Application of Cybernetic Models in the Study of Safety and Economics of Nuclear Power Systems and other High Risk Organizations

A Study of Nuclear Power and High Risk Organizations to understand the central role of management in the safety and economics of these operations

Anthony J Spurgin, BSc (Eng) London

2013

School of Engineering and Mathematical Sciences

City University

London

Abstract

The safety and economics of nuclear utilities and High Risk Operations (HROs) is very dependent on the quality of both the management and operations personnel. The decision-making capability of management is important in ensuring that the operators are adequately prepared to deal effectively with accidents. This means that management has to understand the risk of power production and adequately deal with it, so that the viability of the utility is not compromised, while still operating in an economical manner. The vehicle for enabling management to function effectively is a dynamic designed organizational structure in which all personnel communicate well and is designed to use the best features of human performance according to their roles within the organization.

The purpose of this thesis is to investigate the application of Beer's Viable Systems Model of an organization to see if it fits the requirements of nuclear power plant (NPP) organizations to be both economical and safe and to propose modifications to VSM to more closely match the needs and requirements for NPP organizations.

It is realized that organizations can operate effectively when they are not operating under stress, however the situations changes when they are subjected to accidents. A well designed organization is one that is prepared and can respond quickly to an accident. Because of the possible impact of accidents on organizations, the thesis studied a number of accidents that have occurred in the nuclear industry and to cover the more general case of HROs, accidents affecting other industries were also considered.

Based upon the accident investigations and from the study of human behavior, insights were developed related to characteristics of both managers and operations personnel. These insights led to the development of an understanding of how VSM needs to be considered when dealing with HROs, including NPP utilities. The top down structure of VSM mirrors the basic needs of an organization, but the demands of responding to the safety requirements of an organization requires an understanding of the effects of the time response limits placed upon an organization. These requirements dictate changes to the VSM organization designed for normal commercial organizations, where time for decisions and actions are not so important and these changes are addressed.

Although in normal commercial organizations risk assessment is considered, in the NPP utility and HROs business it is extremely important, since poor decisions with respect to risk can affect the viability of the organization. The thesis covers the use of risk assessment technology to improve management decision-making. Currently, the industry uses risk assessment techniques for total plant risk (more for licensing purposed) and for plant state risk assessment.

The contribution of the thesis is seen as contributing to improvements in the understanding of VSM and making some modifications to it. The importance of time response of organizations in combating accidents and its human performance background is demonstrated and the mechanisms whereby performance is improved by the use of procedures and training is explained.

ACKNOWLEDGEMENT

I would like to thank two people who have contributed much to the thesis. Their contributions are different, but are highly valued.

My wife has been a support throughout my time involved in writing and modifying the thesis. She sacrificed her art room to give me space to work on the thesis.

To Professor David Stupples, I owe much in terms of changing my view of organizations and for his support and intellectual probing. Rather than dealing with just the influence of operators on the safety of nuclear power plants, he gave me the incentive to consider a much broader view of safety and economics in terms of the contributions of top decision makers, i.e. the management of the utility. He introduced me to Stafford Beer and his work on cybernetic organizational structures and the dynamic role of the participants and for that much thanks.

Table of Contents

page

List of Figures ..... page

List of Tables page

CHAPTER 1

1 INTRODUCTION

1.1 Statement of the Issue

The issue is to better understand the role of an organization in ensuring the safety of nuclear power plants, while operating them economically. To carry this out, one need is to have a useful model of the organization, so the selection of a model is the key to developing this understanding. While the safety of a nuclear plant is a deep concern for society it is not the only concern. Without the plant being operated economically, it has no future, so both aspects need to be considered. Developing such an organizational model will be of great use for the nuclear industry, it also holds value for many other industries, such as the oil and gas industry.

The thesis is concerned with an in-depth examination of management aspects associated with nuclear power operations, such as safety of the public and plant personnel as well as the economics of power production, used by electric power utilities. Insights into the characteristics of nuclear operations can be best garnered by the study of accidents and how organizations deal with them. Based upon this work and the selection of an appropriate model, insights related to management and operators, as far as decision-making and communications, will be developed. The results are expected to apply to other industries, especially High Reliability Organizations (HROs).

1.2 Background

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 dominate consideration, however in the nuclear industry it is a defining requirement, if the consequences of accidents cannot be held to have a small impact on society, then nuclear will not be successful in the long term. Another aspect that affects the nuclear power industry is the fear that the nuclear effects 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. These accidents have had an impact beyond their actual 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 accidents that were also the result of the earthquake/tsunami.

Long term pressure has been placed upon industry in general, by society, to improve the undesirable aspects of some processes, such as dealing with waste products, and undesirable airborne products, particulates and noxious gases. The cleanup has been proceeding for many years, including from stabilizing coal tips to the removal of sulphur dioxide (SO_2) from high sulphur fuel oil. These things imply a cost and society decides over a number of years that the cost of change can be accepted and is considered to be worthwhile, so that there can be a net improvement in the quality of life. Initially, most processes were open-loop, meaning that little or no attention was paid to dealing with extraction of minerals from the ground or how one was going to deal with the waste products stemming from a process. Early man did not worry about the impact of cutting down trees or burning them. The prime purpose was keeping warm and cooking food. The same was true of coal and later for processed materials like iron, copper, etc. Even today one can see the ancient remains of early iron smelting in various countries.

The discovery of nuclear energy has to rank with one of the great discoveries of the world and it ranks alongside with the discovery of fire by ancient man. In Greek mythology Prometheus recognized that fire had great potential, but at the same if not handled correctly would and did cause the deaths of many. Even now we have not totally conquered fire, but we have used it for many years, balancing risk with benefit. One wonders where we would be without it. Much the same holds for the use of nuclear power, its power has to be controlled. Fire is a chemical process involving burning carbon products in the presence of air. The power density of combustion is relatively low, however nuclear power has high power density and produces a lot of energy in a small space. This aspect is good, since it can yield high power while taking up little space. Unfortunately, like fire, there is a downside. Nuclear power ends by generating radioactive materials, which if they escape into the environment can cause the death of numbers of persons. So like fire, we need to handle nuclear energy carefully.

Like any new substance or material, we need to be cautious how it is used or employed. However, the joy of finding this new thing tended to overcome any caution that we might have had. Nuclear was introduced to the world through a program funded by the US and under President Eisenhower, called “Atoms for Peace.” This was a move to get countries to focus on the benefits of nuclear processes as useful source of energy and not just as a very powerful explosive or bomb. It appears that the proposition worked, but it did not stop

countries from developing Atomic bombs. Later in the thesis there is a detailed discussion of nuclear power and its development.

Like any new engineering process, our understanding of it develops with experience. Things do not necessarily work properly at first and have to be modified. Failures end up by leading to improvements in design, choice of materials and manufacturing processes. This picture is seen throughout the history of mankind. Ships capsize, locomotives blow up, wheels fracture, guns blow up and cars crash due to unknown causes, which are later found and fixed. In addition to material failures there have been errors made by individuals and systematic failures made by designers and decision-makers. In the early days of the industrial revolution failures were due to deficiencies in materials. The properties of iron, steel, copper, zinc and lead were not understood and the impact of impurities on strength, fatigue and corrosion was not known. Bit by bit, understanding of these things advanced and engineering correspondingly advanced. The journey to where we are now has been long and advances have been accompanied by accidents of one kind and another. Mostly, the loss of life has been relatively small and often did not involve the public, only the persons working with the machines. Later, as factories and transportation became more numerous and bigger, deaths resulting from industrial activities increased. Rules and laws were introduced to try to ensure that persons did not get hurt or killed as a result of industrial operations. Standards relating to industrial equipment and construction processes were introduced in an attempt minimize deaths and injuries.

This was the condition at about the time that nuclear power was introduced into submarines. Prior experience with nuclear processes was restricted to building simple piles of natural uranium together with a moderator in order to produce fuel for Plutonium bombs and large chemical facilities to improve the concentration of U_{235} from natural uranium (natural uranium is that distribution of uranium isotopes that exists in nature). The purpose of U_{235} was the same as plutonium, the construction of ‘Atomic’ bombs. It was quite clear that during the formation of plutonium by nuclear means that much useful heat is generated and could be used for the generation of electric power. After WWII, it was realized that nuclear power could be used in submarines and would turn them into true submarines that could operate for long periods of time without surfacing. The guiding person in this endeavor was Admiral Rickover. Most importantly, he attached great importance to the need to operate the nuclear powered submarines very safely and that the radiation effects should be taken seriously. In fact safe operations were essential. As a result of his measures in training and testing of personnel, ensuring submarine equipment met high quality standards and the whole thing being well coordinated led to the ‘Nuclear Navy’ having a very good safety record.

The civilian nuclear program was initiated and after much investigation in the US of alternative combinations of fuel, cladding, coolant and moderator were made for various reactor types. The industry focused mainly on water cooled reactors with uranium oxide fuel. A couple choices were made for cladding, i. e. stainless steel and zirconium. The preference was zirconium. Other countries preferred different combinations, such as natural uranium fuel in rods, Magnox alloy cladding, graphite moderator and CO_2 coolant. This was the initial choice of both UK and France. The first Nuclear Power Plant (NPP) was Calder Hall and was an outgrowth of the UK's nuclear bomb program and was a Magnox fuelled gas cooled reactor. The second commercial reactor was Shippingport (Pittsburgh) and was essentially a converted submarine reactor design of the Pressurized Water Reactor (PWR) type. More about the development of reactors is to seen in later chapters.

One issue that comes up in managing of any facility or industry is what is the best process for doing this? The current normal way is to have a hierarchical structure defined by an organizational chart with roles of each level being defined. Such a chart really does not define how the system should work. The result is how well the system works depends on the personality and character of the individuals at the various levels. In other words, the organization functions on pure chance, either the reflection the character of the Chief Executive Officer (CEO) and his associates, such Chief Financial Officer (CFO) and President, or just following the tradition of the company.

In the case of nuclear power plant operations, not only should they be run economically, but most importantly safely. In fact, one might consider safe operations the prime operational requirement. In capitalistic societies, failure to operate economically leads to the organization failing. For a nuclear power plant operation, it has to meet the normal capitalistic requirement, but also has to do this without leading to an increased risk of a nuclear accident/incident.

Different organizations participate in the activities of the plant. Each part of the organization has an impact on the plant operation. Also the design and construction of the plant, which involves the plant's designers, architectural and construction companies, has a strong impact on safety. Together all of these organizations influence either directly or indirectly the character of the accident. An accident may be due the result of an underlying design weakness, wrongly set operating rules, a decision related to poor training instructions and confusion related to emergency operating instructions. One thing that is quite apparent is there are different time scales for these activities from responses of control room staff responding to accidents to the decisions made by management in response to the need for plant upgrades and changes, even to what design of NPP should be selected. Figure 1.1

depicts the time scales for some of the different processes involved in nuclear power plant operations. These range from neutronic processes governing the generation of neutrons in the atomic reactions to the decisions of organizations including those of governments.

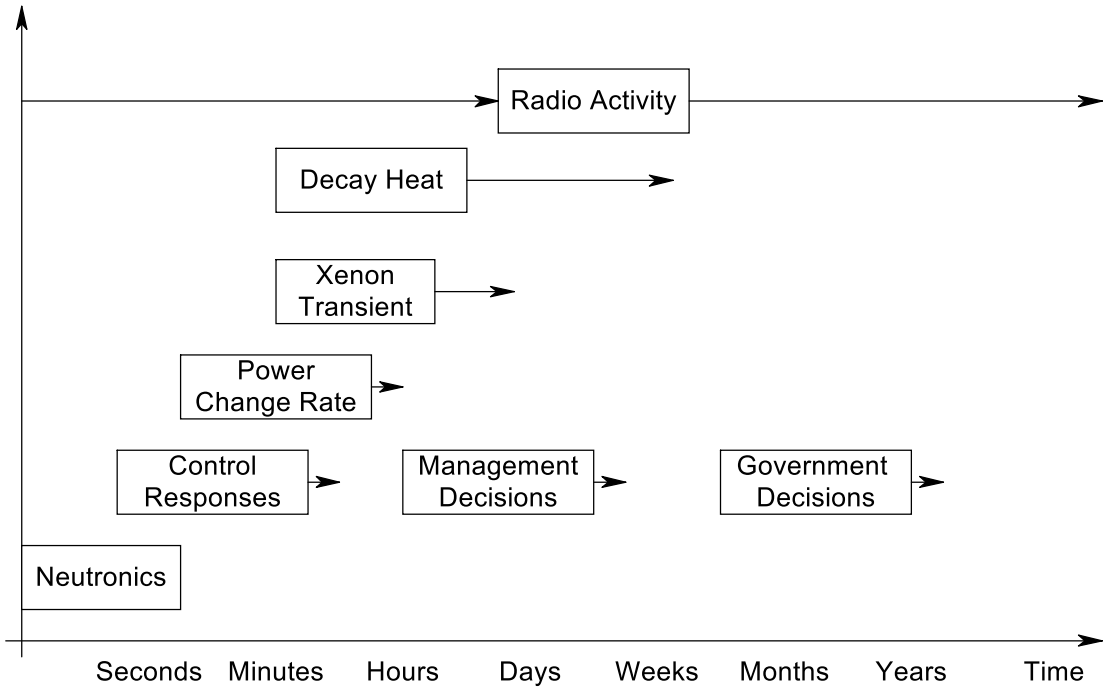

Figure 1.1 Time Scales for Different Processes associated with NPP Operations

All of the processes indicated above are associated with control features involving some degree of feedback for the purposes of control and stabilizing processes. The feedback may be as a result of using negative temperature feedbacks resulting from the design of the reactor internals to limit power excursions, to automatic controls used to manipulate neutron absorbers or change the flow of cooling water to the instituted controls of management and Governments to ensure safety. Clearly, each of the processes indicated in the Figure 1.1 have different time constants associated with them from very small time constants to very large ones, from micro-seconds to many days or months. The time scale of an activity can have an impact on the progress of an accident.

Many times one sees persons, like the control room operators, responding to an accident being held responsible for the accident, when the real responsibility rests with the plant management. One always hopes that the evaluation of the circumstances of the accident is taken to a deeper level than just the superficial causality of human error!

In the formalism of accident analyses and probabilistic risk assessments, the role of management is not usually explicitly identified. However, more and more it is seen that upper management can be identified as a partner in causing an accident, because of the decisions made prior to the accident. In the case of the Daiichi accident, clearly the tsunamis were the agents that led to damage to the plant, but it was the decisions of management that led to the plant being placed in a vulnerable state.

1.3 Consideration of Approaches to Model Organizational Performance

There appear a number of different ways that one could model organizations in order to evaluate the impact of management and personnel on the safety and economy of the operations. The method selected for this study is based upon the Viable Systems model (VSM) of Beer (1985). The advantage of this approach versus other methods is that deals with an organization in a dynamic manner in which elements within the organization react to each other, also VSM reflects both decision making and operations are distinct elements with communications linking the elements. Beer's use of an analog of the body which places importance on the decision-making role of the brain, identifies the upper management functioning in a similar manner for a company. This observation is confirmed by examination of the roles of managers and operators in the case of accidents.

The advantage of developing a VSM model of the plant management and operational structure to the dynamics of the NPP along with the rest of the influences affect plant safety and economics can show that NPP management has the central role in the goal of meeting NPP safety and controlling operational costs. A key aspect that Beer makes is related to the complexity and complication of the task that management has control. A manager has to control the variety in the job that he can deal with; this involves him/her making decisions to reduce the variety while still meeting the objectives of the company in both economics and safety. The success of the manager depends on making good decisions.

Other methods have been advanced as approaches to help in understanding the safety of NPP operations. A critique of these methods is given below. As can be appreciated, dealing with the safety of power plants is a complex business in that it deals with many overlapping areas, such as the reliability of operators taking actions, equipment reliability and how design features affect safety, the central role of management organization operating safely and in a cost effective manner, and to the impact of outside organizations on safety, the Nuclear Regulatory Commission (NRC) and economics, the Public Utility Commissions (PUCs).

The characteristics of equipment and humans have different attributes, but none the less they need to be factored into safety and economic studies. Initially, the emphasis was on the reliability of equipment to ensure plant safety. In time, it was realized to focus on just this aspect was insufficient and that humans played a critical part in ensuring plant safety. This understanding affected different industries in different ways. In the chemical and process industries for example, the Hazard approach gave way to include Hazan. Many engineers thought that the best way to deal with issues involving humans was to replace them with automatic processes. However, this does not seem to be as effective as was once thought and has given way to the attempt to better integrate humans and computer-based systems into the operation of power plants.

There exist a number of different approaches that attempt to cover the need to understand risks of operation. Some of these methods have existed for a while and others are currently being proposed. Some of the methods are: Hazard analysis (Kletz. 1999), Probabilistic Risk Assessments (PRAs) (Frank, 2008), Systems Theoretic Accident Model (STAMP) (Leveson, 2004) and its extension System Theoretic Systems Analysis (STPA) in (Leveson, 2011). All of the methods have some value in the process of trying to improve plant safety. The field in which they are applied has played a role in shaping their formulation. The methods go from being relatively simple to apply to quite complex.

In the early days of reactor design, the methods (1950s – 1970s) used for safety studies were mostly transient investigations of how plant responded to a variety of disturbances. Then analysts/engineers would draw conclusions about the safety of the system. Failures of system components and controls would be investigated to estimate what would be predicted to happen and whether or not other controls/mitigating systems should be added to terminate or mitigate the consequences of the accident. This approach led to the use of mathematical simulation techniques to model the various components of the plant. These models were built to study accident progression then the results were used to design of the systems to protect the plant. The central role of management decision-making in plant safety was not considered, by implication it was considered to be benign and the design would be operated as envisioned by the designers. This turned out to be a poor assumption, since the actual role and impact of both management and operators was not fully understood by the designers.

The above mentioned techniques were used to design the control systems, which were there to keep the plant operating within certain design parameters. Later, there were investigations to examine the interactions of operators with the controls. This was done to see there were interactions that could lead to problems and to examine areas where the

operators were expected to take over controlling the plant in the face of equipment failures. The Issue of limitations in the design of the NPPs and how operators function were to have strong impacts in the industry. The utility management is responsible for the NPP and its operation, so picking the chosen design of NPP and its details, together with the preparation of the NPP operators to run NPPs, rested with them.

The approach to safety was quite different in the nuclear and chemical industries. The nuclear industry was concerned about the consequences that could occur from a range of different equipment failures and what to do to prevent or mitigate their effect on core damage. This approach was deterministic and formed the basis of the regulation of the NPPs. The chemical industry looked at the hazards associated with the chemicals used in the process, and came up with a method called HAZOP analysis (Kletz, 1999) The design process used was to limit the size of the hazard and to limit its effect by the use of some limited containment, venting and sprays. The dynamic and interactive effects between elements within chemical factories did not seem to have been heavily investigated. Later, the role of humans was considered and the method developed into the HAZAN (Kletz, 1999) approach from the HAZOP formalism, which is based upon the use key words to perform the hazard analysis. Even in the nuclear field, a hazard analysis is carried out as a first step in a total risk assessment process, for example it was used in this manner in Yucca mountain repository safety study, DOE, (2009).

The HAZOP Analysis and HAZAN approach has been used in the Chemical Industry for some time, but considering the number of accidents that have taken place in last number of years; the approach does not seem to be very effective. Some recent accidents shows the limitation of this type of approach, the accidents were the fire accident at Texas City refinery, the explosion at Bhopal pesticide factory and the BP oil spill in the Gulf of Mexico; (Spurgin, 2009 and National Commission, 2011). It is not know whether the HAZOP analysis was applied in all of the cases, but it is doubtful whether it would have made a difference, since one of the main influences in these cases was the attitude of management to various aspects of the operations. For example, in the case of Texas City Refinery, it was associated with the basic design weakness compounded with the lack of foresight in allowing trailers in what should have been an exclusion zone. In addition, there was a lack of operator training. All of these issues fall at the feet of management, hence it is unlikely that the HAZARD method would help advance the safety of these operations. One would be looking for a different approach than performing a HAZARD evaluation. It might have helped in the case of Bhopal in pointing out the consequence of a large release of Methyl Isocyanate (MIC) on the population around the plant, which should have made the management organizations more concerned to protect the local population.

It appears that a weakness of the HAZOP approach is that it does not deal adequately with coupled systems, in that a fault in a particular sub-system could affect another sub-system and have a cascading effect throughout the whole plant. Thus a failure to operate a valve correctly could lead to overfilling a tank and this led to a dump system being used. It had a limited capacity. The petroleum product being dumped was released through a safety valve, caught fire and ended up causing the deaths of a number of staff members. This is a short description of the Texas City refinery fire (Spurgin, 2009). The staff of the refinery knew of the hazard, but had no idea how the accident could progress, since the assumption the hazard would be contained by the operation of a safety dump system, but unfortunately the dump had a very limited volume and did not prevent the release

It became apparent in the mid 1960s that the risks from different accidents were not the same; some accidents were more likely than others. Also, society in various countries around world did not have a good measure of the safety of NPPs and had reason to believe that they were equivalent to bombs. The public still has some degree of uncertainty with the safety of NPPs, especially after accidents have occurred, like the Fukushima accident.

The nuclear industry started move away from the concept of the maximum credible accident some while ago and to consider that the risk from different accidents. Accidents with the greatest consequences should have the lowest probability of occurrence and safety systems should be designed accordingly. F. R (Reg.) Farmer (1914 to 2001) led the way into considerations of examining NPP safety from a probabilistic view point with the 'Farmer Curve', a linear decreasing curve of log (accident probability) versus log (consequence). This curve of thought to be a measure of public acceptability of risk and led to the development of Probabilistic Risk Assessment (PRA) and Probabilistic Safety Assessment (PSA) based methods. In some ways this move could be seen as a shift from the failure modes and effects analyses (FMEAs) qualitative analysis to a more quantitative analysis of risk.

The NRC started by looking methods used in the field of equipment reliability and in particular at the work done by NASA based on the use of fault trees (FTs). This approach led to failure probability of systems, so the predicted failure of the rocket system could be predicted as failure following a number of launches, if the failure of a series of components that made up the system could be predicted. Some reliability data was available, because of prior component reliability studies. However, the NRC team was looking for relationships between initiating events, the consequence of that event occurring and also how the probability of could change if other events occurred. The team came up with the event tree (ET) concept that is the basis for the Probabilistic Risk Assessment (PRA) method. These

methods, FTs and ETs became the basis for the work carried out by the NRC into the risks of nuclear power and is contained in the WASH 1400 report (NRC, 1975) on light water reactors (both PWRs and BWRs). Completed at the same time was a similar study performed by General Atomics on the risk of operation of high temperature gas reactors (HTGRs), this was called the Accident Initiation and Progression Assessment (AIPA) report (Fleming, 1975).

The NRC quickly understood that they needed to involve the role of humans within the PRA. They turned to A. D. Swain to apply the approach he and others had developed for examining the safety of assembling atomic bombs. He developed a human reliability assessment (HRA) hand book, based upon his work (Swain, 1973), and this was the method used in WASH 1400.

NRC uses PRAs in the study of plant safety and has encouraged utilities for some time to do the same. However, this does not mean that safety evaluations are limited to the use of PRAs. Their approach is more holistic and involves other measures of safety evaluation. Their approach is called 'risk informed', not just PRA related.

Leveson's book (Leveson, 2011) is very interesting and her approaches (STAMP and STPA) are more qualitative than PRA studies. Her background is in controls and aeronautics. In a way, her thinking is related to that of Beer, in that control systems or cybernetics play a part of the characterization of the whole system. She is also influenced in her thinking about the increasing role of computers in many applications. This she sees as a complication presenting increased complexity in the field of safety. Recently one has to be concerned not only with hardware and humans, but also computer software reliability and interactions between computers and humans.

Leveson is not particularly enthusiastic about the PRA process, believing it has a number of short comings. Below is a list of short comings along with her view and a response to those views. A number of her views need to be answered since it puts PRA in poor light. It should be pointed out that the quality of a PRA depends very heavily on the experience and knowledge of the persons carrying out the studies.

Item	Leveson view	Reason	Rebuttal
Initiating events	PRAs take these as independent events	Many events have dependences and this a failure of PRAs not to take this into account	When initiating events have dependent effects, these are taken into account
PRAs model accidents as linked events; initiating events, equipment failures, human errors leading to consequences	This is too simple a view of an accident	Study of accidents belie this model, it is much more complex	Prior to performing a prediction of events, most persons carry out an event sequence diagram (ESD)* to judge the interactions and assess their importance. Analysts then decide what sequence is important
HRA data	Based upon prior historical data which is insufficient	HRA models are not adequately modeled in PRAs. Cognitive processes not modeled and need to be considered	Most HRA methods are subject to Leveson's criticism. A HRA method** proposed as part of INPP process would cover this concern
Design shortcomings	Design issues are not considered in safety studies	Points to design issues like TMI PORV failure. Need to address these failures in a non-probabilistic manner	She is correct in that in detail plant evaluations have not necessarily pointed out these issues, however accidents have identified these types of failure. Review of ESD details could point out areas of concern
PRAs do not cover software failures	PRA methods cannot predict software failures	Current designs depend on computer-based systems to control and protect plant	Software is more like HRA than hardware reliability, work is going on to help determine how software can be incorporated into PRAs
Accidents thought to be due to operators present a problem in determining who or what is the cause	PRAs use data which does not reveal the real cause of accidents	Back tracking actions taken by operators difficult to determine real source of errors	HRA method** does indicate the source of potential errors due to design, training, etc

Table 1-1: Responses to Leveson's Critique of PRAs

Notes:

* For information about the use of ESD, see Spurgin, 2009, chapter 8

** For information about influences on operator error, see chapter 5 and figure 5.2. The process considers both random and systematic errors

Many of Leveson's objections are agreed to and some of them were already incorporated in later PRA applications and latest evolution in HRA methods. So some of her issues have been taken care of, but unfortunately in the general application of PRAs by current so-called experts, some of these issues are not considered. The approach taken here in the application of VSM into the integrated NPP (INPP) model takes into consideration her

comments about PRAs/HRAs, since they are similar to those of the researcher. However, it is felt that risk assessment methods have a key role in addressing safety of NPPs provided that these limitations are accounted for.

Although HAZOP and HAZAN have been used in the chemical industry, current investigations into the safety of NPPs has proceeded beyond the need to just identify the existence of hazards and therefore a role for using these techniques in INPP is not seen. As to the use of Leveson's methods, these are useful, but the application of improved PRA thinking related to quantified risk considerations offers more in assisting managers in balancing costs versus enhanced NPP safety. Her comments about design and human issues need to be considered by PRA practitioners to ensure their quantified conclusions are valid.

The preferred approach, to be used as part of the Integrated Nuclear Power Plant (INPP) method, is based upon using an improved version of PRA built upon a base of investigations using event sequence diagrams to examine how accidents can progress via different failure (both human and equipment) routes to consequences from core damage to equipment damage to no effect. The impact of managerial decision-making will be taken into account based upon the selection of external disturbances (size and frequency), and human reliability contributions because of staffing, training and other considerations.

Looking at how organizations operate, is seems that a better way is to follow the precepts of cybernetics, which is based upon the concepts and ideas of the control and organization of animal bodies. For effective control, animals have evolved not only central control of the animal via the brain, but have also developed autonomic behavior of individual components of the body, such as the liver. Part and parcel of the body is the nervous systems, which carries information to and from the various parts of the body. Feedback from components of the body is important, since without this information the body could not function effectively, for example if you never felt hungry, would you eat? The stomach sends the information to brain to reveal its state and then it becomes a survival process to find something to eat. The planning function of brain sees the future need for food, based on the experience of the past. In this squirrels decide to find and store nuts. A cybernetic model has a central control as well as distributed control centers tied together by communications covering instructions to take certain actions as well as sending information back to the central control unit.

Beer (1985) became interested in the application of cybernetic principles to management of industrial processes. He developed an approach called Viable Systems Model (VSM) built upon these principles. He saw a company as a living growing viable entity. Of course, the company and an animal do not match one to one, but the idea of the upper managers being

the equivalent of the brain, and middle managers being equivalent local controls of animal components and the local components themselves equivalent to persons producing products, such as shoes. Communications between the various body parts are matched by communications between the various levels within the manufacturing company. This interpretation of a living company is so much more dynamic and adaptive than the concept of a static hierarchical model of a company. There are several areas of importance in this model of how an organizational is managed and controlled. These areas are, as follows, in no particular order of importance:

1. Information is transmitted in both directions, from managers to operators and vice versa
2. Individual production units can be operated efficiently without close control from top management
3. Top management is responsible for developing rules for controlling production rates and the direction of the company
4. Every layer is responsible for its operation within the rules set up by top management
5. Coordination of operations is required to ensure economic health of the company
6. State of the company is the integral of the health of each component part
7. Monitoring and appropriate filtering of information is required to enhance the health of the company, top management needs to understand attitude and requirements of operators to ensure production is kept to a high level without breaks in production due to both equipment faults and human actions

The VSM approach has been applied successfully in a number of industries and offers much in terms of a flexible and adaptive system of improving management of industry.

1.4 Objective of Research

The objective of the research is to apply the VSM method to nuclear power plant management and organization to cover both safety and economic decisions that affect nuclear power plants (NPPs). VSM has been applied to normal economic operations, but has not been applied to the management of organizations deeply involved with safety of the public. The research covered here extends the VSM approach to consideration of NPP safety. Research is expanded to show how experience gained by the industry, via accidents, are reflected in changes in the utility industry. In essence, this can be seen as growing change in the awareness of the actual variety of the utility organizations and the

need to match the requisite variety (Ashby, 1973) of the NPP operations to achieve the economic and safety objectives of the industry.

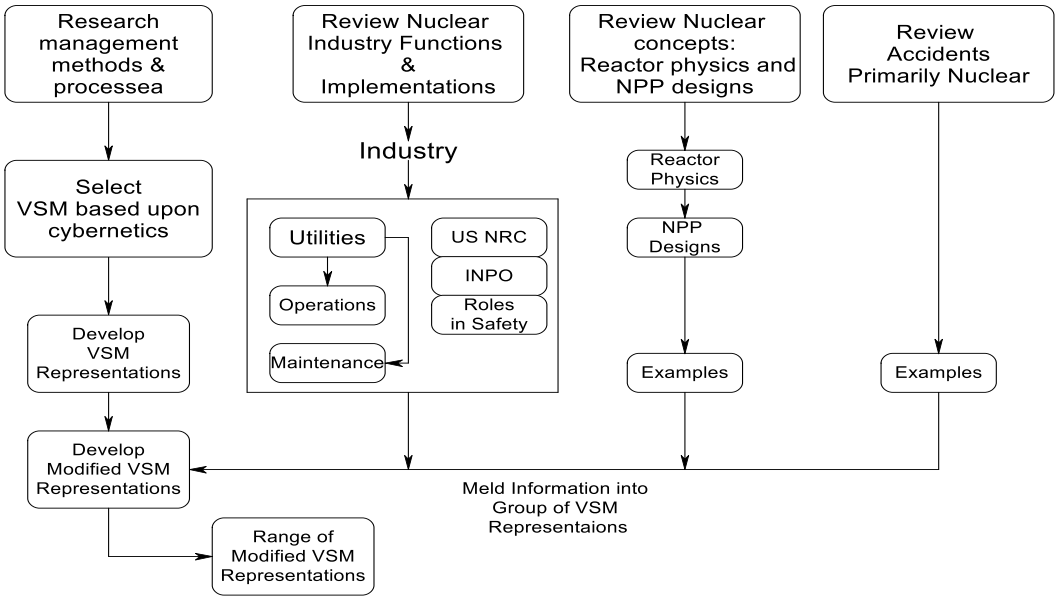

Figure 1.2 Diagram showing Research Areas covered

Figure 1.2 shows the extent of the research. The research covers four main areas, these are: Research into management methods and processes, A review of how the Nuclear Industry Functions, Development of a background into Nuclear Power Plant (NPP) designs based upon a knowledge of reactor physics, and a review of NPP and other accidents to help in the formulation of VSM upgrades reflecting the changes occurring within the nuclear industry over the last number of years.

In order to achieve the prime objective of the research, a series of sub-objectives have been selected; there are four main research components to help fulfill the prime objective, namely a study of the VSM approach to management, an in-depth review of the nuclear industry and how all the pieces function with the objective of constructing VSM versions to not only represent the current state of nuclear industry but also how it has changed over the years, a study of the underlying reactor physics and how it has influenced the design of nuclear power plants (NPPs) and the congruent safety requirements for operating plants, and a study of accidents that have affected both the design of NPPs and manner they are operated. All of these sub-areas of the research factor into the achievement of the prime objective of upgrading VSM to cover safety aspects, but also how changes that have occurred in the industry are reflected in changes to the VSM and how the features of VSM are integrated to reflect these changes.

The research into VSM approach was accompanied by a study of cybernetics, in order to achieve a better understanding of the underlying ideas that led to the formulation of VSM and its principles, so that the modifications stemming from safety considerations would be approached within the VSM/cybernetic framework. An important part of this research was gaining an appreciation of Ashby's concept of Request Variety and how failing to match it can lead to inadequate control over processes.

Although the author has been associated with the nuclear power industry for a number of years, research into the nuclear industry was undertaken to better clarify many issues that have changed over the years with regard to licensing of NPPs, the evolution of the need for the Institute of Nuclear Power Operations (INPO), together with a formalization of NPP management changes that have occurred in response to NRC requirements along with a better understanding of NPP operations and maintenance.

The objective of researching reactor physics and its impact on plant designs is to layout, in a fairly concise way, steps that the industry took over time to develop and select the current set of NPP designs. The safety of NPPs is a function of both the plant design, the quality of the equipment and how the plant is run and maintained. The management function is a key part in the safety and economic running of NPP, but the day to day operation of the plant has to take into consideration the physical plant itself and compensate for possible design limitations that may impact safety. Since the object is to examine the connection of management to safety, one must also consider design aspects, hence this sub research objective.

A strong influence on the industry that has led to both design and operational improvements has been the number of accidents that have occurred over the years. Not all of the accidents have been that influential, but there have been a number that have had a large effect. The objective of this research is to examine a number of accidents and determine how management and personnel decisions have affected the accident progression from before, during and afterwards. This information folds into a deeper understanding of how management fits into VSM, especially long and short terms effects need to be factored into modifications of VSM features to encompass safety. The lessons from accidents have occurred over a number of years, so certain changes in safety awareness also change and these lead to different modifications to VSM. So one of the outcomes of the research are changes in VSM realization towards a more stable form as the impact of accidents is reduced by actions taken by the industry to improve plant safety.

1.5 Outline of the Research

Research here covers the impact of management decisions on the safety of NPPs. Often approaches like Probabilistic Risk Assessment techniques are used to examine the impact of management decisions, but this is when they occur with other failures. Here the objective was to examine the management structure and processes in order to define more clearly the impact of management decision-making on the safety of NPPs. The VSM organizational structure and processes were considered as a start on which to carry out the research.

Research into Nuclear Supply Systems (NSS) management processes and the impact of accidents on how the industry was organized were carried out. This research was undertaken to enable how VSM could be cover both economic and safety aspects associated with control of NPPs production and ensuring its safe operations. These investigations provided a good basis for research into how a Viable Systems Model could be progressively changed to reflect the impact of these industrial accidents on management processes.

A key part of Beer's approach is his coverage of variety as related to management control of organizations and the implications of meeting Ashby's Law of Requisite variety. It appears that the processes by which managers "destroy Variety" (Beer, 1985) do not take into account the need to identify such variety that is needed (Requisite) to ensure effective control of the process. This situation is confirmed by examining various accidents, see Chapter 5. The thesis is concerned with identifying the decisions taken by managers, so one realizes what has been neglected and in the right circumstance can lead to an accident. One can appreciate that not selecting the requisite variety may not lead always to a bad situation. For many years the Tepco NPP managers did not suffer the consequence of not determining the requisite variety, because variety did not cover, at the time, the actuality of a large tsunami, see Chapter 5 for details on the tsunami induced accident.

1.6 Brief Statement of the Thesis

The thesis consists of eight chapters, as listed below:

1. Chapter 1 Introduction
2. Chapter 2 Fundamentals of Nuclear Power Generation
3. Chapter 3 Plant Operation and Safety Considerations
4. Chapter 4 The Viable Systems Model (VSM)
5. Chapter 5 Case Histories
6. Chapter 6 Experience in applying VSM to the Nuclear Industry
7. Chapter 7 Findings
8. Chapter 8 Contributions, Recommendations and Future Work

Chapter 1: Introduction

This chapter covers introductory material about the thesis.

Chapter 2: Fundamentals of Nuclear Power Generation

The fundamentals behind the generation of electric power based upon the nuclear fission process are introduced in this chapter. It starts will an explanation of atomic or nuclear reactions, how the reactions are controlled including the effects of moderating materials on the speed of neutrons. A discussion of criticality and how it affects the design of nuclear reactors is included in this chapter. To convert the energy released during a fission process, one needs to consider both the heat transport capability of a coolant and its impact on nuclear fission efficiency.

The fission process leads to the production of neutrons, generation of heat and also other atomic substances. These latter substances are a series of elements, particles, and radiation. Many of the elements are unstable and in decaying from one state to another do so with a variable delay time or half life. They also change state and in the process yielding heat, particles and radiation. Once a nuclear reaction is shutdown by the insertion of neutron absorbers, the energy given off by unstable elements continues. This energy is called decay heat, since comes from the unstable elements releasing heat as they decay.

This chapter then goes on the discuss how all of these aspects, fission efficiency, choice of coolant and countering the effects of radiation have lead to the design of various types of nuclear power plants (NPPs). Over time, the variety of different types of NPPs has reduced and probably still reducing, as some features are seen as being more effective than others. Selection of the prime NPP designs is a combination of economics and safety considerations. For example, sodium is an excellent coolant, but is difficult to work with when one ties it to standard heat exchangers with water on the outside with leaks developing, which can lead to hydrogen explosions!

The chapter then goes on to cover the design aspects of typical NPPs. The types of NPPs covered are Pressurized Water Reactors (PWRs), and Boiling Water Reactors (BWRs). These are the most numerous of reactor types. There are other types, such as the advanced gas cooled reactors of the UK, the CANDU reactors (Canada) and RMBK's and VVERs (Russia). Other reactor designs continue to be looked at, such as High Temperature Gas Reactors (US). The main focus of this chapter is on the PWR and BWR designs. The Russians, in addition to the RMBK design which is phased out, developed a PWR design called the VVER, which is very similar to the original Shippingport PWR design in that

horizontal steam generators are used, as opposed to the vertical steam generators of current PWR designs.

Chapter 3 Plant Operations and Safety Considerations

Safe operation of NPPs is a prime consideration in the use of NPPs for power generation. This chapter discusses what safety means in terms of safe operation. The safe operation of NPPs depends on having good basic designs that are developed with safety in mind, which reflects upon the concepts of prevention, mitigation and containment of radiation releases following accidents. In addition, the operation of NPPs has to focus on ensuring the reliability of equipment coupled with both redundancy and diversity of the equipment to minimize the possibility of an accident. The operational staff must be well trained to both minimize the occurrence of accidents but know how to control the effects of the accident.

This chapter discusses how attitudes have changed as a result of accidents that have occurred over time. These attitudes have then been translated into to development in safety philosophy, which in turns has led to how NPPs operated and designed. Specific certain accidents have had a greater impact than others. One accident has had a large impact on the NPP industry and that is the Three Mile Island accident that occurred March 1979. The chapter will discuss a number accidents and their impact.

The regulatory process via the Nuclear Regulatory Commission (NRC) and that of the NPP industry organization known as the Institute for Nuclear Plant Operations (INPO) has a strong influence on the industry and this is discussed in the chapter. Ultimately, the objective of examining the safety record of the industry is to track the changes that have occurred and then relate them to organization aspects that have take place.

Chapter 4 The Viable Systems Model (VSM)

The Viable Systems Model (VSM) is a key element in the thesis and central issue of the thesis is the extension of VSM to cover safety aspects of NPP operation and further more how the underlying characteristics of VSM are modified to reflect changes occurring to the industry as result of responding to lessons learned from accidents.

This chapter goes into a detailed discussion of VSM and its relationship to cybernetics and its application to the organization of companies, including layers of management and operators as far as control and information flow are concerned. It is appreciated that management has to deal with the complexities of operating NPPs in both economical and safely. This entails making decisions on what aspects need to be closely controlled and monitored and those aspects that can be referred to others, i.e. controlling the variety of the

processes. It is pointed out in this chapter that the key to management reducing the variety in the NPP processes while still achieving its goals is the need to ensure that Ashby's Requisite Variety is met. More of this is discussed in this chapter.

The chapter also covers a VSM application to air traffic control over Saudi Arabia air space; this is the work of Dr. S. H. Al-Ghamdi (2010).

Chapter 5 Case Histories

This chapter discusses in detail a number of nuclear accidents in detail, including the influential TMI accident. This part of the study is very important in terms of looking at the decision processes that go on before, during and after accidents. This chapter provides the substance upon which to base how management works in guiding and control others within the organization. Management directs the budget allocation, numbers of maintenance personnel, assessment of both middle and lower managers, training of operational personnel, etc. The accident analyses confirm the importance of management, furthermore the impact of Government can be very important in controlling how an accident might affect the general population and its radiation effects spread.

Chapter 6 Experience in applying VSM to the Nuclear Industry

This chapter builds upon prior chapters. A thesis objective is to incorporate changes in VSM to account for not only economic controls but also safety controls. The VSM structure and cybernetics are concerned with the central role of management to control processes via informational channels, which give feedback to central controlling processes to inform it of changes in both the environment and the impact of changes affecting lower management functions and operations.

In normal commercial operations market forces condition how management react. Failure of management to act can lead to failure to respond to changes and ultimately the failure of the company. However, for NPP management failure to prevent an accident also can lead to the public being harmed, as well as the shutting down of not only the individual NPP, but might have a wider effect on the whole Nuclear Utility Industry. This raises the implication of management failure from a local effect to a nationwide impact.

The implication of management actions in reducing variety to a manageable degree, can lead to the situation that the requite variety for control over the processes is not met and this can lead to an incident or accident. Initiating events can change the variety seen during normal operations and if the requisite variety, appropriate to this plant state, is not

understood and considered, could result in an accident or incident. This is covered in this Chapter.

The modification of the VSM to cover the above safety considerations are discussed in this chapter. Furthermore the changes that have occurred in the Nuclear Industry are reflected in changes in VSM, depicting how the impact of accidents can affect basic management/operators/environment inter-relationships.

Chapter 7 Findings

This Chapter covers the prime and secondary findings of the research work, as well as summarizes the work covered in each Chapter. The primary findings are associated with VSM application to the organizational structures of nuclear power utilities and how they have changed over time and affected by accidents that have occurred. A finding is the reinforcement of the VSM representation of the role of top management in controlling the safety and economics of NPPs and HROs. This mirrors the role of the brain vis a vis the rest of the body. This representation was central to Beer's body analog of industrial organizations. Both the analysis of the accidents and the limited evaluation of the NRC's ROP data confirmed the central role of management.

A key finding is the significance of Ashby's Requisite Variety to an understanding of how management decisions, related to encompassing control over the safety and economic aspects of running a utility, are recognized. If during the process of managing the organization, the managers do not cover the requisite variety, then the probability of an accident increases and maybe unavoidable. Later, in the future Research recommendations area, a deep study of the requirements to define requisite variety is recommended.

The secondary findings are associated with improvements in risk assessment techniques, such as Probabilistic Risk Assessment (PRA). One of the principle findings is associated with the integration of utility organizations, plant dynamics, internal and external disturbances affecting the plant along with influence of regulatory rules (NRC) and advice and assistance of an industry organization (INPO) for the purpose of safety and economic risk assessment.

Chapter 8 Contributions, Recommendations and Future Work

Chapter 8 covers what are considered the contributions that the investigator has made to extensions to the VSM approach covering modeling utility organizations in the fields of

safety and economics. The impact of accidents on utility organizations over time are considered and also immediately the effect on organization following an accident. The integral approach to combining VSM along with other effects is a key contribution and can help management visualize the effect of their decisions on both the safety and economic health of the utility.

The chapter also covers recommendations for further work and additional training and experience for top utility managers and persons who represent the share holders on utility Boards of Governors/Trustees. An important recommendation is to carryout research into how to predict Ashby's Requisite Variety for situations, so that safety of HROs can be better implemented. Study of accidents reveals situations in which the requisite variety was identified after the event. Often it is obvious what things needed to be identified and controlled, but only after the accident has happened. There is a need for an identification process to reveal what is important to identify and control.

Also recommended are improvements to be made to the analysis portion of the NRCs ROP program. The data has revealed that causes are due to a number of causes: not having the right procedures, need to determine the safety class of components, ensure that waste materials be removed and not lead to the failure of critical components, etc. These are not random acts of individuals, but rather a failure of decision-makers to make decisions and act, i.e. management functions. It would good to find out how these things come about and in whose domain they fall and was it due to money shortages or other reasons.

Also covered in this chapter are three papers written during the last phases of the research. Two papers were given at conferences and one paper was including in a reviewed international journal.

CHAPTER 2

2 Fundamentals of Nuclear Power Generation

2.1 Introduction

The objective of this Chapter is to introduce nuclear concepts and how various nuclear power plant (NPP) designs operate and their safety systems. The dissertation is an examination of how NPPs are operated and managed seen through the eye glass of Viable Systems Model (VSM). The Chapter is divided into two sections, the first deals with fundamental nuclear reactor concepts, which affect the design and operation of nuclear power plants, and the second part goes into details about the various NPP designs that have evolved over time and their safety characteristics. In a later chapter, the various organizations responsible for running the industry are described and how they have evolved over time. However, in order to understand how all of these things relate, some details about reactor dynamics have to be considered. The following topics are discussed, as an attempt to provide this background:

1. Fission process involving neutron impacting the uranium atom
2. Cascade process and criticality
3. Effect of moderation on neutron capture probabilities
4. Fast and thermal reactors
5. Choice of moderator materials
6. Nuclear fuel
7. Fuel cladding requirements and different cladding materials
8. Enrichment, what it is and why is it important
9. Heat removal fluids and their characteristics
10. Fuel element design
11. Neutron economy and reactor designs
12. Neutron control materials and methods
13. Different reactor types and their advantages and disadvantages

As can be seen from the above list, nuclear power is not an easy topic to understand. A good coverage of Nuclear Reactor Engineering is given in Glasstone and Sesonske, 1955, 1963, that is far more detailed than that covered here. There are items dealing with reactor physics, there are questions related to the choice of materials that relate to material properties that have to be considered from mechanical, chemical, heat transfer and physics points of view. Balances have to be made; the selection of one material may be good from a physics point of view but not from other points of view. Some of these

issues will be covered since they impact on choice of reactor designs and on the safety aspects of a specific reactor design. Each choice of material, be it fuel, heat transfer fluids, moderator and fuel cladding, is looked at from the following points of view:

1. What are its nuclear characteristics?
2. What are its thermal characteristics?
3. How is it affected by radiation?
4. How is it affected by high temperatures?
5. Does it absorb neutrons?
6. How expensive is it to machine/use and does it present a safety hazard?

The list goes on, initially, reactor piles were constructed to transform natural uranium into plutonium for the purposes of constructing 'atomic bombs'.

2.2 Reactor Physics

The objective of this section is to give sufficient information to understand how nuclear reactors function and how reactor physics bounds the design and what are the limitations associated with reactor design from a selection of materials point of view. The optimizing of any given design basically relates to cost and safety, one wants to limit the cost of the materials and the total cost of the design, so compromises have to be made. For example, there is a relationship of the size of the reactor and the degree of enrichment of the fuel. This aspect will be discussed. It is not the objective this chapter to provide a manual to design a reactor, but to provide sufficient information about how reactors work and key features which can affect both cost and safety. This chapter provides the background for chapter 3, which deals with reactor safety.

2.2.1 History

The study of reactor physics history is required to be able to understand the field of nuclear reactors and how they work. Atom physics was an old concept dating back to the Greek philosophy, but became more real following the work of Mme Curie on radium and radiation, J.J. Thompson with the discovery of the electron, Rutherford's work on particles and Chadwick's discovery of the neutron in 1932. Using a neutron to bombard an atom was really to see if one could generate heavier atoms. The concept of using a neutron to bombard a uranium atom was following along this path. It turned out that the atom actually could be split was discovered by Meitner, Hahn and Strassmann in Germany in 1938. Hahn and Strassmann performed experiments in Germany; while Lisa Meitner had fled to Sweden from Germany (she was Jewish). Hahn and Strassmann detected the presence

of stable Boron after neutron bombardment. Meitner and Frisch determined that the presence of Boron led them to the conclusion that the Uranium atom had been split! This was the beginning of the atomic age!

It was detected that in splitting the uranium, an average of three neutrons were released along with the release of energy and other atoms. This meant that it was possible to have a cascade process, in which the number of neutrons released could grow. Later experiments by Enrico Fermi and Leo Szilard (1939-40) (see Byers in Cronin, 2004) indicated that approximately three neutrons were produced that lead to the possibility of a cascade process in which the neutron population could increase.

This process was seen to be such that the energy released could lead to an explosion and a big explosion at that! It appeared that on splitting, the Uranium atom divided into nominally two equal atoms and released three neutrons, see Figure 2.1. Here the two atoms shown are Kr92 and Ba141 (Krypton and Boron). In fact there are a series of elements that the Uranium can split into, but the combination is roughly two, depending on their atomic number.

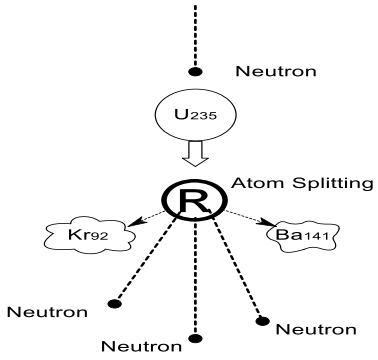

Figure 2.1 Splitting of Uranium Atom (U235) (after en.wikipedia.org figure)

2.2.2 Nuclear Cascade

Figure 2.2 shows a symbolic cascade array. One can see that the consequence of this is that the 'cloud' of neutrons grows exponentially. In the case of a bomb, the energy released quickly causes the bomb material to blow apart and terminates the cascade process, hence the need to keep the critical mass together for as long as possible. Here we are not interested in the bomb and its dynamics. We are interested in the cascade process as far as the nuclear power is concerned. The Uranium isotope of interest in the Meitner/Hahn experiments was based upon U235. It should be pointed out that U238

bombarded with neutrons is converted to Plutonium PU239. Both U235 and PU239 were used as atomic bomb materials in WWII against Japan.

2.2.3 Reactor, Enrichment and Moderation

In building a reactor, one is interested in the controlling the cascade process to produce heat. Here one should introduce the idea of enrichment and natural uranium. Natural uranium is that uranium dug up in nature without performing any operations beyond refining the ore to produce the basic metal. Uranium exists in nature as two isotopes, U238 and U235. However, the percentage of U235 existing in natural uranium is very small, 0.7%. As seen from the Meitner/Hahn experiments, the cascade process occurs with U235 not U238. So it is use of U235 that is central to the development of a nuclear reactor.

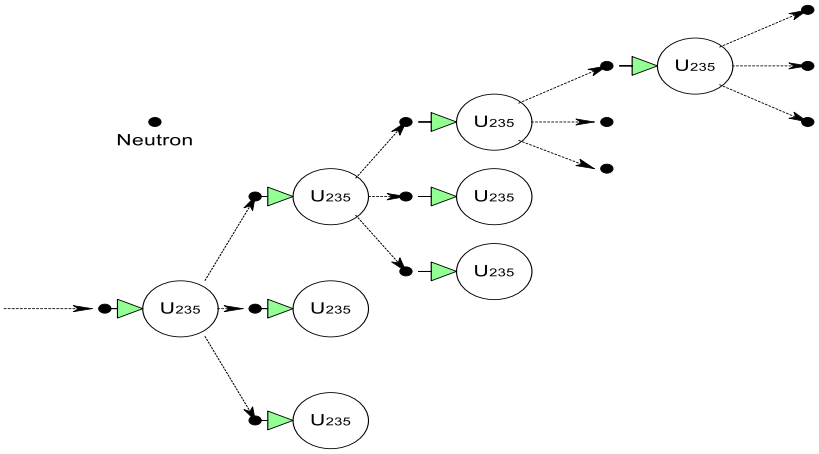

Figure 2.2 Neutron Cascade in a Multiplying Media

One issue is the start of the cascade process, if one has to wait for the random neutron to start the process of doubling the numbers of neutron, one may have to wait some time. To avoid this problem in a reactor, a neutron source is included to start the cascade going from an initially higher starting point. A mixture of Americium (Am) and Beryllium (Be) is often used as a starter source term.

A nuclear reactor is a device designed to contain uranium in such a manner as to promote the reactions between uranium and similar materials and neutrons. Typically, uranium is in the form of rods or plates covered in cladding material distributed in regular matrices and surrounded by a moderating medium. Heat is removed from the generated energy by a fluid. In some designs the moderating medium is also the heat transport fluid.

It has been found that the neutron capture probability of U235 is a function of the energy of neutron. The manner that energy level of neutrons can be reduced is to pass them through a material that slows them done without capturing them in the process. It is like a billiard ball bouncing off a series of balls, which redirects the direction of the ball and slows it down. Several materials have this property, like Graphite (Carbon, C), Heavy water (D2O) and water (H2O). This action is called moderation and the materials are called moderators, i.e. they moderate the speed of the neutrons! Moderators consist of light atomic elements that can slow down neutrons and have a low probability of absorbing neutrons, i.e. are transparent as far as neutrons are concerned. The idea is to slow the neutron speed so as to increase the probability of capture by uranium atoms. Reactors are classified as either fast or thermal reactors corresponding to the speeds of the neutrons at the time of capture, i.e. fast is the speed of the neutron at immediate formation and thermal where the neutron speed corresponds to speeds under thermal conditions.

2.2.4 Reactor Poisons

Given that a cascade process is undertaken and the neutron density within the reactor is increasing, control of the process is accomplished by the introduction of neutron absorbers. This can control the numbers of neutrons produced and the corresponding heat released. Certain materials absorb neutrons very effectively, these materials are called poisons. Boron (B5), for example, is such a poison and there others. To control the nuclear reaction rate, (rate of production of new neutrons), rods made from steel with boron (B5) added are used as control rods. To safely shutdown a reactor, shutdown rods (with higher concentration of boron) or if liquid solutions are used, then boron is dissolved in the liquid (water). Other materials can absorb neutrons while performing structural tasks or heat removal tasks. The choice of some of these materials is necessary to be able to construct a viable reactor. The efficiency of a reactor from a nuclear point of view is to be able to use the available generation of neutrons as effectively as possible, this is particularly true for natural uranium reactors, such as the UK's Magnox reactors and the Canadian CANDU reactors.

2.2.5 Reactor piles/assemblies

As mentioned above, reactors consist of assemblies of uranium fuel immersed in a moderating medium with nuclear reactions started by a source term. In such arrays, neutrons are born; propagate to cause more neutrons to appear, but some get absorbed, and some escape from the environs (outside the reactor vessel). If the numbers of neutrons are stable, i.e. the births equal the deaths, then the reactor is said to be critical. If the number is increasing then the reactor is said to super-critical and decaying it is sub-

critical. In the design of a reactor one wants to be able to control the nuclear density level, since this determines the output power of the reactor. Each fission can releases a certain amount of energy. The sum total of the fissions determines the energy output from the reactor. Reactor physicists developed the following equation to cover the neutron reactions:

The rate of neutron neutrons per volume = the rate of neutron production from fissions per volume – the loss of neutrons per volume

t = Production – Leakage – Absorption ------equation 2.1

Production is dependent on the distribution of neutrons, the higher the number of neutrons then the higher the reaction rate. For a given reactor, there is a distribution of neutrons over the space, with a higher number of neutrons in the center of the reactor versus the outside of the reactor. This distribution is known as the neutron flux. Now neutrons can escape from the reactor and can be absorbed by the materials used to construct the reactor or core. Some of the products of the fission process are also absorbers, such as Xenon and others in their decay process release neutrons, which are called decay neutrons. Also the ability of the moderator may be affected its temperature. Changing the density of the moderator could affect the capture probabilities either way depending on the design of the reactor. This leads to a positive or negative moderator coefficient. The US Nuclear Regulator requires the coefficient to be negative, if the heat goes up the power goes down.

Many reactors are controlled by the removal and insertion of boron steel rods into the core of the reactor. This is the control of absorption rate of the neutrons, and with the rods removed from the core the neutron level increases. Once it gets to a suitable level, the rods are inserted and continually adjusted to ensure the reactor is just critical. A couple of things make life a little more different. Amongst the fission products released (within the fuel and contained by the clad) is xenon. This is a poison and absorbs neutrons, so the controls have to be moved to compensate for this change. In some reactors this balancing act is accomplished by removal of boron from the borated water to reduce the amount of poisons present in the reactor core region.

If the reactor gets into problems, the instantaneous action is to shut down the nuclear fission process by the addition of large amounts of absorbers by dropping rods into the core or flooding the core with highly borated water. This action is called a scram of the reactor and dates back to the time of the first reactor pile put together in the Chicago

University field house, The CP-1 pile went critical in December 1942. Later, the action of Xenon was discovered by Fermi (Dan Cooper, 1998).

2.2.6 Reactor Flux Distribution

The majority of reactors are in the form of a right cylinder with fuel assemblies distributed throughout the cylinder with the axis of the assemblies are arranged along the axis of the cylinder. In most reactors the main axis is vertical, but in the case of the CANDU reactors it is horizontal. The flux or neutron distribution falls off at the edges of the cylinder with some extrapolation. Designers try to flatten the flux shape to give the best power and temperature distributions by using various methods, like burnable poisons, by online replacement of rods or on moving partially burned up fuel. PWRs and BWRs reshuffle partially burned-up fuel to achieve a degree of flux flattening. The fuel is cycled from fresh to used fuel in three groups. Fresh fuel replaces burned-up fuel at fuel reloading time, but the distribution of the fuel loads from previous times are moved around the core to obtain the best use of fuel in terms of life and the reactor's power distribution. Typical fuel recycle is about 18 to 24 months, but utilities try to extend the useful life of the fuel to produce electric power. Sometimes they make use of negative temperature effects on reactivity to extend power by dropping reactor temperatures.

2.2.7 Fuel Assemblies

The previous section discussed the reactor as an assemblage of uranium fuel, without discussing the construction and configuration of the fuel. The fuel is usually made up of uranium in some form as; rods, or plates or pellets. In all cases, the uranium fuel is encapsulated. The function of the encapsulation is to hold the uranium material into a useful shape for heat transfer purposes, like a rod, which may or may not have fins. The fuel encapsulation material or can also has a function to protect the uranium from outside elements and contain fission products to prevent them being released into the coolant.

The canning or cladding material is selected to be transparent to neutrons as far as possible and not absorb neutrons. They should be made of engineering materials having sufficient strength to hold the uranium and byproducts together under high temperatures. Be a good heat transfer material. Materials that have been used for this purpose are aluminum, zirconium, stainless steel, and magnesium.

In cases where gas is used as the heat transfer fluid, designers have developed cans with fins and sophisticated dividers to enhance the heat transfer. Where water is used as the coolant, the fuel rods are grouped in bundles in the form of a matrix array of 17 by 17 rods

for a Pressurized Water Reactor (PWR) with regularly spaced grids to hold the rods apart and enhance flow mixing. Figure 2.3 shows Westinghouse 17x17 fuel assembly and a rod control cluster (RCC). The fuel rods are red, the support structures and rod retaining egg-boxes are blue and the RCCs are yellow. Later in this chapter various reactor types will be introduced along with descriptions of their fuel elements.

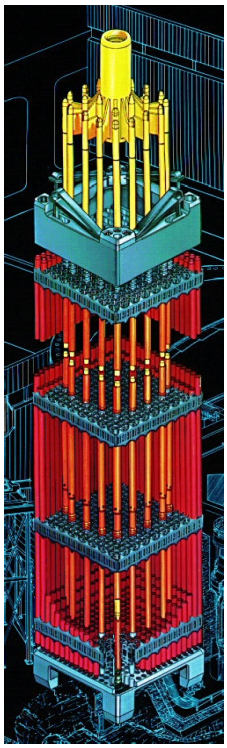

Figure 2.3 Westinghouse Fuel Assembly, 17x17 fuel rods (www.nucleartourist.com-Westinghouse)

2.2.8 Heat Transfer Fluids

The requirements for a transfer fluid are governed by nucleonic, heat transfer, and chemical requirements. These requirements are very similar to the requirements for cladding, i.e. the heat transfer fluid should be as transparent as possible to neutrons (very low capture rate), not breakdown under neutron bombardment and have good heat transport properties. Materials that fit into these criteria are water (H2O), Deuterium Oxide (D2O) Heavy Water, Helium (He), Sodium (Na), Potassium (K) and even Hydrogen (H). What is interesting is how reactor designs are optimized around the choice of fuel, clad and heat transfer fluids.

2.2.9 Fuel Enrichment

It has been mentioned above that there are different reactors, some depend on the use of natural uranium and others use enriched fuel. The discussion here is limited to the use of U235 as the key element that is split. When the concentration of U235 is low, the reactor needs to be large enough so that the neutrons can participate in a collision that leads to a uranium atom being split. If the enrichment is artificially increased over naturally occurring U235 concentration then the size of the reactor core can be reduced, since the probability of a collision is increased.

There are various methods to increase the amount of U235 present in uranium. Most of the methods start by converting uranium metal into a gas. Uranium hexafluoride (UF6) is the gas that is used; the question is what to do with it. Since U235 is an isotope of Uranium, its properties are very similar to U238, which is the isotope that is most prevalent in the ore. So if one considers what the differences in the properties are, one can design means to separate the isotopes. During the Manhattan project, the US decided to use gaseous molecular diffusion. In gaseous diffusion the lighter isotope can diffuse through the pores of the selected membranes.

Later, another method was designed was a centrifuge method, whirling of the gas caused it to separate into light and heavy isotopes, with the heavier isotope going to the outside of the centrifuge. The design of the centrifuge is a long tube-like structure that is whirled at high speed and the heavier isotopes move to the outside thrown by centrifugal force. The design of the centrifuges presents significant design problems, because of the high whirling speed and lengths.

In both processes, the concentration of U235 increases as the gas passes through the processes. As the degree of enrichment increases gradually, one can select at which stage the required enrichment percentage is reached, so for nuclear power plants one can end at 3% to 5%. For bomb materials, one proceeds to very high enrichment levels, say 95%. In both methods banks of diffusers or centrifuges are set up and the UF6 is routed through the banks with the enriched gas going one way and the depleted gas the other way.

Various commercial reactor designs have increased levels of enrichment, which can enable the cost of a reactor station to be reduced, but this has to be balanced against the cost of enriching uranium fuel. A typical enrichment level for reactor fuel is 3% to 5% increase of U235 in U238 fuel. Another advantage of enrichment can be the ability to produce power without having to refuel the reactor. This concept has been very much a consideration in the design of reactors for submarines, which do not refuel for many years. Submarine reactors have high enrichment of 90+% and make use of “burnable poisons” to

balance the effect of the enhanced enrichment. In general, natural uranium reactors have given way to low enrichment reactors, for example UK Magnox reactors have been replaced by Advanced Gas Cooled Reactors and CANDU reactors by Advanced CANDUs. Each of these designs has added U235 enrichment.

2.2.10 Neutron Economy and Reactor Designs

In designing a reactor, attention has to be made to the economy of neutron production and various losses that may occur due to the selection of fuel, cladding, coolant and various structural elements. In addition, the designer has to consider the effect of temperature increases to fuel and moderator. Designers choose to layout the fuel assemblies and the spacing between assemblies to enhance the neutron economy and at the same time try to ensure that increases in fluid temperature has a negative feedback, as this promotes reactor stability. The assemblies are contained within a reactor vessel, which is most often constructed of steel and is designed to withstand internal pressure. The pressure of the fluid within the reactor vessel depends on the type of reactor. It can be from 1,000 psi for boiling water reactors to 2,250 psi for pressurized water reactors.

