Impact of Accidents on Organizational Aspects of Nuclear Utilities

Anthony J. Spurgin[1], David W. Stupples[2]

School of Engineering and Mathematics, City University, London, 4252 Hortensia St., San Diego, CA, USA

School of Engineering and Mathematics, City University, Northampton Square, London EC1V 0HB, UK

[1]a-jspurgin@att.net; [2]d.w.stupples@city.ac.uk

***Abstract*-This paper applies the Beer Viable Systems Model (VSM) approach to the study of nuclear accidents. It relates how organizational structures and rules are affected by accidents in the attempt to improve safety and reduce risk. The paper illustrates this process with reference to a number of accidents. The dynamic cybernetic aspect of the VSM approach to organizations yields a better understanding of the need for good decision-making to minimize risk and how organizations really operate.**

Keywords- Utilities; Organization; Safety; Risk; Accidents and VSM

I. INTRODUCTION

This paper is concerned with an examination of management aspects associated with nuclear power operations, such as safety of the public and plant personnel together with the economics of power production, used by electric power utilities. Key issues associated with nuclear power are safety and economics with the accent on safety. Modern industry is built upon the economic exploitation of various processes for the benefit of both the owners of the processes and society in general. If the processes are not run economically, eventually they will fail, so society exhorts companies to be economic.

Safety for most industries is not a dominant consideration, however in the nuclear industry it is a defining requirement, if the consequences of accidents cannot be held to a small impact on society, and then nuclear power will not be successful in the long term. Another aspect that affects the nuclear power industry is the fear that the 'genie will escape from the bottle'. One can see this effect in the case of the nuclear accidents that have occurred in the last twenty years, namely Three Mile Island, Chernobyl and just recently, Fukushima.

One thing should be said at the beginning of this study, accident reports sometimes lack the detail to be able to conclusively show in detail the impact of the actions of all the parties involved. Oft times the impact of prior decisions of management does not arise in the analysis of the accidents. In some accident reports communication protocols are not discussed, yet communications between parties are extremely important. In aircraft incidents, for example poor communications can play an important role, but in other accidents this issue is not raised.

A number of case studies have been selected from accidents/incidents that have occurred in the nuclear and other industries to examine this

These accidents have had a social impact beyond their actual direct effects, although both Chernobyl and Fukushima did lead to a number of deaths and release of radioactive materials. In the case of Fukushima, the direct effect of the tsunami on the countryside and people was vastly more extensive than the nuclear power plant incident resulting from earthquakes/tsunamis.

II. VSM, A CYBERNETIC VIEW OF MANAGEMENT ORGANIZATION

The purpose of this section is to present information on the Viable Systems Model (VSM) developed by Beer [1] and its application to better diagnose management systems. The hierarchical methods to depict management structures do not help one to understand how these operations actually function dynamically. VSM is a method to underpin understanding of management dynamics in organizations based upon cybernetics.

The key word in VSM is 'viable: capable of maintaining a separate existence'. If one considers the roles of the various parts of an organization, one can quickly recognize that some parts are concerned with ing decisions, others with planning operations and others tasked with carrying out those plans. Between these parts, there are communication channels transporting information about the processes being operated on and instructions to operations personnel to increase or decrease activities.

Beer recognized these relationships as being similar to the detailed actions and responses of human and animal bodies, in other words the same principles being used to understand how animals operate were relevant to the operations of organizations.

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 [2]. Cybernetics is equally applicable to organization and control of physical and social management systems. One application of VSM was to air traffic management (ATM) in Saudi Arabia [3].In later sections, VSM will be applied to the consideration of safety of nuclear power plants as a main thrust of the paper.

VSM was proposed as a better way of understanding and diagnosing organizational behaviour. The approach has been applied to manufacturing, food distribution (Walker, 1991), software development by Herring and Kaplan (2001), etc.

VSM was applied by Beer to government operations in Chile under President Allende, circa 1970-73. This shows the diversity of VSM as a tool for diagnosing various management schemes.

VSM is now discussed. Figure 1 depicts a simple version of a VSM model of a system, in which there is a central management body that determines policy and gives top-level guidance.In this representation, a regulatory/control body controls various activities at the working level (supervisors). Then there are operational activities, from running a Nuclear Power Plant (NPP) to shoe-making, tire production, etc. The environment represents the public, the physical environment or even the Government. Feedback occurs and information or society actions can result from the activities of the plant or the organization. For example in the case of shoes, the public may change its taste from black shoes to red shoes and this would lead to a change in production rates for black and red shoes.

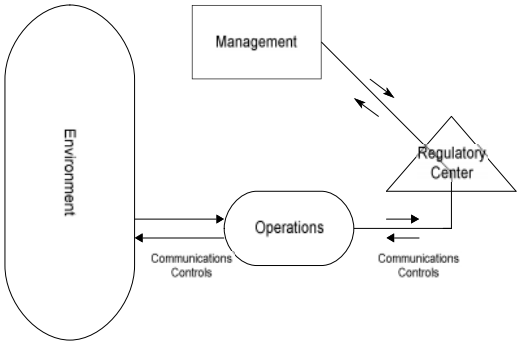

Figure 1 Basic VSM Figure depicting Key Elements within the Approach

The regulator in Figure 1 operates in a similar manner to normal equipment controller. The set point could be related to say the number of shoes to be produced per month as set by top management of the manufacturer. The regulator has a number of rules, which correspond to the algorithm of the controller and can be quite complex. These rules could cover such things as the colour ranges of the shoes, the sizes and selection of materials. The rules may also determine the use of machines, targeted hours per shoe for manufacturing and the length of run producing the shoes. The VSM model depicted here is a simplified model of a shoe manufacturing business. Feedback occurs from the operations function as to the construction and assembly of the shoes and such things as the utility of certain machines to produce different kinds of shoe and of the downtime requirements due to the need to maintain the machines, and the impact of shift changes of operating personnel. The VSM model structures can be expanded to include sub-units with a similar structure to that of Figure 1. The expansion of VSM depends on the needs of the user.

The simple VSM model can be used to examine the relationships between the various key parts of the organization, i.e. management, the control rules for operating the organization, the operations portion and the environmental (the public and other organizations affected by the organizations actions). VSM models focus on both feed-back and feed forward signals that tie the various units together and make it possible for the whole system to work. The dynamic aspect of the VSM model changes an organizational chart into an operating entity; without the roles played by all parts and their communications, the organization is unlikely to function successfully.

In practice a more detailed form of VSM is used to illustrate some managerial and supervisory aspects of organizations. Figure 2 shows a complex 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 as well to select a compact model in order to show the dynamic relationships between the various levels of an organization.

One can see here that the management function is now 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 planning, economics and plant management. The S3* and S2 functions represent co-ordination and auditing functions.

