A Review of the

Emergency Electric Power Supply Systems at PWR Nuclear Power Plants

by THOMAS PATON SMYTH

B.Sc (Electrical & Electronic Engineering) (Honours)

Submitted to the University of Cape Town
in partial fulfilment of the requirements for
the degree of Master of Science in Engineering.

September 1989.

I. Abstract

The Emergency Electric Power Supply Systems at Pressurized Water Reactor Nuclear Power Plants are reviewed, problem areas are identified, and recommendations are made for existing and future Nuclear Power Plants.

A simplified introduction to a typical Pressurized Water Nuclear Reactor is given and the problems associated with the commercial use of nuclear power are discussed. An overview of the Nuclear industry's solutions is presented and covers the Reliability of equipment and the American Regulatory requirements.

The alternating and direct current power supply systems are examined in terms of plant operational state and equipment type (Diesel generators, Grid network, Lead-acid batteries, Battery chargers, Inverters, and Power Distribution networks).

The trends in the design of Emergency Electric Power supply systems at Nuclear Power Plants are presented. The loss of all alternating current power, known as Station Blackout, is discussed and the American and European response to this problem is presented. Problems experienced in the direct current systems are discussed and solutions are presented. The experience at Koeberg Nuclear Power Station with Lead-acid batteries is included in the discussion.

The thesis concludes with recommendations for designers and operators of the Electric Power Supply Systems at Nuclear Power Stations.

II. Acknowledgements

The author wishes to thank C.Dingley of the University of Cape Town for his supervision of this thesis, and J.Combrink of ESKOM (Koeberg Nuclear Power Station) for producing a number of the diagrams.

III. Table of Contents

IV. List of Figures

1. Introduction

Nuclear Power Stations need heat removal systems that are very reliable. An excessive build-up of heat in the Reactor Core can eventually lead to a large release of radio-active material into the environment. The source of the heat is the radio-active decay of the Nuclear fuel. This is a significant portion of the energy output of a Nuclear Reactor. A Nuclear Power Plant without heat removal systems will experience Reactor Core damage within hours.

The electric power systems at Nuclear Power Plants are the main source of energy for the heat removal systems, and therefore need to be very reliable. Conventional coal-fired Power Stations also utilize Emergency power supplies to protect equipment, but these systems have an added importance at Nuclear Power Stations.

The principle function of the Emergency Power Supplies at a Nuclear Power Station is to provide power for the Engineered Safety Features. These are systems specifically designed to remove heat from the Reactor Core, and to minimize the impact to the environment of any Nuclear accident.

Typically, the principle sources of Emergency electric power are two Diesel Generators which can each deliver 5 Megawatts or more of electric power. Supplementary power for Control & Instrumentation systems is provided by Lead-acid batteries, in all some 400 kilowatts of direct current loads can be powered for one hour. The complexity of the electrical network can be gauged from the number of electric cables in a typical Nuclear Power Plant - there are over 40 000 cables with a total length of several hundred kilometers.

The Emergency Electric Power supply systems at a Nuclear Power Plants require a considerable amount of Engineering input and the equipment represents a significant part (R100 million+) of the overall plant cost .

1.1 Purpose

The purpose of this thesis is to review the Emergency Electric Power Supply systems at Pressurized Water Reactor Nuclear Power Plants, to identify problem areas, and to make recommendations for existing and future Nuclear Power Plants.

The author has limited the scope of the thesis to Pressurized Water Reactors[1] (PWR's) as the trend today appears to be toward the use of PWR's [1] and as the author's experience has been confined to PWR's. Nevertheless, much of this thesis is applicable to Boiling Water Reactor Plants as the Electric Power Supply systems are similar to those on Pressurized Water Reactor Plants.

1. The British have chosen a Pressurized Water Reactor of American design for their new Nuclear Power Stations even though Britain has developed its own Boiling Water Reactors.

1.2 Background

The author has been working in the Technical Support section at Koeberg Nuclear Power Station for the past three-and-a-half years. During that time he was trained in France by the French Contractor on the design and installation of the Electric power systems at Koeberg Nuclear Power Station. The emphasis was on the alternating current systems.

The author has had extensive contact with operating and design problems at Koeberg Nuclear Power Station. Solutions were developed which involved knowledge of the plant equipment, International and Local Specifications, and Nuclear Regulatory requirements.

A review of the literature showed that there were very few papers written about the electric systems on Nuclear Power Plants and all were on specific topics in the field. The need for a document which provided both the specialist engineer and the non-specialist manager with a complete, up-to-date information package was evident. This thesis therefore contains a comprehensive introduction to Nuclear Power Plant and the electric systems in particular, as well as the latest information on the design of the electric power systems in Europe and America.

The thesis is therefore useful as a training document for Engineers who wish to become familiar with Nuclear plant and the design of the electrical systems. At Koeberg Nuclear Power Station, the document will be used to introduce new staff in the Technical Support section to the electrical power systems of Nuclear Power Stations.

The author has been personally responsible for investigations and evaluations of the direct current power systems at Koeberg Nuclear Power Station, and has been used as a technical advisor in the 'Station Blackout'

investigations at Koeberg Nuclear Power Station. The author has utilized his experience at Koeberg Nuclear Power Station to identify problem areas and to formulate the recommendations for future power stations which are put forward in this thesis.

The thesis will therefore be of use to ESKOM's corporate Nuclear Groups who will be responsible for the purchase of the next Nuclear Power Station in South Africa.

The information base of this thesis consists of the author's experience at Koeberg Nuclear Power Station, a comprehensive literature search using the INSPEC index of abstracts going back to 1978, the documentation at Koeberg Nuclear Power Station, and informal contacts with experts both inside and out of ESKOM.

The research on which this thesis is based was carried out between July 1986 and July 1989.

1.3 Summary of Contents

A summary of each chapter is now given.

The thesis contains six chapters, the first being this introduction.

The second chapter provides the electrical engineer with a simplified introduction to a typical Pressurized Water Nuclear Reactor and covers the mechanical equipment used to generate electric power from Uranium fuel. Simplified flow diagrams and descriptions of the major systems in a typical Pressurized Water Reactor are given. The hazards associated with the use of Nuclear power for generating electricity are discussed and the Nuclear industry's solutions are presented.

The third chapter provides an overview of the special requirements for Nuclear Power Plants. The main topic of this chapter is the Reliability of equipment and systems. The American Nuclear Regulatory Commission requirements for commercial nuclear reactors are also presented.

The fourth chapter describes the electric power systems of a Nuclear plant in detail. The different operating modes of the plant are examined and the loads that need power are identified. The power system configuration required to power these loads is described, both the alternating current and direct current systems. The principle Emergency alternating current sources are the Standby Diesel Generator sets, while the main direct current Emergency power sources are Lead-acid Batteries. The Emergency Electric Power Distribution network is also discussed.

The fifth chapter identifies trends in the design of electric power systems in Nuclear Power Plants. The increasing use of Probabilistic Risk Assessment for justifying the use of Nuclear power is discussed. Current topics in Europe and America are the loss of all Alternating current , known as Station Blackout, and the reliability of the equipment used in the direct current power systems. In this thesis the Alternating Power trends are discussed by country, and the direct current power systems by equipment type.

The sixth chapter summarizes the problem areas, and presents a series of recommendations for present and future Nuclear Power Plants. A Nuclear Power Plant is a large capital investment and any improvement in the operation of the plant could result in big savings:- one way to effect improvements is by using the experience of other Nuclear Power Plant operators. This thesis therefore concludes with recommendations for existing power plants, and recommendations for plants that are about to be built.

The thesis is intended to be a complete document that can be used to inform non-specialist professionals and managers of the current issues in the design of the electric power systems at Nuclear Power Plants. These readers are invited to read the complete thesis.

Managers and professionals involved with Nuclear Power Plants should review Chapters 3 & 4, and concentrate on Chapters 5 & 6. The recommendations of Chapter 6 are addressed to managers and professionals who are responsible for operating existing plants, or who are responsible for developing new plants.

2. An Introduction to Nuclear Power Plant

A Nuclear Power Station produces electricity in the same way as a power station that uses coal:- that is, by consuming a fuel to heat water to steam, which drives a steam turbine and produces electric power via a generator. However, a Nuclear Power Station is more complex because the fuel used is Uranium, and the phenomena of Nuclear Fission is used to release the energy from the Uranium.

In this chapter, the Nuclear Fission process is described, and a simplified introduction to a Pressurized Water Reactor Nuclear Power Plant is given. The principle components of the Nuclear Reactor are presented, and the manner in which the Nuclear Fission process is controlled is discussed. The main Secondary systems, that is, the Steam Turbine and Electric Generator, are described briefly.

The equipment and systems provided to prevent the release of radio-active material to the environment are examined. These systems are collectively known as the Engineered Safety Features and are designed to cope with the worst postulated Nuclear accident.

2.1 The Nuclear Fission Process

Nuclear fission in Uranium occurs when a neutron collides with a nucleus of a Uranium atom and splits it into two segments called Fission Products. The result is the release of energy and two more neutrons. The process of Nuclear Fission can be made self-sustaining if one of the neutrons released causes another Uranium atom to undergo Nuclear Fission, and so on. The amount of energy released for a given mass of fuel is far greater in the Nuclear Fission process than that produced by burning an organic fuel in oxygen.

The Fission Products of the split Uranium atom are highly radio-active isotopes. A radio-active isotope has a 'half life', that is, the radioactivity diminishes exponentially at a rate that is unique to each isotope. The Fission Products of the Uranium fission process release significant amounts of energy for many years. This energy is in the form of gamma rays and various other particle emissions which are all dangerous to human life. This is therefore the prime reason why Nuclear Power Stations need such reliable equipment.

In commercial reactors of the type used at Koeberg Nuclear Power Station, the thermal power output of the reactor drops to some 6% of the full load power immediately after the reactor fission process is shut down [2]. This thermal power comes from the radio-active decay energy of the Fission Products in the reactor core. The energy released reduces as the Fission Products decay, but it takes years before the thermal power drops to a safe level:- after one month the decay energy is still 0.1% of the full load power.

It is therefore essential that heat removal systems are available to transport the heat away from the fuel elements. If the Fission Product decay heat is not removed, then the fuel elements will overheat and the reactor will be damaged. Then there is also the possibility that the radio-active Fission Products could be released to the environment with disastrous results.

As an example of the hazards posed by the release of radio-active Fission Products from a Nuclear Power Plant, at Chernobyl [3], some 2.5% of the core material was released to the countryside. Fortunately the initial large release missed the nearby town of Pripyat but the

---

2. Westinghouse Training manual "PLANT SYSTEMS ENGINEER", prepared for ESKOM, 1985, Chap.RT-3, page 39.

3. "CHERNOBYL: THE SOVIET REPORT," Nuclear News, October 1986, pages 59 to 66.

surrounding forests were heavily contaminated. Now, even after massive clean-up efforts, all the land up to 30km away from the site remains uninhabitable, and over the next 70 years the Soviets estimate that 2% more people will die from cancer:- that is about 300 people more than the estimated 14 000 that will develop cancer spontaneously. Two hundred and three people involved in the accident were hospitalized with acute radiation sickness and will either die or partially recover.

Thus, we can see why there is so much more risk associated with using Nuclear power:- in a coal fired boiler, the flames are extinguished immediately when the coal and air are shut off from the furnace and no more energy is produced. But the decay heat in a Nuclear plant must be removed even after the Fission process has been stopped. The need for highly reliable heat transport systems at Nuclear Power Plants is obvious and the backbone of any heat transport system is electricity:- that is, power to drive pumps, open valves, and operate equipment that monitors and controls the reactor.

However, before we can discuss the electric power requirements of a Nuclear Power Station, we must first understand how it operates and what it consists of.

2.2 The Nuclear Reactor.

The heart of a commercial Pressurized Water Nuclear Reactor is the Primary Coolant Loop. Figure 2.1 shows a simplified diagram of the Primary Coolant Loop:- the reactor vessel contains sealed fuel rods with Uranium dioxide ceramic pellets inside. A reactor coolant pump forces Primary Coolant water past the fuel rods and the water is heated by the energy released by the Fission process taking place in the fuel rods. The heated water

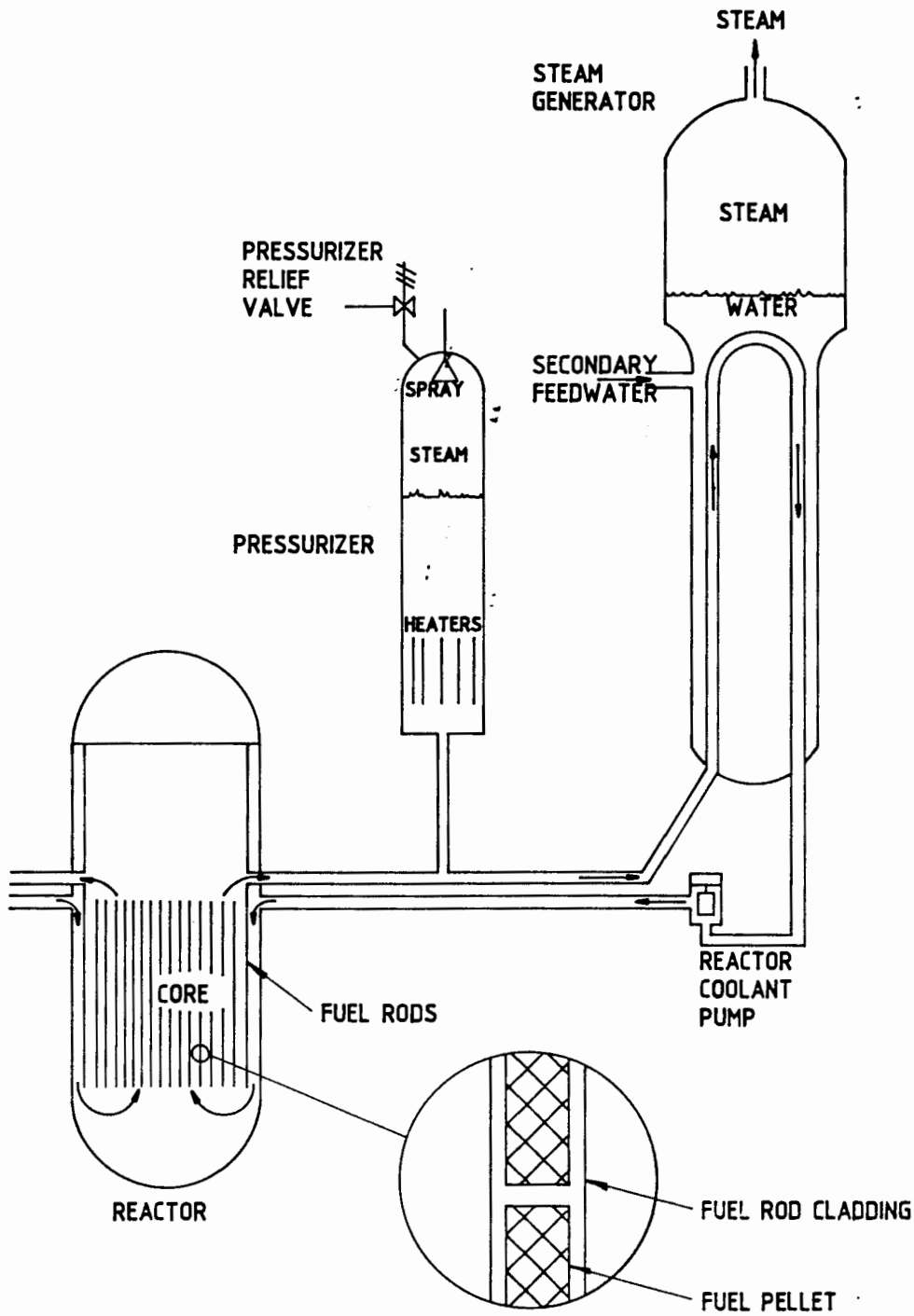


Figure 2.1 "Pressurized Water Reactor Primary Coolant Loop"

then passes through a large heat exchanger known as a Steam generator.

There is no steam produced by the fuel rods and the energy is transferred from the reactor by water that is highly pressurized to keep it from boiling - hence the name of the Pressurized Water Reactor. Thus the Primary Coolant water absorbs energy from the fuel rods in the reactor and heats up. In the Steam Generators, the Primary Coolant transfers the energy to the Secondary Feedwater and the Primary Coolant water therefore cools down again.

The device used to keep the water so highly pressurized (at about 150 Bar) is called the Pressurizer. It works by using the natural phenomenon that if steam is pressurized enough, it will turn to water - with a corresponding drop in volume. So the Pressurizer has Electric heaters which boil the water in it to form a steam bubble. The steam bubble is the feature that controls the Primary System pressure and it works as follows:- should the Primary System volume increase, then some of the steam condenses to water and reduces the volume of the Steam Bubble. The over-all system pressure is therefore maintained because steam volume change compensates for the increase in water volume. And conversely, should the Primary volume decrease, then some of the Pressurizer water vaporizes to steam with an increase in volume, and the system pressure is maintained. This mechanism cannot cope with extreme changes in pressure, so the mean system pressure is controlled by using heaters and cooling spray water to expand and reduce the Steam Bubble in the Pressurizer.

The final control of the Primary Coolant system is the Pressurizer Relief Valves:- these are simply safety valves that vent the Primary Coolant water to prevent the Primary Coolant pressure from exceeding the system design limits.

The Secondary feedwater comes from the Turbine Steam Condenser and is pumped into the Secondary side of the steam generators using Feedwater pumps. The resulting steam is used to drive the Steam Turbine which rotates the Electric Generator. The steam leaving the Turbine is condensed to water in the Turbine Steam Condenser and the Feedwater cycle continues as described previously.

An interesting point is that the Steam Turbine could drive a Ship's propeller and it is, in fact, for this reason that the historical forerunner of the commercial Pressurized Water Reactor was developed:- a Pressurized Water Reactor plant can be made very compact for use in ships and submarines.

An important feature is that the Primary Coolant water is physically separated from the Secondary Feedwater in the Steam Generators:- therefore, any radio-active Fission Products leaking from a damaged fuel rod will be contained in the Primary System.

2.3 Controlling the Nuclear Fission Process

It is important that the Nuclear Fission process is maintained and controlled. As we saw earlier, each Fission event results in the release of Fission Products, two neutrons and energy. In order for further Nuclear fission reactions to occur, other Uranium atoms must be sufficiently close by. In fact, for every combination of Uranium fuel elements and heat transfer medium, there is a Critical Mass, that is, there has to be a certain density of Uranium atoms in an area before the Fission process is self-sustaining.

A typical Pressurized Water Reactor has fuel rods spaced roughly 1.5 cm apart and uses Borated water as a heat transfer medium. The Boron atoms in the water are used to

absorb neutrons and by varying this concentration, we can regulate the number of neutrons (produced by Fission reactions) that go on to cause further reactions. Thus by controlling the number of neutrons moving about in the reactor, we can control the Nuclear fission process.

2.3.1 The Chemical & Volumetric Control System

One of the major plant systems for controlling the neutron density in the reactor is the Reactor Chemical and Volumetric Control system:- a schematic of this system is shown in Figure 2.2. The one function is to regulate to Boron concentration in the Primary Coolant System. This is achieved by continuously drawing off water from the Primary Coolant system and either diluting it with water, or adding Boron to it before pumping it back into the Primary Coolant System. The overall system Boron concentration can therefore be varied albeit at a relatively slow rate.

The other function of the Reactor Chemical and Volumetric Control system is to regulate the volume of Reactor Coolant in the Primary Coolant system. As the Primary Coolant water heats up to the operating temperature (about 320 deg.C) it expands:- the Reactor Chemical and Volumetric Control system maintains the Primary Coolant volume by drawing water out of the Primary system while keeping the water level in the Pressurizer constant.

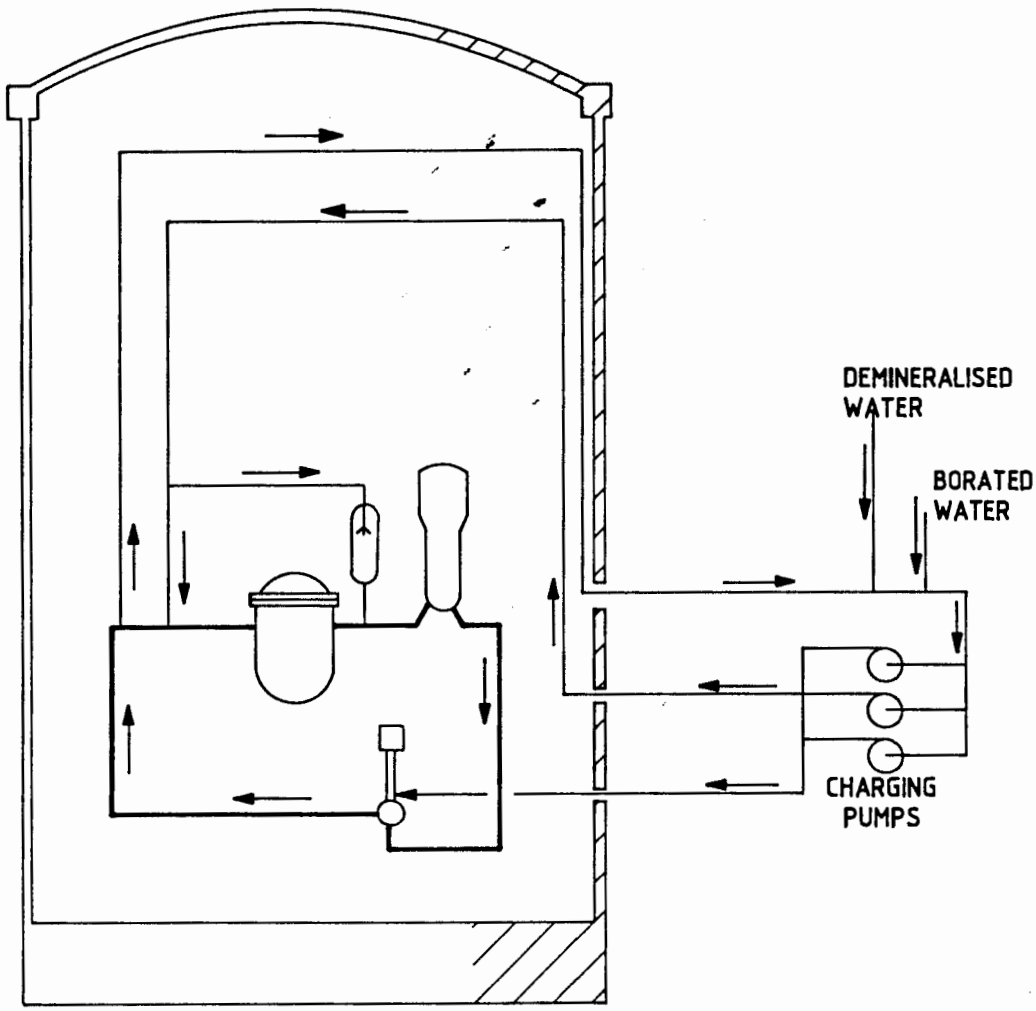


Figure 2.2 "The Chemical & Volumetric Control System"

2.3.2 The Control Rods

The control afforded by the Chemical and Volume Control system is not able to cope with rapid changes in the Nuclear fission process. Therefore, a number of Control Rods are provided to control the Reactor during any rapid transients that may occur. These are metal rods containing atoms such as Silver and Indium, that are very good neutron absorbers. The rods move into the reactor from above in special channels and have complex driving mechanisms that can position groups of rods at any distance into the reactor. The rods can be moved rapidly and provide "fine control" of the Reactor, the "rough control" being the Boron concentration in the Primary coolant.