2.2.11 Control Considerations

It is important to be able to control reactor power to match the requirements of the electric power grid. This means that one has to control the nuclear reaction rate by moving control rods or changing the concentration of boron in the reactor coolant. According to reactor kinetics, there are two grouping of neutrons, those that react promptly to the movement of controlling absorbers and those that are delayed in their response. The first are called prompt neutrons and the second are called delayed neutrons. Reactor control would be difficult if there were only prompt neutrons. The delayed neutrons occur because some of the fission products are unstable and release neutrons after some time, depending on an associated ‘time constant’ of stability. In modeling of reactor kinetics for control purposes, the model may consist of one equivalent group or more exactly six groups with different time constants and different concentrations.

One of the most significant products of the uranium fission is xenon (Xe135). Xenon is a poison with a time constant of 16 hours. The impact of Xenon on the fission process was observed by Fermi during testing of the first pile at Chicago University. Fermi was the first person who associated Xenon with shutdown of the fission process. Xenon builds up after start-up of a reactor and control rods are moved to compensate for this build-up of Xenon, but once the reactor is shutdown, the Xenon continues to build up and this may present a problem if the reactor design does not have sufficient reactivity compensation to overcome

the xenon poison effect until it decays below a given value. The impact of this is that if a reactor shuts down and has limited reactivity control, it has to restart relatively quickly or remain shut-down for a while. Figure 2.4 shows a typical Xenon transient following a 50% increase in power followed by a 50% decrease in power. The half life or time constant for Xenon is 9.2 hours and Xenon concentration reaches its peak after a shut-down some 11.1 hours. The net effect of the Xenon poison effect is that this has to be considered in the design and operation of Nuclear Power Plants. It should be noted that excess reactivity is available at the beginning of life of a particular core, be it either natural uranium or enriched uranium. As the U235 is used up the reactivity effect diminishes and eventually the reactor has to be shutdown, or in the case of natural uranium reactors that have on-line refueling new fuel has to be inserted to replace the used fuel.

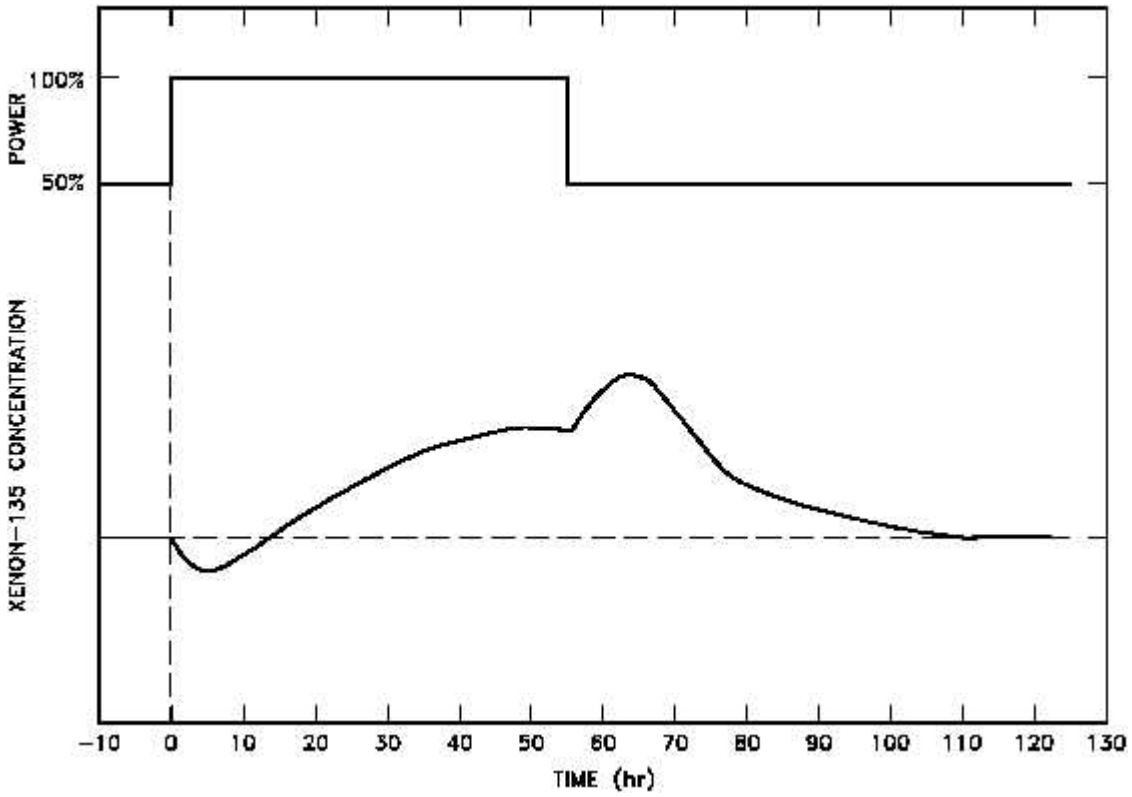

Figure 2.4 Typical Xenon transient following load changes (after DOE Training document)

2.2.12 Radiation Considerations

A reactor core at power is a source of neutrons and other forms of radiation. In order to protect plant personnel from the effects of radiation the reactor is shielded from these effects by the section of shielding materials. Most of us have been exposed to X-rays for medical or dental reasons, so we are used to lead being used for this purpose. Lead is not

a very good engineering solution for large reactors and concrete has been selected to provide shielding. It also provides a platform for the reactor vessel to stand on and the walls surrounding the reactor vessel.

2.2.13 Containment

Containment is the ultimate safety system and has been a feature of US commercial reactors from the beginning. The containment is an encompassing vessel that encloses the reactor and some associated equipment. It is made up of an internal steel vessel and an outer concrete vessel. The containment is there to prevent the release of radioactive particles that may result from an accident to the reactor and fuel. Not only is the containment designed for this purpose, it is designed to ensure that the energy released post accident does not cause the collapse of the containment. For PWRs and BWRs, an accident can lead to the release of high energy steam, which could over-pressure the containment. To prevent this happening, sprays are used to condense the steam and control the pressure rise. The water then falls to the bottom of the containment and drains into a sump. Water is taken from the sump is used to cool the containment space via sprays and also injected into the reactor to cover the fuel elements and cool them.

2.2.14 Refueling

Like fossil plants nuclear fuel gets burned up or used. In the case of nuclear fuel this means that the concentration of U235 drops. As the concentration of the fuel drops the core capability to produce power reduces. Initially, the drop is balanced by reducing the amount of poisons present in the core by either removal of absorber rods or the dilution of boron concentration depending on the type of reactor. For natural uranium fuelled reactors, refueling is done on-line, i.e. used fuel is replaced by fresh fuel. In the case of enriched core reactors, the reactor is shutdown and the used one third of the fuel removed and a third of new fuel replaces it. The core, in this case, is re-shuffled so that the older fuel and new fuel is moved to produce an optimal distribution of fuel as far as the power and temperature distribution of the core is concerned.

In both cases, burned-up fuel is radiologically speaking hot. This means that it has to be handled very carefully, so that operations personnel are not exposed to harmful radiation. In on-line refueling, the spent fuel is replaced by new fuel rod or assembly to a fuel handing machine, which is shielded and the machine then in turns places the spent fuel into a spent fuel pool with sufficient water to cool and shield the fuel. In the case of GCRs, the fuel handling machine is vertical and the fuel assembly pulled up into the machine and replaced a new assembly. In the case of the CANDU, the spent fuel is pushed out by the

new fuel. There is a fuel handling machine on both sides of the horizontal reactor core, one to put fuel in and one on the other side to accept used fuel.

In the case of Light Water Reactors (PWRs and BWRs), fuel assemblies are moved under water from the core to the spent fuel pool along a channel. The fuel is moved by a spent fuel handling tool.

Used fuel remains in the spent fuel pool until the fuel power generation falls to a state that it is possible to move to a more permanent storage facility. Currently, since the US has failed to construct the Yucca Mountain final fuel storage site, the used fuel leaving the spent fuel pools has to be stored onsite in 'dry container,' which are large concrete shielded casks in which a number of used fuel assemblies are stored. Heat from the fuel permeates through the concrete so that the fuel temperature does not exceed some acceptable limit. The safety issue here is that the utility was not expected to store spent fuel onsite beyond a small number of such casks which would be recycled with the spent fuel sent to a long term storage location, such as Yucca Mountain.

2.2.15 Listing of Reactor Types

Various reactor types have been mentioned above, but a listing of types is given below:

PWRs Pressurized Water Reactors

BWRs Boiling Water Reactors

GCR Gas Cooled Reactors

VVERs Russian PWRs

AGRs Advanced Gas Cooled Reactors

CANDU Canadian Heavy Water Reactors (**Can**ada **D**euterium **U**ranium)

HTGR/HTRs High Temperature Reactors (HTGR; High Temperature Graphite Reactor)

RBMK Russian: Steam Cooled, Graphite moderated Reactor (RBMK is in Russian; Реактор Большой Мощности Канальный, which is a High Power Channel Reactor)

The most numerous reactor types are the PWRs, then the BWRs and CANDUs, GCRs are phased out and there are a few AGRs in the UK and a few RBMKs in Russia. Three HTGRs were built, but no longer exist, although the concept is still receiving serious consideration in US and China. The normal fuel is mostly low enriched uranium (LEU).

The early CANDUs use natural uranium. The Advanced CANDUs are being considered for construction and use LEU fuel. RBMKs are being phased out.

Note about containment design for reactor types:

Many early reactor designs did not have containments as such. The GCRs did not have containments. AGRs relied upon the design of the concrete pressure vessel used as the reactor vessel to also act as containment. Early VVERs did not have containments as such, but did try to control releases by having chambers adjacent to the reactor building, which allows gases and steam to pass through a series of bubbler trays before being released into the atmosphere, see Figure 2.11 of Paks NPP below. Later 1,000 Mw(e) VVERs followed US practice and went with a enveloping containment, see Temelin NPP below (Figure 2.12). RMBKs had partial containment around certain reactor piping. Early CANDU designs had reactors buildings connected to a common 'vacuum' building, which enabled multiple reactor units to be placed near large cities, like Toronto. CANDUs have multiple was of absorbing reactor releases and had systems for hydrogen control, which might result from zirconium/steam reaction. The zirconium/steam reaction was a significant part of the recent Fukushima accident in March, 2011.

2.3 Reactor Designs

2.3.1 Introduction

As seen in section 2.2.14, a number of different reactor types have been designed and operated over the years. It is not proposed to cover in detail all of the different designs. This section builds upon section 2.2 and discusses the normal operating design features and safety features of the selected reactor designs. In the last few years, new designs of reactors are being considered, some are under-construction, but currently none are operating. Since the interaction between managers and staff under accident conditions are going to be examined through the lens of VSM, it is not proposed to include all of the older non-operating reactor designs or the newest designs. The selection of reactor types is going to be led by reactor accident history coupled with the numbers of specific reactor types in use.

The purpose of a nuclear reactor, in the power energy business, is to produce heat that can be used to generate electricity. In some applications, as a byproduct of steam to drive turbines, steam/hot water is produced and used for district heating, but this is the primary use. Before discussing all the different types of reactor it is well to discuss the layout of a typical nuclear power plant. Figure 2.5 shows a simplified diagram of a conventional NPP.

There are three circulatory loops, one that takes energy from the reactor and transports to a steam raising unit, a second loop that takes steam from the steam raising unit (SRU) and passes it to a steam turbine and a third loop which cools the low pressure steam to form water. The hot fluid from the reactor is returned via a pump back to the reactor having been cooled by the steam raising unit. Similarly, the high pressure steam from the SRU is used to drive a steam turbine, which in turn drives an electric generator that supplies power to the grid.

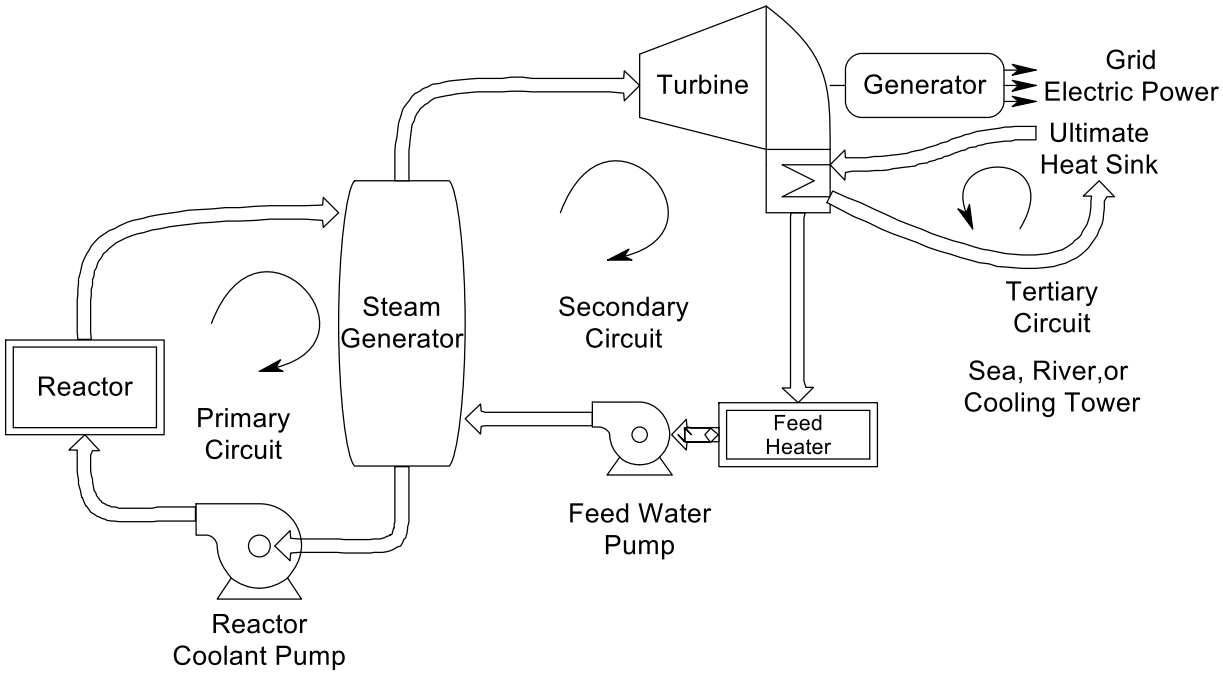

Figure 2.5 Typical NPP Layout of Heat Transfer Circuits

The steam flow at the back-end of the turbine passes into a condenser in which heat exchanger pipes containing cold water convert the low pressure steam to water. The water from the condenser then returns to the SRU via a feed pump and feed heaters. The water going through the condenser heat exchanger pipes is obtained from the sea, local rivers or cooling towers and these are the ultimate heat sink for the reactor. So there are a number of circuits in which heat energy is transferred from the reactor to the ultimate heat sink. The primary circuit is: reactor/SRU, secondary circuit is: SRU/turbine and the tertiary circuit is: turbine condenser/environment. The thermal efficiency of such a scheme is about 30 percent.

It should be mentioned that the majority of reactors use such a three circuit system approach from reactor to electric power and eventually releases heat to the atmosphere. However, in the case of the Boiling Water Reactors (BWR), there is no SRU and the steam produced in the reactor passes directly to the steam turbine.

Figure 2.5 shows the main heat transfer circuits associated with a reactor. However, there are many other systems associated with a nuclear reactor besides these circuits. There are ancillary systems, which support these main systems like; the residual heat removal system, the auxiliary feed system, reactor primary pressure and level compensating systems (pressurizer in the case of a PWR) and there are chemical and volume control systems for controlling boron concentration and adding or removal of water, etc. As has been pointed out earlier, one of the features of reactors is the presence of decay heat, which continues after a reactor is shut-down, which has to been cooled. This is the role of residual heat or decay heat removal system, which has to be operated when the main cooling circuits are not available or not needed.

In addition to these support systems, which are there for operations needs, there are safety systems that are the back-up systems to ensure NPP safety, by shutting down the reactor when the controls fail, remove decay heat, when normal systems fail, supply multiple sources of coolant to remove heat and keep the core covered and the containment pressure within design limits during accidents. Since the plants depend on electric power for running pumps, operating valves and supplying power to instrumentation and controls, etc. there are redundant power sources, such as standby diesels and batteries, as well as power from the electric grid. Information from various displays in the central control room, as well as local information sources, inform the operators and allow them to take action to help terminate or mitigated accidents. The power plant is made up of pressure vessels and therefore untoward increases in pressure must be controlled and relieved by the action of safety valves on both the primary and secondary circuits. Often these ‘code’ safety valves are backed up by non-code relief valves to prevent the need to open safety valves. Figure 2.6 shows a more complete view of a number of these systems for a typical Westinghouse reactor.

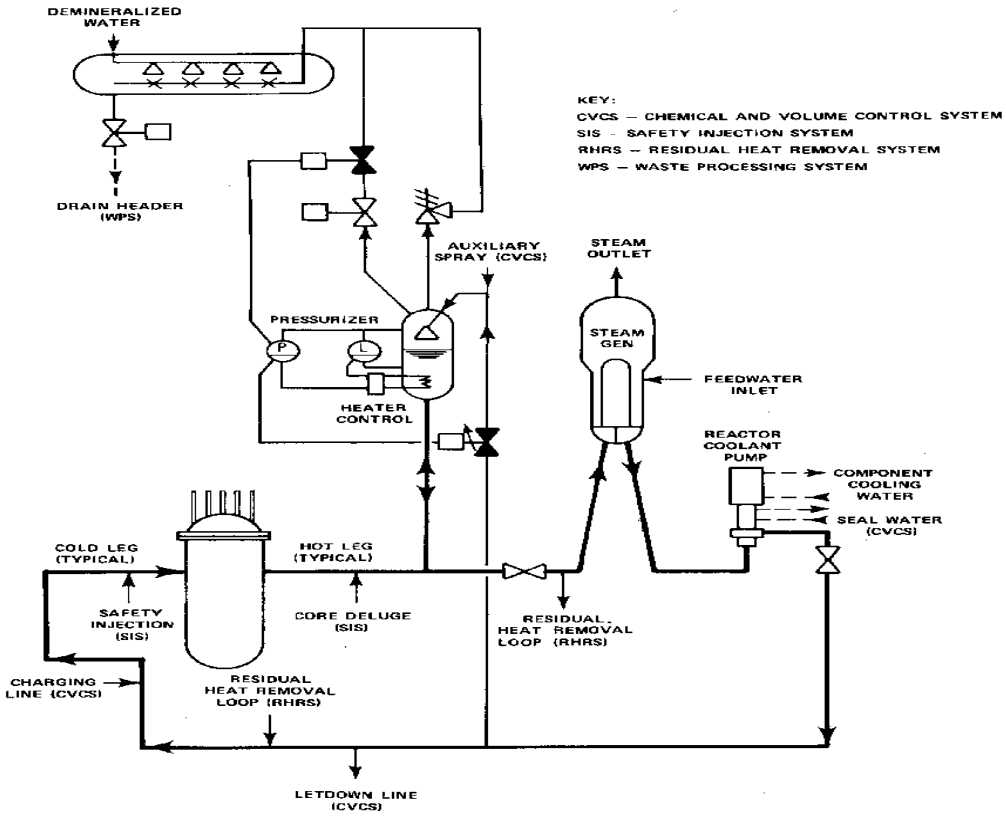

Figure 2.6 Schematic of Main Reactor circuit of a PWR (DOE training material)

Figure 2.6 shows the reactor coolant circuit with reactor, main reactor pump and the pressurizer. The function of the pressurizer is to maintain the primary circuit pressure and also to accommodate increases and decreases in reactor water volume as the primary circuit heats up and cools down. The figure also shows input and take-off points for safety and servicing systems, for example in the chemical and volume system (CVCS) there is a letdown line from the primary system and it can see at the base of the diagram. The figure shows many of the details associated with the pressurizer such as the heaters and sprays for maintaining pressure. Also the safety and relief valves are shown. The steam from the safety and relief valves is released into the pressure relief tank (PRT) via spray nozzles. The support services for the main reactor coolant pump is also shown and come from the component cooling and seal water systems. As the reactor cools down to cold shutdown condition, in which the reactor is shutdown and the decay heat has dropped to a low level, the means of heat removal change from using the steam turbine, then to the use of the steam dump system and then the residual heat removal system. The residual heat removal system is connected to the reactor primary system, see Figure 2.6, there two connections outflow and inflow. The outflow is hot and the water passes through a heat

exchanger and then is pumped back to the inflow connection. The heat exchanger is cooled by “service water” that comes from a river/sea/cooling tower, see Figure 2.5. These are the ultimate heat sinks for a reactor power plant.

In the case of failure or failures of the normal heat removal services, reactors are designed to have backup safety systems to remove the heat from a LWR reactor, and keep the core covered. The safety systems have to operate over a range of conditions from high pressure (PWR) to medium pressures to low pressures (close to atmospheric conditions). To deal with range, the designers have supplied high and low pressure safety injection pumps; see Figure 2.7 for a symbolic representation of such an arrangement. Also, there are pumps which supply water to the containment sprays. Sources of borated water are needed and a large tank of such water is maintained at the station. In addition, as an extra caution, water that does enter the containment is used for both sprays and for covering the core. Reactor system pipe breaks can lead to water leaving the core and going into the containment. It then drains into a low point in the containment, called the sump. Pumps can use this water, in emergency, to cover the core and help prevent core damage.

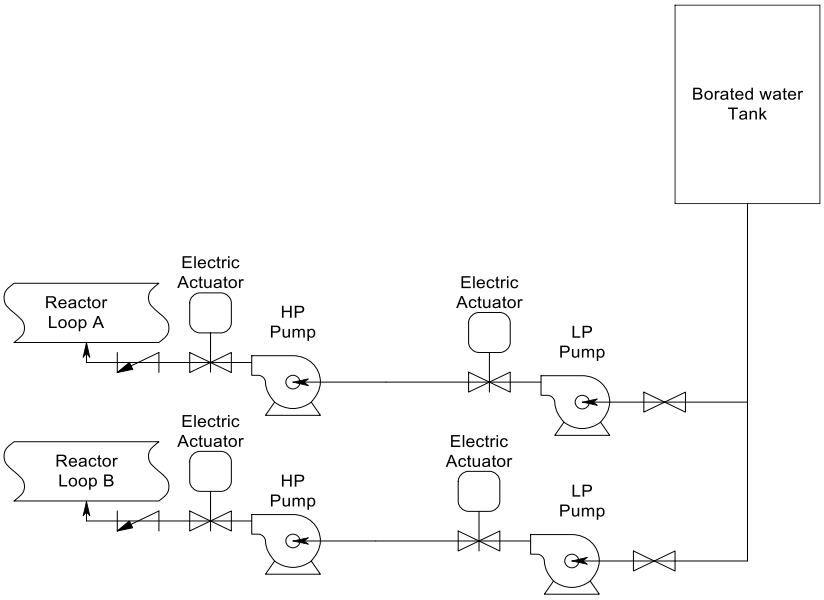

Figure 2.7 Symbolic Representation of HP/LP Safety Injection Systems

The combination of normal, safety and ancillary systems have to be co-coordinated between the designed control and protection systems and the operators, who are licensed to operate the plant by the regulators. The owners and their top managers cannot (or should not) interfere with the operators in the execution of their jobs, unless they are licensed by the regulator to operate the plant. This situation is not usual.

The complexity and overlapping functions of reactors can lead to accidents, but the operators are for the most part well trained by using simulators and are practiced in the use of procedures covering normal, abnormal and emergency conditions. Actions that resulted from the Three Mile Island accident were the improvement of simulators for training purposes, the quality of the information displayed to the operators and of emergency procedures. Essentially, this was due to the fact that previously the role of the operators was underplayed!

2.3.2 Reactor Types

The study includes US and Russian PWR designs, BWRs in the US and Japan, and the Russian RBMK plant, because there was a significant accident that involved this reactor design at Chernobyl. Within the different reactor designs there are some features that are similar and others that are different, for example in the set of Westinghouse PWR reactors there are different layouts and numbers of steam raising units. Westinghouse built numbers of two loop, three loop and four loop reactors. This designation relates to the number of steam generators associated with a given reactor core. For each selected reactor type there will be a generic description followed by a description of differences that might occur within that generic type.

For US PWR plants, there were three different manufactures, namely Westinghouse, Babcock and Wilcox and Combustion Engineering. For BWR plants, there was only one US manufacturer, General Electric. The French initially built close copies of the Westinghouse three loop plants, sub-sequentially built four loop plants similar to Westinghouse four loop plants and then developed the designs to reach higher powers, going from 1100 to 1300 to 1400 MW(e). Currently, they have a much newer design called the EPR being designed and built by AREVA all over the world, but none are operating at this time. Other countries like Japan built nuclear plants under license and then later designed their own plants based upon their experience with the US designed plants. This approach applied for PWR, BWR and CANDU NPPs.

It is proposed to cover the following reactor designs, their layout, their safety features and operation:

1. Westinghouse Pressurized Water Reactors
2. GE Boiling Water Reactors
3. B&W Pressurized Water Reactors
4. Combustion Engineering PWRs
5. Russian PWRs

6. Russian RBMK

2.3.2.1 Westinghouse PWR Designs

Westinghouse PWR designs are by far the most numerous in the world, both as supplied by Westinghouse and those built under license by Framatom/AREVA in France, China and South Africa. In USA there are 104 reactors with the majority being Westinghouse of various types. Westinghouse has designed four sizes of plant, designated by the number of primary side loops, loops connecting SRUs to the reactor: these are one loop, two loop, three loop and four loop plants. As originally designed, the basis was 250 Mw (e) per loop, so there were 250, 500, 750 and 1,000 Mw (e) plants. Only one, one loop plant was ever built (in Spain). Over time most of the plants have increased their power outputs. Figure 2.6 shows many of the details of a Westinghouse PWR primary circuit of vintage 1960 to 1990.

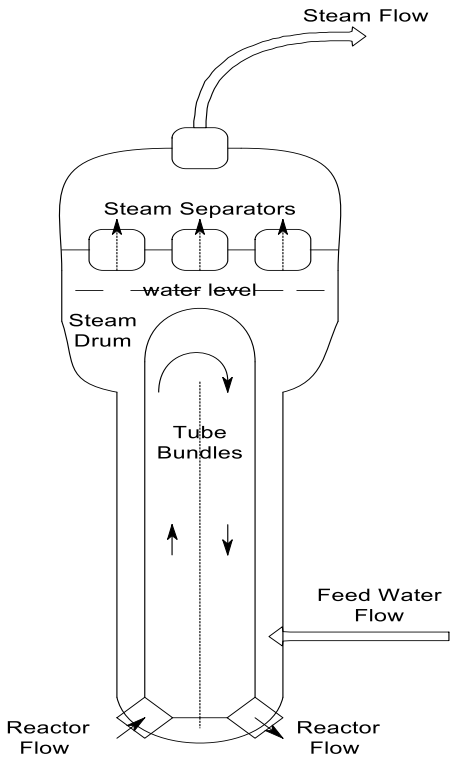

Figure 2.8 Schematic of a Westinghouse Steam Generating Unit

The Westinghouse steam generating units are vertical heat exchangers with the reactor flow passing through a tube bundle in a U shape, shown in Figure 2.8. The early plants were equipped with smaller 44 series SGs with 44,000ft^2 heat transfer surface area and later 51 series (51,000 ft^2). The 44 series cold feed was into the drum and the later

versions of 51 series made use of an integral economizer section at the low end of the tube bundle, see Figure 2.8.

On the water-steam side of the heat exchanger, cold water is pumped into a baffled section acting as an economizer and then the mixture of steam/water passes over the heated tube bundle, which increases the volume of the steam. The steam/water mixture passes through a set of separators to help dry the steam, which then flows to a high pressure Steam Turbine, the water flow down the bundle. The steam leaves the high pressure turbine passes into a reheat/steam separator unit and from there into the low pressure steam turbine section of the main steam turbine. The turbine turns at 3,000rpm (US standard) to drive an electric alternator to supply electric power to the grid with a frequency of 50Hz.

As mentioned above, there is a chemical and volume control system, which includes charging pumps whose duty is to add water to the main circuit. Depending on the state of the reactor, the boron concentration is changed to modify the effectiveness of poison in the core to control its reactivity. At other times, water is added to reduce boron concentration to enhance reactivity. The reactivity control is achieved by coordinating boron concentration with the control rods position to control the power of the reactor and match it to the requirements of the grid. To balance the liquid volume in the reactor, fluid is made up through the action of charging pumps and reduced by water that passes through the letdown system. The water level in the pressurizer increases and decreases as the primary temperature increases or decreases to match the changes in reactor power. The average reactor temperature (Tm) rises and falls as a function of power.

The Westinghouse designed reactors have the safest operating history of NPPs and is due primarily to three factors: The amount of water in the reactor, the design of the SRUs, which also have a large amount of water in the steam drum, see Figure 2.8, and the diverse design of the auxiliary feedwater pumps (one full scale steam driven auxiliary feed water pump and two separate half size electric drive feed pumps. Like other reactors, Westinghouse units have redundant high pressure and low pressure pumps to inject water into the core. These safety systems are essentially two train systems. Large tanks of borated water are available to cool the reactor, and to maintain the reactor in a shutdown state. The design also allows for using water in the containment to be recycled to be used for reactor cooling and core coverage purposes and also for spray in the containment. The water is the containment may result from a number of accident causes including PRV Tank disc rupture due to over pressure, pipe breaks and spray operation.

The design of the NPP Systems, Structures and Components in general are designed to retain function after a design basis earthquake, effects of tsunamis, floods and other natural disasters. Containments are design to resist the effect of aircraft crashes. NPPs depend on the availability of electric power for running safety components and for instruments and controls. During emergencies, like the complete loss of offsite power, diesel generators and batteries are available. Even for a complete blackout of both offsite and standby power, reactors are safe for a limited time, because of the ability of operators to manually open and close valves, but eventually if power is not restored the core is likely to get damaged. No nuclear core heated by decay heat can avoid damage along with a subsequent release of radioactivity if it is not sufficiently cooled. Sometimes this can be many hours and days depending on the physical characteristics of the core, the reactor vessel and containment.

2.3.2.2 B&W PWR Designs

The Babcock and Wilcox PWR designs are very similar in overall design with the exception of the SRUs. Westinghouse's nuclear experience was related to submarine designs in which the SRU was a recirculation SRU with a steam drum. However, B&W's background was very much connected with convention oil and coal fired plant, so they thought that superheating of the steam was an important feature. B&W decided to use an once through steam generator, in which water flows into the unit and leaves as superheated steam with 60 degrees of superheat. It turns out that the thermodynamic advantage of superheat has to be balanced against the low water inventory of the B&W SRU compared with a Westinghouse SRU. Figure 2.9 depicts a B & W Once through Steam Generator. The B & W Steam Generator is a vertical SRU mounted inside the containment. Feed water enters the SRU at the bottom of the unit and passes over the tube bundles heated by the hot pressurizer reactor water and starts to boil, form steam and then the steam becomes super heated up to about 60^{o} F. The amount of water held on the water-side of the SRU is relatively small in comparison with the Westinghouse PWR SRUs and for that matter also with the Russian VVER SRUs.

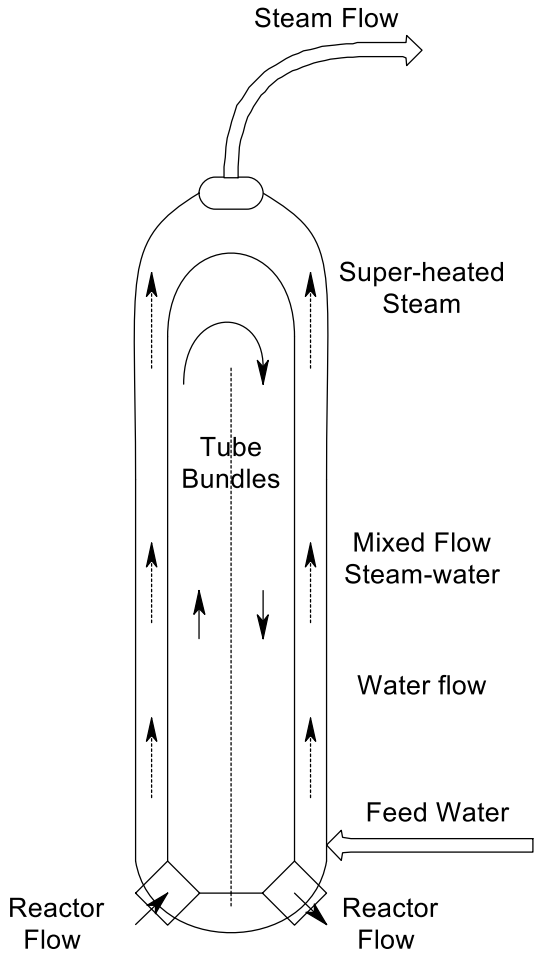

Figure 2.9 B & W Once-Through Steam Generator

The rest of the B&W design for the reactor systems was very much the same as the Westinghouse units. The Once- through Steam Generators (OTSG), which are taller than the corresponding Westinghouse units, but the superheated steam means an increase in steam turbine efficiency. The Safety systems, etc., follow the same basic philosophy as Westinghouse.

2.3.2.3 Combustion Engineering PWR Designs

Combustion Engineering designs of PWR were initially very much like those of Westinghouse. Their later designs of 1000+Mw(e) units differed from corresponding size units of Westinghouse in that they kept the two loop configuration of their earlier plants and developed very large SRUs. The SRUs were of the recirculation type, see the drum recirculation SG unit in Figure 2.8. In these units 2/3rd of the water recirculates and 1/3rd is steam at full load. However, there are four main reactor pumps in all with two pumps

associated with each steam generator. The pumps take cold water from the steam generators and pass it into the reactor through four connections.

2.3.2.4 General Electric BWR Designs

The General Electric Company of the US has been associated with the design of a light water reactor called a boiling water reactor. In this design of NPP, the nuclear reactor is cooled by the use of normal water that forms the steam that is used to power the main Steam Turbine. If one compares the PWR with the BWR, the three circuits of the PWR with two circuits for the BWR. From a simplicity view point the BWR is simpler. The PWR during normal operation does not allow boiling in the primary circuit whereas the BWR boils the water in the core to power the main turbine. There appear to be both advantages and disadvantages with having a design like this. The pros and cons are not discussed here, but just to acknowledge that both types exist and are used. In a later chapter, safety issues associated with the various reactor types are covered. In particular, the accident that occurred just recently at Fukushima, Japan was due to a large tsunami and involved BWR plants. Along with other manufacturers, reactor designs have changed over the years in one aspect or other. The original BWRs were designed to meet Atomic Energy Commission push to develop a useful BWR that could be used for power production and based upon using boiling water to power a steam turbine. Later, GE came up with the idea of supplying NPPs based on a turn-key fixed cost contract. Here GE would supply a NPP and the utility would pay once it was built. This was a new concept and the GE design was the so-called Mark 1 containment. This idea led to the rapid expansion in the number of plant ordered by the US utilities in the 60s to the 70s.

2.3.2.5 GE BWR Mk 1 Containment

Figure 2.10 is a diagrammatic representation of an early GE BWR Reactor Building confined to the steam generating portion of the power plant. The key item of the reactor unit is the so-called light bulb, which is the central portion of the reactor unit. The reactor vessel (RPV) is the mauve colored vessel in the center of the light bulb. The control rods are not shown on this very simplified representation of a BWR plant, the rods enter from below the reactor and are inserted by a hydraulic rod drive system.

GE does not have a conventional plant enveloping containment and makes use of the light bulb as the containment. In addition, there is a torus at the base of the unit, which is the suppression pool. Steam or hot water released from the reactor passes into the water in

the ring via a series of nozzles. It is difficult to design efficient nozzles to pass steam into water to ensure that the steam is cooled and reverts to water. Much testing was carried out to ensure correct suppression occurred. The suppression pool is called a wet well (WW), the rest of the light bulb is the dry well (DW). One issue that is of particular concern with the BWR plant is radiation control. The reactor vessel area has a concrete shielding wall (Suppression Chamber Shielding Wall, SCSW) and there are a number of concrete walls that help shield personnel around the Dry Well and the Wet Wells areas. Since steam leaving the reactor can be contaminated, the main turbine and other units have to be shielded. This is decidedly less advantageous for BWR operations compared with PWRs. The GE containment and reactor are mounted quite high relative to ground level, because of the control rod drives being under the reactor vessel. As a consequence of this arrangement, the GE designers decided to place the spent fuel pool (SFP) inside the containment building, rather than outside the containment. This allows the fuel to be removed from the core and moved under water into the SFP. As shown in Figure 2.10, the Reactor Building crane is shown in orange/yellow and moves the reactor shielding, yellow, the reactor head and dry well closure. The top area is then flooded to allow fuel to be moved shielded by the water through a channel to the SFP. New fuel is then moved back into the core in a reconstituted form; see section 2.2.14, on refueling.

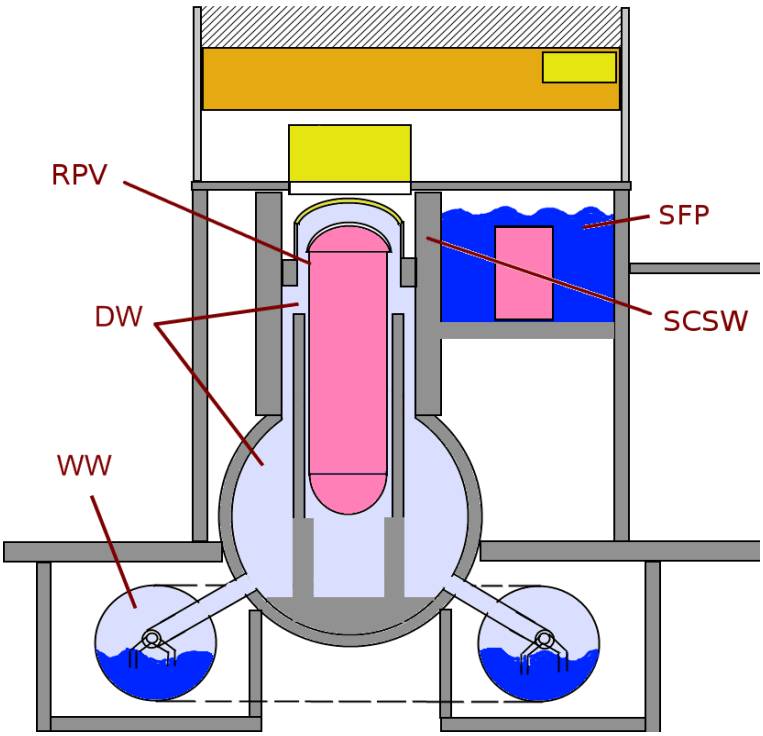

Figure 2.10 Diagrammatic Representation of a GE BWR Reactor Building (Braun, 2011)

This diagram is a very simplistic rendering of a BWR and some of the functions affecting the response of the BWR to an accident are not shown here. However, it does indicate the differences between the BWR plants and others. In later chapters when the features of BWRs are necessary to understand accident progressions like the Fukushima accidents that took place in March 2011, they will be discussed. The secondary sides of BWRs are similar to other nuclear plants in configuration; the exception is the need for shielding of the main turbines and feed heaters in the case of BWRs compared with units using steam generators.

2.3.2.6 Russian PWR Designs

Russian designed PWRs are conceptually similar to Western designed PWRs. There are a some differences, the early Russian plants were 440 Mw(e) units with six horizontal SRUs and the containment was a partial containment with the steam/gases from the reactor containment passing through a column containing bubblers, or trays like those used in the chemical industry to mix different fluids. The bubblers are capable of suppressing particulates, soluble gases and reducing the energy releases by cooling steam releases. Later, designs of Russian reactors have moved towards the US concept for containment. The 1,000 Mw(e) plants have containments and reduced numbers of steam generators per unit.

2.3.2.7 440 Mw (e) Designs

A typical 440 Mw (e) plant is the Paks Hungarian power station, which has four 440 Mw(e) units. These units have operated successfully since 1988. Like US plants, these plants have been upgraded in a number of ways, for example they have changed from analog control and protection systems to the more modern digital systems. Paks designed the control and protection systems themselves based upon Siemens equipment. They experienced a radiological accident in 2006, when they were cleaning some fuel elements to removed iron related oxides on the fuel. Although serious, its impact was limited to one person being exposed to radiation.

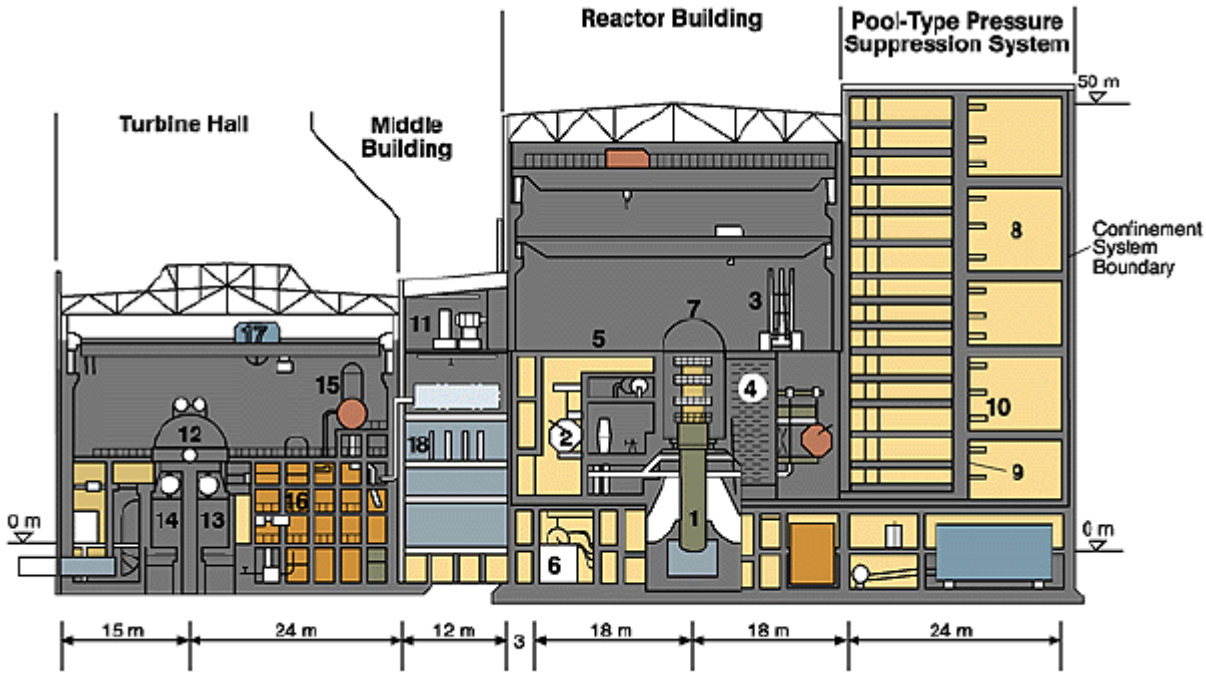

Figure 2.11 Arrangement of a 440 Mw(e) [after Paks NPP, International Nuclear Safety, report 2001(PNNL.gov]

The main features of the NPP are shown such as the Turbine Hall, and Reactor Building in Figure 2.11. Additionally one can see the Pressure Suppression System, (bubbler/tray system) mentioned above on the right hand side of the Figure. A steam generator are shown as item 2, and the reactor as 1. The figure indicates that the reactor building is quite a light structure, but there are radiation shielding walls to protect personnel and that primary breaks lead to the suppression system by large passages from the reactor space.

2.3.2.8 1000 Mw (e) Designs

The VVER 1,000 Mw(e) plants are a later development of Russian PWRs, the first was constructed at the Novovoronezh test site close to the city of Voronezh, south of Moscow. There are a number of these type of units in Russia, Ukraine and other locations, such as the Temelin NPPs in the Czech Republic. Figure 2.12 shows the Temelin, this plant is the product of trying to bring Russian designed NPPs up to the safety standards of the West. The 1,000 Mw(e) plants are equipped with Containments. Figure 2.12 shows a simplified over-view of the Temelin VVER. The figure shows a single reactor coupled with a single steam generator and reactor coolant pump. In fact the actual reactor has four steam generators and corresponding coolant reactor pumps.

Figure 2.12 Pictorial Representation of the 1000 Mw(e) Temelin NPP, Czech Republic (www.allforpower.com)

The figure shows the reactor core (#3), the rod drives, core and RPV vessel as items #2, #3 and #1. The horizontal steam generator is #7, the reactor coolant pump is #6 and the containment is #9. Steam flows from the steam generator via the steam line #8 to the turbine/alternator (items 10 and 12). The ternary cooling loop, like that shown in figure 2.5, made up of condenser, #11, cooling tower #14 and the circuit including cooling water pump. The secondary loop goes from the turbine (#10), the condenser (#!!) and the feedwater pump (unmarked). The output electrical power from the alternator (#12) goes to the main transformer (#13) to the grid (#15). Not shown in the diagram is the pressurizer, which is feature of every PWR and is connected to the reactor primary system on one of the cold legs, or return loops from the steam generator to the reactor. Some of the features are similar to Western PWRs, but there are some differences in the safety injection systems, and auxiliary feed water systems. The control and protection systems hardware for Temelin NPP has been upgraded by Westinghouse based upon digital technology.

2.3.2.9 Russian RBMK Designs

The RMBK reactor designs are large reactors cooled by water with a graphite moderator. Figure 2.13 shows a simplified arrangement of the primary loop, which links the reactor to the steam generator. The reactor is made up of numerous tubes that allow water to pass the fuel elements and cool the fuel rods. The primary circuit is a boiling water reactor, with

boiling occurring within the tubes. The steam-water mixture passes into the steam separator/drum. In this type of NPP, the PWR steam drum and the RMBK steam separator are fulfilling similar functions. Feed water from the secondary side of the plant is pumped into the drum section of the separator and cold and hot water mix and is then fed into the intake collectors and then up into the reactor via reactor coolant pumps. The secondary and ternary circuits of the RMBK are fairly standard systems. The RMBKs do not have large containment structures like Western LWRs and 1000 Mw (e) VVERs have, but there are limited containment structures around the hot and cold water primary system loops.

Radiation control is present to safeguard operational staff, so there are shielding walls around the components, but these walls do not act as containment to stop releases of energetic steam or explosive gases resulting from burning fuel or graphite, as happen in the Chernobyl accident. One feature that should be mentioned is the design of the control rods, normally designers distribute poisons, such as boron, uniformly through the rods. The Russians had a composite rod consisting of poisons and a lower section of Graphite. This scheme was chosen to increase the nuclear efficiency of the core, but on review following the Chernobyl accident this did not seem to a very good idea and aided in causing this accident. In addition, the RMBK has a positive void coefficient which means that if water cooling the core develops a void, the neutron capture probability increases. This is in the direction of increased risk due to positive feedback and is normally avoided in designing reactor cores. For instance, US PWRs core are designed to have negative temperature coefficients. Another complexity in the design of RMBKs is having both short and long control rods. The short rods are inserted from beneath to core in order to axial control flux shape (distribution of neutrons), to avoid high flux regions in the lower sections of the core.

The RBMK fuel, which is slightly enriched uranium dioxide fuel (2% enrichment) and burnable poisons are included to help control flux distribution across the core. A good power distribution during operation and enhanced life of fuel are the objectives of the nuclear physics designers. The fact of shuffling fuel in the case of PWRs and on-line refueling of natural uranium fueled reactors are methods for improving the neutron economy of reactors. Some aspects of RMBK responses are covered in a later chapter, especially during the Chernobyl accident analysis.

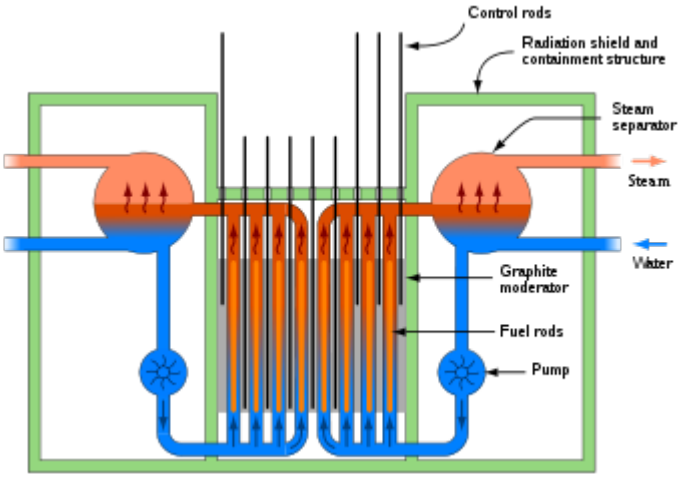

Figure 2.13 Diagram of the RMBK Reactor Primary System (Wikipedia.org)

2.3.2.10 Canadian CANDU Reactor Designs

Most of the different reactor designs have been developed by their host countries, so the Russians developed the RMBK and VVER designs, the US has developed a number of different designs, such as the Westinghouse PWR, GE BWR, HTGR (Helium cooled-high temperature gas cooled reactor). The UK developed the AGR and the GCRs and SGWR and of course the Canadians developed the own design, CANDU, the Canadian Deuterium Uranium Oxide Reactor.

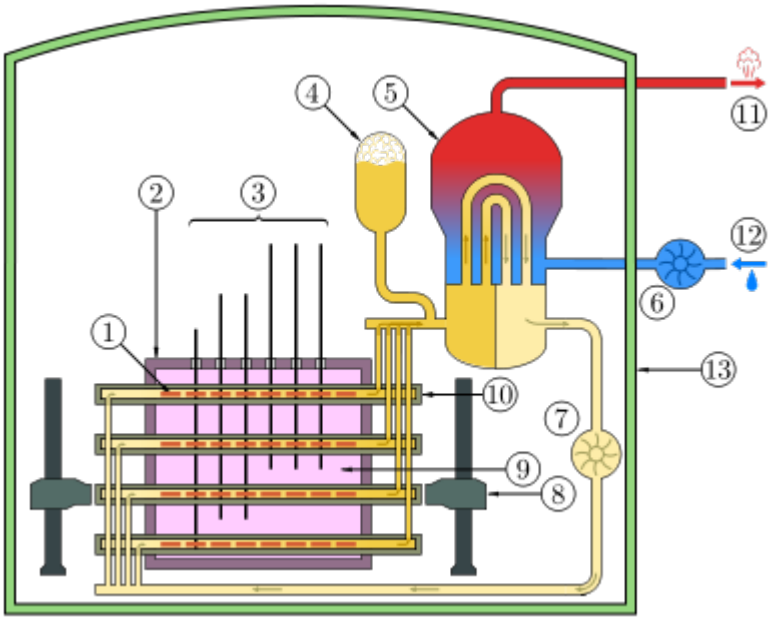

Figure 2.14 Schematic of the Primary Loop of a CANDU Reactor (Wikipedia.org)

Figure 2.14 is a depiction of a CANDU reactor. A CANDU is a multiple tube reactor, which is designed to operate with natural uranium fuel. Later developments of the CANDU have made the move to use enriched fuel. The reactor unit is a right cylinder lying on its side, as shown in the figure, is made up of a series of pressure tubes (#1). The fuel is contained in the pressure tubes through which ordinary water flows under pressure. This reactor is a pressurized water reactor, and the pressurizer is item #4. There are headers on each side of the reactor, which either collect or distribute water to cool the core via a reactor coolant pump (#7) or take hot water to the a recirculation steam generator(#5) and also used for fuel loading or unloading via the fuel handling machines (item #8). The moderator is the deuterium held in a tank (item #9). The secondary circuit is not shown, but is fairly standard. Cold water enters the steam generator from the feed line (12) via a feed pump (item 6). Steam from the Steam Generator (5) passes to the steam turbine via line #11.. The primary system is held within a containment (item 13). The control rods for the CANDU are shown as item 3 and are unusual in that they are at right angles to the fuel pressure tubes that make up the core. This makes the physics calculations to define the neutron flux shape in the core somewhat different to all other nuclear reactors, but it seems to have been overcome satisfactorily, since many CANDUs are operating in Korea, India, Romania, as well as Canada.

2.4 Conclusions

The objective of this chapter was to provide a background to nuclear physics so that one can understand how nuclear power plants operate and their main features. The next step was to introduce the various kinds of NPPs and how they are operated.

CHAPTER 3

3 Plant Operation and Safety Considerations

3.1 Introduction

The objective of this chapter is to introduce the various important components of the nuclear industry, the utilities, the regulator and a key industry organization (INPO). The chapter will cover how the industry it is organized, how it operates and is regulated. This latter function is critical to ensure that the industry operates safely and does not lead to harm of the public. This information is a required part of the background needed to help formulate a cybernetic model (VSM) of the organizations, which covers both safety and economic aspects. A cybernetic model of an organization is more than the hieratical layout of an organization, it reflects the dynamic character of the organization, its control rules and decision-making, communications and planning functions to ensure its financial and safety viability. The dissertation is primarily concerned with management control and decision-making in the nuclear industry, but the ideas can be applied to other HROs. Of particular interest are changes in how the industry operates that has occurred over the years and how these changes were due to actions taken in response to accidents. Inherent in the design of Nuclear Power plants (NPPs) is the need to ensure that weaknesses in the design do not lead to unacceptable releases of radioactive materials, which endanger the public. Designs are tested using a set of accidents along with certain equipment and human failures. The processes used in the design of NPPs have evolved over time as more experience has been gained. The designs of NPP have been scrutinized more closely and use of probabilistic risk methods has been invoked, so that the designer's focus on where the risks really reside. The balance has changed from large loss of coolant accidents to accidents like the steam generator tube breaks, since the risk of the first item is assessed to be much lower than for SGTR. These things are part of the evolution of the industry and there is a need for the nuclear organizations to reflect what has occurred in both structural and operational processes. Later in the chapter the importance of accidents is considered.

3.2 Organization of the Nuclear Industry

This section introduces the elements that make up the industry from the operating utilities, the regulatory authority (US NRC), the Institute of Nuclear Operations (INPO) and even the US Congress/President of the United States, see Figure 3.1.

The Nuclear Regulatory Commission (NRC) has been formed by the Congress to regulate the Nuclear Utility industry to ensure that the industry operates safely. The NRC Commissioners, of which there are five) are appointed by the President. The current

President has appointed three of the Commissioners and appointed one of the Commissioners to be Chairman. The Commissioners are supported in their position by some 4,000 NRC employees, performing different tasks from research to site inspectors.

Nuclear Power Plants (NPPs) are licensed by the NRC to operate and they are run by different utilities. Some utilities have a number of NPPs and others have few. Each NPP has to be run by licensed operators. The NPPs are built to strict standards and maintained to rules defined by the NRC, such as Design Basis Criteria, Maintenance Rule, etc. One of the fundamental US safety requirements for reactor power plant installations is the concept of 'Defense in Depth.' The US developed this concept early in the development of Nuclear Power and relates to reducing the pathway for radioactive materials to get into the biosphere. There are three components; the containment of the fuel ('cans'), the reactor vessel and then the containment, which encloses the reactor and associated equipment.

In addition, there is another organization set up by the utilities to monitor and train utility personnel, so that operational standards across the industry are held to a high standard, and are encouraged to improve their performance. This organization is called the Institute of Nuclear Operations (INPO), set up in Dec. 1979) see www.INPO.info.

There are also other professional organizations that generate standards that are used by the industry. Standards have a long history in history and usually reflect current practice, such as boiler standards codes and wiring standards; such as organizations like the American Society of Mechanical Engineers (ASME), Institute of Electric and Electronic Engineers (IEEE), American Nuclear Society (ANS), etc. In the nuclear industry a number of key standards were generated to help designers and were based more upon the thoughtful deliberations of industry experts and established 'good' practices, rather than the development of good practices over time. The NRC reviewed these standards and mostly accepted them under the guise of regulatory guides. The early days of the industry, it was the industry (reactor designers) that had the expertise rather than the regulatory staff. Over time this relationship has changed as experts have joined the NRC.

The utilities are influenced by a number of different organizations, such as public utility commissions whose job is ensure that the public has access to inexpensive and reliable power. There are other organizations which have a role in dealing with the utilities to affect some aspect or other of their operation. Figure 3.1 depicts the inter-relationships between the utilities and other organizations, such as Occupational Safety and Health Administration (OSHA), Environmental Protection Agency (EPA), etc. Like most companies, there are the company officers, Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) and

Board of Trustees/Governors (Board). Later in this chapter details of the NRC and INPO organizations will be covered, along with a representative utility.

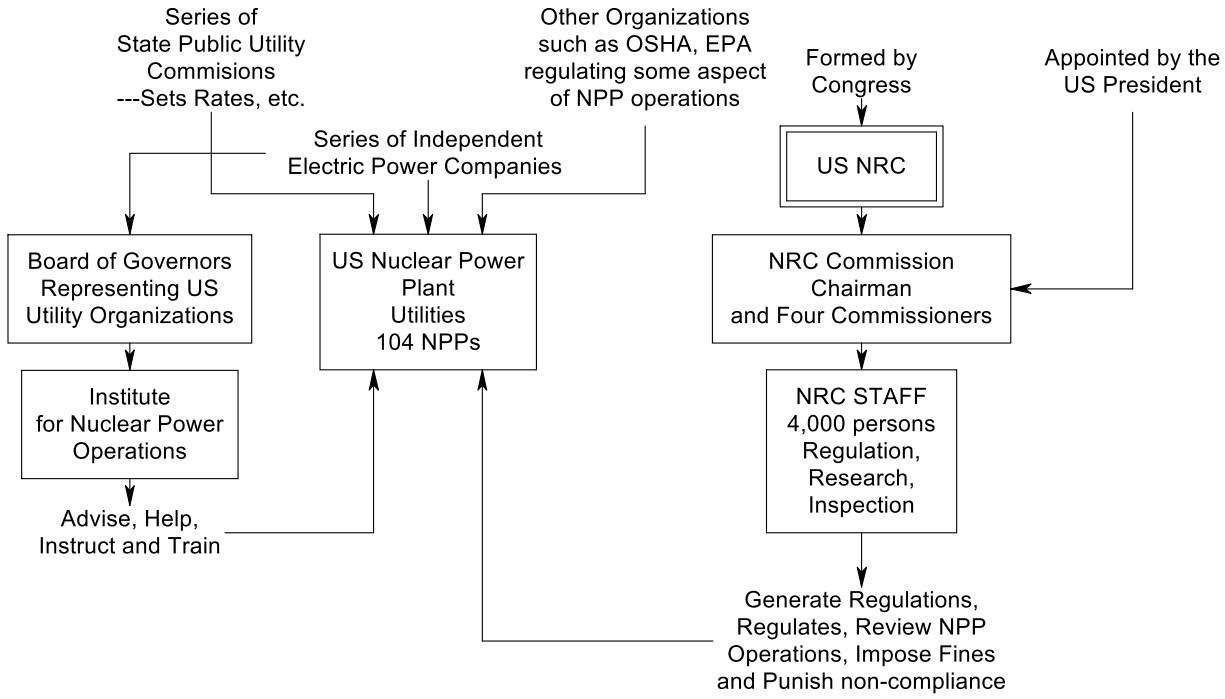

Figure 3.1 Diagram showing the Interrelationships within the US Nuclear Industry

3.3 Examination of Key Utility Functions

This section of the chapter is concerned with a more detailed examination of the roles of the various management levels within a utility covering maintenance and plant operations. Figure 3.2 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 (IAEA.1998) captures the management structure in an idealized form. One of the authors of the report is a very experienced person having served as a Training manager at a US NPP, as a consultant and later as a Vice President at INPO.

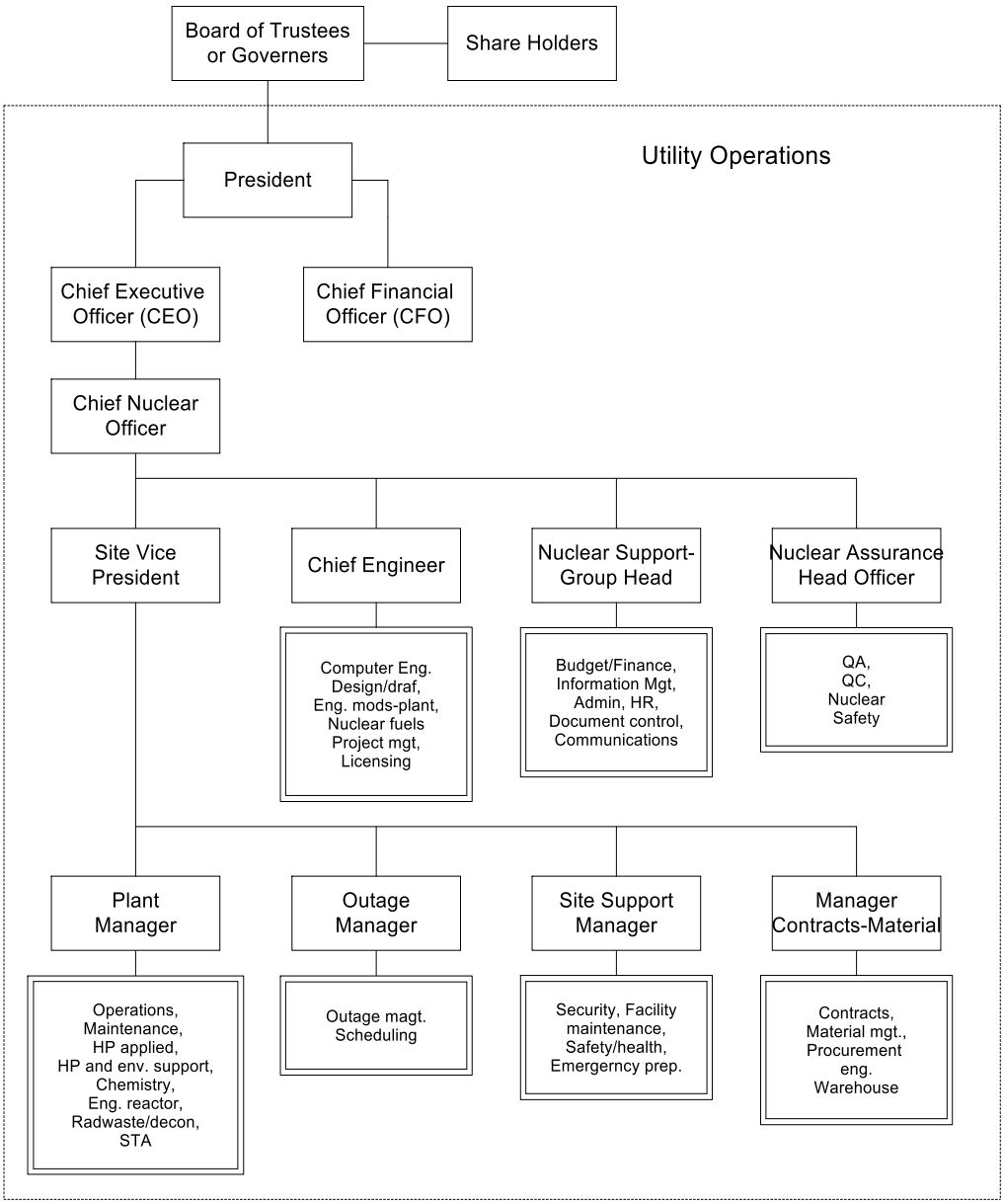

Figure 3.2 Typical Nuclear Power Plant Organization

The figure reflects 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 the Fleet organization. The 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, both 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.

The Figure 3.2 shows that there are four main functions the site: Vice President covering plant operation, the Chief Engineer covering engineering matters, the Nuclear Support Group Head, in charge of nuclear support and the Nuclear Assurance Head Officer in charge of nuclear assurance aspects.

Reporting to the site Vice President are the following: the Plant Manager, who has the responsibility for day to day plant operations, including control-room and plant operations staff, maintenance, health physics personnel, chemistry personnel, reactor engineers and Shift Technical Advisors (STAs) and radiological waste; the Outage Manager, who is responsible for outage planning and control of outage staff (including outside personnel); the Site Support Manager, who is responsible for site security, plant facilities (storage, etc.), industrial health/safety and emergency planning; and then there is Contracts Manager covering contracts, materials, procurement and warehousing.

Clearly, a number of the departments are not directly concerned with safety or economic issues. If one is interested in safety issues; one becomes more interested in how the reactor control room operations are controlled or how maintenance of critical equipment is organized. Figure 3.2 symbolically shows the relationships between the various departments in the plant organization as they relate to maintenance and control room operations, which come under the control of the Plant Manager.