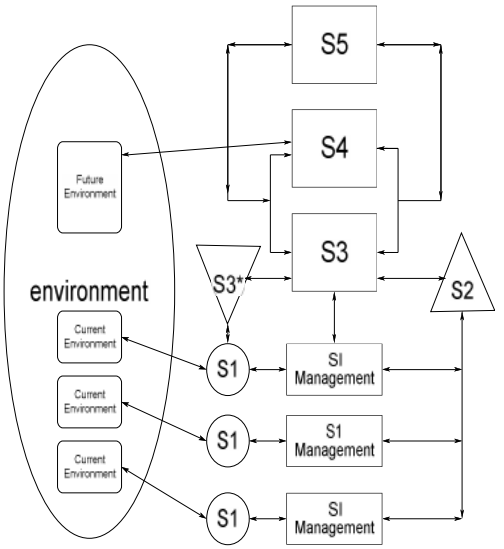

Figure 2 More Complex Version of VSM

III. LATER, SEVERAL ORGANIZATIONS WILL BE EXAMINED TO SHOW HOW DEFICIENCIES WITHIN ORGANIZATIONS CAN LEAD TO ACCIDENTS AND EVEN TO THE DEMISE OF ORGANIZATIONS.NPP ORGANIZATIONAL STRUCTURE

This section is concerned with a more detailed examination of the various management levels within a utility covering maintenance and plant operations. Figure 3 shows a typical nuclear power plant organization. A number of utility organization structures were examined during the early phases of the project, but the one given in the IAEA report [10] captures the management structure in an idealized form.

The figure reflects some of the various functions carried out at single station NPP. The share holders and the Board

are not part of the operating plant but are important in terms of holding the President, CEO and CFO accountable to the public and of course to the interests of the share holders and the other stake holders, the employees. Utilities with multiple stations (or Fleet organization) would have a corporate structure covering each station within a Fleet organization.

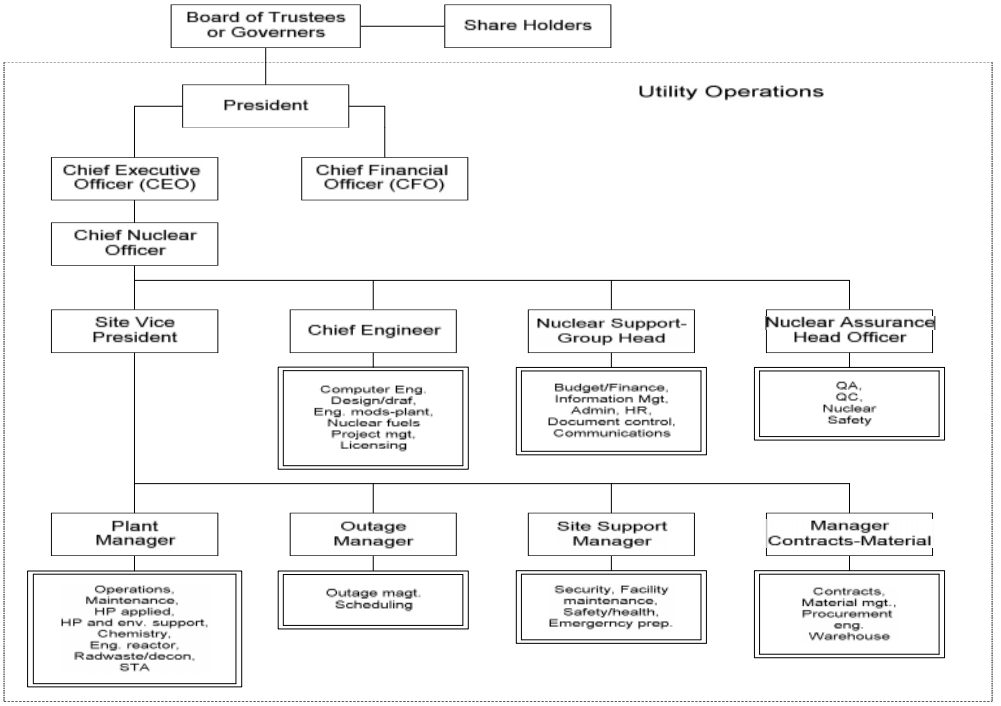

Figure 3 Typical Nuclear Power Plant Organization

A Fleet organization may have some advantages over the single unit organization both economically and operationally, since some functions are carried out for all stations. The figure indicates that the overall responsibility for a plant, economic and safety is with the Chief Nuclear Officer (CNO). The CNO may have a committee advising him on safety and economic issues. The committee may consist of internal plant personnel and outside experts. The CNO reports to the Utility President and Chief Operating Officer.

Like most companies, there are the company officers, President, Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) report to the Board of Trustees/Governors. Later, details of the NRC and INPO organizations will be covered.

The utilities are influenced by a number of different organizations, such as public utility commissions whose job is to ensure that the public has access to inexpensive and reliable power. There are other organizations which have a role in dealing with the utilities affecting some aspect operations. Figure 4 depicts the inter-relationships between the utilities and other organizations, such as Occupational Safety and Health Administration (OSHA), Environmental Protection Agency (EPA), etc. The main organizations that interface with the nuclear utilities are the United States Nuclear Regulatory Commission (NRC) and the Institute of Nuclear Operations (INPO). Also the President and Congress have their part to play in this process.

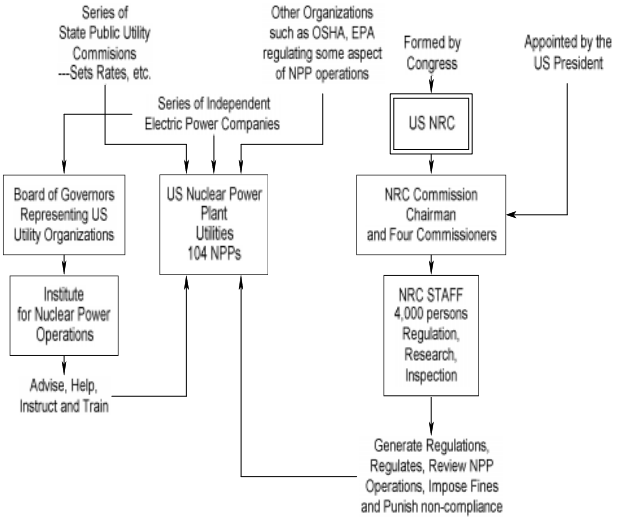

Figure 4 Diagram showing the Interrelationships within the US Nuclear Industry

The NRC regulates the US Nuclear Utilities. The NRC has five main components that enable them to regulate effectively:

1. d Regulations and guidance for licensees;
2. licensing utilities to operate NPPs;
3. oversee NPPs to ensure licensees comply with license requirements;
4. research is also covered by the NRC to provide insights into the causes of accidents;

5. PRA techniques are also used to support commission decisions;

6. the NRC evaluates operational experience, and event assessment.