The Control Rod Drive Mechanisms drop the rods immediately on loss of power to the Rod Control system and the effect of all the Control Rods dropping into the reactor at once is to immediately stop all Nuclear fissions. Historically, this is known as a SCRAM from the words "Safety Control Axe Man":- in the early days of Nuclear research the Control rods were held out of the reactor by a rope over a pulley and the only safety system was a man with an axe who would chop through the rope if anything went wrong! Today the SCRAM function is fully automated and designed to be highly reliable.

2.3.3 The Residual Heat Removal System

The Reactor Chemical and Volumetric Control system and the Control Rods are used to control the reactor during power operation and the energy produced in the reactor core is transferred to the Steam Generators and eventually leaves the plant as electric energy. However, when the Reactor and Generator are shut down, the decay heat is removed by the Residual Heat Removal System

The Residual Heat Removal System is shown schematically in Figure 2.3 and consists of two pumps which circulate the Primary Coolant through two heat exchangers. The heat exchangers are cooled by a closed loop cooling system - the Component Cooling System - which transfers the heat to the Ultimate Heatsink (often the sea). The principle of using multiple barriers against radio-active material release is used here as well - the Primary coolant could possibly leak into the Component Cooling System, but it would be detected here long before it could escape to the environment.

The above systems are essentially all that is needed to control the Reactor during Normal operation. We shall see later that further special systems are provided to cope with any accidents that may occur. Having explored the Primary Coolant system, we shall now go on to discuss the Steam Turbine and the Generator:- the Secondary systems.

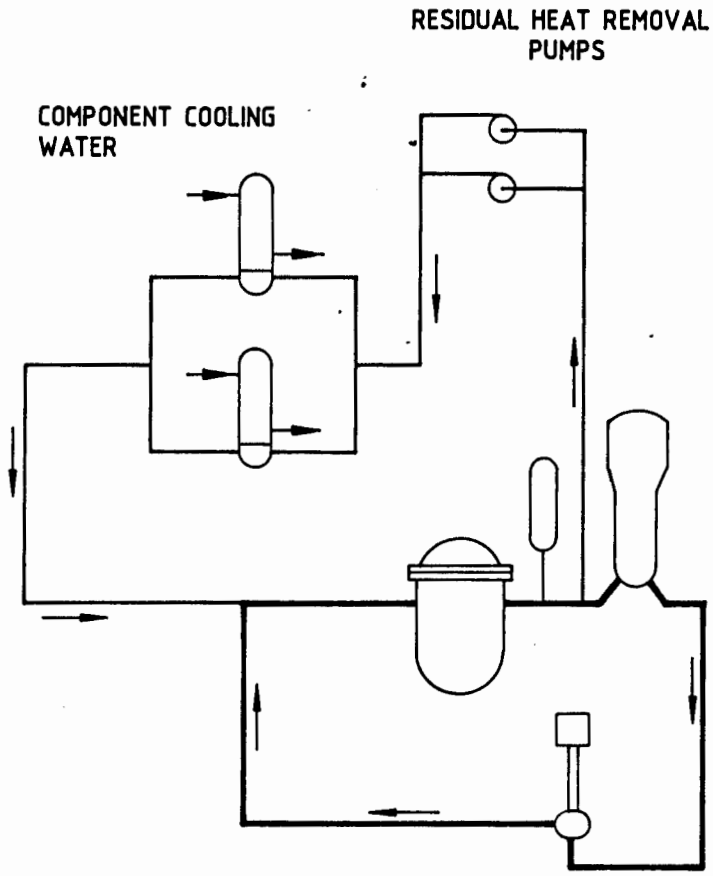


Figure 2.3 "The Residual Heat Removal System"

2.4 The Steam Turbine

The Steam Turbine is driven by the steam produced in the Steam Generator and provides the mechanical power to drive the Generator. Figure 2.4 shows a typical Westinghouse Steam Turbine layout. The Steam Turbine is divided into various stages to make the best use of the steam's energy. A High Pressure stage is optimized for the steam produced by the Steam Generators and the Low Pressure stage is optimized for the steam that exits from the High Pressure stage. The Low Pressure stage typically consists of two or three Low Pressure steam turbines in parallel.

In plants of Westinghouse design, the steam that exits from the High Pressure stage is reheated in Moisture Separator Reheaters before being passed through the Low Pressure stage. The heating medium for the Moisture Separator Reheaters is steam tapped of just before the High Pressure stage.

The steam that exits from the Low Pressure stage is condensed to water in a large heat exchanger known as a Condenser. The Condenser is cooled by water pumped from the Ultimate heatsink by the Circulating Water system.

Water must be pumped into the Steam Generators to replace that which is boiled off as steam. The Steam Turbine flow cycles are indicated in Figure 2.4:- Water, known as Condensate, is pumped by Condensate pumps from the bottom of the Condenser and passes through a couple of Low Pressure Heaters which heat the Condensate. Feedwater pumps then transform the low pressure Condensate into Feedwater which has sufficient pressure to overcome the Pressure inside the Steam Generators. The Feedwater is heated by High Pressure Feedwater heaters before it enters the Steam Generators.

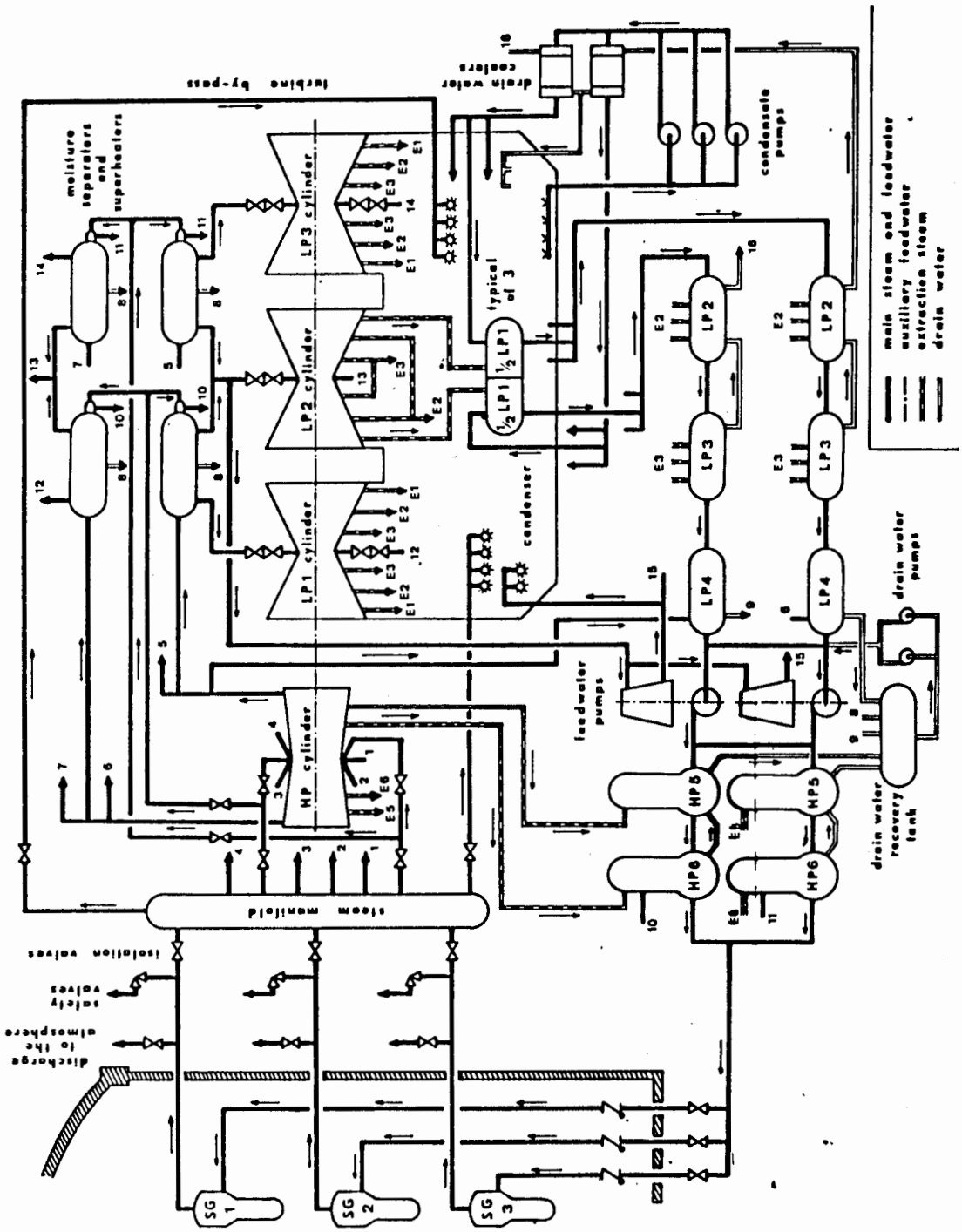


Figure 2.4 "Steam Turbine Flow Diagram"

The purpose of the Low and High Pressure heaters is to improve the overall thermodynamic efficiency of the Secondary cycle. They are simply heat exchangers which use steam bled from various stages of the steam turbine to heat the Feedwater. The steam condensed in the Feedwater heaters is recycled back into the Feedwater cycle, either back into the Condenser, or is injected into the Condensate circuit by large pumps.

2.5 The Generator

The Generator transforms the mechanical power produced by the Steam Turbine into electric power. This power flows into the Grid network and is thus transported to the end users of the electric power.

The Generator can be connected to the Grid network in a number of ways. One method is shown in Figure 2.5:- the generator output passes through a Generator Circuit Breaker, the Generator Transformer, and then out to the network through a High Voltage Circuit Breaker. The Unit auxiliaries, that is, all the motors and other electric loads in the power station, are supplied through a Unit Transformer.

Another method is similar but uses a motorized isolator in the place of the Generator Circuit Breaker. This is a cheaper alternative, but has one disadvantage:- if the Generator must be shutdown due to plant problem, the High Voltage breaker must be opened and so the supply to the Unit auxiliaries is lost. Thus, the advantage of the Generator Circuit Breaker over the motorized isolator, is that the Unit Auxiliaries are secure even when the Generator is shut down.

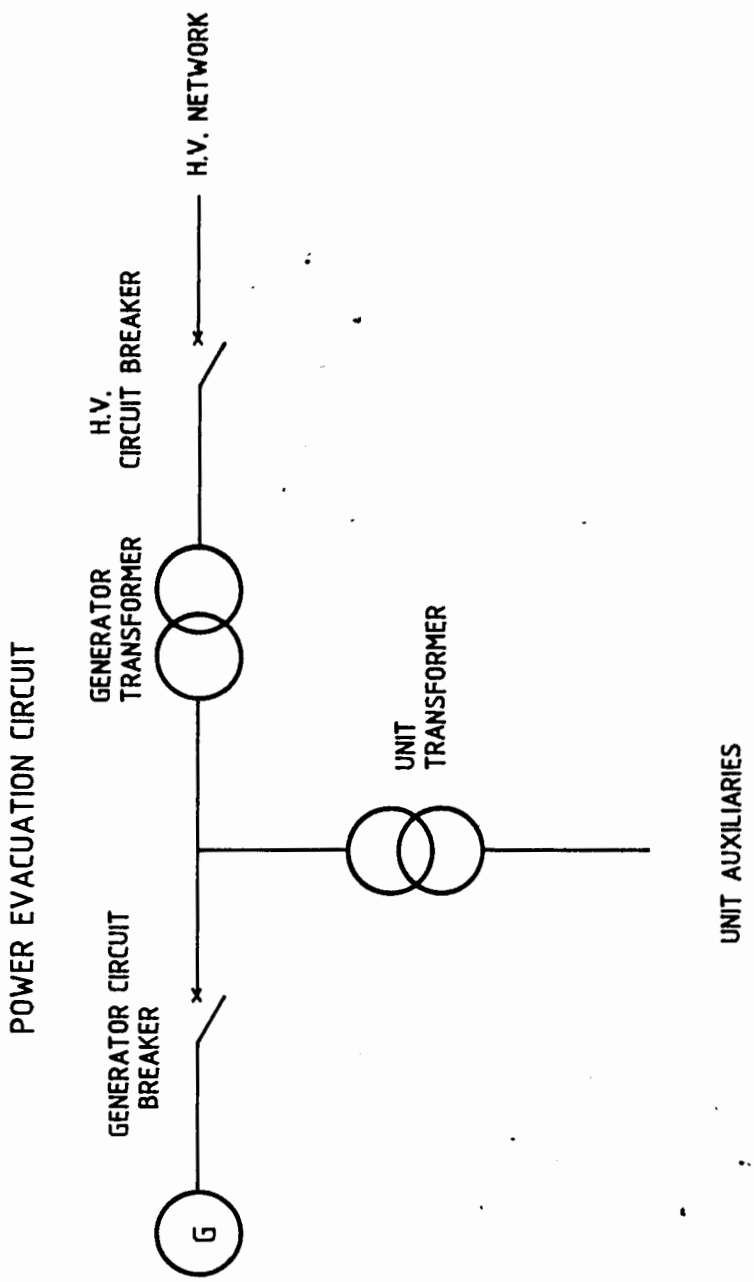


Figure 2.5 "Generator connection using Circuit Breaker"

Both these schemes have an advantage over the Scheme shown in Figure 2.6:- here the Unit Auxiliaries are supplied directly from the High Voltage network. The Unit Auxiliaries therefore remain secure in the event of a Generator shutdown, even if the High Voltage breaker has to be opened. However, the possibility of "House Loading" is lost.

The expression "House Loading" is used to describe the supply of the Unit Auxiliaries by the Generator in the event of a loss of High Voltage power. Referring to Figure 2.5, say a Grid fault causes the High Voltage breaker to open. Now, if the Generator and Reactor survive the transient without the automatic protection systems shutting them down, then the Unit Auxiliaries will be supplied by the Generator via the Unit Auxiliary Transformer.

The opening of the High Voltage breaker while at 100% power is quite a severe transient on the power plant and it is difficult to retain control of the plant without exceeding plant safety limits. Once these limits are exceeded, the Reactor and Generator are immediately and automatically shutdown. A typical probability for house loading is 3 successful transfers out of 10 attempts.

The Turbine and Generator have forced oil lubrication on all bearings. The oil is pumped into the bearings by an oil pump driven from the Turbine shaft, or by electric oil pumps. One of the electric oil pumps is powered by a dc motor which has a battery backed supply to provide lubrication in the event of an ac power failure.

A motor is provided to slowly rotate the Turbine shaft when the steam is shut off and the turbine is still hot:- if the shaft is not kept turning, then it will not cool evenly and will bow. The uneven cooling is caused by the large cool condenser space below the turbine shaft.

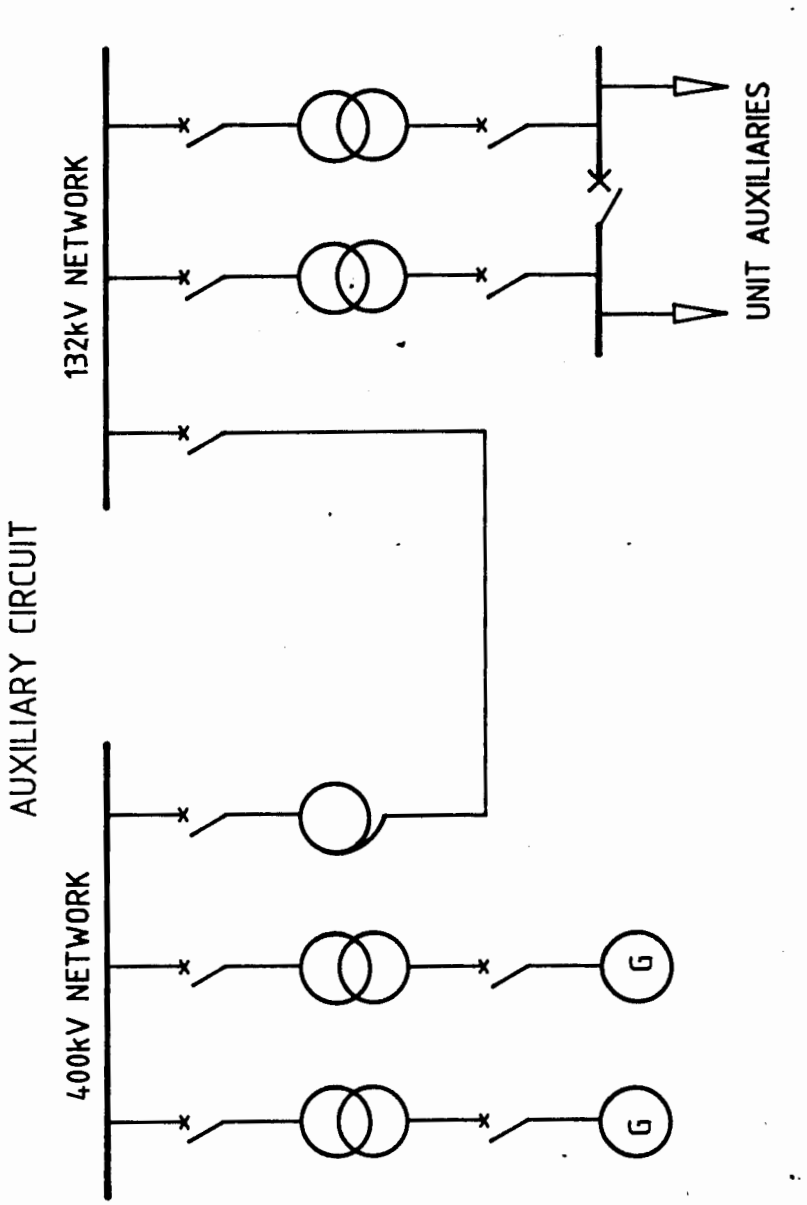


Figure 2.6 "Unit Auxiliaries - Direct supply from Network"

2.6 The Engineered Safety Features

All the systems described previously are the main systems necessary for normal operation of a Nuclear Power Station. There are however, other important systems known as the Engineered Safety Features which have been specifically designed to prevent the release of radio-active material into the environment, even if a Nuclear accident should occur.

2.6.1 Postulated Accidents

The Engineered Safety Features are designed to cope with all probable accidents:- the two worst failures are-

1. The complete shearing of the largest pipe in the Primary Coolant system, and

2. The complete shearing of the main steam pipe from the Steam Generator.

These accidents are known as the Design Base Accidents (DBA). The consequences of both accidents is that all the water in the ruptured system flashes over to steam. The loss of water in the Primary Coolant system results in the Reactor core being uncovered and the decay energy therefore causes temperature of the fuel rods to rise. If no cooling water is provided, the fuel rod cladding will eventually melt and allow the release of the radio-active Fission Products.

The consequences of the Main Steam Line Break are that the Reactor undergoes a severe thermodynamic transient which may cause the Nuclear fission process to go out of control.

2.6.2 Multiple Fission Product Barriers

We have already discussed elements of the first Engineered Safety Feature:- the use of multiple Fission Product Barriers. The fuel rods contain a large amount of radio activity and some of it is in the form of radio-active gases such as Xenon, Krypton and Iodine which result from the various Nuclear reactions in the fuel rod. The fuel rods are sealed to prevent the release of the Fission Products and are therefore the First Fission Product Barrier. However, if the fuel rods get damaged then some of the Fission Products will escape. The Primary Coolant system boundary is the Second Fission Product Barrier and will contain any Fission Products released from the fuel rods. Should the Primary Coolant system rupture, the Fission Products will be contained by the last Fission Product Barrier - the Reactor Containment building.

It is interesting to note that at Chernobyl there was no Containment Isolation building and the large releases of radio-active material may have been reduced if one had been built. But the reactor type used at Chernobyl is of the Boiling Water Type and is much larger than the Pressurized Water type, so the cost of any containment building is significant. Even after Chernobyl, the Soviets maintain that there is no practical possibility of providing a Containment building of the Pressurized Water type at their Boiling Water reactors [4].

Thus three Fission Product Barriers exist on Pressurized Water Reactors. Commercial Nuclear Power Stations have Engineered Safety Feature systems installed that are specifically designed to maintain the Fission Product Barrier integrity under all postulated accident conditions. These are:-

---

4. "CHERNOBYL: THE SOVIET REPORT," Nuclear News, October 1986, pages 59 to 66.

2.6.3 The Containment Isolation System

The Containment Isolation System consists of special valves in all pipes and ducts that penetrate the Containment Building. All these valves can be closed remotely, and when they are all closed, the design leak-rate of the Containment building (at 5 Bar air pressure and over 24 hours) is 0.3 percent of the air mass inside the building [5]. The Containment Building integrity is tested every 10 years to check it's ability to withstand a Design Base Accident.

The worst Design Base Accident for the Containment building is the Main Steam Line Break:- the pressure inside the Containment reaches a peak of 3.8 Bar.

2.6.4 Containment Building Heat Removal Systems

Two systems are installed to remove post-accident heat from the Containment building. These systems also remove Fission Products from the Containment atmosphere.

After a Design Base Accident the steam released causes the temperature and pressure inside the Containment building to rise. The energy in the steam is removed by the Containment Building Heat Removal systems and this limits the temperature to a maximum of about 170 deg.C and the pressure to 3.8 Bar. If the Containment atmosphere is not cooled, then the steam pressure will build up and eventually rupture the Containment building. The first Containment Building Heat Removal system is the Containment Spray System.

---

5. Electricite de France. "EDF 900 MWe NUCLEAR POWER PLANTS, SHORT TECHNICAL DESCRIPTION." issued by Service d'Equipment Nucleaire Exterieur, 11-13 Avenue de Friedland, 75008 PARIS, May 1983.

2.6.4.1 The Containment Spray System.

A schematic of the Containment Spray System is shown in Figure 2.7. The containment atmosphere is cooled by water sprayers. The water is pumped from a large tank of Borated water known as the Refueling Water Storage Tank. The water and condensed steam is collected in sumps at the bottom of the Containment building and is re-cycled when the Refueling Water Storage Tank runs dry. Heat exchangers cool the hot water from the sumps before it is re-sprayed.

