Nuclear Industry Organizations: Shaped by Accidents

Anthony J. Spurgin[*a], David W. Stupples [b]
[a] City University, San Diego, California, USA
[b] City University, London, United Kingdom

Abstract: This paper introduces the concept of the VSM method being used to represent the organization of NPPs in responding to accidents. The Fukushima accident is addressed as a method for the examination of the VSM method and its utility is seeing the 'big' picture as far as the decision-making aspects of organizations are concerned. The impact of accidents upon the NPP management operations is covered and how the organization has to change following an accident is covered. The paper points out the fact that often accident situations and their responses are affected by the long term decisions of management. The decision of TEPCO to disregard advice on the possibility of a large tsunami occurring was a critical fault and preventive methods should have been considered along with the risk of not taking actions. Recommendations are made for improvements in emergency procedures during accident control and mitigation, the procedures should be flexible and based upon something like the symptom-based procedure approach and should consider beyond design-basis events.

Keywords: Accidents, Organizations, Safety, VSM

1. INTRODUCTION

This paper is concerned with the influence of accidents on the development of nuclear power organizations. It should be noticed that significant changes have occurred over time in the operation of nuclear plants, most of these changes have been initiated in response to accidents. Some of the accidents have had a stronger influence than others.

The paper not only deals with the impact of accidents on the way that nuclear power plant organizations are organized, but also covers how these organizations could be modelled based on a cybernetic model of organizations developed by Beer [1]. Most accident studies are based upon models of NPPs coupled with limited operator models, but the inclusion of management decision-making is omitted. Here plant models including automatic control and protection modules are connected to the Beer model called Viable Systems Model (VSM). During an accident the normal VSM Nuclear Power Plant Organizational model morphs into a compact VSM and this process is discussed in the context of the Daiichi TEPCO NPP accident induced by earthquake/tsunami during March 2011.

The normal focus of interest associated with accidents seems to be the operators, who are persons seen to be most closely involved with the accident and the organization's response to the accident. In fact, the situation is more complicated than that. Reviews of accidents indicate that top decision-makers in organizations have a great deal of responsibility in setting up the environment that makes the accident more likely. This is the case in the Daiichi accident.

The paper explores this topic to try to understand the limitations of nuclear organizations that cause this to happen. Several authors have advanced reasons why top management makes decisions that eventually lead to the accidents. For example, Marc Gerstein [2] has advanced the idea that managers fail to carryout a considered risk assessment. Often he suggests analyses offered up by experts may be inconclusive. He states that in management decision-making intuition often trumps knowledge. Here he was referring to a particular situation; the case of the NASA Columbia accident due to the impingement of iced foam on the carbon leading edge of the wing. It was the lack of action by management to try to resolve what might have happened and what could they do to recover the astronauts.

Having an integrated view of organization in controlling the plant should help in avoiding accidents. Management should be in a position to understand how accidents affect the plant and be proactive in preventing accidents rather than waiting for accidents to occur before taking steps, particularly in the case of

severe accidents? One would have thought that the consequences would have been powerful enough to cause organizations to take steps to reduce risks. Well, maybe the answer is that organizations cannot achieve the goal of improving plant safety independently of accidents. Why is it that the industry is still surprised when a new accident occurs?

If one looks at the industry as a whole, we have regulators deeply involved looking at every misstep, we have Institute of Nuclear Plant Operations (INPO) and World Association of Nuclear Operators (WANO) helping utilities to improve their operations and then we have US National Laboratories and Universities deep into theories and ideas, yet accidents pop up and change the way we think about the situation.

One could just wave ones hands and say this is the fate of mankind to dream the impossible dream, and nature will point out our limitations. It has been pointed out, that the people involved in trying to solve these problems themselves seem to have a common mode of thinking; hence the solution depends on thinking differently. If one steps back, one sees that progress in life in all fields is dominated by this kind of effect, the inability to see all interacting issues to understand the weakness of a specific approach, or some part of it. Sometimes, the way that society works precludes the ability of individuals to see clearly what are the issues controlling risk. Then they focus on the wrong items/people. In the story about the King's new clothes, it was a child that saw the truth. So what do we have to do? Become aware of our limitations and cast the issues in a new light
The size limitations of paper does not allow for full explanation about the development of VSM and descriptions of accidents.