The NRC plays a strong role in regulation; however the rules and procedures of the process have changed over the years as a result of lessons learned from accidents, both in the US and abroad.

As a result of the Three Mile Island, unit #2 accident in March 1979 [7], INPO was set up by the NPP utilities to assist the NPP utilities to enhance their "professionalism" in dealing with reactor power plant safety. The word "professionalism" is associated with Admiral Rickover and the US Nuclear Navy, meaning a well trained and conscientious group very aware of the need to follow safety policies. Although the Admiral was concerned with submarine operations, much of his approach applies to the civilian NPP operations. Many leaders in INPO have come from the Nuclear Navy. Rickover's philosophy has influenced INPO's approach in working with the US utilities. Accordingly INPO's mission statement is:

"To promote the highest levels of safety and reliability – to promote excellence – in the operation of commercial nuclear power plants." (INPO web site, www.inpo.info)

INPO has four main activities:

1. plant Evaluations, INPO teams observe NPP operations, analyse processes, 'shadow personnel' and question personnel;

2. training and Accreditation, the INPO National Academy for Nuclear Training provides training and support for nuclear professionals;

3. events Analysis and Information Exchange;

4. assistance, at the request of NPPs.

INPO provides assistance with specific technical and management issues in the area of plant operation and support. The interactions between INPO and the utilities are close and complex depending on the needs of the utilities. INPO performs many tasks such as training improvements, independent reviews of plant operations. Some interactions are frequent and others are based upon assessed needs.

IV. VSM APPLIED TO NPP ORGANIZATIONS

Earlier a VSM was depicted in Figure 2 ('More Complex Version of VSM'), which is a version of Beer's original VSM. He referred to a number of parts of the organization and denoted them as sets of System's from S1 to S5. The upper management functions were S3 to S5 and the lower level functions were S1 to S2 and also included S3* which was an audit function. Here that VSM model structure has been modified to conform to a US nuclear utility organization. This modified VSM is shown in Figure 5.

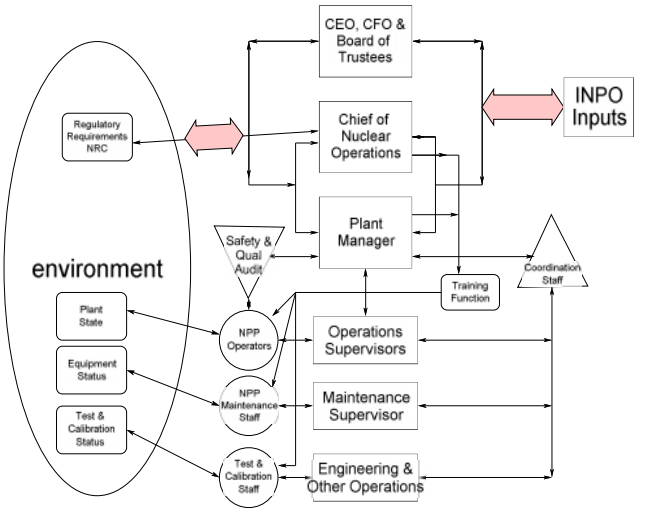

Figure 5 VSM model of a US Nuclear Utility

The figure models a current single US NPP type of organization, which involves the lessons learned over the years from the impact of accidents upon the structure of the utilities and the rest of the industry. The structure of both the industry and each utility was less complex at the beginning of the nuclear utility age. The Three Mile Island, (TMI) accident has had a deep influence on the US industry and led to the formation of INPO. The impact of the accident led to the need to enhance the importance of the reactor operator in performing key safety functions in the operation of NPPs. This has led in turn to modifications and changes in a number of support organizations. Modifications to Beer's VSM figure have been made to reflect these changes in that INPO and a training feature have been added. Operator training was included from the beginning, but the degree, complexity of training and importance has been increased since TMI. So the general structure of control of the organizations has remained much the same, but a number functions added to reflect the need to factor safety within the VSM representation.

Figure 5 reflects the VSM equivalent of the organizational chart shown in Figure 3. The VSM model covers the roles of the CEO, CFO and the Board of Trustees together as equivalent to S5. In Figure 3, there is also a President, which has been subsumed within the S5 category. This combination covers the top decision-making function of VSM.

The Chief Nuclear Officer (CNO) fills the S4 category of VSM, which covers the environmental influences upon the functioning of the NPP, so here it is way of binding together the needs of the environment to the requirements of the organization.

The posture of the CNO towards the CEO, etc. is important. The CEO is responsible to ensure both financial and safety viability of the utility. The CFO supplies the analysis and requirements for financial viability of the organization and Board represents the interests of the stockholders.

The CNO should uphold the safety requirements of the NPP and ensure the efficiency of the organization in

meeting safety requirements while being fairly frugal. The Plant manager reports to the CNO and is responsible for the running of the plant. The operations manager and supervisors report to the Plant manager, along with Maintenance and Test and Calibration. Plant manager is equivalent to the S3 function in the case of VSM. The lower level managers/supervisors for operations, maintenance and test/calibration and their staff are equivalent to S1 functions.

The other functions covered in the Beer VSM are S2 and S3* functions. In the case of the utility, the S2 is a coordination role to ensure that operations, maintenance, test/calibration are coordinated.The staffs of the latter two functions have to coordinate their activities with the reactor operators to ensure that the safety of the plant is not affected by these activities.

Additionally, the operators draw upon the office of the Head of Assurance via the group performing plant probabilistic risk assessments (PRAs). Usually the operators have access to PRA program aids that enable them to switch certain pumps and valves, etc to see if loss of these components would increase the risk of operation and by how much. There are also technical specifications for operation that guide the decisions made by the operators, for example pump, P#2134 can be withdrawn from service for no more than 10 hours after which the plant has to be shutdown. If this operation is being carried out with operations of valve, V#2334, then the plant has to be shut down.These operations are carried out under the guidance of rules called technical specifications for running the plant and agreed with the NRC.

The S3* function is there to audit the operations to see if they correspond to defined operations outlined in operational or maintenance manuals. The control room operators have a log in which all maintenance, etc. operations are recorded and when they occurred. This record also records accidents/incidents and is carried out as part of the operators' role. There are also automatic recorders, displays and computer output to backup the functions of the operators to ensure accurate records are available for post accident/incident analysis. As mentioned before, the utility has to inform the NRC of accident/incidents within a short time after the accident/incident. The on-site NRC inspectors will also investigate and report to their area inspection group.

With a view of trying to simplify the VSM representation of the utility organization certain parts of the actual organization have been omitted., for example, the following functions have been omitted: Engineering, Nuclear support group, Outage group, Site support and Contracts. This is not to say that these functions are not important, but rather the examination of utility response to accident is that which is of concern here.

V. OUTLINE OF SOME ACCIDENTS

The purpose of this section is to examine a series of accidents to consider the organization causal aspects associated with them. Also it is also an exercise in using VSM methodology to see what might be improved relative to the organizations to consider the balance between safety and economics and how to adapt VSM to high risk organizations.