Radio-active iodine is released into the Containment atmosphere when the fuel rods are ruptured as Iodine is one of Uranium's Fission Products. If human beings are exposed to Iodine, the substance concentrates in the Thyroid Gland, and as the Iodine is radio-active, the person is irradiated from a source within the body. This is the reason that Potassium Iodide tablets are given out to the public near some Nuclear Reactors:- in the event of a release of radio-active Iodine, the public take these tablets which saturate their Thyroid Glands with Iodine, and the radio-active Iodine is not taken up. The Soviets used a youth organization to effect widespread distribution and use of Potassium Iodide tablets after the Chernobyl accident. This was the first large-scale test of this technique and the results show that it is effective:- there were no side-effects and tests of the population show radio-Iodine levels in the thyroid that were significantly below the health limit [6].

---

6. "CHERNOBYL: THE SOVIET REPORT," Nuclear News, October 1986, pages 59 to 66.

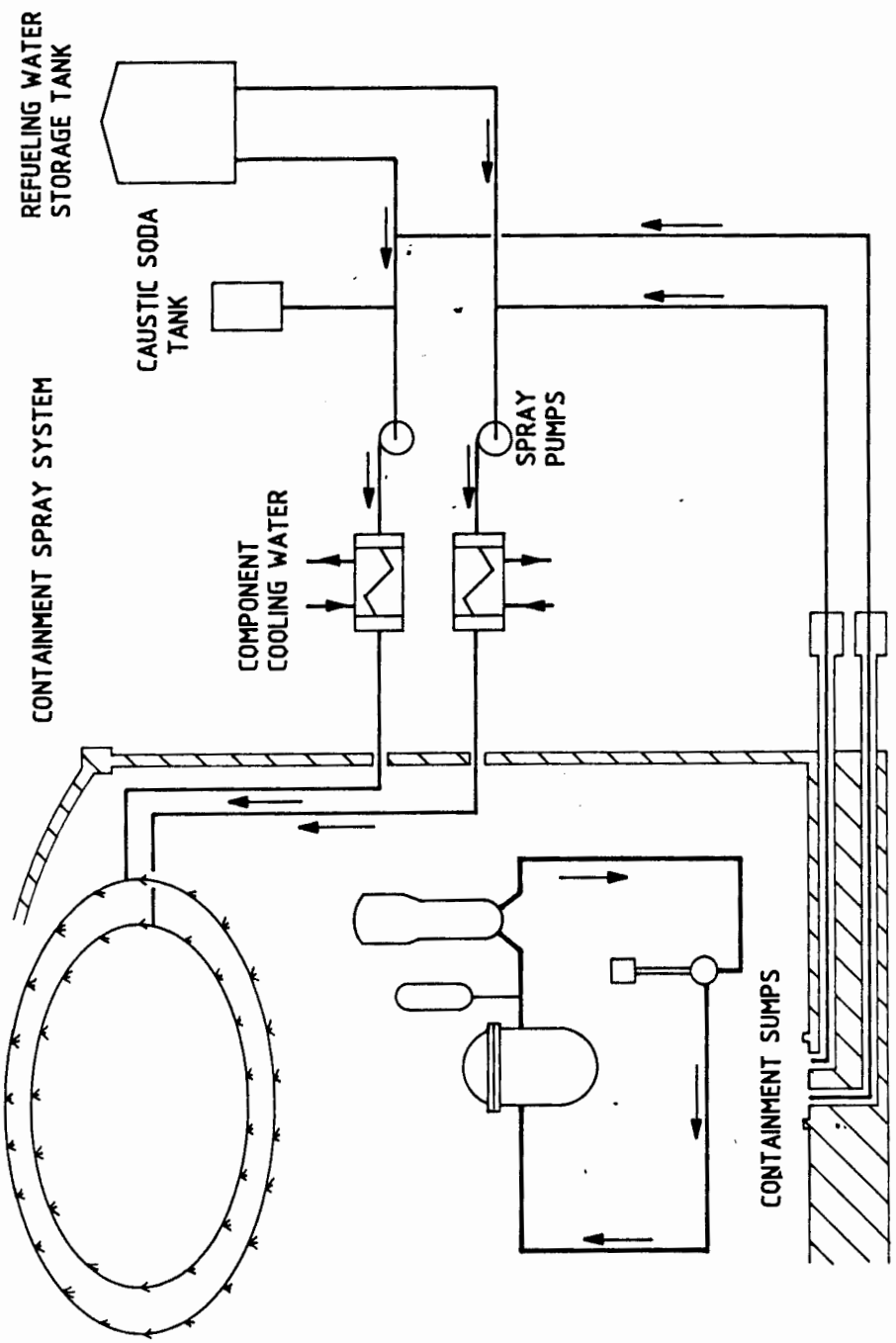


Figure 2.7 "The Containment Spray System

Interestingly, there is not as much concern about radio-active Xenon and Krypton (which are also released in a DBA) as these are both inert gasses and do not chemically react in the human body. They are therefore breathed in and exhaled, irradiating the body only when in the lungs. However, Iodine remains in the body and is a serious health threat. As a reference, at Chernobyl, the release of Xenon had six times more radio-activity than the Iodine release [7], but the Iodine release was the important one as far as the population health is concerned.

To control the release of Iodine, Sodium Hydroxide is added to the Containment Spray Water to react with the Iodine in the Containment atmosphere. Without the Sodium Hydroxide, the Iodine remains in the Atmosphere even though water is sprayed. However, with Sodium Hydroxide in the water, a reaction occurs with the Iodine and the result is NaOI, which is soluble in Water. Iodine is therefore not released should the Containment rupture as much of it is dissolved in the Containment Spray Water.

Thus the Containment Spray system not only removes energy from the Containment Atmosphere, but it also controls the amount of Iodine in the Containment Atmosphere.

2.6.4.2 The Containment Air Purification System.

The second system provided to remove heat from the Containment atmosphere is the Containment Air Purification System. It consists of four cooling units:- during normal plant operation, containment air is circulated through heat exchangers in the cooling units to keep the air cool. However, in accident conditions, a high efficiency particulate air filter is brought into the air circulation path and is used to extract radio-active Fission Products

7. "CHERNOBYL: THE SOVIET REPORT," Nuclear News, October 1986, pages 59 to 66.

from the Containment atmosphere. Again the Containment Air Purification System has the dual function of removing energy and Fission Products from the Containment atmosphere.

Thus the Containment Spray System and the Containment Air Purification System both cool and clean up the Containment atmosphere.

2.6.5 The Combustible Gas Control System

During the Three Mile Island accident, there was much concern that there was a build-up of Hydrogen gas inside the Containment Building. The danger is that the concentration of Hydrogen could reach explosive levels and the Containment building would be damaged. The gas is generated in accident conditions by a reaction between the reactor coolant water and the Zircalloy cladding of the fuel rods. This occurs at temperatures above 983 deg.C and becomes significant at temperatures above 1200 deg.C.

Another source of Hydrogen is from the radiolysis of water in the Containment Sumps. Radiolysis is a reaction that takes place in water when it is irradiated with Gamma rays given off by the Fission Products washed down into the sumps. Hydrogen and Oxygen are produced.

Two electric Hydrogen Combiners are usually provided, one as a spare. Should the Hydrogen Combiners fail to keep the Hydrogen concentration below 4 percent, the limit for explosiveness, then a purging system is used. Fresh air is blown into the Containment and the air drawn out is passed through High Efficiency Air Filters and Charcoal Filters to minimize the Environmental release of radio-active Fission Products.

2.6.6 The Habitability Systems

These systems are provided to protect the plant operators in accident conditions. The plant control room habitability system controls the temperature and humidity of the room and keeps it free from radio-activity, smoke and poisonous gasses. Food, water, medical supplies and sanitary facilities are provided to support seven people for a week. Protective clothing and breathing apparatus is also provided.

2.6.7 The Emergency Core Cooling Systems

In accident conditions, the purpose of these systems is to keep the Reactor Core sub-critical, that is, no self sustaining fission reactions occurring, and to remove the Core decay heat and prevent the melting of the Fuel rod cladding.

There are three parts to the Emergency Core Cooling System:- the High Head Safety Injection System, the Low Head Safety Injection System, and the Accumulators. A schematic of the Emergency Core Cooling Systems is given in Figure 2.8.

2.6.7.1 The Accumulators

The Accumulators are passive injection devices:- they are tanks containing water and pressurized Nitrogen at 45 Bar. A flap valve at the bottom of the tank remains shut so long as the Reactor Coolant pressure is greater than

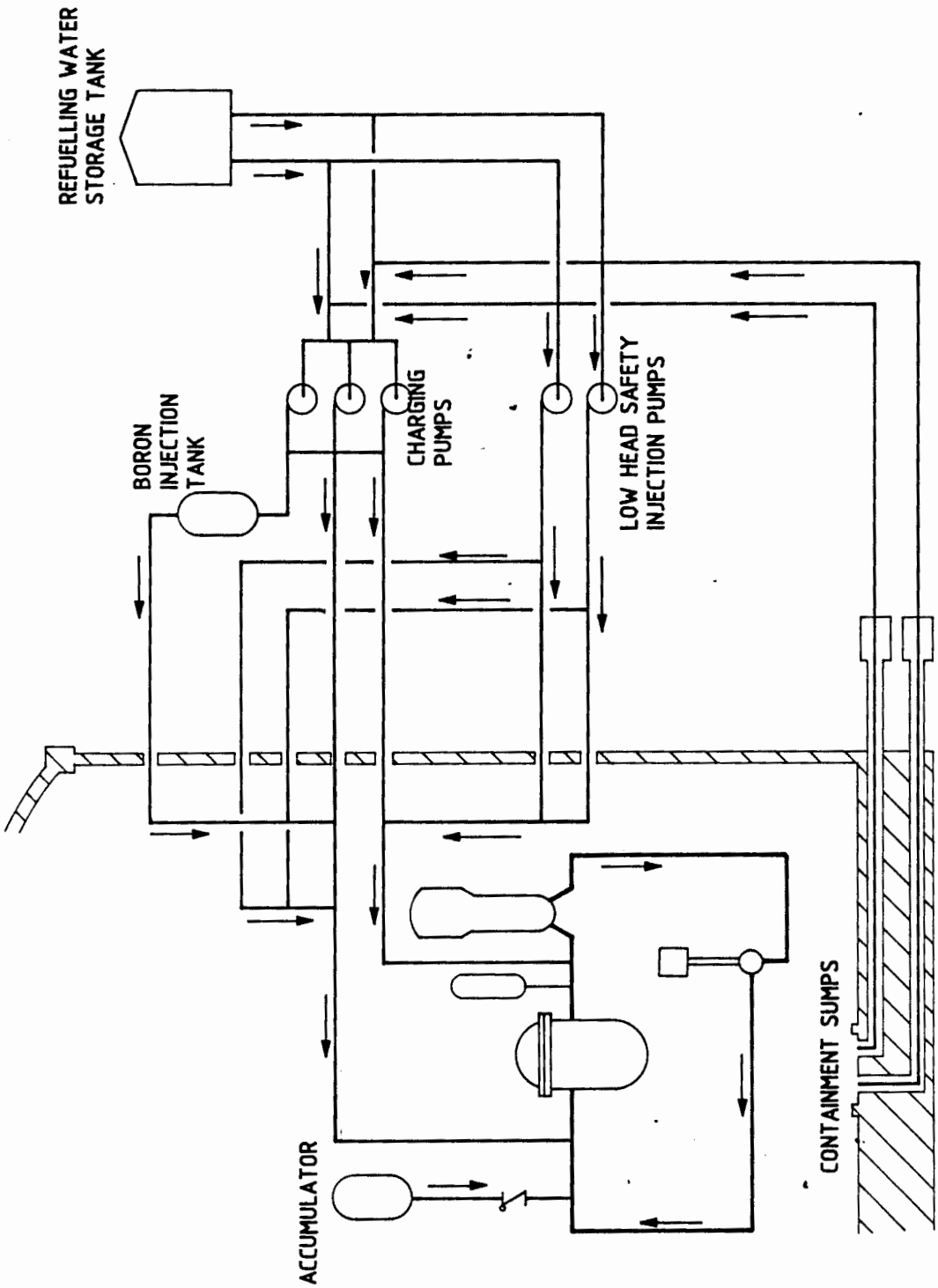


Figure 2.8 "The Emergency Core Cooling Systems"

45 Bar. When the Loss of Coolant Accident (LOCA) occurs, all the Primary system water (which was at 154 Bar and 340 deg.C) flashes over to steam, and the core is uncovered. The pressure of the Primary Coolant system drops to the Containment building pressure and the pressurized Nitrogen in the Accumulator vessel forces the water out through the flap valve into the Reactor vessel. The Accumulators provide cooling water quickly before the Safety Injection pumps are fully operational.

2.6.7.2 The High Head Safety Injection System

The High Head Safety Injection pumps are able to inject water into the Primary Coolant System under normal operating conditions. The pressure is very high (154 Bar) and the flow is relatively small. These pumps are also used in the Chemical and Volumetric Control system to pump the water back into the Primary Coolant system.

The High Head Safety Injection System is used to make up the water lost when there is a small Loss of Coolant Accident, that is, when there is a small leak in the Primary Coolant System. The source of injection water is the Refuelling Water Storage Tank which means that the water is Borated.

The High Head Safety Injection system is also used to inject the contents of the Boron Injection Tank into the Primary Coolant System when a Main Steam Line Break accident occurs. Due to the thermodynamic consequences of the steam line break, there is a cooldown of the Primary Coolant System which in turn enhances the Nuclear fission process. This is why a massive injection of Borated water is necessary after a Steam Line break:- the Boron absorbs neutrons and stops the Nuclear fission process.

2.6.7.3 The Low Head Safety Injection System.

A large Loss of Coolant Accident results in the loss of all the Primary Coolant. The Accumulators provide some cooling immediately after the rupture, but the Low Head Safety Injection Pumps provide long-term cooling. Initially, the cooling water is taken from the Refueling Water Storage tank, and when this tank is empty (all the water has been pumped into the Containment), suction is taken from the Containment building sumps. The water in the Refueling Water Storage tank is Borated to inhibit the Nuclear fission process.

The Low Head Safety Injection System therefore has two modes of operation:- the Direct Injection mode where water is drawn from the Refueling Water Storage tank, and the Recirculation mode, where water is drawn from the Containment Building sumps, cooled in heat-exchangers, and pumped back into the Primary Coolant System. In some plants, the actual pumps used to effect the Low Head Safety Injection function are the Residual Heat Removal pumps.

Two sets of Safety Injection pumps are needed because high pressure and a large water flow are not economically provided by one pump design:- therefore, the High Head Safety Injection pumps are designed for high pressure and low flow (typically 173 Bar at 0.57 m^3/min) while the Low Head Safety Injection pumps produce a large flow but at a low pressure (typically 19 m^3/min at 5.8 Bar).

Thus for all Primary Coolant system pressures likely to be encountered, the Emergency Core Cooling Systems can provide core cooling water .

2.6.8 The Auxiliary Feedwater System

The final Emergency Core Cooling System is the Auxiliary Feedwater System (Figure 2.9):- this system provides a flow of cooling water to the Secondary side of the Steam Generators in the event of the loss of normal Feedwater or a Main Steam Line Break. There are three Auxiliary Feedwater pumps:- two driven by electric motors, and one driven by a Steam Turbine. The steam to drive the Auxiliary Feedwater Steam Turbine is taken from the Steam Generator outlets and the water for the pumps can be taken from the Condensate Storage tank or from the Service Water system.

The steam produced in the Steam Generators can be dumped either to the Atmosphere, or straight into the Turbine Steam Condenser. A heat transfer path therefore exists for energy to be extracted from the Primary Coolant System:- the Auxiliary Feedwater System pumps water into the Secondary side of the Steam Generators where energy from the Primary Coolant System heats the water to steam which is dumped to the Atmosphere or the Turbine Condenser.

2.6.9 The Engineered Safety Feature Support Systems

The Emergency Safety Features require some support systems:-

2.6.9.1 The Ultimate Heatsink

The Ultimate heatsink is where the decay energy can be dumped:- this is usually a large river or the sea.

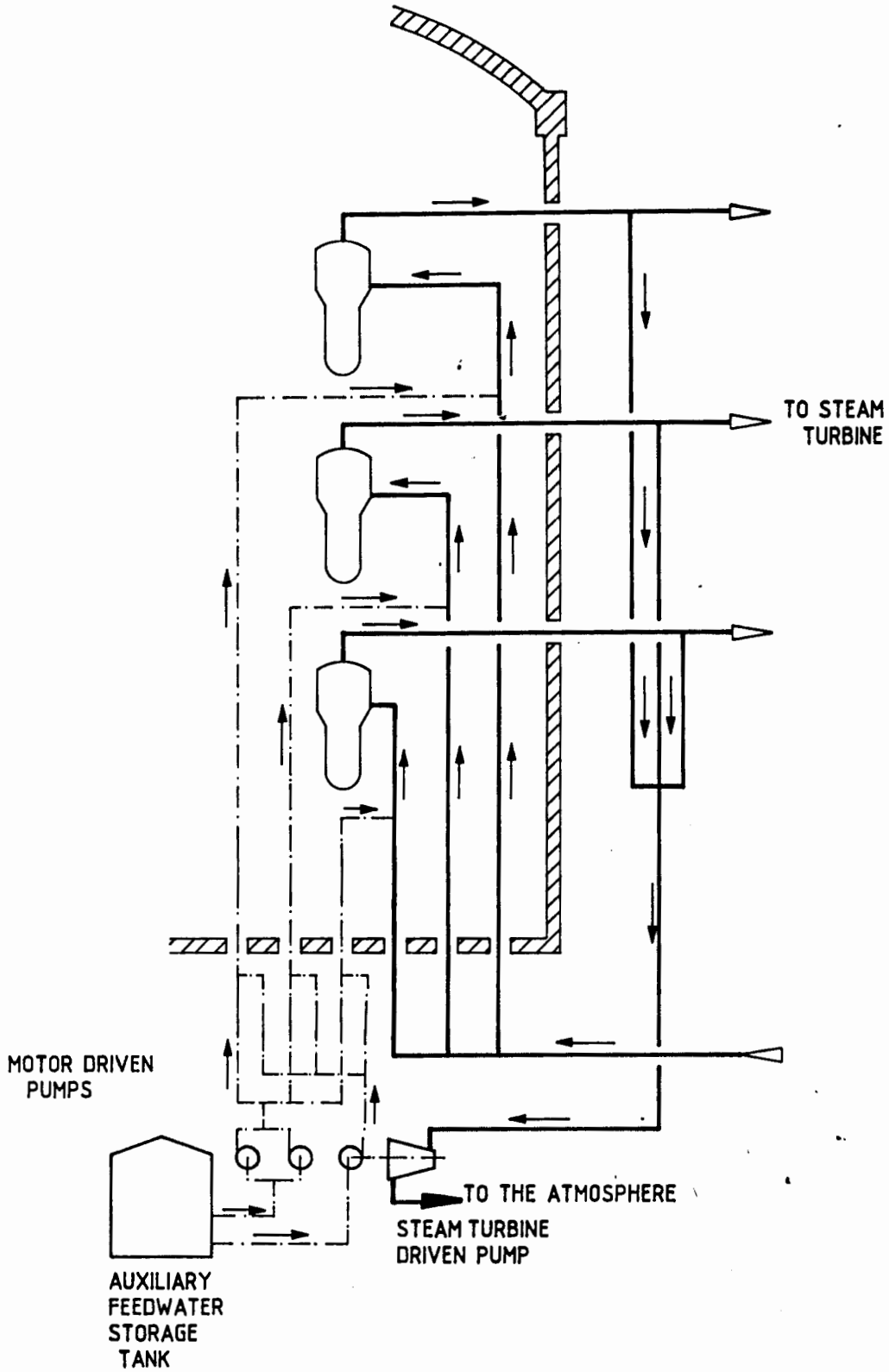


Figure 2.9 "The Auxiliary Feedwater System"

2.6.9.2 The Service Water System

The Service water system pumps water from the Ultimate heatsink to the Emergency Safety System heat loads that have no radio-active risk:-

The Component Cooling Water Heat Exchangers
The Reactor Building Cooling Units
Air Conditioning Mechanical Chillers for the Habitability systems.
Cooling water for the Diesel Generators.

2.6.9.3 The Component Cooling Water System

The Component Cooling Water System provides cooling water to the Containment Spray System Heat Exchangers. These heat exchangers pump highly radio-active water in certain accident conditions and, should a tube leak occur, the radio-activity will be detected and contained in the Component Cooling Water System. As the Component Cooling Water System is a closed loop, there will be no release of radio-activity to the Environment.

2.6.9.4 The Emergency Electric Power Systems

The last Emergency Safety Feature support system is the Emergency Electric Power System. Two diesel generator sets form the backbone of the Emergency power supply, with lead-acid batteries providing power for selected loads.

Thus the Engineered Safety Features protect the first Fission Product Barrier (the fuel rod cladding) by controlling the reactor core temperature and fission process stability with the Emergency Core Cooling Systems and the Auxiliary Feedwater system.

The Second Fission Product Barrier (the Primary Coolant System boundary) is protected by the Pressurizer Relief valves, the High Head Safety Injection of the large dose of Borated water, and the Auxiliary Feedwater system.

The Third Fission Product Barrier (the Containment building) is protected by the Containment Spray system and the Combustible Gas Control System.

The concentration of radio-active Fission products in the Containment atmosphere is reduced by the Containment Spray system and the Containment Air Purification system.

The Containment Isolation system ensures that few Fission Products escape from the Containment building.

2.7 Summary.

We have discussed the Nuclear fission process and discovered that the source of decay heat is the energy emitted by radio-active Fission Products. Further, we have explored the Nuclear Reactor and the associated systems required for the Normal generation of electric power.

The systems utilized in Normal operation are:-

1. The Primary Coolant system containing:-

    1.1 The Reactor vessel containing the Fuel rods and the Control Rods.
    1.2 The Reactor Coolant Pumps.
    1.3 The Steam Generators.
    1.4 The Pressurizer.

2. The Chemical and Volume Control System.
3. The Control Rods.
4. The Residual Heat Removal System.
5. The Steam Turbine and Generator comprising of:-

    5.1 The Steam Turbine and Steam Condenser.
    5.2 The Generator.
    5.3 The Condensate and Feedwater pumps.
    5.4 The High and Low pressure heaters.
    5.5 The Oil Lubrication equipment.

The Engineered Safety Features provided to minimize the impact of the postulated accidents by protecting the Multiple Fission Product Barriers are:-

1. The Containment Spray system.
2. The Containment Air Purification System.
3. The Combustible Gas Control System.
4. The Habitibility Systems.

5. The Emergency Core Cooling Systems comprising of

5.1 The Accumulators.
5.2 The High Head Safety Injection system.
5.3 The Low Head Safety Injection system.

6. The Auxiliary Feedwater System
7. The Engineered Safety Feature Support Systems comprising of

7.1 The Ultimate Heatsink.
7.2 The Service Water system.
7.3 The Component Cooling Water System.
7.4 The Emergency Electric Power Systems.