3.3.1 Maintenance Operations

Normally maintenance activities are planned activities and depend upon the estimation of what needs to be carried out to keep the plant operating safely. Failures of equipment are important from both an economic and safety view point. Failures can be an initiating event and also so-called latent failures, which can increase the consequences of an event. The maintenance operations are one area that has increased in importance over time, so much so that the US NRC has introduced a ‘Maintenance Rule’ 10 CFR 50.65 (NRC, 1991). Of particular concern was the number of plant transients and scrams due to balance of plant systems and components. Implementation guidance was produced by NUMARC 93-01, ‘Industry Guidelines for Monitoring the Effectiveness of Nuclear Power Plants. The NRC confirmed the guidance with regulation guide (RG 1.160). Later, Nuclear Management Resource Council (NUMARC) was replaced by Nuclear Energy Institute (NEI).

A Nuclear Power Plant can be considered to be broken down into Systems, Structures and Components (SSCs). Typically these SSCs consist of combinations of valves, pumps, electrical power, detectors/sensors, compressed air lines, compressors, and connecting pipe work. These are components that function together as systems. There are also structures, which support these systems and components. All of the SSCs support the production of power in one way or another and maybe directly or indirectly involved with the safety of the plant. Each of these SSCs needs, at some time or another, to be maintained in order that they continue to work efficiently and continuously. If the consequences of SSCs failure are unacceptable on economic or safety grounds, then techniques are used to predict when SSCs should be removed from service, maintained and then returned to duty. The practice of maintenance has changed over the years and now the two main processes are prediction of failure rates and condition monitoring to yield information on changes in equipment characteristics indicating approach to failure. The first method is based upon historical data and can be modified by working conditions; the second method is based on identifying noise signals that indicate a change in state. In the case of structures, one may use ultrasonic signals to indicate structural changes that are precursors to failure, thin walls due to corrosion, etc.

The maintenance operations are in constant motion, monitoring SSCs, planning maintenance activities, coordinating them with plant output goals, so as to ensure plant availability is not reduced due to maintenance operations. Sometimes, the needs of the plant does not coincide with predicted maintenance operations and then these operations have to wait till the needs of the power network become less pressing and maintenance operations can go ahead. Figure 3.3 shows the relationships between some of the top management positions (CNO, Plant Manager, etc) and lower level supervisors and operators.

The figure shows the case of a problem being detected during operation. In the case of a planned maintenance operation, all of the pre-requisites related to the actions needed to be taken established. These actions are planned and include answering questions such as does the plant need to be shutdown, i.e. presents a hazard to the public. The planned activities are reviewed not only by the maintenance department but by other departments to ensure that the entire operation is safe.

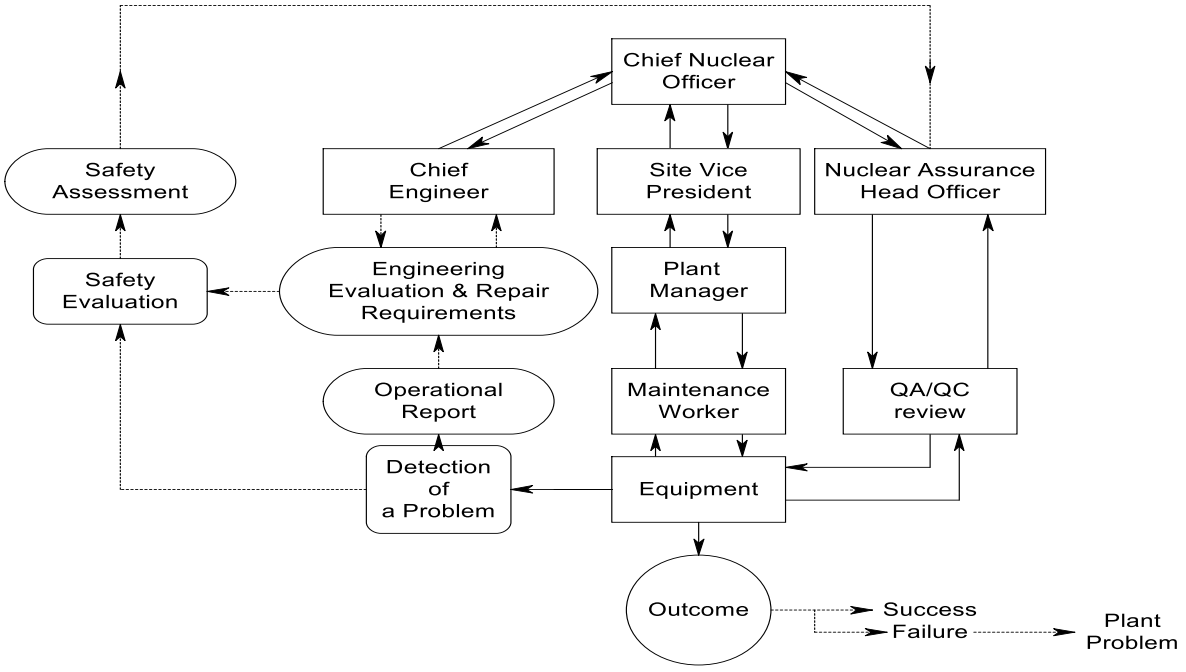

Figure 3.3 Symbolic Maintenance Operations

A whole bunch of different technologists can be involved in the process including: radiological technicians needed, and test personnel. Also depending on the maintenance task, the following maybe involved: mechanical, electrical and I &C personnel. Before starting a maintenance operation, it has to be coordinated with operations to try to schedule the operation so as not unnecessarily impact the station's output or fail to coordinate with local power distribution system (grid). The control room operators should be informed before any operation is carried out, since they are responsible for the safety of the plant. Depending on the maintenance activity key safety components maybe affected and these bring into effect certain rules relative to continued operation of NPP. These rules cover limitations of operation, for example if a particular pump is not returned to service within four hours, the NPP has to be shutdown. The control-room staff is very informed about these limits and also the use of a Probabilistic Risk Assessment (PRA) to determine if there is an increase in the unacceptable plant risk due to maintenance operations. The control-room staff puts labels on affected equipment controls to avoid incorrect actions.

In addition to planned maintenance activities, there are also activities involving maintenance personnel. For example a pump may fail, its failure is detected by the control room crew and they shut down the system and report it to their management and produce a report. The situation is then evaluated by engineering and a plan is developed with the participation of maintenance personnel. The action plan is reviewed and the maintenance personnel are

either told to proceed or otherwise. Depending on the importance of the problem, a safety evaluation is made and the results presented to the CNO and others for decision. Other parts of the organization maybe called upon to perform additional analyses, such root cause analysis.

In the case, of safety issues the incident is reported to NRC and the local NRC inspectors are kept informed. There are both utility and NRC rules related to the processes and procedures for reporting events, and actions taken by the utility. The NRC is always interested in how the failure came about and whether the utility was prudent in trying to avoid impinging on the safety of the plant and thereby increasing the risk to the public.

The utility is held to high standards so as not to increase the risk to the public when operating the plant. They are also required to produce electric power reliably, so they do tend to take steps to keep the plant on-line whenever possible. Also, the NRC sees random trips as a measure of poor NPP operation. Behind this idea is that if the plant gets out of control of the operators an avoidable reactor trip occurs. The operators are charged with keeping the NPP under control at all times. Of course, occasionally something unexpected occurs, like a large tsunami. Here the actions of the crew and station staff are required to safeguard the public by their actions, even if there is consequential damage to NPP and its equipment.

Figure 3.3 shows divisions and departments within the NPP organization as it involves maintenance operations. There are a lot of both feedback and feed-forward paths in the whole organizational structure. Some of the separate roles are indicated, such as safety evaluation, QA/QC review, etc. The whole structure for running any NPP is very similar and is made up of similar groups, but whose functions may vary. Also, the exact relationships, functions and rules applied at any given time may depend on the incident being covered. Even the balance may change, with one group taking the lead in one case and having a supporting role in another case. In a later chapter of the dissertation, case histories are examined to see how organizations function and how the effect of good/poor communications, understanding of the operating rules of nuclear reactors, and leadership of the NPP play a key part in the responses.

The analogy to a process controller can be seen from the both figure 3.3 and the discussion. The man-machine organization show here is very much like a variable multi-path complex control system with the top level control objectives being running a safe plant producing economic electric power. The various pathways have different functions, some are associated with the control of direct actions, some are associated with determine the best strategies to use and others to ensure that safety is not impacted. In the case of a purely

commercial organization, the risk factors considered would be associated with the impact on the market and its economic impact, not on the safety of the public.

3.3.2 Control Room Operations

Control-room operations are normally concerned with making sure that the power plant is producing power corresponding to the needs of the electric power grid. The operators receive instructions from grid operators, who use power predictions, to match grid needs to power production. The grid operators try to ensure that the grid load distributions are met and power lines within the grid are not overly stressed, which could lead to line trips. The control room operators are not exposed to accidents very often, but are trained to respond as required.

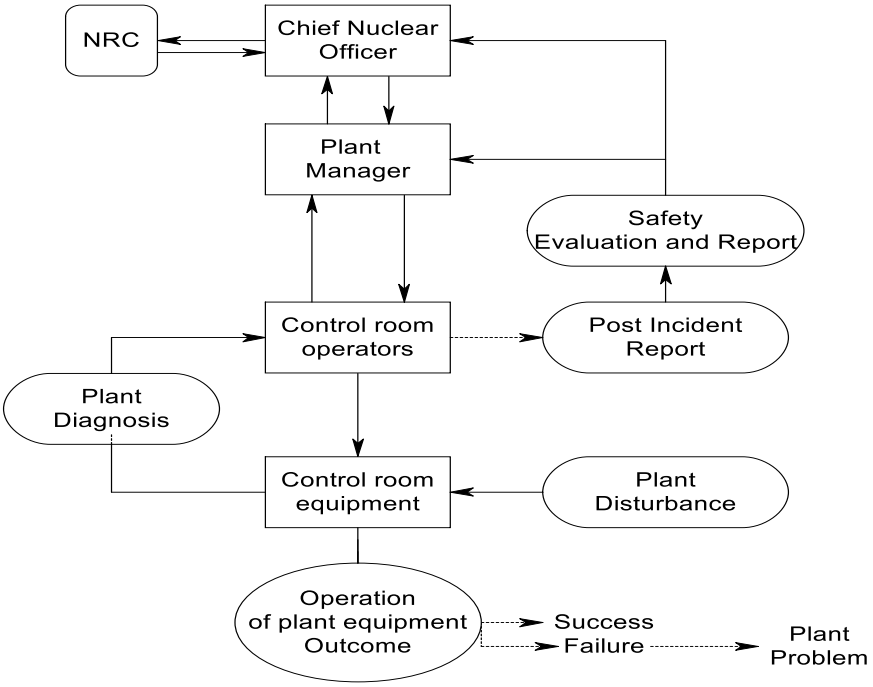

Figure 3.4 Symbolic Control Room Operations

Figure 3.4 shows the relationships between various management and control room operations as they respond to an accident or incident. The impact of the disturbance upon the plant is seen through the changes on the main control room indications and the responses of control room operators standing watch at the power plant. The operators take actions based upon these indications and alarms. Their actions are informed by their experience, use of emergency and abnormal procedures (AOPs/EOPs) and training they have received on full scope power plant simulators.

The control room crews are the personnel charged with responding to accidents or incidents, since they hold plant operating licenses. In cases when the situation goes on for a long time, the current crew is replaced by other control room crews, who also hold licenses. Management is not allowed to interfere with the operation. Information does flow from the crew to the plant manager and the CNO on the state of the plant and progress getting things under control. Depending on the duration of the emergency, the NRC will be informed of the situation and progress by the CNO. Certainly, the NRC local inspectors will monitor the situation and also inform the NRC head quarters.

There is a tight feedback path from the change caused by the accident initiator to the power plant and its response to the displays to the operators, who then take action. However, there are other feedback loops involving plant managers and other personnel and the NRC. These loops are not directly associated with accident control, but do result from the accident process and they are much slower in their response. The purpose of these loops is twofold; first to see if the consequence of the accident calls other resources, during the operators can call for the NPP staff to be evacuated along with informing local police and authorities to the possibility of evacuating the public to safer locations and secondly learning from the accident to improve operator performance in the case of future accidents by making changes in training, procedures or displays/controls. Figure 3.5 shows another illustration of the process. The long term feedback loops, in the case of control room operations, actions taken maybe to introduce changes in the tools that the operators use to control or mitigate the effects of accidents.

NRC role is to pressure the utilities to take action to correct what has happened by the use of fines and other punishments. More about the role and actions taken by the NRC are covered in detail later in the chapter. The NRC assumes that the utility should have been aware of the potential weakness of the ‘control’ processes before the onset of the accident initiator, hence the imposition of the fine or other punishment. This process works on the belief that without this kind of pressure a utility may not look for ways to improve current ‘control’ processes. This process has been in operation for a long time and appears to have worked, but is there a better way? INPO try to make the utility management aware of limitations in control room operations during their reviews and earlier plant contacts, relative to training, procedures and displays. INPO views are known by the plant management but they may not have acted on those recommendations before the accident! It does appear that INPO is normally proactive, whereas the NRC is mainly reactive.

Apart from the long term feedback paths mentioned above, the organization can influence how the performance of the control room operational control is carried out. Figure 3.5 shows

how the management decisions can affect control room crew performance. From prior studies into the reliability of operator performance [Spurgin, 1990], the following features have an effect on performance: how information is presented to the crew, the quality the emergency and abnormal procedures (EOPs and AOPs), the quality of the training given to the crews and the selection of personnel. By quality of the EOPs and AOPs is meant both the technical quality of the information but also how information is organized to assist the crews to take the required actions with minimal errors. By training quality, one means that the crews are prepared by the use of appropriate methods, i.e. exposure to simulated accidents, introduced to plant and reactors dynamics by lectures to give them insight into how NPP behave during accidents and they should be introduced into both the how and why EOPs and AOPs can help them cleanly recover NPPs after accidents.

Of course, decisions taken relative to certain items above may not have been made by the current management team. However, it is up to the CNO to ensure that the lower level managers and supervisors are always keen to discover possible weaknesses in any of the key items which affect crew performance. Data taken during simulator training exercises can reveal possible drifts and changes in the optimal performance of the crews. It does seem that NPP managements have not really understood the value of data collected at simulators as far as operator effectiveness, Training Department efficiency and the impact of control room displays on operator performance is concerned.

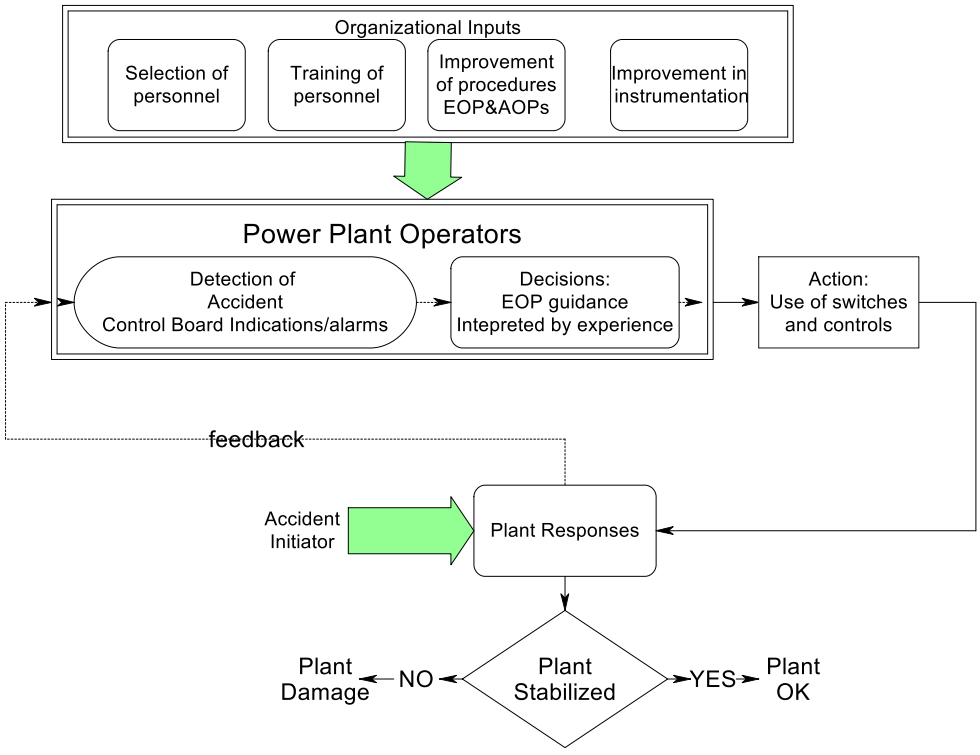

Figure 3.5 Organizational Inputs that affect Control Room Operations

3.3.3 Review of Maintenance and Control Room Operations

There are differences between how maintenance and control-room operator responses are seen from a control point of view and this also reflects attitudes to immediate and later needs of the power plant and the plant management. As far as both normal and emergency operations are concerned the control-room operators are expected to be in control of the reactor at all times.

Of course, sometimes as mentioned above the power plant is producing steadily producing electric power at these times the control-room crew is just monitoring the plant and possibly making minor adjustments. They become more involved when something is happening from changing power or responding to accidents/incidents. The long term control loops seen in figure 3.5, such as the use of emergency procedures and the safety evaluation after the accident come, into play after something untoward has happened.

In the case of maintenance operations the short term loops come into operation after the long term loops have decided what needs to be done and how it should done. A large amount planning goes on before maintenance activities are undertaken. Figure 3.3 shows the various departments who play a part in the review and planning process. The Engineering Department becomes involved if equipment has failed, to see if there is a need to change equipment or components. The Safety Department will examine both the equipment failure and the proposed maintenance process to be sure that no safety rules are or have been broken (this covers both plant safety and radiation exposure of personnel).

3.4 Nuclear Regulatory Commission

The NRC Regulatory Commission has five main components that enable them to regulate effectively: Developing Regulations and guidance for licensees and other applicants (not of interest here), Figure 3.6.

1. Licensing utilities to operate NPPs
2. Oversee NPPs to ensure licensees comply with license requirements
3. Research is also covered by the NRC to provide insights into the causes of accidents.
4. PRA techniques are also used to support commission decisions
5. The NRC evaluates operational experience, and event assessment

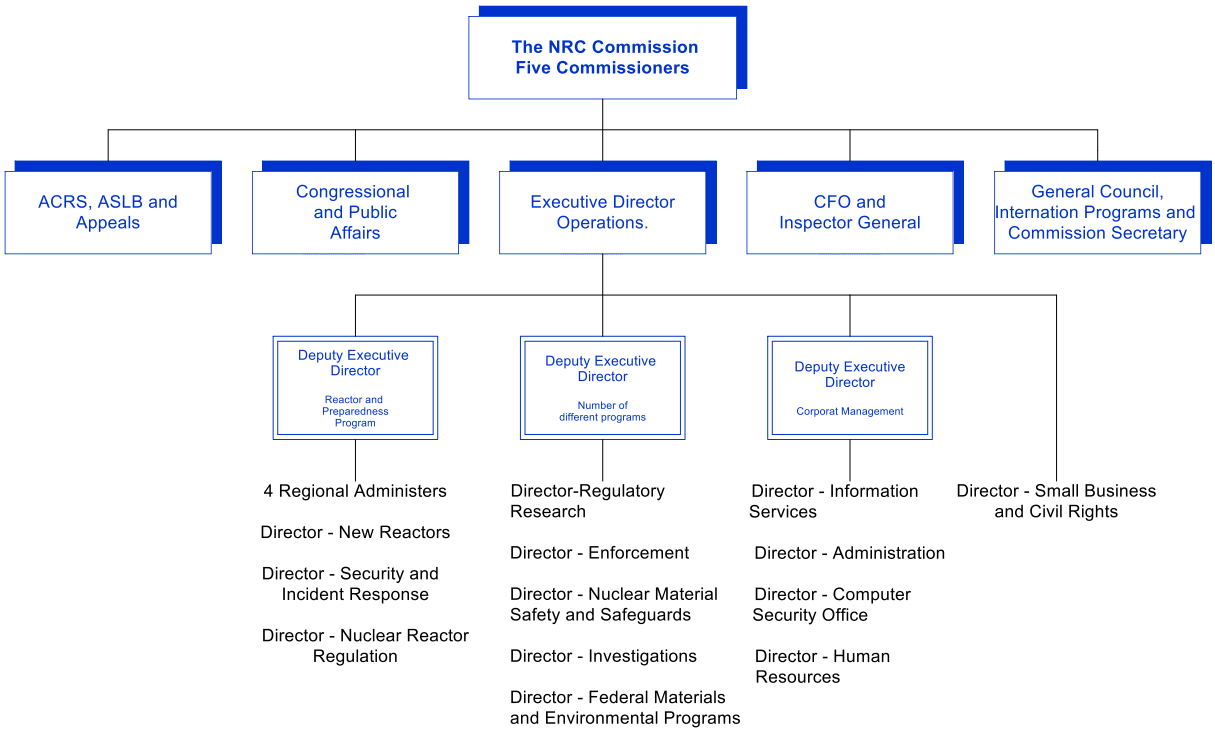

Figure 3.6 Chart of the NRC Organization (www.nrc.org)

The NRC has some 4,000 persons involved in its work, plus being able to call upon support from the US Government Research Laboratories and consultants, if needed.

3.5 Institute for Nuclear Power Operations (INPO)

INPO was set up by the NPP utilities in 1979, after the TMI accident (March 1979) see Kemeny report (1979) 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. See appendix A for a summary of Admiral Rickover’s philosophy relative to nuclear plant operations. Although the Admiral was concerned with submarine operations, much of his approach applies to the civilian NPP operations. Many of the leaders of INPO have come from the Nuclear Navy and Rickover’s philosophy has influenced INPO approach to 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)

The World Association of Nuclear Operators (WANO) is in many ways an offshoot of INPO, although it is a separate organization with centers in London, Atlanta, Moscow, Paris and Tokyo. WANO was established in May 1989 in response to the Chernobyl accident. WANO's mission is similar to that of INPO:

"To maximize the safety and reliability of nuclear power plants worldwide by working together to assess, benchmark and improve performance through mutual support, exchange of information and emulation of best practices". ***(www.wano.org.uk)***

In the formation of INPO, the utilities, in the words of Joseph Rees (1994), felt like they were 'Hostages of Each Other," in other words they reasoned if one utility failed and led another big accident (here they were referring to the Three Mile Island accident that occurred in March 1987), the nuclear utility business would be shutdown in the US. So they reasoned that they had to set up an organization to help enhance safety to try to ensure that did not happen. Incidentally in so doing led to improved NPP availability. The improvement in performance was from ~ 60% to >90% availability. This implies that safety is an integral part of business and not an either/or case with profitability.

INPO has four main activities:

1. Plant Evaluations, INPO teams observe NPP operations, analyze processes, 'shadow personnel' and question personnel. From these actions the teams assess the following:
    a. Knowledge and performance of plant personnel
    b. Condition of systems and equipment
    c. Quality of programs and procedures
    d. Effectiveness of plant management

Additionally, INPO also conducts corporate evaluations focusing on safety and reliability aspects

2. Training and Accreditation, the INPO National Academy for Nuclear Training provides training and support for nuclear professionals
    a. INPO holds training courses in the Atlanta training facility
    b. Evaluate the individual plant training program; identify individual strengths and weaknesses and recommends changes.
    c. Selected training programs are accredited through the Independent Nuclear Accrediting Board
3. Events Analysis and Information Exchange

a. Assists in reviewing significant events at NPPs

b. Through INPO information exchange and publications, it communicates lessons learned and best practices in the nuclear industry

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.

3.6 Safety of Plants: Design Criteria

One should appreciate that the safety of a NPP depends not only upon the organization and management but also on the design and construction of the NPP. Earlier, persons focused upon the reliability of equipment but now one must take a holistic view of all aspects of design, operation and construction, this includes training, selection of materials, and testing. This holistic view of the components of safety can be symbolically represented by the following equation.

> Pr (success) = F (power plant design, choice of materials, environmental impacts, operational rules, number of efficiently trained operating staff needed, management decisions) ---------equation 3.1

If one analyses the above equation one sees that susceptibility of a NPP to fail can be attributed to various aspects: such as the design of the NPP, selection of materials and the continuous review of their conformance to the duty, selection and training of sufficient personnel to run the plant safely, the ability of the plant to overcome environmental effects, like winds, earthquakes, etc. and the NPP being run by educated management making the correct short and long term decisions. The following sections will address the needs and requirements of the utility in conjunction with the NRC and INPO to address these issues. One must not forget the role played by the plant designers and constructors to understand and implement the Design Criteria layout in 10CFRpart 50, Appendices including Appendix A.

As mentioned above the regulatory authority in the US is the NRC. The legal document covering the licensing, construction and operation of nuclear plants is contained in 10 Code of Federal Regulations Part 50, ‘Domestic Licensing of Production and Utilization Facilities’ and its appendices. 10CFR50 covers up to parts from 50.1 to 50.150 (there are gaps).

There are appendices from A to S. Of the appendices is 10CFR50, Appendix A, General Design Criteria for Nuclear Power Plants. A couple of other Appendices might be mentioned are Appendix R (Dealing with fire) and Appendix S (dealing with seismic events). This does not mean that some of the others are of lesser importance, but rather the wish to point to these three for consideration here.

The aim of 10CFR50 is to cover all aspects associated with licensing of nuclear facilities and therefore has to cover a large number of topics, such as construction permits (50.35), power plant Technical Specifications for operating the plants (50.36), combustible gas control (50.44), notification of change in operator or senior operator status (50.74), etc. Some of the requirements cover different conditions of the plant life, but the utility and its associated partners have to be aware and respond correctly. There are two types of license one should hasten to add, of course NPPs but also medical facilities and R & D centers where radiological issues pertain.

As far as a NPP design is concerned one should be interested in 10CFR50, Appendix A: General Design Criteria. The document covers the following"

1. Overall Requirements
2. Protection by Multiple Fission Product Barriers
3. Protection and Reactivity Control Systems
4. Fluid Systems
5. Reactor Containment
6. Fuel and Reactivity Control

The document set up some 64 Criteria: from Criterion 1 referring to quality standards and records to Criterion 64, which refers to Monitoring of radioactivity releases. There are a number of interesting criteria, such Criterion #2: Design Basis for protection against natural phenomena (earthquakes, tsunamis, etc.), Criterion 11: Reactor inherent protection, nuclear feedback characteristics should tend to compensate for rapid increases in reactivity, Criterion 17: relates to Electric Power Systems, includes core cooling and containment integrity maintained in the event of postulated accidents related to the need for power sources and batteries. Some of these are mentioned here since situations will occur later to a need to understand the limitations of the criteria relative to some accidents. These criteria are often re-examined; the last time that the GDCs were examined was in January 12th, 2012, very recently!

Many of the key items mentioned in the GDC were contained in an early key document related to the design of reactor instrumentation systems, IEEE 279, published initially in

1968. This document covered the single failure criterion, testing, quality requirements, separation of systems to enhance reliability, independence between control and protection activities, containment penetration requirements, etc. In fact, at one time; this document was listed in 10CFR50 requirements.

Many of the aspects covered in the GDC are described in the discussions related to the descriptions of the plants, see Chapter 2. The concepts of multiple barriers, fuel cladding, reactor vessel and containment were covered, the design of the control and protection systems, emergency systems to remove decay heat and of course the function of the containment were touched upon in Chapter 2. Most of the later plant designs have covered the items discussed in the GDC document. One of the key items in the design of any product is to see if it passes appropriate tests. In the case of a NPP, the unit has to pass certain predicted accident tests and not harm the public. Additionally, the control and protection systems are assumed to be in a partially failed state and this goes for other safety systems as well (under the single failure criterion). These systems have to pass reliability goals by having both duplicative and diverse channels, so as to reduce the probability of the risk to an acceptable number.

The accident scenarios selected to test the designs are called design basis accidents. Over the years, an evaluative tool called Probabilistic Risk Assessment (PRA) tool has come into great use to better define the risk of operation. The old and limited accident scenarios have given way to more complex accident scenarios, which are seen as being more realistic and reflect possible combinations of problems that can crop up. Section 3.7.1 covers a listing of possible accidents, these are much larger than the original accidents used as the design basis set. One should point out that reactor operators were originally tested on their responses to major breaks (Loss of Coolant Accidents, LOCA) and lesser breaks; small and medium LOCAs, Loss of Reactor Flow, Control Rod ejections, reduction in boric acid, cold water inflow, dilution of boron concentration, loss of residual heat removal, etc. These were straight forward transients and the operators had simple emergency procedures to help them at this stage of NPP development.

As a result of the Three Mile Island Accident, things became more serious in that the importance of the operators was more appreciated and the significance of the limitation of automatic protection systems to cover all contingencies. Also another outcome of the TMI accident was the appreciation that even small accidents, such as a steam generator tube rupture could cause confusion on the behalf of the operators and lead to significant accident. This led to the development of symptom-based procedures rather than event-based procedures, since what does the operator do, if he/she does not diagnose the event

correctly? The next section discusses some of the accidents that can occur in operating NPPs.

3.7 Reactor Accident Considerations

3.7.1 Introduction

As mention above the safety of specific reactor designs have been evaluated by considering a set of so-called design basis accidents. The set of such accidents are listed below:

1. Loss of Feedwater
2. Anticipated Transients without Scram
3. Bypass of the feedwater heaters
4. Small Break Loss of Coolant Accident (SB-LOCA)
5. Large Break Loss of Coolant Accident (LB-LOCA)
6. Rod Ejection Accident
7. Fuel Handling Accident (Spent Fuel Area)
8. Fuel Handling Accident (Containment)
9. Rupture of Steam Pipe (Large/Small)
10. Environmental Consequences of LOCA
11. Long Term Cooling following LOCA
12. Dilution events (dilution of boric acid content in the reactor coolant)
13. Subcriticality Events
14. Steam Generator Tube Rupture (PWR only)
15. Uncontrolled rod withdrawal (subcritical and at power)
16. Loss of Reactor Coolant Flow
17. Loss of all AC Power
18. Control rod misalignment
19. Chemical and Volume Control System Malfunction
20. Startup of an Inactive Reactor Coolant Loop
21. Loss of External Electrical Load
22. Accidental Release of Radioactive Liquids
23. Accidental Release of Waste Gas

Some of the above accidents are considered in Safety Reports considered by the US NRC and probably by a large number of other countries' regulatory authorities. As one can see, these accidents are reactor centric and tend to be accidents initiated by a single cause. Most of these accidents are 'design-basis' accidents that are used to test whether or not safety systems function to terminate or mitigate the consequence of an accident. The list

above is more extensive than the original list of design basis accidents. The earlier focus was on the primary system rather than the complete plant.

In 1975, the WASH 1400 Probabilistic Risk Assessment (PRA) was released and had been applied to a couple of plants, PWR and BWR. The PRA approach was and is different to the earlier methods of safety evaluation of plants by looking at specific accidents. PRA deals with the probability of a combination of events that may occur along with the consequence of those events occurring. The pros and cons of this approach is not discussed here, but it has become a feature of examining the safety of NPPs and other high risk operations.

There are a number of areas in the operation of NPPs that are being affected by this approach. One way is to look at how risk could be affected by the removal of a piece of equipment during operation. Another aspect has been the move from training operational personnel on design basis accidents towards multiple failure scenarios. The NRC has adopted the PRA as a significant element in its regulatory process and the utilities have also invested money in having comprehensive PRA studies for their own specific NPPs. So numerical risk awareness is something that has grown in the nuclear business in the last twenty years. Each US plant has its own plant specific PRA, which is used by operations personnel and management in assessing actions and decisions being made that could alter the safety of the NPPs. The topic of accidents and how they come about and progress with be returned to later chapters.

3.7.2 NRC Evaluation of NPP Accidents

As mentioned above in section 3.4, the role of the NRC is to regulate the industry to ensure that the public is protected from the actions of the NPP utilities that might lead to radiation release accidents and its impact on the public. The NRC has evolved a process of investigation and evaluation of incidents/accidents over the years. The method is called Reactor Oversight Process (ROP). What follows is a short description of the process, as is show in Figure 3-7. The prime purpose of the NRC is to safeguard the health and safety of the public. There are three performance areas that the NRC monitors in order to meet its mission, these are Reactor Safety, Radiation Safety and Safeguards. The NRC reviews seven areas, as show in figure 3-7. Most of the areas are directly associated with reactors and the impact of accidents and incidents. The last area is called security and is an extension to cover the terrorist actions to cause accidents leading to safety consequences for the public. This issue is not addressed here. The main review of the NRC practices is to look at the effect on the plant, personnel and environmental effects.

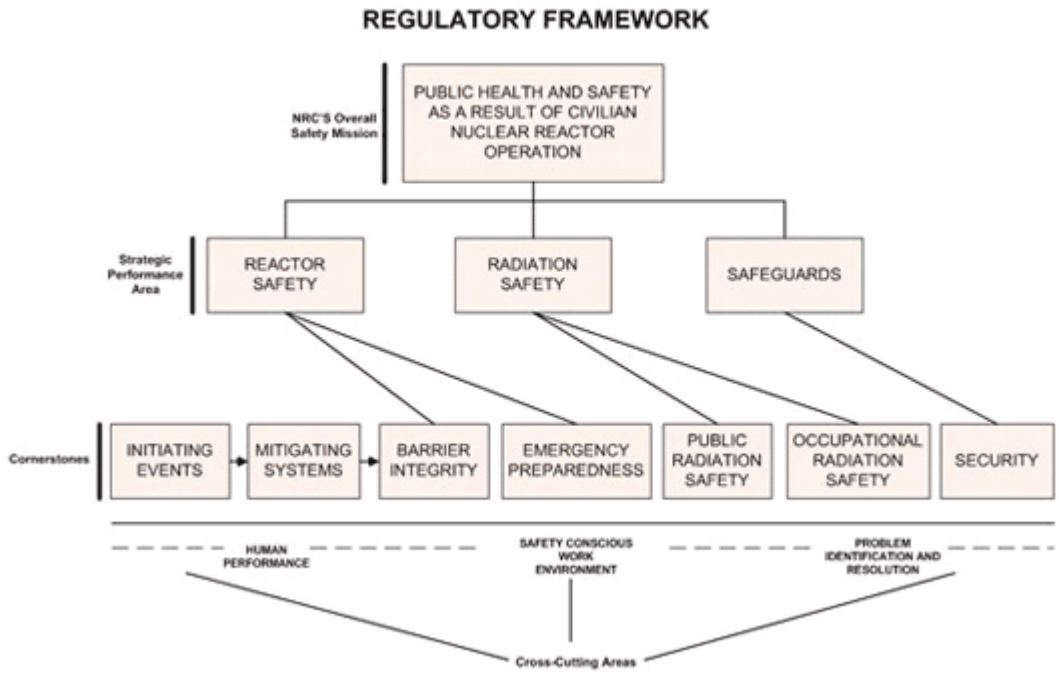

Figure 3.7 Figure shows the ROP Framework (www.NRC.org)

This is done in two ways, monitoring plant operations on a continuous basis using residential inspectors and also by reviewing incidents and accidents that can occur from time to time. The utility is obligated to declare to the NRC any deviations in operations; some are small and others much larger. If the deviation is small, the NRC usually just acknowledges the report. Other times the incident is investigated and action taken by the NRC to fine or punish the utility for this action/actions.

Figure 3.8 is a chart showing the steps in the ROP following an incident/accident. The first steps are taken by the utility responding to the incident. They should be in the termination/mitigation process and afterwards they have a responsibility to inform the NRC. The NRC site inspectors are likely to be involved in understanding what is taking place. Of course, if the situation is very critical the utility Chief of Nuclear Operations (CNO) would contact the NRC. The utility would produce a report, which is reviewed by the site inspectors to determine the severity of the incident. In the process of their review they are likely to interview the personnel involved in the situation. In the ROP process, there are several levels of activity that depend on the possible impact of the event upon plant safety/public health.

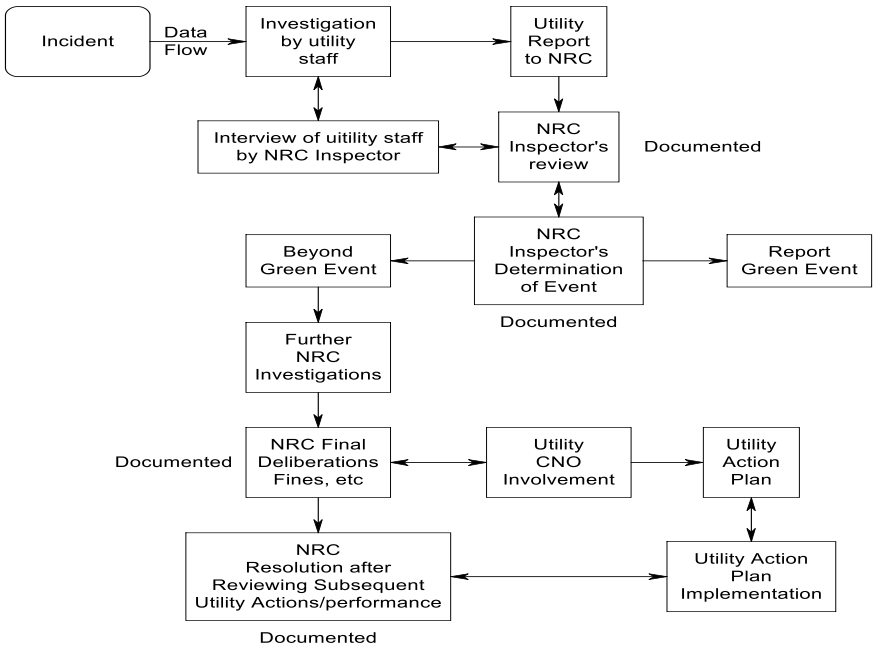

Figure 3.8 Process Diagram Depicting Steps in the ROP process

The NRC's monitoring program serves as both a short term and long term performance activities. The long term view is to have a meeting with utility management several times a year to review plant performance; every six months to identify whether plant performance is falling, twice a year to see what regulatory action is needed for 'watch list' plants and then every year to two years, the NRC performs a Systematic Assessment of Licensee Performance (SALP). This is a numerical rating in four areas: plant operation, maintenance, engineering and plant support.

The NRC has a color code system for denoting performance levels from Green, White, Yellow and Red. Depending on the combination of colors that have been assigned, the NRC has different response. The NRC also uses a term called "Cornerstone' meaning a key element in the safe operation of the facility. The NRC also refers to 'cross-cutting elements which are things that can affect more than one cornerstone element. The elements of the color coding system are shown below:

Red: High safety or security significance

This indicates a decline in plant performance that has resulted in an unacceptable loss of safety margin. However, there is still a sufficient safety margin to prevent undue risk to public health and safety.

Yellow: Substantial safety or security significance

This indicates a decline in plant performance that is still acceptable – with *safety cornerstones* (see seven items in Table 3.1) being met – but with a significant reduction in safety margin.

White: Low to moderate safety or security significance

This indicates plant performance is acceptable, but outside the nominal risk range. Safety cornerstones are being met, with a minimal reduction in safety margin.

Green: Very low safety or security significance

This indicates plant performance is acceptable and cornerstones are being fully met, with nominal risk

The NRC's assessment process covers both inspection findings as well as performance indicators (PI), which are then coupled in the evaluation process. For example, a Green inspection indicates a deficiency in licensee performance that has a very low risk. A Green PI is an acceptable performance and allows the licensee to take action before increased NRC activity is called for. However if the White is coupled with a poor PI, then action can result. White, Yellow or Red inspection or PI findings triggers can lead to increased regulatory attention.

Performance Indicators are plant related indications of issues associated with running the plant, so instances one PI could be how many reactor trips occurred in the past 7,000 hours of critical operating time? So one is looking at the possibility of deteriorating performance, The plant might go from acceptable performance to White to Green, in fact examples are given in Regulator Assessment, Performance Indicator Guideline (NEI, 2009)

Safety Cornerstone	Performance Indicators
#1 Initiating Events	• Unplanned reactor shutdowns (automatic and manual) • Loss of normal reactor cooling system following unplanned shutdown • Unplanned events that result in significant changes in reactor power
#2 Mitigating Systems	• Safety system availability and reliability • Safety system failures
#3 Barrier Integrity	• Fuel cladding (measured by radioactivity in reactor cooling system) • Reactor cooling system leak rate
#4 Emergency Preparedness	• Emergency response organization drill performance • Readiness of emergency response organization • Availability of notification system for area residents
#5 Occupational Radiation Safety	• Compliance with regulations for controlling access to radiation areas in plant • Uncontrolled radiation exposures to workers greater than 10 percent of regulatory limit
#6 Public Radiation Safety	• Effluent releases requiring reporting under NRC regulations and license conditions
#7 Physical Protection	• Security system equipment availability • Personnel screening program performance • Employee fitness-for-duty program effectiveness

Table 3.1 Relationships between Performance Indicators and Safety Cornerstones (www.NRC.org)

One can visit the NRC's web site (www.nrc.gov) and look at individual US NPP performance as judged by the NRC. One can look at listings of ROP Inspection findings in summary form for a given quarter. The summary lists finds for each US NPP for each cornerstone, for example there was one RED finding under the mitigating systems cornerstone and there were four YELLOW findings and the rest were WHITE, GREEN or no finding.

3.8 Summary

The objective of this chapter was to provide a background on how the various organizations operate together and try to ensure the safety of the public in the process of running nuclear powers. The organizational structures for the NRC, INPO and a typical utility are discussed. In particular, the key operations of running a power plant from the control room and carrying out maintenance operations are covered. As part of this discussion, the involvement of the utility in responding to plant accidents and equipment failures is illustrated. These things then lead to the role of the NRC as a regulator in responding to accidents/incidents that occur in the utility domain. A significant point of view of the NRCs activities is that it devotes a lot of attention to the slow deterioration in the performance of a utility and to help ensure that the utility has the opportunity to recover from a poor state before a more significant accident occurs.

The information contained within this chapter enables one to see how these organizations operate together in the safety domain and how decisions are made in both utilities and NRC

and how INPO is integrated into the process to enhance safety. The decision-making, communications and roles of the different groups is important in terms of constructing a cybernetic VSM and how the model of these processes has changed over the years. For example, INPO was not there before 1979 and the NRC's safety evaluation program has evolved over the years.

CHAPTER 4

4 The Viable Systems Model (VSM)

4.1 Overview

The purpose of this chapter is to present information about the Viable Systems Model developed by Beer (1985) 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. VSM is a method to be able to understand management dynamics of organizations based upon cybernetics. The key word in VSM is 'viable: capable of maintaining a separate existence.' If one considers the roles of persons in various parts of an organization, one can quickly recognize that some of them make decisions, others plan operations and yet others carryout those plans. Between these persons, 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 operational levels within humans and animals, in other words the same principles being used to understand how animals operate were relevant to the operations of human organizations. More is discussed about the internal systems and processes in a later section about cybernetics.

This chapter will also cover control systems concepts so that one can appreciate how simple controllers work along with ideas about how feed-back and feedforward signals are used in the control of processes. Some further concepts related to controls are introduced so that the jump to the complexity of cybernetics is more easily understood. Modern technology shows that more and more computers are being are being used in ways that resemble cybernetic processes. One example of this is the control of automobile engines. The automobile manufacturers have responded to the public needs by designing complex interconnected control schemes to control pollution, release of noxious gases, while at the same time increase fuel economy and increasing power output. This has been done by developing controllers acting very much like cybernetic machines.

Cybernetics is the study 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, (1964).

Cybernetics is equally applicable to organization and control of physical and social management systems. .

VSM is built upon the ideas derived from cybernetics and its application to understanding the relations of the brain and the nervous system of the human body. VSM was proposed as a better way of understanding and diagnosing organizations to understand their behavior. 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 and understanding the operation of management structures.

The structure of VSM applied to the control of organizations will be discussed later in more detail and showing the relationship to cybernetic controls of human and animals. A significant aspect of VSM is its representation of the dynamics of control. As in bodies there are brains and other parts, necessary for the functioning of the bodies, so there are managerial persons guiding the organizations and other units carrying out the operations. These persons are dynamically connected by communication channels, so responses to outside changes can be detected and acted upon.

The pathway to the development of the VSM approach starts with concepts about control and regulation of processes, passes through the development of cybernetics and its association with the human brain and the branching nervous processes controlling the activities of the body. Beer then saw the relationship of regulation and control aspects of the brain to the operation of human organizations and this led to the development of VSM. The next sections of this chapter introduce the following items: control systems, cybernetics and the human nervous system and a simple human feedback system dealing with the regulation of blood sugar control. Also covered are the different interpretations of the meaning of control. This then leads to the construction of the VSM representation of a typical industrial company.

A review of the application of VSM to air traffic management (ATM) in a foreign country, Saudi Arabia (Al-Ghamdi, 2010) is given below to depict an example of a dynamic industrial process implementation of VSM. In later chapters, VSM will be applied to the consideration of the safety of nuclear power plants as a significant element in the study, along with consideration of these aspects to other HROs.

A couple of key concepts to the field of cybernetics are covered in Beer's books: Brain of the Firm and Heart of Firm. These are the concept of variety and requisite variety. The latter

term was discovered by Ashby (1965) and its significance to the organizational field was recognized out by Beer in his work on VSM. The author only became aware of its deep significance late in his research. Although incorrect decision-making by management is the causal factor of accidents, it's the failure of organizations to realize the requirement to satisfy the Ashby's Law of Requisite Variety that leads to accidents being uncontrolled. Management's actions in reducing variety, without ensuring that the requisite variety is kept, can lead to problems. The driver for management to do this is trying to reduce the number of states that they need to control, without the knowledge and understanding behind taking this action!

To make things a little clearer the definitions of Variety and Requisite Variety are given as:

VARIETY is defined as the number of possible states of whatever it is whose complexity we want to measure, (Beer, Heart of Enterprise, page 32, Beer classic library 1995 reprint).

REQUISITE VARIETY is the least number of states (Variety) that have to be controlled for the system to meet its objectives, (Author)

It should be pointed out a system has to include the impact of the environment, in that it can affect how the system behaves. So what is acceptable from an organizational point view at one time may not be acceptable in another condition. The Requisite Variety is not invariant and can change depending on how the states change when considering the bounds of the system. If the system boundary is drawn one way, the variety is invariant and so is the requisite variety. However, if the boundary is re-drawn it may involve capturing influences which are random and affect the system dynamics. For this situation, the Requisite Variety has to be changed to reflect this new condition.

4.2 Interpretations in the Meaning of Control

The word 'control' comes up all the time in the context of VSM and the NPP environment. It should be recognized as having different meanings and these differences have different effects in the case of operating NPPs, for example the management is in control of the plant and so are the automatic controls. The control-room staff is also in control; in their case it covers plant operations. One needs to understand these differences and differentiate between them.

The NPP consists of a number of separate parts, such as the reactor, steam generators, etc, as has been covered in earlier chapters. In addition, it needs control and protection systems which ensure that the plant personnel can change power and respond to accidents in an automatic manner. In addition, the power plant personnel perform tasks to help run the plant

and to step in, when required, to help safeguard the plant and the public. The operation of the plant is controlled by the management, who job is to direct operations to run the plant economically and safely.

There are other important organizations, such as the NRC, INPO, etc, which factor into the running of the plant. Each of these organizations play an important part in the control of the plant. This section tries to clarify what each of the control systems are, how they function and the part they play in running the plant.

The plant and the various organizations, which consist of plant managers, plant personnel and outside organizations, as well as systems like the reactor protection system are all important and form a system that should be considered, as a whole, in the analysis process. The word 'control' is associated with each of them in some manner, but there are differences in meaning and are modeled differently. In the case of management, control relates to the act of directing of personnel and making decisions related to the whole operation. The impact of management control actions are often delayed in time and their consequences often seen much later. This is even truer of outside organizations, such as regulators and governments.

Time is an important influence on both analysis of developing situations and the actions that need to be taken. If management and the organization are prepared for an accident situation that is developing, then time may not be a big constraint. However, if the organization is not prepared, then the time available for analysis and taking actions may be insufficient and the ability of the organization to prevent or terminate the accident could be severely compromised.

Management is responsible for both the economics of the plant and its safe operation. For the control room personnel it is the exercise of monitoring the plant and taking manual actions in response to changes in plant state or responding to instructions from electric grid management. Each aspect covered can be associated with the word control, but the meaning of control is different in its interpretation. The reactor control relates to the automatic control system that continuously monitors the plant state and automatically adjusts the reactor control rods or other parameters to increase or decrease power. The actions of the operators tend to match that of the automatic control systems, but there are differences in the characteristics of these two 'control' processes. The automatic control system is a deterministic system, see Figure 4.3, once it is set up it responses in an identical manner to a given stimulus, Figure 4.1.

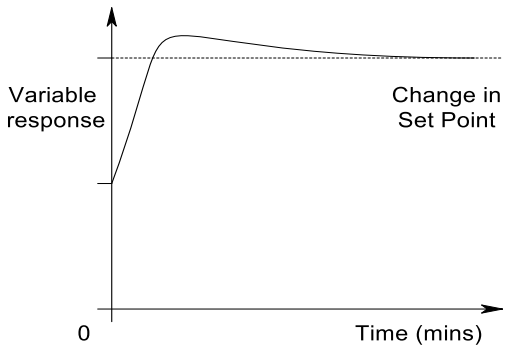

Figure 4.1 Typical Controller Response to a Set Point Change

However operator control is probabilistic, as results from plant simulators have shown, (Spurgin, 1990). Also the source of errors/failures for these two control methods is derived from different sources. In the case of the automatic control, it is related to the reliability of the hardware and software, whereas the human error cause can have both random and systematic sources. These sources can be traced mainly to management and designers.

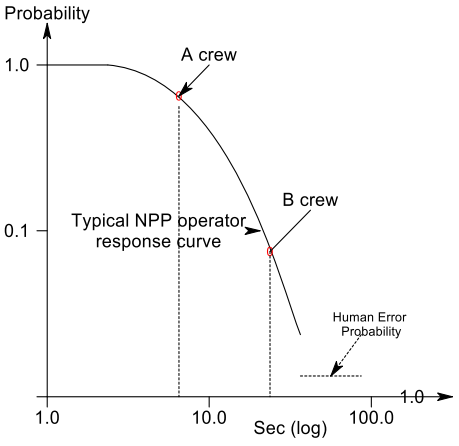

Figure 4.2 Typical Time Reliability Curve showing Operator Response Probability

A word of explanation about Figure 4.2, the Time Reliability Curve (TRC) represents the probability of any crew taking an action in response to a stimulus, such as an accident. Any crew's action should fall onto the curve, including the possibility of causing an error. So the probability of a crew taking an action increases with time. In a set of crews responding to an accident, some crews act early, crew A and others, such as crew B respond later. If the available time in a specific accident by which the crew must act is in excess of 100 seconds then in this case the majority of crews would have acted and taken the correct action in time

to prevent an accident. Figure 4.2 shown relates to the crews' response to an Anticipated Transient without Trip (ATWS) event, in which the crews are expected to respond quickly. This fast response is achieved by understanding how the transient can be terminated. This includes an understanding of the indications related to the accident and what actions must be taken to terminate the accident. Additionally, the crews must be informed of the indications and actions via procedures and then trained on a simulator to carry out these steps quickly and accurately.

In other cases, the TRC is likely to cover many minutes. In assessing the possibility of acceptable of operators taking correct actions, designers use a time window by when the crews should act to prevent damage to plant or equipment. So provided the crews act correctly before the time taken exceeds the time window, it is then acceptable. In the case of the automatic control schemes the time taken is usually much tighter, the time taken to bring the plant to a safe state is usually as quickly as possible within constrains on rates of change in power, pressure or temperature or limits in the deviation of a given parameter, like nuclear power not to exceed say 105% power.

The crews' actions are guided by procedures, which fall into the following categories: normal, abnormal and emergency. The categories relate to operating the plant in normal conditions, such load increases and decreases, normal start-up and shut-down, abnormal conditions when something off normal occurs and leads to the plant problems, such as small leak, which has to be detected and acted upon, but the plant is not in an accident. However, when the plant gets into a severe condition, it is in an accident situation and the emergency procedures have be used. The crew responds by following the procedures starting with tripping the reactor, and initiate operation of safety systems, such as fluid injection systems to keep the core covered, cooled, etc. It should be pointed out for a correctly designed safety protection system, these actions will be taken automatically and the operators act as a protection shield if the safety systems fail to act properly. Simulators are used to prepare the crews for all manner of circumstances, such as if the safety systems fail to act correctly in the presence of equipment failures or human errors. The crews during training sessions are exposed to different accident scenarios, covering even multi-failure scenarios based upon the unavailability of dynamic units, such as of pumps and valves, failure of passive components, such as feed lines, various human errors and for different disturbances, including the effects of flooding of equipment.

The understanding of the different meaning of control is important in establishing the safety of the NPPs, and what's important and expected of all personnel is to be safety conscious.

These differences will be addressed later in terms of their effect and influence. Perhaps, the singular most important consideration in control is the impact of the control activities of the top management since they can influence the resistance of organizations to the propagation of accidents and in responding to accidents.

Importantly, the management is tasked with the job of balancing safety and economics. It appears that these two aspects are closely connected. It appears that you cannot run an inexpensive NPP operation that is highly reliable and safe. Inherently, an NPP is an expensive power plant to operate when compared with a gas-fired fossil plant. The NPP is a much more sophisticated plant with multiple pieces of equipment that need to be carefully maintained and there are redundant equipments for many functions to ensure plant safety when challenged by some internal or external disturbance. The case of the gas fired power plant safety is not great requirement, since the effect of an accident to the plant has a very minimal influence on the public.

4.3 Controller Design and Operation

This section discusses the actions of controllers and compared them with company operations. Controllers receive signals from the process via transducers and sends out signals to the actuators, which in turn move to influence the system under control. A significant aspect of controllers of any type is the importance of feedback on the performance of the system. Feedback signals can be either negative or positive. Negative feedback is generally stabilizing and positive feedback is generally destabilizing. Both methods of feedback can have their uses and the choice depends on the overall behavior needs of the system performance. Even negative feedback can be destabilizing if the loop gain and phase of the process is poorly matched. Similarly, Management receives signals from staff on production levels and following evaluation sends commands to change production rates to balance the needs of the market. Incorrect or poorly timed information about the state of the market can cause bad consequences for the company.

The market needs are monitored over a period of time to see if production matches the needs of the market/public. If need be the managers issue instructions to personnel make further changes, as required. These changes are made until stability is reached implying that production is matching the needs of the market. Of course, these can change in the market raising or lowering the need of a particular product. Figure 4.1 shows how a simple controller responds to set point changes (production level) or process system disturbance changes (value of money changes). This is like a company making changes to products or responding to public shopping needs.

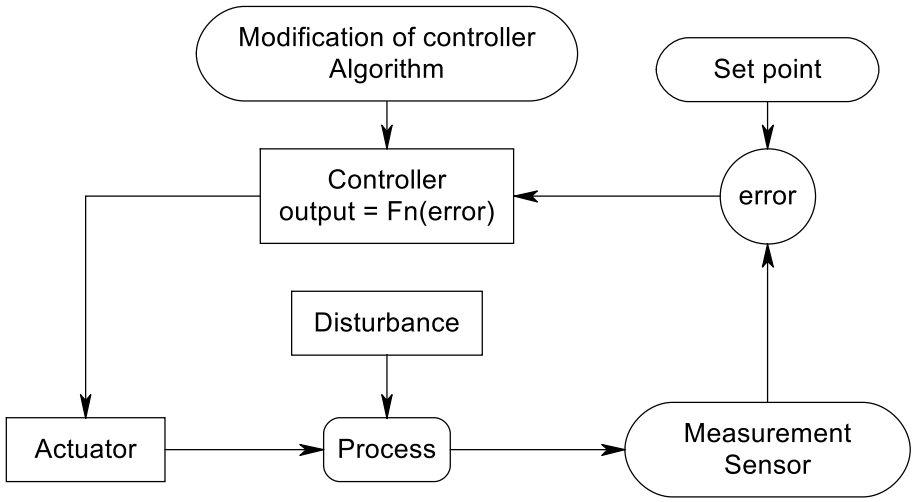

Figure 4.3 Simple One Loop Controller and Process

The components of the control system are a.) a controller that embeds the control rules {or algorithm Fn (error}}, b.) an actuator which affects the control action to produce a change in the process, c.) a sensor detecting changes in the process and d.) an input set point to demand to establish the required state of the process. The output from the sensor is the feedback signal and is compared with the desired state setting. The differences between the two signals determine the error between the current state and the desired state. The controller acts through rules to effect the necessary change in the process to reduce the error to zero and bring the actual state to be in conformity with what is desired. The most often used algorithm in process control is the PID controller, (Proportional, Derivative and Integral controller). The equation for this is:

Controller Output = a (error) + b (d/dt (error)) +c$\int$(error)dt …….equation 4.1

where: error = actual signal – set point value

a, b, and c are controller settings selected by the user to modify response to changes.

4.3.1 Controller Response

Figure 4.3 shows an approach which incorporates an algorithm adjustment process. There are many ways that the controller algorithm can be modified. One way is to do so automatically in response to changes in the process, like having different settings when the plant is at high power or low power. In the aerodynamic control of a plane, the controller algorithm could be designed to change according to altitude or Mach number to enhance stability or controllability of the plane. By this process, a plant or vehicle could be more optimally controlled and be more stable under varying conditions.

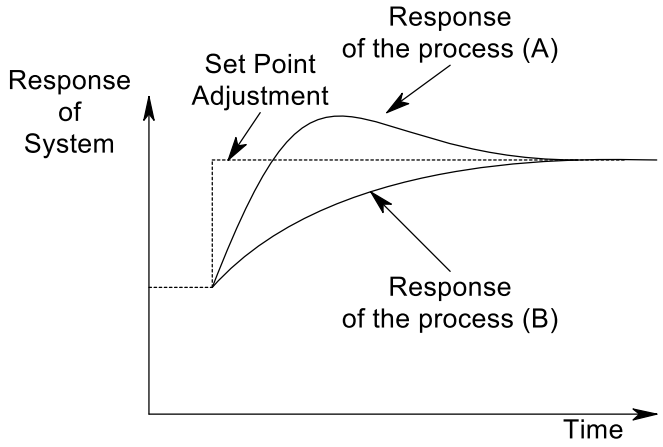

Figure 4.4 Plant responding to a set point change with different algorithm settings (A (a_1, $b_1$and c_1) and B (a_2, b_2 and c_2)

In the system shown in Figure 4.3, the actuator may be connected to a valve, whose movement causes the process to respond and changes the plant state towards the desired plant state as determined by the set point. Also, if the plant is disturbed in some manner, the controller acts to return the plant back to its desired state, and this is the value of the feedback signal.

4.4 Cybernetics

Cybernetics has developed from an understanding of control theory and issues associated with communications. A key feature is the feedback process in the stabilization of system's responses. Feedback can be negative, and positive. Negative feedback is used to stabilize processes and positive feedback tends to destabilize systems. Systems can also be 'open loop', i.e. not having any feedback paths.

Cybernetics, as mentioned above, is concerned with control and regulation of human bodies as well as industrial processes. In the early days of industrial development, simple control systems were developed, such as the fly-ball governor were developed empirically. As industrial development went ahead, systems became more complex and the field of control system design developed and started to involve mathematics to better capture and predict the performance of systems. As mathematicians became involved concepts of simulation of processes developed and ideas of stability of these controlled processes called upon branches of mathematics and the work of such persons as Lyapunov, etc.

Although control systems are getting more complex, the most complex cybernetic systems are seen in the animal world. For example Figure 4.5 is a depiction of the nervous system of the human body. The nervous system connects the brain to the various components of the body. The nerves fall in two groups; motor and sensory nerves. Figure 4.5 really focuses on the motor nerves, such as the Femoral and Median nerves, which control the movement of the legs and fingers. The motion of the legs and fingers are detected by sensory nerves and these form the feedback signals.

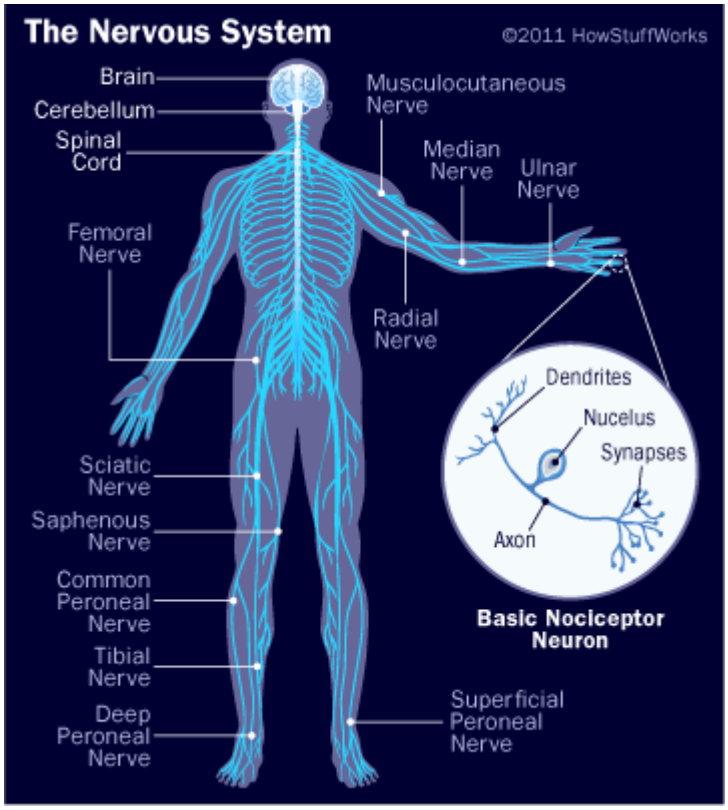

Figure 4.5 Shows a diagram of the nervous system connecting the brain to the rest of the body along with details associated with neurons (HowStuffWorks.com)

4.5 Human Body

Cybernetics covers essentially the application of mathematical processes applied to many fields including the human body. This section reviews some of the body's functions as a lead into the understanding of the development of Beer's model of industrial organizations related to the functioning of the body.

.

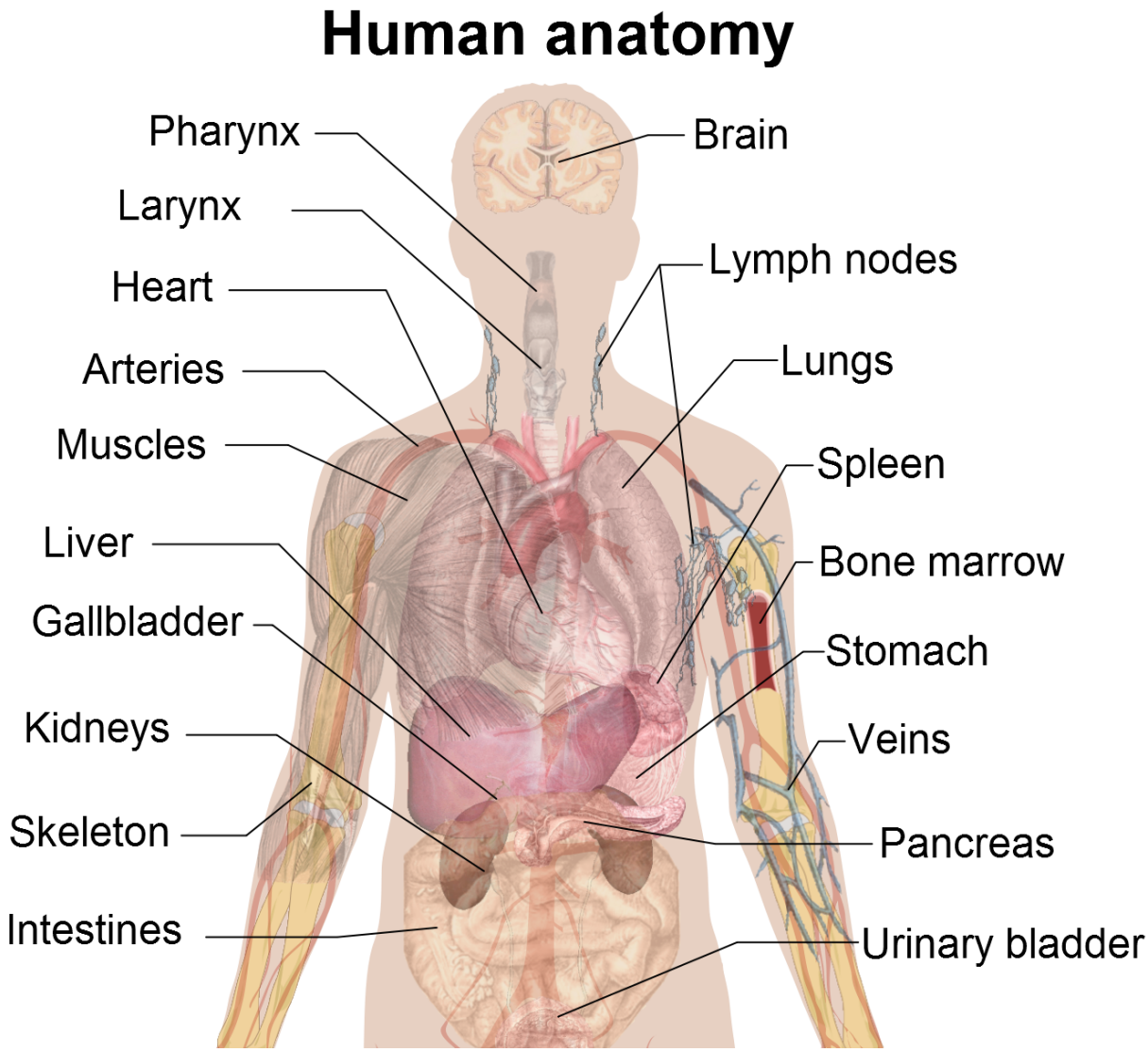

Figure 4.6 Depicts some of the internal components of the body (blissreturned.com)

The body is essentially controlled by the brain, but there are a number of autonomic functions as well, i.e. components of the body which can operate without the intervention of the thinking brain. There are other components which operate without conscious effort from the brain, how the brain can intervene to over-ride the autonomic process, such as changing the breathing rate. Figure 4.6 shows some of the components (parts) of the human body

One can see the presence myriad connections in Figure 4.5. These are motor nerves passing messages to parts of the body, for example the ulnar nerve passes signals to operate fingers. Not seen are sensory nerves passing information back to the brain relative to touch, heat and position, which in turn is used by the brain to help determine future movement instructions. It is these sensory signals that form the feedback signals to enable the various components to function correctly. Within the body components, see Figure 4.6, there are feedback signals which help the components meet the needs of the body as a whole.