One purpose of VSM was as a tool to diagnose organizational structures and manner of operation. One can use VSM to help diagnose various management relationships from top management, governments to lower level managers interacting with operators. By analysing accidents, one can see how the various units, making up the organization, work together or otherwise. The dynamics of the processes are on display, which are difficult to see during steady state operation. However, even if an accident has not yet taken place, it may be possible to examine the consequences of decisions. Sometimes, the effects of managerial decisions can take awhile to manifest their effects upon the operation.

Here a number of case studies are 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, wherever possible in order to understand both the causes of the accident and its propagation. Included in the set of case studies are examples of different sources of accidents.

Nuclear accident analysis is key part of this paper, but it is considered useful to examine accidents in other industries, since it is likely that the lessons can be learned from these other accidents that are applicable to the nuclear field and vice versa. As was stated in the beginning of the chapter, there are multiple reasons to study accidents: to understand the accident progression, what are the organizational causes of an accident, how does one organization compare with other organizations and what can one learn from the accident in terms of what is important about an organization's characteristics to minimize or fail to minimize the occurrence of an accident and terminate/mitigate its effect.。

A number of case studies have been selected from accidents/incidents that have occurred in the nuclear and other industries to examine this propostion.

The following cases are addressed here:

1. Three Mile Island Unit #2, March, 1979
2. Fukushima Accident, March, 2011
3. Challenger Shuttle Accident, January, 1986
4. North East Utilities issues leading to failure of utility due to change of management, circa 1986 to 1997, [8]
5. Unknown Utility: leaking valve packing situation [9]
6. BP Oil rig, both BP and US government issues, April, 2010 onwards with the leak officially sealed

September, 2010 There are many other cases that could be studied, for example:

7. Davis Besse accidents, loss of feed and auxiliary feed, Outage report June 1985 to December 1986 from Union of Concerned Scientists
8. Davis Besse near accident reactor vessel head penetration, March 2002
9. Millstone Unit 2, white finding Aug 8, 2011, reactor trip from over-speed of turbine during turbine valve test, see NRC report, raises question about NRC oversight
10. BP Texas City refinery fire and explosion, March, 2005

Since the space available here is limited, attention is paid primarily to TMI, Unit#2 and Fukushima accidents. TMI caused a major shift in US thinking about the role of humans in control of accidents. The Fukushima accident is likely to have large effect on the Japanese Government and Utilities. It also has some strong messages for other countries' industries. This is not to say that the other accidents are not significant, they are, but here the concentration is on these two accidents.

A. Three Mile Island, Unit #2 Accident

The accident started with a loss of main feed due to an incorrect filter switchover procedure. The Three Mile Island NPPs are designed by Babcock and Wilcox and have once-through steam generators. Attention to water quality is paid for all steam generators, but once-through units are particularly sensitive. The main feedwater has in-line filters to improve the feed supply quality, but they need to be replaced at frequent intervals. It was during the switch-over process that the main feed flow was cut off.

Both the reactor and the main turbine trip automatically. In response to this, the auxiliary feedwater system should have started, but failed to start due to a maintenance error. This was not spotted by the control-room crew, since all auxiliary feed isolation valves were closed. All safety injection and residual heat removal pumps started due to the correct generation of the Safety Injection (SI) signal. Due to heat-up of the reactor primary system, reactor pressure increased and the pressure operated relief valves (PORVs) opened. This is the normal response. Subsequentially, the reactor pressure dropped and continued to drop until it reached the saturation temperature pressure and boiling in the core started.

Once the reactor pressure falls below a low pressure set point the PORVs should have closed. The PORVs did not close, but the operators thought that they had, since the PORVs were indicated as having closed. Error in indication was caused by poor instrumentation design for the PORV. Following boiling in the core, the generated steam rose to the top of the reactor dome and displaced the water there. The displaced water moved into the pressurizer and the level within the pressurizer rose. Eventually, the pressurizer fills. The operators thought that the reactor pressure was under control and that Safety Injection was continuing to inject water and the change in water level was due to the safety injection flow. Therefore, they decided it was not necessary to continue to run the safety injection pumps and shut them off. The reactor decay heat continued causing boiling and eventually the top of the reactor core was uncovered, the cladding was not being effectively cooled by the steam flow and its temperature rose and melting of the clad occurred. The clad is one of the three barriers to the release of radioactivity, along with reactor vessel and steam generator tubing and the containment. With the failure of the cladding some fuel pellets fell to the bottom of the reactor vessel.

Subsequently, the control-room crew with guidance from a unit #1 supervisor realized that the core was uncovered and switched on the Safety Injection (SI) system.This further accelerated core damage by shattering the overheated clad, when it was exposed to the cold safety injection water. The consequence was that the core of the Unit #2 reactor was destroyed and there was a mixture of reactor fuel pellets, and cladding fused together at the bottom of the reactor vessel.

The whole unit was written off, a large economic loss, but very few people were affected, since most of the radioactive material was contained within the reactor and containment. This was in line with the "Defence in Depth" philosophy of the United States.

B. Fukushima Daiichi NPPs Accident

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 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 an entirely correct response. The actual ground acceleration was 0.56 g versus 0.447g. 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 for various reasons and were not operating.

One result of this type of earthquake (a sub-duction fault) was a series of large Tsunamis were generated. The INPO report [10] was produced later than the Braun report [12] and is much more detailed, but still does address questions related to why certain actions were and were not taken. The Tsunami caused devastation of the area around the region 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. The INPO report indicates that there were multiple tsunamis, seven altogether. It also states that several after-shocks of lower magnitude occurred before the tsunamis arrived. At least 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 18.7 feet (5.7 meters), so the

actual largest tsunami was well above the design basis and the ground level. Figure 6 shows the various measurements related to the building, and water levels achieved during the tsunami. In addition to the above mentioned earthquake damage, the tsunamis were of such a size that they overflowed the NPP seawall protection, which was supposed to be bigger than the design basis for the NPPs

.

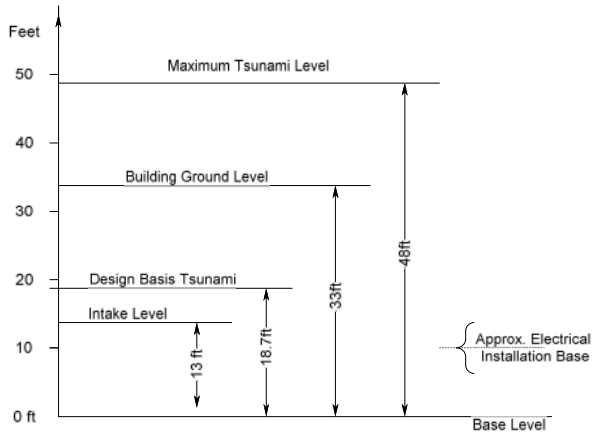

Figure 6 Diagram showing various key water levels related to the Accident

The sizes of both the earthquake and Tsunami magnitudes exceeded the design bases for the NPPs. It has been reported that seismic experts had informed TEPCO about two years earlier that this same area was devastated in 875 AD one of a similar size to this Tsunami and that information should have been included in the data base from which the design basis Tsunami was selected [11].