At this point we have an overview of all the main systems in a typical Pressurized Water Reactor Nuclear Power Plant. These systems have been provided to address the particular requirements of the Normal and Emergency operation of the power station. For the power station to pose only a small risk to the public these systems must have an appropriate reliability:- the special reliability requirements for Nuclear Power Plants will be discussed in the next chapter.

3. Special Requirements for Nuclear Power Plants

We have seen previously why Nuclear Power Stations have such complex safety systems:- the overall aim of all these systems is to minimize the release of radio-active matter into the environment, during both Normal operation and Accident conditions.

For the release of radio-active matter to be minimized, the safety systems must operate correctly. However, in the real world where the force is for things to go from a state of order to state of disorder [8], the safety systems of a Nuclear Power Plant have a certain probability of changing state, possibly into a state of system failure. The techniques that have been developed to quantify the probability of system failures is known as Reliability Engineering.

Nuclear Power Stations as whole must be reliable, as must the individual components in the safety systems:- the way this is achieved is to recognize that systems can fail, and to design the systems accordingly.

This chapter has three sections:- the first addresses the reliability of equipment and systems; the second outlines the American Nuclear Regulatory requirements; and the third the IEEE Nuclear Specifications.

3.1 Reliability

We will initially consider the concept of Reliability by using a common example of a complex system that can have lethal effects in the event of failure:- the motor car.

---

8. Boikess,R.S. and Edelson,E. "CHEMICAL PRINCIPLES", Harper & Row, New York, 1978, page 394.

The following points illustrate the how the various activities of making a motor car can contribute to the reliability of the vehicle's operation.

A. The Design of the vehicle:- the car could be a poor design with mechanical weakness in the chassis or engine. Engine failure at speed can have lethal consequences. An electrical example of a design weakness (although not lethal in the event of failure), is if the alternator is operating at full output most of the time:- the stator windings will be near the maximum design temperature of the wire, and premature failure is likely as the life of electrical insulation is inversely proportional to the operating temperature.

B. The Manufacture of the vehicle:- depending on the competence and motivation of the workers, at certain times the chances are high that certain components are not assembled as specified by the design. Thus, although the design is good, poor manufacture can cause failures. Other causes of failure due to manufacture are the use of incorrect material, the use of incorrect tools, and inexperience of the manufacturer.

C. The activity of Inspecting and Testing the vehicle:- the purpose of inspecting and testing both the parts and the assembled car is to detect design and manufacturing faults. If the motor car is not comprehensively tested in the manufactures works, then faults will persist and the vehicle will one day fail.

D. The Operation of the vehicle:- if the owner of the motor car operates the car outside of the manufacturer's recommended limits, say he consistently runs the engine into the red zone on the

revolution counter:- then the engine will fail prematurely as the engine parts are overstressed.

E. The Maintenance of the vehicle:- the various components in a motor car have a finite service life and the manufacturer gives recommended times for replacement. For example, if the engine oil is never changed then the bearings in the engine will most likely fail early as they will not be lubricated as the designer intended.

The reliability of a motor car could be increased by improving the Design, Manufacture, Testing, Operation, or Maintenance of the vehicle. Any improvement will usually cost more and there will be a point where the cost of increased reliability is not justified either in terms of economic viability or operational safety. There is therefore a trade-off between reliability and cost.

3.1.1 Measuring Reliability

The reliability of a component is quantified as an expected failure rate. A power capacitor, for example, could have a failure rate of 0.1 per million hours operation. This means that if we have 1000 capacitors operating simultaneously, we can expect 100 to fail for every million hours of operation. That is, one every 10 000 hours.

The reliability of a component can be determined by testing, or by using the operating history of a population of components. The failure rate of a component is not constant, but follows a "Bathtub" curve [9] as shown in Figure 3.1. The number of failures is high initially as components fail due to small manufacturing defects. This is known as the "Burn-in" period. There-after, the failure rate is constant and this is the working life of the component. Finally, near the end of the component's life, the incidence of failures again increases:- this is the "Wear-out" period. Here bearings wear out and other aging mechanisms cause equipment failure.

There are a number of sources of reliability data:- many large organizations keep records of component failures, and after many years, they can predict fairly accurately the failure rates of these components. Two examples are included in the References [10] and [11].

3.1.2 Designing for Reliability

There are many ways to design equipment that is reliable. The first is to use reliable components. Today the techniques for consistently making reliable components has been formalized into a new subject, that is, Quality Assurance.

---

9. Report IEEE Standard 650 "IEEE STANDARD FOR QUALIFICATION OF CLASS 1E STATIC BATTERY CHARGERS AND INVERTERS FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1979. Appendix B, page 22.
10. Report IEEE Standard 500 "RELIABILITY DATA",The Institute for Electrical and Electronic Engineers, New York, USA, 1977.
11. United States of America, Military Document Ref.MIL HDBK 217 "RELIABILITY DATA".

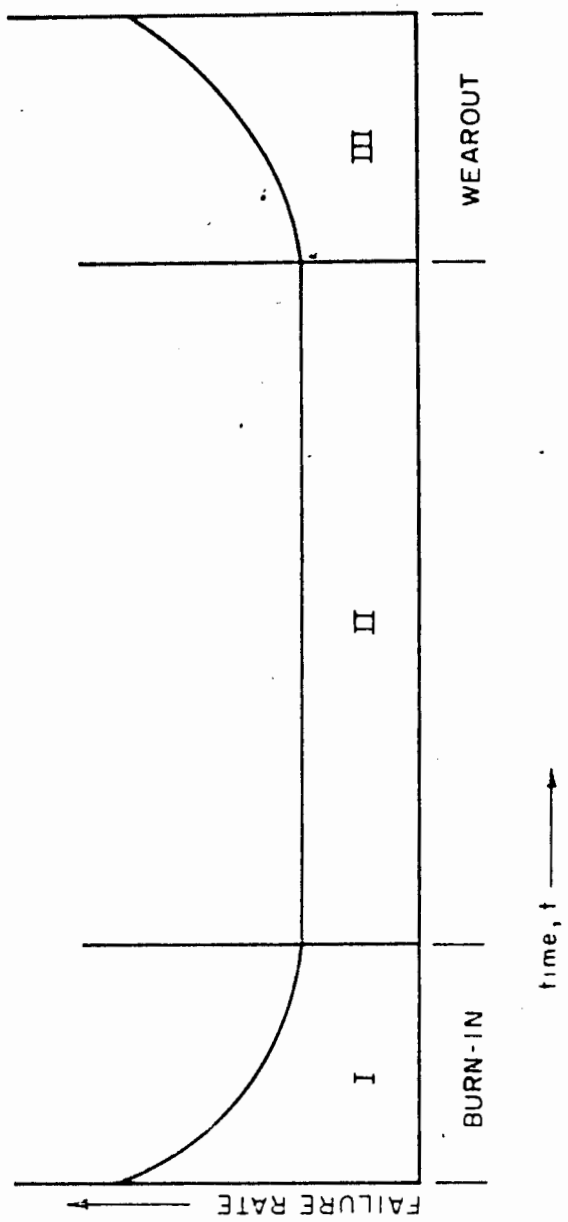


Figure 3.1 "The Bath Tub Curve"

3.1.2.1 Quality Assurance

The control of the Design, Manufacture, Testing, Operation, and Maintenance of an item to assure it's quality is often called Quality Assurance. Quality Control forms a part of Quality Assurance in that Quality Control happens in the Manufacturing and Testing phases.

We have seen in our discussion about a motor car that Quality Assurance is simply common sense. But the advantage of using Quality Assurance techniques is that this common sense is written down in Quality Assurance procedures and is therefore not forgotten.

The essentials of a Quality Assurance program are:-

Design Control
Manufacturing Control
Inspection
Installation Control
Testing

Procedures for each of the above topics are developed:- the Quality is assured because the controls and methods specified in the procedures are used to audit the work done.

In Nuclear Power Plants the components that are important to the operation of the safety systems are designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with an appropriate Quality Assurance program. The components are very reliable, but also expensive.

Components not important to Nuclear safety are also given some form of the Quality Assurance program depending on their importance to the plant availability, or the expense of the component. The Generator Transformers, for example,

are expensive and vital to the plant availability:- they therefore have a comprehensive Quality Assurance program to assure their reliability.

Thus, by using Quality Assurance techniques we can be assured that all work needed to produce an item (or a Nuclear Power Plant) is controlled and therefore the end-product should be reliable. There are nevertheless some design techniques that significantly enhance the reliability of a system.

3.1.2.2 Over Rating

The over-rating of a component usually leads to a longer service life of that component. The Safety Injection pumps at Koeberg Nuclear Power Station are 710 kW motors, but the maximum load they have to drive is less than 650 kW. The temperature rise of the motor is therefore below the maximum design temperature and the insulation therefore lasts longer. The bearings and shaft are also less stressed.

The concept of over-rating to provide reliability is intuitively recognized. One often hears the comment:- "In the old days things lasted much longer." Today to be cost effective we use advanced analysis to design items nearer the limit of failure, but in the past designers had no sophisticated computer analysis programs and items were therefore grossly over-designed to be safe. Thus the items lasted much longer.

3.1.2.3 Redundancy

The reliability of a system can be increased by using identical systems in parallel, that is, to have redundant systems so that if one fails, the redundant system is able to fulfil the system output requirements.

This approach is often used in equipment that has to be reliable. The American space shuttles use a number of computers in parallel to control the spacecraft. The actual control output is determined by a Majority Vote scheme. Thus if one computer fails, the craft will still be safely controlled by the remaining computers.

Another everyday example is the brake system on a motor car:- the front and back brakes have separate hydraulic lines so that one line failing will not result in a complete brake failure. The handbrake is another redundant system for stopping the vehicle.

3.1.2.4 Independence

When two or more redundant systems are used to provide an output, it is important that the redundant systems are independent from each other. It would be pointless to have five redundant systems all powered from the same electric power supply for they would all be disabled if that one power supply failed.

In a motor car, the handbrake is independent from the footbrake:- the footbrake actuates the break pads hydraulically while the handbrake actuates the brake pads using a steel cable.

In the new Advanced Gas Reactors in Britain, two redundant systems are used to control certain operations on the reactor:- apart from being physically independent, they use independent technologies. The one Division uses micro-processor based equipment which is not vulnerable to earthquakes, while the other Division uses relays which are not vulnerable to temperature extremes [12]

12. Daniels,G.H. "ELECTRICAL SYSTEM DESIGN FOR FUTURE AGR POWER STATIONS", IEE Proceedings C (Generation, Transmission and Distribution), Volume 128 no.2, March 1981, pages 123-8.

Generally, in Nuclear plants, separate power supplies and ventilation are used for each redundant system. The redundant systems are also physically separated from each other to prevent fires and explosions in one system from disabling the other systems.

3.1.2.5 Periodic Testability

Testing is an important part of keeping a system reliable. The ability to test a system, possibly on-line, is designed into systems that need to function reliably.

Immediately after a piece of equipment has been tested, it is highly unlikely that it will fail as the test should have verified the functionality of all the parts of the equipment. However as time goes by, the chances of the equipment failing increases. Therefore if the equipment is tested frequently the probability of the system being inoperable due to a "hidden" failure will remain relatively small as the fault will be detected by the tests. This can be summarized as:- the probability that the equipment will fail is directly proportional to the failure rate of the equipment (failures per year) and inversely proportional to the testing frequency.

The logic part of Reactor Protection System at Koeberg is tested by injecting short pulses into the inputs and measuring the output of the system. This happens while the Reactor Protection System is actually monitoring the reactor, and the reason the output does not trip the reactor is that the output pulses are too short to activate the Reactor Trip Breakers. The testing frequency is very high and the system is therefore very reliable:- a fault is detected virtually as soon as it occurs. [13]

13 This analysis assumes that the repair time is short. If the repair time is so long that the probability of another failure occurring is significant, then a more intricate

3.1.2.6 The Single Failure Criterion

The American Nuclear industry has defined a criterion that is used to formulate the configuration of the safety systems in Nuclear Power Plants. The IEEE Standard 379 "IEEE Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E equipment" [14] describes the criterion:- the Single Failure Criterion.

The Single Failure Criterion states that the system shall perform its protective function even with one single failure in the system. The failure mode must be detectable in the periodic testing of the system, or if the failure mode is undetectable, then the system must perform its protective action in the presence of all undetectable failures, and with any one single detectable failure. The reason for this is that if the failure is undetectable and could inhibit the system protective action in conjunction with a detectable failure, one could have a situation where a single detectable failure inhibits the system protective function.

Using more than one redundant system to effect a protective function meets the requirements of the Single Failure Criterion provided that the redundant systems are independent. A single failure occurring in one redundant system will not prevent the other redundant systems from completing the protective function. If the redundant systems are not independent, say power for different redundant systems is supplied by a common switchboard:- then the failure of this single component will inhibit the system protective function.

---

analysis is necessary. The concept of frequent testing to improve system reliability is still valid however.

14. Report IEEE Standard 379 "IEEE STANDARD APPLICATION OF THE SINGLE FAILURE CRITERION TO NUCLEAR POWER GENERATING STATION CLASS 1E SYSTEMS",The Institute for Electrical and Electronic Engineers, New York, USA, 1977

3.1.2.7 Probabilistic Risk Assessment

The Single Failure Criterion is useful for designing the configuration of safety systems, but does not provide a quantitative figure for the reliability of a protective function. In many instances it is important to know the different failure modes of a system and the frequency at which they are expected to occur. The most significant failure, may be due to a Single Failure, or it may be due to two independent failures.

The failure modes and probabilities of systems can be determined by a Probabilistic Risk Assessment. This analysis technique is being utilized more and more frequently to determine the reliability of Nuclear Power Stations. Koeberg Nuclear Power Station is licensed by the Atomic Energy Corporation based on Probabilistic Risk Assessments of the station.

The acceptance criteria for Koeberg Nuclear Power Station are detailed in the Atomic Energy Corporation document LBG1 [15]. This document is based on the Farmer Curve (Figure 3.2). Farmer based this curve on his proposal that a release of radio-active Iodine with an activity of 1000 Curies should not happen more frequently than once in a 1000 Years [16]. As a comparison the release of radio-active Iodine from Chernobyl amounted to 7.3 million Curies [17]. The shape of the Farmer curve implies that if the health risk to the public of an event is large, then the likelihood of that event occurring must be kept small. Events that have a small impact can be quite common.

---

15. Atomic Energy Board of South Africa "LICENSING OF NUCLEAR INSTALLATIONS: A GUIDE TO THE REQUIREMENTS FOR SAFETY ASSESSMENT", document no. LBG/1, issue 3, May 1979.
16. Winkler,B.C. "QUANTIFICATION OF SAFETY STANDARDS," Nuclear Safety and Reliability Assessment Course organized by the Atomic Energy Corporation of South Africa and the University of Cape Town, Pretoria, 24 June to 5 July, 1985.
17 "CHERNOBYL: THE SOVIET REPORT," Nuclear News, October 1986, pages 59 to 66.

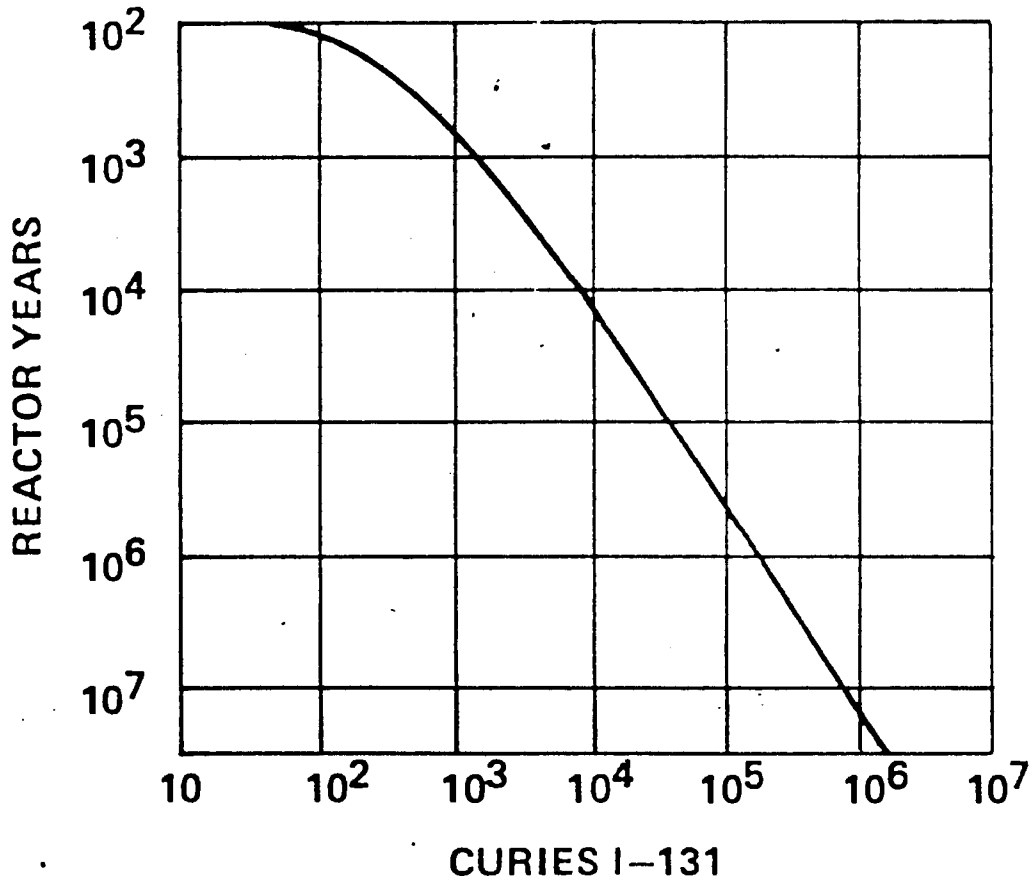


Figure 3.2 "The Farmer Curve"

The Atomic Energy Corporation has evaluated the siting of Koeberg Nuclear Power Station and has produced a curve similar to the Farmer Curve which takes into account the acceptable risk per person living near the plant, and a survey of the wind conditions prevailing at the plant [18].

The core of a Probabilistic Risk Assessment is the Fault Tree. The Fault Tree for the braking system on a motor car is developed to illustrate the method. The schematic for the braking system is shown in Figure 3.3.

The Fault Tree for the Braking System (Fig. 3.4) starts with the Top Event:- "Brakes fail to stop vehicle". This event occurs when the hydraulic brakes fail (Fig. 3.5 and 3.6), and the handbrake fails (Fig. 3.7). Each of these events can be broken down further. For example, the hydraulic brakes fail only if both the front AND back break systems fail. The Fault Tree is developed down to the initiating events:- "Brake hydraulic pipe ruptures." as an example.

Once the Fault Tree is complete, cutsets of the fault tree are calculated using Boolean logic. Essentially, this is simplifying the logic equation defined by the fault tree. A cutset is a minimum combination of initiating events that cause the Top Event. Thus, labelling each initiating event alphabetically, the cutsets for our fault tree are:- AGH, AJ, AK, BCGH, BCIJ, BCIK, DGH, DIJ, DIK, EGH, EJ, EK, FGH, FJ, and FK. The cutset AJ is the failure mode "Hydraulic pipe ruptures" AND "Hand brake lever fails":- if these two events occur together, then the vehicle will have total brake failure. Similarly, each of the other cutsets result in total brake failure.

18. Winkler,B.C. "QUANTIFICATION OF SAFETY STANDARDS," Nuclear Safety and Reliability Assessment Course organized by the Atomic Energy Corporation of South Africa and the University of Cape Town, Pretoria, 24 June to 5 July, 1985.

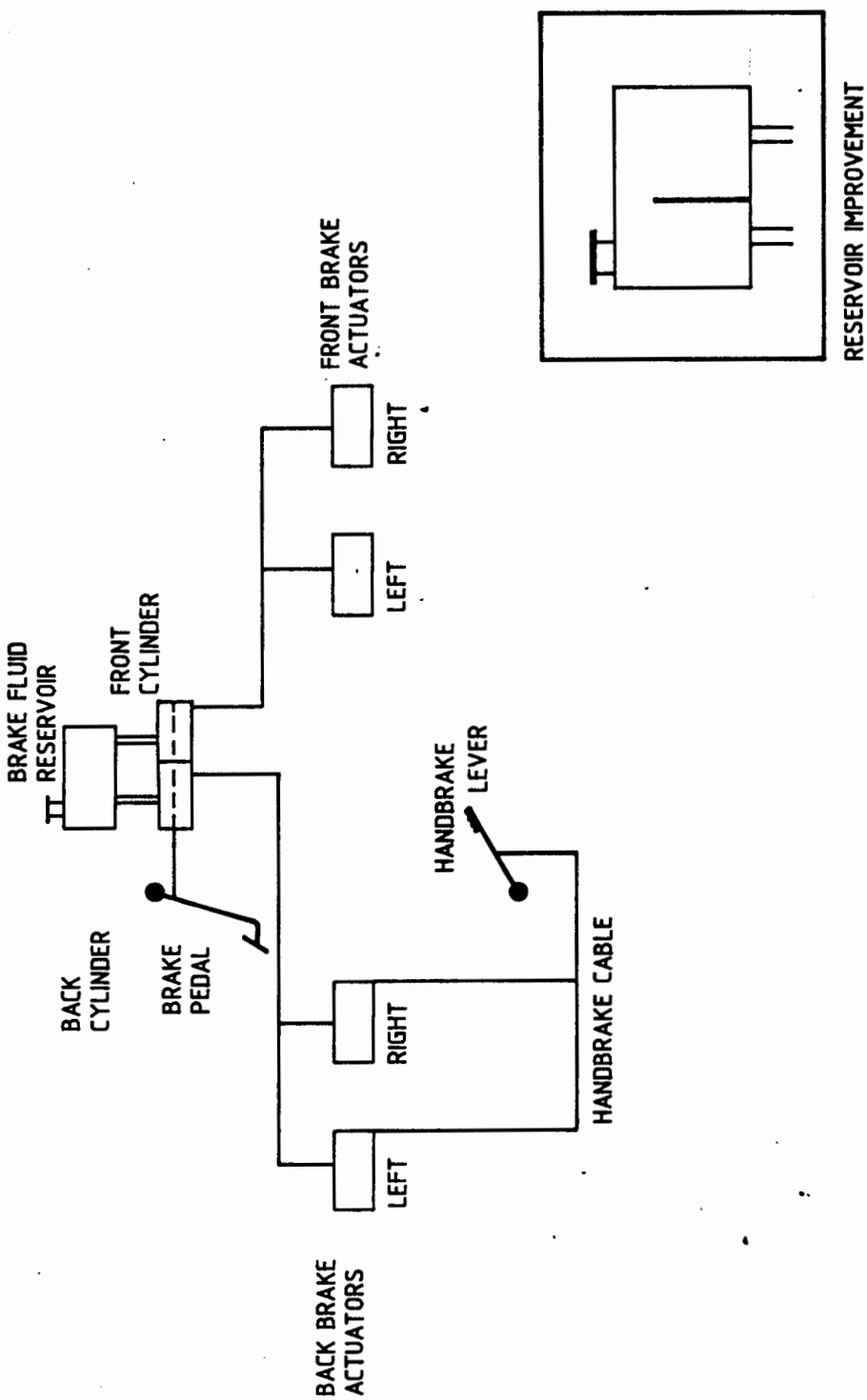


Figure 3.3 "Typical Car Brake System"