Figure 4.6 shows the complexity of the human body with all of its different systems. This is not a dissertation on the functions of the human body, but rather on the functions associated with business organizations. Cybernetic analysis has been applied to systems within the human body and Figure 4.7 illustrates the regulation of blood sugar levels within the body. One can see depicted the use of various chemicals that participate in the regulation of blood sugar levels, such insulin and adrenalin. This is a very complex process that encompasses control and regulation and feedback paths to ensure the blood sugar fulfills the needs of the body under different operating conditions, running to sitting or when threatened. The various functions are modeled mathematically (simulated) and their functions can be studied and compared with actual bodily responses in clinical trials, (see some of the discussions in Wiener (1948).

Similar block diagrams to those seen in Figure 4.7 have been developed for the control of nuclear power plants (NPP) and cover the dynamics of the reactor, steam generators, pumps, valves, etc. An early study was one applied to the design of NPP controllers and to study the responses of a NPP to command signals and disturbances. Mathematic models of the plant components were developed to ensure that the control of the NPP was responsive to the needs of the station. Later, the actual station control system was tested and checked against the predicted NPP results during start-up tests (Spurgin and Carstairs, 1967).

One can imagine the development of a complex control system similarly covering the operation of a manufacturing industry integrated with requirements set by management and the equipment operated by workers. The organization can thought to function in a similar fashion to the body with autonomic features corresponding to the activities of the plant operators responding with little direction from top managers and the mental activities of the brain corresponding to the activities of the top managers.

One can use mathematical concepts to model biological processes, so feedback signals in the mathematical sense are modeled by complex equations, whereas the biological

functions that are mirrored by mathematical expresses are the result of chemical/physical reactions. For example in the formation of alcohol from sugar, there is a modification of the reaction rates due to the impact of the alcohol formation. The end result is that the alcohol concentration follows an exponential response looking similar to the response of a controller to a step change, see Figure 4.1. The response rates of the biological processes can be changed by changing certain parameters, such as the temperature.

Thus the complex human chemical/physical processes that occur in the body, such as shown in Figure 4.7 can be modeled by a series of mathematical expressions, which capture the essential responses of the various body components indicated in the figure. In the body, the connections between the body components are fluids with varying concentrations of blood laced with other elements, such a salts of various kinds. The controlling signals of detection and action are nerves of different kinds carrying electrical signals, which pass from one component to another component. In practice, the modeling of the body processes is confirmed by performing tests.

The same is true of modeling of nuclear power plants for ensuring that the designs conform to the specification for delivery of power and responses to both power demands and accident initiators. This is true of the mechanical side of the plant designs to be sure that the predicted responses are confirmed with an acceptable degree of uncertainty. This process of testing has been applied to the actions of operators, but not the response of the organization as a whole. What has been done is to produce probabilistic estimates of how the combination of plant plus staff is like to respond to a series of accidents and what the consequences are likely to be. This describes the probabilistic risk assessment (PRA) approach to safety evaluation.

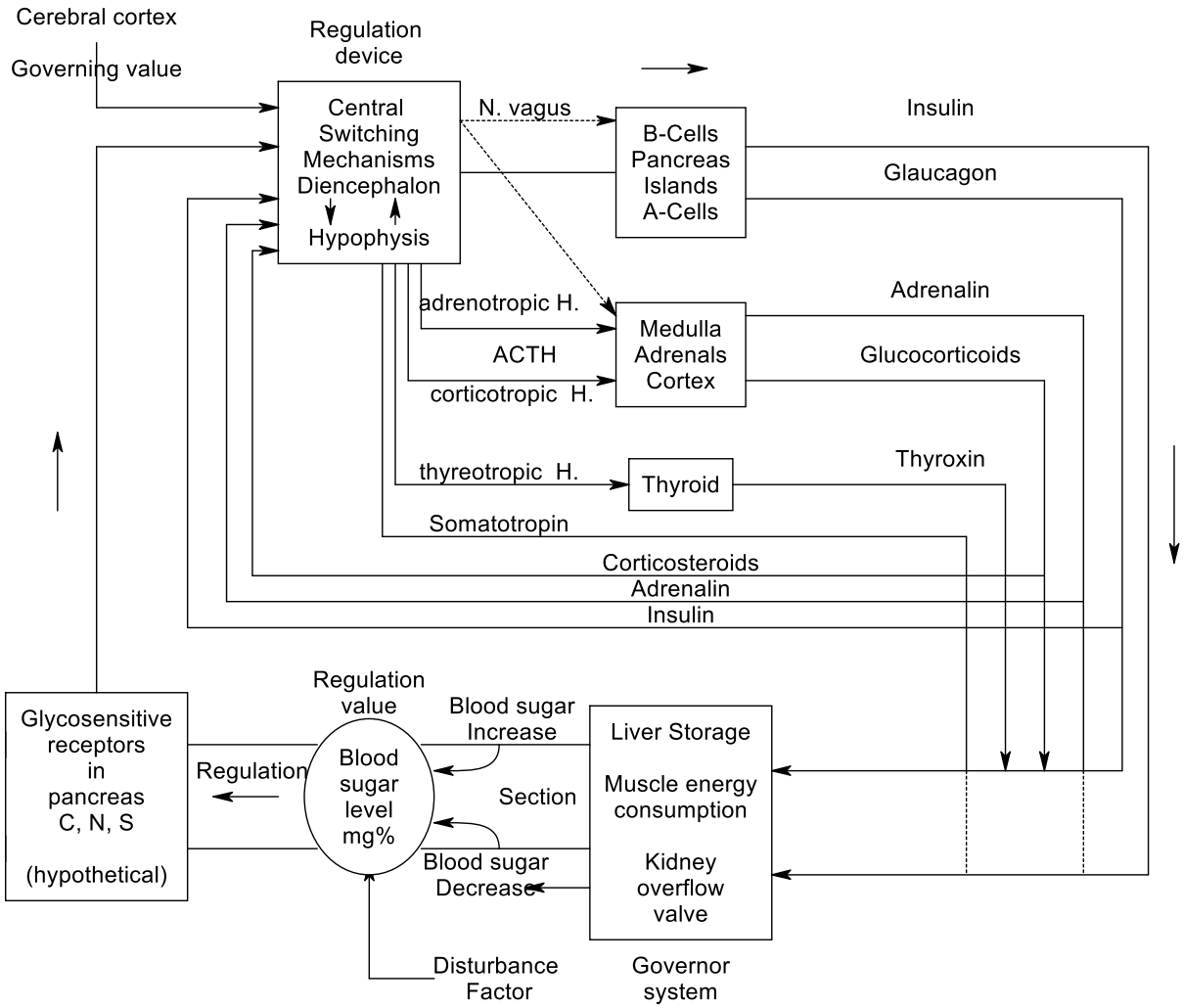

Figure 4.7 Homeostatic Regulation of the blood sugar level, (Bertalanffy,1969 after Mittlestaedt. 1954)

There are, of course, some differences between the series of activities of the brain/body and that of an organization. However, even in the case of bodily injuries or disease leading to failure of a component, and needs for doctors to intervene. Such is the case when the pancreas fails to produce insulin, The case of equipment failure is its equivalent; leading to the call for outside experts to solve production issues

Beer saw the similarity between operation of the brain, bodily components and the outside world relative the operation of industrial companies. In his book, “Brain of the Firm,” (Beer, 1981), he produced two figures; one for the brain, parts of the body and the outside world

and the other his version of a 'firm' (or company) with subsidiaries A, B, C, and D, see Figures 4.8 and 4.9.

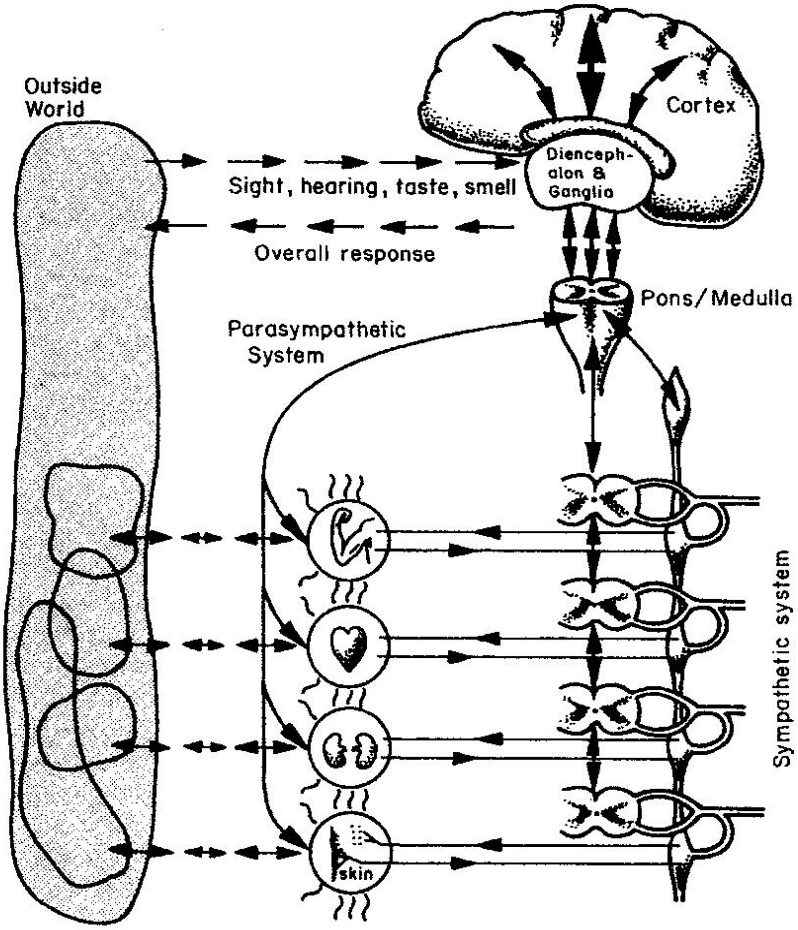

Figure 4.8 Two dimensions of the neuro-physiological control showing the vertical command system and the response systems (sympathetic/parasympathetic) (Beer, 1981)

It is not appropriate here to discuss the functions of the various components depicted in Figure 4.8 beyond seeing the relation of the brain's actions relative to receiving information from the outside world and responding to those stimuli. The brain processes the information then acts through the sympathetic system to achieve the required result. The parasympathetic systems functions to return components to normal working after actions. There appear to be multiple feedback signals covering all operations of actions and recoveries. For example, there are motor controls going the hand muscles to move the hand/fingers (Figure 4.5) and sensory nerves to provide feedback to ensure movements are as required, then there are blood vessels going to muscles to provide chemical energy and

also removing the products of muscle use. The blood is processed by the body to remove products of 'combustion', clean, purify and oxygenate and refresh it, see figure 4.7 the components of the body performing these functions, such as the kidneys, liver, lungs, etc.

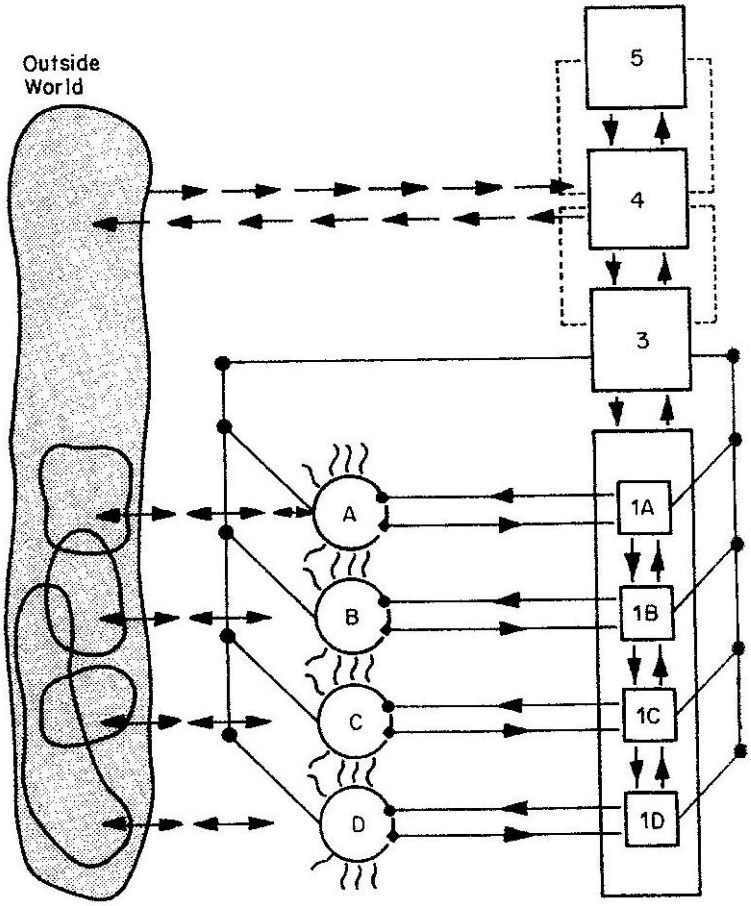

Figure 4.9 Representation of the automatic systems of a firm having subsidiaries A, B, C and D (Beer, 1981)

In Figure 4.8 one could decide that the lower sections are related to activities carried out, then next level co-ordinates and stabilizes these activities. The next level co-ordinates the messages from the top level (cortex) with outside information and passes instructions to the 2nd level, as well as receiving information from this level.

Beer's company organizational structure depicted in Figure 4.9 is an analog of the bodily functions depicted in Figure 4.8. Examination of his figure shows four company subsidiaries corresponding to the autonomic functions of the body. The subsidiaries cover separate manufacturing activities of a company. Each subsidiary has operators and supervisory personnel with operators depicted as elements A, B, C, and D and correspondingly supervisors as 1A, 1B, 1C and 1D. Element 3 corresponds to the stabilizing and

coordination aspect of the body (Pons/Medulla) and is a mid-level manager coordinating the subsidiaries and reporting to the top and upper level managers covered by elements 4 and 5. The element 5 corresponds to the top level manager deciding the current and future direction of the 'Firm' and relates to the Cortex of the body. Element 4 is a high level manager responsible for day to day operations of the company (Firm) and corresponds to the Diencephalon and Ganglia.

As was stated before Beer's model is an analog of the bodily decision and control functions of the body. The importance of Beer's analog is that it introduces the concepts of cybernetics into the field of management dynamics and emphases the aspect of control dynamics and importance of structured decision-making (separation of upper management functions from those of operations) and information flow (communications) throughout the company on the performance of the company. The model emphasizes the importance of correct feedback to enhance the dynamics of the company, much the same as having the correct algorithms for controllers associated with systems.

One weakness of the system is that it does not address the issue of improving the quality of decision-making. The information feed-back from all members of an organization can help the decision-maker, but ultimately the responsibility rests on the top decision-maker, in fact many times the top decision-maker acts against advice given, examples of this are addressed in later chapters! Later chapters do address how better decisions can be made, but the result cannot be assured.

Another important aspect for both organizations and human bodies is the time of response to stimuli. For the body there are short time responses taken by autonomic systems, like drivers responding to accidents, and long term responses to the need relocate to better environments. Similarly, organizations respond quickly to equipment break-downs and slowly to market changes and need for modernization to match global trade changes.

4.6 VSM System

Following the description of how a normal controller works (Section 4.3), and the basis for VSM is now discussed. Figure 4.10 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. There is a regulatory center which controls various activities at the working level. This is the role of the supervisors. Then there are operational activities, from running a Nuclear Power Plant (NPP) to shoe-making, tire production, etc, these are fulfilled by operators. 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/ organization on the environment. 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 of black and red shoes.

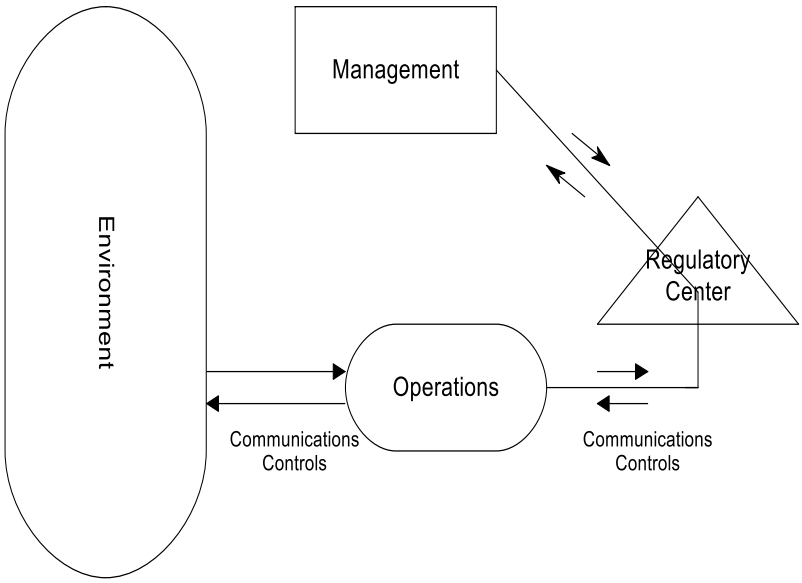

Figure 4.10 Basic VSM Figure depicting Key Elements within the Approach

The regulator in Figure 4.10 operates in a similar manner to the controller depicted in Figure 4.3. The set point could be related, to say, the number of shoes to be produced per month as set by top management of the shoe 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 color ranges of the shoes, and 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, also 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 4.9. 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). The VSM models does focus on both feed-back and feed forward signals, which tie the various units together and make it possible for the whole 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. Later, several organizations will be examined in Chapter 5 to show how failures within organizations can lead to accidents and even to the demise of organizations.

4.7 The Use of Feedback in VSM

The figure shown in Figure 4.10 can be viewed as a simple representation of a utility, but it can be considered to be a building block representing any organization. In essence, the management block represents the higher functions performed by the top management, such as optimization of the cost and safety effectiveness of the organization, reacting to information relayed by the rest of the organization, setting operational rules and allocating resources. The regulator function covers the local management function (supervisors) that control the work product and reflect guidance from the top management. The operational block carries out the required tasks ascribed to the organization. The product of the organization then affects the 'public' or the environment.

As mentioned above, feedback occurs at all levels of the organization, both forward and back. One item always of concern in any cybernetic situation is the quality and frequency of the signal (information or control). Each operating part of the organization needs to ensure the information neither overwhelms not is deficient as far as the receiver is concerned. Some filtering is required, but clearly management can make poor decisions if the quality of the information is defective. Equally, the top management has to make good decisions to minimize both economic and safety risk to the organization and not compromise the environment. An intrinsic requirement of an organization is to operate efficiently and safely. Risk is not just associated with accidents; it can be due to poor decisions made by managers to repair/replace equipment. The replaced equipment then fails leading to prolong shutdown of the plant. A prime example of an issue like this was the decision to replace worn-out steam generators (SG) with ones that failed very rapidly on replacement due to poor design (Fairwinds, 2013). Not only does the utility face cost of replacing the new SGs, but costs associated with shutting the plant down to resolve safety issues, raised by the regulator related to the possibility of a rupture of a number of SG tubes at the same time

due to wear. Costs associated with shutting the units (2) include paying for replacement power and servicing the debt on the non-operating plants.

In the VSM approach, the term regulatory is another word for controller and it is not to be confused with the term Regulator as associated with the regulatory function of say organizations like the US Nuclear Regulatory Commission (NRC) or other similar bodies. In the government sense, the term Regulator is used in the legal sense of a person or persons, who regulates the actions of organizations to ensure they fall within legal constraints.

VSM operates in an environment, reflecting the outside world and its variability. The system senses and acts on environmental changes via the communications and control channels depicted in Figure 4.10. This information is then fed back to the regulator and hence to the management function. The information and control channels are also used to characterize the health of an operation. The regulator examines the information and determines if it can act on it, or that the information is such that the management needs to be consulted to change the operating rules. If the regulatory response is within its permit, then action is taken by sending messages to operations. However, if management is to be involved, information is sent to management and they in turn send instructions to modify the rules. Following the route does take time. Of course, the management might require more information before being in a position to change the operating rules.

In manufacturing organizations, changes in regulation might be to increase production of say, a certain type of shoe to match the demands of the environment (public). Information derived from the environment is analyzed to see quantity likely to be required. In the case of a shoe manufacturer if because of changes in the public's attitude to a shoe's design, the market share falls, then the action process is more complicated and management should be involved. Management should analyze what steps should be taken, such as changing the design of the shoes, to enhance market share.

The VSM approach is a cybernetic approach to what is normally a hierarchical approach, where the center of operations is the management function, which implicitly includes the regulatory function. This means that decisions and regulation of the operation is held by management. In the VSM approach, the management determines the rules, and the regulator controls the process via information obtained from the operations and the environment. The operations function carries out tasks, such as manufacturing, construction and running the processes. All features of the enterprise operate together to meet the needs of the environment (client). This concept is a much more shared system involving management and operators with actions/decisions taken locally as appropriate.

4.8 Complexity of Operations

The aim of an organization is to satisfy the needs of the public and to do so profitably. Of course, if one looks closer into what does the public requirements cover, it soon becomes obvious that it covers more than just the impact of the delivery of a number of shoes. Although individual persons might be satisfied with the shoes produced by the organization, other organizations representing the populous call for constraints on the on the manufacturing of the shoes, so the environment depicted in a simple way in Figure 4.10 implicitly covers the integration of all of these forces, i.e. the needs of the industry with the requirements and concerns of the public.

As the complexity of the system increases, relationships between the various entities have to be factored into the VSM structure. However, the basic concept of an organic process is still maintained, as other elements are introduced in the environment, operations, regulation and management. Information has to flow between the elements with the related actions indicated in the normal control manner. The importance of each part of the organization in satisfying the goals and objectives are still maintained. Failure or success in meeting any of the organizational needs or requirements can lead to failure or success of the enterprise.

Management is tasked with controlling the organization, but maybe overtaken by the complexity of the task. To balance the task requirements against his/her capabilities he reduces the complexity by in the words of Beer 'destroys the systems variety,' (see page 38 of The Heart of Enterprise). The key to good management is to carry this out in a manner that does not run counter to Ashby's Law of Requisite Variety. This raises an issue, how does management do this. As we see in Chapter 5, we can determine this retrospectively by seeing what decisions were taken or not taken by management which ended in an accident. By examining the Fukushima tsunami accident, we can see what decision was taken and could argue that Ashby's Law was not met in this case, despite information given on the tsunami probability, the managements decided to ignore the information. This was done it appears, since they reasoned that if they told the Government, it would cause them to shutdown the plant and build a higher sea wall. This information came out well after the accident during post accident investigations.

4.9 Enhanced VSM Representation

VSM can be applied to higher or lower levels of representation of the systems, for example if the company consists of a number of factories making different products, such as shoes, clothing, handbags, etc., the combination of these factories should be combined in order to

consider the health of the overall organization. Equally, it can be used to used to represent the details of just the shoe making operation. Each factory within a set of factories could be represented by Figure 4.10, operating as a partial entity of the whole organization. Later in this chapter, a complex organization covering Air Traffic Control Management system of a country is analyzed. In the case of multiple factories, there are as many VSM blocks as there are individual factories. All of these sub-units come under the control/influence of a senior manager, but each individual unit would be self regulated or autonomic. In addition, to the top management function there would be other functions to ensure the balance between the sub-units in terms of meeting overall management objectives for both the whole and the individual sub-units, this is the equivalent to the Pons/Medulla depicted in Figure 4.8 or block 3 in Figure 4.9.

Within the sub-units, there could be sub-functions dealing with maintenance, finance, human resources, material purchases, etc. Each of these sub-units would function as a self regulated unit, but they cannot exist as an independent organization except within the main organization. For all of these organizations, units and sub-units to function, communications has to be timely, efficient and accurate. The top management needs to receive credible information upon which to make the best decisions. The speed of information has to high enough and filtering of the information is such that it is clear, accurate and unambiguous, this is a key cybernetic function. Equally, all persons within the organization should be informed about decisions affecting them and how they are expected to perform.

For most organizations, they operate as closed loops, however they have react to how the markets changes and be prepared to act to modify their products, either in quality or quantity. They are also required to respond to availability of raw or processed goods and also to monetary shifts. As in human body, the level of control depends on changes in the environment, so some organs with the body are under autonomic control and for others the higher levels of controls have to take over. In the absence of good and effective communications, the top management is required to step in and ensure the operations are carried out efficiently, but the organization is much more effective if each component operates efficiently without outside controls.

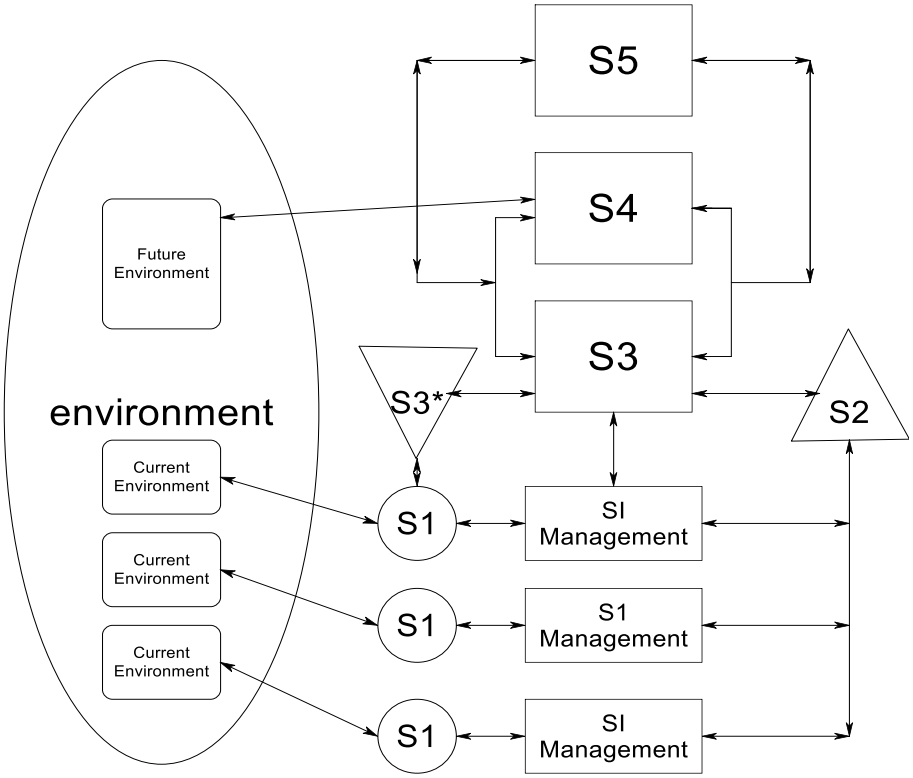

Figure 4.11 More Complex Version of VSM

The above considerations led to an enhanced VSM model to cover these aspects and are shown in Figure 4.11. It was appreciated that there was a need to produce some measure of stability, management wise, between production units. Therefore, it is necessary to link organizations to achieve this, and outside of the main part of the organization there was a need for a regulator to cause each operation to act more in concert. Clearly, some degree of acceptance by managers and personnel has to accompany these control measures to make them effective. The stabilizing organization has to communicate with upper management and if necessary get it to understand and comply with the strictures. Figure 4.11 diagrammatically depicts these processes for a set of related organizations. The figure shows the connections between senior management and sub-organizations, this is equivalent to Beer's Figure 4.9. Connections to other organizations have been omitted for clarity. Each operation itself consists of multiple sub-operations each performing operations directed towards the objectives of the organization as a whole.

A discussion of the meaning of the various boxes, control and information lines and other devices shown in the figure is given below. VSM is made up six processes and connecting channels see Figure 4.11. Beer referred to these processes by System (S) designations:

System 1: Operational or implementation units. This is where the organization produces what the customers/users want. It is the production area where goods, cars, electricity, etc., are produced. Note that S1 management is local management or supervisors in direct control of the work

System 2: The coordination activities are here, coordinating activities between production and control/management

System 3: This is the management and control used to inform production, System 1, what is required of them and to monitor activities

System 3*: This is an auditing and stabilizing function, which cross checks that systems S1 and S2 are working effectively

System 4: This operation looks at the external environment to examine the acceptability of the products and see how the market might change, producing an intelligent prediction of market/environmental changes

System 5: This is the management policy group balancing the current and future direction of the organization and ensuring the viability of the organization

The whole concept of VSM is to replicate the ability of organisms to respond to changes in a flexible manner. Issues can occur in the environment to problems with production, etc. Rigidly designed management structures do not respond quickly to changes. The other thing pointed out by Beer (1985) is to devolve considerable responsibility to the lower level, i.e. S1. The closer one is to the action, potentially the faster response or recovery. This is conditional on having transferred enough authority to the lower levels for them to feel confident to take the necessary actions. Clearly there may be situations that fall outside of S1 fields of competence, in which case the top management S3 needs to be involved. If S1 operations can respond then this is good. However, if changes have to be made to the processes themselves or the rules governing the operations, then the management needs to be involved. This may call for budget changes or changes in basic company policy, and then these decisions may take a lot of time. Actions involving the government take a long time to occur, one example of this is the Japanese government response to the tsunami induced nuclear plant accidents at Fukushima, in March 2011, (Joksimovich, 2011). In a later chapter how the Japanese NPP crews responded to the accident is discussed and is in-line with the dynamic characteristics of the various systems, i.e. S5 is slow to act and S1 acts more rapidly and S3 can supply the guidance to ensure the actions are correct.

4.10 VSM Application to a Foreign Air Traffic Control Study

This study was the result of a PhD research topic (Al-Ghamdi, 2010) undertaken to examine the workings of the Saudi Air Traffic Control (ATC), its reliability of operation and make recommendations as how it might be improved. This was a mixed problem dealing with both organizational and human reliability issues. For the organizational aspect the study used the VSM approach and for the human reliability issues the CAHR method of Straeter (2001) was used. The objective of considering this study in detail is to examine how VSM is to used and show how VSM can be applied in real studies. This study has a deal of similarity in need to the study of safety in the case of nuclear power plant operations, since ATC operations do present issues associated with human reliability. Failure of controllers to perform correctly can lead to accidents affecting the lives of passengers and airline staff.

In performing his study, Al-Ghamdi looked at other organizational methods and also different HRA methods, before selecting VSM (Beer, 1985) and CAHR (Straeter, 2001). One organizational approach reviewed was Systems Theoretic Accident Model and Processes (STAMP) (Leveson, 2004), however Al-Ghamdi (2010) decided to use the Beer method in conjunction with CAHR. It is interesting in that both Beer and Leveson both based their work on cybernetics and referred to Ashby (1964). It appears that STAMP integrated cybernetics with human reliability and social influences, but the combination of VSM and CAHR were considered by Al-Ghamdi to better cover the Saudi ATC situation. A review of some of the other HRA approaches that were examined is listed later. The use of the Viplan (Espejo, 1989, 1993) approach in the study was a good formalized way of dealing with the requirement to analyze the Saudi air space incidents. This is another part of the approach that fits well together with VSM and CAHR.

As stated above the Viplan approach was used in the study to help Al-Ghamdi organize the analysis of the Saudi airspace ATC. It is not proposed to go into details of the approach, but just mention the steps of the process:

- Establish the identity of the organization (Saudi ATC)
- Model the structure of the organization activities
- Break apart the structure complexities: establish various structural levels
- Model the discretionary controls at different levels within the organization
- Within the organizational structure; Study, and diagnose the design of the regulatory (control) mechanisms (adaption and cohesion factors)

Quite a number of approaches to solve issues, use a systems approach to breakdown the analysis into separate steps before integrating them to help solve the problem. For example, in the case of studying HRA for inclusion into a Probabilistic Risk Assessment (PRA), a method called the Systematic Human Action Reliability Procedure (SHARP) (Hannaman and Spurgin, 1984) fulfills that need and it is a multi-step process. In the case of selecting VSM and CAHR, Al-Ghamdi had the support of Viplan and the CAHR systems analysis structures in helping him in performing the ATC study.

4.10.1 Air Traffic Control in Saudi Air Space

In order to understand the issues associated with this application, one needs to understand how air traffic control works. Planes are guided from take-off, passing through air space to landing at their destination. Flights are directed along given pathways (flight paths in space) and hold to different heights depending on which direction they are traveling. The whole purpose of this approach is to enable freedom of travel of individual planes coupled with a degree of control to enhance safety. So if planes are traveling in the same general airspace, safety is ensured by separating the planes by either height or distance. Like this planes should not run into each other, if the pilots follow the rules. This is a virtual equivalent of a highway system. Clearly, planes with different capabilities need to be factored into the mix. Local slow moving planes should not operate at the same height as fast moving, intercontinental travel planes, for example the Concord operated at heights of 55,000 to 60,000ft, well above local commuter planes.

Ground facilities follow the progress of planes traveling in space, approaching the airfield, landing and taxing on the ground. In space, planes are located by radar and their location is passed from one ground station to another as they fly overhead. Aircraft contact the various ground stations via changes in frequency of communications to minimize confusion. Thus pilots change the frequency of communication as they pass out of control from one ground station to another. Controllers hand over control of the aircraft to other controllers in this manner.

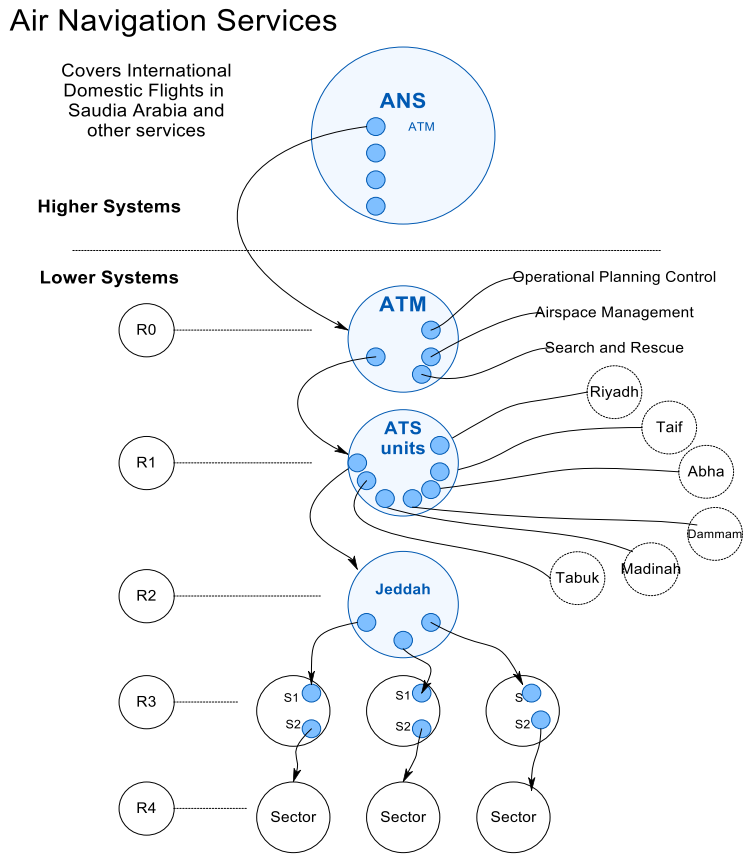

Figure 4.12 Relationships between Service Areas (after Al-Ghamdi, 2010)

As planes approach their proposed landing strip, control passes from Area Control Center (ACC), to the Approach Control Center (APP) and then to the Tower (TWR). Figure 4.12 covers all of the air control aspects from far space to ground movements. The process is pass the plane from one controller to another controller, so there is contact at all times between the pilot and a controller. It is of course not continuous but only as required. Thus planes are tracked all the way from distance locations to the local airspace then to touchdown and finally during maneuvering on the ground. ACC covers the contact with pilots from 16,000ft and above, APP covers contact from 16,000ft till 4,000ft and TWR from 4,000 to an the ground, including ground movements.

The top layer is the navigation services, which contact planes arriving from foreign airspaces to leaving for foreign airspaces. They also monitor planes within the Saudi airspace. This type of process goes on all over the world. Planes are monitored by radar and communicated from time to time as needed by ground sites, as mentioned above. Pilots have to register their flight planes ahead of time and if they want to make changes because of weather, then these have to be revealed and agreed to by the controllers. This is to ensure that planes do not fly into other planes flight paths!

The breakdown into various management and control areas are useful since VSM structure matches the various grouping and the kind of actions covered by these various routes affect the reliability of the controllers interacting with the pilots. The author of the Saudi study related each of the operations to the factors that influence the human reliability assessment, so for example he relates the skills required of the controllers, the tools that they use such as procedures, displays, etc. He also considered the consequences of human errors and whether they are recoverable or not, and what safety indicators there are, such of number of accidents due to a given cause, etc.

4.10.2 Analysis of the ATM Operation

The VSM process diagnoses the organization into various levels and examines the relationships between the management and operational aspects. The power of the Viplan (Espejo, 1989, 1993) was that it appeared to help Al-Ghamdi's understanding of how the air traffic operations at the various levels could be fitted into the VSM formulation. This in turn helped define the interactions between pilots and controllers and helped him understand the pressures that the controllers worked under in terms of time pressures. These things affect the Human Error Probabilities (HEPs) values selected and the significance of various Performance Shaping Factors (PSFs) given in the thesis.

Al-Ghamdi examined the workings of the Saudi ATM, ATS, Jeddah unit and ACC, APP, and TWR levels based upon the Viplan approach. Figure 4.12 depicts the network of parts that makes up the Saudi Arabia air traffic control system. The network includes other sectors airports other than Jeddah, but the lower level elements have only been indicated for Jeddah, the others are very similar.

The corresponding VSM figure relating to ATM and Saudi Airspace depicted in Figure 4.12 is shown in Figure 4.13 below. The figure indicates the relationships between the head of the Jeddah operations, the planning head and the head responsible for day to day operations at Jeddah. The functions are broader than just the commercial air traffic control functions. Of prime interest in the study are the commercial air traffic control and the roles of the controllers and pilots as far as reliability of ATC operations. One can see by examining Figure 4.12, there are managers associated with ACC, APP, and TWR functions. For each level shown in Figure 4.12, a VSM could be constructed which reflects the characteristics of each level. Each of the VSMs is similar in construction, but there are some features which are different, for example the VSM representing ATS units has seven S1 elements corresponding to each of the individual airports, Jeddah, Riyadh, etc. Figure 4.14 shows a series of icons representing a VSM array corresponding to the elements in Figure 4.12. This

figure shows a representation of the icons, which are unfortunately the same icon not the actual icons, but the array is correct.

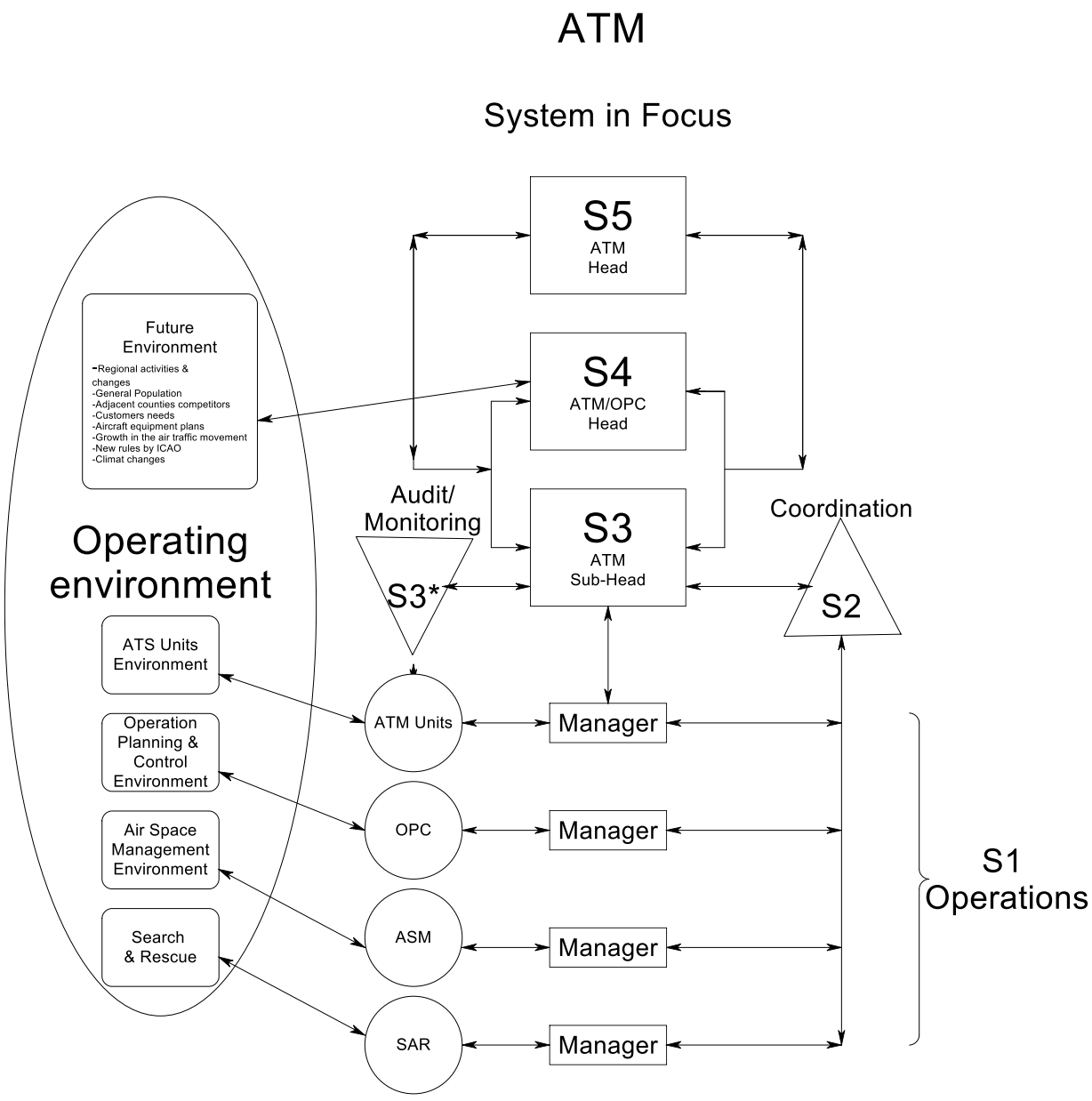

Figure 4.13 Air Traffic Management (after Al-Ghamdi (2010)

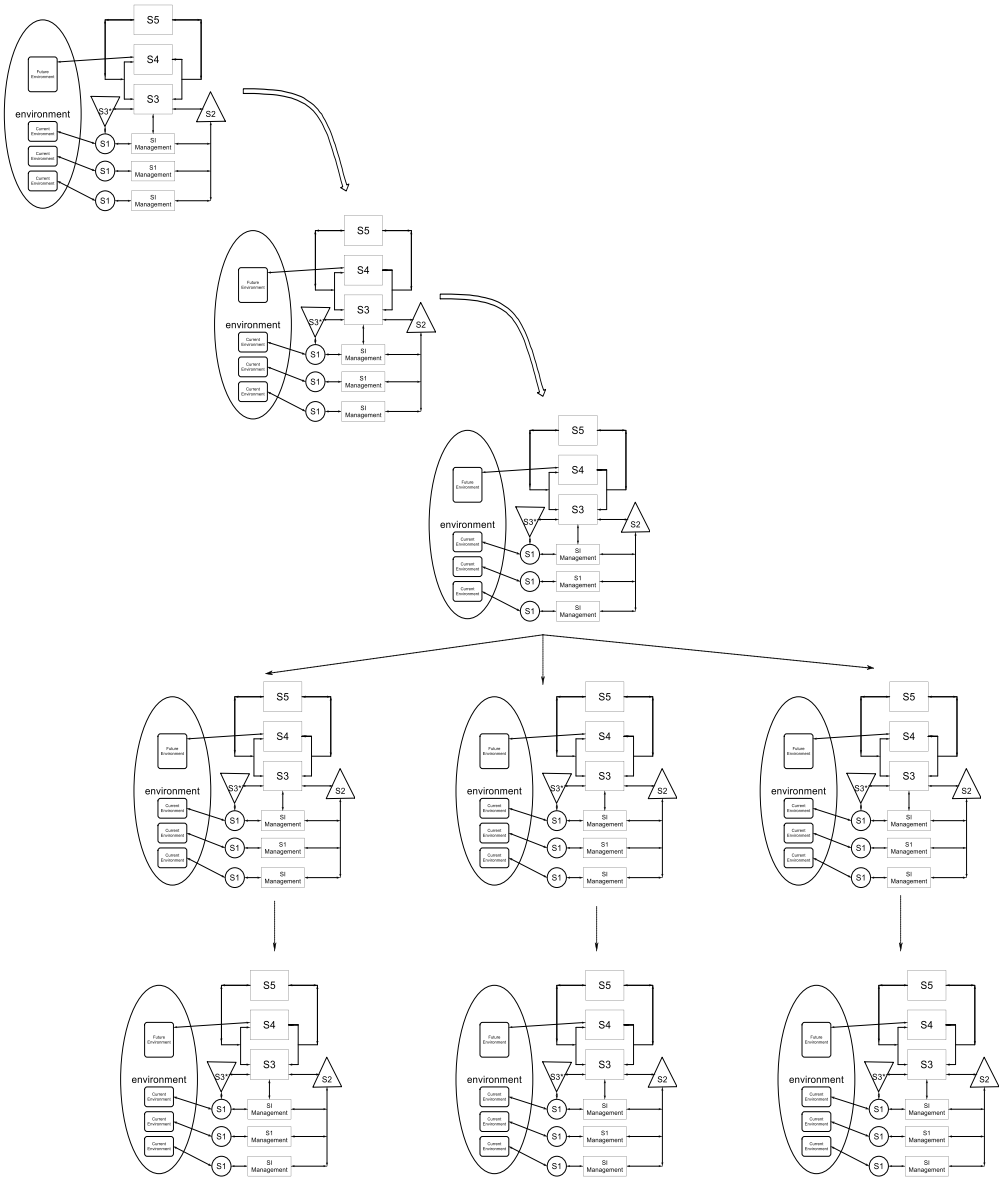

Figure 4.14 VSM Diagrams relating to various Operational Stages

4.10.3 Human Reliability Assessment

The safety of the Saudi Air Space depends not only on the organization of the air space control but also on the reliability of the pilots and controllers to understand and coordinate their activities. The VSM development undertaken by Al-Ghamdi covers the organizational aspects. It also sets up the understanding of the different duties carried out by controllers, supervisors and managers at the different levels within the ATM organization.

A key part of the complete safety and control study of the operation is the assessment of the human reliability of the staff as they function in performing their control functions. To that

end Al-Ghamdi evaluated a number of HRA methods and techniques. These methods were: Human Error Reduction in ATM (HERA) (Isaac et al, 2002), Technique for the Retrospective and Predictive Analysis of Cognitive Errors IN ATC (TRACER) (Shorrock,2002), Technique for Human Error Rate Prediction (THERP) (Swain and Guttman, 1983), Human Error Assessment and Reduction Technique (HEART) (Williams, 1988), A Technique for Human Event Analysis (ATHEANA) (Cooper et al,1996), and Connectionism Assessment of Human Reliability (CAHR) (Straeter, 2000). A critical review of other HRA methods as well as some of those listed above can be seen in Spurgin (2010).

The method selected for the study was CAHR. The method was developed based upon nuclear power plant data studies for German Nuclear Power Plants (NPP), but has also been applied to ATC studies for Eurocontrol. There are several points of interest with respect to CAHR in dealing with performance shaping factors (PSFs), contribution weighting for each PSF, and weighting of tasks depending on the perceived difficulty of the various tasks. The concept of PSFs was started by the father of HRA (Swain) as a method for accounting for different situations in which data was available and to estimate what it might be for an actual situation. The method took a basic human error probability (HEP) and modifying the basic value to account for the differences between the interactions associated with the known HEP and the current HEP being evaluated. A large number of HRAs have used this approach. Straeter also added a modifier, based on Rasch (1980), to account for the difficulty of the task being performed by a controller. Easier tasks have higher success values than more cognitive challenging tasks. He also makes use of modified influences of some PSFs in given scenarios than in others. A large number of HRA approaches have use PSF corrections, but Straeter seems to be the only one to have additionally used a Rasch modifier.

Straeter has developed a programmed way of dealing with the analysis of events to collect not only errors seen in the event but also helps to identify what PSFs affect the error. The key elements of this tool are:

- Framework for a structured data collection
- Method for qualitative analysis
- Method for quantitative analysis

It has been stated that CAHR, as used, is a virtual advisor for performing HRA studies related to ATC controllers (Trucco et al, 2006). Al-Ghamdi states that some 42 Saudi air space events are used in the study to evaluate error types and causes of human failures. The analysis of the events shows that there are 309 errors altogether with 262 due to

controllers and 47 due to pilots. This indicates multiple human failures per air space event (average = 7.35), seems like a large number of significant errors associated with an event!

4.10.4 Linking VSM and CAHR

VSM indicates the arrangements between the management, controllers and linkages to the planes/pilots as they move through the air space from take-off to landing. When events occur they are analyzed and here the method used is CAHR. The objective of the analysis process is to understand the errors made by the parties and how to learn to improve the error rate and reduce the number of incidents. Figure 4.15 shows the linking between the VSM models of the ASM process and the CAHR method for evaluation of incident reports, analysis and recommendations. This is an iterative process with improvements being made to the man-machine interface, training, procedures and of course introducing more controllers to help distribute the workload.

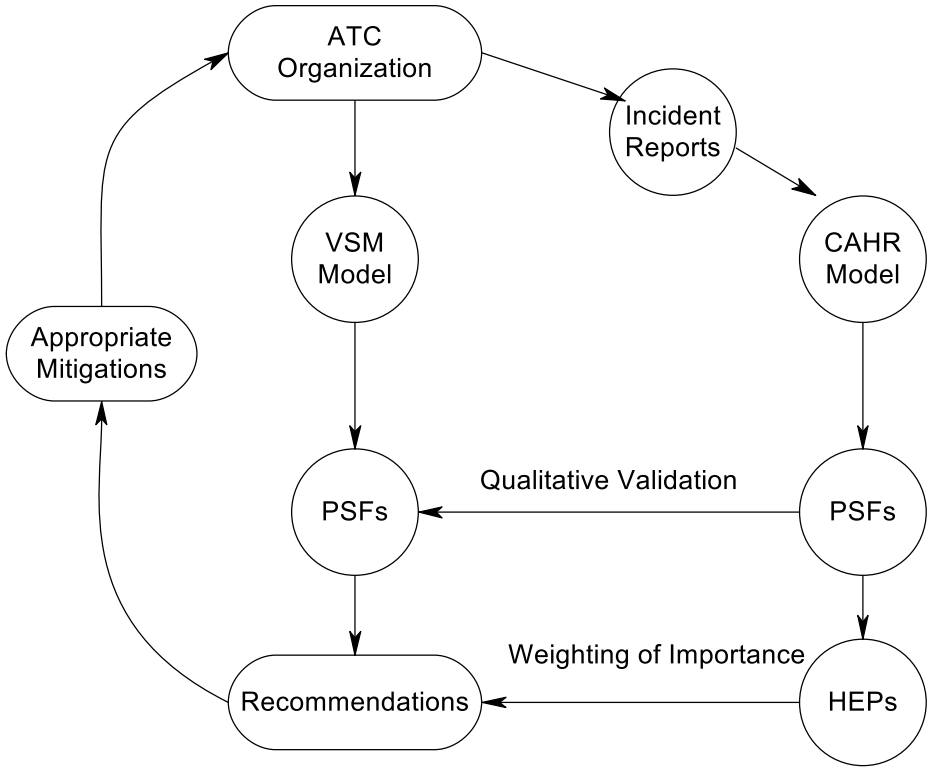

Figure 4.15 Framework for Integration of CAHR and VSM

4.10.5 Comment

The air traffic control study for the Saudi Air Space is an illustration of the application of VSM and also show the advantages of supporting VSM applications with a systematic process like Viplan for guiding persons applying the VSM approach. The HRA approach taken by the investigator is a good choice for this application in that the method used helps the analyst carryout a systematic process as well as being a qualitative method. Often, HRA methods focus mainly on the quantification approach. Some questions about some of the details of the analysis of the HEPs and their application can be raised, but this is not the objective of reviewing this current study.

The study itself made some recommendations related to the need to increase the number of qualified air traffic controllers based upon the study of the reliability of the current group of operators. The PSFs covered by the study were ones that were used as part of Straeter's work as part of air traffic control in Europe, known as Eurocontrol, (Straeter, 2000) The PSFs covered man-machine and training aspects, which would have been very similar to world standards, so one is left with the need to improve the workload of controllers. The proposal is to increase numbers of controllers and increasing their effectiveness by the addition of support staff. These are Al-Ghamdi's recommendations resulting from the study.

4.11 Summary

The objective of this chapter was to introduce Beer's VSM management concepts derived from the study of how the brain and nervous systems and a study of cybernetics. The chapter covers VSM development from the study of the human aspects of the brain and nervous system and then to the development of the idea as an analog to represent manufacturing/business organizations. In the process of covering the Beer development process, reference was made to a central part in the study of organisms of the use of cybernetic concepts and the representation of the brain/nervous system as a cybernetic process. Cybernetics is very much related to the mathematics of control systems analysis and of communications theory. The evolution of Beer's method was covered from a simple control/regulator to a more complex representation of the various parts of Beer's representation; S1 through S5. These blocks aim to cover the functions present in a business organization and mirror the brain and the nervous systems.

As was mentioned earlier, an important issue relative to Beer's and Ashby's work was the idea of variety and in particular Ashby's Law of Requisite Variety. The author was late coming to realization of their importance, to an understanding the deep significance of the

Law relative to the effective control of accidents and the steps that management attempts to 'destroy' or restrict variety to match their capacity to manage their business.

The Beer method has been illustrated by an application to a real problem. The problem was the examination of the reliability of controller operations in flight control over the Saudi Arabian air space and to make recommendations on how to improve reliability of controller operations. The objective has been met. Further, the field of control was been illustrated by the introduction of a simple one loop controller and how it works. The complexity of bodily functions has been depicted in cybernetic type block diagrams, which illustrate how feedback controls are used in the body to respond to changes and ensure stability with controlled responses. This complex field is only lightly touched upon for the purpose of relating VSM to the model of the brain and the associated nervous systems.

Later chapters will expand the application of VSM to the field of nuclear power plant (NPP) safety and economics as well as other HROs and will build upon the knowledge developed and analyzed here.

Chapter 5: Case Histories

5.0 Introduction

The purpose of this chapter is to examine a series of accidents to consider the causes of the accidents and the organization aspects associated with them. Also it is also an exercise in using VSM methodology to see what might be improved relative to organizations to consider the balance between safety and economics and how to adapt VSM to high risk organizations. One thing should be said at the beginning of this study, accident reports sometimes lack the detail to be able to conclusively able to show in detail the impact of the actions of all the parties involved in the accident. Oft times the impact of prior decisions of management do not arise in the accident analysis. Also in some accident reports communication protocols are not discussed and yet it is realized that communications between parties can be extremely important. In aircraft incidents, for example poor communications can play an important role, but in other circumstances this issue is not raised.

We know in control theory, communication quality is extremely important and one pays close attention to the impact of the appropriate filtering of signals. The wrong filtering can lead to sluggish controls or the failure to eliminate the impact of noisy signals, yet it does not appear that the impact of imperfect signals being transmitted from management to operators is considered in the case of plant accidents. The VSM cybernetic approach covers the aspect of communications as well as control actions, i.e. resulting from management decision-making. Herein is the potential strength of the VSM organizational approach to expose the working structure of the organization and its strengths and weaknesses in fulfilling its role in the business of running operations both safely and economically.

One purpose of Viable Systems Model (VSM) was as a tool to diagnose organizational structures and manner of their operation. One can use it to help diagnose various management relationships from top management and governments to lower level managers interacting with operators. By analyzing 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 maybe more 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 taken earlier. Sometimes, the effects of managerial decisions can take a while to manifest their effects upon the operation.

Here a number of case studies will 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, 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.

5.1 VSM and Cybernetics

VSM is based upon cybernetic concepts was stated in Chapter 4. Cybernetic concepts cover a whole range of applications from mathematical control applications, to explanations of animal functions and to the operation of industries. Clearly, in a broad-based way, these applications are similar in that they involve control principles, communications between active systems and decision-making by command structures. However, when one set up mathematical representations of these different embodiments the implementations are not identical, for example the communication processes and information content are different. In the case of control systems, communications may be analog or digital, representing either a continuous variable of an action state or discrete stop or go actions.

One can see this type of representation in the works of Wiener (1989) on cybernetics. In the case of controls, his thoughts are associated with continuous controls, filtering processes and tools for analyzing these systems, like autocorrelation functions. He does also discuss signal transmissions within animals in terms of state changes and binary effects. This is all good material especially at the time he was writing, i.e. 1948 and 1961.

The interpretation of cybernetics for organizations has to move from mathematical processing of filtering and shaping signals to the human process of shaping and filtering signals. Humans carryout this process in a different manner, effectively it may be similar, but the process takes measures unrelated to the signal itself. In the case of managers, they may appear to ignore or otherwise the signal (message) depending on the status of the messenger! Also, instructions or orders may be misinterpreted. This means that the repeatability of communications in the case of organizations can be variable. In operating mechanical/electrical systems this is very unlikely, except when components start to fail. The meaning of this is that the strict analogy between science-based cybernetics and human-based organizations does not hold, the process is subject to interpretation.

5.2 Consideration of Cybernetics in Organizations

In the various case studies discussed here, a number of requirements relating to decision-making and communications, which are required for safety, do not seem to be met. In evaluating an organization's capability to be considered a highly reliable organization (HRO), one should examine whether critical requirements are met. This process should apply to both small units within a large organization up to a nation's energy industry including the government itself. The necessary requirements will be discussed following the analysis of the set of accidents covered below. One of these requirements should be the knowledge and understanding of the upper management of the foundations of plant safety. The decisions made by top management must be made in the knowledge of plant safety requirements. The safety record of the US Nuclear Navy is founded upon the philosophy of Rickover (see Appendix A), who emphasized the importance of reactor safety and radiation control above operational needs.

The rules and regulations for an organization are the equivalent of controller algorithms in the world of automatic controls. To complete the analog, one should mention that communications between organizational elements are the equivalent of signals driving a controller's action. The communications are orders/instruction given by managers to personnel to take action or information given by personnel to managers on the state of the plant/equipment. If the parts of the structure, orders/instructions and communications are not correct then the organization is exposed to random failures that can lead to accidents. One must remember that personnel in lower company positions are strongly affected by top management decision-making and attitudes. A strong safety culture needs to be formulated throughout the organization to ensure that the lower level personnel follow the dictates of the safety-conscious top management.

Although the lower levels within the organization have more limited impact on the organization they can have a very significant impact on the course of an accident, as one can seen in some of the cases discussed below. The failure of upper management to effect certain policies, such as in-depth training of personnel, can place the 'sharp-end' personnel in the unfortunate position of not having skills and knowledge and confidence to terminate or mitigate the consequence of an accident. The 'sharp-end' personnel are those persons with direct control over processes, such power plant operators.

It is postulated that the "regulator" control algorithms determine how an organization will act. In chapter 4, it was pointed out that the regulator in the VSM process was analogous to the controller in an ordinary control system. The rules and regulations contained within the "regulator" correspond to the controller algorithms. Here the word algorithm will be used for the group of rules in the VSM models used in the various case studies. The regulator in the

VSM approach may be distributed in real cases between various layers of management. It is convenient to group the rules and regulations within the regulator module.

In the VSM approach, the regulator is only one part of the process, the approach also covers the communications between the various components and their corresponding filtering, and not all communications are equally important. Also implied for both management and operators is the level of experience, knowledge and the possible need for improvement in each of the attributes. For example in the case of safety awareness, the operators need to know of the fundamentals of safety, such as the 'Defense in Depth' concept, see Chapter 3. Before an operator can be a licensed operator he/she must pass an exam to be accepted. It is the responsibility of the management to ensure this is the case and failure to do this leads to the Regulatory Authority taking action against the utility, such as leveling fines.

In designing a control system, the dynamics of the 'controlled' plant needs to be understood and the controller algorithm is selected on that understanding. Organizations act like controlled systems, however different elements in an organization or groups of organizations respond differently. Operators will respond quickly to changes in a plant condition to prevent damage to systems or components whereas top management act more slowly to plant improvement needs, since money needs to be budgeted, designers need to be engaged, designs generated and checked, and so on. Things are even slower when the government is involved, laws have to be written, voted on and release for public comment, re-evaluation, etc, see Figure 1.1 for the time scale of events in the world of Nuclear Energy.

5.3 VSM Model of a Utility Organization

In Chapter 4 a VSM was depicted in Figure 4.3 ('More Complex Version of VSM'), which was a version of Beer's original VSM and discussed various elements within the model. 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 type of organization. This modified VSM is shown in Figure 5-1.