2. VSM AND A CYBENETIC VIEW OF ORGANIZATIONS

The purpose of this section is to present information on the use of Viable Systems Model (VSM) developed by Beer [1] and its application to management organizations running high reliability organizations (HRO).
Beer based his VSM model on the science of cybernetics. Cybernetics is the study of the structure of regulatory or control systems, which are seen in animals as well as in business systems. Cybernetics is closely related to control system theory. An introduction to the underlying techniques of cybernetics is given in Ashby [3]. Cybernetics is considered to be equally applicable to organization and control of physical as well as social management systems. VSM is a method to underpin understanding of management dynamics in organizations based upon cybernetics.

VSM was proposed as a better way of understanding and diagnosing organizational behaviour. The approach has been applied to manufacturing, food distribution, Walker, [4], software development by Herring and Kaplan [5], etc. VSM was applied by Beer to government operations in Chile under President Allende, circa 1970-73. A closer application of VSM closer to Nuclear Power was one which applied it to air traffic management (ATM) in Saudi Arabia [6]. The main thrust of this paper is the application VSM to the consideration of safety of nuclear power plants.

In practice a detailed form of VSM is used to illustrate some managerial and supervisory aspects of organizations. Figure 1 shows such a version of VSM that will be used in relation to utility management and associated personnel when considering the impact of accidents on management. It is useful, rather than getting caught up in the minutia of organization charts to select a compact model in order to show the dynamic relationships between the core working levels of an organization.

One can see here that the management function is represented by S5, S4 and S3, the communications are represented by S2 and S3* and operations by the S1 groups (both supervisors and operators). The environment is made up of local and global effects. The environment covers public and the regulators. S3, S4 and S5 represent the top management functions of top management (CEO and President), planning (Safety & Risk assessment-CNO), economics (CFO) and plant management (Station Manager, VP). The S3* and S2 functions represent co-ordination and auditing functions.

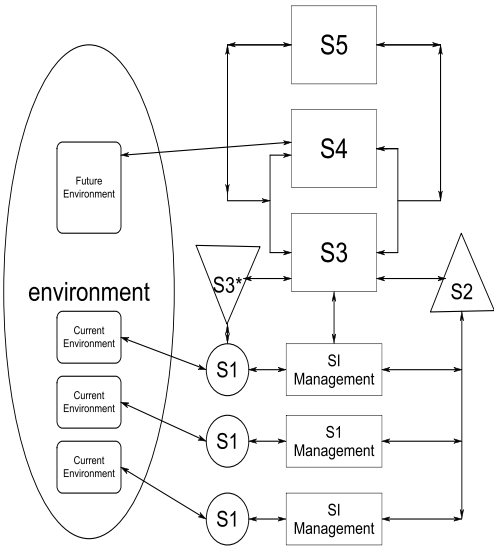

Figure 1. Complex Version of VSM

The VSM model of a utility organization is shown as a system to control and monitor a power plant. The organization acts like a layered control system with some controllers acting directly on the process and others controlling the set points of local controllers.

Here decisions are made at different levels within the organization; to meet the long term objectives of the company are covered by the top management, planning and risk assessments at the CNO level and at the plant management level decisions are made relative to the day to day running of the plant. The plant operators and supervisors are the persons committed to actually running the plant equipment.

Feedback is provided to the various elements by plant data, information from audits and from operators. It is this feedback that stabilizes the plant operations much the same as in a regular control scheme. Also there are internal feedback signals from the managerial levels that also ensure that top level decisions are exposed to critical review and comment.

It not always clear to top management, that the functional stability and responsiveness of an organization is dependent on all of these feedback signals. In fact, many may not even be recognized. Accidents can be examined to show how deficiencies within organizations can lead to accidents and even to the demise of organizations, for example see the failure of Northeast Utilities recorded in MacAvoy and Rosenthal [7].

3. **ACCIDENT ISSUES**

Accident case studies can be used to shed light on how organizations operate and what are the rules required to ensure that the whole organization works safely and economically. In studying the forces at play in an accident, one may come to the conclusion that in some cases it is the interactions of a small group of persons (supervisors and operators) and in other cases it is the decisions the top managers that leads to an accident.