FAULT TREE FOR BRAKE SYSTEM

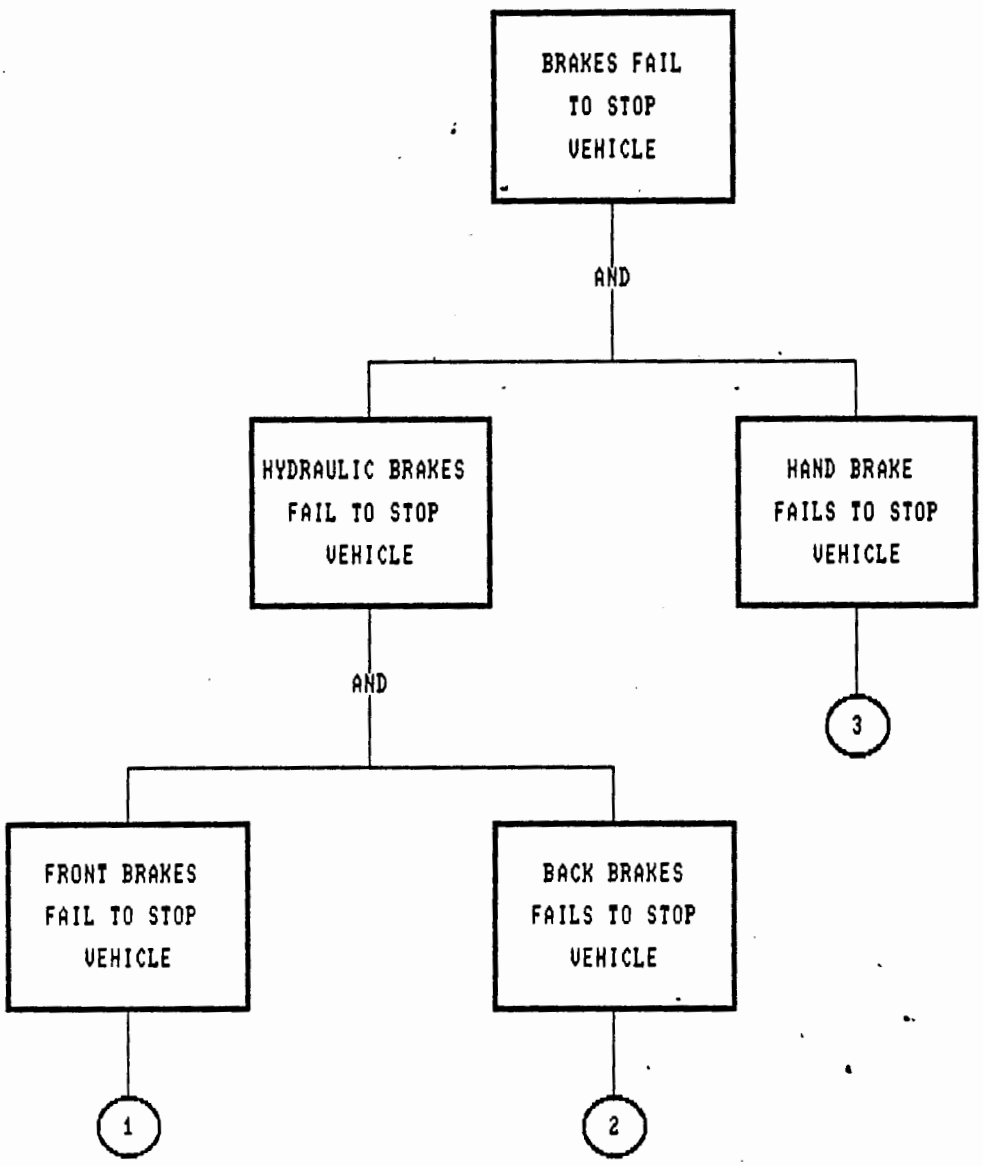


Figure 3.4 "Fault Tree for Car Brake System"

FAULT TREE FOR FRONT BRAKE SYSTEM

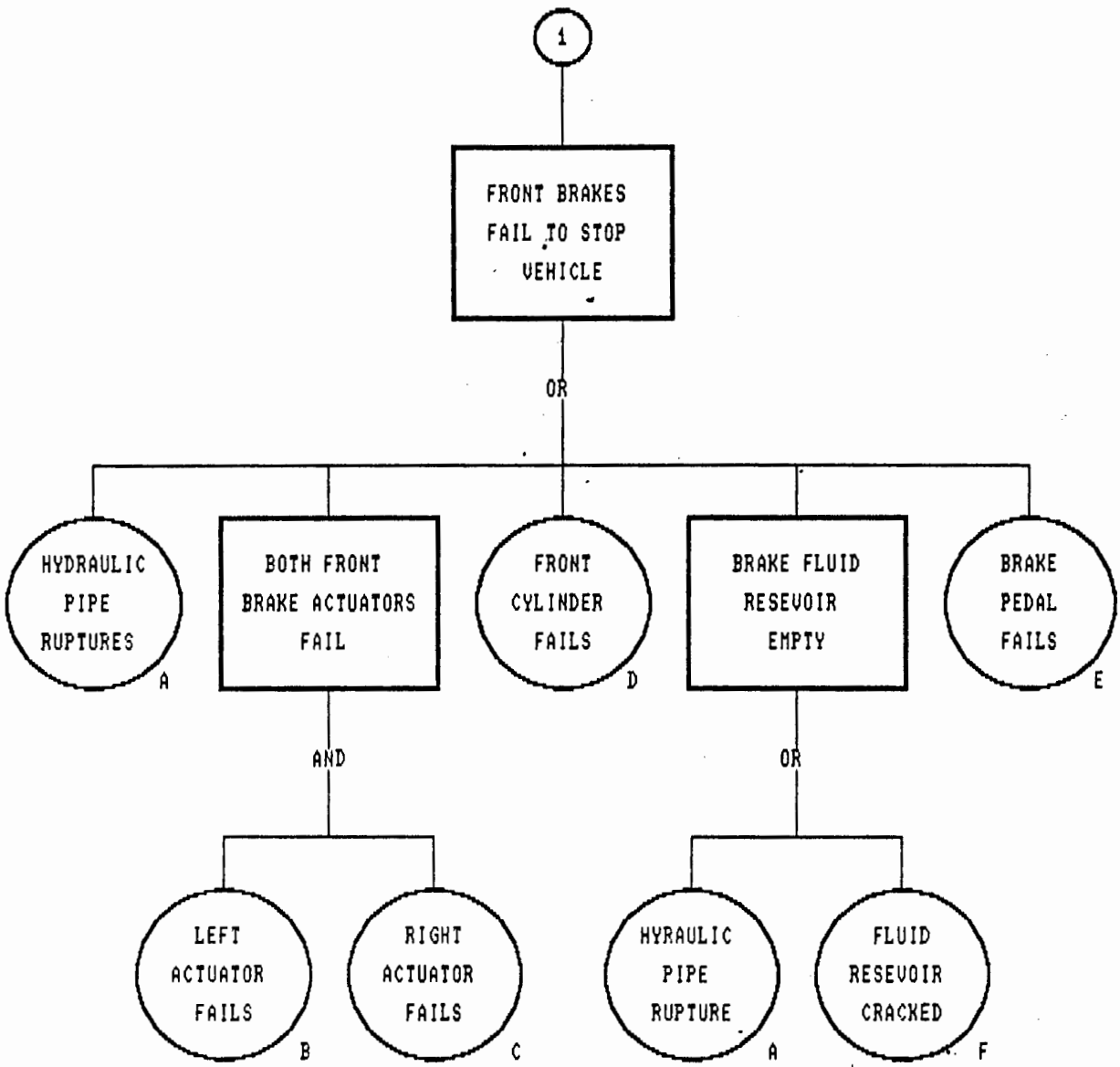


Figure 3.5 "Fault Tree for Front Brake System"

FAULT TREE FOR BACK BRAKE SYSTEM

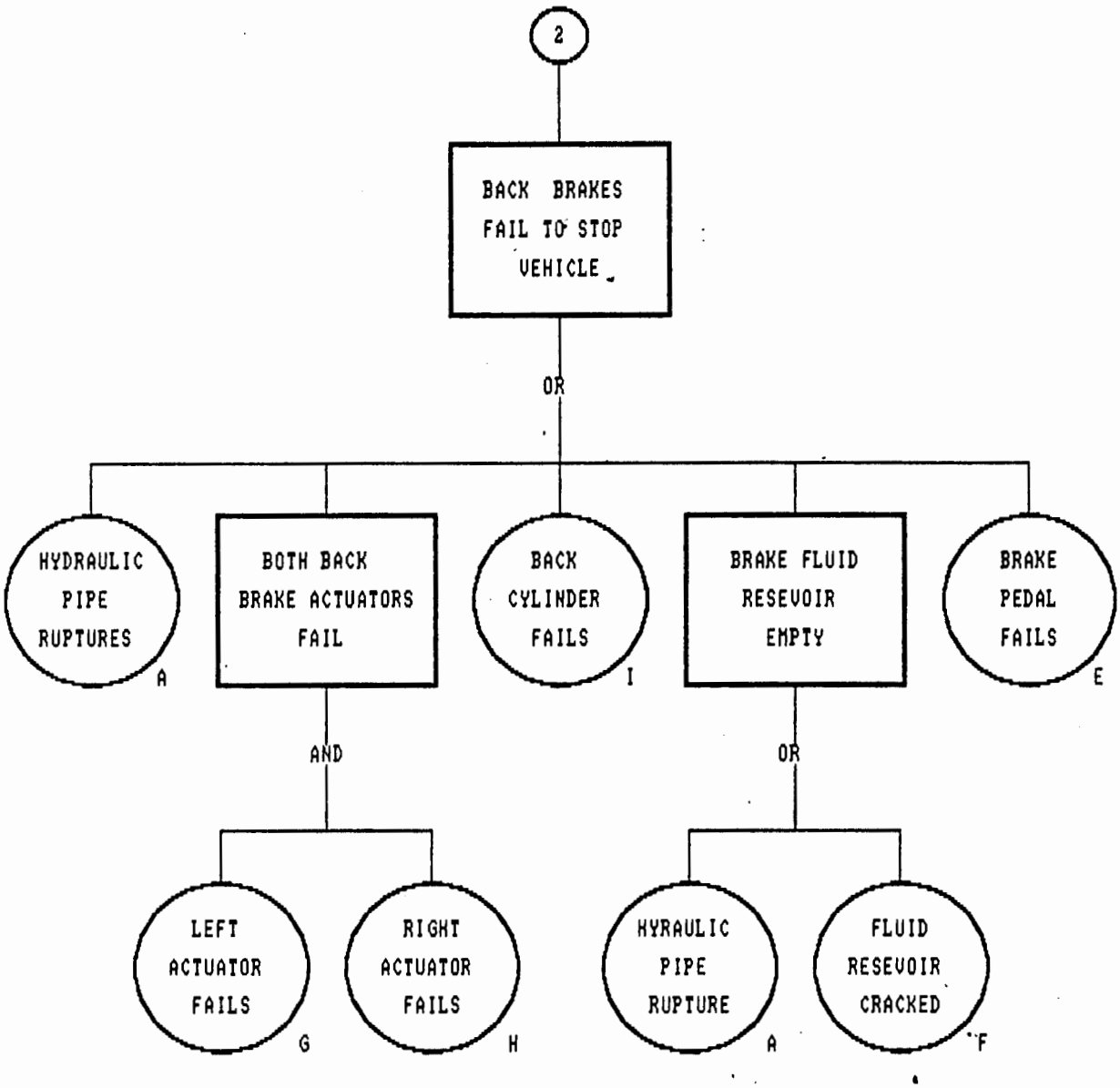


Figure 3.6 "Fault Tree for Back Brake System"

FAULT TREE FOR HAND BRAKE SYSTEM

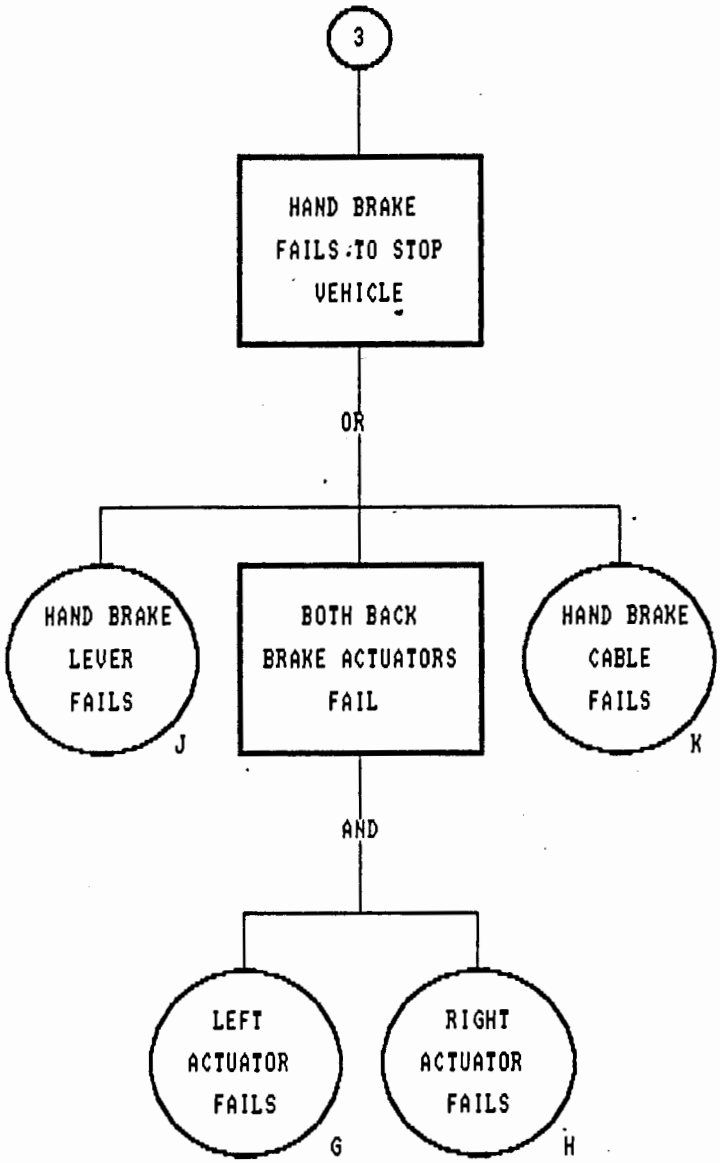


Figure 3.7 "Fault Tree for Hand Brake System"

Now a probability of failure is determined for each initiating event and these are propagated through each cutset of the Fault Tree. To simplify the mathematics, the value 0.001 is used for each initiating event. In reality, the values would be determined by testing, calculation, or by historical data.

Cutset	Probability
AJ	1.0×10^{-6}
AK	1.0×10^{-6}
EJ	1.0×10^{-6}
EK	1.0×10^{-6}
FJ	1.0×10^{-6}
FK	1.0×10^{-6}
AGH	1.0×10^{-9}
DGH	1.0×10^{-9}
DIJ	1.0×10^{-9}
DIK	1.0×10^{-9}
EGH	1.0×10^{-9}
FGH	1.0×10^{-9}
BCGH	1.0×10^{-12}
BCIJ	1.0×10^{-12}
BCIK	1.0×10^{-12}
Total:	6.0×10^{-6}

It is immediately obvious which are the more likely failure combinations. The most probable failure modes involve five initiating events:- "Hydraulic pipe ruptures" (A), "Brake pedal fails" (E), "Fluid reservoir cracked" (F), "Hand brake lever fails" (J), and "Hand brake cable fails" (K).

Thus even though the Single Failure Criterion applies and the car can be stopped in the presence of one failure, the probability of failure of the system may be considered too high and improvements may be needed. The Fault tree analysis identifies the most significant contributors to the Braking system unreliability.

The loss of independence between redundant systems is a difficult situation to quantify:- these are known as

Common Mode Failures. In our motor car example, the event "Brake Fluid Reservoir cracked" is a Common Mode Failure because it will disable both the front and rear hydraulic systems. The solution is to prevent a single leak (of the reservoir, or a burst brake pipe) from emptying the whole reservoir and this can be done by providing a separating wall between the outlets as shown in the insert in Figure 3.3.

Common Mode failures can result from Manufacturing or Maintenance errors, or from a Design problem on a component common to all redundant parts of the Safety System. Thus to prevent Common Mode Failures, the same technician should not service more than one redundant system, for he may make the same error on all redundant systems. The same principle is used when writing software for redundant computer systems:- have independent teams write the software using common input and output specifications. The probability that independent teams will make the same errors, is remote.

Of course, a comprehensive Quality Assurance Program will reduce all failure modes including Common Mode Failures. This is the primary reason for the Qualification of Safety equipment [19]

3.1.3 Equipment Qualification

Part of the task of ensuring a reliable plant is to Qualify equipment for the Service Conditions. In a Nuclear Plant there are two special categories for the Qualification of equipment:- Environmental and Seismic.

---

19. Report IEEE Standard 323 "IEEE STANDARD FOR QUALIFYING CLASS 1E EQUIPMENT FOR NUCLEAR POWER GENERATING STATIONS",The Institute for Electrical and Electronic Engineers, New York, USA, 1983, page 10, sect.4 para.2.

3.1.3.1 Environmental Qualification

The conditions inside the Reactor Containment building are harsh even in Normal operating conditions:- the radiation levels are typically 1 MRad per Year and the ambient temperature 40 deg.C.

In Accident Conditions, the Radiation levels rise to 40 MRad per year and the temperature and pressure peaks at 170 deg.C and 3.8 Bar respectively. In addition, the Containment Spray water contains Caustic Soda, Boric Acid, and various Radio-active Fission Products.

Equipment that is inside the containment and that is required to operate during Accident conditions must be qualified to survive these arduous environmental conditions.

3.1.3.2 Seismic Qualification

Nuclear Power Stations built in areas susceptible to earthquakes are designed to withstand the largest probable earthquake of that area. All safety systems are therefore Seismically qualified.

3.1.3.3 Qualification Methods

Qualification methods used are:-

1. Type tests. For Environmental Qualification, samples of the Equipment are exposed to the postulated Environment; the equipment is considered qualified if it functions correctly after the required amount of exposure. For Seismic Qualification, samples of the equipment are stressed on a shake-table with the postulated forces due to a Design Base Earthquake.

Again, the equipment should survive and operate. The assumption is that if new equipment is manufactured in the same way as those items type tested, then the new equipment is also qualified for installation in the Nuclear Power Plant.

2. Operating Experience. If data from similar equipment indicates that it operates successfully under similar Service Conditions, then the new equipment can be considered qualified.

3. Analysis. Equipment can be qualified by mathematical calculations. For example, electrical cabinets can be Seismically qualified using Finite Element analysis.

An important requirement for reliable equipment is that all facets of the process used to make the equipment is fully specified. To this end, the authorities controlling the use of Nuclear power for commercial power generation have produced many specifications and guidelines.

3.2 American Regulatory Constraints

In typical fashion, Mankind has sought to rationalize all the processes and requirements necessary to keep Nuclear power safe. Historically the Americans were amongst the first to develop comprehensive regulatory requirements. Other nations have based their Nuclear programs on the American example, notably France whose Nuclear program is based largely on the American Westinghouse Pressurized Water Reactor. South Africa, having purchased its Reactor from the French therefore follows the US Nuclear Regulatory Commission requirements closely.

Essentially, the Nuclear Regulatory Commission lays down all the requirements for prospective applicants who want to build a commercial Nuclear Power Plant. The details of the licensing procedure and license requirements are published in the American Code of Federal Regulations Title 10 - "Energy" Part 50 - "Domestic licensing of production and utilization facilities" [20]. The short form reads 10CFR50. As an electrical designer, many sections of 10CFR50 are of no immediate concern, but the sections that are important are:-

10CFR50.34	"Contents of Applications; technical information"
Appendix A	"General Design Criteria for Nuclear Power Plants"

3.2.1 Technical Information

The technical information required by the Nuclear Regulatory Commission must be in the form of Safety Analysis Reports. The Preliminary Safety Analysis Report

20 "Code of Federal Regulations, Chapter 10, Energy", Published by the Office of the Federal Register, United States of America, January 1981.

must present all information necessary for the Nuclear Regulatory Commission to be able to ascertain the impact of the plant on public health and the environment. The Preliminary Safety Analysis Report is submitted before the plant is built. When the plant is built, the Final Safety Analysis Report is submitted which is used to finally determine the overall safety of the Nuclear Power Plant.

The Safety Analysis Reports contain a description of the design and operating features of the Nuclear Power Plant and, to ensure a common framework, the Nuclear Regulatory Commission provide their minimum design requirements in Appendix A of 10CFR50 "General Design Criteria for Nuclear Power Plants."

3.2.2 General Design Criteria

The General Design Criteria applicable to Electric power systems are General Design Criteria 17 and 18.

3.2.2.1 General Design Criterion 17

The General Design Criterion 17 calls for two main sources of electric power:- onsite and offsite. These power sources should be designed so that the systems important to safety will always be available. The capacity and configuration of these power sources should be such that the Fission Product boundaries remain intact during all possible operational conditions, and that the reactor core is cooled and reactivity contained for all postulated accident conditions.

The batteries and distribution systems of the onsite electric power supplies should have sufficient independence, redundancy, and testability so that they

fulfill their safety functions even with a single failure occurring.

The electric power from the offsite transmission network should be supplied by two physically independent circuits which are designed and located so as to minimize the chances that they will fail simultaneously. The Nuclear Regulatory Commission allow a common switchyard and a common right of way for the two independent feeders. Again, each of the offsite power sources must be available independently of whether the other one fails, or all onsite the power sources fail. One of the offsite electric power sources should be available in a few seconds following a Loss of Coolant Accident to ensure the containment of radio-active material.

This General Design Criterion draws the designer's attention to the fact that neither a generator trip, nor an offsite power loss, nor any onsite power losses, shall cause the loss of any of the remaining power supplies.

3.2.2.2 General Design Criteria 18

General Design Criteria 18 gives the requirements for the inspection and testing of the electric power systems. The electric power systems important to safety should be designed so that periodic inspection and testing of the wiring, insulation, connections, and switchboards can be carried out. The purpose of these inspections and test are to ensure that the electric power systems remain as reliable as possible. Both the systems as a whole, and the parts there-of are tested periodically under conditions that mimic the design operating state as closely as possible. Examples of system components are relays, switches and busbars; and system examples are the reactor protection system, and the electric power transfer systems

between the offsite, onsite and intra-unit power sources and sinks.

A comprehensive summary of the sections of 10CFR50 that are of interest to the electrical designer is given in Appendix 1.