Because of the size of the Tsunami, sea water caused the standby power diesels to fail, the diesel fuel tanks to be blown away, some battery rooms, and the levels in turbine halls flooded. There were some diesels that air started, but could not be used since rest of the electrical systems had failed. The grade level for reactor buildings was at 33 feet, but the electrical equipment Switch gear, Batteries and Emergency Diesel Generators were below grade level. The inlet cooling system structures were at 13 feet and it 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. A Blackout is a situation in which offsite power and station generated power are lost. The station generated power is derived from standby diesels, which are supposed to start up on the loss of offsite power within a short time. In this case, the diesels started and then stopped due to the tsunami flooding the diesel locations.

The Reactor control room personnel were placed into an emergency condition with four units in a hazardous condition. Even well 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 take action. Initially, all went well following the earthquake, the reactors shut down (control rods inserted into the reactor core), the auxiliary electric supplies via the diesels came on and the initial stages of decay heat removal was being taken care of.

There may have been some damages 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 instrumental 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. The crews were also faced with the fact, that their families and friends might have been killed by the effects of the earthquake and the tsunami.

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. 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.

A number of accident reports relating to Fukushima were available shortly after the accident, for example see [11], but they focused on the accident progression, what actions were taken and what was the state of the plants at various intervals. The 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 effected 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. It is not clear whether NPP staff and managers recognized the possibility that whatcaused 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 sources. It will be some time before a complete account of the accident sequence and the sources of radioactive releases are agreed.

The INPO report [10] covers some of the difficulties that the site personnel had. A couple of paragraphs give an insight into the problems that the personnel had.The locations were dark, radiation was highin some locations, equipment was not working, earthquakes caused vibrations and the threat of explosions existed.

This extract is from the report [10] dealing with unit 3:

'The operators understood they needed to depressurize the reactor but had no method of opening an SRV. All of the available batteries had already been used, so workers were sent to scavenge batteries from cars and bring them to the control room in an attempt to open an SRV.

At 0450 (T plus 38.1 hours), workers attempted to open the large air-operated suppression chamber containment vent valve (AO-205). To open the valve, workers used the small generator to provide power to the valve solenoid. An operator checked the valve indication locally in the torus room, but the valve indicated closed. The torus room was very hot because of the previous use of RCIC, HPCI, and SRVs; and the room was completely dark, which made a difficult working environment. By 0500, reactor pressure had exceeded 1,070 psig (7.38 MPa gauge), reactor water level indicated 79 inches (2,000 mm) below TAF and lowering, and containment pressure indicated 52.2 psia (0.36 MPa abs)'.

Later:-

'A large hydrogen explosion occurred in the Unit 3 reactor building at 1101 on March 14. The explosion destroyed the secondary containment and injured 11 workers. The large amount of flying debris from the explosion damaged multiple portable generators and the temporary power supply cables. Damage to the fire engines and hoses from the debris resulted in a loss of seawater injection. Debris on the ground near the unit was extremely radioactive, preventing further use of the main condenser backwash valve pit as a source of water. With the exception of the control room operators, all work stopped and workers evacuated to the Emergency Response Centre for accountability'.

The acronyms are: SRV=Safety Relieve Valve, Torus is part of the containment of a BWR (Figure 2.9 noted as WW), RCIC =Reactor Core Isolation Cooling and HPCI = High Pressure Coolant Injection, TAF = Top of Active Fuel

Given that a blackout had occurred and that the tsunami had impacted the site with 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 and cover the reactor cores.The loss of power affected not only pumps and valves, but also lighting and availability of instrumentation, for example the staff did not know the water level in the reactors. The crews located car batteries and connected 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 the fact that given almost nothing worked, the question was what pieces of equipment could be placed into some degree of working and what actions did one have to take to accomplish this This is carrying out an emergence planning on the fly, as one can see from the second paragraph above.

C. Challenger Shuttle Accident

On the day of the accident the Challenger was launched and all seemed to be going well at first, but a short time later the main fuel tank exploded due to hot gases impinging on the tank coming from one of the solid rocket booster (SRB) units attached to the shuttle. The leak was due to a SRB joint not functioning correctly. The joint was made up of bolted flanges between two sections of the rocket body.

In fact, the rocket was made up of a number of segmented sections that were bolted together and was designed in that manner to aid in transporting these long SRB by plane. In order to prevent the joints leaking, there were two sets of flexible "O" rings, which allowed the joints to flex during take-off. For the "O" rings to work, they needed to be flexible and squeezed to seal the space between the two flanges associated with each of the SFB sections.

It was asserted that the failure was caused by the lack of flexibility of the "O" ring material under environmental very cold temperatures from before and up to launch time. The "O" rings lost the ability to seal the joints. The consequence of this lack of sealing was the hot gases, formed by the solid rocket fuel burning to provide thrust for the Orbiter take-off, ended up impinging on the Main Fuel Tank and causing it to explode. The Main Fuel Tank provided fuel for the Orbiter's three main rocket motors. Following the failure, the Shuttle crashed and the crew all died.

D. Northeast Utilities Operations 1986 Onwards

The previous cases listed devolved around accidents; in this case there was no single critical accident. However, there was a gradual deterioration of the plants' performances over the period under study. The deterioration stemmed from the conscious decisions made by the top

management to reduce the cost of generating power from all four NPPs (later another plant was added) by reducing manpower in the operational and maintenance areas.

As a result of the top management actions taken to reduce staff and being heavily focused on costs, led to plant availability falling from about 90% to 56%. Problems that occurred at the plants could eventually, it is believed, to a severe accident. Luckily, this did not happen. Plant shut-downs occurred due to equipment problems induced by failures to service equipment. Later, it was discovered that there were issues associated with corrosion of pipe work; this could have led to an initiating event for a major accident. Also, there were deficiencies in following up on Final Safety Analysis Report (FSAR) related to non compliance of the plant components and systems to requirements spelled out in the FSAR. Again these problems were associated with shortage of staff.

It could be said that the Millstone plants were very much approaching the point that a severe accident could have occurred due to issues associated with both systems problems and operational problems. In the process of staff reductions due to early retirements and layoffs, the skill bases of the plant staff were gutted. Reductions led to loss of supervisors and managers. In addition, staff also informed the top managers that plant safety was being impacted by their actions. This information was ignored and conflicts grew between management and staff.

The NRC became aware of these issues by being informed by whistle blowers, was concerned about its impact on plant safety and also became concerned whether there was sufficient protection for whistle blowers from management action.