The VSM approach is used here to capture these various interactions, in order to understand both the causes of the accident and its propagation. Nuclear accident analysis is key part of this paper in that lessons can be learned from these and other accidents, but there is no space for many analyses here. The focus will be on the Fukushima Accident, March, 2011. The Fukushima accident is likely to have a large effect on both the Japanese Government and Utilities, and also send strong messages to other countries. The Tsunami caused devastation of the area around and north of where the NPPs were located. Thousands were killed and their property destroyed, roads swept away and rail transport ceased along with a loss of communications. In the surrounding areas, people were killed and injured, houses were damaged, transportation affected, cars washed out to sea, etc. It is believed that in somewhere in excess of 20,000 people died and more than 110,000 houses were destroyed principally by the action of the tsunamis. Loss of life due to the nuclear plant accidents was very small, but there was a high economic loss and a long clean-up process because of the radioactivity releases.

The Fukushima accident took place in Japan on March 11th, 2011 and affected a number of nuclear plants operated by the Tokyo Electric Power Company. The plants were the six units of the Daiichi station and Daini station and are about 160 miles north of Tokyo on the north-east coast. The four of the six plants that made up the Daiichi were the ones principally affected. The accident was caused by large earthquakes and later followed by enormous tsunamis. The largest earthquake and the some of the tsunamis exceeded the design bases for the nuclear power plants (NPPs).

A large seismic event (Richter Scale 9.0) occurred on March 2011 off the north-east coast of Japan followed by a series of tsunamis (7) and caused massive amount of damage including affecting electric power distribution and led to the automatic shutdown of the Fukushima NPPs (Daiichi and Daini). This was a correct response. The standby diesels started up and the plants were operating safely. Of the six NPPs of Daiichi only units #1, #2 and #3 were operating the other three NPPs were shutdown.

The INPO report [8] is a very detailed analysis/accounting of the accident, but does not address questions related to why certain actions were or were not taken. Of interest is that it states that several after-shocks of lower magnitude occurred before the waves of tsunamis arrived at the coast. One of the waves was approximately 46 to 49 feet (14 to 15 meters) based on water level indications on the buildings. The design basis tsunami was 18.7feet (5.7meters), so the largest tsunami was well above this design basis, and this was the base cause of the extensive damage to plants and also to the surrounding area.

The earthquake and Tsunami magnitudes exceeded the design bases for the NPPs. It has been reported that seismic experts had informed TEPCO that higher tsunami should have been selected [9]. Sea water flooding caused by the tsunami caused the standby power diesels to fail, the diesel fuel tanks to be blown away, battery rooms, and turbine halls to be flooded. There were some diesels were air started, but could not be used since rest of the electrical systems had failed. The inlet cooling system structures became blocked with the debris caused by the tsunamis and led to cooling water pump failures.

The loss of diesels and battery supplies led to the plant being in a "Blackout" condition. Initially, the diesels started and then stopped due to flooding at the diesel locations. Initially the reactors shut down (control rods inserted into the reactor core), the auxiliary electric supplies via the diesels came on and decay heat removal was taken care of. There may have been some damage from the earthquake, but it did not lead to extensive damage at the plant.

However, within an hour of the earthquake the tsunami struck and from then onwards, the safety systems failed, the batteries failed to supply instrument power to allow valves to be operated. Under these conditions, it was nearly impossible to prevent core damage and loss of cooling to the spent fuel pools. The crews' only action was to try to reduce the pressure in the reactors to a point where they could use fire pumps to inject water (initially fresh water then sea water) into the core. Even trained operators, with a well developed emergency plan, would have a great difficulty in knowing what to do and they had very little time to act before the cores would be damaged, leading to possible radiation releases and hydrogen explosions.

The site superintendent was involved in the stabilization process, but it appears that the emergency procedures that they were practiced in were not designed to deal with such difficulties. Confusion abounded in the plant, around the plant and resources to help the personnel were not readily available.