3.2.3 Regulatory Guides

The Nuclear Regulatory Commission issues Regulatory Guides from time to time. The purpose of these guides is to make available to the public the methods acceptable to the Nuclear Regulatory Commission staff for implementing specific parts of the Commission's regulations, and to provide guidance for license applicants.

Typical Regulatory Guides applicable to Electric Power Systems in Nuclear Power Plants are:-

1. Regulatory Guide 1.6 "Independence between redundant stand-by (onsite) power sources and between their distribution systems [21]."

2. Regulatory Guide 1.9 "Selection, Design and Qualification of Diesel-Generator Units used as Standby (Onsite) Electric Power Systems at Nuclear Power Plants [22]."

3. Regulatory Guide 1.32 "Criteria for Safety-related Electric Power Systems for Nuclear Power Plants [23]."

---

21. Regulatory Guide 1.6 "Independence between redundant stand-by (onsite) power sources and between their distribution systems," United States Nuclear Regulatory Commission, Washington, D.C. 20555.
22. Regulatory Guide 1.9 "Selection, Design and Qualification of Diesel-Generator Units used as Standby (Onsite) Electric Power Systems at Nuclear Power Plants," United States Nuclear Regulatory Commission, Washington, D.C. 20555.
23. Regulatory Guide 1.32 "Criteria for Safety-related Electric Power Systems for Nuclear Power Plants," United States Nuclear Regulatory Commission, Washington, D.C. 20555.

4. Regulatory Guide 1.53 "Application of the Single Failure Criterion to Nuclear Power Plant protection system [24]."

5. Regulatory Guide 1.75 "Physical independence of Electric Systems [25]."

---

24. Regulatory Guide 1.53 "Application of the Single Failure Criterion to Nuclear Power Plant protection system," United States Nuclear Regulatory Commission, Washington, D.C. 20555.

25. Regulatory Guide 1.75 "Physical independence of Electric Systems," United States Nuclear Regulatory Commission, Washington, D.C. 20555.

3.3 International Nuclear Standards

Many countries have generated specifications for all sorts of things to provide a common framework for activities. Thus specifications for Nuclear Power Stations have also been generated.

The Institute for Electrical and Electronic Engineers in the United States of America has a large suite of Nuclear specifications which deal with topics from Radiation Detectors to Emergency Diesel Generators for Nuclear Power Plants.

Many European countries have their own Nuclear specifications:- these will not be examined in this thesis as they are similar in principle to the American specifications [26].

3.3.1 IEEE Specifications

The Institute for Electrical and Electronic Engineers (IEEE) in the United States of America has published a series of Nuclear Standards which are intended to guide Nuclear Power Station licensees so that the Nuclear Regulatory Commission requirements are met. Figure 3.8 shows the relationships between the different IEEE standards.

The central standard as far as Electric power is concerned, is IEEE 308 of 1980 "Standard Criteria for Class 1E Power Systems" [27] which spells out in more

---

26. For an extensive list of German, French, United Kingdom, American, and IEC standards, refer to IAEA-TECDOC-390 "SAFETY ASSESSMENT OF EMERGENCY ELECTRIC POWER SYSTEMS FOR NUCLEAR POWER PLANTS", subtitled "A manual on the use of IAEA Safety Series No.50-SG-D7: Emergency Power Systems at Nuclear Power Plants", issued by the International Atomic Energy Agency, Vienna, 1986.

27. Report IEEE Standard 308 "IEEE STANDARD CRITERIA FOR CLASS 1E POWER SYSTEMS FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1980.

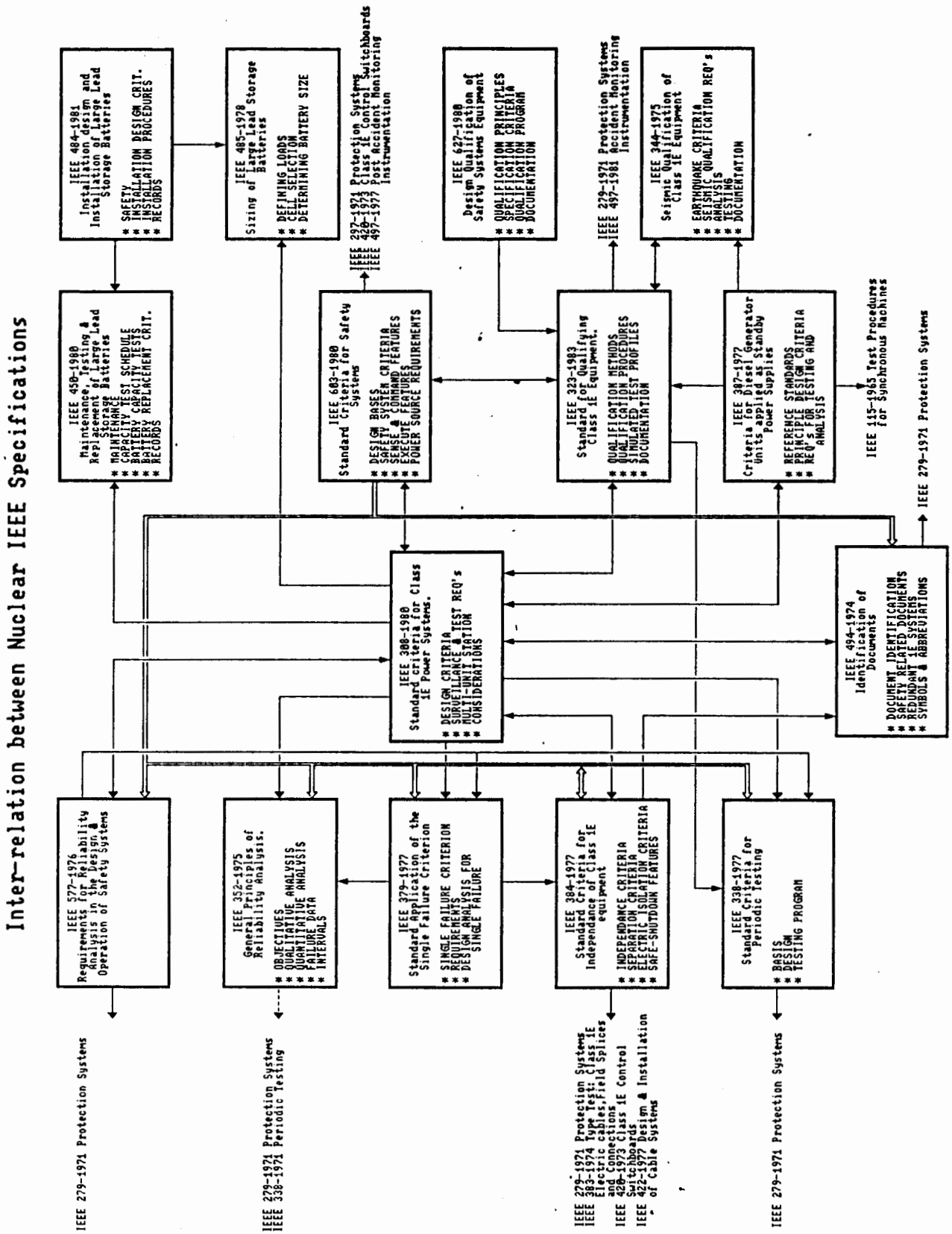


Figure 3.8 "The Relationships between Nuclear IEEE Standards"

detail the Nuclear Regulatory Commission requirements of General Design Criteria 17. The standard IEEE 603 of 1980 "Standard Criteria for Safety Systems" [28] has a more general scope and does not apply to electrical power systems only, but to the protective and control systems as well. Both these standards refer to more specific standards that give requirements for Reliability Analysis, Periodic Testing, Independence, Documentation, and Equipment Qualification.

IEEE 603 of 1980 "Standard Criteria for Safety Systems" is applicable to all parts of the safety systems from the sensors to the actuators. The standard gives criteria for the safety systems and defines three categories for safety related equipment:-

1 Sense and Command features: Equipment here includes the process variable sensors and all the signal processing, both continuous and discrete, right up to the input terminals of the execute features. Examples of these are pressure and temperature sensors along with the analogue signal processing equipment and the logic control circuitry.

2 Execute features are equipment that receive signals from the Sense and Command feature output and perform some function. Examples of these are valve actuators and pump motors.

3 Power Sources are equipment required to generate or transform power. Examples of these are the battery systems that feed inverters and switchgear.

28. Report IEEE Standard 603 "IEEE STANDARD CRITERIA FOR SAFETY SYSTEMS FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1980.

3.3.1.1 Safety Systems

The concept of a Safety System composed of Safety Groups is developed in the IEEE Standards 308 and 603.

The example given in Appendix A of IEEE 603 is useful for clarifying the components of a Safety System.

1 DIVISIONS

The Emergency Core Cooling System will be used as an example to illustrate the concept of a Division in a Safety System. A Division is a set of components, physically and electrically independent from other redundant sets of components.

In terms of the analysis in IEEE 308 & 603, a Division is divided into three sections. The first is the "Sense and Command Features". The Sense and Command Features of a Division of the Emergency Core Cooling System are shown in Figure 3.9:- various sensors detect pressures, temperatures and other physical quantities from the reactor. The Reactor Protection System implements the Protection Logic that determines when a Safety Injection is necessary. The Command signals originate in the Reactor Protection Logic.

The Execute Features are added in Figure 3.10:- The Safety Injection Pumps and the Emergency Core Cooling System heat exchanger is shown. The injection water is taken from a large storage tank initially, and when this is empty, the water is re-cycled from the Containment Building Sumps. Motor operated valves are used to select source of the injection water.

Some Auxiliary support features are added in Figure 3.11. The Closed Loop Cooling Water system and the

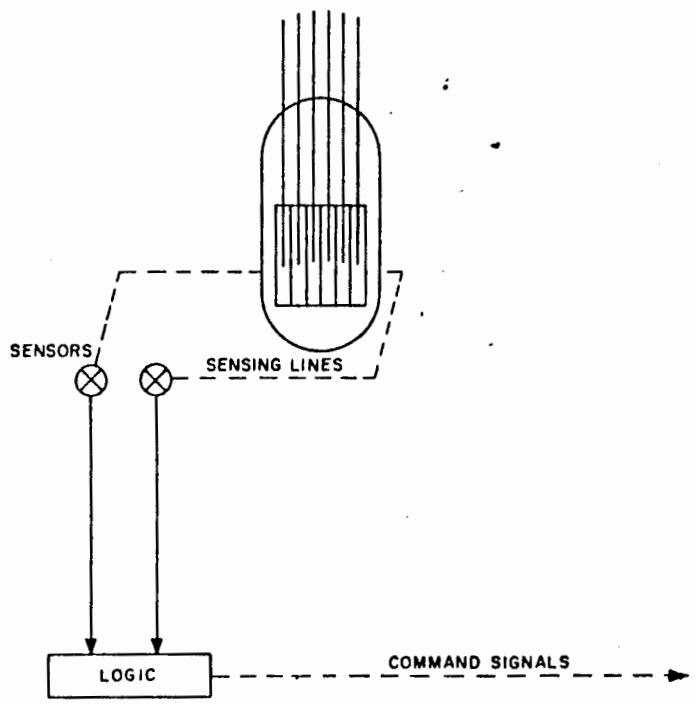


Figure 3.9 "Sense & Command Features of ECCS"

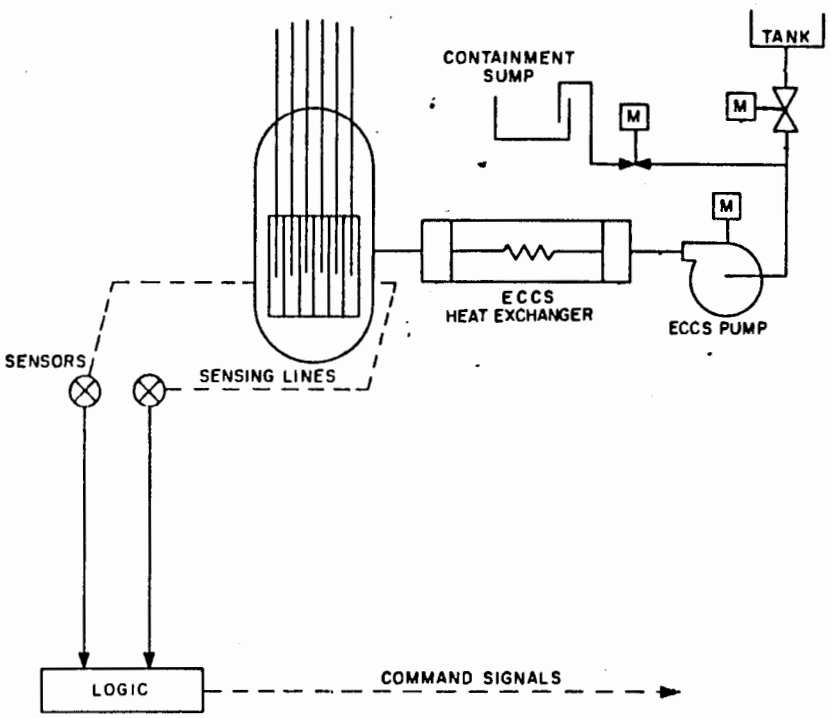


Figure 3.10 "Execute Features of the ECCS"

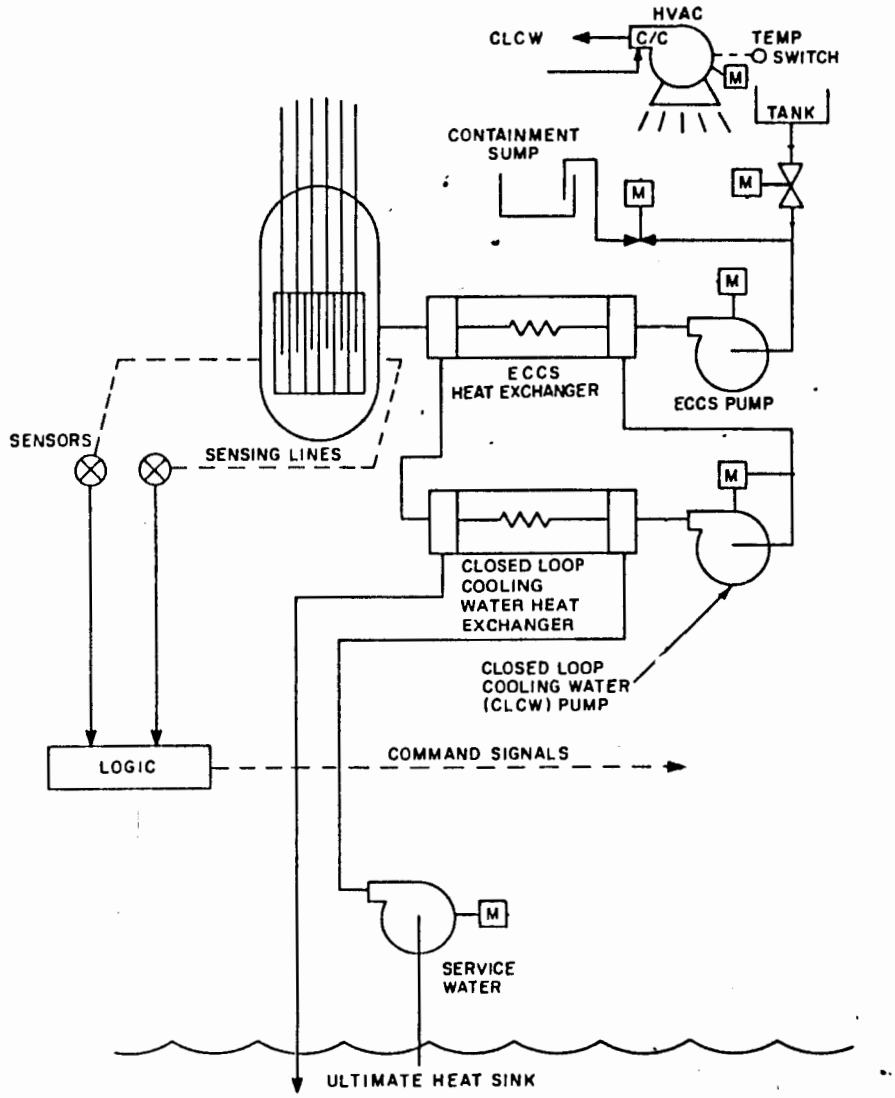


Figure 3.11 "Auxiliary Support Features of ECCS"

Service Water system are used to transfer heat from the Emergency Core Cooling System heat exchanger.

The Emergency Core Cooling System equipment is cooled by Air Conditioning plant:- without this the Emergency Core Cooling Pump motors would overheat.

The last Auxiliary support feature added is the Class 1E power systems (Fig. 3.12). The heart of the Class 1E power system is a Diesel Generator which powers the Emergency Core Cooling System actuators when the Off-site power systems fail. The Diesel Generator generates power at Medium Voltage; the large loads are supplied at this Medium Voltage while the small loads, like the motor operated valves and air conditioning are supplied with Low Voltage. The Low Voltage is derived from the Diesel Generator Medium Voltage output.

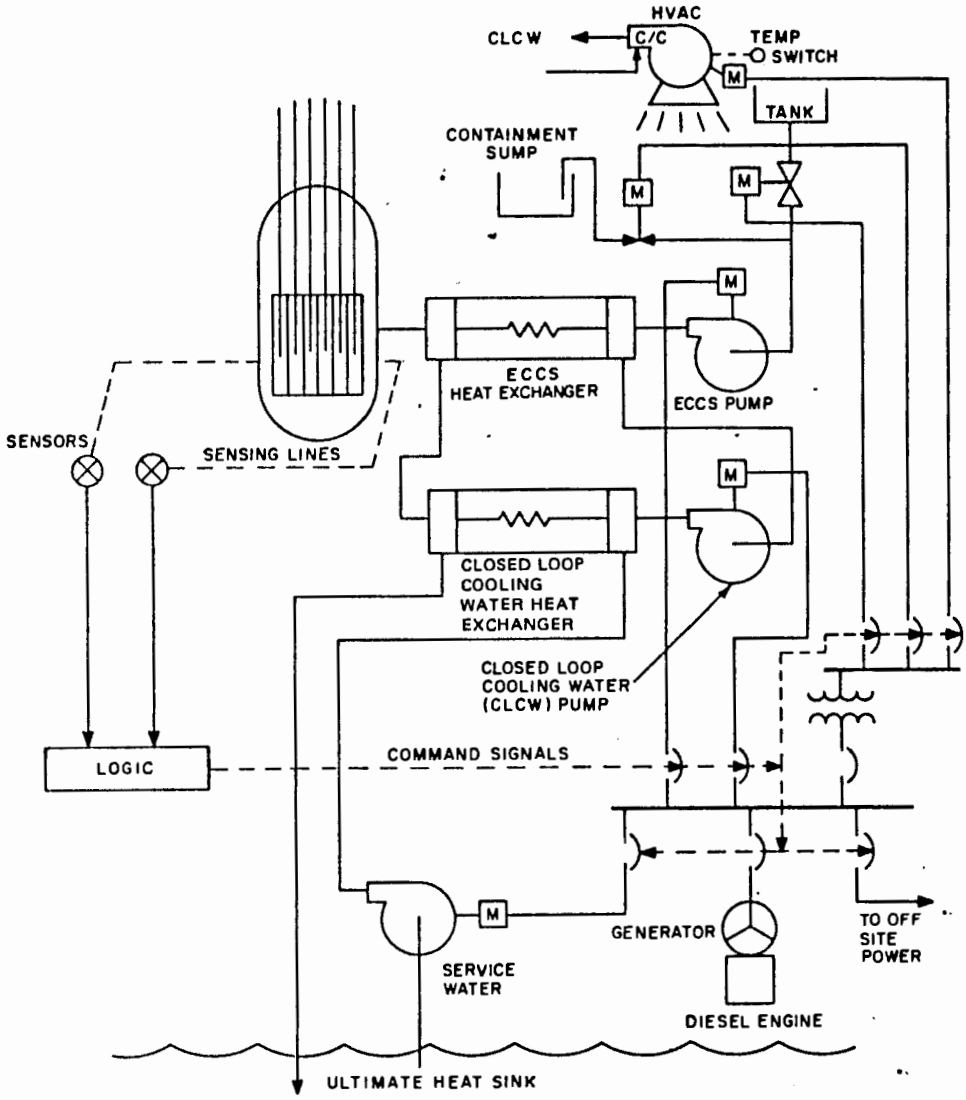


Figure 3.12 "Class 1E Power Supply Systems for ECCS"

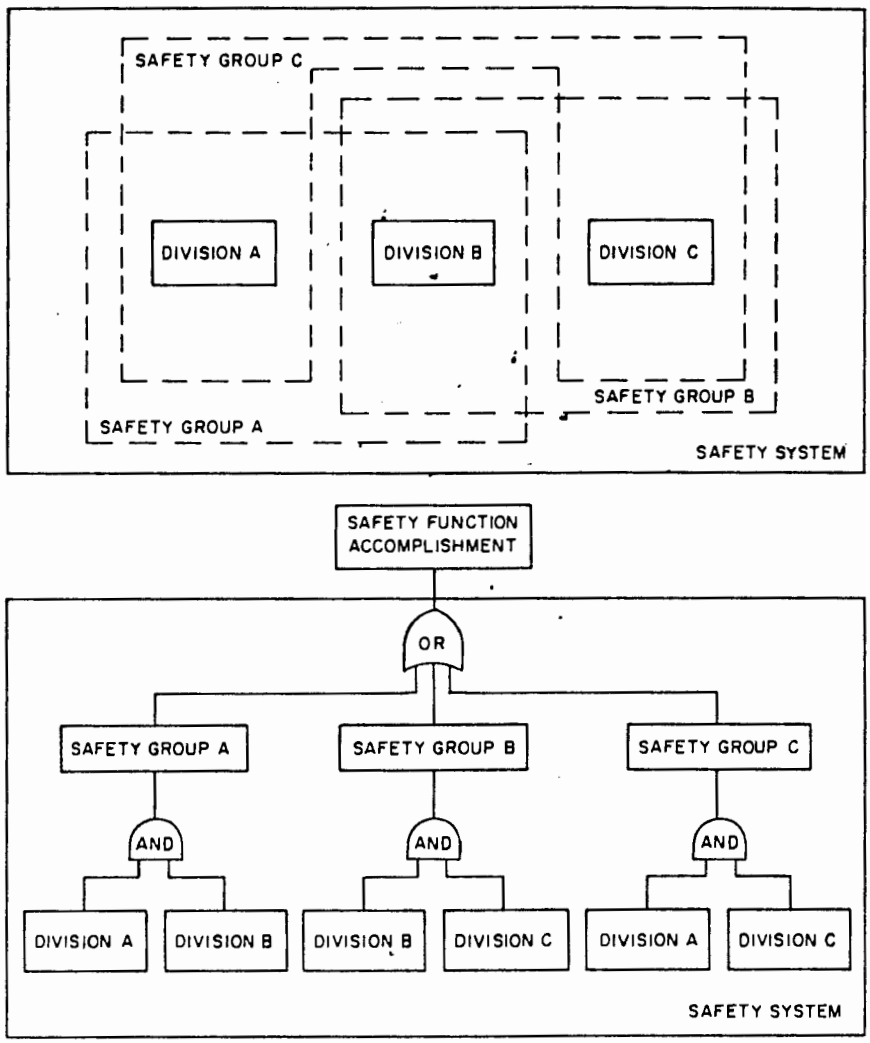
2 SAFETY SYSTEMS

A Safety system has a Safety Function:- the Safety Function for the Emergency Core Cooling System is to remove heat from the reactor after an accident. A Safety System consists of a number of redundant Safety Groups:- a Safety Group is a combination of Divisions.

