Such indicators include the use of operational experience feedback, the use of research findings, licensee's voluntary initiatives to improve safety, the rate of proactive versus reactive actions to improve safety, the use of safety performance indicators, attention devoted to training and qualification, processes for decision-making, arrangements for independent safety review and its results, quality of the self-assessments, openness to external reviews, attention to human factors, etc.

Acknowledgments

The authors would like to thank to William R. Corcoran, Ph.D. (https://www.linkedin.com/in/williamcorcoranphdpe) for the peer-review of this paper, as well as for his contributions, which have been incorporated in the text with italic type.

References

1. International Nuclear Safety Advisory Group, Summary Report on the Post-Accident Review Meeting on the Chernobyl Accident, Safety Series No. 75- INSAG-1, IAEA, Vienna, 1986
2. International Nuclear Safety Advisory Group, Safety Culture, Safety Series No. 75-INSAG-4, IAEA, Vienna, 1991, http://www-pub.iaea.org/MTCD/publications/PDF/Pub882_web.pdf
3. International Atomic Energy Agency, The Management System for Nuclear Installations, Safety Guide, IAEA Safety Standards Series No. GS-G-3.5, Vienna, 2009 (para. 2.6-2.37 and Appendix I), http://wwwpub.iaea.org/MTCD/publications/PDF/Pub1392
4. "Report of the President's Commission on the Accident at Three Mile Island - The Need for Change: The Legacy of TMI", John G. Kemeny (Chairman of the commission), 1979, http://www.threemileisland.org/downloads//188.pdf
5. "Three Mile Island; A Report to the Commissioners and to the Public," Mitchell Rogovin, George T. Frampton, NUREG/CR-1250, Vols. I-II, 1980,http://www.threemileisland.org/downloads/354.pdf
6. The Chernobyl accident: updating of INSAG-1 : INSAG-7 : a report by the International Nuclear Safety Advisory Group. — Vienna : International Atomic Energy Agency, 1992, http://www-pub.iaea.org/MTCD/publications/PDF/Pub913e_web.pdf
7. The National Diet of Japan, The Official Report of the Fukushima Nuclear Accident Independent Investigation Commission, Executive Summary, 2012,http://warp.da.ndl.go.jp/info:ndljp/pid/3856371/naiic.go.jp/wpcontent/uploads/2012/09/NAIIC_report_lo_res10.pdf
8. INPO 11-005, Special Report on the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station, Institute of Nuclear Power Operations, 2011,http://pbadupws.nrc.gov/docs/ML1134/ML11347A454.pdf
9. INPO 11-005 Addendum, Lessons Learned from the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station, Institute of Nuclear Power Operations, 2012, http://www.wano.info/Documents/Lessons%20Learned.pdf.
10. Reassessment of Fukushima Nuclear Accident and Outline of Nuclear Safety Reform Plan (Interim Report), TEPCO Nuclear Reform Special Task Force, 2012, http://www.tepco.co.jp/en/press/corp-com/release/betu12_e/images/12121e0201.pdf