Early reports were classical in that they focused on the accident sequence. Giving information about what was going on, such as hydrogen explosions occurring, and radiation releases, etc, but very rarely does one get a glimpse of what was happening as far as instructions to operators from plant management, TEPCO upper management, and the Japan Government, etc. Of course instructions might have had little effect initially, in that the plant was already in a state where the operators could not determine what actions to take, since there was no electric power and battery power to instruments and controls also quickly disappeared. Truly, not only was the plant in a 'black out', but so were the operational staff.

TEPCO's top management seemed to be out of touch during the early stages of the accident. It is presumed that advice and help was slow in arriving. The Japanese government was deeply involved in trying to establish control over the affected surrounding regions. It was a catastrophic event for the people of Japan.

It is little wonder that even the issue of a reactor disaster was not immediately given enough attention and resources to terminate the accident and mitigate the effects of core damage. In some ways, the site personnel did very well to stay and try to address problems. Is not clear whether NPP staff and managers recognized the possibility that given the failure of fuel cooling, that the water covering the fuel would boil away and the fuel cladding would heat up and react with the steam and form hydrogen. Photos of the reactor buildings indicate that hydrogen explosions had taken place. Later, ground personnel were seen pumping water in the direction of the spent fuel pools, which are high up in the remains of the reactor building.

The general impression is that local NPP personnel were overwhelmed by events but were trying their best to cope with the situation. TEPCO headquarters' personnel could not help to improve the situation. Subsequently, radioactivity spread throughout the area. Some of it was airborne and some leaked from the reactor building and spent fuel pools. The full story is not yet available as to where all of the sources were located. It is believed that some parts of the reactor vessel and its containment system were impacted by the earthquake and a leakage path to the sea could have come from here as well as other locations. It will be some time before a complete account of the accident sequence and the sources of radioactive releases are agreed.

The INPO report [7] covers some of the difficulties that the site personnel had in trying to tackle the consequence of the accident. Some of the difficulties are; locations were dark, radiation was high is some places, equipment was not working, earthquake aftershocks caused vibrations and the threat of explosions existed. Roads made impassable with debris and even oil tanks were moved by the force of the tsunami, the station staff tried very hard against odds to cool the reactors. The loss of power affected not only pumps and valves, but lighting and availability of instrumentation, for example the staff did not know the water level in the reactors. The crews scrambled to recover and used car batteries to connect instruments to determine reactor water level. As a side issue, it is considered that this information was erroneous due to voiding in the reference legs of the level instruments.

The site personnel were faced with a situation in which nothing worked, the question was what pieces of equipment could be placed into some degree of working condition and what did one have to take to accomplish this? This is carrying out an emergence planning and response on the fly.

4. ORGANIZATIONS

The representation of an organization by VSM has been explained. The VSM models the decision and control functions of a NPP organization along with the maintenance, test and calibration actions taken by the station personnel. There are of course other functions carried out by station personnel, but here the focus is on plant operational aspects.