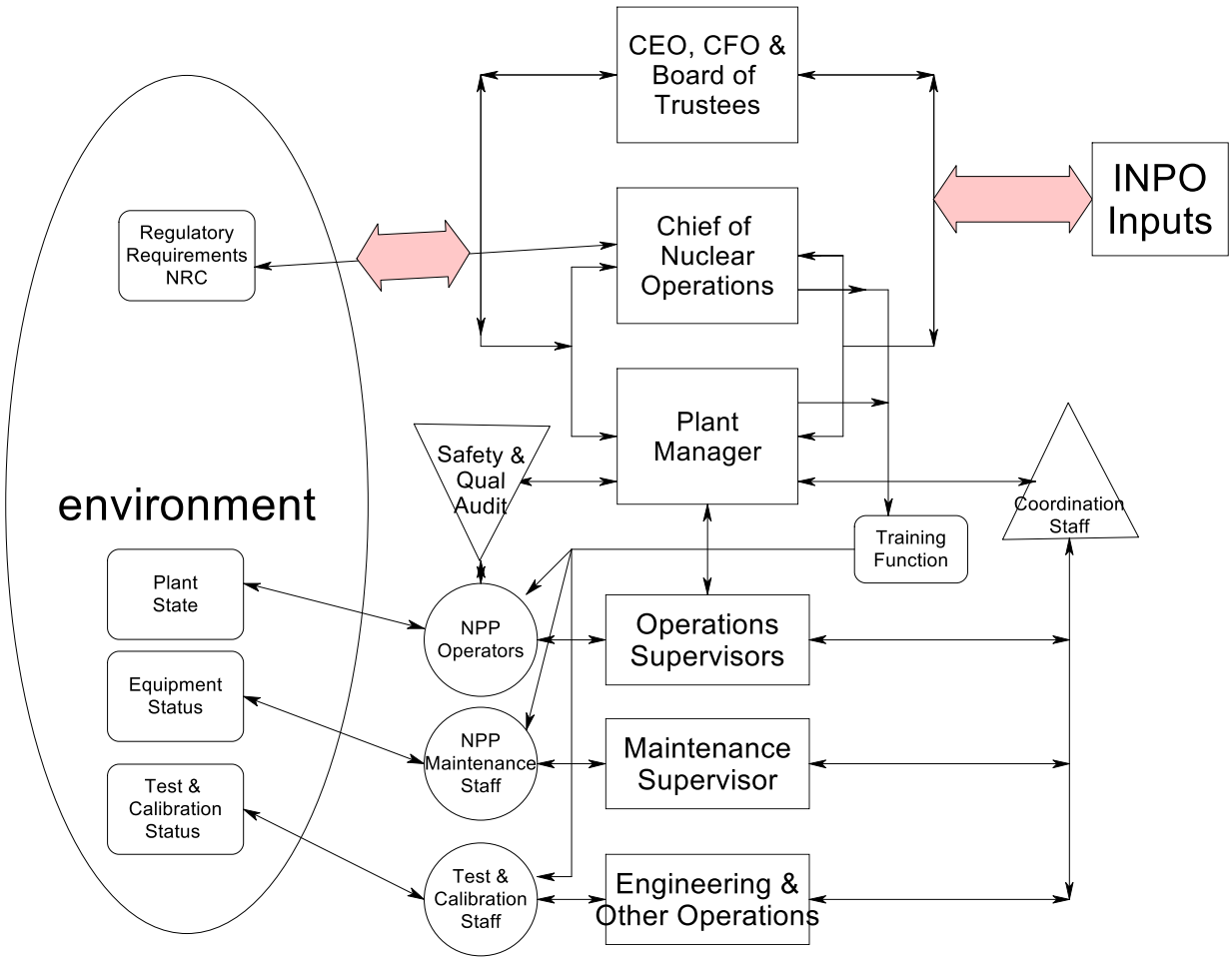

Figure 5.1 Depiction of a VSM model of a US Nuclear Utility

This figure models the current single US NPP type of organization, which involve 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, unit #2 (TMI) accident has had a deep influence on the US industry and lead to the formation of INPO. The impact of the accident lead 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 lead 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 and complexity of training and its importance have been increased since TMI. So the general structure of control of organizations has remained much the same, but a number functions added to reflect the need to factor safety within the VSM representation.

Figure 5.1 reflects the VSM equivalent to the organizational chart shown in Figure 3.2. The VSM model covers the roles of the CEO, CFO and the Board of Trustees together as equivalent to S5. In Figure 3.2, 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 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 personnel. 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 rules for operation coordinated with the NRC 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 at the same time that operations on valve, V#2334 are being carried out, 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 good 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 has occurred. 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 an accident is that which is of concern here.

5.4 Organizational Interactions and Safety

In order to more clearly understand the interactions within and between organizations a set of case histories are diagnosed here. The cases show that there are various areas within the organization that things can go wrong, but often the problem may have its origin in other parts of the organization. This concept was covered in chapter 3, section 3.6 and symbolically depicted by equation 3.1. For example, manning needs may not match actual implementation requirements, leading to components not being maintained. Later, accident initiating events may result from the failure of these components. One could say that the fault lay with the maintenance personnel for not taking action; however the real cause was the maintenance department did not have sufficient personnel to cover all of tasks in a timely manner and some components did not get the required maintenance.

A similar result could occur, in this is might not be due to insufficient staff, but rather due to organizational inadequacies, such as poorly trained staff, poor work control, etc. So failure to take timely actions can be due to a number of different causes. To return to the controller analogy, the rules (algorithms) maybe correct, but they are not being acted on for a variety of reasons.

One can often trace plant related problems back to decisions made by top management. Figure 5.1 depicts the relationship from top management (CEO/CFO) to the CNO and then to the Training Function. If the decision is to cut the Training budget, this in turn could affect the performance of training in a number of ways, such as insufficient training staff, insufficient time for analysis of training needs and failure to update the simulator software, etc. This is how management decisions can affect operator actions because of training budgets restrictions that leave control room operators unprepared to respond correctly to certain accident scenarios.

Figure 5.2 tracks the connections between the upper management and the control room operators that pass from decisions made by upper management then implemented through local decisions made by middle managers to actions taken by the operators. This figure is based upon and understanding of how the nuclear industry works and on human modeling concepts stemming from human reliability studies of actual and simulated accidents (Spurgin, 2009). This diagram has been simplified to illustrate the connections and does not include middle managers or supervisors. In practice, these individuals can influence the actual process steps, either for the good or to make the situation worse. The diagram shows both regulatory and economic influences. Economic influences can stem from regulatory action. Regulatory actions do not only include the effects of the NRC but also that of Public Utility Commissions. The NRC actions can lead to increased costs that do not enhance plant safety by requiring unnecessary regulatory demands, so the actions of the NRC are not always for the good. The PUC can take actions which accede to or deny rate changes, which directly affect the economics of plant operations and in turn can affect plant safety.

A series of case histories, not limited to the nuclear industry, are examined below, in order to better understand how errors develop and how all levels within the utility organization can be involved. As one can see in the figure, there are influences coming from outside the utility such a need for cost effective operations and also responses to regulatory actions. Economic forces may influence utility CEOs to reduce staffing levels to reduce operating expenses to lower the cost of electric power; and equally the regulatory forces may cause the utility to increase training of staff, which can lead to greater expenditures! The CEO must try to balance these competing forces and run a safe but economic business.

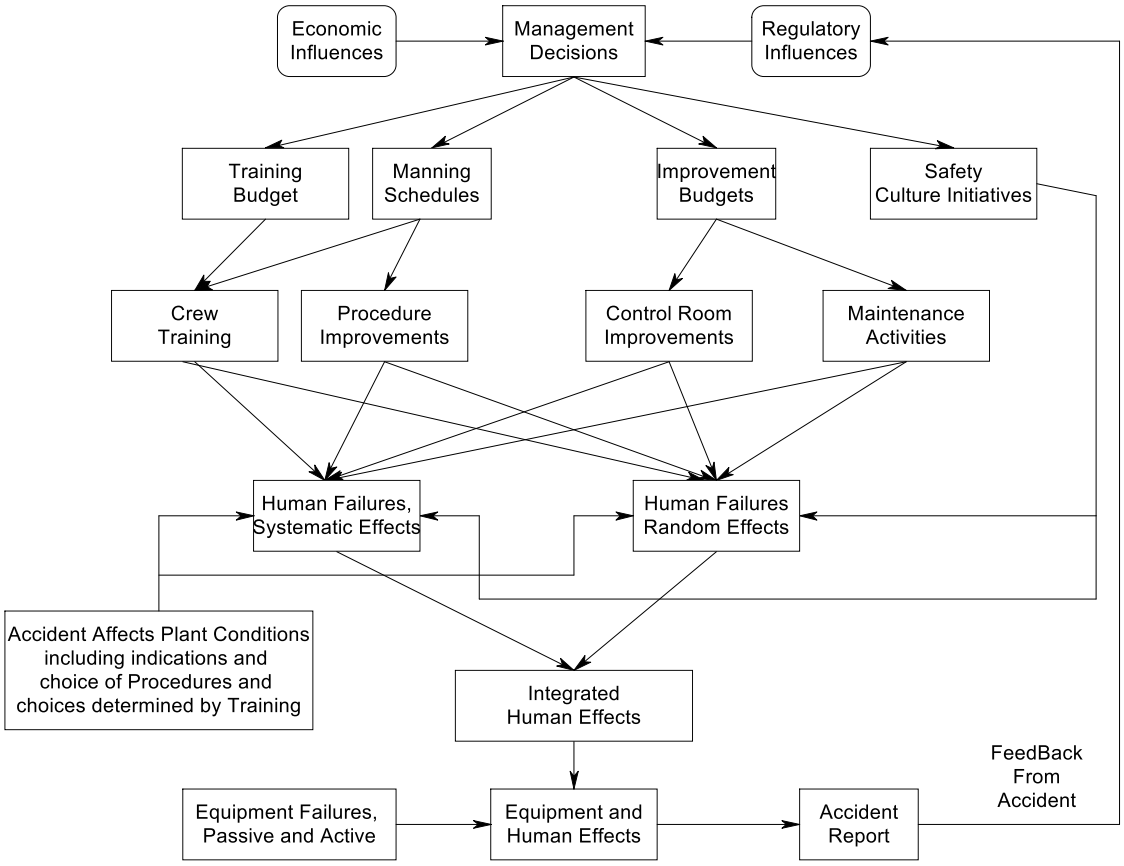

Figure 5.2 Relationships between Management Decisions and Actions

5.5 Case Studies

It is realized that nuclear is key part of the dissertation, 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 the 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.

Thus a number of case studies have been selected from accidents/incidents that have occurred in the nuclear and other industries to examine this proposition. 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, see MacAvoy and Rosenthal, 2005
5. Unknown Utility: leaking valve packing situation, Perrin, 2005
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
11. Storm in North East US-Sandy, October, 2012

The idea here is to briefly describe each accident, items 1 through 6, not so much from the accident sequence point of view but rather from the decisions made and who made them. In general, the approach will be the same if possible for each accident, but some details may not be available from the available accident reports. Each report given here will draw conclusions and recommendations. As one can see not all of the accidents are nuclear related. The accidents have been selected to illustrate the range of types of organizations that have safety issues and they involve management decision-making aspects from operators to Governments.

5.5.1 Three Mile Island, Unit #2 Accident

There are many reports and descriptions for this accident, which was a classic for the US Nuclear Utility Industry, March 1979 (Kemeny, 1979, and Rogovin, 1980). The accident description below is derived from the reports that were read many years ago and compared with other authors' reconstructions. The author of this document was also at Electric Power Research Institute (EPRI), when the industry and EPRI were fully engaged in analyzing the accident.

5.5.1.1 Accident Description:

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, see section 2.3.2.2. Attention to water quality is paid for all steam generators, but once-through units are particularly sensitive. The main feedwater system 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 tripped automatically. In response to these things happening, the auxiliary feedwater system should have started, but failed to start due to a maintenance error 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. Boiling in the core followed and the generated steam rose to the top of the reactor dome and displaced the water from there. The displaced water moved into the pressurizer and the level within the pressurizer rose. Eventually, the pressurizer filled. The operators thought that the reactor pressure was under control, that safety Injection was continuing to inject water and the change in water level in the pressurizer 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 continued boiling and eventually the top of the reactor core was uncovered. The cladding was not effectively cooled by the steam flow, its temperature rose and melting of the clad followed. The clad is one of the three barriers (Defense in Depth requirement) to the release of radioactivity, along with reactor vessel and steam generator tubing and the containment. With the failure of the cladding 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 persons were affected, since most of the radioactive material was contained in the reactor and containment. This was in line with the “Defense in Depth” philosophy of the United States.

5.5.1.2 Accident Analysis

Operators, and the maintenance/testing staff could be declared to be the responsible personnel for the accident. The operators were the ‘sharp edge’ personnel in this case taking action. However there were a number of others involved, such as the designers of the plant in specifying those particular PORVs. The PORV was poorly designed in that the signal indicating that the value was open or closed was derived from the control signal and not the actual position of the valve. So the valve appeared to be closed, but was actually stuck open.

In addition to the operators, others should be held responsible. The industry and NRC leaders should be really held to be responsible in that they did not appreciate how important decay heat was to the safety of NPPs. Also, both parties down played the role of operators during the accident control and mitigation process. See the fundamentals of nuclear power development given in chapter 2. As a result, training of the control room operators was defective.

The management of TMI should also be included in that they were responsible for reactor safety and should have been better trained themselves in reactor and accident dynamics. They represented the norm for the industry. At this time, the best technical knowledge about reactor and plant dynamics was resident in the reactor designers, but they did not understand the limitations within both the utilities and licensing authorities or even that they had a responsibility to address those weaknesses.

Figure 5.3 shows the connections between the various parties and some of the things that went wrong and is a reflection of the text above. The parties to the accident were the utility and its management, the utility staff (control-room, maintenance and test), the NRC and the designer of the TMI units (Babcock and Wilcox). The diagram shows the accident sequence the bottom of the figure and then relates various actions and decisions taken by various persons, notably by the control-room operators. However, other persons were also responsible from designers to top level managers and the NRC must also be held responsible as well. The figure shows that the initiating event was the trip of the main feed caused by the filter transfer being incorrectly performed. The closure of the auxiliary feed isolation valves was caused by maintenance staff, which further confused things by incorrect placement of the work tags on the isolation valves. The control room staff can be faulted by

not being in control of the work authorization process for the auxiliary feed water system tests, which required the isolation valves to be closed. It could be said that the control room staff should have spotted that there was an effective small loss of coolant going on. However, the indications of the valve and high temperature indication at the PORV blow-down line exit could be confusing for poorly trained staff and therefore the blame flows to the utility management and NRC organization. One further thing, is the good action of the unit one operator was somewhat negated by not realizing that the fuel was very hot and then turning on the SI flow, which was cool, could shatter the clad. However, the damage had already occurred, it was just an extension to the damage!

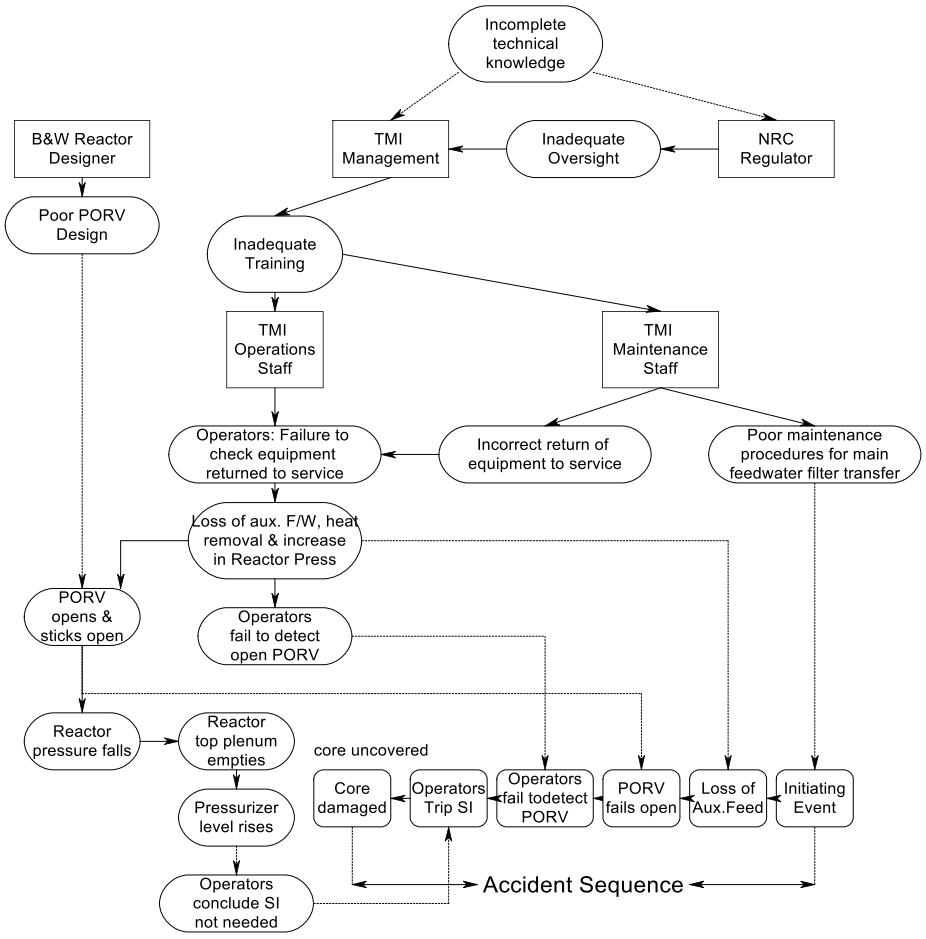

Figure 5.3 Three Mile Unit #2 Accident Relationships

5.5.1.3 Organizational Analysis

The top level of industry consisting of utilities, manufactures and AEs and NRC, there was a lack of understanding of basic accident analysis and the role of control-room operators, especially the role of decay heat removal in accident progression. In the case of the Manufacturers, the failure was to transmit their understanding of these issues to the utilities

in a clear manner of the need to play attention to decay heat removal. It is not clear that manufacturers had a clear idea of the competence of operators to be able to control multi-failure types of accidents, especially operations involving decay heat. In the case of accidents involving stuck open PORVs, a number of operators had dealt successfully with this issue, but information about the issue did not seem to be distributed throughout the industry. Later, one of the functions of INPO was to act as a distributor of accidents reports and lessons learned, so this was an improvement in the way the industry operated.

At TMI, the management was at fault; because of training needs for the control-room operators were insufficient to tackle the TMI type accident. The maintenance/test personnel were at fault on a number of counts firstly because of poor work processes during changing feedwater filters leading to reactor trip, and secondly for not returning the auxiliary feed isolation valves to their open position after performing auxiliary feedwater systems tests. The failure of the main feedwater flow led to the initiation of a reactor and turbine trip. Later the operators failed to institute heat removal from the reactor via the steam generators, because the auxiliary feed water isolation valves were closed and the auxiliary feed was unavailable. They could have opened the valves and started the auxiliary feedwater system and this would have helped the situation.

The operators were also at fault for not checking the isolation valves either on shift change or before issuing releases for the Maintenance and Test (M/T) work. So there was a management problem here as well. The maintenance and operators actions are relatively standard to returning valves to operational conditions. These actions do not require complex thought processes but just close attention to detail. These actions point towards a lack of management attention to operational details together with an unsatisfactory approach to safety.

In addition, the operators seemed to have a poor understanding of how NPPs behave and a lack of understanding of basic reactor plant dynamics. The operators seem not to appreciate the fundamentals of heat removal from the core to prevent core damage. The NRC and their personnel were responsible for testing the operators. This process was done frequently. So the NRC was also to blame for a lack of knowledge relative to complex accidents and the role of decay heat in accidents. The NRC personnel in charge reflected a lack of technical understanding of the reactor plant dynamics. This lack of knowledge was not uniformly distributed through the industry, but seemed to be absent at the key decision levels, like the utility management.

5.5.1.4 Review of VSM model following TMI Organizational Analysis

The VSM model shown in figure 5.1 relates to a later time, and it has been redrawn, see Figure 5.4, to reflect the state of the industry at the time of the accident (3/1979). This diagram is quite different in some of its details compared with figure 5.1, since many of the features and processes have come about because of the impact of the TMI accident upon the industry and NRC. One key item that affected the TMI accident was the knowledge and experience of the TMI operators and in both figures an element has been introduced to represent the training function explicitly, as a marker for this critical function. In the case of a normal VSM representation, this function would be subsumed within one of the high level management functions. Some utilities even have a Director of Training, however his position still ranks below that of Plant Manager, but including this function explicitly does emphasize the impact of training and simulator training on the safety performance of the plant. It should be emphasized that training for other staff is also important, such as maintenance and radiology personnel. One can see the failure of the test personnel to return the auxiliary feed-water isolation valves to their working condition was a failure of the organization all round, failure to use checking lists (procedures), failure of control by the operators and failure of safety training on behalf of management/supervisors. Nowadays this would be called a failure in the plant's safety culture.

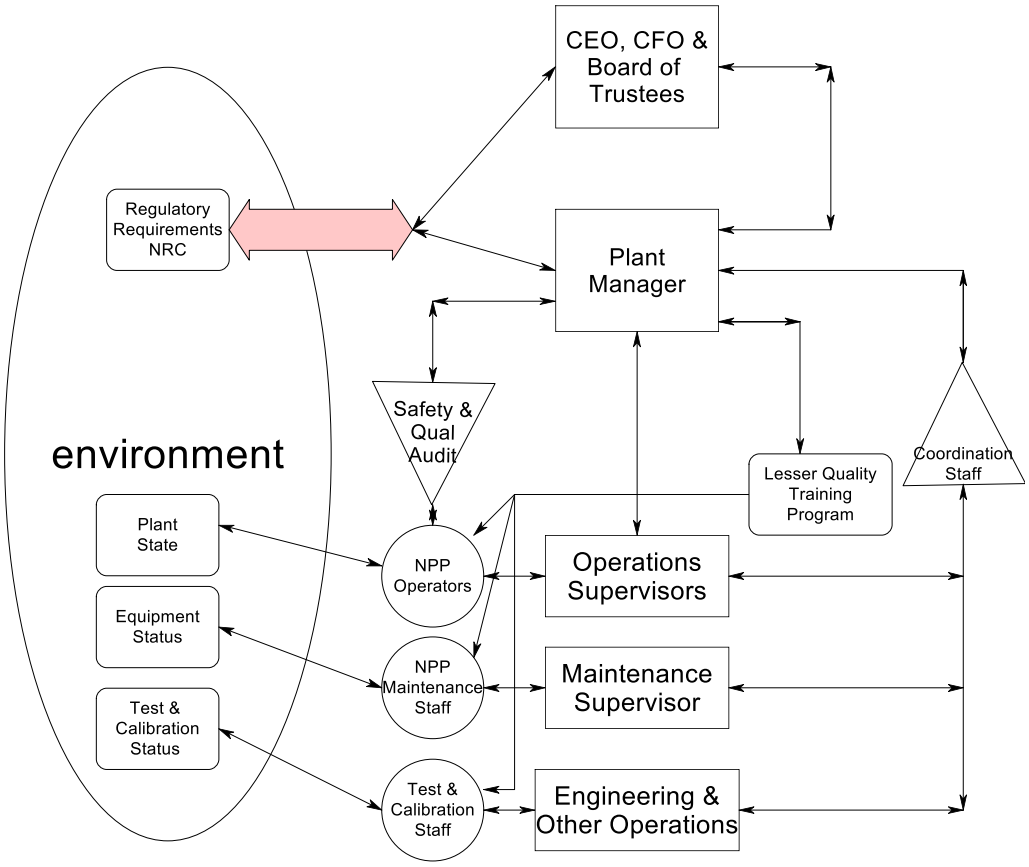

Figure 5.4 VSM version of the GPUN TMI Organization prior to the Accident in 3-1979

At the time of the TMI accident, the NRC licensed the control-room operators as they still do, and the operators had to be trained and tested in responding to various accident sequences. Mainly this training was carried out in a classroom, since there were a small number of simulators available. Control room operators might even trained on simulators that were not duplicates of their plant, for example crews at Connecticut Yankee NPP, an early 3 loop Westinghouse PWR, trained on the Zion 4 loop Westinghouse NPP simulator as late as 1985! During the TMI accident period there were a limited number of plant specific simulators and they were not full scope in that the secondary side (feedwater/steam) was not dynamically modeled. Even in the early days of simulator training and testing, simple design basis accidents were selected for training, as opposed to the later approach of exposing crews to multi-failure transients. The earlier approach to preparing the operators was approved by the NRC and in retrospect it was founded on the belief that the automatic protective functions would protect the plant and the public and the role of the operators was less critical.

It is interesting the General Public Utility Nuclear (GPUN) organization wanted Admiral Rickover to study the changes in their organization to run TMI unit #1 to ensure that it had been changed sufficiently to match his view of a safety conscious organization (Rickover, 1983).

There are both visible and hidden differences between figures 5.1 and 5.4. The two most visible differences are the presence of INPO and the management position denoted by CNO, or Chief Nuclear Officer. If one studies the two VSM models one will realize that many of the functions indicated by the same name are in fact performed differently. As pointed out in chapter 3, the existence of INPO is directly due to the effect of the TMI accident on the industry (Rees, 1994). But TMI's influence was more invasive than just the development of INPO. The whole position of humans within the industry changed as the messages stemming from reports generated in response to the accident, namely Kemeny (1979) and Rogovin (1980) became known. In particular, there were many things aimed at improving the performance of the control-room operators. The following lists some of these:

1. Improvement in Emergency Operating Procedures from event-based to symptom-based

2. Requirement for each station to have a full scope simulator for each different reactor type at the station
3. Each control room should be reviewed for human factors compatibility for the needs of the operators to better respond to accidents
4. An engineering trained person to assist the operators in the analysis of symptoms following an accident. The person was a Shift Technical Advisor
5. A display tool to help the operators called Safety Parameter Display System (SPDS) to help them define which parameters were key to their understanding of an accident as it proceeded

Requirements have been added for all persons working in NPPs, in response to the actions taken after the TMI accident. Figures 5.3 and 5.4 relate to the actions taken by the crews and the TMI at the time of the accident. One finding was that all parties making decisions need to be well founded in knowledge of plant behavior and to be well trained in the nuclear arts. In the case of the utility management, there is a need to be aware of NRC regulations, an understanding of fundamental reactor safety, including such things as “Defense in Depth”. The top managers are responsible for running the plant, selecting good personnel and getting the plant to run efficiently (cost control) and safely. Well trained and competent personnel are required throughout the NPP organization. The top managers need to be involved in all aspects of the plant operations and this seems to be a key need to ensure plant and radiation safety and economic operation.

Table 5.1 tries to summarize the comparison between typical VSM representations of nuclear power plant utilities both before the TMI Unit #2 accident and the current state of utilities. The table addresses the differences between Top Management (CEOs, etc) and other influential managers, such as plant managers as far as attributes are concerned. The top managers do not seem to be held to high standards of NPP safety as are the control room operators, but it appears that more of the managerial staff are more aware of nuclear safety requirements. INPO have promoted the idea that top managers to get training in NPP safety. Rickover was very careful in both picking and training officers to serve on ‘his’ submarines.

The pre-TMI structure may look similar to the later VSM model, but the functions are not the same and their involvement and responsibilities are different. The differences, the motivations and scope!

Item	Pre TMI VSM	Current VSM

Top Management	Unlikely to be Nuclear Trained	Some Limited Nuclear Training-variable
CNO	N/A	Nuclear Trained
Plant Manager	Likely SRO Trained	SRO Trained
Training Manager	SRO and Training Experience	Director grade, SRO and Simulator trained
EOP Design	Event-based	Symptom-based
Communications	Mgmt to staff-one way	Better communications between personnel
NRC	Limited role for operators	Better awareness of operators requirements
INPO	N/A	Strong connections with Utility mgmt/personnel

Table 5.1 Showing the Comparison between Pre TMI and Present Utility Organizations

5.5.1.5 Comments and Conclusions

The main conclusions (needs stemming from the TMI accident) were:

1. Better training of all utility personnel from managers to operators
2. Better understanding of reactor/plant dynamics by all personnel
3. Use of simulators to make operators better aware of plant dynamics
4. Need for better procedures for plant operations
5. Increased operational awareness and checking of plant conditions (safety awareness)

These essentially are the same as the recommendations of the Kemeny Commission (Kemeny, 1979), they did add better human factors design of the main control room and

other facilities. Kemeny was thinking of improvements related the utilities. Thinking about things a little later, recommendation would have included the NRC and INPO (formed later), especially with regard to using the simulators as a source of data on operator and training department performance. Remember the operators are at the sharp end of accident prevention, termination and mitigation!

The conclusion from the examination of VSM representation of the NPP organizations both before and after the TMI accident indicates that the difference fall into two parts, some organizational modifications in the structure, but a lot of changes in how these organizations are expected to operate and work together and this cover proper communications between managers and personnel. Some of the issues are associated with training and knowledge of key personnel and other issues are communications between operators, control room staff and maintenance personnel. A central role of management is to train and prepare their staffs to act in the appropriate manner during both accidents and normal maneuvers. Often in accident investigations the 'sharp end' persons are found guilty, however the accident investigators should look deeper to the underlying causalities. This has been pointed out by Dekker, 2005 amongst others.

One tool that has become more widely used after TMI is Probabilistic Risk Assessment (PRA), as a tool used by the utility management and by operations personnel in judging what actions can be taken without incurring unreasonable risk. The NRC uses PRA as a supportive tool and they talk about risk informed actions. This means that they do not totally rely on PRA, and use it to help them form judgments. It is pointed out that if one was not careful in considering human reliability concepts and just applying HRA modeling rules, one would find that the probability of the TMI accident would have been very low, i.e. unlikely. However, given the training of the control room crew, once the main feed water tripped and the maintenance crew left the auxiliary feed water isolation valves closed; the control room crews were very likely to fail with a probability of 0.5, 50/50 chance of failing as opposed to 1/100 or lower for trained crews.

The above are comments related to the TMI accident. There is a need to understand what needs to be known about an organization before one can judge whether the elements in an organizational method are necessary or appropriate. The approach taken here is to study an accident and see what is relevant and what is not so important. The VSM approach seems to reflect the structure of the organization, but it emphasizes quality control or regulator actions along with the same for communications. This is good, as failures in these areas are keys to failing to respond correctly to accidents. However, one need is to

determine what a good regulator is and also what defines good communications as far as the organization mission is concerned.

Clearly training of all personnel is great need in any organization. Deep knowledge of the process helps to define what actions need to be taken in any circumstance, and this is a requirement for both operators and managers. One aspect of VSM method is that it has underplayed are the requirements placed upon staff and management operating within a VSM framework. The training requirement could have been missed in the literature on VSM, but the training feature has been explicitly added in both Pre-TMI and the later VSM models to compensate for this shortcoming.

Here the conclusions are focused on the applicability of VSM as a method to understand the strengths and weaknesses of an organization. As far as the basic structure is concerned VSM has identified the roles of top management, lower management and the operations staff in terms of their relative positions in the hierarchy. VSM points out the need for good communications, leadership and decision-making. In this VSM replicates the requirements of controls and cybernetics. What more needs to be clarified is the exact design of the equivalent of the control system design and the characterizing of the communications between the various layers within the VSM structure or organization.

The VSM models of a typical US Nuclear Utility before TMI and later have been built based upon Beer's VSM model. The VSM elements within each of the utility models have been constructed based upon the interpretation of how the utilities functioned at specific times. The pre-TMI VSM is based upon an understanding of the industry at that time and the current VSM model is related to the current understanding of how the industry operates now. Industry management controls and operations have clearly changed over the years due to enhancements stemming, primarily, in response to accidents. Accidents have a way of informing society of what is important and what can go wrong. The supposition that something can go wrong does not seem to work very well with decision makers; but once it does go wrong then the proof is there and cannot be denied!

Seen in the light of Ashby's Law of Requisite Variety, see Chapter 4. It could be said that the industry did not realize that their view of how to control decay heat led to a failure to recognize the need for operators to fulfill the requirement of Ashby's Law and hence the accident proceeded to the point of destroying the reactor core!

5.5.2 Fukushima Daiichi NPPs Accident,

The accident referred to as 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 Station were the ones principally affected. The accident was caused by large earthquakes and later followed by large tsunamis. The largest earthquake and the some of the tsunamis exceeded the design bases for the nuclear power plants (NPPs).

The Fukushima accident is likely to have a notable effect on the nuclear community. The accident has also lessons on the scope of VSM and effect on the structure and interrelationships within the nuclear related VSM models. Before decided what are the lessons learned and their applicability to VSM modeling, the details of the accident need to be addressed. Analysis of the accident will be carried out and lessons as far as VSM implementation is concerned will be extracted. An early review of the accident (Braun, 2011) indicates that many of the details, which could be relevant to organizational response are not available. Some information of discussions before and during the accident between the top management, the government and the site personnel are missing or identified as suppositions and/or rumor. It is likely, that details may gradually come to light, but does not help here. Inferences made in the analysis process may be deduced from indications; it might be worthwhile to consider the impact of these uncertainties on VSM modeling.

The Fukushima accident took place in March 2011 and the news sources were full of statements about the accident for many weeks. Two sets of reactors owned by the Tokyo Electric Power Company (TEPCO) on the north-east coast of Japan were involved; these were Daiichi and Daini, Dai 1st and 2nd stations. The reactors were initially affected by a large earthquake (9.0 on the Richter scale) followed about one hour later by devastating Tsunamis. The earthquake appears to have done some damage, but the biggest effect on the reactor units was the Tsunamis. A short description on the accident sequence is given, but the emphasis here is on the roles of the plant operators, the plant management, TEPCO management and the Japanese Government, as well as can be judged and then related to VSM for diagnostic purposes.

5.5.2.1 TEPCO and Fukushima Plant Organizations

The following three figures 5.5, 5.6 and 5.7 are the organizations closely associated with the Fukushima accident. Figure 5.5 shows the relationship of the Japanese Government to Ministry of Economy, Trade and Industry (METI), Japan Nuclear Energy Safety Organization (JNES) and Ministry of Education, Culture, Sports and Technology (MEXT). METI has jurisdiction over Nuclear Power. JNES is an incorporated Administrative Agency with

experts who carryout facility inspections and offers technical support. MEXT is responsible for radiation monitoring. The office of the Prime Minister has a role in that there is a Nuclear Safety Commission (NSC), which deals with Policies to ensure nuclear safety, regulations and fundamentals of prevention of hazards due to utilization of nuclear power, radiations from fallouts and ensure the safety is important in being dealt with.

The second figure, Figure 5.6 is a simplified representation of the TEPCO organization with a focus of the managerial responsibly related to nuclear aspects, especially after the Fukushima accident, since the units are in recovery actions. The units are unlikely to operate ever again, because of the extensive damage and long term effects of radiation release.

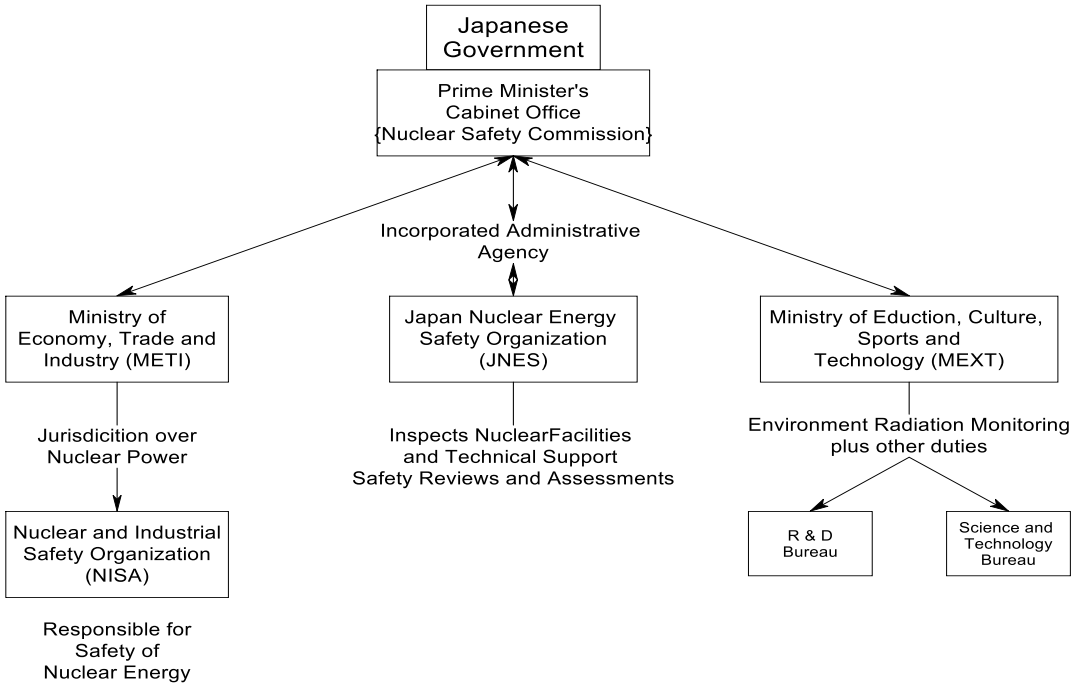

Figure 5.5 Overview of the Japan Regulator Organizations

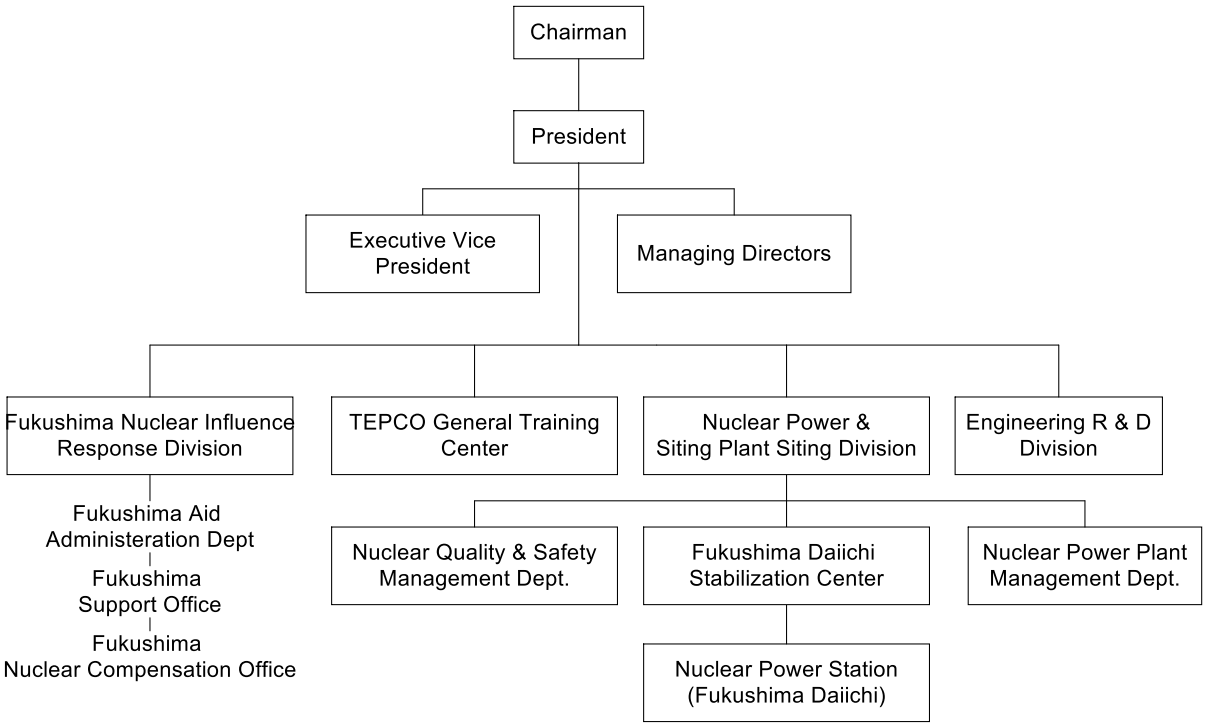

Figure 5.6 Simplified Version of TEPCO Organization

The site organization for the Daiichi units is shown in Figure 5.7. This figure was retrieved from the INPO report on the Fukushima accident report (INPO, 2011). The titles and working positions are not identical to those of a US NPP organization, see Figure 3.2. The Site Superintendent appears to be equivalent to the Site Vice President and the Unit Superintendent is equivalent to a Plant Manager and the Operations General Manager to an operations manager, the Shift Supervisor to a control room supervisor, Unit Senior operator to a reactor or 'at the controls' operator, Unit Main Shift Operator to a balance of plant operator, Assistant Senior Operator to a field supervisor and Auxiliary Operator to a non-licensed operator.

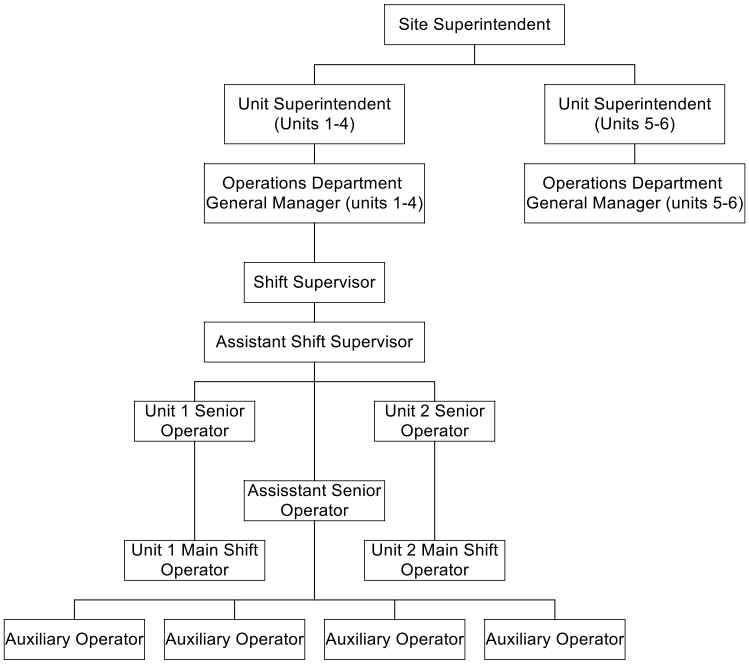

Figure 5.7 Fukushima Daiichi NPP Organizations

note: units 1 and 2 and 3 and 4 each have common control rooms

5.5.2.2 Comments on the Pre-accident Status

Before one can totally understand what happened one needs to understand some of the underlying history with respect to TEPCO and a little about the reactor designs. It has been recognized by various parties, such as the Japanese press and even organizations such as WANO, that TEPCO management were not the best in the industry. The BWR reactors at the Fukushima site were relatively old being designed before 1970s and that several upgrades had been recommended to deal a number of issues including hardening vents to avoid the possibility of hydrogen explosions that could cause the failure of the reactor building. In addition, the Japanese press reported that TEPCO's operations were not good. It was even suggested that certain tests of containment leakage rates were incorrectly carried out.

All NPP designs have been updated to ensure that they are better able to meet the latest safety standards. People have also review the bases for external events to see if more care needs to ensure that NPPs can safely ride through all external events, such as earthquakes, floods, etc. Studies by organizations, such as the US Geological Survey have pointed out new fault lines that have been discovered and these new faults may lead to a higher ground acceleration condition than that the plant was designed for, the so-called design basis event. The regulatory then orders that changes should be made.

In the case of TEPCO, they were warned by Yukinobu Okamura (Head of Active Fault and Earthquake Center) some two years before the Fukushima accident that the site could be threatened by a tsunami greater than the design basis event (CNN, 2011). TEPCO has been accused of not being very open to questions, (Shirouzu & Smith, 2011) and was found to have falsified records some time ago. TEPCO appeared not to take the suggestion about the tsunami very seriously and did not increase the seawall height or waterproof the NPP electrical installations. The managerial elements involved in the process of assessing and making safety changes are TEPCO management, the Japanese Regulator,(NISA) and the Japanese Government represented by the METI, see Figures 5.5 and 5.6.

5.5.2.3 Accident Description

A large seismic event (Richter Scale 9.0), was above the design bases for the plants and occurred on March 2011 off the north-east coast of Japan and caused large 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 accepted response. The actual ground acceleration was 0.56g versus 0.447g (design value). 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.

A result of the type of earthquake (a sub-duction fault), a series of large Tsunamis were generated (INPO, 2011). The INPO report was produced later than the Braun report and is much more detailed, but still does address questions related to why certain actions were taken. The Tsunami caused a lot of devastation to the area around the region where the NPPs were located. Many people were killed and their property was destroyed, roads swept away and rail transport ceased along with a loss of communications. The INPO report indicates that there were multiple tsunamis, some seven altogether. It also states that several after-shocks of lower magnitude 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 18.7feet (5.7meters), so the actual largest tsunami was well above the design basis and the ground level. Figure 5.8 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.

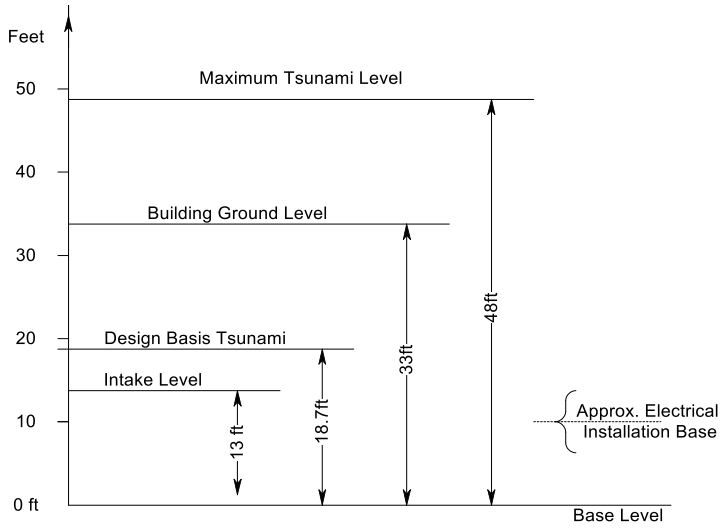

Figure 5.8 Diagram showing various water levels

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. (CNN.2011)

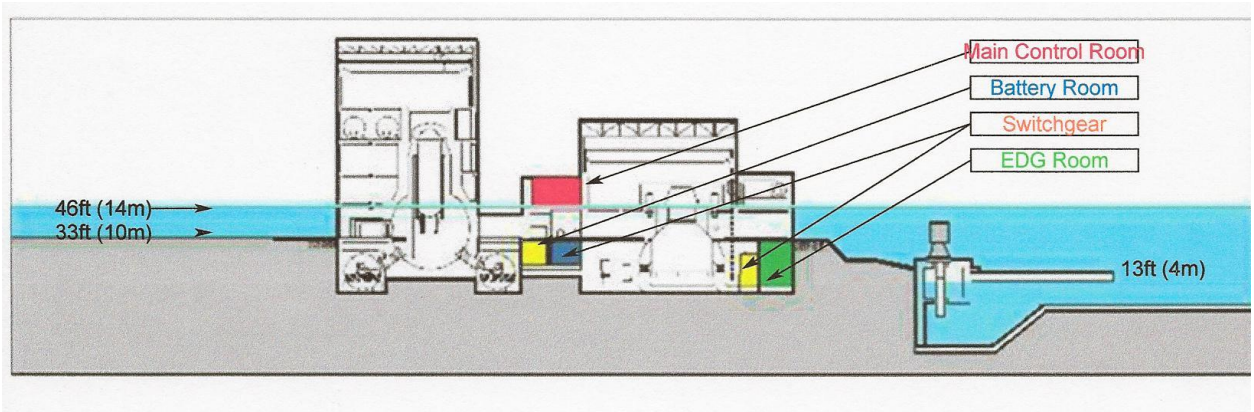

Figure 5.9 Diagram of NPP showing General Elevation and Flooding Level during Tsunamis (NEI.org)

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 to be

flooded, see Figure 5.9. There were some diesels that were air started, but could not be used since rest of the electrical systems had failed. The grade level for reactor buildings were 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. The usual mechanism considered for the loss of diesels is a failure of the diesels to start related to diesel generator failure mechanisms. 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 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 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 then organize the 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 were practiced upon were not designed for 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 (Japan Fire Department, 2011).

A number of accident reports relating to Fukushima were available shortly after the accident, for example, see Matthias Braun, 2011 (AREVA), 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 in the region of the various spent fuel pools, radiation releases, etc. Very rarely does one get a glimpse of what was going on 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 very involved in trying to establish control over the effected regions. The figures are that some 20,000 people were killed, many more were injured and missing, large tracks of houses were destroyed. It was a huge catastrophic event for the people of Japan. It is no 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 the problems. Is not clear that the NPP staff and managers recognized the possibility that given the failure of spent 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 into the direction of the spent fuel pools, which are high up in the remains of the reactor building.

The general impression is that the whole local NPP personnel were overwhelmed by the events but were trying as best as possible 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 others through leakage from the reactor building, and spent fuel pools. The full story is not 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 might be some time for a complete accounting of the accident sequence and the sources of radioactive releases are agreed.

The INPO report covers some of the difficulties that the site personnel had. Included in this dissertation are a couple of paragraphs to give an insight into the problems that the personnel had. The locations were dark, radiation was high is some locations, equipment was not working, earthquakes caused vibrations and the threat of explosions existed.

This extract is from INPO report dealing with unit 3:

'The operators understood they needed to depressurize the reactor but had no method of opening a safety relief valve (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 Center 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 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 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.

5.5.2.5 VSM for TEPCO Daiichi Organization- Prior to Accident

Prior to the accident, a VSM model of the TEPCO organizations associated with the Daiichi and Daini Stations would look similar to VSM plant models for other NPP organizations. Figure 5.10 depicts the organization from the TEPCO Chairman to the staff of Daiichi #3 unit. Compared with Figure 5.1 for a US NPP, there are some differences notably the presence of a CNO and INPO. There is an increasing emphasis on Probabilistic Risk Assessment (PRA) techniques, but maybe even in the case of the USA; use of these techniques could be extended. The CNO role is important in that it brings emphasis to nuclear safety and a better balance between economics and safety. If the TEPCO's top management had looked at the risk of a tsunami over the design basis size, they would have not taken the risk of failing to take action to increase the size of sea walls, move diesels to higher ground and have better water protection for their electrical equipment.

INPO is a US organization, but the World Association of Nuclear Operators (WANO) functions somewhat like INPO and TEPCO is associated with WANO. It appears that the Japanese utilities do not feel that the relationship with WANO to preclude future safety issues is sufficient and have stated that they will establish a new organization under the auspices of the Federation of Electric Companies of Japan (FEPC), as the Chairman said "We intend to create an environment that proactively accepts evaluations and advice from external perspectives so that the new system will function continuously in an effective manner rather than becoming a mere façade, (FEPC, 2012). This implies that in the mind of the Japanese utilities the net job done by WANO and TEPCO was not satisfactory, to quote…"a mere facade."

It is suspected that the issue was with TEPCO, but maybe WANO was not persistent enough. Not having a CNO position means that safety issues are not as strongly considered as they ought to be. Following the accident, the organization dealt with the reactor trip and loss of offsite power. The Head quarters Major Disaster unit was established at this time.

Initially, the response was carried by the control room operators. Warnings relative to the situation were issued by the site management to TEPCO management.

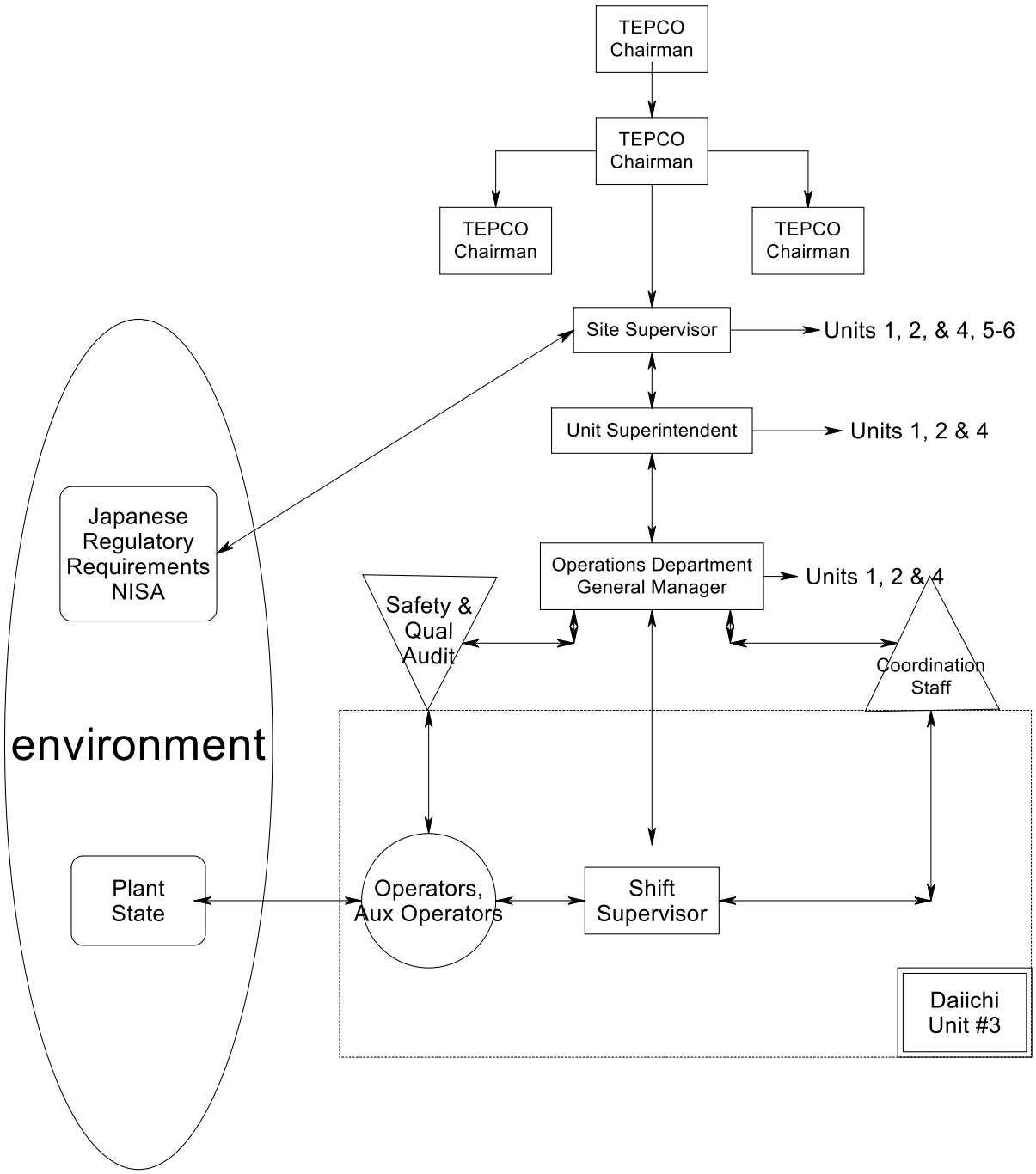

Figure 5.10 VSM model of the TEPCO Site Organization to the Daiichi Unit #3 level

5.5.2.5 Reorganized Daiichi VSM during response to Emergency

Soon after the tsunamis hit the stations, electric power was lost leading to a station blackout, and the staff morphed into one dealing solely with responding to the consequences of the worsening accident. The Emergency Response Center (ERC) was set up and the emergency plan was entered based on loss of AC power. Coordination of the responses for all Daiichi units was via the ERC with the site superintendent directing operations including investigations into how to inject water into the reactor to cover the core, etc.

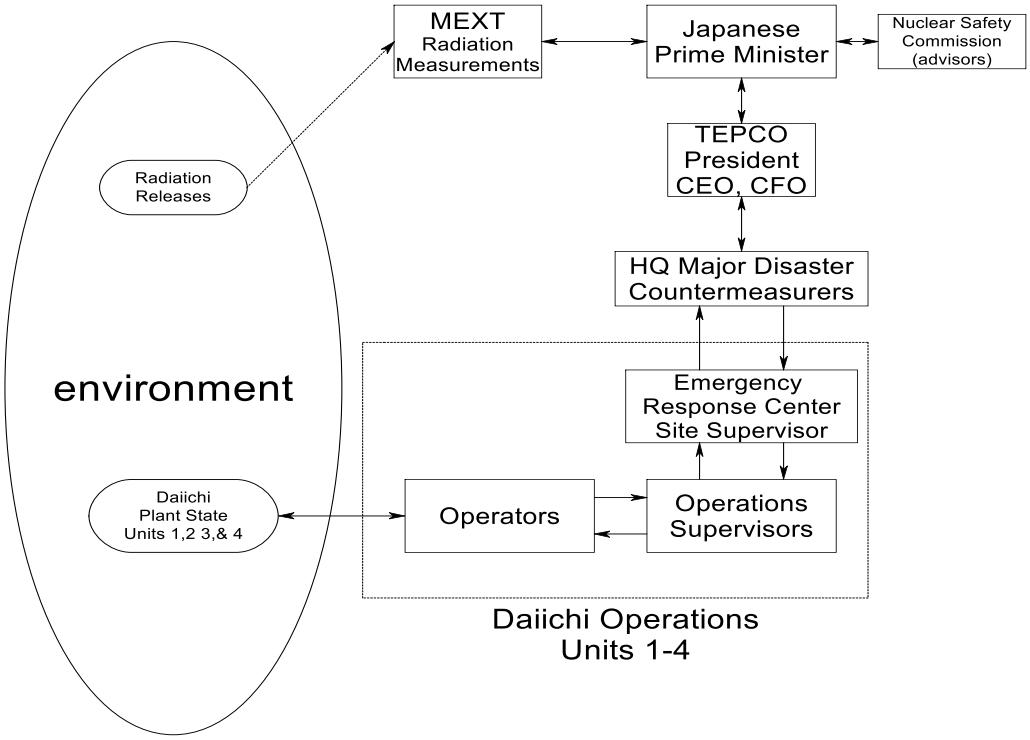

Figure 5.11 VSM Model of the Daiichi Emergency Operation Organization

Operators at each of the units were trying to energize various instruments and open valves in response to need to operate vents, depressurize the reactor, try to start pumps, isolation condenser, etc. depending on the assessed need of the specific unit and directed by the ERC. So the VSM structure corresponding to this situation differs from the VSM for the normal operation. The VSM model of the Fukushima Daiichi response structure to the accident is depicted in Figure 5.11.

This structure was much tighter than the normal organizational structure commensurate with the need to make local decisions depending on the state of plant and equipment. The bulk of the decisions and actions were taken at the lower levels of the organization. However in one case, the crews waited to take an action not wishing to place the local population at risk if the reactors containment was vented. Most of the public had been evacuated, but some people had not left. If the population was there during a release it is likely that that they could have been exposed to radiation damage. The staff later requested permission to do this and the Japanese prime minister gave permission.

5.5.2.6 VSM Considerations

As was stated at the beginning of the chapter, although the details of the accidents are interesting what is being investigated is the utility of the VSM approach to representing an organization. Here the NPP Organizations represent those of a different country. So there are some differences related to how organizations are set up in Japan, but also insights into Japanese culture and its effect during an accident. The impact of US nuclear technology and regulatory measures has had an influence upon the Japanese nuclear industry; however it does not exactly replicate US NPP industry. Table 5.2 shows a comparison between Fukushima Daiichi Station and a typical US station. The data given in the table is based upon various reports, but the Fukushima data has not been obtained directly from TEPCO.

Some of the lessons that have been built into the designs have been derived from experiences with accidents and interactions with INPO and the NRC having had an effect on the US industry, but does not appear to have changed TEPCO. The CNO position is one that does not appear in TEPCO's organizational chart but does appear in the US utility organizations. Another question arising is in the training of operations personnel with respect to risk identification, via PRAs and better training on station simulators. However, the operators performance and that of the unit and operations supervisor and their staffs seemed be very good and they should be recommended for their courage.

The principle issue seems to be one that tends to affect top decision-makers, making decisions without deep consideration of safety and overall risk to the enterprises that they control. Clearly, the seawalls should have been built-up and all electrical equipment moved to higher locations, including the diesels.

Item	Fukushima	VSM Representing

		current US utilities
Top Management	Not Nuclear Trained Seemed distant from NPP Operations	Some Limited Nuclear Training
CNO	N/A	Nuclear Trained
Plant Manager	Likely SRO Trained	SRO Trained
Training Manager	Central Training Facility Do have a plant simulator	Director grade, SRO and Simulator trained
EOP Design	Symptom-based	Symptom-based
Communications	Mgmt / staff-restricted	Better communications btw personnel
NISA/NRC for US NPPs	Limited role for operators	Better awareness of operators requirements
WANO/INPO	Limited visits by WANO	Strong connects with Utility mgmt/personnel
Risk Mgmt	Early PRA models	PRA, limited conditions
Emergency Planning, abnormal conditions	Limited	Emergency Planning under limited conditions

Table 5.2 Comparison between Fukushima and a typical US NPP

However, the designers of the BWRs do play a part in this decision process. The whole design of the BWR was promulgated based on reducing overall plant costs. Civil engineering construction costs dominate NPP costs, it used to be 4 to 1 for civil and layout costs versus nuclear manufacturer costs! Hence the need to integrate equipment into buildings to save as much space as possible, hence putting electrical equipment in basement areas of the reactor and its buildings.

The change in an organization following an accident, especially one that results in extensive plant damage, is seen as a change in control and direction. In normal operation, the top managers clearly are in charge and make decisions based upon their perspectives related to safety and plant economics. However, once the situation changes the local plant personnel are fully in charge and are dependent on the planning previously carried out and the skills

and knowledge of the plant personnel. The impact of the top management is much less than actions of the operators trying to recover certain equipment to get it to operate under very difficult circumstances of no power, lost instrumentation, difficult access to means to energize the equipment, etc. This is where deep understanding of the plant and how it is operated is required. Such questions come up; where is the air supply for this relay and can it be operated by an air bottle? How can I get to it? What is the radiation risk?

The Daiichi staff assembled drawings and white boards, to help solve some of these problems. This takes time, including reconnoitering the damaged plant to see what state the equipment is in. In the case of this accident, time was of the essence in that releases of hydrogen needed to be made before an explosion occurred and wiped out much of the good done by the actions of the crews. The lesson from this is to go through scenarios that are more severe than might be expected, so that a whole range of questions related to availability of tools, and aids can be addressed before one is left searching for something that might do, such as a appropriate battery rather than going to ones' car to see if it will do! Clearly, some emergency planning had been done, but the situation looked much more extreme than was planned for. For example, did the planning cover the fact that the conditions in the torus were bad and that the crews would need to go into it? So it seems that some change of scope is needed relative to emergency planning to extend the planning to things more severe than the design basis events. Much the same as the move that was taken to run multi-failure scenarios on the simulators, as opposed to the older single failure scenarios, to better help operators when actual accidents occur.

Observing the station's response to trying to prevent or terminate core damage is equivalent to meeting Ashby's Law incrementally by identifying the Requisite Variety necessary to control the outcome of damaging the core. Unfortunately, their actions were unsuccessful because of time limitations.

So the lessons from the Fukushima accident as far as VSM modeling for NPP organizational structures are that the whole emphasis behind the design of the organization can change in response to an accident. The worse the accident, the bigger is the change. VSM models have identified the presence of a planning group that looks at the environmental changes to help predict what steps management needs to make to response to these changes. In the commercial world of shoe manufacturing, it might mean a change to the color of the shoes or the shape. In the world of nuclear power operations, it means consideration of safety and risk in changes in operations, but also if an accident occurs and how best prepare to minimize the risk to the public and to the company. One can see here in this accident, the viability of TEPCO is questioned. It is likely that the Japanese Government may have to

come to their rescue to prevent their financial demise. VSM indicates the elements within the structure that ought to be identified, but as important is to recognize what their role is and how important it is to the survival of the organization, both from a safety and from an economical view point.

So there are two things that need to be identified relative to VSM models as far as nuclear power plants are concerned. These are to identify the position of a representative at a senior level to represent safety at the top management organization , equivalent to a CNO, and identify a function to carryout broader risk studies not only for safety of the public but also financial survival and expose top managers to this information. The ability of NPPs to recover from accidents is important both for the public and for the company's survival.

Another thing to consider is that NPPs must have trained staff and resources to quickly respond to a range of accidents. This means more than just thinking about probable accidents but NPP crews must be able to respond to improbable (maybe one should say less probable accidents, like the large tsunami in the case of Fukushima)! This function should be the integration of the CNO position and the training department. During the studies under the auspices of the CNO, the investigators would cover emergency response planning for different accident trajectories along with training requirements and devices needed during execution. During the studies they would also identify time lines for needed actions and the consequences of not meeting those time lines.

Here in the analysis of VSM models, one defines the improvements in the VSM structure and the requirements for each of the functions. Clearly, some utilities have been functioning quite successfully, but every accident can reveal potential strengths or weaknesses in the management structure and plant operations of a given organization. The weakness of the TEPCO organization may not have occurred in another organization and this also goes for weaknesses in another utilities BWR plant design. As was pointed out in chapter 3, equation 3-1, the failure probability is made up of several components, including power design and management decisions.

5.5.2.7 Conclusions and Comments

Some of the conclusions can be derived from the study of the Fukushima accident itself and others are derived from the development of the VSM relative to the accident. The conclusions from the Fukushima accident itself are as follows. Reading of the references, particularly the INPO accident progression description along with comments from Japanese representatives, such as Mr. Madarame confirmed problems beyond underestimating the size of the large tsunami that helped destroy the plant. There were some weaknesses in the

design and layout of the plant, which made the damage worse, but a significant contributor was the failure of staff to respond quickly to limit the damage and release of radioactivity. Again, this was a case of not being prepared and having a detailed and practiced emergency plan to deal with the developing situation. The station crews tried to act correctly, but it was beyond their capabilities. They needed a developed plant, and tools, like batteries, lights, power lines, etc. so that they kept ahead of the wave of accident induced effects, like hydrogen explosions.