E. Unknown plant: Near Accident caused by a Valve Failure

This situation was one of the topics discussed in [9] and covered the detailed activities of maintenance and test crews at a un-identified plant. The issue was focused on leaky stem packing associated with a safety significant valve and the activities of a large number of personnel connected one way of another to the valve.

The valve issue started after there had been a long shutdown and the problem was due to leakage past valve packing. Another factor that had a major affect on performance was the pressure to return the plant to operation.Meetings were held a number of times and different levels of understanding of the issues among the participants and various solutions were proposed.Apart from the leakage past the packing, there was a concern about the functionality of the valve and stem connection.

The plant at this time was shutdown, at low pressure and temperature. The correct solution to the problem was to cool the plant further and then take the plant to a condition analogous to a refuelling condition, but it appeared that most groups did not wish to do this and were looking for short cuts of one sort or another. One such option was to freeze the fluid in the pipe and that would allow work to proceed on the packing and fixing the valve/stem problem.

However, there were considerable problems between the top management and personnel, which was manifest by safety issues being brought up with management and even the NRC. These issues were due to reduced manpower and loss of the more skilled personnel taking early retirement or being laid-off. The book [9] indicates a couple of things, a lack of awareness on the part of some of the staff of the defence in depth requirements as they relate to valve boundaries and the lack of management directions for the various working groups.

F. BP Accident

The Gulf oil disaster occurred during the drilling of a deep oil well in the Gulf. BP was the client in the drilling of the oil well at the time of the accident given that they were the owners of the well site. The exploration rights were leased by the US Government to BP.BP personnel were in charge of the operation, Transocean was the owner of the drilling rig, and ship and provided personnel for these operations, and Halliburton was the provider of cement and drilling "mud". The accident is described here to give an overall picture of the accident, but later the focus will shift to the measures taken by the parties to control the accident, terminate it and minimize the effects on the neighbouring states.Although the cleanup led to a large number of jobs, the accident's real impact was on the long term loss of fishing and vacation-related jobs. The accident was both an ecological and economical disaster and will have a long term depressive effect on the region.

The oil rig was a ship with a drilling rig mounted on its deck. The rig crew had just celebrated a ten year no accident period and managers from the various companies associated with this achievement were present for the celebrations.

The drilling operation was behind schedule and there was pressure to quickly drill through to the oil pool below. Some of the operations, which go into preparing the hole, depended on the use of special cement to constrain the oil paths and prevent the ingress of water. There was also the use of a number of spacers within the bore. It was said later that the cement was sub-standard and the number of spacers were less than what should have been used. Clearly, this is a question of opinion. It has been asserted that testing of the quality of the cement was not done correctly and it should not have been used. The spacing decision was taken to speed up the drilling process, again this was an opinion. This will continue to be discussed and turn up in committee meetings and in court.

The significant event was that during the drilling there was a large release of gas, possibly due to solid methane being transported to the surface and then evaporating on the way up. From a safety point of view, one of the deck crews failed to warn the ship's company of the problem and there was an explosion, which killed a number of crew members.

VI. IMPACT OF ACCIDENTS ON MANAGEMENT

Accidents have had an impact on NPP organizations and changed them in a number of ways, some structurally and some in redefining how they operate. The early days of nuclear power the utilities followed the practices of the fossil, coal, gas and oil, power plants. For these plants, safety of the public was of little concern, because the zone of influence of explosions was small.

The main criterion was the cost of operations so the price of electricity was kept low. Utility management thought of NPPs as being the same as fossil plants, but with a different heat source. The complexity of NPPs was new to them and the attention to safety had a secondary impact on them. The net result of this was that the organizational structure was very similar to fossil plants.

Also during this period, the industry as a whole, this includes manufacturers, and the regulators, thought that the safety protection of the plant was insured by automatic means and the role of operators was not too critical. The influence of decay heat following a reactor trip was underestimated.

All of these were to change with the Three Mile Island accident.The role of the operator was upgraded, training emphasised and man-machine interfaces improved.

Additionally, the industry as whole decided that they need to improve the safety of their plants and formed the Institute of Nuclear Operations (INPO) to help bring that about.Subsequently, utilities have seen the need to introduce a management position as a focus for nuclear safety. The position is called the Chief Nuclear Officer (CNO) of the company.

Figure 7 shows the VSM model of a US Utility with interactions between the NRC and INPO.The internal communications within the utility shows the central role of the CNO, interfacing with the NRC and INPO. The plant manager is in communication with the maintenance and operation staff and there are monitoring and audit staff ensuring operations are being carried out per instructions and procedures.

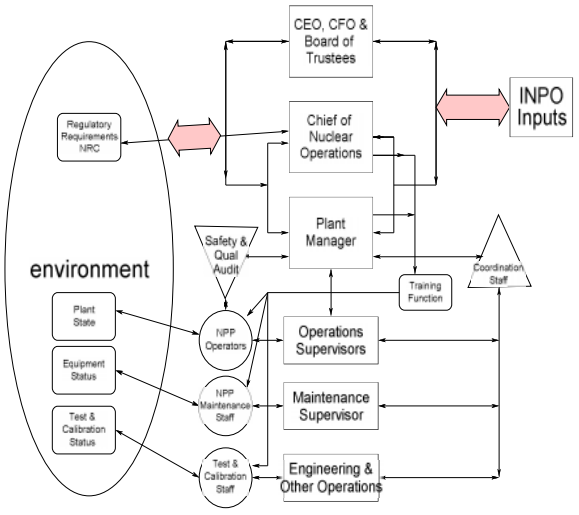

Figure 7 Depiction of a VSM model of a US Nuclear Utility

A VSM model of a utility in the early days of nuclear power would not have these features. There would be no INPO, no CNO and controls and procedures would be much less. Training of the operators would most likely not use a training simulator on a regular basis since the utility was likely not own and operate one. Emergency operating procedures are now symptom-based as opposed to event-based. Other accidents have also had an impact on the utilities, maybe not quite as significant as TMI, up to this time.

One can think of the NPP business as a business than needs to learn and in fact INPO calls itself a learning organization. However, it is observed that the industry is less likely to learn from deep understanding of the issues than from the direct effects of an accident. Opinions can be argued around, but it is difficult to withstand the fact that an accident has occurred! The model for improvement is captured in F8.