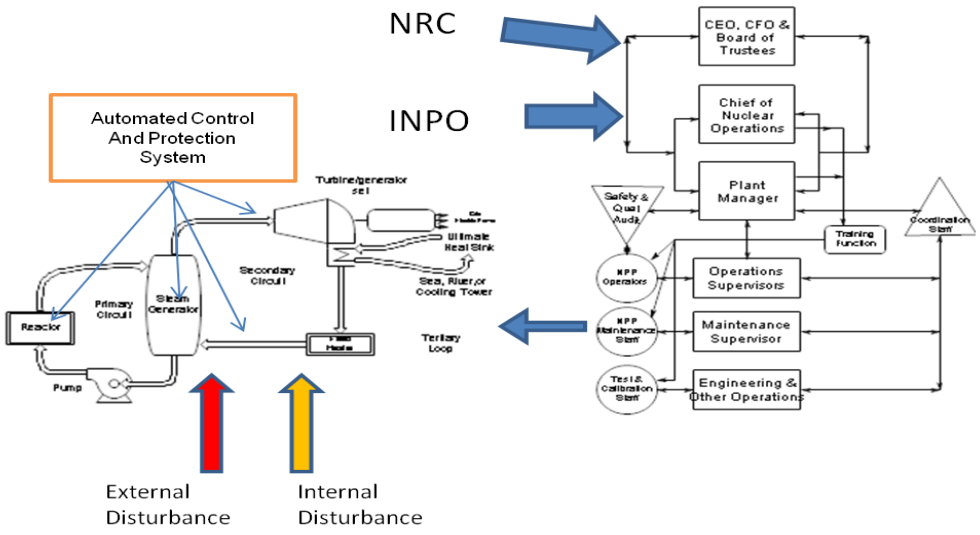

Figure 2 Integrated Depiction of Plant, Management and other Influences

Over the years, accidents have had an impact on the structure and the function of the separate entities within an organization. Some accidents have had a greater impact than others. For example, the whole concept of role of the operators, their training and displays for operators was changed by the Three Mile Island (TMI) accident. It is expected that the Fukushima accident will have a similar effect. VSM NPP model integrated with the plant, the plant controls and protection systems along with internal and external accident initiators yields a useful dynamic model of most of the interactions. This integrated model gives one a better tool to examine the role of management decision-making as it related to accident causality, termination and mitigation. Figure 2 depicts such an integrated plant/VSM model, INPO, NRC and disturbances.

Following accidents, lessons are learned and implemented by the actions of utility industry. In the case of TMI, the short comings of the industry were revealed in the Kemeny report [10], and the NRC followed this with an action plan to incorporate suggestions on how to improve the industries' performance. The Industry also acted to fill a void in the relative responsibilities of individual utilities to the industry by the forming the Institute for Nuclear Power Operations (INPO). These changes and the role of the NRC can be incorporated into a modified version VSM, whereby feedback and feed forward signals representing these two bodies. Figure 3 indicates the process of accidents influencing the organizational changes as represented by VSM.

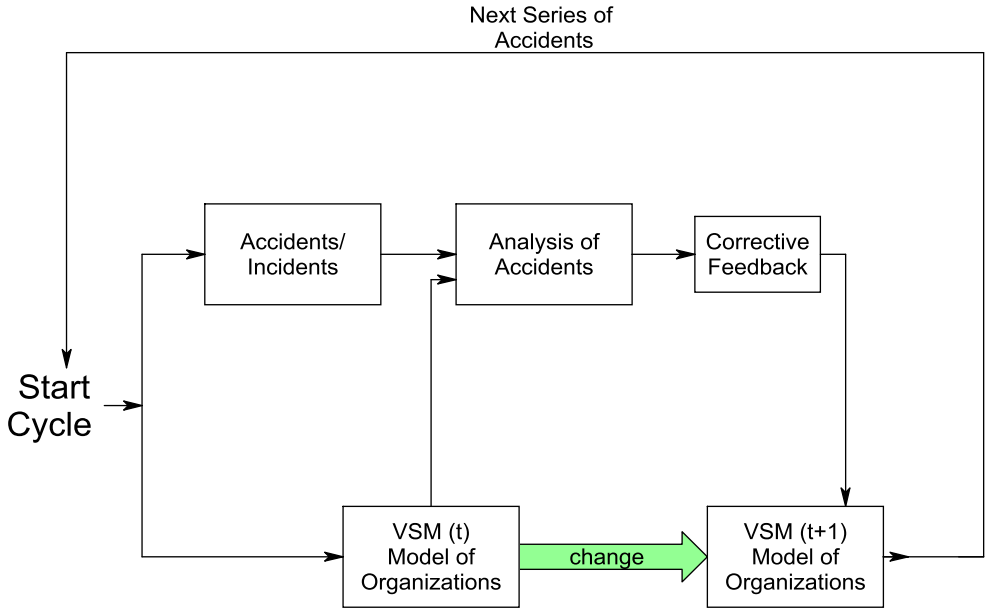

Figure 3: Depiction of the Improvement Pathway

It is expected that Fukushima will lead to further changes in the industry. One can see among the changes, the introduction of a FEMA like function to assist in bringing resources to help combat the effects of widespread dislocations in transportation and help with getting extra staff, electrical materials (cables, batteries, generators, etc), and defining the morphing process to reduce full staff to the emergency response team.
An examination of the integrated systems figure shows the influence of various decision-making entities within the organization. The top management's effects are long term, whereas those of the operators are more or less instantaneous.