NPP issues:

1. Failure of TEPCO and METI/NISA to re-examine design-bases of the plants with respect to advice on possibility of a larger tsunami accident in the light of decisions related to the possible of a much larger than design basis tsunami
2. Failure of TEPCO to develop and practice comprehensive emergency plans. They did have emergency plans, but not based upon what actually occurred
3. Failure of the Japanese government to understand limitation of licensing process and their responsibilities in the face of large accidents beyond the scope of the utilities operating license, *note #1
4. Failure in understanding need of speedy decision-making to minimize the effects of the accident, ** note #2
5. Possible limitation of Japanese culture of conformity, waiting for top management decisions in use of sea water injection and reactor venting, ** note #2
6. TEPCO's general lack of transparency, safety awareness, and avoidance of carrying plants' safety upgrade recommendation, ***note #3

Note #1: Mr. Haruki Madarame, the head of the Japanese Nuclear Safety Commission (NSC), that is part of the Japanese Prime Minister's office said, "the country' regulations were flawed", (New York Times, 2012)

Note #2: Mr. Madarame also said, "there was a bundled response", (too slow to act)

Note #3: Madarame said, "although global standards kept on improving, we wasted time coming up with excuses why Japan didn't need to bother meeting them"

Clearly, the lessons learned from the Daiichi NPPs accident could apply most countries. Given here are a set of things that should be carried out:

1. Develop an organization that has a direct communication channel between top management and the plant supervisors and identify a top manager to be directly responsible for plant safety

2. Check to see if emergency plans are developed and tested. Ensure that changes in plant design basis leads to a modified emergency plan
3. Check to see any environmental and/or engineering information should lead to a change in plant design bases, every year or so
4. Licensing authorities need to consider whether the license imposes requirements on the government as well as the licensee
5. Check and test understanding of top managers, plant managers and station personnel whether they have a good understanding of reactor safety
6. Check to see if cultural attitudes have a poor effect on decision-making and evolve ways to deal with its effects

5.5.3 Challenger Shuttle Accident

The Challenger accident is another well know accident, but it is useful to look at the accident through the eyes of the VSM analyst. In the analysis section a very brief accounting will be given sufficient to provide context for VSM modeling and to draw conclusions about some of the shortcomings of the NASA organization. The Challenger accident is covered in The President's Commission Report (Rogers, 1986) and is very detailed. The material given in this section is for the purpose of understanding the decision-making process and communications leading up to the accident rather than focusing on the accident progression.

5.5.3.1 Accident Description

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 (SFB) units attached to the shuttle. The leak was due to a SFB 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 SFB units 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 was killed.

5.5.3.2 Accident Analysis

In the history of Shuttle launches, there had been a number of near misses with the "O" rings in the past, but none had actually succeeded in burning all the way past the two rings. But there was sufficient proof that there was a problem associated with the SFB joints and the "O" rings. The seals consist of two "O" rings plus packing materials. There were different degrees of damage for launches from none to some. After normal launches the SFBs were recovered and restored for future launches. It was during the refurbishment process that the degree of burn-through the rings was discovered. This information was important element in the decision process for engineers and managers.

The two groups formed a different view of the data, when it came to the launch of the Challenger. The view of the engineers was conservative in that they said that the conditions for launch were too cold and it should be postponed until conditions were warmer. The engineers felt that the conditions were outside the range of known results and therefore one should wait until such time they were more predictable, i.e. warmer!

The managers formed the opinion that the fact that since there were no complete "burn-through" conditions for the previous conditions, the data just confirmed that the design was acceptable and therefore the launch should go ahead. The results seem to suggest that things were worse the colder things got.

However, before ordering the launch they contacted a Vice President at the solid rocket company for support of their position and after some discussion he complied with their position. 'The customer is always correct! and if the customer is not correct, read the first statement'! This seems was a case of NASA managers only wishing to hear support for their position. There was a political reason behind the moves of the top NASA managers, in that one of the astronauts was a teacher and President Reagan was to announce this fact during one of his speeches. The launch went ahead and the result is known. The managers were wrong and should have taken a more conservative position. This position was a move away from the normal mode of behavior of NASA, especially as SFB joint was judged to be a Category 1 level risk contributor! It is important to understand the politics of the time; President Regan was going to announce a "teacher in space" plan. This was supposed to be announced in a speech due to be made shortly after the launch. What NASA forgot is that rockets are not that reliable and they were trying to sell the idea to Congress that NASA

had a bus type operation with the shuttle, not a very dangerous operation, and this was what was behind the plan. It seems that they proved the case, rockets are not that reliable!

5.5.3.3 Organizational Analysis

Figure 5.12 depicts the VSM equivalent of the NASA launch organization. The diagram shows a number parts of the NASA organization with personnel in Houston and the Kennedy launch site. The top managers and mission control are at Houston and the shuttle and associated personnel including the astronauts are at the Kennedy Space Center (KSC). The Morton Thiokol facilities are in Utah. So launch preparations and launch are centered on KSC and the decision-making are centered in Houston. Communications are by phone and are extremely important, and the decision-makers do not see each other face to face.

The analysis of the organization actions are relatively simple, the top management of NASA simply did not wish to delay the launch of Challenger and believed their analysis of “O” ring reliability despite the advice received from their own engineering staff. They later contacted the solid rocket supplier (VP) and requested his support in this analysis, which understandably was given later. This position was counter to NASA’s own expressed view of tolerable risk. NASA often delayed launch under much less onerous conditions such as when a redundant sensor or computer was not functioning correctly. The conservative position and engineering advice position would have been to delay launch until shuttle temperatures would have been higher and not as cold as was recorded. Also, NASA should have more closely investigated the “O” ring characteristics following the occurrence of near failure reports. This is an indictment of the whole organization. Why were these indications neglected?

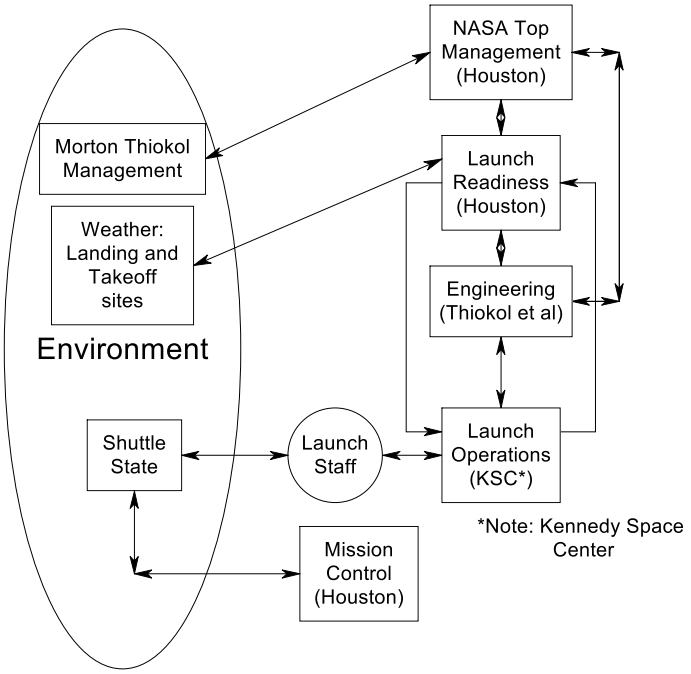

Figure 5.12 VSM equivalent of the NASA Launch Organization

5.5.3.4 Conclusions

This section discusses the conclusions relative to accident and the NASA decision-making, but also considers the lessons learned relative to the use of VSM characteristics about this organization and is there anything to be learned that could be applied in both cases.

The conclusions from the Challenger accident study are relatively straight-forward:

1. NASA top management wanted to launch the Challenger on time and did not wish to hear any engineering 'overly conservative engineering opinions', because of implied political pressure. Interesting the pressure seemed to be self imposed by NASA, since no trace of a request from Reagan has been located.
2. NASA should have investigated the "O" ring near failures earlier. This was a failure on the part of NASA and Morton Thiokol. There are suggestions this was a failure of personnel at lower levels to forward information on the problems with the design of the "O" ring joint
3. NASA had a launch review procedure, the launch directors should have followed a more conservative process based upon engineering advice

If one was considering what could be done by NASA shortly after the accident, the following set of requirements might have been useful, that opportunity has passed. NASA did not seem to be prepared for the next shuttle accident that occurred, Columbia in 2004.

1. Base evaluation of a situation on the best advice available and take a very conservative view
2. If there are indications of a key system or component approaching a failure state confirm issue with tests covering worst case environment and redesign to reduce risk
3. Evaluate the risk parameters and compare them with the benefit
4. Do not assume that the government necessarily wants to accept responsibility for an operation
5. Never assume that the system is safer than has been shown

5.5.3.5 VSM Considerations

It was stated at the beginning of the investigation of the accident, that there might be lessons learned relative to the application of VSM to organizations and features that might affect VSM itself. Since VSM is based upon cybernetic principles, one can see some of the weaknesses in the NASA organization. These weaknesses relate to communications and having a better assessment of risk. The communications seem to be based upon the old fashioned management approach hear what I say and do not talk to me, my mind is made up! Clearly you employ people because of the expertise and therefore you should listen to them, otherwise why did you hire them. In the cybernetic world a system does not work too well with only one way communications. It can lead to an instability, the other way is failure to control the process*.

*Note: *Beer has introduced ideas associated with attenuation and amplifying variety between managers and processes, see Heart of Enterprise, pp. 98-100, which can affect Requisite Variety. In this case NASA management attenuated the variety of the process and this in turn led to the failure to see that the launch would lead to the shuttle failure. They did appear to be open up to advice to amplify the variety, but 'forced' the VP of Morton Thiokol to support their position.*

NASA management did not at this time take into account of probabilistic risk assessment, particularly if one considered uncertainty. Later versions of VSM relative to high reliability industries it has been suggested that they use risk measures to guide their decision-making. Clearly, the NASA management did not factor risk assessment into their decisions and jumped to the conclusion that if all was OK before, it must be OK now, even though the parameters had changed and they did not do a re-evaluation. Incidentally, all organizations ought to have a risk assessment group to evaluate the risk of decision-making even in the commercial world, without it one is diving off the high board to land where?

5.5.4 North-East Utilities Operation, 1986 onwards

The point of examining the North-East Utility operations was to draw from operations that can go wrong even after having been operated successfully for some time. The study should provide light on the requirements for management in terms of what works and what does not. It could be that the structure of the organization is the same, but how the jobs are carried out and the effects of informational direction and feedback can be critical on the effectiveness of the operation. It is understood, in the field of controls and cybernetic, that feedback is important; the degree of feedback can be stabilizing or destabilizing. The same is true in organizations, but one must also understand the decision rules used by the organization. In this example, both sets of issues are present.

Not all situations involving organizational problems result in an accident. Sometimes, a change in the top management operational philosophy can lead to a changes for either for the better or worse. In the case of North-East utilities (NU), it was for the worse. The author was a consultant to NU and was involved in a Probabilistic Risk Assessment study for one of their plants, Connecticut Yankee NPP. At this time, NU was considered to be one of the most progressive organizations among the US NPP utilities. NU operated four nuclear plants at the time, Connecticut Yankee (CY) and Milestone Units 1, 2, and 3. CY was a Westinghouse Pressurizer Water Reactor (PWR) NPP, Milestone unit #1 was a Boiling Water Reactor (BWR) (General Electric), Milestone unit #2 was a Combustion Engineering (CE) PWR and Milestone unit #3, was a Westinghouse PWR. Having reactors of different designs is not an easy task to manage and operate all efficiently and safely. This aspect can lead to problems if staff numbers are reduced significantly.

The top managers were: Bernard Fox, President and Williams Ellis, Chair and CEO. These managers had a philosophy based upon the idea that NPP utilities had to be cost effective and compete with the low cost coal or gas electrical generation plants. There were indications that there were going to be changes in the industry as it moved to a deregulated world. A report prepared by McKinsey suggested that there would be moves toward lowering of cost of electricity due to entry of low cost suppliers, such as units using gas as the fossil fuel. It was not going to happen soon, in the opinion of the Connecticut regulatory agency, the Department of Public Utility Control (DPUC), who thought that NU management considerations was an over-reaction to possible competition in the electric markets. It should be pointed out that Ellis was previously employed by McKinsey and acted as a consultant to NU.

5.5.4.1 Accident Analyses

The previous cases studied devolved around accidents; in this case study 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. Details of the reductions are given in the section below.

As a result of the top management actions taken to reduce staff and being too heavily focused on costs, led to plant availability falling from about 90% to 56%. Problems occurred at the plants could eventually could lead, it was 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 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 was 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 and was concerned about its impact on plant safety and whether there was sufficient protection for whistle blowers from management action, the usual concern was "kill the messenger" approach to issues by those in control.

5.5.4.2 Analysis of the situation

The development in management philosophy led to change in the philosophy of how the plants would be operated. The analysis of NU operations from the period 1986 to 1996 depends on data gained from a book by MacAvoy and Rosenthal, 2005.

The President and CEO decided that overall costs of operating the plants had to be reduced and to do that they had to reduce man-power costs, i.e. reduce the numbers of staff. President Fox presented to senior managers, "A Strategy to Meet Competitive Threat," in October 1987. The basis of the presentation was a reduction target of 13% below projected

costs by 1990, with a 7% reduction in operations and maintenance costs and 13% reduction in Nuclear Engineering and Operations costs, (MacAvoy and Rosenthal, 2005).

If one compares operating a nuclear plant with a gas fired plant, one quickly realizes that staffing requirements are much higher for NPPs, especially in the areas of operations and maintenance staff. This is due to two effects, the greater need for safety and the greater complexity of NPPs. Interestingly, both aspects are linked, since a NPP has greater redundancy than either coal or gas fired plants.

The philosophy of running a NPP is to try ensuring that failure of a system does not lead to an unsafe condition. This means that one must pay attention to both maintenance of equipment and having sufficient well trained operational staff to run the plants. Under the previous operating philosophy, all four plants were well run and the NRC rating was high based upon their performance

For a fossil plant, if a system fails, the worst case situation would be some limited physical damage to the plant and the possibility of a small number of staff getting hurt or killed and the plant would be shut-down for while, repaired and restarted. In some cases, if a system fails the plant can keep going and repair can be made while it is still producing power. Safety systems in the case of fossil plants are very limited, compared with NPPs. In the worst case scenario a nuclear plant would be contaminated, permanently shut-down and there could be a number of deaths and persons affected by radiation leakage, see Daiichi NPP accident.

The actions taken by management led to a reduction in staff by the mechanism of early retirement and by lay-offs. Some figures may reveal how the reductions were working: Mr. Fox announced that some 1,500 work force positions were to be reduced over five years in a statement made in 1992, see page 66 of MacAvoy and Rosenthal.

The strategy adopted by NU management clearly led to a situation, which brought it into conflict with NRC imposed safety criteria in terms of availability of both reliable equipment and well trained personnel, since both were affected by NU actions to reduce costs. In addition to conflicts with the NRC and also, inferred, with INPO. The NU staff also became involved, since they reported plant related safety issues, first to NU management and finally to NRC.

The operational history of the plants gave concern to the NRC and even the DPUC, who asked about reliability of power supply to customers. The NRC interacted with NU on the problems associated with the plants, leading to shutdowns and trips. Bit by bit NU plants

moved from top rated plants to bottom rated. In response to NRC pressure, NU management (Fox) made promises under a Performance Enhancement Plan (PEP) to improve plant performances by adding 450 staff in Operations & Maintenance (O & M) and leading to capital expenditures of $40 million in 1992. PEP was proposed to take care of forced outages at the Millstone plant in the period 1991 to 1992. The objective was to restore NU to high level of excellence with 450 employees added by 1994.

The expected enhancement in performance did not occur and a '442' event occurred in August 1993. This event was related to a safety-related valve failure in which NEU staff tried to fix by usual maintenance techniques without realizing its safety implications. The actions and processes are discussed in great detail in the first case study in a book; Constance Perrin, 2005. Although she takes care not to mention the plant, however reading the MacAvoy & Rosenthal book enables one to make the connection and the plant is Millstone unit 2. This incident is covered in the next case study. Also the NRC did not consider this to be an isolated incident!

By 1994 considerable deterioration had occurred in running the five plants, including New Hampshire Seabrook PWR NPP, which had been added to NU's portfolio of plants. The average capacity factor was 57.6. This occurred at a time when overall industry availability was more like 90%. The deterioration in plant performance got to point in that in 1995 both the NRC and INPO had meetings with the Board of Trustees rather than management to draw attention to the problems. There was no documented response by the Board to these meetings, but nothing was changed as a result. INPO was, as has been pointed out earlier, the industry's self regulator. This response to the situation was not expected by INPO. The NRC's Executive Director, James Taylor, met with the board to point out the lingering problems at the Millstone station. As a result of these two meetings nothing changed and the NU management remained in place!

In 1996, the NRC designated NU a Level 3 company on the watch list, [Systematic Assessment of Licensee Performance, (SALP list)] and ordered all the Millstone plants shutdown and not started up until they were reconstructed and relicensed. The final stage occurred with full core offload of the Millstone #1 plant, was found to be outside of the Final Safety Analysis Report (FSAR) requirements. This was brought to the attention of the NRC by a whistle blower after many times trying to bring this to the attention of NU management. This action, in turn led to the process of looking at compliance with the FSARs for all three plants. This led to deeper NRC reviews which in turn led in turn to a finding of a lack of an "effective corrective action process" by the NRC as to the condition at the NU plants. This revealed important instances in which "degraded and nonconforming conditions were not

properly corrected." The line management was found not to have responded to their quality assurance organization and of root causes were not identified!

In a later report, by M. D. Quinn of Millstone staff (MacAvoy and Rosenthal, 2005) stated that the objectives of the PEP program had not been met! Reviews of plant state found many instances of all kinds of problems stemming from failures due to a lack of staff in engineering, to decreased reviews and a lack of understanding of the FSAR requirements and the elimination of some engineering supervisor and manager positions! A lot of details are not given here, but the message is quite clear, the reduction in staff and capital eventually meant that things did not get fixed. Staff tried to keep the plants running by 'work-arounds.' 'Work-arounds' are usually temporary fixes to enable systems to continue to operate. In the case of safety systems, this approach is not acceptable, since the required reliability cannot be met. In the case of the severe problems, the plant should shutdown. If the issue is with a redundant channel of the safety system, there may be technical specification allowing the channel to be removed, fixed and returned to service, but the time allowed for this is limited.

Eventually, the Trustees got the message, but it was too late! There was a reconstitution of the Trustee group. Following the Millstone plants shutdown, the board kept the current management in position. Finally, they fired Mr. Busch nuclear chief and replaced him with Mr. Kenyon, who ousted several other executives. NU did not survive as a nuclear utility and the NPPs were sold. However, the top managers never were punished for their activities!

5.5.4.3 Organizational Analysis

It is possible to use VSM approach to analyze the NU organization, along with relationships with the NRC and INPO, as well as with its own staff. The approach is similar to those taken above, that is to look at what are the key interactions and rules that were not followed. NU's management philosophy meant that as far as NU was concerned it lead to short term improvements in profitability by adopting an approach which was in conflict with NRC's mandate from Congress. This mandate is to ensure safety of NPP operations and ensure the health and safety of the public from the effects of radiation. In the long term, the policies of the NU management lead to the destruction of the utility, hardly a case for celebration. Many of the participants cannot be congratulated for their roles in this case. None of the following can be pleased with what happened:

1. Board of Trustees failed to sack Messers Fox and Ellis even when informed of their activities by NRC and INPO

2. NRC for failing to act sooner and being too willing to believe Fox and Ellis's proposals to fix things, such as the PEP program
3. The Connecticut DPUC for failing to clearly state that they would not institute a low cost policy for electric power
4. Showed INPO's perceived strength dealing with utility management could be overplayed

The idea of a utility pursuing a high efficiency operation is not the issue. NU undermined this idea by the way in which they did it. If they had worked with their staff to make them more responsible to determine areas of increased efficiency to reduced costs, it might have worked. They pursued a cut manpower policy to reduce costs, which in the end caused deterioration in both equipment reliability and personnel motivation. They also disregarded the messages coming from their staff and even more having placed their line managers in a poor situation caused by lack of funds and staff, fired them when the NRC said that these managers were at fault. Equally, the NRC can be blamed for not getting at the root cause of the problems!

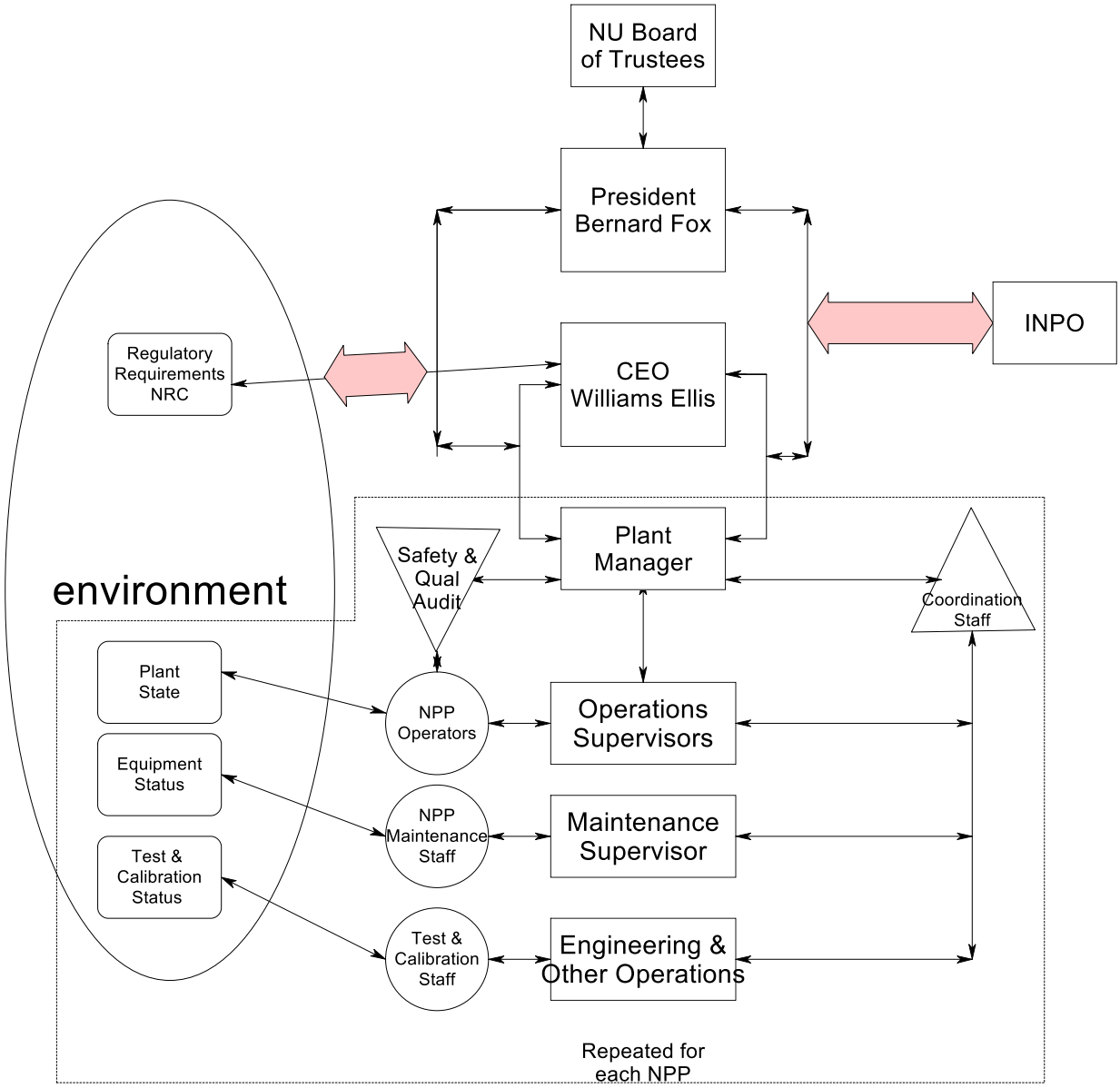

Figure 5.13 Organizations associated with NEU NPP Operations

5.5.4.4 Conclusions

There are a number of conclusions stemming from the NU fiasco and how they are related to how NU was run, what their relationship was with the NRC and INPO. Clearly, like the management of NASA, the NU management pursued their ideas almost without reference to

others and even their own staff. Even the Board of Trustees did not understand their responsibilities and allegiances in this case.

1. Boards of Trustees represent the owners (shareholders) interests not that of the management
2. NRC should follow up poor performances quickly and act to shut down operations before a large accident occurs
3. Utilities should learn from poor NU management decisions and approach efficiency enhancements without degrading plant safety
4. Utilities should pay attention to staff concerns
5. Middle management should take a strong position on operational issues with upper management
6. State PUCs should be careful in dealing with NPP rate issues, to ensure rate payers interests are not only be reflected in low electricity charges, but also in safe NPP operations

5.5.4.5 VSM Considerations

Figure 5.13 represents the structure of Northeast Utilities at the time of the incidents. It shows how the organization is interlinked and operates. Unfortunately, the structure of itself does indicate how it operates. From prior investigations, it has been pointed out how an organization can improve by the introduction of the Chief Nuclear Officer (CNO), who represents the safety requirements of the plant. There was a lower level person that had something approaching this responsibility, however either his voice was not heard or his opinion was overruled.

When the top managers in an organization pursue courses outside the real interests of the organization, it is unlikely that anyone at levels below them can affect any change. These persons have not power. It is up to the Board to correct the situation, but many times they do not have the information to correct the situation. The only outside organization that has the power to take strong actions, in this type of case, is the regulator. However, they cannot remove the management only shutdown the operation. INPO can advise and in concert with other utilities discuss the consequences of the utility continuing in its poor behavior.

Figure 5.13 reflects NU just before it went out of business and if the actions recommended by NRC and INPO had been taken by the Trustees earlier, it may have been possible for NU to continue as a viable utility as it was before the actions taken by Ellis and Fox, aided by others. One additional point, to be made, is the role played by the McKinsey Company in coming up with an economic based study on reduction of costs in the nuclear utility

business, possibly without realizing the implications behind the cost savings. It might still be possible to run NPPs more cost wise efficiently, but the first thing to remember is that the plant must run in such a manner that safety is the highest need! Many of the recommendations should apply to utilities and others in the nuclear power generation field, or other safety sensitive industries.

One could argue that Fox and Ellis did not understand that their actions reduced variety and that the requisite variety was not met to ensure both safety and economics. If they had not destroyed variety by their actions in reducing staff levels without compensating by increasing station personnel efficiency things could have worked. Furthermore, they failed to listen to outside bodies (NRC and INPO), who warned and advised them to change their attenuation of what are now seen as necessities.

The key finding from this study is the power of the top management to dominate the actions of a utility and this holds equally for other organizations, for example NASA. The role of the Board of Directors or Trustees is the key to ensuring the top management adheres to the right principles of running a company from a number of points of view. One can suggest how an organization can be effective, but if the wrong selection of the top manager is made then it falls on the Board to act, rather than wait for an accident or reduction in the effectiveness of the company to intercede. Clearly, accidents are very strong feedback mechanisms.

5.5.5 Arrow NPP: a near Accident caused by a Valve Failure

This is an account of a near accident at a Nuclear Power Plant called the Arrow plant. This is in fact a fictitious name given to the plant by the author, Constance Perrin. In her book she deals with the organization aspects of the Arrow NPP staff dealing with a leaky valve and she has analyzed it in detail in her book, *Shouldering Risks: The Culture of Control in the Nuclear Power Industry*, 2005. On closer analysis, it appears that the plant was the Millstone Unit #2 (Combustion Engineering NPP) and the problem was mentioned in MacAvoy and Rosenthal's book as problem with valve in event 442. It is not proposed to discuss this near accident in detail, but rather draw on Ms Perrin's work relative to the workings of the lower levels within the NU organization and their relationships to each other and the top management. Figure 5.13 shows the NU organization and here the focus is on the lower branches personnel in the diagram.

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, as discussed the above section. These issues were due to reduced manpower and loss of

the more skilled personnel taking early retirement or being laid-off. Ms Perrin's work indicates a couple of things, a lack of awareness on the part of some of the staff of the defense in depth requirements as they relate to valve boundaries and the lack of management close direction of the different working groups.

Ms Perrin is a cultural anthropologist and her approach was to interview persons in various teams in a manner similar to doing an anthropological investigation and draw insights from these interviews about the organization and how it operates. Groups within the organization were from:

1. Maintenance
2. Operations
3. Root cause analysis
4. Engineering

These groups are identified in figure 5.13, with the exception of the root-cause group, which it is believed was within the safety analysis/audit group. Her approach is very different that that taken here. Her method is to interview all crew members and record their very detailed comments relative to the valve problems and the decisions made and actions taken. The information provided by her, illuminates the relationships between all of the different crew members but also the underlying impact of management on decisions and actions.

The valve issue started after there had been a long shutdown and the problem appears to be leakage past valve packing. Another factor, that had an effect, was the pressure to return the plant to operation. Meetings were held at different times and different levels of understanding of the issues among the participants and hence different 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 and 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 refueling condition. 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.

The report by Ms Perrin is very detailed and conveys a measure of confusion and conflict between and among the personnel. The teams did not work together as one would wish. Ms Perrin is a cultural anthropologist and has caught the attitudes and views of the group of workers and managers. The situation presented is worrying in terms of the ability of the teams to quickly and correctly solve pressing safety issues.

These issues point to a lack of coherence in the approach to safety issues. There was a need for the teams to work closely together to solve the problem having first defined the problem. The situation seems to reveal a lack of training in problem solving and clear understanding of the roles of the various departments in this process. The upper management has the obligation to ensure that all supervisors and line managers are trained in plant and radiological safety. The stepwise training processes adopted by Rickover for the Nuclear Navy could be very well been applied here, see Appendix A.

A review of Ms Perrin's chapter on the valve problems indicates a lack of attention of top management to training, preparation of personnel and their direct involvement in directing work activities. At a minimum, one would expect that they would at least check to see if the next level of management below them was deeply involved. As mentioned in the NU case study, the top management was more interested in budgets and control of expenditures, than ensuring safe NPP operation. The lack of trained supervisors and line managers, because of early retirement, could have been an underlying cause. In her observations, Ms Perrin also noted that the groups turned inward and the opinion of an experienced person, who had recently joining this unit, was discounted. This further indicated the falling apart of the previously successful NU organization.

It is best to, at least, describe the situation and its possible consequences. As described by Perrin, a valve was allowing steam to leak past the packing around the valve stem. It was decided that the valve packing should be replaced and that it was to be undertaken by the maintenance staff. They started working on the valve, which was in a position that made it difficult work on. What the maintenance crew failed to realize was the valve, by its function, was considered to be part of the reactor's vessel and as such a safety structure. Also the packing was also considered to be part of the reactor vessel by extension. So what was thought to be a simple maintenance operation turned out to be a safety issue, bypass of a safety barrier..

Several other trade groups became involved including persons involved in root cause analysis. During discussions, it was pointed out that not being able to isolate the valve could mean that the maintenance crew could be affected by hot steam and water. Further one of the groups discussing the valve pointed out that this type of valve often did not seat correctly and its stem might also be broken. The maintenance manager thought that that it was possible to just replace part of the packing as they had done that before on non-safety related valves. Eventually, after much discussion it was decided that the operation could not be carried out and the plant would have to shutdown. The ins and outs of the details have been shortened.

The remaining point is that persons were prepared to work on safety equipment that could have lead to a reactor problems as well as exposing persons to radiation and steam when working on the valve. The valve was quite a small one and the release rate might have been small, but none the less it showed the issues with the staff because of lack of experience, training and being supervised by unqualified persons. This reflects badly on the top management and organization. As pointed out in the earlier sections, the role of training cannot be under estimated. In this particular case, training applied to a lack of knowledge about the plant as well as a failure to concentrate on how best to perform maintenance operations. Team skills aspects needed to be worked upon.

5.5.5.1 Conclusions

This case study reinforces the conclusions coming from section 5.5.18 case study. The implication is that the guidance and principles held by the top management strongly influence the performance of the lower line managers, supervisors and operators. The message for regulatory organizations should be to look deeper into the causal factors that affect the performance of staff. Ms Perrin's work shows how a lack of knowledge and organizational discipline can end up impacting safety boundaries. The event here records that a valve with a small leakage could end up leading to both harm to the maintenance crew (burns and effects of radiation), and the possibility of a small break loss of coolant. A loss of coolant into the containment could lead to an extended shutdown of the plant for cleanup purposes, plus the fact that the reactor was at risk. In this particular case, the risk was probably small, but poor operational standards can escalate.

The study provides an insight into what was becoming a significantly poorer run operation. Perrin states that the plant at the time was in the period of an extended shutdown. Most organizations proceed carefully having been shutdown since many systems are being returned to service at about the same time. This calls for much care, a well trained knowledgeable return to power crew and a lot of them. This is exactly, the kind of situation in which NU personnel would be stretched and more likely to overlook or cause problems.

5.5.5.2 VSM related Observations

The previous comments related to VSM were mainly focused on upper level control and competence. The impact of upper level management is see in a different light as illustrated by the activities of the lower level work force. Decisions made by top management can impinge on the safety of a NPP by the lack of experience and understanding of a problem. Here the maintenance crew could have been burned by hot steam, exposed to radiation and

caused an accident to the NPP. VSM model has to recognize the need to define functions and inter-relationships in some detail above and beyond the organizational structure.

5.5.6 Deepwater Horizon/ Macondo blowout Gulf of Mexico Oil Accident

This accident is being examined because it involves some interesting decision-making not only by British Petroleum (BP) personnel, but also the participation of other organizations, including the US Government. BP, Transocean and Halliburton organizations were involved in a drilling operation, which went wrong. The accident makes for an interesting case in decision-making involving different organizations, but the fact that the oil leak was so large, it involved a number of states and the US Government in this decision-making process. This is a prime case of multiple decisions made by companies, states and the US Government that occur together and did not produce a good effect. Also involved, are other countries that offered help in the form of oil skimmers, etc. It is not proposed to examine the offers beyond the fact that they were made. The refusal of this help is quite interesting in its own light, especially in that it was between those countries and the US Government!

The BP caused oil leak into the Gulf of Mexico was one of the single biggest releases of oil in recent time, some 4.9 billion barrels of oil were released along with methane gas. There have been many oil leaks over the years. Significant leaks have come from oil tankers that have been damaged at sea by collisions with other ships or running into rocks. The Exxon Valdez was one such accident. The Valdez accident occurred in Alaska and released tons of oil into the bay damaging animal, birds and fish, while covering beaches with tar and oil deposits. The impact of oil releases at sea are much the same as mentioned. The oil leak from the 'Deepwater Horizon' rig affected a large number of states around the Gulf area from Louisiana to Florida.

5.5.6.1 Accident Description

It is as well to discuss the drilling operation and what was their involvement. BP was the client in that they were the owners of the site, the exploration rights were leased by BP from the US Government. 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 release of oil, terminate it and minimize its effects on the neighboring 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, NRDC report on the

effects of the accident after one year (NRDC, 2011). The accident was both an ecological and economical disaster and will have a long term depressive effect on the whole region.

The oil rig was a ship with a drilling rig mounted on its deck. The rig crew had just celebrated a ten year of no accidents 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 should have been used. Clearly, this is a question of opinion and should be tested. 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 crew members failed to warn the ship's company of the problem and there was an explosion, which killed a number of crew members. This was followed by a large release of oil and the Blowout Preventer (BOP) safety valve system failed to cut-off the oil flow. For this situation the oil does need to be pumped out of the ground, the oil pressure in the pool is very high and just flows out under high pressure. The system under these circumstances the valve needs to close and shutoff the oil flow to the surface and all would be fine.

5.5.6.2 Accident Analysis

It appears that the key event to the large uncontrollable release of oil was due to complete failure of the protection systems to shut off the oil. The safety design appeared to have been designed with both redundant and diverse aspects. From a theoretical point of view, this was the correct approach. Accident analysis has told us that a mixed redundant/diverse combination is the way to go. The idea of using diverse elements is to obviate the impact of "Common Cause' failures. However, the designers seemed to have missed out here in that the effects of the explosion wiped out all controls and probably distorted the pipes. This common event then led to the massive release of oil into the Gulf.

Everyone asks questions about the sequence of the accident in detail, who was responsible and subsequently who should be punished? Clearly, there were a number of factors at play, the design of the shutoff mechanisms, the quality of the concrete, number of spacers, pressure from local management, failure of the person to warn others, etc. BP did publish a report of the accident contributors from a mechanical point of view. However it failed to consider the event from a total point of view, from design to final cleanup. But then that was not the direction given to the mainly research team. The brief description above is sufficient to at least indicate the presence of certain actors. Clearly, BP is the ultimate holder of responsibility for causing the leak. There are other companies that play a significant part in the accident, but BP personnel were in charge.

There were things that BP appeared not to do, one of which was a risk based study of what could go wrong including the consequence of failure of the safety systems to perform as designed. Often, the designers of such systems are the last people to consider what can fail. One wants to move from success space to failure space and designers often cannot make that transition. It appears that the basic failure that led to the accident was the failure of the safety system to function correctly. Even if there were contributory influences that speeded up the event, like poor quality concrete, failure to deal with solid methane effects, BP supervisor pushing the drilling staff, we always come back to the failure of the redundant/diverse safety system failure as the main failure. In this BP and the designer must take responsibility. BP for failure to review the design from a probabilistic risk point of view, including the risk to the company of its failure, and for the designer for not reviewing system problems leading to failure to work including loss of signals, actuator failures, etc.

However, once the release was underway what should be done and who should be held responsible? So now we move into the release stage of the accident. People at BP, etc. will focus on the technical issues of the mechanisms associated with the stages before the explosions and the immediate actions taken by BP and others. In some ways more interesting from a management point of view is to diagnose the actions that BP, Coast Guard, local authorities and the US Government to respond to the release and the issues that come up. The first thing is to ask is; what are the responsibilities of the various parties.

From a legal point of view, it would seem that BP should be held responsible, since they started the process. However, the licensing authority has some involvement; by their actions found that BP was a capable company to do the drilling, so by implication they should be held equally responsible unless BP was deceiving them in some way?

The US government is a key player here and has a responsibility to protect and defend the public. So surely they needed to have responded quickly, possibly through the Coast

Guard, to assemble skimmers, and other oil collecting ships to remove the oil as quickly as possible even using the US government's good offices to enlist help from other countries. They should set aside and trade constrains, which prevented offered help arriving. Like setting aside the Jones act. So what is the difference between this situation and responding to various hurricanes and storms?

The US Government continued to pursue BP to get them to assemble a large group of ships to minimize the effects of the oil spill. It appears that the US Government did not understand the limits of BPs capabilities relative to the requirements. Only the US Government had the prestige and resources to respond to the accident in a timely sense and minimize the ecological and finance effects of the spill. Although BP is a large and wealthy company, its wealth is tied up in its oil wells, refineries and personnel. Given time, they could have negotiated to sell resources, but the value of the resources would be worth less than their face value. Time was of the essence and the US government waited too long to act and oil leaked ashore doing damage to sensitive areas.

5.5.6.3 Organizational Analysis

Figure 5.14 depicts a VSM diagram with the BP company officials, the Obama Administration, the Licensing and leasing department of the US Government and the US Coast Guard. The companion companies involved in the oil exploration are subsumed within the BP Organization. The oil licensing and leasing authority was called Mineral Management Service (MMS) and one result of the accident was to redefine the role of MMS. It is now called the Bureau of Ocean Energy Management, Review and Enforcement (BOERF) and they cover more than leasing. The function of the Coast Guard is law enforcement on the seas and search and rescue. In the case of the post accident situation, the Coast Guard was given the task of co-ordination of the response to the spill.
The object behind using the VSM approach in this case is to diagnose the accident situation in terms of recovery actions. The figure also shows the limitations of both lower and upper levels of the BP and associated organizations in not taking the correct actions to minimize the possibility of an oil leak or gusher in this case. Within BP there does not appear to be the necessary resources to deal with such a major release.

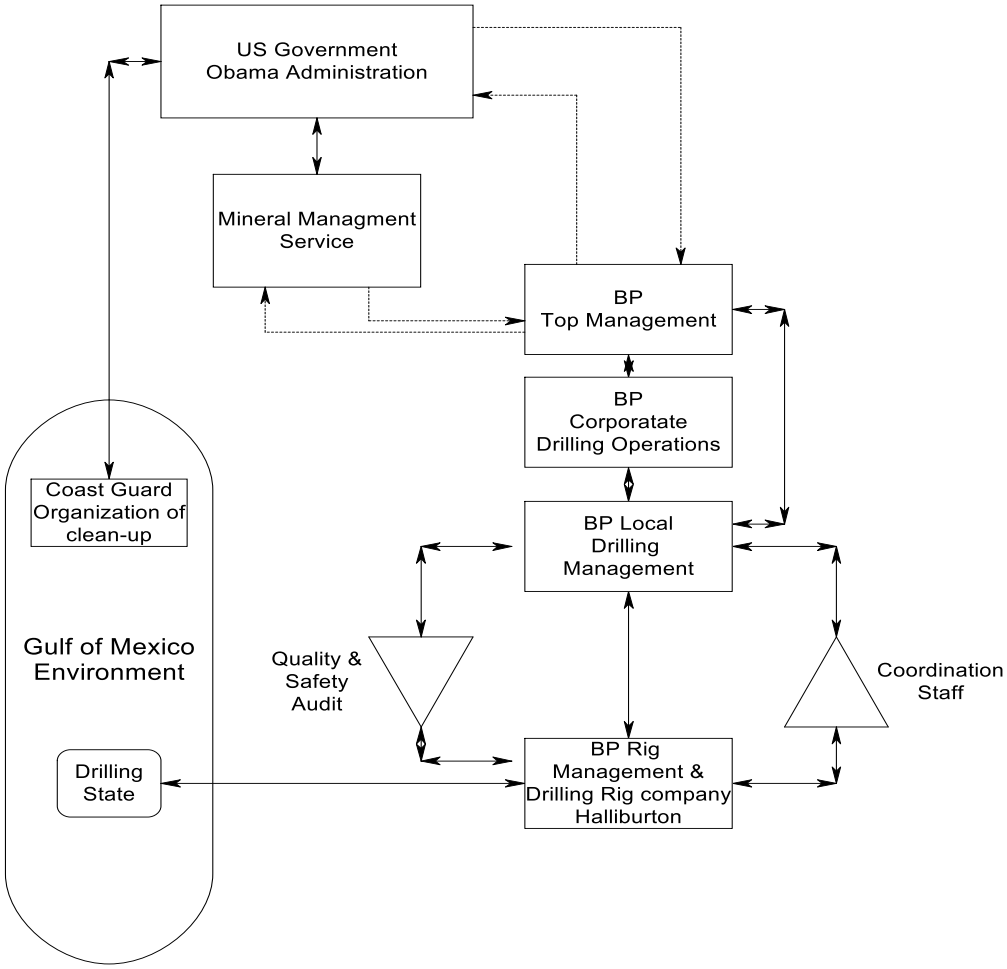

Figure 5.14 Organizations associated with the BP Oil Leak in the Gulf

With respect to the large volume of oil released, the failure of the US Government to act quickly to hasten oil recovery ships, pontoons and portable oil barriers led to the large oil release. Although BP is a large organization their ability to react to the situation in a very large way is limited by their actual influence with other countries and organizations. The US government is in a much better position to do this. As far as resources are concerned, BP is a wealthy company, which does not mean that they can instantly have large amounts of cash on hand to pay for all of the rescue vehicles and personnel needed. Probably BP's money is tied up in facilities.

5.5.6.4 Conclusions

Figure 5.14 shows a number of different managers and organizations, associated with BP Oil Company as a whole, which covers exploration, refining oil, and distribution. This is the center of the company and the controlling body. Then there is the part of the company associated with exploration of oil properties throughout the world and then there is the

organization, which covers the drilling operation, and later it turns its job over to exploitation group that collects the oil and passes it to the oil refineries.

The VSM model covers these operations to the best degree possible. Included in the local drilling operation are the usual groups trying to ensure that the drilling operations are monitored, audited and coordinated. Within these operations are persons responsible for the safety of operations. These are communications and actions within the BP orbit as far as the drill operation is concerned. It is within these local operations that things failed. Advice from drilling personnel was supposedly over-ridden by the local BP project manager. Also the person monitoring safety indications did not it appear to observe warning lights relative to presence of methane gas and alert the staff on the boat. Some 11 persons died because of the methane explosion and fire.

Further it is believed that the fail-safe aspect of the blow out preventer (BOP) failed due to loss of signals to isolate the drilling tube and prevent release of oil. The precise mode of failure of the BOP has not been released as far as the author is concerned. Clearly, the BOP failed and there were other contributory failures including some human and equipment related ones. In the design of things, the BOP failure is something that was not expected and if it had not failed, it is likely the topic would not be addressed here. However, there were other contributions to the accident from other sources for example how was the frozen methane released and why did it cause an explosion. Why did the observer not give an alarm? The key issues appear to be the uncontrolled release of methane, the explosion caused by the release and the apparent failure of the BOP device following the explosion. This left the oil to gush out of well with no significant way to stop it in a short time. The actions of the BP manager to continue to drill may or may not have been significant, however one is left with idea that some caution should lead one to hold off for a while until the situation is understood better. The ability of the frozen methane to pass through the drilling pipes maybe due to poor cement, etc. is questioned? For example, does the missing spacers and poor cementation hava any real effect upon the accident and its sequence and consequence?

Other organizations depicted on the VSM diagram also played a part in the accident. The MMS organization enters into the process by leasing the site of the Macondo well. In retrospect, the Obama Government questioned what safety precautions were demanded by MMS and what regulations were required to be followed by BP (and other drilling operations) in the drilling at these depths. One would have thought that it was in the interest of BP to have a clean operation, since the loss of 4.9 million barrels of oil at say $20.00 to $50.00/barrel represents $196 million to $490 million depending on the price of oil at the well

head. The loss of the well, the boat and people have to be added to the losses, are not insignificant. One has to add to that the cost of cleanup.

A review of the accident indicated that the Obama Administration or government agencies such as the Coast Guard operating under Administration directives did not act quickly enough to avoid the spread of the oil to the coasts of States from Louisiana to Florida. It does not seem right not to hold the US Government responsible for its failed to act quickly to minimize the effects of the oil on the populations of the States, the flora and fauna and the local business (fishing to tourism).

The conclusions from the accident are:

1. BP underestimated the issues with the local management relative to taking actions not in the real interest of BP as a whole. Decisions were made to save relatively small amounts of money, while risking much more. Lack of perspective on behalf local management
2. BP main management failed to have a risk study to identify the consequences of a failure of the BOP valve isolation system. Superficial understanding of common cause issues led to a locally reliable system that failed to perform, when exposed to the accident environment
3. Local BP management did not have an effective quality control program
4. Local rig members seemed to be not as well trained in safety aspects as they should have been
5. BP analysis of the possibility of stopping the leak along with others was too optimistic leading to a failure by BP management to state the correct time needed to stop the massive leakage
6. US Government was fixated on BP's responsibility in the case of the leak and failed to see what their proper role was. They acted much too late and even then did not fully commit both US and other resources. In fact they seemed to act against the interests of the citizens living the Gulf regions

5.5.6.5 VSM Comments

The VSM model generated here seems to cover the main aspects of the various organizations involved. The main items not covered are the viability of the BOP system to stop the oil from gushing from the well. The connections between the various parts of the BP organization seem to be represented and some of the functions were carried, but one must ask the success of these communications, since the head of the BP seemed not to be

too concerned with his responsibilities in this case. In the VSM diagram, a management block directly associated with safety of operations has not been drawn. It is noted that the person who led the scientific investigation of the accident has been appointed to manage safety of operations. One feels that BP should have investigated the consequences of BOP failure and what mechanisms could lead to BOP failure to achieve its mission. This review function could have been incorporated into an audit function, similar to the CNO of a NPP organization.

The VSM model does include the US Government, the Coast Guard and the MMS in its depiction. Clearly, the US Government stepped in to assume a leading role, but in a regulatory mode, not as a proactive organization to ameliorate the effects of the accident on the populous. It is interesting to compare the actions of the Japanese Prime Minister's role in the Fukushima accident with that of the US president in this case. Here the US President seemed to be more interested in punishing BP, not coming to the aid of the persons in the surrounding states.

The US Government could have taken to minimize the oil releases from reaching the land and contaminating the shores of several states. However, the Obama Administration attenuated the variety by not authorizing the Coast Guard to take necessary actions to check the oil distribution using all availability resources including specially designed foreign boats volunteered by their Governments.

5.5.6.6 Post script on the Macondo Well Accident

A review was made of the BP report on their analysis of the accident (BP, 2010). The report was very extensive and very technical, but somehow a little off course in that while it goes into great detail on the accident, but did not deal with the key elements of decision-making under high pressure conditions and how to avoid human errors leading to a massive oil release. Interestingly, BP awarded the leader of the analysis team with the post of head of safety! It was a very detailed report and several organizations and experts were involved.

5.6 Conclusions from the Study of Accidents

The objective of this series of case histories is to examine six accidents from the point of view what can learned about applying VSM or cybernetic thinking to organizations under the stress of an accident. The process used was to analyze each accident to understand what part was played by the organization, top managers, middle managers, supervisors and operators. Accidents involving the Nuclear were the center of the study, then it was realized

that much of the thinking about safety and its importance could be applied to other industries. In many industries, there has to a balance between economics and safety. Nuclear is not the only industry where a balance has to be maintained between these two aspects.

Each of the studies drew conclusions about the application of VSM and also findings about the accidents themselves. There are some common lessons learned from the studies with respect to the roles of management and operators in causing accidents and recovering from accidents. There are conclusions to be drawn relative the use of VSM to analyze organizations. If one concentrates on the structure of VSM, one can see what elements have to be present so that certain issues are addressed. The VSM structure identifies various elements such as top managers and others within the organization. It mirrors control systems, since they are both cybernetic processes, so the right kind of communications are important and also the functions performed at the various levels are equivalent to the controls algorithms. In the case of a control system, the designer of the control system selects the controller algorithm and tests it to see if it performs as required. The bandwidth of the communications is also chosen and the strength of the action element is matched to the needs of the complete design.

In any organization, the objectives of the organization are defined and structure of the organization is designed to fit in with a command structure along with an action group. Equipment is selected to accomplish the function of the organization, so for a power plant, the equipment consists of a power generator taking fuel and converting into electric energy, which is sold. To run this system you need staff to operate the units, maintain the equipment and a group of managers to organize the operators and maintainers. Also, there are a bunch of support personnel to attend to all of the ancillary functions, such as billing agents, guards, etc. So one needs trained people at all levels.

The exercise of examining the six accidents has been good in shedding light on the use and value of VSM. The value of VSM approach helps one see what is important, since it turns an essentially static process into a dynamic process. Time is very important in dealing with accidents, actions have to be taken at the appropriate time, as one see in the case of the Fukushima accident, the crews were laboring against time and in failing to take action at the correct time led to things being undone. Another theme coming from the examination is planning for events outside of the design bases for the plant. Another lesson, which maybe the most important one is top managers taking decisions based purely on their gut feelings or limited knowledge. In many cases, if communications with lower echelons in the organization were respected then the probability of harm could be limited.

In the next chapter, the application of VSM to the nuclear and other industries will be examined in some detail and will draw upon the above studies. VSM may not be the perfect tool by which to examine management organizations, but it has some good features that enable it to brush away some of the obscuring features of organizational charts and identify what parts of management need to work together for the health of the organization as a whole. It is tool to point towards what is critical versus what is just required.

Although VSM points to the role of the top managers, it does not identify the characteristics of a good manager. The study of the accidents points to role of the top managers of organizations in terms of their ability to set up accidents and even prevent possible recoveries or mitigate the effects of an accident.

An important issue with management decision-making is it appears to be a case of limiting the variety of the processes without consideration behind their decision. So the requisite variety to ensure success is not addressed. Key states are excluded from their thinking; hence their likelihood of success is doomed from the beginning. More research on this topic needs to be undertaken.

It seems unlikely that systematic approach to structuring an organization can ever ensure the choice of a manager who will prevent all accidents occurring. However, it should be possible to enhance the VSM process in the area of decision-making to the point that the probability of an accidents reduced by better decision-making. It appears that VSM is correctly structured dynamically with appropriate communication lines, control bodies and distributed decision-making entities, however there needs to be better upper management training, availability of decision-making tools, and for them to be open to good balanced advice. The company directors need to be independent of the managers and knowledgeable in their own right so as to provide a balanced force in running the organization.

CHAPTER 6 Experience in applying VSM to the Nuclear Industry

6.0 Introduction

The previous chapters dealt with nuclear power, VSM technology, accidents, etc. This chapter covers the lessons stemming from diagnosing how organizations, which have been affected by accidents, react and make improvements. Also, ideas have been generated resulting from the structured evaluation of the accidents seen by referring to the VSM approach. These observations cover not only issues associated with the nuclear industry and its organizational structure but also related to understanding of the VSM approach and how it has to be re-interpreted or modified to reflect these lessons. From the observations of accidents, the role of management is seen as important in decision-making but limited in its capability to respond quickly, i.e. in the time scale of accident progression, equally the knowledge base of the operators needs to be expanded by the use. This implies limitations in the Beer view of organizations as far as organizations which might be exposed to significant accidents.

6.1 Evolution of Organizations

Beer selected the human body as a model for an organization and this led to the generation of the Viable Systems Model (VSM), which is covered in Chapter 4 in detail. The human body is the result of many years of evolution and the functional development of the brain, nervous systems, and components, like the liver have taken some time to perfect.

Using the characteristics of the human body, particularly the brain and nervous systems, as the model of an organization is very good. It is a useful starting point and it could have formed the basis for a utility organization in the early days of nuclear power. It would have made it much clearer that there is a top decision body, middle level personnel to guide and control the operation and a group of personnel empowered to run the operation. It would have emphasized the need for communications to ensure instructions and information flowed freely and was seen as important to the effective running of the organization.

However, the utility industry chose to use the current organizational structure based upon fossil fuel plants. For these plants, the organization structure was much simpler, safety and economic risk associated with the non-performance of both management and staff is much less. Fossil plants may experience some loss of life and limited economic loss resulting from accidents. The early utility managers appeared to think that NPPs were like fossil plants but with a different heat source. Also, that the AEC (precursor to the NRC) would take care of safety issues by their overview of the NPP designs.

The short comings of the industry in dealing with nuclear power became clear as accidents occurred, which exposed the lack of understanding of how the power plants should be operated, the roles of both managers and staff, the dynamics of the whole process and the risks involved. These risks were both public risks and economic risks for the utilities.

It is not clear that using a different model of the whole organization would help, since there was a technology and risk appreciation gap in the whole industry. Bit by bit these gaps are being closed. The evolution of the industry has being driven by a series of major accidents.

Some of the lessons learned from nuclear accidents, can be applied to other HMOs. Clearly most HMOs do not involve radiation effects, but they can involve risks for the public as well as financial risks for the companies involved. Issues associated with decision-making at the highest levels within companies and organizations can influence risk exposure, see Challenger, various oil rigs (such as Macondo) and Texas City accidents.

The VSM structure seems to work well in the case of normal business organizations and fits the same kind of things that covers body functions of assessing situations and taking actions, i.e. brain functions and autonomic actions. The assessment of risk is present in the case of humans and is associated with the cortex, so this feature is implicit in both the human and VSM models. However, in many organizations, safety risk is not as important as it is in the case of HMOs. In HMOs, the risk evaluation should be formalized and be systematically applied. For risk assessment processes to be applied correctly, data used in the process, needs to be validated. Risk assessments based on invalid data is worse than useless and can cause managers into making poor judgments about safety or economic issues. Many of the accidents recorded in Chapter 5 were the result of poor judgment of risk on the part of the top managers, see for example the role of TEPCO's top managers vis a vis the need to build sea walls big enough to protect the plants from the effects of large tsunamis.

Careful consideration of VSM could have helped the industry evolve a better organizational structure by the emphasis it places upon the identification of the roles of the various elements, such as S5, S4 and S3, see Figure 4.11. This should have lead to an understanding that the risks of operating a utility rests primarily with the top decision-makers, i.e. the CEO, CFO and the Board of Governors, not the Nuclear Regulators. The S4 and S3 roles should have covered the roles of advisors to be aware of nuclear accident risk and correct functioning of the lower levels within the utility. Their involvement would cover the environmental effects and issues associated with maintenance and plant operations. The equivalence of roles is covered in Figure 5.3, where the decisions taken at the top level (S5, S4 and S3) determine the controlling influences on the operators (S1 & S2) performance.

It should be noted that the decisions made by the upper ranks of the organization affect the whole organization, whereas the decisions taken by the operators are limited to their specific actions. Figure 5.2 depicts errors made by the operators, namely random and systematic. The random errors are limited to individual operators making errors stemming from their psychological issues, such concerns about their homes, etc. and therefore limited to individual operators and do not affect others, and slips. However, systematic effects can affect all operators and there is a high probability of leading to errors in a given accident situation. So the probability of an accident is much smaller for random errors than for systematic accidents. Equation 6.1 below relates the probability of an accident to the probability of an initiating event occurring at the same time an operator makes an error, which makes the situation worse. If the operator who is likely to make an accident worse is not on duty, then the probability of the accident is significantly reduced.

$$p\,(\text{damage event}) = p(IE)*p(HE)*p(EF) \quad \text{.....equation 6.1}$$

where:

p = probability

IE = Initiating event, which could lead to damage if not addressed correctly

HE=Human Error made by a crew member responding to the IE

EF=Equipment Failure before or during the transient following the initiating event, which makes the transient worse

6.2 Importance of Time in Accident Termination and Mitigation

As indicated in equation 6.1 the combination of events can lead to accidents, which can have undesirable results for NPPs or HROs. Examination of the factors that affect the accident probability there is one common factor: management decision-making. Management decisions affects the selection and design of the NPP, staff training and can influence how outside influences, like the weather, are considered in the choice of plant location and weather defenses, like water barriers.

This does not mean that management is totally responsible, since there is always a question of predictability associated with initiating events, human errors and equipment failures, but correct decisions by management should reduce the probability of an accident.

Although management decision-making is the key, there are limitations to what managers can control and take actions to terminate accidents. It is useful to understand one of the limitations is the ability of management to assess and take actions terminate an accident, particularly one that is evolving quickly, seconds to hours. The basis for this judgment is the work of Rasmussen (1983) and this will be explained below. The NRC has made the same

judgment by limiting accident response to control room operators. Clearly, in the case of very rapidly changing accidents, managers are physically unlike to be nearby to take action anyway. For a slowly evolving accident they could be called, but then it could take them some time to absorb how the accident is evolving and then determine the best course of action to terminate it. This process is likely to take a large amount of time, during which the accident could proceed to an irreversible state with the reactor core damaged.

Management should be in thinking ahead of what steps need to be taken before an accident occurs and preparing the operations department to be in a good position to respond, quickly and efficiently, to an accident. The role of the human body operates in a similar manner in that the mind considers the situation and the rest of the body takes the actions. This is the apparent position of Beer and the basis of Viable Systems Model. Of course, there are a lot of internal connections and controls, which make both the body and the organization function. There are communications lines, control lines or instructions, and there are monitoring functions for both systems. All have their uses in keeping the systems operating, like the blood function in the case of the body and the maintenance function in the case of a utility.

Rasmussen (1983) presented a paper on human behavior, in which he discussed the different characteristics of cognitive functions versus manual operations; this is the VSM equivalence of S5 and S1, or management and operators. In particular, one is interested in the time responses of these functions. The cognitive function is based upon knowledge and is slower in formulating ideas and then taking actions. Manual operations are much quicker in assessing the state and taking a course of actions. The manual operations base their actions on the matching of a known situation to the actual situation and then using a predetermined course of action (or procedure) upon which to act.

Rasmussen called these two modes of behavior: Knowledge-based and rule-based behavior. He also identified another response called skill-based behavior. The latter comes about when operations are repeated over time and there is not too much change or deviation in the series of actions.

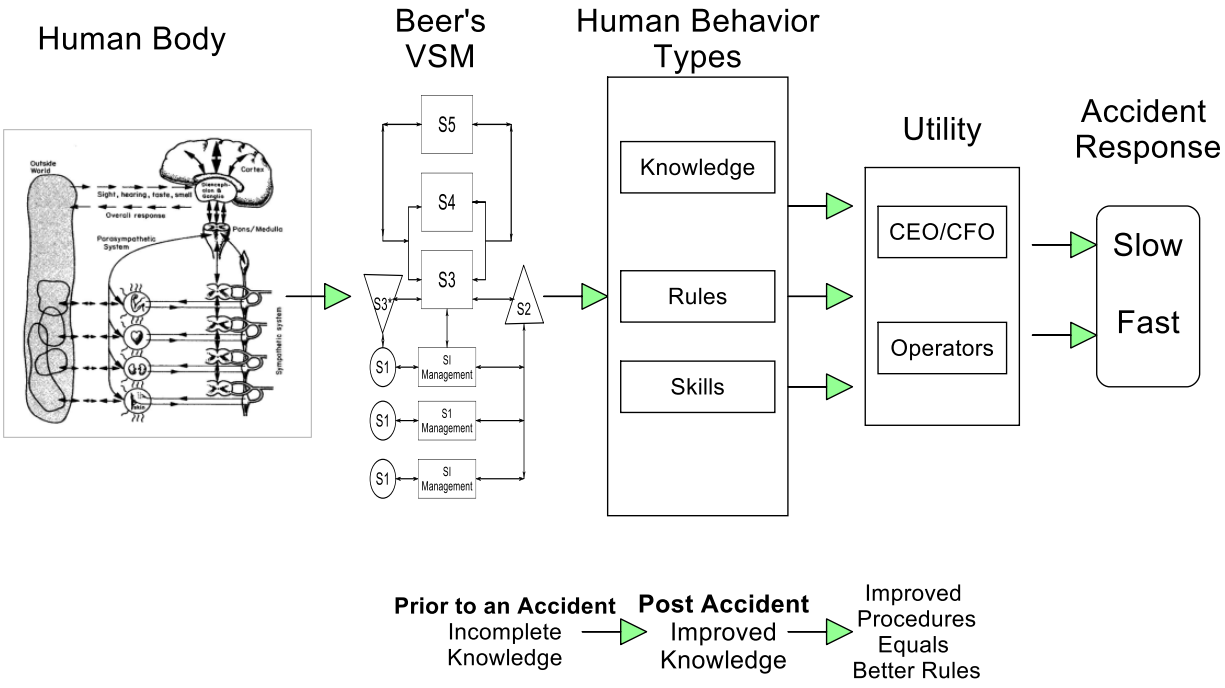

Figure 6.1 Insights gained from Beer to Accidents Responses via Rasmussen's SRK Human Behavior

Figure 6.1 depicts the conceptualization of idea connecting the cybernetic model of the human body, Beer's VSM, Rasmussen's behavior types to utility responses to accidents. It points out why organizations dealing with safety issues have limitations in dealing with accidents. Managers are not equipped to act quickly when faced with an accident and operators are only really effective when they are fully prepared to meet the accident by being educated in the use of the correct procedures for the accident.

Both knowledge- and rule-based behaviors have their shortcomings. In dealing with an accident, the management may be too slow in dealing with a rapidly changing system and not reacting in time to mitigate or control the accident. This is why the onus of responding is transferred to the front line operators, who are capable of responding quickly.

The question then arises how to use the capabilities of both groups to take advantage of their behaviors. Clearly, the management group needs knowledge of the possible accident to even think about taking action. Equally, the operations group needs to understand the rules, before they could use them to terminate, or mitigate the accident. The responsibility of the management is to understand the accident and how it occurs and to use this information ahead of time to generate the appropriate rules for the operators to follow. To ensure that the rules are understood and followed, the management must train the operators and

subject them to tests to ensure that the rules are clear to the operators and that by following them will lead to success and the NPPs will not be damaged by the accident.

One can illustrate the short comings of organizations in dealing with organizations by examining two accidents, namely Three Mile Island (TMI) and the Tepco Daiichi accidents. Also, one can see how issues associated with human behavior can affect the situation.