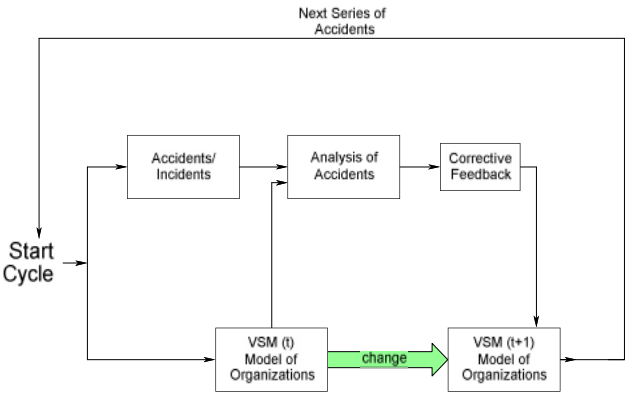

Figure 8 Depiction of the Improvement Pathway

The figure shows how the improvement process works seen as changes in the VSM structure and rules.

It has been observed that the significant causes of accidents are to be laid at the feet of management, since it is management that can effect change in the way the organization is run.

Often, the agent involved in an accident is the operator, so for example in the case of TMI it was the control room staff that that caused the accident by virtue of their actions and lack of actions. On close examination, it was ruled that they were undertrained, did not have the right kind of procedures. Also there were design issues associated with the PORV position indications. So even in this case, the operators were placed in their position by the acts of others.

As in the case of the other accidents, the role of management in leading to an accident is significant. In the case of the Challenger, it was the decision of NASA management to proceed with the launch in the face of advice from engineers not to proceed.

In the case of North East Utilities (NU), the decision to cut staff and reduce maintenance work to increase the profitability of the operation was the decision of top

management, President and CEO. The NRC was very slow in acting to ensure good safe operations, but in the end did act to shutdown the utility. INPO found that their arguments for NU to improve their operations were unsuccessful.

The Board of Trustees, who represented the shareholders and could sack the President and CEO, failed to do so even when informed of the issues by NRC and INPO.

One can also see in the case of the leaky valve issue and the BP oil rig accident, the role of management is critical. Incidentally, in the leaky valve near accident case, the management of the plant were the self same NU managers mentioned before. This indicates the management was poor in controlling operations. The operators needed to have better understanding of the safety issues involved and the organization of the workforces was poor. Here the management was focussing on force reductions without the compensating feature of improving efficiency of the operation.

In the case of the Oil rig operation, BPs local managers were pushing the pace of drilling when there was a need to move slowly and carefully. There were issues with setting concrete correctly and in the poor application of using drilling mud plus the unexpected presence of frozen methane being released. The unexpected release of methane lead to explosions and fires on the rig. The BOP device failed to operate correctly(possibility due to the fire/explosions) led to the large oil release. It appears the BP had no prior plans for containing such a spill. Also the US Government failed to act quickly to prevent the spill spreading. The Government seemed to have more interest in blaming BP than trying to prevent the subsequent ecological and economical damage to the various Gulf States. So here again the role of decision-makers is critical. There was a problem with the failure of one of the operators in failing to warn the other operators of the possibility of fires occurring leading to a loss of life.

In the case of the Daiichi NPPs accident there are many things to learn. The following portion of this section will concentrate on this accident. There are things associated with decision-making in both the long term and short term.

The earthquake and the tsunami were unexpectedly high relative to what the TEPCO management expected. The earthquake was 9.0 on the Richter scale and the level of the tsunami reached 48 ft, which was well above the design basis level of 18.75 feet. The nuclear accident seen by itself was very bad, both economically, radiation release wise and from the death of a number of people. However, seen in the context of the effects of the tsunami on the surrounding land this seems small. The direct result of the tsunami about 20,000 people died and 110,000 houses damaged.

The Daiichi accident initiator was the tsunami, however the consequences can be laid at the feet of the top management of Tepco. They turned a tin ear on the statements that the area around where the plants were positioned had been subjected to tsunamis of a greater magnitude than allowed for in the design. This meant that the steps taken to protect the plant were well below which was necessary to over-ride the accident.

Since they had failed to take action, it followed that their emergency disaster procedures would be less than adequate, so the staff at the plants were less prepared and practiced to take care of the subsequent stages of the accident progression. Often in responding to accidents time is of the essence. In this accident time was lost because of the lack of preparedness due, in fact, to the incorrect decision-making of management.

Given their state of unpreparedness, the station staff did extremely well in trying to prevent further damage to the reactor cores and the release of radioactivity. Often, as can be seen from the INPO report [10], their work was often undermined by subsequent hydrogen explosions, which destroyed equipment and led to obstructions hindering further attempts at fixing the problems. Because of the tsunami flooding, most of the electrical equipment did not work. Diesel generators failed, batteries failed and switchgear flooded, the result was pumps did not work, indicators did not show reactor conditions, lights were unavailable, etc. The station personnel were put into the position trying to get things working by bringing car batteries, going into very dark areas to try to manually operate valves, etc.

These persons had to evaluate and plan to do operations, ab initio, under the direction of the station manager. Consequently, the accident progressed faster than the personnel could effect change. One of things that the local personnel did was to form a tight group trying to effect a credible response to the accident, so the normal NPP organization morphed to a smaller organization, see Figure 8.

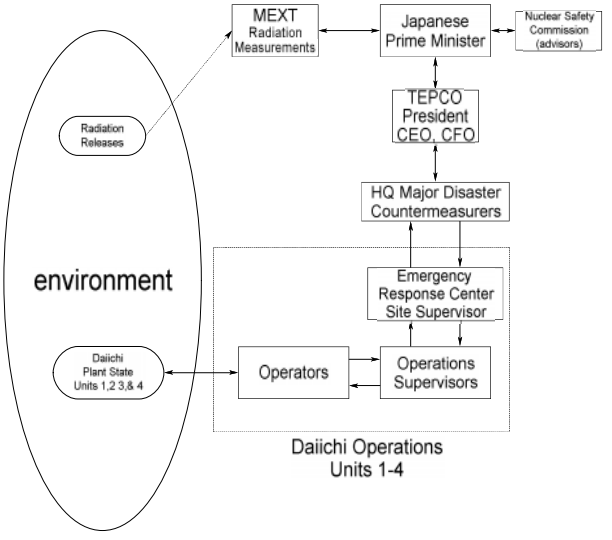

Figure 8 Emergency Daiichi Organization

The figure shows the presence of the Japanese Prime minister, who was involved, and others. However, the principal burden was on the skills and tenacity of the site personnel.

The emergency organizational model is in fact a VSM model, which evolves in emergency conditions from the

normal VSM organizational model. The decision-making, communications and control dynamics are features of a cybernetic process. In order to be effective, the organizations needs to be trained, practiced, and have both procedures and ancillary equipment to support the timely actions of the operators.

VII. COMMENTS AND CONCLUSIONS

Although many accidents that have occurred over the years have had an effect upon the nuclear industry, some have had a more significant effect than others. The TMI accident had a large effect, since there was a forced change in the appreciation of the role of humans in terminating and mitigating accidents. This then led to changes in the industry relative to training, type of emergency procedures and displays to assist operators perform their tasks. Other accidents have clearly displayed the need for better monitoring of top management decision-making. This has been borne out by a number of accidents mentioned in the list at the beginning of the paper.