Another change that was observable was the change from a loose large TEPCO organization at the start of the Fukushima accident into a tight plant directed organization. This seemed to evolve under the direction of the site supervisor. The basic structure remained a VSM type of organization with control and decision-making by the site supervisor with operators taking actions. This model morphed from the large integrated VSM model in figure 2 into the tight VSM model depicted in figure 4. Although the TEPCO management and even the Prime Minister were involved the main burden was with the site personnel. They had to evolve procedures and processes as they went along in the accident.

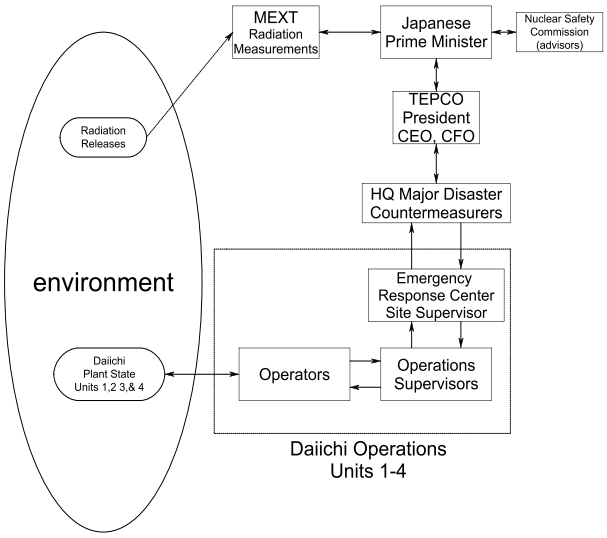

Figure 4. Emergency Daiichi Organization

Clearly, there is a need to do two things: develop a well based emergency procedure for dealing with known severe accidents plus a generalised procedure for dealing with unknown accidents, maybe complex accidents, somewhat along the lines of the symptom-based procedures. The requirement is to be prepared for all eventualities, loss of power, breakdown in communications, loss of transportation, fires, radiation, and the loss of experienced personnel and blockages of access to controls. These were some of the set of circumstances that occurred during the Daiichi accident. Also, carrying out preparatory work of this kind could determine what resources are needed that could be coordinated with other organizations and what training is needed by station staff.

If one looks at the roles of the utility management, NRC and INPO, we see that they cover a number of different, overlapping functions. The NRC is there to regulate the industry, learn from other accidents and near accidents affecting the general state of the industry; INPO has access to similar data, but also has closer contacts with the utility and does look operator training. It also performs reviews if invited to do so by the utility and also advises utility on operator training. The utility is focused on running NPPs efficiently and operating within NRC parameters for safety with the major decisions made by the CEO. A key role within the utility is the Chief Nuclear Officer (CNO). The CNO's function is to be concerned with the safety aspects of operating NPPs.

In the VSM model, there is a function, within the management that looks at planning and considering how the organization should change in order to be prepared for environmental changes. Beer was thinking about market changes that the organization has to respond to. In the utility this function should be carried out by the CNO, especially as far as safety is concerned. Somewhere in the utility organization the risk factors related to both external and internal induced events should be considered and actions promulgated to minimize public health and economic risks.

In the case of the Fukushima accident, it appears that the process of considering risk was not taken far enough by the top TEPCO management. In discussions about risk and making decisions the matter is often decided in words of Gerstein [2]; "***Unsubstantiated intuition had just trumped inconclusive analysis.***" So the idea that there was a high probability of a large tsunami occurring sometime soon affecting the Fukushima NPPs was decided to be ignored and therefore the seawalls were too small, and flood protection for the diesels, batteries and electrical circuits, which would have helped ensure the reactors would not destroyed, was not taken. The inference from Gerstein's comment is that the decision-makers can intuitively know what can work without any form of risk analysis. This type of decision-making crops up again and again. It is a case of 'don't confuse me with facts, my mind is made up'! Sometimes an analysis of the situation is inconclusive, this does not mean that one should just go ahead as though all is acceptable but rather one should look at the consequences of making and not making a decision and then re-examine the situation.