If each Division has 100% capacity to fulfil the Safety Function, then in terms of the Single Failure Criterion, only two redundant Safety Groups are required.

If each redundant Division has only 50% capacity, that is, two Divisions are necessary to fulfil the Safety Function, then in terms of the Single failure Criterion, three redundant Divisions forming three Safety Groups are required. This is shown in Figure 3.13:- a single failure in one Division inhibits two Safety Groups, but the remaining Safety Group is able to complete the Safety Function.

Often, four 50% capacity Divisions are installed:- three are necessary for the safe operation of the plant while the fourth can be tested and maintained. Thus, all divisions can be tested and maintained frequently by swapping around the spare Division.



NOTE: Each division consists of a 50% capacity system. Therefore, two divisions are needed for each safety group to accomplish the safety function.

Figure 3.13 "System Safety Function with three 50% Divisions"

3.4 Summary

Over the years, as people have tried to make equipment more reliable, techniques have been developed to:-

1. Measure equipment reliability.
2. Control the Design process.
3. Control the Manufacturing process.
4. Control Equipment Inspection and Testing
5. Control the Installation of Equipment.

Designers have developed configuration strategies to ensure a better reliability:-

1. Components are over-rated.
2. Systems are divided into redundant divisions which are independent.
3. Equipment is tested regularly to ensure operability.

For Nuclear Power Plants, special techniques have been developed to assure reliability:-

1. The Single Failure Criterion is used to determine the configuration of systems important to safety.
2. Probabilistic Risk Assessment is used to assess the overall reliability of systems.
3. Equipment is Qualified to assure that it will operate under the special Environmental and Seismic conditions present in Nuclear Power Plants.

Thus methods have been developed to make equipment that is reliable for use in commercial Nuclear power reactors and techniques have been developed that measure the risk posed to the public by these Nuclear Power Plants.

The American Nuclear industry has generated a large body of documentation to define and control the use of commercial Nuclear power. Specifically, the Institute for Electrical and Electronic Engineers has developed Specifications for the Electrical and Electronic equipment used in Nuclear Power Plants.

4. Electric Power Systems in Nuclear Power Plants

At this point the reader has had an introduction to Nuclear Power Plant systems and the special requirements for Nuclear Power Plants. The details of the electric systems at a typical Pressurized Water Nuclear Power Plant will be discussed in this chapter. The emphasis will be to see how these special requirements for Nuclear plants dictate the configuration and design of the electrical equipment.

The major electric loads in a typical Pressurized Water Nuclear Power Plant will be compiled and the equipment function classified, that is, whether the load is part of the Engineered Safety Features, or not.

4.1 Electric Power Loads

The electric loads differ depending on the power station operating state. Three general plant states can be defined:- the Normal plant operation is the state the plant is in for most of its life, that is, generating electric power. When it is off load for the refuelling of the Nuclear reactor, the plant is in the Refuelling, or Outage state, and when something goes wrong in the Nuclear related part of the plant, it is in an Accident state.

The major electric loads in a typical Westinghouse Pressurized Water Reactor, classified by Plant State, are now presented [29][30].

29. Electricite de France, "PALIER-900," Information brochure, June 1982.

30. Electricite de France. "EDF 900 MWe NUCLEAR POWER PLANTS, SHORT TECHNICAL DESCRIPTION." issued by Service d'Equipment Nucleaire Exterieur, 11-13 Avenue de Friedland, 75008 PARIS, May 1983.

4.1.1 Normal Plant Operation

The primary function of a generating plant is to produce electrical power of a specified quality. In normal operation, the plant should be reliable:- a plant that is always breaking down is not very economic. The degree of reliability required for any generating plant is determined from economical considerations.

4.1.1.1 Electric Loads in the Nuclear Systems

The major electric loads on the Nuclear part of the plant during Normal operation are:-

1. Three Reactor Coolant pumps, each absorbing 7200 kW at Medium Voltage (6.6 kV).
2. Two High Head Safety Injection pumps, each absorbing 710 kW at Medium Voltage.

4.1.1.2 Electric Loads in the Conventional Systems

The major electric loads on the Turbo-generator during normal plant operation are:-

1. Three Condensate pumps, each absorbing 3 500 kW at 6.6 kV.
2. Three Drainwater pumps, each absorbing 3 000 kW at 6.6 kV
3. Two Circulating Water pumps, each absorbing 3 000 kW at 6.6 kV.

4.1.2 Plant at Refuelling Shutdown

The main electric loads during the refuelling shutdown are:-

1. Two Residual Heat Removal pumps, each absorbing 355 kW at 6.6 Kv.

4.1.3 Plant under Accident Conditions

The Engineered Safety Features require power in Accident Conditions. The principle electric loads in the Engineered Safety Features are:-

1. Two High Head Safety Injection pumps each absorbing 710 kW.
2. Two Low Head Safety Injection Pumps each absorbing 250 kW.
3. Two Containment Spray pumps each absorbing 450 kW.
4. Ventilation Systems totalling 1000 kW.
5. Four Service Water pumps each absorbing 225 kW.
6. Four Component Cooling Pumps each absorbing 400 kW.

4.2 Powering these Loads

We have seen that there are three distinct categories of electric load on a typical Nuclear Power Station:- those loads needed only during normal operation, those needed during the refuelling shutdown, and those needed in the event of an accident.

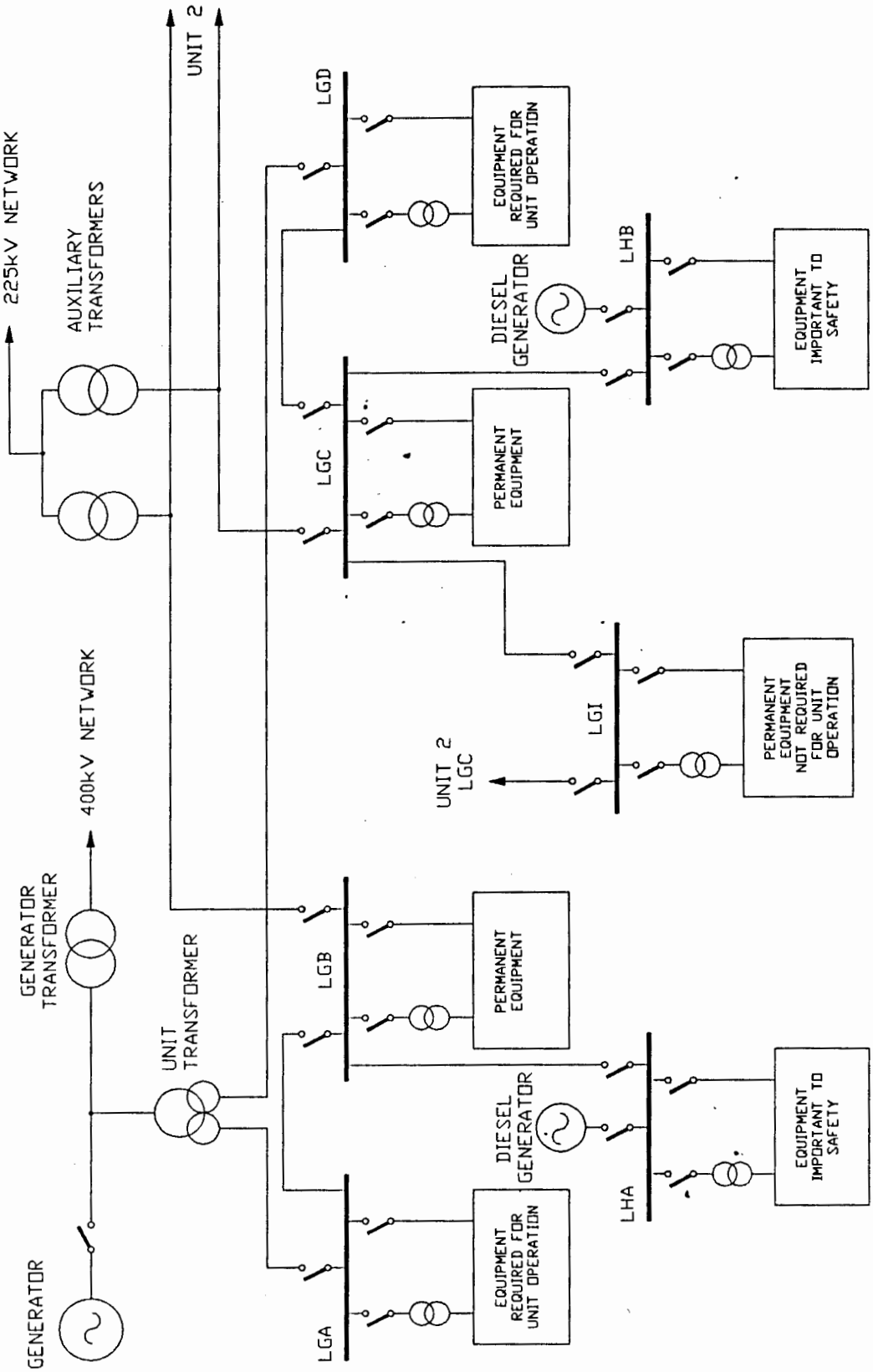


Figure 4.1 "Typical Electrical Power System Layout"

lead to a significant risk increase during Refuelling Outages.

In the intermediate stages when the plant is shut-down but the Primary Coolant System is not yet opened for Refuelling, the Engineered safety Feature systems are kept available to remove decay heat in an Emergency situation.

Thus during the Refuelling outages when all the Fuel has been removed from the Reactor Vessel, the Engineered Safety Feature switchboards are supplied from the Permanent supplies allowing the Diesel Generator sets to be serviced.

An alternate source of ac power is provided via the Auxiliary transformers. These can supply the Permanent Equipment Boards if there is a transfer between the Unit transformer source (LGA) and the Auxiliary transformers. Thus, during the outage when the Generator is off-line, the Permanent loads are supplied via the Auxiliary transformers.

In the event of an accident, the Engineered Safety Features draw electric power from the Safety Related Switchboard (LHA). The power for this board can be sourced from either the Generator if it is operating, or from the Auxiliary Transformers, or from the Diesel Generators. Thus, even if the off-site power fails, the Diesel Generators will still supply the Equipment important to safety.

The description above describes only one Safety Division, or Train. There is another identical redundant Train which supplies Equipment required for Normal, Permanent, or Safety-related operation (LGD, LGC, and LHB).

Figure 4.2 shows where the loads described in Section 4.1 are connected to the system.

The low voltage ac power is used to supply small loads:- typically, loads with power ratings of less than 160kW. Examples are valve actuators and small motors.

The dc system provides power for equipment control:- switchgear control, diesel generator control, and Auxiliary Feedwater system control. The dc system also supplies power via inverters to the Vital Instrumentation and Control ac busses which power the Reactor Protection Systems.

The electric system layout described meets the Regulatory requirements of 10CFR50 Appendix A as there are two physically independent sources of power from the off-site grid, and there are two onsite diesel generators to provide emergency power in the event of off-site power loss. The onsite system is divided into two independent and redundant Divisions or Trains.

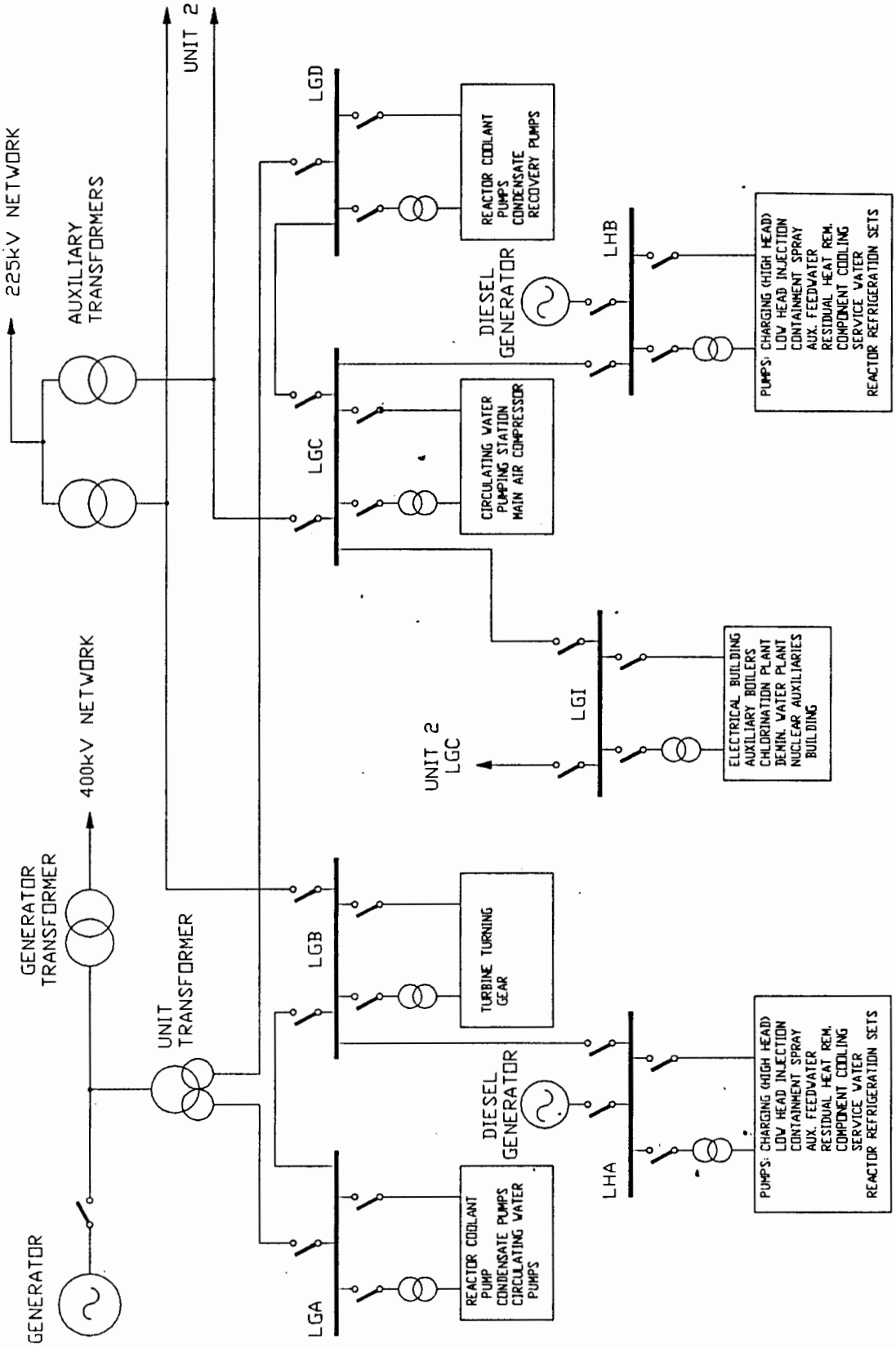


Figure 4.2 "Connection of Major Loads to Power Supply System"

4.2.2 The Alternating Current Power Systems

The parts of the electric power supply system will now be discussed and the Regulatory requirements described.

4.2.2.1 Floating Neutral

Not using Direct Grounding the neutral in the Medium voltage systems has certain advantages [33]:- the distribution system can tolerate one earth fault without the need to isolate the faulty cable or piece of equipment. The plant availability is therefore enhanced. The neutral grounding resistors are sized to absorb the maximum power developed from the capacitive currents which flow when one phase is grounded. The high resistance neutral resistor also minimizes the transient voltages caused by arcing grounds and, by limiting the current flow, the fault does not cause so much damage.

Typical maximum earth fault currents are 35 Amperes on 12 kV systems and 7 Amperes on 4.16 kV systems.

4.2.2.2 The Diesel Generator Sets

The requirements for Diesel Generators at Nuclear Power Plants are set down in the IEEE Standard 387 "Criteria for Diesel Generator Units applied as Standby Power Supplies for Nuclear Generating Stations" [34]. Essentially, the diesel generator set must be physically independent from the power station, and electrically independent from the off-site power supply system.

---

33. Nielsen,D. "AUXILIARY POWER SYSTEM FOR THE DIABLO CANYON NUCLEAR PLANT," IEEE Power Engineering Society Summer Meeting (Text of A Papers), Portland, ORE, USA, 18-23 July 1976, pages A76 300-4/1-5.
34. Report IEEE Standard 387 "IEEE STANDARD CRITERIA FOR DIESEL-GENERATOR UNITS APPLIED AS STANDBY POWER SUPPLIES FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1977.

The block diagram of a typical Diesel Generator set is given in Figure 4.3:- typically the Generator can produce about 5000 kVA at Medium Voltage.

Special features of Diesel Generators used for Emergency Power Generation at Nuclear Power Stations are:-

1 Dual Starting Systems

To make the start-up process more reliable, the diesel has two starting systems:- one is a pneumatic turbine powered by compressed air, and the other is a direct feed of compressed air into the engine cylinders. In addition, the diesel is always kept warm by keeping the water cooling system warm.

2 Reliable Cooling Systems

Some diesel configurations use an air cooling system consisting of force draft cooled radiators to remove the diesel engine heat losses. Others use a heat exchanger cooled by the plant Service Water System. The disadvantage of this is that the diesel will overheat of the Service Water system fails.

3 Automatic Loading of the Diesel Generator

On receipt of a Engineered Safety Feature actuation signal, the Diesel engine starts up and all electric loads on the Engineered Safety Feature switchboard (LHA) are disconnected. The incomer from the Permanent supplies is also opened. After 10 seconds the Diesel is at rated speed and the Diesel incomer

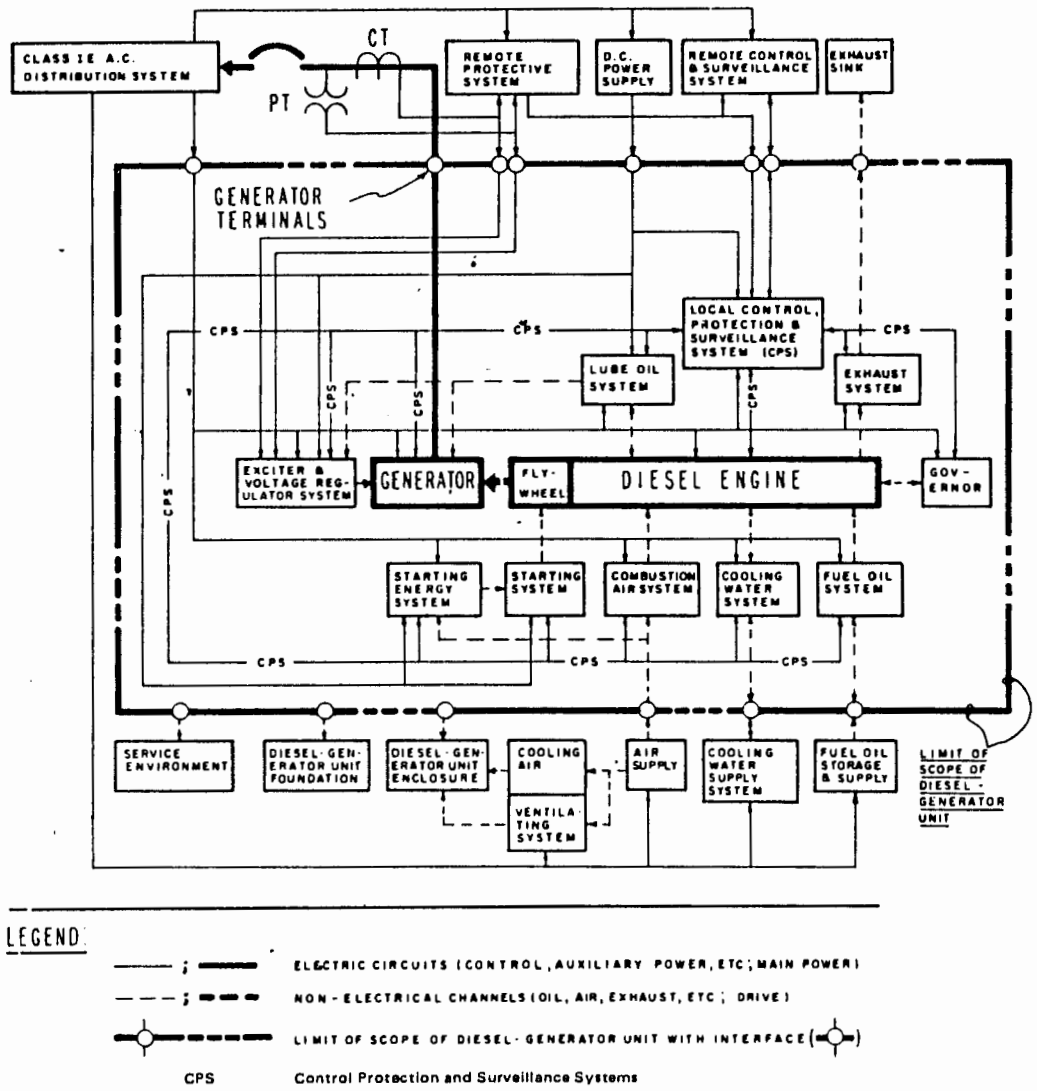


Figure 4.3 "Typical Diesel Generator Layout

to the Engineered Safety Feature switchboard is closed.

The loads are re-connected in blocks so that the Diesel Generator output voltage and frequency do not vary excessively.

4 Periodic Testing

The principle of periodic testing is used to ensure that the diesels are reliable. The IEEE standard recommends that the Diesel Generator be tested on load at least once per month. The diesel control logic allows automatic switch-over from the test mode to the operating mode if the Engineered Safety Feature actuation signal occurs while the Diesel is being tested on load.

4.2.2.3 The Preferred Power Supply.

The IEEE Standard 765 "Preferred Power Supply for Nuclear Power Generating Stations" [35] is provided to give detailed design criteria for the Preferred Power Supply and expands on the requirements given in 10CFR50 and in IEEE Standard 308 "Standard Criteria for Class 1E Power Systems".

The Preferred Power Supply should consist of at least two independent circuits from the off-site transmission system connected to the Class 1E power distribution system. Figure 4.4 shows a typical configuration. The Preferred Power Supply is not a Class 1E system and therefore does not need to meet the Class 1E requirements for redundancy, independence, separation, the single Failure Criterion,

35. Report IEEE Standard 765 "IEEE STANDARD FOR PREFERRED POWER SUPPLY FOR NUCLEAR GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1983.