For example, the Challenger accident, in a way it was a certainty, since the top NASA pre-empted the advice of the engineers and further more went looking for others that would support their ill advised decision.

The Tepco management decision not to increase the height of the tsunami protection and further look at better defences against water ingress in the zones where there were electrical equipment was another poor decision.

In some ways, the decisions taken by NU top management were worse, in that they were warned by their own staff, the NRC and INPO against doing what they doing. Additionally, the PUC also were concerned relative to the reliability of electrical services and they pointed out they were not looking to pressure NU to reduce the cost of electricity.

In the case of BP and the Gulf disaster, there did not seem to be pressure from BP top management to complete drilling the well, but clearly the local management felt a pressure to push ahead strongly, when there were voices saying hold on and check before pushing ahead. So this was a poor decision, again against advice. Also, there did not seem to be any attention paid to the risk fact as to the possible consequences of a bad decision. Equally, one must also hold the US Government responsible for not deciding to take steps to contain the oil spill, timely action by the Government to organize a quick response and use other countries ships could have reduced the size of the spill and protected the states in the Gulf from the effects of the oil spill. So lacking of timely decision-making is not restricted to industry.

The Fukushima or Daiichi accident is a wonderful case to examine for issues. There are a number of issues that we can examine and provide some suggestions that might help reduce accidents in the future. One thing that can be said before proceeding is that the VSM model of an organization provides one with a good vehicle to analyse organizations because it focuses on the dynamics in the organization as to who is making decisions and who is taking them. The other thing that one should accept is that sometimes the management decision is not in the same time frame as an accident. For example in the case of the Challenger accident, the decision to select the jointed version of the solid rocket boosters was made a long time before it became an issue.

A review of the Daiichi accident clearly points to the main fault, that the management was not prudent enough and hoped that the tsunami defences were sufficient. They used PRA methods to obfuscate the issue of the tsunami. PRA techniques are useful to check the main safety situations, but one must use very carefully chosen probabilities to represent the plant, the crews and also the frequency of initiating events. Often, one looks at events with a probability of 1E-3/year to define the design basis accident initiator. In this case the selected probability of a large tsunami was nearer 1E-2 and estimated not to exceed 18.7feet.

It is recommended that one should look for weaknesses in the design by looking the sensitivity of design features by incrementally changing the initiating event size, i.e. height of water (floods), wind velocity (hurricanes), etc. Carrying this out here would have revealed the weakness of the design to flooding, leading to a complete blackout, with loss of diesels, batteries, switchgear and instrumentation. It is clearly the function of the CNO to sponsor this type of consideration on behalf of the utility.

It is interesting to note that the Japanese Prime Minister's office had a group of advisors, Nuclear Safety Committee to offer advice on nuclear safety philosophy. Later, the Chair of this committee criticized Tepco and authorities for their attitude to safety.

One of the lessons from the TMI accident was the move from event-based procedures to symptom-based procedures. It appears that a similar type of approach could be used here in dealing with the emergence disaster procedures. In other words move from a set of defined events to determine how the station personnel respond to a set of ill defined events, which can destroy many of the tools and aids set aside to help recover the plant. Time is of importance here, since the message from Daiichi is respond quickly, before the situation gets worse, so one should practice the actions to be taken under these kinds of conditions. In the Daiichi accident: no lights, blocked access, slow responses from outside, no backup high pressure pumps with diesel power, and some design features inhibiting progress. Vents to disperse hydrogen and other gases were difficult to operate under these conditions, ultimately led to hydrogen build up and explosions. The damage caused by these hydrogen explosions led to further problems for the teams, including injury to their members.

REFERENCES

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

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

[3] S. H. Al-Ghamdi, "Human Performance in Air Traffic Control Systems and Its Impact on Safety", A PhD dissertation, City University, London, 2010

[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] IAEA, Nuclear Power Plant Organization and Staffing for Improved Performance: Lessons Learned, IAEA-TECDOC-1052, International Atomic Energy Agency, Vienna, Austria, 1995

[7] J.G, Kemeny, "The Report to the President on the Three Mile Accident," Published by US Government Publishing, Washington, 1979

[8] Paul W. MacAvoy & Jean W. Rosenthal, "Corporate Profit and Nuclear Safety," Princeton University press, Princeton, New Jersey, 2005

[9] Constance Perrin, "Shouldering Risks: The Culture of Control in the Nuclear Power Industry," Princeton University Press, New Jersey, 2005

[10] 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

[11] CNN, "Expert: Japan Nuclear Plant Owner warned of Tsunami threat", CNN World Report, Asia, March 27th 2011

[12] Matthias Braun, "The Fukushima Daiichi Incident", AREVA report, Series of Slides produced by Dr.Braun (matthias.braun@area.com), March 26th, 2011

Anthony J. Spurgin: Was born in Bury St. Edmunds, England and obtained a BSc (Eng) in aeronautics at Northampton Engineering College, London University. He has worked for Vickers Armstrongs, General Electric Company, Central Electricity Generating Board, Westinghouse Electric, and General Atomics. While at University he worked for Percival Aircraft and SAAB (Sweden) in the summer. On leaving University he was a graduate apprentice at Vickers for 18 months and then worked on aeroelastic studies of various aircraft. His time from leaving Vickers, he worked on the design of control and protection system design, and transient analyses of a range of power plants from Gas Cooled and Pressurized Water Reactors to fossil fired power plants including super critical boilers. He progressed from being an engineer, to senior engineer to group leader. He later became a independent consultant performing research in the fields of risk assessment and human reliability and has consulted with a large number of organizations, including EPRI, NRC, DOE, EDF, IAEA, and a number of Nuclear Utilities. He has published more than 50 papers on a variety of topics from dynamics of heat exchangers, control system design, control room operator reliability studies using simulators and the development of human reliability assessment methods. He has published a book on Human Reliability assessment. Mr. Spurgin is a Senior Life member of the IEEE, and a Member of the IMechE. Was a member of IEEE Nuclear Engineering Committee and Power Generation Committee and Chairman, and VP of San Diego IEEE Section and been the chairman of the local reliability and the controls chapters of IEEE. Currently he is the chairman of a Nuclear Super Session at the IEEE 2012 PES meeting in San Diego.

David W Stupples: Professor David Stupples (BSc (Hons) MSc (Eng) PhD FIEE FInstMC) specialises in research, development, and specification of large and complex engineering systems. For a number of years he undertook research in the area at the Royal Signal and Radar Establishment at Malvern, followed by systems research for NATO, and then in systems research and development with Hughes Aircraft in the US. Until 2003, David Stupples was a senior partner with PA Consulting Group where he was responsible for the company's consultancy work on the design, build and operation of large and complex engineering systems. He has applied systems engineering to a significant number of large-scale engineering and technology systems around the world, and has particular expertise in the effective design for full lifecycle ownership including socio-economic considerations.