In the case of TEPCO's decision not to improve the tsunami defences, a careful review might have indicated the need, as a minimum, to waterproof the diesels and prevent flooding of electrical gear. Some of the diesels could have been moved to higher ground, watertight doors could have been fitted, and the procedures for the emergency crews (morphed teams) could have been thought through. Other tactics could have been examined to reduce risk given that a large tsunami could hit the units. A risk reduction-cost benefit study in this case could have been carried out to determine which changes yields the best approach to reduce the risk to a level that is acceptable to the utility and the country.

The integrated plant/VSM model pulls together the all of the actors in the representation so that the roles of all parts can be examined in terms their contribution to ensuring a good outcome given the occurrence of an external or internal event. The size of the disturbance can be varied to see where risks increase rapidly and why.

5 Conclusions and Recommendations

NPP organizations are living organisms and as such are dynamic. The paper has shown the need to understand the relationship between decisions made and actions taken. The methods used and regulation actions taken seemed to have concentrated rather on actions taken at the 'sharp end' rather than at the 'blunt end', i.e. more holding operators responsible as opposed to decision-makers.

Coupling of the VSM model with the power plant and the disturbances should bring home the fact that management decisions play a key role in the dynamic control of NPPs, even though they might not be immediately apparent. The time scale for decision-making is not the same as the operators' responses to an accident. In fact, accident progressions maybe affected by decisions made by management many years earlier, for example the management decision, made by NASA on transportation costs, led to the jointed booster design for the Shuttle. The subsequent decision by NASA to launch in cold conditions cemented the certainty of an accident.

However, the role of the decision-makers is very clear in the case of the Fukushima accident, both in not providing adequate defences and not having in place good emergency procedures accompanied by adequate tools to assist the crews stem the effects of the accident. The crews appear to have done a credible job along with the site manager of tackling an impossible job.

It seemed that for every step forward, there was one step back caused by the accident progression moving faster than the crews' actions to negate the effects of the accident. Trying to develop ways of responding under these conditions is very difficult. A well thought out and practiced emergency plan along with the required tools would have helped minimize the effects of the tsunami, but ultimately would not have saved the situation. The key decision not taken by TEPCO management was to consider the seriousness of the tsunami threat and take the appropriate actions. In designing control systems, one always explores the boundaries where instability maybe encountered and then designs the system in a way to avoid these zones.

The study of the Daiichi accident has brought home the need for management to think beyond the design basis events as far as accident emergency procedures are concerned. A more generalized approach to accident control and mitigation needs to be evolved along the lines of the symptom-based procedures. There is a need to be more concerned with unlikely accidents or complex accidents instead of being stuck with specific accidents.

References

[1] S, Beer**,** Diagnosing the System for Organizations, 6th Edition, John Wiley & Sons, Chichester. 1985

[2] Marc Gerstein, Flirting with Danger, Sterling Publishing Co., New York, 2008

[3] W. Ross Ashby, An Introduction to Cybernetics, 3rd edition,University Paperbacks, Methuen & Co, Ltd, London, 1973

[4] Jon. Walker, The Viable Systems Model: a Guide for Co-operatives and Federations, Manual, Part of a Training Package for Strategic Management in Social Economy (SMSE), ICOM, CRU, CAG and Jon Walker, England, 1991

[5] C. Herring & S. Kaplan, The Viable System Model for Software, Report, Department of Computer Science and electrical Engineering, University of Queensland, Brisbane, Australia
[6] S. H. Al-Ghamdi, Human Performance in Air Traffic Control Systems and Its Impact on Safety, A PhD dissertation, City University, London, 2010
[7] Paul W. MacAvoy and Jean W. Rosenthal, Corporate Profit and Nuclear Safety, Princeton University Press, Princeton, New Jersey, 2005
[8] INPO, Special Report on the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station, INPO 11-005, Institute of Nuclear Power Operations, Atlanta, Georgia, USA, 2011
[9] CNN, Expert: Japan Nuclear Plant Owner warned of Tsunami threat, CNN World Report, Asia, March 27th 2011
[10] J.G, Kemeny, The Report to the President on the Three Mile Accident, Published by US Government Publishing, Washington, 1979