In the case of the TMI accident, there was a lack of understanding of the importance of decay heat in the post accident situation and therefore the knowledge base of the industry was lacking, this in turn led to the operators being under trained and left without suitable procedures to follow. So the operators could act quickly, but did not have the correct set of rules or training. The industry learned from the accident and changed the procedures to symptom-based procedures and further more emphasized training and introduced simulator training so that the operators were better prepared.

The Tepco Daiichi accident was different in that the accident was caused by a large earthquake followed by a series of immense tsunamis. The interesting thing about this accident was that the management was unprepared on two counts, they decided not to build a breakwater of sufficient to prevent the tsunamis affecting the NPPs and secondly did not prepare the operators to deal with the tsunamis with suitable procedures, and tools. On top of that the operators were not practiced in dealing with the post accident situation. Section 5.5.7 of the thesis covers details of the Daiichi accident and the response of management and operations to that accident.

The course of the accident could have been better if the Tepco management had a better idea of how to deal with accidents. The site operations personnel realized that there was a clear need to cover the reactor cores with water to prevent core melt, also they realized that hydrogen was being formed from the action of steam on zirconium fuel cladding and to prevent an explosion the hydrogen needed to be released into the atmosphere. Actions on both of these awaited the decisions of management. In both cases, the decision to act was too late. This represents the delay time effect associated with management.

Operations did what they normally do, in that they were trying to respond to the accident and terminate it, but lacking correct procedures and training they failed. The local supervisor tried to do what the Tepco management failed to do ahead of time i.e. redesign the procedures and actions as fast as they could. They were trying to achieve the essence of what the actual organization should have been, i.e. the operators needed the procedures and knowledge to respond correctly.

The action by the plant supervisor in response to the accident underlines what has been said about preparing ahead of time so that one has procedures coupled with training to deal with the situation. The supervisor was operating in knowledge-based behavior trying to think through what has to be done and this leads to slow responses. However, the site personnel quickly realized that water needed to be injected into the reactor vessel to cover the core to prevent core damage. Unfortunately, authorization to use sea water was slow in coming, since the Tepco management was concerned that the use of sea water would mean that the reactor would be badly affected by the salt water. The loss of the plant had already gone past the point of saving and not cooling the core would in fact increase the costs associated with the accident, because clean up costs would be higher and the release of radioactive materials would increase as long as the core was not cooled adequately.

The correct functioning of the operators is dependent on management providing procedures, experience and training for the operators. So management's role is either use their understanding of NPP accidents to generate acceptable procedures or to learn about accidents in general and gain an understanding of accident progression and what is needed to deal with specific accidents. In essence, the regulator (NRC) can fulfill this role, but the management needs to be better prepared in accident analysis and not just be a better accountant!

If a NPP organization is not challenged by an accident, it can successfully operate in a quiescent state, as it appears many NPPs are doing just that! However, an examination of the NRC's ROP data base indicates that all is not totally acceptable, since some 20% of US plants have some minor operating issues. A close examination of this data indicates issues associated with plant management not paying close enough attention to potential accident initiators, see section 6.10.

6.3 Development in Nuclear Utility Organizations arising from Accidents

One of the key elements of this study is in the observation of how utilities have developed and changed as a result of accidents that have occurred in US and in other countries. Chapter 5 covers a number of accidents, but there are many others that have not been covered. Of the accidents, some have led to major changes in how the NPP industry is run and others have led to less noticeable changes, but are also important.

A criticism of the industry might be that it has not been a sensitive to other forces of change in safety awareness and only seems to have reacted to accidents as the method of change, see Pool, 1997. Clearly, if an accident has taken place, its probability of occurrence has

gone from near zero to one, so it becomes hard to avoid, hence it has to be fixed. This is the historical way in which things have changed.

Thinking what might happen is fairly easy, but deciding it is worthwhile to fix is another matter. In the early stages of nuclear power plant development, there was a lot of thinking about what accidents might occur that could lead to significant releases of radioactivity. This thinking led in the early days of nuclear to a set of postulated accidents. These postulated accidents were used as tests in the design of the NPPs, since few accidents had occurred. However, people could see that if something went wrong the consequences of an accident could be devastating. The actuality of the atomic bomb was in people's minds and continues to be so.

Over time the thinking about the approach to safety has changed in a number of ways, from the deterministic to probabilistic, importance of decay heat relative to reactor reactivity effects, internal events versus external events. The NRC approach of the risk informed approach has a lot of advantages in that it keeps NRC's options open. This is particularly important in cases when the probability of an event is very low. The question being do you ignore accidents of supposedly very low probability? Here the concentration is on the influence of accidents on the structure and rules of nuclear industry. The process of improvements is illustrated by figure 6.2. Each accident or incident that occurs is analyzed and insights are developed.

This process is going on as can be seen in the actions of the NRC, IAEA, and other National and International bodies. The bigger accidents get the bigger attention, so TMI unit #2, Chernobyl and now Daiichi receive great attention. However, even small errors by operators and maintenance personnel receive attention. The NRC has a grading system for deciding what actions are needed; some are more serious than others. The NRC has a color grading scheme, but starts with no action, through warnings, fines and shut down of the plant, see chapter 3. Lessons from the NRCs Reactor Oversight Process (ROP) are discussed in section 6.10 below.

It is interesting to note that the industry had decided via probabilistic methods, that some of the early accident initiators could be of reduced interest, such as the rod ejection accident. The basis of this choice was the fact that no accidents of this type had occurred. Fairly recently, at the David Besse NPP (NRC, 2008), it was discovered that cracks were present in the stub welds in the reactor vessel used for the purpose of control drive mechanisms and that the reactor vessel was eaten away by the action of boric acid, since the protective layer of stainless steel was bypassed by cracks, luckily no accident occurred. If an accident had happened, It would have been one that was the combination of a rod ejection

accompanied with a loss of coolant. This reminds one that something assessed as a very low probability event can still occur and the need for monitoring effectively is required to maintain NPP safety.

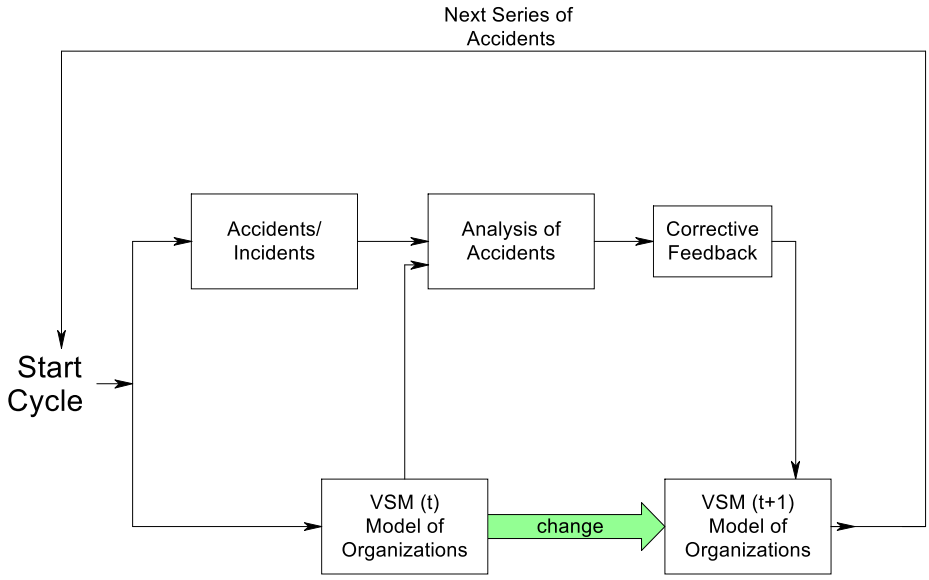

Figure 6.2 Impact of Accidents of changes in VSM Model

The concept of transitions that occur from one VSM representation to another in the nuclear business is brought about by the impact of accidents and incidents. Organizations react to the accidents and this led to modifications in the organizational structures of Utilities and even NRC and INPO. The impact of an accident can lead to the introduction of other functions in the structure and changes in the importance of elements within the VSM structure. For example one consequence of the TMI accident was to raise the importance of operator training as a way of reducing the probability of an accident. This important aspect has been factored into the structure of VSM, this is one difference compared with the original VSM formulation.

6.4 Limitations of Beer's VSM for Safety-based Organizations

The VSM structure has been suggested as a reasonable vehicle for modeling organizations in that it is based on cybernetic principles of control and communications. Beer based his VSM structure on the human body, see discussion in Chapter 4. His cybernetic approach works quite well and has been applied to a number of commercial operations. However, it appears that VSM has limitations in dealing with safety–based organizations due to the importance of responding in time to terminate or mitigate accidents.

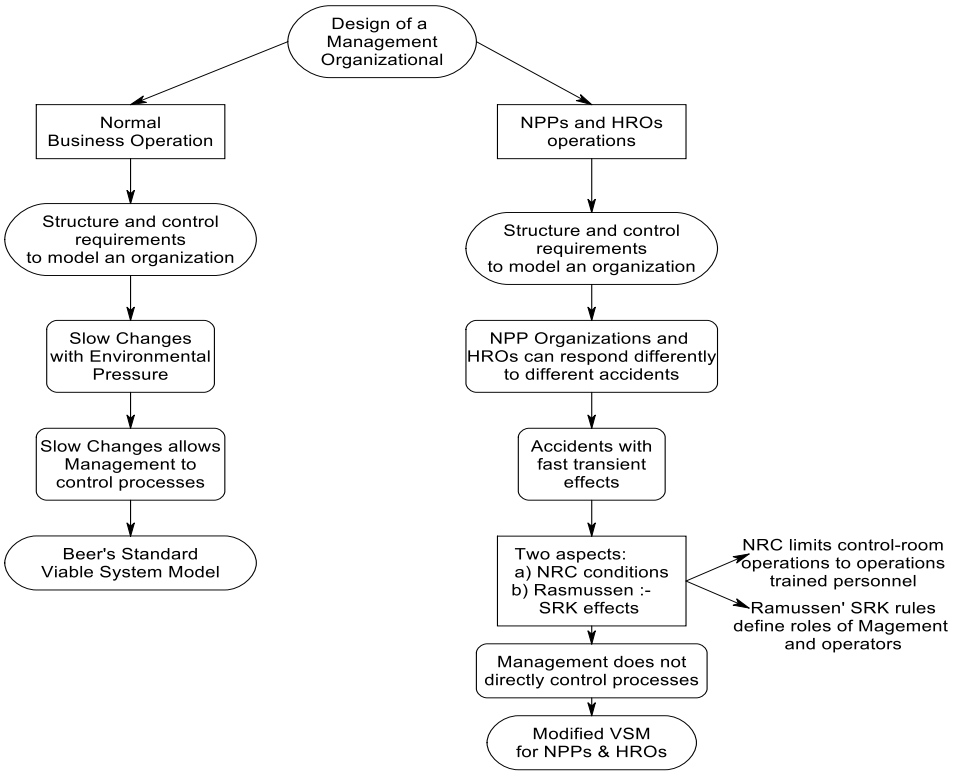

Figure 6.3 Design of Viable System Models for Commercial and NPP/HRO Organizations

Figure 6.3 lays out the difference in the selection of either the original or modified VSMs for a normal commercial business or a safety related business. The key difference between the ordinary business and an HRO is the need to clearly understand the need to quickly and accurately respond to accident situations. In both cases planning is a feature of both VSM variants, however commercial VSMs do not need to train their operators to respond quickly to situations, whereas in the case of HROs managers are not positioned to control the processes directly and have to rely on appropriately trained operators to act on their behalf.

In order for the HROs to operate safely, the management must ensure that the preparation of the operators matches the characteristics of the set of accidents so that the accidents do not cause either a problem for the public or cause economic damage to the HRO. To achieve these objectives, HRO management needs to prepare itself and the operators to deal with accidents.

The operational state for NPPs is that the NRC has set rules on who operates the plants and they are the licensed operators and not the managers. The interpretation of the Rasmussen

rules would confirm this choice, in that managers operate from a knowledge-based and the operators from a rule-based behavior point of view.

In a normal commercial business, time lapses are not too important and the characteristics of management decision-making fits into the time scale of the operation. Things evolve in manufacturing relatively slowly from months to years. Production lines are set-up and then they run for long periods of time. One can see this in the car industry. Before the new models come out, there is intense activity in market research, design, and testing. The manufacturing process continues year by year without the construction of a completely new design. It is an incremental process of improvement and the management can deliberate on the decisions and essentially take their time. So the decision-making time scale of management fits into this process.

However, for the management to be involved in the day to day operations of NPPs does the viable system model (VSM) really fit the needs or requirements of the utility? This is even more so in the case of accidents, Rasmussen (1983) pointed out the characteristics of human behavior in his SRK classification; the following comments are my interpretations. It appears that Skilled-based behavior is fast and this is achieved by the person being well trained in undertaking repetitive tasks. As we say the person is skilled at certain tasks, i.e. he does them quickly and accurately! The next case is Rule-based behavior, here the person follows the rules closely and his performance is accurate and reasonably fast, but it does depend on the quality of the rules and the individual's training with executing those rules. The last case is Knowledge-based behavior, here the response to situations tends to be slow, since the person has to think through his knowledge base and construct an argument about what to do and if possible test the ideas. This makes the process slow, not too reliable, and depends heavily on the quality of the knowledge and its recency.

6.5 Accident Analysis depicting Transient Responses

Transients can occur both during normal and abnormal conditions, including accidents. It is the responsibility of the operators to monitor the automatic responses taken by control or protection systems and act to correct the responses. To do this successfully the operators need to well trained and follow instructions laid out in the Normal/Abnormal and Emergency procedures. The role of the managers is limited to ensuring that the operators have correct procedures and are well training in those procedures to be able to respond quickly to terminate or mitigate consequences of the accident.

An example of a rapid transient that has been seen at operating plants is an Anticipated Transient without Scram (ATWS). There are a number of transients that fall under the

category of an ATWS, such as turbine trip, feed pump trip or the failure of some other piece of equipment. The example used here is the main turbine trip due an electric fault on the distribution line. This transient was observed a couple of times at a PWR NPP at the Public Service Electric and Gas utility in New Jersey. The design of the reactor protection system is such that if a turbine trips, then the reactor should be tripped along with the main feedwater system (main feed pumps trip). This means that the energy from the reactor ought to drop quickly to the decay heat level and this heat can be removed by the auxiliary feedwater system, which is initiated on the loss of main feed or low water level in the steam generator.

However, in the above cases, the reactor trip breakers failed to open, the control rods did not drop into the core, the reactor was not shut down and continued to generate power at the same rate as before. The operators seeing that the turbine tripped looked to see if the reactor had tripped (annunciators alarmed) and that the rod position indicators (all on the main control board) showed that the rods dropped to the bottom of the core (time to drop 1.6 seconds). The operators confirmed that the rods did not drop and hence they had to trip the reactor in some way and ensure that the reactor was shut down. The operators had a few minutes to act before the core would be uncovered and the core damaged.

Figure 6.4 shows the event sequence diagram (ESD) for this incident. One can see that failure to open the reactor trip breakers can lead to core damage.

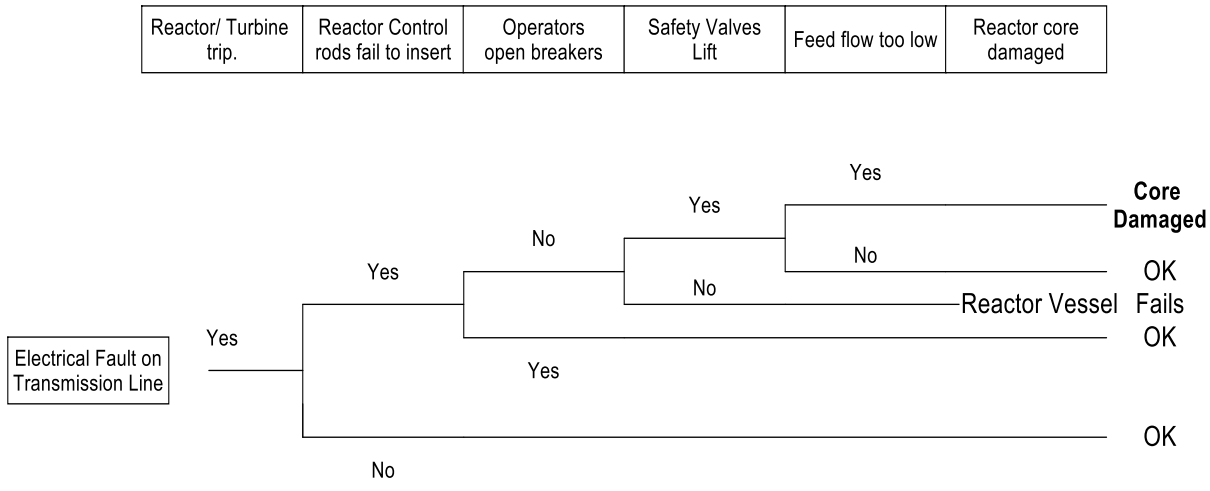

Figure 6.4 Event Sequence Diagram (ESD) for an ATWS incident

To describe what the operators could do in this circumstance, one needs to describe the reactor trip breaker logic and the associated electric circuitry, see Figure 6.5. The electric

one-line diagram is a simplification of the actual circuits. The Reactor trip breakers are powered by the same power supply as a number of essential pumps. The trip breakers are two, either one can interrupt power to hold or drive the control rods. There are two channels of reactor trip logic, based on a number detection circuits. The circuit we are interested here is one derived from the turbine trip logic. However, in this case, the breakers did not open because they were not maintained correctly and they both stuck in the closed position. Practiced actions by the operators (mean time 10 seconds) can open the manual trip breaker on the 480 volt supply line. Figure 4.2 shows results of operators responding to this accident on a simulator. The operators' actions are: seeing that the rods do not drop, they tried to manually trip the reactor breakers, via logic circuit, and then they trip the power supply including power to various pumps, once the rods drop the operator re-instates the power to the pumps. If the rods do not drop, then the operators will use high pressure pumps to inject high concentrated boric acid into the core to shut it down, this is much slower than the action of the rods in shutting the reactor down.

This is a very rapid accident requiring an equally rapid response from the operators. Without training and a well thought out procedure, the operators would not have succeeded. The point to be made is that for the actions of both management and operators to succeed to control accidents, one needs pay attention to the skills and limitations of both parties. Resolution of the response to this accident came about by an incident that did occurred, fits the learning process of engineering, see figure 6.2.

As identified by considering Rasmussen's human behavior models (1983), we have to rely on management to organize the processes, an intellectual pursuit, which can take a time to devise and confirm. The operators have to be trained and tested in correctly applying the procedures in a timely manner.

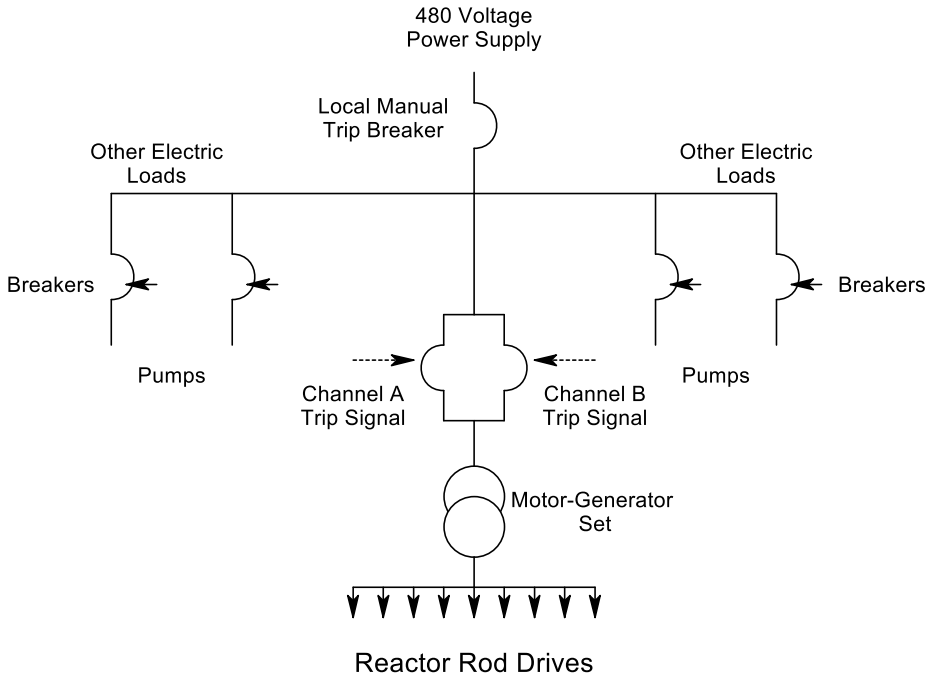

Figure 6.5 One line Diagram of Power Supplies including Reactor Trip Breakers

Clearly, management would not be able to respond on this time scale or interact with the operators in any meaningful way. One could expect management to make a decision in a day to a week's time scale, therefore the process has to be left to the operators. The responsibility of management is to set up a system to provide tools for the operators to take action. One could define this process ab-initio, but the industry has already defined the basic process of selecting the possible accidents, their probabilities, the procedural help [emergency operating procedures (EOPs)] for the operators and training requirements. It is responsibility of the management to embrace the whole approach.

The role of the operators is to be trained in responding quickly and effectively to the likely set of accidents that can occur. It is the function of the management to supply the environment to ensure that the operators succeed when faced with accidents and to determine, with advice, what are the accidents that should be considered. Management must have the knowledge and understanding to supply the tools to support the operators. This knowledge must be comprehensive enough to make correct decisions not only the treatment of accidents, but also open to the possibility that the defined set of accidents maybe too limited in scope.

In practice although the management has the responsibility of developing emergency operating procedures (EOPs) to be used by the control room operators, the task is handed off to experts in developing the procedures. Each of the utilities associated with a so-called

users group, such as the Westinghouse users group for those utilities operating Westinghouse PWRs. The utility still checks the procedures, both technically and from a human factors point of view. The procedures are continuously reviewed and updated by the utility staff.

Management should not only very knowledgeable but be open to take advice on not only accident probabilities but also on the modification of equipment and help guide their decisions with regard to all of these issues. One cannot expect that managers are knowledgeable about all aspects of maintenance, operation and engineering, as well as accident probabilities. The industry has changed fairly recently and the position of Chief of Nuclear Operations (CNO) has been created to meet these demands. This is step in the right direction, but more needs to be done to minimize the risk of NPP operations. Safety and economics have merged together in that even small accidents can threaten the economic viability of utilities. Experience with Tepco has underlined issues with respect to making poor decisions relative to both radiation effects on the public but also the costs associated with clean-up and replacement of electric generation.

6.6 Integral Diagram representation of NPP Organization and Environment

In order to see the real value of the ideas behind the use of the VSM model of a utility organization, one needs to put the Utility VSM model into the context of the rest of the associated organizations and the plant. Although Beer conceptualized the environment in which VSM models operate, he seemed to be less concerned with identifying the details of the operating environment, but he realized that the environment had an effect on the organization. In the case of nuclear utility operations, it is important to understand how these different organizations and plant functions interact with each other and with and the utility.

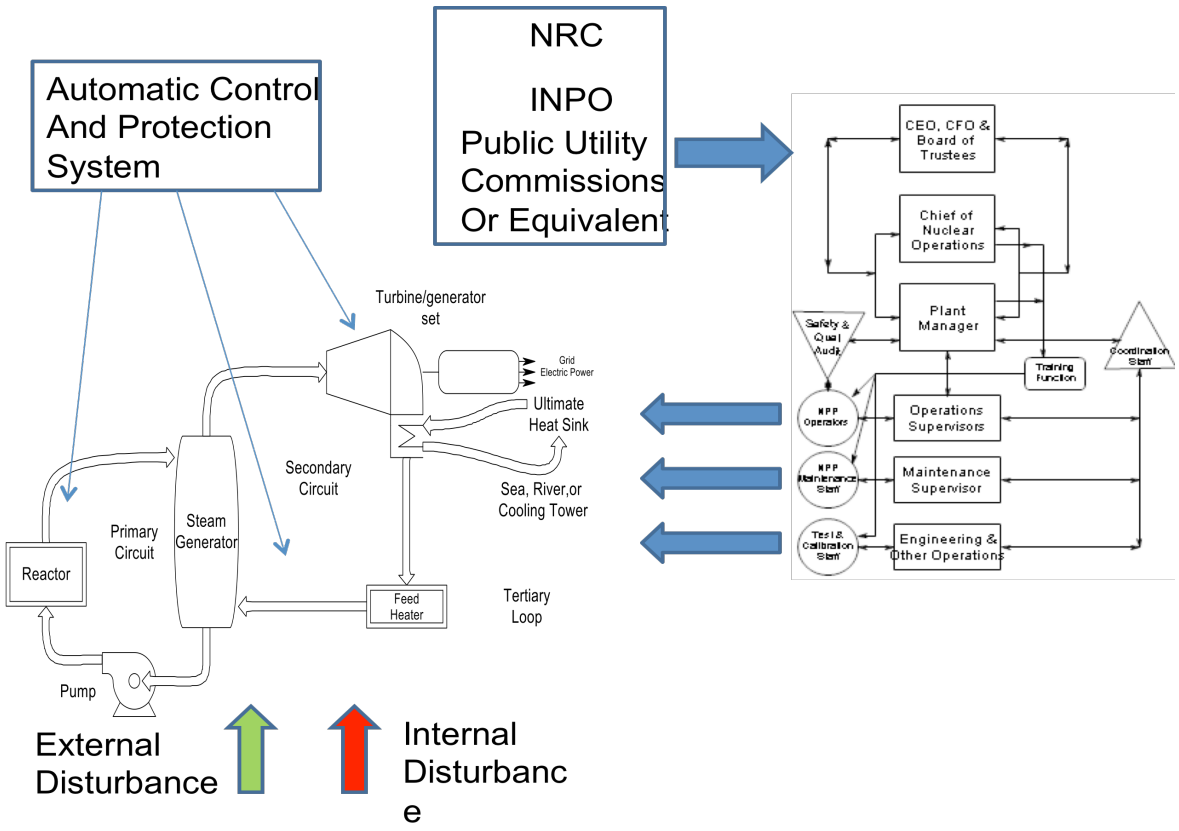

Figure 6.6 Integral Diagram of a Reactor Plant showing Control and Protection Systems, the NPP Organization, and other Organizations along External and Internal Disturbances

Figure 6.6 depicts an integrated diagram showing a NPP, the NPP organization (VSM formulation), the NPP control and protection system, the NRC and INPO, other actors in this system are the organizations that set the electric rates upon which the economic viability of the utilities depend also there are disturbances emanating from external and/or internal sources that can impact safety of operations. Useful insights can be gained by considering all of these units together, so one can appreciate their interactions and the time scales associated with their effects. Interactions between some of the units are considered in separate studies, for example in designing the basic control systems, the plant's dynamic behavior is studied by the use of computer-based simulations of the plant. In the case of the design of the protection systems, different mathematical models are considered and may depend on the characteristics of the accident initiator, so in one case the steam generator may be modeled in detail and in other cases it's the reactor core that is modeled in much detail.

In the use of the integrated plant, and organization model, one has to also integrate understandings derived from the limited studies into this integrated model. The model is not

at this stage of development a big all-encompassing model, but rather the integrated mind model of all the parts. Since these deterministic models can coexist with the probabilistic models; so an integrated model can co-exist with these other models.

One of the issues brought up in the past was how to account for organizations in the study of safety. It is generally conceded that how organizations function have a great influence upon safety. Many persons have said what is needed is for the organization to have safety culture, as though that is the answer. Accident analyses have pointed to decisions made by management as key issues affecting accident initiation and progression without defining how to resolve the issue. Clearly, the regulatory authorities think that the answer is to license the control-room operators. This action helps, but still is does not solve the problem. At one time, research organizations talked about developing organizational factors as an equivalent to human factors but covering organizations. But none of these things seemed to move the industry forward in understanding what needs to be done to improve safety. Clearly the message of history is that accidents seem to sort out what works and what does not work, considering the progression indicated by figure 6.2

The approach advocated here is thought address this issue, since it ties how an organization affects the actions taken by all personnel to improve safety or otherwise. In the case of industry, the accident/incident approach to improvements seems to be well proven from cathedrals being built and falling down, to bridges collapsing, to trains running into each other, to TMI, and Daiichi. However, the nuclear power business was supposed to be different! It was stated that “we cannot allow a large accident to occur”, since the result of an accident could be catastrophic. Then why do we have accidents? Is it because we do not care; that we are stupid, or what? There are a whole lot of reasons and one would not attempt to try to answer this question. Perhaps having a more encompassing model of NPP behavior and its interaction with its environment might improve our prediction capability.

The figure consists of the following parts, the reactor power plant, here a PWR NPP is used just to illustrate an NPP, the reactor control and protection system, the NPP utility organization, the NRC and INPO and the presence of disturbances, internal and external. Each of the elements has been described in Chapters within the dissertation. So these will not be discussed here. However, some mention should be made of likely disturbances. These are things which can occur, upset the stability of the NPP and cover the concept of an accident initiator. In classical risk assessments, one always starts the assessment process thinking about what can upset the normal activity of the plant. Of course, other things are also considered such as the actual state of the plant, are all of the critical plant components working and does the crew respond correctly to the accident. There is one technical feature

that should be mentioned and that is, if all things work properly, is the plant still capability of surviving the accident?

It should be seen that the central and controlling structures of VSM are the two blocks representing the CEO, CFO and Trustees (S5), and the second block of the CNO (S4). These blocks represent the persons, who are in charge of the utility. The NPP is being operated by utility members via the office of the plant manager (S3), who reports to the CEO. The utility operating staffs are the operators including supervisors, the maintenance and test personnel (S1) that report to the plant manager. The CEO and CFO report to the share holders via , representatives, the Board of Trustees. The utility organizational structure was discussed in Chapter 3 (section 3.3). Here the discussion is focused on how the VSM model operates relative to the power plant itself. The overall control lies with the CEO and he is ultimately responsible for all decisions taken, except for the direct operation of the plant via the control room operators (note this is by regulation). For this purpose the control room operators are licensed, see comments in section 6.2.

In an ideal situation, the CEO would be guided by his staff, including even lower level personnel who can have an input, before taking actions which could affect the safety of the plant. In an open safety conscious organization, information about changes in the safety state is passed to the CEO or his immediate staff for evaluation and checking. However, some of the information may be filtered and not come to the attention of the CEO or CNO. The safety awareness of the CEO and his actions in pursuing safety during operating the NPP is a key to the development of a safety culture. The actions of the CEO, aided by his staff, should be involved in enhancing the safe operation of the plant by his decisions. In this decision process, he has to be careful to balance economics with safety. He can help to ensure that both safety and economic goals are met by encouraging the staff to be more efficient in running the plant. This may be done by introducing cost saving processes, like condition monitoring of equipment, better training methods, etc. One of the things that have been carried out by the utilities to ensure the safe operation is to use PRA techniques in a semi-automated manner to help ensure that removal of equipment for maintenance does not lead to a reduced safety state.

The Utility Management has the important role of being the key decision-makers starting with the selection of a NPP in the first place through the operational life of the plant. The life of a NPP plant can cover a period of 40 to 50 years and maybe more. During the life cycle of the plant from design through operation to final closure and deconstruction, there are many changes of management; however each current CEO is left in the position of being the

decision-maker. The types of decisions to be made may change over the life of the plant, including responding to regulatory requirements to industry wide electricity cost changes.

In the initial stages, the management is focused on the design of reactor that is to be selected and its cost. As pointed out previously the designs are not equal in terms of cost and safety. Accidents that have occurred have underlined this fact. It appears that PWRs, such as the Westinghouse and Russian VVER designs are safer than B&W's PWR design (TMI accident). The above PWR designs, not including B&W's design are better than GE's BWR design (Fukushima accident). The RMBK (Chernobyl type) is less safe than the other types. Utility management was faced with something beyond their skills and capabilities in the selection of the 'right' NPP. In many cases, they were advised by the architect engineering companies, but even their skills were not much better from a safety point of view. The industry was not in a very good position at that stage of development. Accidents have led to improvements in NPP safety and also a better understanding of the risks of operation of NPPs.

The correct choice of reactor system appears now to have been very much a guess and maybe related to something other than an understanding of the importance of safety. The point being made here is that decision process needed to be questioned, the persons making the decisions needed to be better informed, and this observation holds even for today.

Another issue that should be emphasized is the need for the utility to be aware of issues buried in the past that could related to safety concerns. Decisions made earlier about the station in terms of equipment, operation and hazards, should be revisited on a regular basis. Beer in his design of VSM had a branch that was connected from the environment to the top levels of the VSM. This branch was there to account for changes in the environment that could affect the output of the factories, and also accounted for changes in the market. The information could make the industry aware of the changes sufficiently early to make modifications to the factories' products and prevent economic losses by continuing to make unwanted goods. In the utility industry, this feature would be used to help ensure that the plant is kept at a high level of safety and that earlier features that reduce plant safety are identified and changed. This feedback feature should also coordinate with INPO and factor NRC's rules and requirements to ensure that the utility top management is fully informed of potential risks to the NPP and make the necessary changes before there might be an accident.

The group responsible for this work should also learn from other plant's accidents and near accidents to understand the implications for their plant. For example, a plant, Davis-Besse

NPP, (NRC, 2008) experienced a problem with cracks in the reactor vessel cladding, which could have led to a loss of fluid along with a control rod ejection accident; luckily it was detected in time. The message for each plant was to examine their records to see if something like this is could occur at their plant. The NRC has initiated actions industry wide, but the message could apply to cases in which the NRC did not act. The responsibility for plant safety and economics lies with the utility. INPO does have a data-base on incidents that can be reviewed by utilities to help in the investigations; unfortunately INPO does not permit this data-base to be used by persons outside of the utilities and their associated companies. The utility should be in a good position to support CEO in his continuing assessment of the risk of operations and the effect of changes in operations.

The CEO and his team are concerned with making judgments between the cost of doing business and the safe operation of the plant. As mentioned above the CEOs need to be brought up to date on the effects of decisions made by prior CEOs and they also have to make day to day decisions on how best to operate the plant. The CEO also has to look to the future to see what decisions should made to enhance safety, increase efficiency of operations as well as being aware of the loss of experienced personnel over time. Currently, there does not appear to be an educational process to produce such persons (CEOs) with the required capabilities: of judgment, training, safety awareness, and experience. INPO has a short course to train CEOs in an appreciation of safety, but this seems very little compared with the need. The quality of CEOs and their assistants, with respect to knowledge and experience, is variable.

The NRC has from the very early days had requirements for the people (control-room operators), who are in direct control of the plant. The initial education standards are not too hard, but during their preparation to be operators, their education is enhanced in that an understanding of reactors physics, plant equipment and safety is taught and tested. Their education is progressive and they serve in a number of roles from plant assistant to board operator to reactor operator. Also they are exposed not only to theoretical studies but also to controlling accidents on simulators. When one reviews the requirements for control-room operators vis a vis the CEOs and even CNOs, one wonders whether this is picture is the best for the industry. One should realize that the decisions taken by top management affect all parts and operations within the utility. It was pointed out in Chapter 5, Figure 5.2, how the decisions taken by management can affect the performance of the control-room operators and others. Section 6.10 uses the ROP program data to examine the persons involved in the causes of accidents, unfortunately the NRC do not go beyond establishing the root causes of the accidents, in particular the role of the decision-makers in establishing how their decisions affected the process. Figure 5.2 constructs how decisions made at a high

level within a utility can affect error execution. It's a pity that the incident evaluations do not go deeper.

6.7 Inter-relationship for Safety and Economics

In Chapter 1 economics were discussed in the context of a capitalistic society in that for a company to succeed it must pay its way and more over create a profit to reward it's investors for the risks they take with their capital. Moreover the concept of a profit is a measure of how efficient an organization is relative to the needs of society, i.e. the bigger the profits the more likely the company meets the needs/requirements of society.

However, in the case of the generation of electric power there has been a move to see electric power as service to be fulfilled by an Electric Power Utility. In this case, the local state government enters into a relationship with the utility to grant it a monopoly for the generation and distribution of electric power. For this monopoly situation, the state specifies the costs that the utility can charge for supplying power. In other words, the electric rates are fixed for a specific time and renegotiated from time to time. So by this method the public, through its officials, sets the conditions under which power is costed. However, there is a move in some US States to move away from Public Utility Commission (PUC) control to a competitive world, in which the utility can charge what it can and still remain competitive with other suppliers, i.e. a capitalistic rather than a monopolistic situation.

The United States Government, within its mandate, is responsible for the safety of NPPs and acts through the NRC. The NRC is not really concerned with economics, only does the plant meet its safety rules? In some countries, these set of rules is called a "safety case." If the NPP meets the rules/safety case, then it is issued a license to operate the NPP. Of course, if things change the regulator can come back and request changes to meet the new situations that have occurred, for example an accident to another NPP may indicate that the rules and regulations were insufficient to ensure NPP safety. Currently, many regulators world-wide are reviewing their regulations with respect to the lessons learned from the Fukushima accident.

The nuclear regulator does not care whether monopolistic or capitalistic situations pertain; its role is to ensure that its rules are followed. So the utility has to ensure that it meets the NRC rules to keep its license, equally it has to meet the needs of consumers to reliably meet their electric power needs within the safety rules of the regulator plus the keeping to the rates set by the public utility commission. In addition, it has to meet the shareholders' investment requirements with reasonable returns on their investments.

The utility management is faced with meeting these set of requirements with relatively little room for margin. If a change occurs in the safety requirements then the utility is forced to return to the PUC for additional compensation. Of course, these things take time to resolve, both the enhanced safety additions and PUC upgrades. The PUC serves the public/politic masters, so changes to the rates may not be approved.

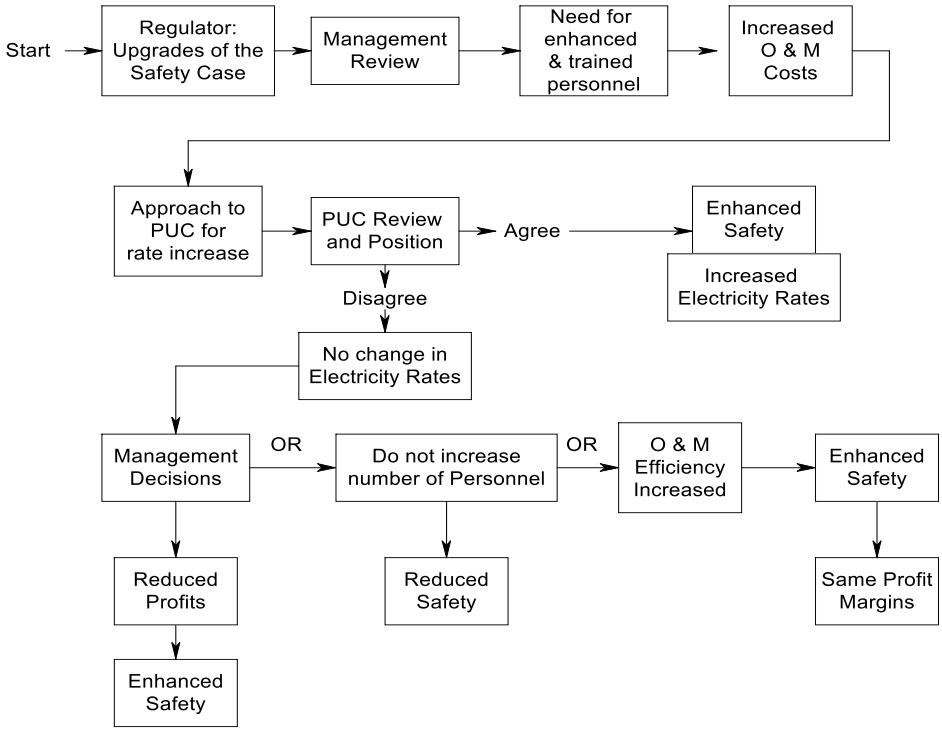

Figure 6.7 Overview of Cost-Safety Decision Process

Figure 6.7 shows an overview of the decisions processes related to changes that can occur in response to safety case changes under the circumstances of a utility operating under PUC rules. Reduced safety can occur if the PUC does not grant increased rates or the utility fails to improve operational efficiency when the PUC fails to act or reduce profit margins to pay for safety enhancements. A concern that the PUC has is that if it authorizes rate increases and the utility fails to act in a fiscally responsible manner and not use the rate increases to improve plant safety.

The utility, when operating in an open competitive power supply world, is faced with a much more difficult situation. It has to decide how to best to meet the regulator's requirements. The options are much less; achieve higher efficiency with lower labor costs, lower profit margins or fail to meet safety goals. That is unless the public is prepared to pay higher electric rates for the nuclear option, but this condition is unlikely.

In both of these cases, the way for the management to assess the situation is to use a decision process as depicted in Figure 6.7, before deciding what route to take. The problems facing utility management in trying to reduce costs without a well developed plan to meet the safety case is illustrated in MacAvoy and Rosenthal (2005).

This section of Chapter 6 indicates the interlinking of both safety and economics in the decision process. It is not an either or situation as far as safety improvements go. One must also recall the effect of management taking poor decisions relative to meeting safety concerns such as the Tepco Daiichi accident. The result of not improving safety is to risk the viability of the utility enterprise. From the point of view of society, plant safety is paramount, but the plant management should equally see this from a company survival point of view. It is likely the investors would rather take a lower return on their investment rather than higher returns along with higher risk of a loss of investment.

An interesting study of the US nuclear power industry has been carried out by Davis and Wolfram, 2011. They have studied the moves taken in the USA of States thinking of deregulating control over the electricity power industry and the sale of 48 of the nation's 103 NPPS to independent power producers selling power in competitive wholesale markets. They have shown that these producers are about 10% more efficient than the dependent power producers, but are uncertain as to exact cause. They say that this improvement is predictable by economic theory. They consider a number of possible reasons such as centralizing services, better managers, etc, when operating under incentives. However, they emphasize that operating efficiency is only one part of considerations in evaluating the overall impact of electric power deregulation. They point out that one important issue is the effect of restructuring on the risk of accidents. They say their results show mild evidence of reactor safety improving because of divestiture, but evaluating this is a priority for future work. Divestiture here is the sale of a power plant by a utility to a bulk power producer.

Interestingly, their studies have indicated a reduction in man-power along with increased efficiency of operation and the need to hold on to the profitability of the operations. The quality and deep understanding of management limitations in their effect on possibly precursors of accidents is key to preventing accidents, which can in turn destroy the company. The model indicated in Figure 6.7 covers the key processes. The difference for an unregulated industry is that the utility has to evaluate what the market might tolerate, so the onus is on them to decide how to use their resources. This in turn could affect plant safety and cause problems with the regulator.

6.8 Influence of Decision-making in the Consideration of Initiating Events

Depicted on the integral figure there are two groups of disturbances that have to be considered in the design and operation of a NPP. These are internal and external disturbances. The external disturbances are related to the location of the plant. For example, tsunamis arise from the interaction of an earthquake and the ocean and occur at the coastline, whereas tornadoes can occur in the center of lands.

Internal disturbances are mainly related to the design and layout of a plant, although sometimes there can be a confusion when cooling water may be drawn from a dam close to the plant. A pipe break inside the plant is an internal event, whereas the failure of the dam leading to flooding of the plant is an external event.

Although initiating events (IEs) are usually well defined by the regulator and known, management decisions are at the heart of what is to be accounted for, unless there are edicts issued by the regulator, such as the definition of peak ground acceleration values for certain parts of the country and those values should be taken as the design basis earthquake for a NPP. In general, the regulator is not going to ascribe to anything that has not been witnessed over a long period of time, so high ground accelerations are required in California and not in New England. For the regulator to do more is to take over the role of management. It is up to the management to propose the basis for the design and for the regulator to ask for proof that that this is prudent.

In the case of the Japanese tsunami in March 2011, it appears that neither TEPCO nor the Japanese Government acted prudently, as far as the protection of the Daiichi NPPs. The assessment of risk (safety and financial) is still a function of the management. Management is and should be concerned about costs, since unless the organization is financially supportable it will cease to function. The best way to tackle both safety and costs is for management to promote personnel effectiveness and efficiency

The current management of a NPP should be aware of earlier management decisions, particularly those that can lead to unacceptable risks including high costs in the loss of the investment and impacting the safety of the public. They should re-evaluate the situation and be prepared to take actions to reduce risk levels. The Tepco position with regard to the size of tsunamis was regrettable, in that the Tepco management did not act, in the light of later information, to shore up the sea defenses around the Daiichi NPPs.

In the case of internal disturbances, management has a role to play in how they deal with the presence of these disturbances. Many internal initiating events come from burst pipes, such as Steam Generator tube leaks/ruptures. In the case of these tubes, it is difficult to monitor them prior to them leaking or rupturing, so management has accepted the fact that

they will shut the plant down quickly on discovering a tube leak and then plugging the tube or tubes. Having shut the plant down, the additional cost of checking other tubes at the same time is relatively small. For other pipes, such as the main feed and steam lines, one can carry out in-service inspections to detect the presence of incipient pipe failures and take action accordingly. This latter approach to the role of management is to reduce the probability of an initiating event by taking a leaf out of reliability engineering practices and use condition monitoring to be more efficient and reducing plant losses.

6.9 Influence of Outside Bodies on Accidents

Responsibility for operating power plants lies with the NPP owners. In the US, the regulator, Nuclear Regulatory Commission (NRC) has been setup by Congress to play an important part in trying to ensure that NPPs are operated safely and act to protect the public. The process is set up in such a manner, that NRC promulgates rules and regulations that the operating utilities should follow and position inspectors residing at the NPPs to observe whether or not the utility follows the rules.

The NRC by its actions cannot prevent or stop an accident occurring, they can only set up a process to push the utility into a position whereby the utility takes the appropriate steps to ensure that the plant is operated safely. If an accident occurs, it is analyzed by the NRC and new rules may be generated to help prevent a similar accident occurring. This is a very reactive process, of course, and the hope is by having NRC inspectors at the site, they will see situations developing, advise their management to intervene and thus prevent an accident. The review of accidents and incidents indicates that the chances of the inspectors of detecting situations that can lead to accidents are limited, often utility personnel are the ones that disclose to the inspectors the near-accident situations.

Other influential bodies in the picture are the Institute of Nuclear Plant Operations (INPO) and the World Association of Nuclear Operations (WANO). INPO is a US based organization working with US utilities, see Chapter 3. WANO acts beyond the US and covers many of the same fields as INPO; in fact they often use INPO personnel to further their effectiveness. INPO can help the utility to improve its operations by assisting with training of utility personnel, performing reviews of utility operations and being a vehicle to pass information on good practices from other NPP operations. INPO also records problems that have occurred at other utilities that might undermine operations at a utility's NPP and passes this information to the group of INPO utilities..

One factor that is not seen to be very influential in the operation of NPPs, but it fact is very important, and that is the cost of power on either the open market or as determined by the

utility's Public Utility Commission (PUC). As mentioned in section 6.7, the cost of power can determine the attitude of management and how it runs the operation. It is easier to afford good people and take time to maintain equipment, when one is not too concerned about profit margins. If the market squeezes the NPP operation, then it takes excellent management to handle financial issues and still run a safe plant. If the state is aware of the needs of NPPs to be viable from a safety and financial view point, then they can apply rules to help ensure plant is operated safety. Equally, if the NPP management is not good, even if lots of money is available, the plant could be run in an unsafe manner. The rules that apply to VSM management functions must take into account the needs of the utility as a whole. The viability of the company depends on the management processes and how effectively they are embodied in the operating rules. The VSM system S5, in particular, has the responsibility to operate in a manner that leads to the utility fulfilling its role as both a safe operation and run in a financially prudent manner.

6.10 Lessons from Review of NRC ROP Reports

Accidents have had a measureable impact on HROs, but are the issues associated with poor management decision-making only visible on these occasions or are they present at other times? Some of other lesser accidents were listed in Chapter 5, these indicated that poor utility operations could lead to big accidents; other accidents/incidents can occur and still have an influence on the industry, see list in Section 5.5. It should be pointed out that these are not the only ones to have occurred. Incidents do occur all of the time, indicating that utility management needs to aware of operational deficiencies that can occur at any time.

In this section, reference is made to the US NRC's Reactor Oversight Program (ROP). Section 3.7.2, that reveals insights into the operation of NPPs. Many issues covered in ROP are associated utility management decisions discovered during power plants operation. The thesis covered some management induced problems in Chapter 5, these were related to the management of Northeast Utilities in the years 1986 to 1995 (Section 5.5.21), and they are also discussed in Perrin's book, (see Section 5.5.27).

The intent in this section is not to cover all the years of NPP operation, but to cover some parts of the ROP record to reveal some of the details contained within ROP records. A number of incidents that occur and their characteristics are discussed here. Observations in the historical data insights are examined to see how the observations are related to functions covered in VSM. The purpose is to see if there is any support for the view that management decision-making is a more important contributor to generation of accidents or incidents than that of the operators.

A section of the ROP data base has been selected for examination. It is assumed that the basic characteristics of the data within the selected data base are typical and no one recent year is very different to another one, so the conclusions drawn are much the same for one year as another. However, there is one proviso; the impact of the NRC attention can cause a utility to modify its attitude taking it from one class to another. Equally, deterioration can cause a utility to drop as a good performer. Overall one could expect the characteristics of the data to remain fairly constant. This has not been proven here. It is believed that there are outliers, which do not confirm to this assumption. The industry organization INPO is also believed to have a smoothing effect on the data by reducing the numbers of outliers; this by virtue of its role in helping utilities with training and organizational improvements.

The data referred to here was obtained from the NRC web site, www.USNRC.gov. Entry was made to the ROP portion of the web site and the current set of data was accessed. The ROP data base allows one to gain access to the data which covers US stations. One can see from the data that most of the stations (units) are run very successfully, but some stations did not have such a good record and did experience some problems. Most of the problems were seen to be fairly minor, but others were of greater significance. Even, the most significant issues were not accidents, but rather incidents. The data does show that the management of some NPPs is not as good as the majority.

Table 6.1 shows the list of 'problem' plants' of which there were 19. The rest of the US NPPs (84 units) had acceptable performance and were placed in a category whereby they are inspected occasional, rather than operating under tight enforcement. The assumption is for these nominal well run plants, management is operating fairly effectively and there is no reason to carry-out any further investigations. This means that about 22% are under a varying degree of risk and are under some enhanced monitoring by the NRC. The experience with the Northeast utilities indicates that it is possible to operate plants poorly and not get into an accident. It is the combination of both not operated the plant correctly and then not being exposed to an unexpected initiating event that can develop into a major accident. This state could be called a quiescent state of operation with the utility just waiting for an initiating event to come along to lead to a major accident. A couple events that could cause an accident in the case of these plants are the arrival of a large winter storm, like Sandy, and the failure of an internal pipe leading to flooding of any one of the units. The Millstone plants could have been in the path of a large storm travelling up the coast!

ROP Action Matrix Summary (Up to date 2/4/2013)

Licensee Response Column	Regulatory Response Column	Degraded Cornerstone Column	Multiple/Repetitive Degraded Cornerstone Column	Unacceptable Performance Column
84 NPP Units	15 NPP Units	3 NPP Units	1 NPP Unit	0 NPP Units

Table 6.1 NRC ROP Action Matrix Summary

However, as the Northeast Utility experience informed us the deterioration in plant performance induced by management activities leads to increased unavailability of the plants systems and possible increased risk of a major event. The Tepco experience leads us to the conclusion that failure of the management to understand the risks associated with external initiating events and act to minimize their effects can end up causing the near demise of the company and long term problems for the country.

The ROP data reveals that some 20% of plants do have problems, which can be minor to more severe. Examination of the NRC site inspectors' reports can reveal different problems. The inspectors' reports are grouped into the following areas, see Figure 6.8:

1. Initiating Events
2. Mitigating Systems
3. Barrier Integrity
4. Emergency Preparedness
5. Public Radiation Safety
6. Occupational Radiation Safety
7. Security

The first four are associated with reactor safety. The next two are associated with radiation safety and the last with safeguards. The NRC inspectors in their reviews of incidents place the incidents into one of these groups. All of these groups are associated with internal events and do not cover the topic of external events, like earthquakes, etc. In other words these events result from the activities or lack of activities of the NPP organization personnel.

Seen from the VSM view point, these activities can then be related in some ways to Systems 1 through 5. One can go to the NRC web site and see the reports associated with given plants. The reports point out which area that the incidents are identified with and what they think that is the cause of the incident. In these public reports no person identified as the cause of an incident. Also, the area covered under 'security' is not covered in the data given

on the web, since it might give key information about security weaknesses at the plant, for obvious reasons.

Covered here is one particular plant, Robinson 2, for the four quarters of 2012. Figure 6.8 covers information on the Significant Inspection Findings for the four quarters.

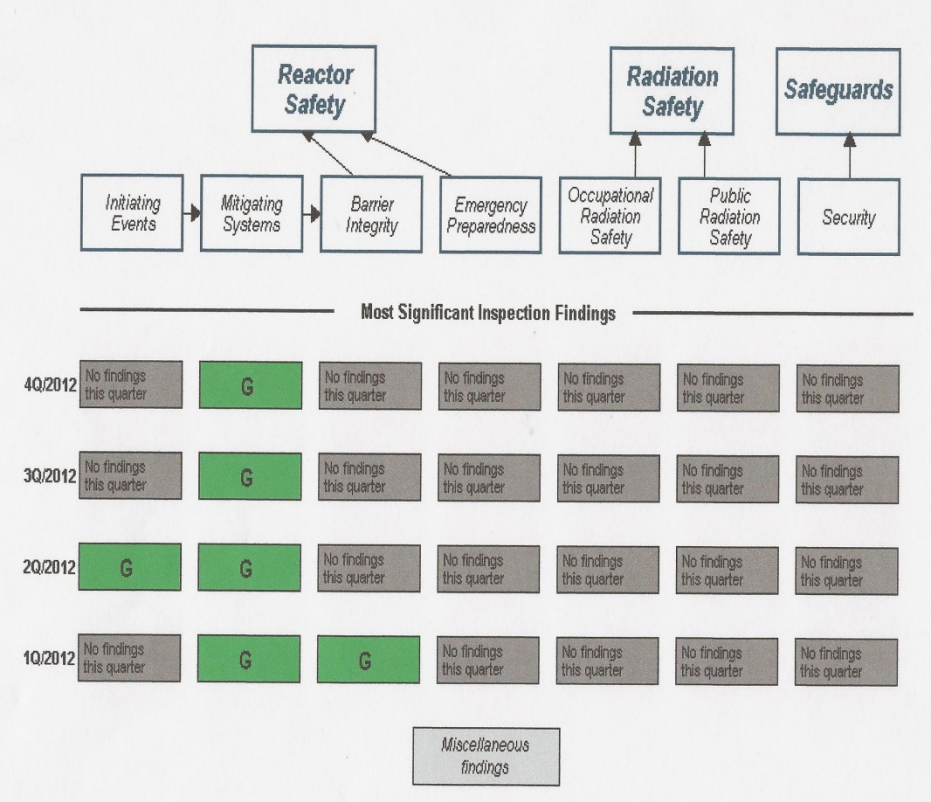

Figure 6.8 Performance Summary for 2013 for Robinson #2, 2012 (NRC.gov)

The table shows that there are some GREEN areas (see Chapter 3.11) events that occurred in 2012, that were Reactor safety issues associated with Initiating events, Mitigating Systems and a Barrier Integrity event.

To illustrate these reports, an example is given below:

Significance: G Jun 30, 2012
Identified By: Self-Revealing
Item Type: FIN Finding
Lack of preventive maintenance on feedwater control switch results in an automatic reactor trip
A self-revealing Green finding was identified when the licensee failed to establish adequate preventative maintenance for equipment associated with the feedwater control systems. Specifically, the licensee's inappropriate classification of the

feedwater flow loop selector switch as a "run-to-failure" component permitted the switch to remain in service, without preventative maintenance, until its failure on March 28, 2012, which resulted in a feedwater transient and reactor trip. Corrective actions included the replacement of the failed switch and future replacement of seven additional switches that were deemed to be at risk for a similar failure. This issue has been entered into the corrective action program (CAP) as Nuclear Condition Report (NCR) #527203.

The licensee's inappropriate classification of plant equipment in accordance with ADM-NGGC-0107 Rev. 1, Equipment Reliability Process Guideline, which permitted feed flow selector switch 1/FM-488B to remain in service, without preventative maintenance, until failure was a performance deficiency. This finding was determined not to be a violation of NRC requirements. The finding was more than minor because it was associated with the initiating events cornerstone attribute of Equipment Performance, and it affected the associated cornerstone objective to limit the likelihood of those events that upset plant stability and challenge critical safety functions during shutdown as well as power operations. Specifically, the performance deficiency caused an automatic reactor trip from 55 percent power operations on March 28, 2012. The finding was determined to be of very low safety significance (Green) because the finding did not contribute to both the likelihood of a reactor trip and the likelihood that mitigating equipment or functions would not be available. The performance deficiency had a cross-cutting aspect of Evaluation of Identified Problems in the area of Problem Identification and Resolution, because the licensee failed to thoroughly evaluate the events in 2010 and 2008 such that the resolutions addressed the causes and extent of conditions as necessary.(P.1(c)) (Section 1R12)

There are several points to be made from this inspection report. The incident was a reactor trip caused by a feedwater transient induced by the failure of feed water selection switch, so this was an initiating event, which could lead to reactor safety incident. The maintenance personnel failed to categorize the switch correctly and placed it in a run to fail rather than in the maintenance prevention category. Apparently, there were other occasions, where the maintenance personnel failed to do this task correctly.

The NRC does not further analyze the situation and identify whose responsibility it might be. Seen from a VSM view point clearly the Control Room operators were not responsible, they just responded to the event and did take an action. Maintenance staff was not directly the cause, since they would maintain the equipment as instructed. The ultimate responsibility rests with the Chief Nuclear Officer (CNO) and his staff supported by the PRA group looking at the effects of both equipment and personnel actions on the safety of the plant. The plant engineering group under the Plant Engineering Manager should also be involved to help other personnel understand how the plant operates. The good thing here is that this was an incident identified by the plant personnel.

Taking this report together with Figures 5.1 and 5.2, we can see the involvement of S1 (Maintenance supervisors), S3 (Plant Manager) and S4 (CNO). The maintenance categories ought to have been established initially by the NPP designers, but this was a long time ago. The Control and Protection design logic was done in 1967 (private information, Spurgin was the designer of C&P systems). It is the responsibility of CEO (System 5) to have had a review of requirements carried out every few years. It is responsibility of the CNO (and Staff) to review the safety systems to ensure that plant is not exposed to too high a risk.

Although the main responsibility rests with the utility to ensure that the plant is safe and not exposed to undue risks which can impact the economics of operating NPPs. The NRC (or other Regulators) can perform a useful function of investigating seemingly minor incidents, which can reduce the risk of larger accidents occurring. Additionally, experiences with similar plants having a variety of problems can aid the utility to review its operation to see if the same type of problem is present in their plant.

6.11 Reconfiguring of Organizations: Post Accident

Among the lessons to be learned from the Fukushima Daiichi accident is how NPP organizations should react to an accident that has occurred. A NPP organization should become very focused on combating the effects of the accident. All of the non-necessary personnel should be evacuated and the rest of the personnel directed to activities to help terminate or mitigate the effects of the accident. One point should be made about the Daiichi accident is the fact that the site personnel and management were not trained to deal with an accident of this magnitude. As a result, the site manager had to work with personnel to review the state of the plant, take out drawings and formulate an action plan of the “fly”.

Things would have gone much better if there had been an effective plan supported by trained personnel and helped by having supplies set aside for such an emergency. In the case of Daiichi, personnel were scrambling for batteries, lights and other tools, when they would have been better off actually fixing problems like closing/opening valves, venting hydrogen from inside the reactor building, injecting water into the reactor cores to keep them covered and ensuring the accident did not progress. However, the supplies were not available!

Had the management not “destroyed variety’ a la Beer, this would not have left them with reduced capacity to attend to an unexpected transient. If management had a better idea of the requisite variety for these sets of circumstances, they would have gone from developing

a higher dam to stronger water tight doors to the supply of batteries, etc. But then maybe the accident would have not been the 'worst accident,' since Chernobyl!

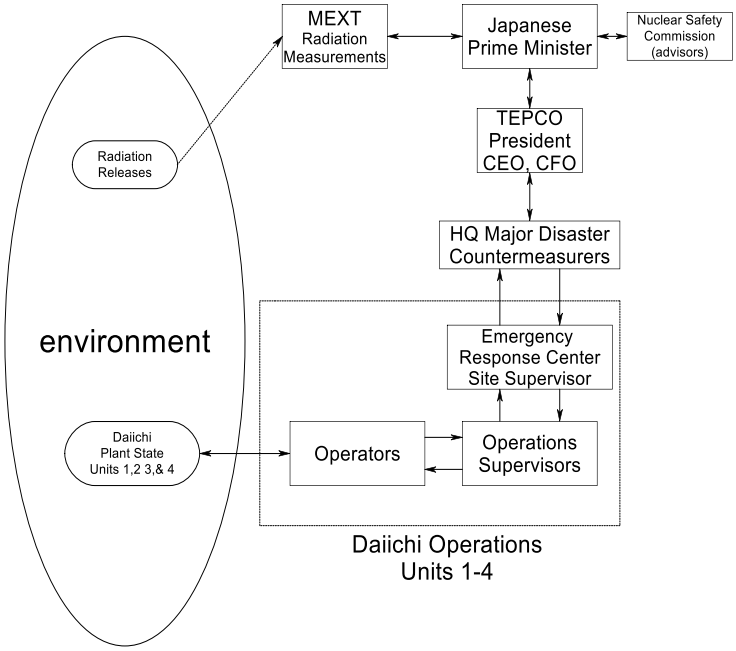

Figure 6.9 VSM of a NPP Organization: Post-Accident

Figure 6.9 shows a VSM representation of the compact Daiichi organization formed after the accident had occurred. One can see how the normal VSM representation has 'morphed' into the more compact organization. The only problem is before this organization became effective, they had to develop a plan, check the possibilities for taking action and try to assemble tools to make it possible. The analysis of the situation and the assessment of what to do took valuable time. This work should have been initiated by management well ahead of the accident. The crew was not successful in achieving the goal of limiting progression of the accident. They seemed to have been personally very courageous, but the accident got worse at time passed, reactor cores were damaged and there were multiple hydrogen explosions that further damaged equipment and led to radiation releases. Also, access routes were affected by tsunami debris and hazarded by the effects of explosions and continuing earthquake aftershocks.

The top management further delayed responses by waiting to authorize the flooding of the reactor core with seawater. Furthermore, because of restrictions on venting the reactor

system also delayed things. The venting of steam from the reactor vessel would have enabled the pressure to be dropped and allowed water to be pumped into the vessel. This restriction was in response to government requirements to evacuate nearby persons before venting.

The initial tsunami effects could have been prevented by the correct design of sea walls/break waters, by the placement of diesels and the incorporation of water covers and hatches to prevent the ingress of sea water to short the electrical systems and prevent their use to operate equipment. This failure rests at the feet of TEPCO management; no amount of heroic activity could have prevented this accident. In fact the Japanese Government has much to take blame for, not forcing TEPCO to build sufficiently high sea walls but also for not investigating how to prevent the loss of life and property in the district affected by the tsunami. It is considered that if a well designed tsunami system had been set up much damage could have been prevented and many people would have survived.

The full scope VSM NPP model (Figure 5.1) shows a planning pathway between the environment and the NPP management team. There needs to be a manager responsible for planning and implementing ways to reduce risk from accidents beyond design basis. The managers associated with both planning and nuclear safety should consider risks associated with both internal and external disturbances and design the appropriate measures to reduce both safety and economic risks. In the case of the lessons from Daiichi, this means the preparation of measures to reduce risks by developing emergency plans, training personnel to use procedures to speed the process of performing in such a way to reduce safety and economic risk and have available tools to enable actions to be taken.

One other point should be made here is that the ideas that led to the development of the symptom-based procedures after TMI should also be applied here to consider what actions might be needed in the case of accidents that fall outside the design basis approach. For example, what happens if the plant is affected by multiple initiating events rather than one specific initiating event at a time? This would answer the question about how much worse could it get and what additional things would be required to restore the plant to shut-down conditions.

6.12 Application of Integrated NPP Model

The integrated NPP (INPP) model (Figure 6.6) depicts the central role of management in the operation of a NPP. So how does one use the model to generate insights into management operations? Management has a balancing act to perform between safety and profitability (Figure 6.10). The top management is faced with making decisions in both these areas, as

is show below in the figure. A review is always carried out by concerned members of the utility team and it is recommended that risk evaluations are made before final decisions are taken. The Chief Nuclear Officer (CNO) has a special responsibility for nuclear safety and risk evaluations. The risk evaluation should be carried out as indicated above based upon PRA calculations. Quantitative evaluations are to be preferred so like can be compared with like, otherwise one returns to the state when the consequences maybe the same but the likelihood one event is so much more so than another. The higher probability event should be tackled first, but this does not mean one should forget about other events. To operate safely, management needs to evaluate the risks of operation and then reduce the risks in a cost effective manner. Equally, the management needs to increase the effectiveness and efficiency of all maintenance operations to maintain costs under control. Steps to reduce costs without paying attention balancing those without increased emphasis in effectiveness and efficiency can lead to unsafe operations and the reduction in plant availability; this message is clearly given in MacAvoy and Rosenthal, 2005.

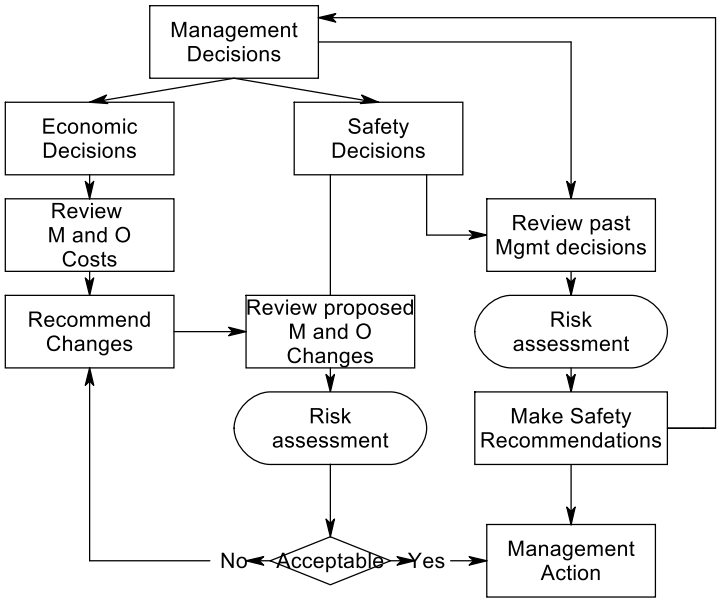

Figure 6.10 Management Decision Process

The figure shows the breakdown between economic and safety decisions. Both are important and both have to succeed in order to have a viable utility/industry. On the economic side, management should be reviewing how two important cost centers, maintenance and operations, are organized and carried out while looking ways of introducing technological and efficiency concepts to reduce labor costs, while examining the use of these techniques from a safety point of view. These ideas cover improved training methods and better logging processes.

On the safety decision side, management needs to be aware of changes that could call into question the assumption that the decisions made in the past, with respect to environmental effects and internal plant risks are still valid. The industry has learned from accidents how things can change and how past ways of doing things have to be modified to ensure these accidents are not duplicated in other plants. The data bases of both NRC and INPO should be accessed from a learning point of view and the lessons applied by management to their plants.

Having identified areas of enhanced risk, management needs to understand how important these risks are. Are the risks large or small, management needs to determine what is the consequence of a particular issue and how likely is it to occur? If the risk is small, then it can be put on a list to attend to later. If the consequences of the accident are high, in terms of reactor core damage and consequentially led to the write-off of the investment in the plant, then management should heavily review the analysis process to see if the probability of such event occurring is high enough for them to be concerned. Credibility of the probability assessment should be increased by getting independent reviewers to review the assessment.

Currently the industry is using PRA techniques in a number of different ways, for licensing purposes and for running the station. The use of PRA for licensing purposes is tied somewhat to the approaches recognized by the NRC, so this use will continue. In the case of plant operations, the PRA is used to evaluate how maintenance/test operations are carried out so the increased risk of doing is tolerable. This use of PRA mirrors the use of the technical specifications to control NPP risk exposure.

It is considered that one of the prime uses of PRAs should be used to support management decision-making and for re-evaluating decisions made previously by management, as discussed above. PRAs should be part of the constant improvement process in operating the plant. The PRA itself should be subject to improvements not considered a fixed implementation way of doing business. For example, Prof. Leveson in her book (Leveson, 2011) has raised a number of issues with respect to the viability of PRAs, some of these objections have addressed, see Chapter 1. The PRA is a key tool to be used in the evaluation and control process associated with the Integrated Nuclear Power Plant (INPP) process. Figure 6.11 shows a risk assessment as part of the process of ensuring safety in the operation of NPPs and is a key element in the manner that management exerts control over plant operations to ensure both safe and economic operation. It should be mentioned that management has a responsibility to help ensure plant personnel are safe during the

time they are working in the plant from a variety of personnel risks including radiation, dropped loads, exposure to steam and high pressure water, etc.

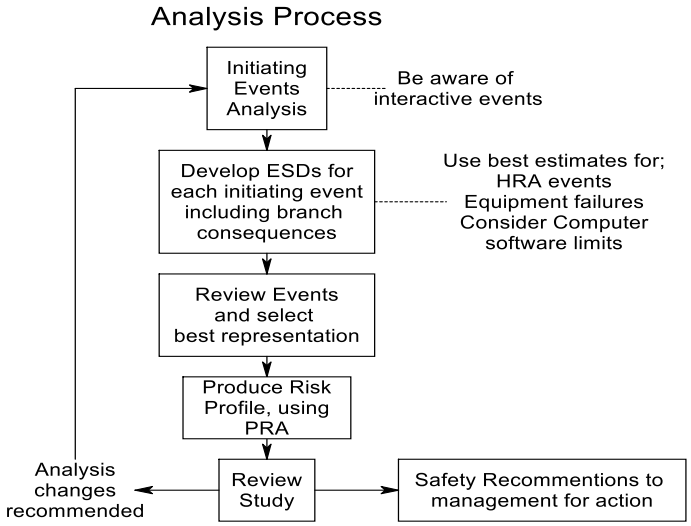

Figure 6.11 Suggested Analysis Process for Safety Improvements

The above discusses the tools to be used and the studies to be carried out before decisions are made, but no mention has been made with respect to training, background or experience of the top management personnel. This seems to be a sensitive area for both the NRC and INPO. It seems strange that the NRC has requirements with respect to control room operators related to training and experience, but next to nothing with regard to personnel beyond the level of control room supervisor. INPO's background is very much related to the US Navy, since many of their leaders have come from the Navy. The Nuclear Navy was very much the child of Admiral Rickover and he was adamant about the need for extensive training and the requirement to escalate the individual responsibility of personnel serving on submarine crews. He was concerned with radiation and pushed the personnel to understand that topic and the safety aspects of nuclear submarines. Appendix A covers some aspects of his views on the subject.

It is believed that for top managers to make decisions related to safety without a clear understanding of the topic, the tools and basic data leaves them exposed to increased risk of making poor decisions leading to possible accidents, exposing the public to radiation releases and large economic losses for the utility. The history of accidents covered in this dissertation points to issues where top management has either taken incorrect decisions or failed to take correct decisions, leading to bad accidents.

Two cases come to mind, the fatal launch of the Challenger (1986) and the recent Fukushima (2011) accident, and it should be noted that these are not the only cases. The

first was a case of not taking advice from NASA engineering staff on not to launch because of possible problems with “O” ring sealing capability when cold and then continuing to launch the shuttle and the second for failing to heed to Japanese seismic experts on the possibility of large sized tsunamis occurring and not taking action to evaluate the plants’ current design basis tsunami impact as to predicted height of the incoming tsunamis. The cautionary point being is to make sure the decision-makers have sufficient skills to be able to check their evaluation relative to others.

There are issues that aid in seeing the big picture a combination of: transient analyses, accident analyses, PRA, controller studies, modeling both human and equipment by controller models, management models and psychological models. There are a whole group of things one can look at, each contributes some insights, but the integral model should help with combining many of these things together to aid management, including CEOs and CNOs.

6.12 Risk Methods used for Decision-making at various Levels within Organizations

Currently, risk methods are used within the nuclear utility industry to assess the overall risk of power operations, mainly in response to regulatory requirements to indicate the risk to the public is low enough to be tolerable. The measure used is to compare the Core Damage Frequency (CDF) as estimated with a figure of 1.0E-4/year, or something very similar. The CDF figure is the province of the regulator. This seems to be a ‘pro-forma’ requirement to assure the public of the safety of NPPs through their representatives (Congress) and their appointed regulators, the NRC.

Weaknesses within the NPP operations can be found by the NRC inspectors and also self revealed by utilities. The impact of some of the weaknesses is further examined by carrying out PRA studies and the results can lead to changes in equipment or operations. This information is then released to assure the public that the industry is properly regulated and the NPPs are safe to operate. The NRC likes to combine both PRA and classical safety studies in their evaluations of NPP safety.

The industry has been known to perform PRA studies with a view to see if regulatory requirements are too severe and defend their positions, as far as safety of the plant is concerned. The industry has, for the last few years, used PRA techniques to examine whether removal of safety equipment for maintenance purposes can lead to unacceptable increases in risk. The concern here is to ensure that reactor control room operations staff does not allow essential safety systems functions to be affected and place the NPP into a situation that mitigating systems functions are not available when needed, i.e. during an

accident. The Main Control Room (MCR) staff is required to sign off on plant equipment changes and to indicate in the MCR which equipment is unavailable. These actions are required before the maintenance department can proceed. Examples of such actions that are not correct are the deactivation of a pump in the high pressure water safety injection system and at the same time as working on a valve the redundant high pressure system, ending with both safety systems out of commission. Earlier, a set of rules were agreed with the NRC on what equipment could be worked on and how long it could be removed from service. These conditions were covered by "Technical Specifications". The MCR staff has a version of the plant's PRA available to them in the MCR, so they can see the effect on the plant's CDF as a result of removing a key component from service.

6.13 Summary

The objective of this chapter was to examine the features of Beer's VSM with regard to the operation of nuclear power utilities from the management of safety and economics. In examining VSM and its potential use in being considered for NPP applications; the whole field of NPP design and operations has been examined including the important area of NPP organizational approaches to accident control and mitigation. An important question raised during the study: 'is the VSM a useful organizational structure for NPP Utility organizations, particularly with respect to handling safety issues"? A corollary question is; 'can it be modified to better fulfill that requirement'?

Accidents have had a central and important place in the development of the NPP industry. It appears that the NPP organizations have been able to operate quite successfully as long as they are not affected by some form of accident initiator, be it internal or external. In other words as long as the environment is quiescent, all is fine. However, if the organization is tested by some form of incident then things are not so good. The organizational changes that have occurred over time have come down to the adaption of the industry to the reality of certain accidents.

Insights have been gained from the study of some of the key accidents along with the study of human performance methods to establish how organizations actually operate, and why organizations fail to deal with accidents quickly and efficiently. VSM in its normal organizational form can be used to represent a NPP organization in the quiescent state, but needs to be modified to address the issue of time sensitive actions to be taken to prevent or limit the impact of the accident.

The chapter covers a number of different areas related to how NPPs operate including the central role of the utilities' management in the decision process and those things which

influence the behavior of the organization relative to time to take actions. Figure 6.6 covers the relationships between utility management and staff as indicated by the integration of VSM NPP management and personnel with other organizations and features that influence NPP operations. Features, which can affect the behavior of the plant, are the dynamic characteristic of the plant and its control and protection systems, and internal and external disturbances. Organizations which affect NPP operations are the regulator (NRC) and an industry group (INPO). The NPP management and personnel are there to control and manage the operation and respond to disturbances which can affect plant and public safety.

The use of VSM of itself does not improve either safety or reliability of NPPs. The selection of the right staff, including the CEO, can help ensure both safe and economic NPP operations. Knowledge of VSM along with an understanding of risk measures and human performance issues can help this happen.

The thesis covers the analysis of NPP operations when faced with safety issues, as regulated by the NRC and under conditions of being assisted by INPO. The emphasis here is with the evolving role of the top management in the whole process in operating NPPs safely and efficiently from a cost point of view. Many safety studies of NPPs have not focused on the role of management in affecting plant safety. The structure of VSM clearly indicates that decisions are made by management, this process can be evaluated and recommendations can be made to improve their decision-making. An understanding of the manner in which both management and operators react to accidents can be used as a guide to better define the roles of management and operators within the VSM structure. The VSM systems S3, S4 and S5 are concerned with decision-making and planning, whereas systems S1 and S2 are associated with taking actions and directly responding to accidents. The first group is associated with knowledge-based behavior and the second group associated with rule-based behavior (Rasmussen, 1983). This means that we should expect the first group to be involved in the review and consideration of accidents in terms of what is the likelihood of an accident and what preparations should be undertaken? The second group is under the control of the first group and is dependent on the decisions taken by the first group. The first group decides the quality of the procedures and their extent (relative to what accident set they should respond to). They also consider the associated training of the operators to enable the operators to operate in an effective rule-based mode, when dealing with accidents. To expect them to operate in knowledge-based mode to cover the inadequacies of management is to be hopeful, since they are not likely to have the deep knowledge required not to be able to carry-out the correct responses in time. One can see this very well in the case of the actions of the site personnel following the accident at Tepco Daiichi NPPs, Section 5.5.12.

The chapter concludes that despite the all of the design efforts of the NPP designers, the safety considerations of the NRC and its associated research organizations, the National Laboratories, accidents still occur. It is pointed out in the chapter the role of accidents in shaping how the industry is changing, see Figure 6.2. Changes have come about in the design of the protection systems, the role of humans in responding to accidents and the training of operations personnel. The NRC has become more involved and has been generating a growing number of rules to cover the issues revealed by these accidents. INPO came about because of the situation in the industry at the time of the TMI accident. It was felt by the industry at that time, that an accident at one plant could affect the whole industry and there was a need to have an industry based organization, this was INPO, to help improve performance of the NPP industry. INPO had effectively two roles, improving training methods, reviewing operations and feeding back information on the performance of utilities on best practices. The effect was to have two external organizations NRC and INPO acting as feedback mechanisms on the quality of the NPP operations, but in different ways.

Management should be aware of the impact of main control room (MCR) of instrument and display layouts coupled with procedure design on associated risk factors. This kind of information needs to be available to management before deciding to spend funds in the hope improving safety and/or economics.

Another lesson derived from accidents is the possibility that decisions taken by earlier in the life of the plant may not have improved plant safety and should be changed. This means that management should review past decisions on a continuous basis and upgrade plant safety. The evaluation of earthquakes, tsunamis, floods, hurricanes, etc. can change over time. The earthquake/tsunami in Japan exposed flaws in Tepco decision-making relative to the flooding aspect of tsunamis. The Daiichi NPPs were completely unprepared for this event and the complications resulting from their degree of unpreparedness.

One thing that sticks out of the review of the role of management in the control and decision-making related to plant operations is the lack of formal educational processes on the selection of top managers or members of the Board of Trustees. This is in contra-distinction to the steps taken to train control room operators. The industry has a model for how to have a training program for operators and executive personnel to operate nuclear plant (submarines), which ensures that the trainees focus on safety and control of radiation effects, see Appendix A. The officer grade personnel get technical and leadership training and experience in applying these skills.

The industry has developed the position of Chief Nuclear Officer, who is expected to be well trained and experienced in nuclear matters, but none the less the CEO is still the main

decision-maker. By connecting VSM to plant has given a method to closely tie management decisions to plant operations. Figure 6.10 outlines a management decision process resting on both current concerns and effect of past management decisions. It is suggested that risk assessment studies be carried out by management before making important decisions. Figure 6.10 depicts a suggested process for carrying out a risk assessment weighing economic and safety issues associated with past decisions and current decisions related to manpower costs. Figure 6.11 depicts the analysis process for evaluating the risk associated with changes in initiating events or their estimated probabilities.

The plant model should include re-evaluation of the failure modes of the plant and equipment. The human element should also be re-considered based upon the latest data on personnel performance. For example, the Tepco accident illustrated amongst other things the effect of floods on the strength of flood resistant doors; flood forces occurred due to unexpected height of the water plus the impact of the tsunami waves. As a result of an earlier incident at the Blayais NPP on the Gironde Estuary (IPSN, 1999), Electricity de France re-evaluated their flood protection for NPPs near major rivers and estuaries.

The risk assessment processes indicated in Figure 6.10 could have been used for all of these cases. The use of risk management techniques like PRAs coupled with advice from CNOs and insights generated by concerned workers on safety can enhance plant safety. The outside world plays a part by having an energy policy that recognizes the special requirements of NPPs compared with fossil and other methods of power generation.

Economical operation is important in nuclear power to enable utilities to continue to capable of competing with alternative power sources. It is more important that they should be operated in such a manner that accidents, which can affect the public and the viability of the utility, be prevented. One can see that accidents like the Daiichi accidents have severe implications for the continued existence of the Tepco organization, due to the core damage and plant clean-up, which might go on for years. It is not so much a case of how many people were killed, there were two plant personnel or even do to the escape of radio activity (long term effects seem to be limited as mentioned by the World Health Organization, 2013, but the loss of the plants, clean-up of the site and surrounding areas. It should be noted that even a smaller accident, which contaminates the reactor can have large effect on the viability of the utility to cover the costs; loss of a unit, clean-up and supply of lost power.

Although VSM is a useful concept, for NPP utility application the characterizations of the systems S1 through S5 have to be modified. SI and S2 characterization should include the need for the associated personnel to have access for well-designed procedures and training to enable them to work effectively and efficiently, S3 through S5 characterization should

include the need of the associated personnel to be aware of their time response deficiency, the requirement to be trained and experienced in nuclear operations and be responsible to support S1 and S2 personnel with the tools necessary to ensure both the safe and economic operation of NPPs.

S5 management needs to be aware that they should use the facilities of both the NRC and INPO to ensure that the utility is operated safely. Both the NRC and INPO should be prompted to help ensure that the utility is a viable entity, this can be done by supporting the utility's evaluation processes to supplement the utility lack of resources. In addition, risk-benefit awareness is needed by S5, S4 and S3 in making decisions along with access to the appropriate tools. They also need to draw upon experts to perform these analyses. We have seen cases where the decision-makers have relied upon their own knowledge, which is of questionable value and have come to the wrong decision, for example see the Challenger accident.

Figure 5.1 depicts VSM structure of a US utility and covers the connections mentioned above between the utility, the NRC and INPO. Chapter 3 covers the functions of the NRC and INPO from their point of view. As identified by Figure 5.1, the connections are not one way and the utility should draw upon the facilities of the NRC to help define both the possibility of an accident occurring, its probability and consequence and what needs to be done to prevent it occurring. The INPO relationship is different in that they are prepared to help the utility within their capability.

Beer System, Outside Organization	Positions and Type of Organization	Requirements
S1 and S2	Operators and Shift Supervisors (also covers Maintenance)	Knowledge of reactors and plant, trained in the use of procedures and experienced in using simulator and operating the plant, Good communications with supervisors on plant state, be aware of the need for good procedures to cover accidents
S3,S4 & S5	CEO, CFO, CNO, Plant Manager	Good knowledge of nuclear plant operation experienced at other grade levels, capable of using risk techniques and accepting advice on highly technical issues. Good working with people and communicating with lower level staff. Need to be aware of time response limitations in dealing with accidents and how one can compensate by the use of trained personnel and

		good procedures. Use NRC research to compensate for lack of utility resources
NRC	Regulator and Research Organization	Carryout normal regulatory requirements, work with utilities to achieve a safer industry by carrying out accident investigations and communicating findings to utility management and work with industry to solve problems before accidents occur.
INPO	Monitoring and Training	Continue to operate as they do now; assisting in training of all levels at the utility and giving advice when requested. Advocate better understanding of Nuclear operations and training for CEOs

Table 6.2 Definition of Requirements for Elements in VSM Representation in Figure 5.1

What is missing in the Figure is the attitude of S5 person or persons (including the Board of Directors/Trustees) to be aware of their shortcomings and develop a better approach to the operation of running a high risk operation, which has both safety and economic concerns.

Table 6.2 is an approach to define the elements of the modified Beer's VSM to reflect the needs of a utility as far as safety and economics are concerned. As one can see the considerations are fairly general, but they do high light the key differences between a commercial organization and a NPP/HRO type of organization. The key difference for an NPP/ HRO versus the normal commercial organization is that one has to deal with the possibility of an accident and one cannot deal with it on the fly. Management has to realize that the time available to respond is usually insufficient for them to be involved directly, they have to plan and work through others (operators) to ensure safe operations.

The possibility of an accident has to be considered ahead of time and the organization has to be thoroughly prepared to deal with it. Not only should one consider the accident, but also the time lapsed consequences of the accident. The environment may be effected by debris, which can affect the actions of the recovery personnel, preventing easy access to key equipment, such as valves. Walls fall, rooms become filled with radioactive materials and tanks become blown off their supports and prevent trucks transporting tools and personnel, this was seen at Fukushima and was a lesson for all. Pre-accident training scenarios need to factor these kinds of constraints into the processes and procedures.

Upper managers must be involved in the process of reviewing the list of possible accidents and assessing their probability and consequences as far as the utility and the public is concerned. Safety, as far as the public, may be controlled, but the risk to the utility of survival is questionable. Small accidents can have severe effects for the health of the utility. Money and time spent on safety mechanisms including developing procedures and improving training for adverse conditions may preserve the utility.

As mentioned above Beer's VSM has some of the right ingredients to represent safety-related organizations, which have some aspects in common with commercial organizations. However safety-related organizations have needs that are singularly different to commercial organizations and some of them have been covered above.

One of the key concepts in Beer work is the idea of variety and requisite variety (Ashby), as mentioned earlier. If management has a good understanding of these things and the actions required to satisfy the requisite variety in different accident contexts, then the results of having a initiating event should be a tolerable situation and not an accident that tests the viability of the company and possibly leads to the general public being exposed to radiation.

CHAPTER 7 Findings

7.0 Introduction

The basic objective of the dissertation was to examine Beer's VSM cybernetic management control principles, as applied to industrial organization, to see if it could be applied to the Nuclear Utility Industry to enhance the safety and economics of Nuclear Power Plants (NPPs) in a meaningful manner, particularly with respect to management decision-making and organizing responses to accidents. The investigation also considered other HROs, such as oil refineries.

Currently, the industry appears to be more focused on equipment, operational personnel and outside disturbances in the evaluation of plant risk rather than the decisions and actions of top management. It is felt that decisions made by management are much more at the center of the risk of nuclear power plant operations than the random actions of lower level personnel. Currently, there does not appear to be a method to connect management decision-making and the risk of nuclear operations. It is felt that VSM offers the possibility of being able to better integrate management into the whole plant process to evaluate the safe operation of plants and this has been done here.

The industry has been aware of the importance of well run organizations on the safety and economics of power plant operations. Concepts such as organizational factors and safety culture have been discussed, but somehow it did not go beyond that. There did not appear to be an approach that is capable of tying the NPP organization (managers and personnel) to plant dynamics and control, plant disturbances and the effect outside agencies together, so one can get a better understanding of operational risks related to management (past and present) as well as the relative importance other actors in the safety process.

The dissertation addresses the above issues, makes a contribution to the understanding and use of the VSM methodology to the nuclear field and helps satisfy the need to have a more comprehensive process to study risk of nuclear plant operations, particularly associated with management decision-making. This latter process can be applied to HROs, by integrating the plant and its controls along with environment effects together with the organization's dynamic characteristics of control, decision-making and information flow.

The study of accidents draws attention to a key difference between management and operators in their dynamic performance and how this affects the whole response by the industry to accident management. This time dependent manifestation is deeply imbedded in how accidents should be addressed and is something of little interest to the normal commercial world of organizations. Beer's VSM addresses the world of management

control, operator actions and dynamic communications, but normal operations, so it is necessary to modify VSM to deal with the needs of the utility industry under the threat of accidents.

This means that one has to first determine what organizations require to be able to respond effectively to accidents, how the characteristics of persons occupying different positions within an organization can shape the responses to accidents and how those characteristics can be molded to match the needed requirements. Additionally, to minimize the risk of NPP operations, formalized risk assessments for both managers and operators can be proposed and used by organizations. This aspect should be included in the set of tools used within the VSM formulation identified for the NPP industry and for HROs in general. This is not say the risk techniques are not needed in the normal commercial, they should be. One can see the problems of not using these techniques appropriately in the banking and mortgage industries.

The above aspects have been studied within the dissertation and modifications to Beer's VSM have been identified along with the bases for understanding not only the difference between management and operators, but also the underlying dynamic difference between the two. Changes have been proposed to VSM to cover these aspects within the VSM structure. VSM clearly identifies the cognitive and manual portions of an organization, but these basic concepts need to be expanded to cover who can fill these roles and the corresponding educational requirements.

The basic VSM diagram is insufficient as it stands and more needs to be added to define who can fill a given slot, how they operate and how they are prepared and supported for those roles. The NRC and INPO have given much thought to the lower level personnel, but much more is needed for the upper management levels.

Guidance is given here with respect to the identification of the S, R and K characteristics of managers and operators (Rasmussen). These characteristic determine what is expected and how the roles of the persons should be considered, along with their support needs and training.

7.1 Summary of Research Studies

In order to understand how the VSM approach might help improve an understanding of the factors affecting the safety and economics of nuclear power production, a variety of research topics were studied:

1. Fundamentals of Nuclear Power Generation: A review of nuclear physics was carried out to understand the fundamentals underlying of nuclear power, this is covered in Chapter 2. The Chapter also discusses a number of the different Reactor Power Plant designs and their features. An important topic covered in this Chapter is the time scale of actions and interactions, from fast neutronic processes to the long term deliberations of governments. The time scale of things affects all aspects of nuclear operations from the interaction of neutrons to controlled changes in electric power to the impact of government decisions on cost of power and its safety.
2. Power Plant Operations and Safety Considerations: This Chapter deals primarily with the organization of the nuclear power industry within the United States and covers the organization of the Nuclear Reactor Commission, the Institute of Nuclear Plant Operations (INPO) and how they operate to help ensure plant safety. Also the chapter details how a typical Nuclear Utility is organized and the relationship of management to maintenance operations and control room operations including how accidents are dealt with.
3. Viable Systems Model and its basis: The fundamentals of VSM were researched including its relationship to control systems, cybernetics, and the brain and nervous systems of the body. This chapter is built upon the ideas that Beer had formulated of the relationship between the human body's cybernetic connections between the brain, nerves and hands and industrial and government organizations. The similarities between the body and companies are discussed and details of Beer's management structures are covered. The research investigated the application of VSM to a number of different types of organizations. A specific application was examined in detail. It is related to air traffic in Saudi Arabia air space (Al-Ghamdi, 2010). This application gives one a deep appreciation of how VSM can be applied to complex situations.
4. Case Histories of Accidents: Research into a number of different accidents was carried. This was done since it was felt that insights into the management operations for safety purposes can best be understood if one can see the context of management decision-making and resulting operational actions being played out. Since VSM is fundamentally dealing with management and personnel in controlling operations, it was considered that studying accidents should be a good way to understand the roles of all levels of management and operational personnel during the processes leading up to and including an accident. Ashby's Law has been seen to be important. Failure to be aware of requisite variety by the management has been revealed in the studies of accidents. The need for a technique to identify the parameters of the requisite variety has been identified as being an important step for

management awareness in controlling accident propagation. Post accident, it is clear what controls should be in place to terminate or mitigate an accident, but this is too late. The normal approach is to learn from the accident to deal with specific accident causes, but to proceed to deal with things from a generic point of view are missing, hence it is recommended that this approach should be examined.

5. Experiences in applying VSM to the Nuclear Utility Industry: This research is built upon the study of accidents mentioned earlier. The concept of integrating VSM representation of a NPP organization with NPP plant dynamics, control and protection systems, outside and internal plant disturbances, and regulatory and industry organizations was introduced here. This approach was taken to better represent the risk of NPP operations. A number of topics are covered here, such as impact of accidents in shaping industry organizations. The topic of distinguishing between failure processes associated with automatic systems and manual actions was covered earlier. Research was carried out to determine how management processes might be improved. Covered here is how managerial decision-making and PRAs could be used to improve this aspect of plant management. The chapter also covers the issue of the importance of the balance between economics and safety and how failure to pay attention can end up having safety consequences and lead to the demise of the corporation. It is also suggested that top management including Board of Trustees should be better trained and experienced in the tasks about which they are making decisions. Research was also carried out to see if there were indications within the NRC data base to determine who was more likely to cause accidents; front-line operators or top managers. This was in-line with the idea that human errors could be divided into two categories, random and systematic. A limited set of NRC ROP data was examined, but it appeared that there were more cases of systematic than random errors, but more needs to be done to support this conclusion. Definitely management has a bigger role in the error generation process than hitherto considered.
6. A key aspect of Beer's work that was arrived at late in the study was the importance of Ashby's Law of Requisite Variety. It appears that knowledge of this would have been a help to management in avoiding experiencing accidents. Unfortunately the state of knowledge is such that one needs to experience accidents in order to determine what are states that are not being understood in order to effect control over them. Some tools have been suggested such as PRA studies, to emphasize the risk aspect, but more is needed in terms of advice from knowledgeable persons. This it appears is not sufficient, since both the tools and advice has been available, but has not been availed of by managers. What is needed is a methodology to better

detect and make available to the decision-makers information about the requisite variety associated with given plant states and conditions.

7. The work of Rasmussen was reviewed to understand the implication of his Skill, Rule and Knowledge-based behavior models on utility responses to accidents. In particular, how the decision-making role of personnel characterizes whether a person falls into a specific behavior category, which in turn determines how they operate (time related) and their training and support requirements to achieve good performance.

7.2 Findings

1. Viable Systems Model has been shown to be a useful concept for studying organizational roles of top management, middle management and operating personnel when studying economics and safety of NPP operations. The VSM offers a dynamically based model that mirrors how management systems actually work, in contrast with the normal hierarchal presentation of organizations.
2. VSM of itself does not improve either the economics or safety of NPPs or HROs. The success of an organization still succeeds or fails based upon the knowledge and experience of the leadership of an organization. VSM cybernetic model could be a good tool for management to use and understand the roles of all in the organization, even the front line personnel operating the plant.
3. A study of SRK human behavior sheds light on how VSM' systems functions should be modified to take account of the time action limitations of managers and the need to reinforce operators actions by the use of better procedures and training. Also indicated is better technical training of managers for them to understand how better training in nuclear technology and risk assessment can prevent accidents and enhance utility survival.
4. A key finding derived from the study of accidents is that company exposure to increase economic and safety risk is related to the quality of the manager's decision-making capability. The industry and the regulators did not seem to be sufficiently concerned with this issue to set up training processes for managers. This failure should be compared with the exacting requirements for front-line operators, i.e. operators are licensed to operator NPPs. It could be that a formalized process to understand Ashby's Law and its implications for HRO operations could reduce the requirement for managerial excellence. It appears that very good managers are hard to come by.
5. Some management functions identified under manufacturing VSM structures as planning functions had to be re-interpreted, for Nuclear NPPs, as safety

assessments associated with risk assessment and regulatory interpretations rather than market evaluations. It was also determined the management needs to better understand the operating environment, this was a role identified as key element in cybernetics of operation of the plant

6. It was found that NPP organizations converted effectively to a lower order VSM model in response to accidents. Top managers' communications and control functions were replaced by more direct local management, often by lower level managers and supervisors. This is equivalent to the human body's response when faced with a high stress condition, when some systems are effective shutdown. The shorter links between information and decision cuts down on idle time, making for a more responsive response. It should be noted that effectively the Fukushima station crew was in effect trying to respond to Ashby's Law under difficult circumstances and they had neither the time nor experience to succeed in this.
7. Training of personnel was found to be very critical for NPP and other high risk operations than for normal manufacturing industries. The risk factor is inversely proportional to degree of preparation/training. Lower risk with better prepared staff, this is the message from the Three Mile Island accident! A branch function was added to the VSM structure. Training of operational staff became much clearer to the industry as a result of the Three Mile Accident (3/1979), also the relationship between manual control (operator actions) and dealing with decay heat.
8. The connections between VSM and the environment became identified as being of key importance in understanding the role of management and the influence of current and past management decisions on the safety of NPP operations, especially with respect to external and internal disturbances. The Tepco accident emphasized the need for top management to validate their decisions by consulting outside experts, who are knowledgeable about external disturbances (tsunamis).
9. It has been observed that NPP accidents in the US and other countries had a profound effect on NPP organizations and therefore the VSM structure and functions have changed over time in response to the effect of accidents. These changes reflect the way that normal human progress is made, rather than the earlier held belief that the nuclear energy business was different and could avoid the accident method of behavior modification, i.e. the nuclear industry could perform better than previous industries in avoiding significant accidents. Clearly, this was not the case.
10. Other methods have been proposed for the evaluation of plant safety, such as Hazop and Hazan, STAMP, FMEAs, and of course PRAs and these were reviewed. It appears that the combination of using the NPP Integral process with VSM, ESDs and

modified PRAs offers the best evaluation process at the moment and this is recommended as part of the decision process to be used by NPP management.

11. Dr Leveson has some great observations with regard to limitations associated with PRA, design limitations including software and HRA methods. A critique of her observations is covered in Chapter 6. Her comments should be borne in mind when applying PRA/HRA techniques.
12. Regulation does not prevent accidents. Regulators are like firemen, they can reduce the effects of a fire spreading. Also, it appears that their influence is effectively limited in their dealings with top management, because of their charter from the Congress (US).
13. INPO does do good work in counseling utilities, but the utility has to appreciate the need to be counseled in the first place.
14. The NRC and INPO can be seen to stabilize the industry by providing feedback derived from reviewers and analyzes of accidents, including accidents that affect plants in US and other countries.
15. A review of NRC accident reports was carried out. The reports indicate that some 20% of the operating plants had incidents during a year. Mostly these incidents were not serious, but did provide information on whether the incidents were caused by random or systematic effects. Reports led to knowledge of the causes, but not who was actually responsible. The ROP method has been reviewed and its data analysis could be improved to go beyond identifying the immediate causes of incidents.
16. The connection between safety and economics has been identified as critical in the operations of NPPs and that failure to do this can have severe consequences for the organization. Lack of some safety considerations can lead to highly costly economic effects. Even slight damage to the core can cause the utility to lose the use of the plant and this has an effect on the economy of the utility.
17. SCE case indicates that management decisions can lead to utilities being economically affected by equipment failure that have safety involvements. The NRC has prevented the restart of the units, because of SG tube rupture potential. Generalizing:- this type of economic issue, starting with poor analysis of equipment impact on economics as well as safety

7.3 Conclusions

This section deals with lessons learned from a review of the above findings. In addition to the findings on the research topic, were there other conclusions that might be drawn in the process of undertaking the investigation associated with the application of VSM to the study of nuclear power organizations?

The findings can be divided into two parts; one part deals with the lessons learned as a result of seeing how the VSM approach can be modified to better serve the requirements of the nuclear industry and the other part of the findings covers ideas identified during the research of improvements in the analysis processes used in the study of plant safety. The first part covers organizational and functional modifications of the VSM approach to identify those things that need to be addressed in the nuclear power generation world that set it apart from the normal commercial world of capitalism. The second part deals with an improved ways of identifying the importance of management decisions on safety of power plants and then integrating those into the safety assessment evaluation process. Management decision-making is pervasive and affects training operations, staffing levels, maintenance operations, risk assessment considerations, judgments of the importance of internal and external disturbances, and interactions with regulators and industry related organizations like INPO/WANO. A key item was determined during the course of the research, that an understanding of Ashby's Law of Requisite is the key to understanding how to combat accidents, since it means that we need to understand how the variety of a situation can change and what is needed to effect better control under these new conditions.

Through the research, the investigator came to understand the strengths and weaknesses of both the utility and other organizations, the roles they play and some of the constraints under which they labor. Ultimately, the utility management is responsibility for both the safety of the plant and the possible effects of accidents on their staff and the public. They are also responsible for the economic operation of the plant, producing satisfactory returns for investors, and not risking the enterprise by taking undue risks in trying to generate high short term profits or by ignoring accidents, which could be predicted and effects minimized.

CHAPTER 8 Contributions, Recommendations and Future Work

8.0 Introduction

This chapter brings together the main research contributions made to the field of understanding of the dynamics and control in the field of managing the safety and economics of nuclear power plant operations. The research started with an appreciation that managing risks in the nuclear power industry is needed and starts with the management structure and how it relates to the operating personnel, so that power plant operations are both safe and economic. It was suggested that Beer's work encompassing the Viable Systems Model as a cybernetic process was a good place to start. The VSM model was researched then evaluated and it was confirmed as a good place to start.

It was considered that safety is not an issue in a quiescent state and that problems with organizations are best studied when they are in a state of responding to an accident. Weaknesses within the organization are revealed by their failure to take appropriate action in a timely manner. Therefore, research was undertaken into the various accidents that have affected the nuclear industry and it was this research together with an understanding of VSM that led the inquiry. The structure of VSM with its emphasis on top management's role in the decision process made the division of labor quite clear. How decisions made by management affected the operation of the plants is examined.

Direct actions are not taken by management in response to accidents, but they do set-up the environment by their decisions and actions. Their operations staffs are those that take actions, which lead directly or indirectly to accidents. In fact, regulators and others do focus on the staff and their actions, rather than looking deeper at the underlying causes of accidents, often blaming the operational staff. It was not clear from accident reports of the key role that management decisions played in the accidents. In the case of TMI unit #2 accident is was not the case and the industry as a whole was considered complicit in the accident by virtue of not understanding the role of operators and the need for both training and good procedures.

This section identifies some of the contributions made during the research work.

8.1 Contributions

In researching the Beer VSM methodology and its possible application in improving the safety of nuclear power plant operations, a number of contributions have been made to VSM and adapting it specifically to the world of nuclear power. This section enumerates the contributions relative to VSM and other areas resulting from this research.

1. The first contribution is the extension of VSM to apply to the nuclear industry, as depicted in Figure 5-1. The extension started from the definition of what is called a more complex VSM model; see Figure 4-3, which was developed by Beer. The utility based version identifies the equivalence of Beer's systems (1 through 5) with the corresponding utility positions within their organization. So that the utility CEO is equivalent to S5. This development was generated from an understanding of both of VSM and the Nuclear Industry organizations, including the regulator (NRC) and industry sponsored group, Institute of Nuclear Operations (INPO). It should be pointed out that this version of the Utility VSM represents a late stage in the development of VSM models of a utility and reflects the effect of accidents on the modification of utility management scope of activities. There are at least a few structural changes that reflect the actual changes made by the industry.
   These are:
   a. INPO role (TMI accident)
   b. Emphasized Training (TMI accident)
   c. Addition of CNO (accumulative response to accidents)
   d. Enhanced Safety evaluations via PRA (maintenance operation induced incidents)
2. Another contribution is made for the development of the integrated representation of the VSM organization with an elaborated plant dynamic model including controls and disturbances and accounting for the activities of the NRC and INPO, see Figure 6-2. This representation is a cybernetic model of the whole interlinked organizations and systems that can affect the plant safety. This representation enables one to appreciate the central role of utility management in controlling risk and the influence of outside organizations in moderating risk.
3. The next contribution is the visualization of the effect of accidents upon the industry management in the form of a control system diagram, see figure 6-1. As accidents occur they do not tend to impact plants later in the same way as earlier, since hopefully the industry has learned from previous events and taken actions to prevent repetitions. The figure displays this process. The VSM organization associated with one state of the industry is depicted as VSM (t) and after the lessons are learned transforms to VSM (t +1). Of course, the changes maybe either major or minor in VSM. The changes post TMI were extensive, but even in cases where there was no major accidents, changes in the VSM organization might be advisable, see section 5.5-18.
4. Another contribution is related to the re-structuring of a normal operating VSM into one which represents how the organization functions, when dealing with an accident.

The top management is less involved in the minute to minute decisions. The local supervisors and their staffs are fully involved in trying to control the accident and mitigate its consequences. It should be pointed out is that the top management role is to take actions ahead of time to ensure that the accident response teams are prepared by having good procedures, are well trained and have tools and materials. Clearly a short-coming of the Tepco management was that they were not prepared for a large tsunami generated accident. They failed to build tsunami defenses and failed to prepare their staff for the events that followed, see case study 2, section 5.5-7. Maybe some of the effects of the accident could have been mitigated, for example the reactor cores could have been covered with water much more quickly.

5. A major contribution to understanding the limitations of both the management and operators to deal with accidents stemming from time and preparedness issues. This contribution came from an understanding of the impact of Rasmussen's SRK characterization on the response capabilities and requirements of the managers and the operators. Managers operate in knowledge-based mode and this limits their fast response capabilities. Operators operate in a rule-based mode and this enables them to act quickly but puts them into a need for good procedures and careful training.
6. Another contribution is to identify need for top management to use a decision-making process with regard to economic and safety decisions and this links with the knowledge-based behavior characteristic of management. Figure 6.7 depicts such a process. It should be pointed out that an accident, like Fukushima, affects both safety and economics. Some people think that it is either/or. Further, if the reactor is destroyed or damaged there are large costs incurred to clean-up the site. The costs associated with core melt may end up with causing the utility to be bankrupted. For Tepco to continue will depend on the Japanese Government to fund the company losses. Associated with this contribution is a suggested risk evaluation process, which should be considered by management. The process is depicted in Figure 6.8. The analysis process outlined depends on the use of PRA together with the use of Event Sequence Diagrams to review the accident domain and organizational responses.
7. Another contribution is the identification that the Board of Directors is a potent force to moderate the decisions of the CEO and CFO in the operation of the utility and to point out that they need to be educated in Nuclear Technology and Safety appreciation as it affects the viability of the utility.
8. A contribution was the identification that top managers and the Trustees should be that they are better prepared and checked for their positions by the NRC. It should

be demanded of them that they have a better educational background, directed nuclear experience and be exposure to critical decision-making. A model of this process that developed and used by Admiral Rickover. His personnel were prepared for the jobs that they were selected for and it was a progressive training process.

8.2 Recommendations for Future Work

It is recommended that the VSM approach be applied to other industries, such as the Oil Refinery and Chemical business. In fact the author did examine the Deep Well Horizon accident in the Gulf of Mexico and concluded that the VSM approach could be used and found that the decision-making process should be extended to include the US Government.

It is recommended that where decision-making processes are keys to the survival of the industry or the country, the VSM approach has a role to play. For example, Al-Ghamdi (2010) applied the concept to the air traffic controls in Saudi Arabia air space in a meaningful way.

The studies of accidents indicate that it should be possible to predict problems rather than for waiting for an accident to occur and then setting up rules to prevent future events. The issue appears to be that management is not capable of identify key variety changes within a system, that can occur as a result of a disturbance (plant accident initiating event). Changes in a system can lead to changes in the associated Requisite Variety; it is these changes that management needs to be aware of. Failure to understand the changes and act on the information can ensure damage to the plant. It is recommended that research into a better understanding of the Law of Requisite Variety under conditions of changing variety due to disturbances and the impact of other organizations, such as USNRC, should be undertaken. Turning the knowledge of Requisite Variety and the use of the knowledge into a set of rules and guidance for management to generate needed controls to prevent or mitigate accidents. This work could be of great use to the HRO industry.

The role of PRA in the management decision-making has been examined and it is recommended that it has a very useful role in management decision-making. It forces the management to use an explicit approach to decision-making by considering both qualitative and quantitative approaches to risk evaluation.

It is recommended that management play more attention to the use of scientific based information gained from their staff. VSM method does include feedback pathways from staff to top managers and vice versa. A weakness of the PRA method appears to rest on the fact that it is difficult to identify some equipment and human failure modes that might lead to

causing an accident or making an accident more severe. To discover these items requires very experienced personnel or as has been said above accidents can identify these items. It is always likely that these items will lurk in the sub-strata of an industry. It would be very useful to develop a method for locating these items before they cause an accident.

The NRC's ROP process has been reviewed and it appears to stop short of determining the source of decisions, which lead to accidents and incidents. Currently, the method indicates intermediate root causes, but the deeper root causes are not revealed. It is recommended that research into what can be done to improve the process be carried out. ROP reveals issues with procedures, combustible materials left in wrong locations, etc. What is needed is to have a more precise cause, was it due to poor training because of cuts in funding, etc. The resolution of this is issue maybe political or technical. If technical it would relatively easy to resolve. If political then this is likely to be difficult to resolve.

One should echo the statement made by Davis and Wolfram, (2011), that more work is needed to determine the effects of industry restructuring on the risk of nuclear accidents.

8.3 Publications related to this Research

Three papers have been produced relating to the research carried out on the topic of incorporating VSM concepts into the field of enhancement of nuclear power plant safety. These are:

Spurgin, A. J. and Stupples, D. W. (2012), *"Impact of Accidents on Organizational Aspects of Nuclear Utilities",* International Journal Engineering Management and Economics, Volume 2, Issue 4, November 2012

Spurgin, A. J. and Stupples, D. W. (2012), *"Nuclear Industry Organizations: Shaped by Accidents",* Published in Conference Proceedings of Probabilistic Safety and Management 11, (PSAM 11), June, Helsinki, Finland

Spurgin, A. J. and Stupples, D. W. (2011), *"Impact of Viable System Model (VSM) Type of Organizational Concept on Safety Regulations of the Nuclear Industry",* ANS PSA 2011, International Meeting on Probabilistic Safety Assessment and Analysis, March, Wilmington, NC (available on CD from American Nuclear Society, LaGrange Park, IL

References

Al-Ghamdi, S, H, 2010, 'Human Performance in Air Traffic Control Systems and its Impact on Safety', A PhD dissertation, City University, London.

Ashby, W. Ross 1973, *An Introduction to Cybernetics,* 3th Edition, **University Paperbacks, Methuen & Co Ltd, London**

Braun, Matthias, 2011, *Fukushima Daiichi Incident,* Fukushima Engineering Presentation, AREVA-NP, GmbH, www.matthias.braun@areva.com

Beer, S, 1979, *Heart of the Enterprise,* **John Wiley & Sons, Chichester.**

Beer, S, 1981, *Brain of the Firm, 2nd Edition,* **John Wiley & Sons, Chichester.**

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

Cooper, Dan, 1998, *Enrico Fermi: and the revolutions in modern physics,* **Oxford University Press, New York, NY**

CNN, 2011, *Expert: Japan Nuclear Plant Owner warned of Tsunami Threat,* **CNN Wire Staff, March 28th, 2011**

Cooper, S. E. et al., 1996, *A Technique for Human Error Analysis (ATHEANA),* **NUREG/CR-6350, U. S. Nuclear Regulatory Commission, Washington, DC**

Cronin, James (Ed.), 2004, *Fermi Remembered,* **University of Chicago Press, Chicago, IL,** *(Nina Byers: Fermi and Szilard)*

Davis, Lukas W and Wolfram, C, 2011, *Deregulation, Consolidation, and Efficiency: Evidence from U.S Nuclear Power,* EI @ Haas WP 217, **Energy Institute at HAAS,** UC Berkeley, CA

Dekker, Sidney, W, A, 2005, *Ten Questions about Human Error,* **Lawrence Erlbaum, Mahwah, NJ**

Discovery 2011, http://dsc.discovery.com/tv-shows/curiosity/topics/nervous-system-pictures.htm, Figure 4.5

DOE, 1993, *DOE Fundamentals Handbook, Nuclear Physics and Reactor Theory, Volume 2 of 2, DOE-HDBK-1019/2-93,* **US Department of Energy, Washington, D.C. 20585 (FSC-6910)**

DOE, 2009, *Yucca Mountain Repository, Safety Analysis Report, DOE/RW-0573-Rev 1,* **Department of Energy, Office of Civilian Radioactive Waste Management**, Las Vegas, NV

Fairwinds, 2013, *2.206 Presentation: San Onofre Units 2 and 3, Replacement Steam Generators*, Presented for Friends of Earth at a meeting requesting Enforcement Action against Southern California Edison under 10 CFR 2.206 (available on the Web).

FEPC, 2012, *Utility industry to establish independent nuclear safety organization,* The Denki Shimbun, (The Electric Daily News), 1/24/2012, Tokyo, Japan

Farmer, R 1977, *Today's Risks: thinking the unthinkable,* Nature 267, 92-93 (12 May 19977), **Nature Publishing Group,** London

Fleming, K, N et al 1975, *HTGR, Accident Investigations and Progression Analysis (AIPA), Status Report,* **General Atomics,** San Diego, CA

Frank, M, V 2008, *Choosing Safety: A guide to using risk assessment and decision analysis in complex high consequence systems,* **RFF Press,** Washington, DC

Glasstone, Samuel and Sesonske, Alexander, 1963, *Nuclear Reactor Engineering,* **Van Nostrand, Princeton, New Jersey,** (note: initial versions published in 1955)

Herring, C. and Kaplan, S 2001, *The Viable System Model for Software,* Report, Department of Computer Science and Electrical Engineering, University of Queensland, Brisbane.

IAEA, 1998, *Nuclear Power Plant Organization and Staffing for Improved Performance; Lessons Learned,* **IAEA-TECDOC-1052, International Atomic Energy Agency, Vienna, Austria**

INPO Web Site, www.INPO.info Institute of Nuclear Power Operations, Atlanta, Georgia, USA

INPO, 2011, *Special Report on the Nuclear Accident at the Fukushima Daiichi Nuclear Station***, INPO 11-005, Rev 0, Institute of Nuclear Power Operations, Atlanta, Georgia, USA**

Isaac, A., Shorrock, S. T., and Kirwan, B, 2002, *Human Error in European Air Traffic Management: HERA Project, Reliability and Safety, (75), pp257-272.*

Japan Fire Department, 2011, *FDMA Situation Report No 135, see earthquake web site, http://earthquake-report.com*

JNES, 2011, *Brochure on JNES Organization,* Issued by Japan Nuclear Energy Safety Organization (JNES), October 2011, www.jnes.go.jp

Joksimovich, V, 2011, *Management of the Fukushima Accident,* Presentation before San Diego IEEE Section, April 27th, 2011. *Slides available on www.SDIEEE.org***,** *date 5/1/2011.*

Kemeny, John, G 1979, *The Accident at Three Mile Island,* President's Commission on the Accident at Three Mile Island, United States Publishing, Washington, D.C.

Leveson, Nancy 2004, *A New Accident Model for Engineering Safer Systems*, Safety Systems, vol. 42, No 4, April 2004, pp. 237-270.

Leveson, Nancy, G 2011, *Engineering a Safer World*, *Systems thinking applied to Safety*, The MIT Press, Cambridge, Massachusetts & London, England

MacAvoy, Paul, W and Rosenthal, Jean, W 2005, *Corporate Profit and Nuclear Safety: Strategy at Northeast Utilities in 1990s,* Princeton University Press, Princeton, NJ

National Commission, 2011, *Deep Water: The Gulf Oil Disaster and Future of Offshore Drilling,* Report to the President, National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, U S Government Printing Office, Washington, DC.(available from Amazon, Barnes and Noble)

NEI, 2009, *Regulatory Assessment: Performance Indicator Guideline,* **NEI 99-02, Revision 6, Nuclear Energy Institute, Washington, DC**

New York Times, 2012, *Japan Ignored Nuclear Risks,* **February 15th, 2012, NYT, NY, USA** *(Comments made by Haruki Madarame, Chair of NSC (Japan)*

NRC, 2008, *Davis-Besse Reactor Pressure Vessel Head Degradation: Overview, Lessons Learned, and NRC Actions Based on Lessons Learned (NUREG/BR-0353, Revision 1),* **US Nuclear Regulatory Commission, Washington, DC**

NRC, 2012a, *Domestic Licensing of Production and Utilization Facilities, Code of Federal Regulations, Part 50, last reviewed January 12th, 2012,* ***US*** **Nuclear Regulatory Commission, Washington, DC**

NRC, 2012b, *Design Basis Accidents, General Design Criteria (GDC), 10 Code of Federal Regulations, Part 50, Appendix A, last review January 12th, 2012,* **US Nuclear Regulatory Commission, Washington, DC**

NRC Web Site, www.nrc.org, US Nuclear Regulatory Commission, Washington, DC

NRDC, 2011, *The BP Oil Disaster at One Year: A Straightforward Assessment of what we know, what we don't know and what questions need to be addressed,* National Resources Defense Council, NRDC Report, see www.nrdc.org/energy/bpoildistasteroneyear.asp

Perrin, Constance, 2005, *Shouldering Risks: The Culture of Control in the Nuclear Power Industry*, Princeton University Press, Princeton, Massachusetts

Pool, Robert, 1997, *Beyond Engineering: How Society Shapes Technology,* Oxford University Press, New York, Oxford

Rasmussen, Jens, 1983, *Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models*, IEEE Transaction on SYSTEMS, MAN, AND CYBERNETICS, Vol. SMC 13, #3, May 1983

Rickover, H, G, 1983, *An Assessment of the GPU Nuclear Corporation, Organization and Senior Management and Its Competence to Operate TMI-1,* Report by Admiral H. G. Rickover, USN, 19th November 1983 for GPUN

Rogers' 1986, *Report to the President by the President's Commission on the Space Shuttle Challenger Accident, June 6th,* US Stationary Department, Washington, DC

Rees, Joseph, V 1994, *Hostages of Each Other,* The University of Chicago Press, Chicago and London

Rogovin, George, T 1980, *THREE MILE ISLAND: VOLUME II, PARTS 1, 2, and 3. A REPORT TO THE COMMISSIONERS AND TO THE PUBLIC,* US Publishing, Washington, DC

Rogovin G, T, 1980, Nuclear Regulatory Commission, The Rogovin Report, Hearing before the Congress, Committee on Government Operations, Environment, Engineering, and Natural Resources, Sub-Committee, Feb 13, 1980, University of Michigan, Library (Jan 1st, 1980)

Shirouzu, N. and Smith, R. 2011, *Plant's Design, Safety Record are under Scrutiny,* **Wall Street Journal, March 16th**

Shorrock, S 2002, *Error Classification for Safety Management: Finding the Right Approach,* In C. W. Johnson (Ed) Investigation of Incidents and Accidents IRIA 2002, pp.357-67, HTTP://www.dca.gla.ac.uk/-johnson/IRIA_2002.pdf

Spurgin, A.J. and Carstairs, R.L, 1967, *Overall station control at Hunterston A,* Proceedings of the Institution of Electric Engineers, vol. 114, no.5, pp.671-678, May

Spurgin, A. et al, 1990, *Operator Reliability Experiments using Power Plant Simulators,* **NP-6973, Volumes 1,2 and 3, Electric Power Research Institute, Palo Alto, California**

Spurgin, A. J. 2009, *Human Reliability Assessment: Theory and Practice,* **CRC Press, Taylor and Francis Group, Baton Rouge, Florida**

Straeter, O 2000, *Evaluation of Human Reliability on the Basis of Operational Experience,* GRS-170 Report, **GRS** Kohl, Germany

Swain, A. D. and Guttman, H.E 1983, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications,* **NUREG/CR-1273, US Nuclear Regulatory Commission, Washington, DC**

TEPCO, 2011, *TEPCO Organizational Chart as of June 28, 2011,* see http://www.tepco.co.jp/en/corpinfo/overview/p-chart-e.html

Trucco. P, Leva. M, and Straeter. O, 2006, *Human Error Prediction in ATM via Cognitive Simulation: Preliminary Study, PSAM 8, New Orleans, Louisiana*

Walker, J 1991, *The Viable Systems Model: a Guide for Co-operatives and Federations,* Manual, Part of a Training Package for Strategic Management in Social Economy (SMSE) carried out by ICOM, CRU, CAG and Jon Walker.

WASH 1400, 1975, *Reactor Safety Study – An Assessment of Accident Risks in US Commercial Nuclear Power Plants,* **NUREG-75/014, US Nuclear Regulatory Commission, Washington, DC**

Wiener, Norbert, 1989, *Cybernetics: or Control and Communication in the Animal and the Machine,* **MIT Press, Cambridge, Massachusetts**

Williams, J, C., 1986, 'HEART –A Proposed Method for Assessing and Reducing Human Error', *Ninth Advances in Reliability Technology Symposium,* Birmingham, **IMechE, London**.

WHO, 2013, 'Health risk assessment from the nuclear accident after the 2011 Great East Japan Earthquake and Tsunami', World Health Organization, Geneva, Switzerland

Appendix A: Admiral Rickover's Management Principles

A.1 Introduction

This Appendix refers to the work of Admiral Rickover. The reason why the work of Rickover is discussed is because of his influence on the US Nuclear Industry, both by virtue of the personnel he (or his organization) trained that entered the nuclear utility business, but also because of the influence of his philosophy on the leadership of the Institute of Nuclear Power Operations (INPO), who had previously served as Admirals in the Nuclear Navy.

His contribution to the building of the Navy Nuclear Program is well known, but he also evolved a management process very specifically addressing the needs of a program that focused on safety issues related to operating nuclear power plants. In his case, the nuclear power plants were those needed to run submarines. Before the invention of nuclear power plants, submarines were really surface ships that occasionally submerged. After the use of nuclear power plants, submarines became real submarines that occasionally came to the surface. Their time under the sea was limited by provisions and the needs of the crews.

However, before submarines could operate this way, the safety of the power plants had to be assured and the crews protected from the possible effects of radioactivity. Rickover was very concerned with both of these items. He tackled these two issues in several ways, by attention to having reliable equipment, and by the selection and training of navy personnel. Many things that he did caused him not to be liked, but for a large time his success enabled him to proceed with his approach, for instance he gained the support of the US Senate who insisted that he be retained, when Navy wished to retire him.

One of the issues that are really important is the safe operation of nuclear reactors. His first insistence was that submarines not be sent out on duty until they were considered to be safe to operate. This often led to conflicts between him and the operational personnel of the Navy. The operational part of the Navy had their duty areas, places to set 'Boomers' and patrol zones for attack submarines. The conflicts mirror the dichotomy between economics and safety in the case of NPP operations.

The management methods of Rickover have lead to the safe operation of the Navy's submarines and are worth considering seeing if it is possible to draw on them to shape the civilian NPP programs. In some way, Rickover's training of Navy personnel has already had an influence on the utility NPP business in that many Navy personnel have joined the commercial NPP business and also INPO has been staffed by Rickover trained persons including a number of Admirals.

A.2 Rickover's principles

In the review of 'General Public Utilities Nuclear Corp organization and senior management and its competence (after the Three Mile Island 2nd unit accident in 3/1979) to operate TMI-1' by Rickover, see (Rickover, 1983), he states his principles of operation in the form of management objectives:

1. Require rising standards of adequacy
2. Be technically self-sufficient
3. Face facts
4. Respect even small amounts of radiation
5. Require relentless training
6. Require adherence to the concept of total responsibility
7. Develop the capacity to learn from experience

In his words, 'these principles express attitudes and beliefs. They acknowledge complex technology and that safe nuclear operation requires painstaking care'. He also points out senior management must technically informed and be personally familiar with conditions at the operating plants.

Of course, others may have different ideas and priorities for each of his objectives. Some things do stick out, like items 5, 6 and 7. Radiation control and understanding of the consequence of radiation exposure and release should be part of everyone's training if involved in NPP operation. INPO has adopted much of Rickover's philosophy, but this is not too surprising. Since many of the top personnel come from the Nuclear Navy.

A.3 Consideration of Rickover's Principles

One must recognize the value of Rickover's contributions. It is clear in an organization that not all of the personnel are equal in terms of their impact on the viability of the organization. The leaders in an organization provide the guidance and decision-making for the organization. They provide the direction for the whole, but there are others who provide guidance for others and information to the leaders on whole the operation is functioning. The leader cannot do everything and needs support at all levels within the organization.

Some of the key roles that Rickover played were those of selecting the officers and also ensuring the scope of training that the crews should undertake. He also maintained pressure on ship yards and suppliers by insisting on quality products. Rickover believed in

progressive training and with increasing responsibilities. The result of this process was to produce technically competent personnel capable of making good decisions and being responsible for their decisions. One advantage that Rickover had over say leaders in the utilities was the tightness of the Navy organization. The personnel signed as volunteers, and wanted a career in the Navy, particularly the Nuclear Navy. This is not to say that utility personnel are not dedicated, but that the organizations are much looser and opportunities exist elsewhere at different utilities/organizations. So the culture of the Nuclear Navy was and is different to that of civilian organizations.

In the matter of training, Rickover had a number of land sites in which operating reactors were used for training purposes. In this way Rickover gained a duplicate power module to that existed within a submarine. How more realistic can one get? At that time, he was not for mathematical simulators, which he believed were incapable of preparing his crew to the stresses induced when things went wrong. However, during his review of TMI unit#1, he must have realized that it was much more difficult to have duplicate NPPs for training purposes and also the quality of NPP simulators had improved to make them more acceptable for personnel training. The simulators are more realistic than in early days of nuclear power.

A.4 Conclusions

Looking at Nuclear Utility Operations, how should one interpret Rickover's principles? The first thing that comes to mind is Rickover's emphasis on safety and quality of equipment used. Clearly, these should be the same for NPP operations as for submarines. Failure of either personnel or equipment can lead to a 'lost' mission or the failure to supply power to the public, impact the environment along with the potential of large economic loss for the utility itself. The unsafe operation of a nuclear power plant in a submarine can lead to the loss of the crew, an environmental disaster dependent on where the accident occurs, and potentially the loss of a war, in the case of combat.

The unsafe operation of a NPP can lead to some deaths of personnel, loss of power generation capability, a huge economic cost for the utility, and a significant clean-up problem for society/utility along with possible radioactivity release depending on the subsequent actions of the utility and Government. One thing that is an advantage to prevent the spread of radioactive materials is the containment and its support systems!

In the case of the NPP utilities, their operations are monitored by the NRC and by INPO. For these two organizations, the processes and actions are quite different and these processes are discussed elsewhere in the thesis. The NRC's actions are regulatory and reactive. Those of INPO are proactive and can be somewhat limited depending on the response of the utility management. Responsibility for safe operations lies principally with the utility.

In the case of the Nuclear Navy, the captain of a submarine is the responsible officer at all times for the safe operation of the submarine. If anything happens, then he is empowered to act and if he fails so to do, then it is likely that he would have to leave the service. The responsibility of the CNO in the case of a utility is less well designated, so what is expected in the Nuclear Navy does not necessarily carry over to a utility. The NRC may find the utility at fault in an accident and not hold the CNO, President or CEO individually responsible, unless it can be proved that it was criminally inspired.

The case studies found that often decisions by CNO, Presidents and CEOs can provide the environment under which accidents can occur. One thing that is important is the education and training of personnel to perform tasks from simple to complex. The decision to reduce training and education to save money can lead to accidents or near accidents. There is a cost of doing business. Like the captain in the Navy, the CEO and CNOs have the responsibility to ensure the quality of the training programs. This also holds for the quality of materials and the maintenance operations. Also, the selection of personnel is important, since the utility needs good quality and trained personnel to perform exacting tasks. In fact, this might be more important in the diffused atmosphere of a NPP than in the close confines of a submarine.

One thing that has seemed to come to the surface over the last few years is the safety culture of an organization. It is supposed that the Nuclear Navy has a uniform safety culture by view of the training program and the fact that they are volunteers in the military. Schein in his lectures to INPO (Schein, 2003) refers to sub-cultures as being important, because of problems arising from: different views of one's job, how one is paid and what is expected. One would think that in the Nuclear Navy, there could be some cultural problems between Executives (Captains, and above.), officers and ratings. Interestingly, Rickover did not made any comments on this topic and it does not turn up to be an issue in his review of GPUN management of TMI Unit #1!

Although Admiral Rickover contributed much in terms of developing the US Nuclear Navy and the associated management organizational, which focused on safety and radiation

control, he was not without his critics. Among the charges, were his tight control led to a failure to develop other submarines, such as one like the Russian Alfa submarine that was faster and dived deeper than US designs. He was also charged with eliminating serious competitors, see comments by Schratz, 1983 during a review of a book by Polmar and Allen on "Rickover," 1982, Simon and Schuster. Rickover served for 63 years and was too long in the eyes of many, especially in the key position that he held!

One of the prime issues associated with management, is how does one remove top managers, when they are found not to advance the safety or competiveness of an organization? Eventually Rickover was removed or retired from active duty, but that was hard to accomplish. Utility organizations rely on the board of directors to ensure that Presidents and CEOs do function correctly relative to the health of the utility from a safety or economical standpoint. Sometimes, the Boards of Directors fail to perform as required, see, MacAvoy and Rosenthal, 2005, to protect the shareholders, employees and the public from the poor decisions of management.