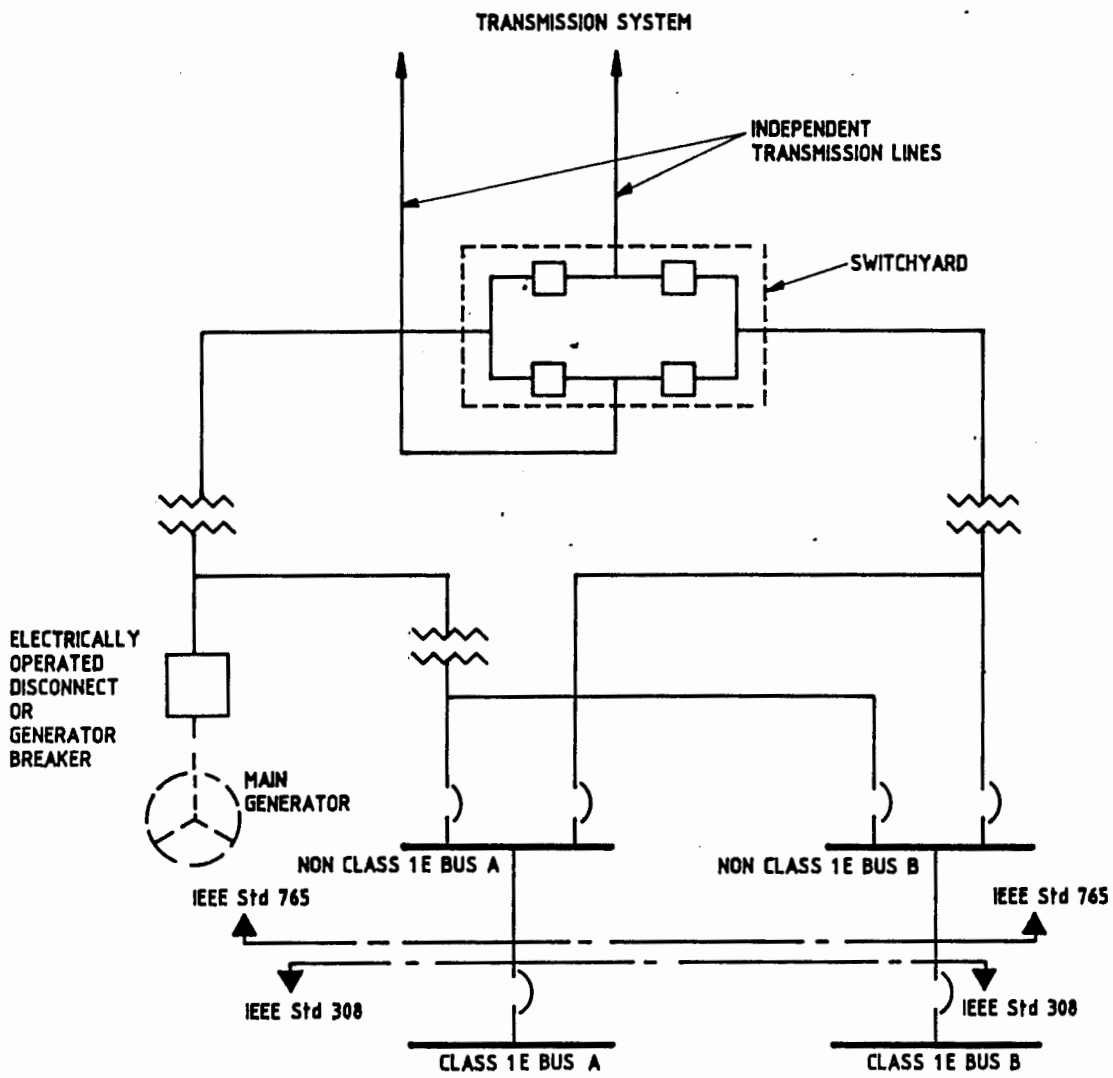


Figure 4.4 "Typical Layout of Preferred Power Supply"

Seismic and equipment qualification. This does not mean that the use of physical independence or any of the other criteria for reliability used for Class 1E equipment cannot be used for the Preferred Power Supply:- the application there-of is determined using a cost-benefit analysis.

A typical layout of a Preferred Power Supply for a French 900 MW station is shown in Figure 4.1. The generator electric output is transformed to 400kV and carried to the 400kV switchyard where the power joins the Grid network. The Unit auxiliaries are powered by a Unit auxiliary transformer.

The alternate (Backup) off-site power supply is taken from the 225kV switchyard and transformed to 6.6 kV by two auxiliary step-down transformers.

The reliability of the Off-site grid network is very much dependent on the grid configuration. In the United States of America, the probabilities for the loss of Off-site power are as follows [36]:-

Type of Failure	Failures per Year
Loss longer than 30 minutes	0.041
Loss less than 30 minutes	0.044
Loss of Backup off-site power but not Normal power.	0.012
Loss of Normal supply, but not Backup power.	0.056

The reliability of the grid network is improving because plants with repetitive problems have implemented major corrective actions, and because as more plants are added to the grid network the number of interconnections grows.

In the winter of 1983/84, Sweden had a major failure in its grid network which resulted in the loss of 40% of the countries electric loads [37]. None of the Nuclear plants in Sweden managed to transfer successfully to House Load mainly due to the nature of the grid disturbances and deficiencies in the adjustment of the House Loading systems. The Engineered Safety Feature Diesel Generators were used to supply the critical plant loads in the power stations and all Diesels started successfully. But the fact that the Nuclear stations did not House Load and were therefore unable to quickly pick up load again after the incident was noted by many laymen in Sweden.

---

36. Wyckof,H. "LOSS OF OFF-SITE POWER EXPERIENCE AT U.S. NUCLEAR POWER PLANTS-ALL YEARS THROUGH 1984", Proceedings of the American Power Conference, Chicago,Il,USA, 22-24 April 1985, pp 791-6.

37. Reisch, F. "TECHNICAL NOTE: SWEDEN'S DECEMBER 1983 GRID COLLAPSE AND THE NUCLEAR POWER PLANT'S RESPONSE", Nuclear Safety, Vol.26, No.2, March/April 1985, pp 153-6.

4.2.3 Direct Current Power Sources

The IEEE provide a standard summarizing the requirements for the design, qualification, maintenance and testing of Safety-related dc power systems. It is the IEEE Standard 946 "IEEE Recommended Practice for the Design of Safety Related DC Auxiliary Power Systems for Nuclear Power Generating Stations" [38].

Typical dc system loads are Circuit breakers, Relays, Solenoids, and Inverters. In terms of the Class 1E power system criteria, each safety-related Division should have its own independent dc power supply system. The dc power can be provided by one battery, or two batteries can be used:- one for power circuits and the other for control loads.

Supplying non Class 1E loads from the Safety-related dc power supplies is discouraged as these loads are not Qualified and could, for example, cause a short circuit on a Class 1E dc busbar if the supply breaker should fail to trip. There are, therefore, non Class 1E batteries at Nuclear power Stations which are used to supply loads on the Turbo-generator set, the High Voltage Switchyard, and Emergency Lighting for example.

In addition to the Safety-related batteries provided for each Division of the Engineered Safety Features, Safety Related batteries are provided for the Reactor Protection System as well. The reason is that this protects the Reactor from unnecessary transients that could occur if spurious power failures caused the Reactor Protection System to trip the reactor, or even initiate a Safety Injection.

---

38. Report IEEE Standard 946 "IEEE RECOMMENDED PRACTICE FOR THE DESIGN OF SAFETY RELATED DC AUXILIARY POWER SYSTEMS FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1985.

The basic dc system configuration is shown in Figure 4.5:- the battery is on Float charge while the battery charger supplies the dc loads. The battery supplies the loads when the ac power to the charger fails, or when the peak load on the battery charger exceeds the maximum charger output. The battery chargers for Safety-related dc systems are supplied with power derived from the Diesel backed Emergency power distribution boards.

4.2.3.1 Batteries

Lead-acid batteries are used extensively in power stations because they are relatively cheap and are made in large sizes. A typical pasted plate lead-acid battery is shown in Figure 4.6. The plate consists of a lead-alloy grid which has openings for the porous lead active material. The lead-alloy is used to give mechanical strength to the plate and to provide an efficient conduction path for the electricity.

These batteries are, however, not perfect. Three side reactions affect the efficiency and life of Lead-acid batteries [39]:-

1. The decomposition of water resulting in Oxygen and Hydrogen. The equilibrium voltage for this reaction is 1.23 Volts. Even though the open circuit voltage of Lead-acid cells is about 2.0 Volts, the rate of Hydrogen and Oxygen generation is extremely low. The end result of this process is the loss of water from the cell.

---

39. Berndt,D. "STATIONARY LEAD ACID BATTERIES, OPERATIONAL CONDITIONS, FUTURE ASPECTS," presented at Symposium on Standby & Uninterruptable Power Supplies, organized by South African Institute of Electrical Engineers and The Association of Municipal Electricity Undertakings of South Africa, 17 to 18 September 1986, paper I1.

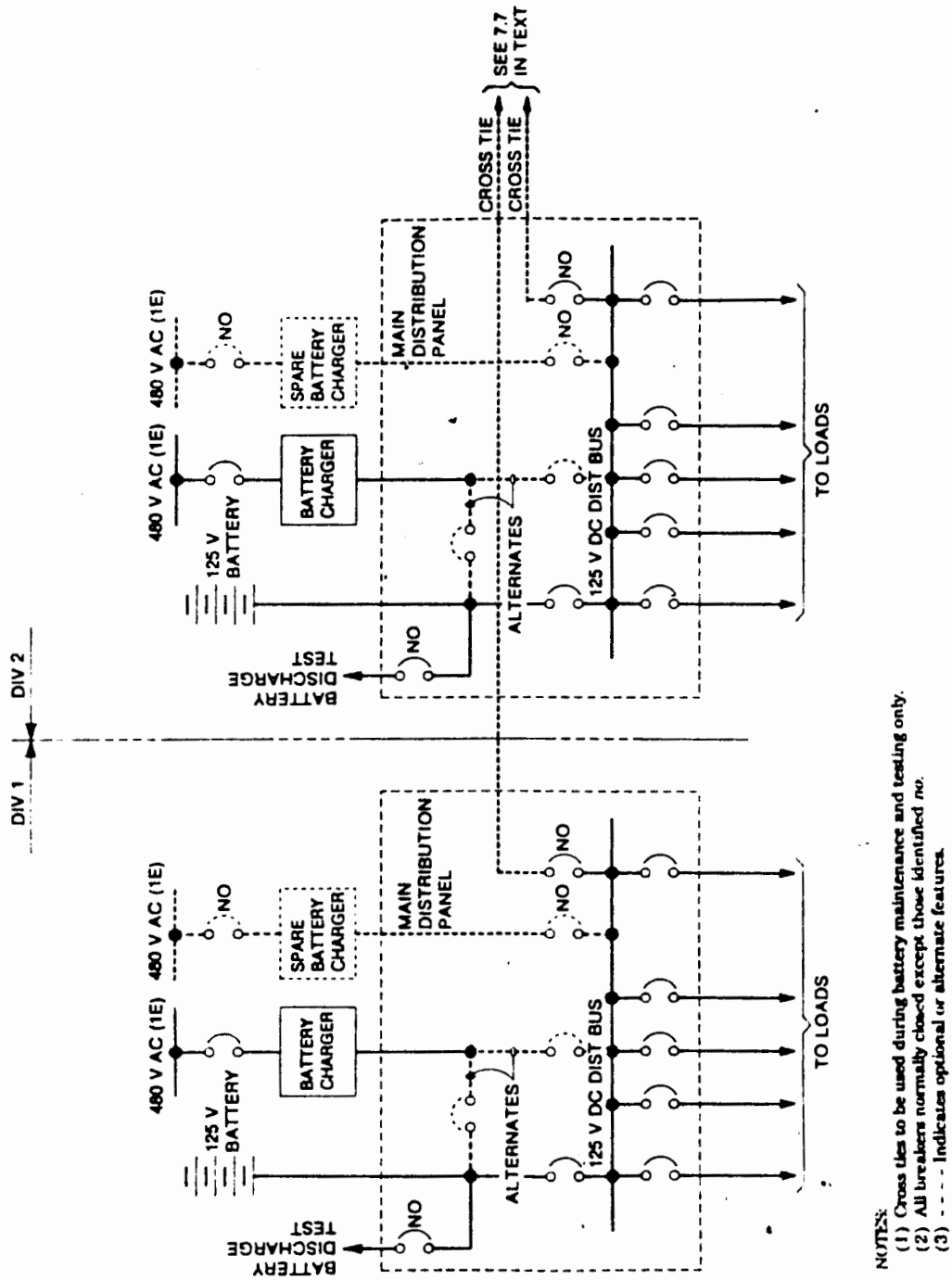


Figure 4.5 "Schematic of Direct Current System"

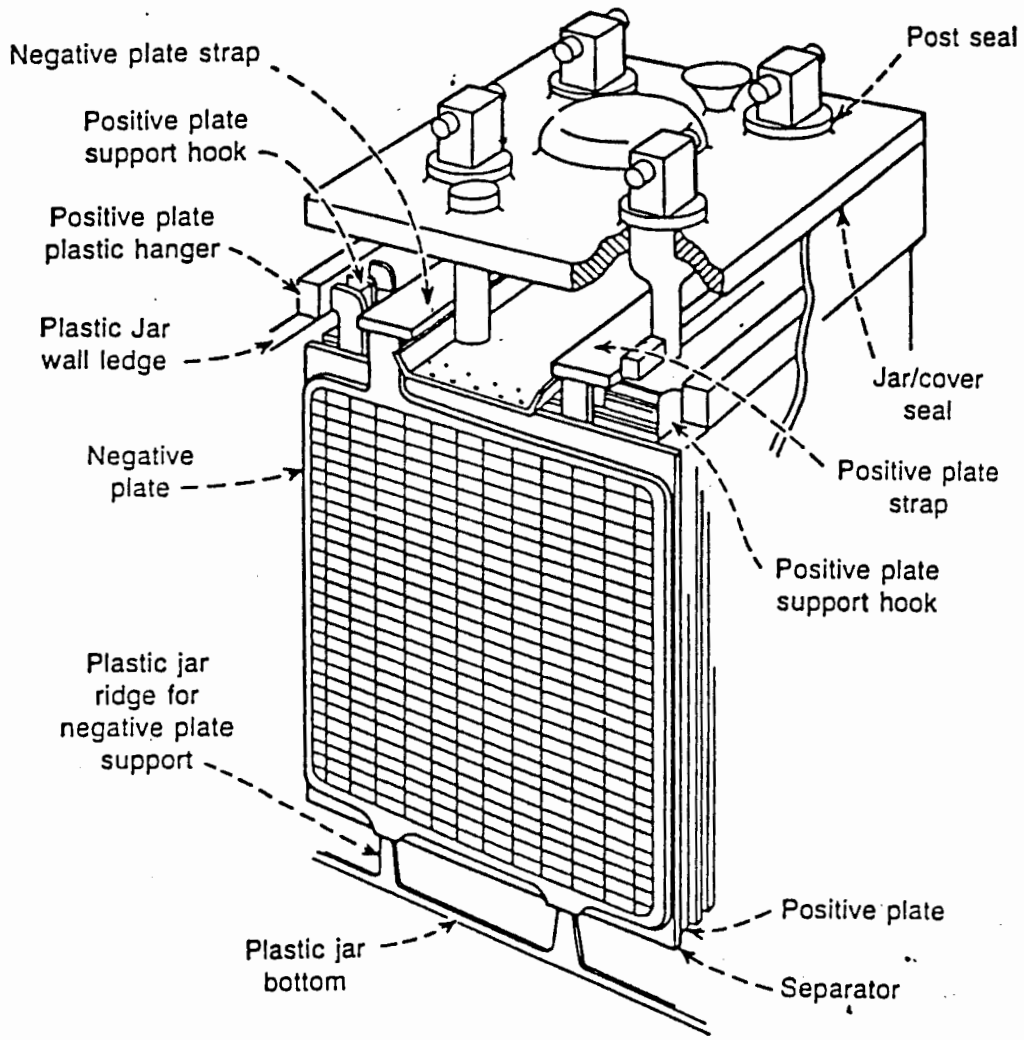


Figure 4.6 "The Pasted Plate Lead-acid Cell"

2. The Hydrogen generated by the decomposition of water, even though at a low rate, does affect the negative electrode of the cell:- this electrode supplies the electrons needed for the Hydrogen evolution and consequently results in the gradual discharge of the electrode. This is known as the "self-discharge" of the lead acid cell, and is the reason that lead-acid cells need constant recharging. Cells are "Float" charged at a constant voltage sufficiently high to counteract the "self discharge" and keep the electrodes charged.

3. The corrosion of the Cell internals. Most of the cell conducting parts contain lead and where the lead is part of the positive electrode, the Sulphuric Acid of the cell gradually eats the lead away. The reactions are complex, but typically result in the corrosion loss of 1 to 2% of the lead in the positive electrode per year.

Thus the maintenance of lead acid batteries essentially consists of floating the cells at a suitable voltage to overcome the self-discharge phenomenon and topping up the cell electrolyte level with water to replace that lost due to the decomposition of water.

The sizing of the batteries is discussed in the IEEE Standard 485 "IEEE Recommended Practice for Sizing Large Lead Storage Batteries for Generating Stations and Substations" [40] and is dependant on a number of factors.

The first step is to determine how long the dc loads need to be supplied with power in the event of an ac power failure. The configuration and reliability of the power station ac power system is used in this evaluation:- how

40. Report IEEE Standard 485 "IEEE RECOMMENDED PRACTICE FOR SIZING LARGE LEAD STORAGE BATTERIES FOR GENERATING STATIONS AND SUBSTATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1983.

long will it take to restore ac power to the Safety-related battery chargers? How many Diesel generators are there and is there sufficient flexibility in the ac distribution network to allow Cross-ties between distribution boards? Or are there cross-ties in the dc systems?

The process of determining the required dc supply duration therefore involves previous operating experience with different network configurations, and Engineering judgement.

Once the supply duration is established, typically between 0.5 hours and 4 hours, the battery duty cycle for that period must be determined. Usually, a number of scenarios will become apparent depending on the type of equipment failure causing the power loss, and these will form the final battery duty cycle. The battery is sized to meet the power requirements of the loads (as defined by the duty cycle) for the duration determined by the plant configuration and equipment reliability.

The IEEE recommendations for installation of batteries are contained the IEEE Standard 484 "IEEE Recommended practice for Installation Design and Installation of Large Lead Storage Batteries for Generating Stations and Substations" [41].

The location of the battery is discussed:- for example, the location should be free from vibration, be clean and dry, not have large temperature variations, and water rinsing facilities should be provided to was off spilt acid. The mounting of the battery is commonly in a single tier steel rack with the cell bases isolated from the floor with porcelain insulators.

---

41. Report IEEE Standard 484 "IEEE RECOMMENDED PRACTICE FOR INSTALLATION DESIGN AND INSTALLATION OF LARGE LEAD STORAGE BATTERIES FOR GENERATING STATIONS AND SUBSTATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1981.

The ventilation of the battery room should limit the hydrogen accumulation to less than 2% under all operating conditions.

The IEEE recommendations for maintaining, testing and replacing lead acid batteries is contained in the IEEE Standard 450 "Recommended Practice for Maintenance, Testing, and Replacement of Large Lead Storage Batteries for Generating Stations and Substations" [42].

Maintaining batteries is an art:- the detailed operation of lead acid cells is still not completely understood and to detect deterioration in cells is not easy. The battery is at Float charge most of the time between Unit Outages with monthly Equalizing charges. The duration between outages is typically 12 months extending up to 18 months in some cases [43]. There is no opportunity to "work" the cells by performing discharges and complete charging while the Unit is on-line so the potential for gradual discharge is high. The French battery supplier for the cells at Koeberg Nuclear Power Station recommends a discharge-charge cycle at least once a year; the more frequent, the healthier the battery [44]. Thus, the operational and maintenance requirements cannot be simultaneously satisfied.

---

42. Report IEEE Standard 450 "RECOMMENDED PRACTICE FOR MAINTENANCE, TESTING, AND REPLACEMENT OF LARGE LEAD STORAGE BATTERIES FOR GENERATING STATIONS AND SUBSTATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1980.
43. Electricite de France. "EDF 900 MWe NUCLEAR POWER PLANTS, SHORT TECHNICAL DESCRIPTION." issued by Service d'Equipment Nucleaire Exterieur, 11-13 Avenue de Friedland, 75008 PARIS, May 1983. Page 59.
44. Tudor representative, verbal communication, February 1987.

A typical monthly battery maintenance inspection would include:-

1. A visual inspection of the cleanliness of the installation.
2. Charger output voltage and current.
3. Electrolyte levels.
4. Visual inspection for cracks or electrolyte leakage.
5. Ambient temperature and operation of ventilation.
6. Pilot cell voltage and specific gravity.

The three monthly inspections include all the monthly activities as well as:-

1. The terminal voltage and specific Gravity of each cell.
2. The electrolyte temperature of selected cells.

At the Unit Outage, the intercell connections are re-torqued and a qualification discharge is done on the battery. The battery is replaced if the Capacity is 80% of the manufacturer's rating.

Using Specific Gravity to ascertain the cell state of charge is fraught with problems. A Specific Gravity gradient may exist in cells that are charged at high currents:- the high Specific Gravity acid generated during the charging sinks to the bottom of the cell. When the Specific Gravity is measured (at the top of the cell), a low value is indicated which will gradually increase as the diffusion process equalizes the Specific Gravity gradient.

A similar effect occurs when water is added to the cell to make up for water lost during Float operation:- the water dilutes the electrolyte near the top of the cell and misleading Specific Gravities can be measured.

Other small difficulties encountered when measuring Specific Gravity are that the temperature of the electrolyte affects the Specific Gravity, and the level of the electrolyte in the cell also affects the Specific Gravity:- the lower the level, the more concentrated the chemicals in the electrolyte become, and the Specific Gravity therefore increases.

The applicable IEEE Standard for the Qualification of Lead-acid cells is:- IEEE Standard 535 "IEEE Standard for Qualification of Class 1E Lead Storage Batteries for Nuclear Power Generating Stations" [45].

Lead acid batteries for use in Nuclear Power Plant are qualified in terms of the chemical and physical deterioration due to aging, and in terms of their ability to withstand postulated earthquakes. Qualification can be done by three methods, that is:- Type Testing, Operating Experience, and Analysis.

At the present state of the art, the IEEE cautions against using mathematical modelling of aged cells as the processes are complex.

Cells to be qualified by Type testing are aged either naturally or by an accelerated aging process. The accelerated aging process consists of keeping the cells at an elevated temperature for a defined period of time. Tubular cells, for example, are aged by one year for every 23 days they are kept at 71 deg.C. The actual qualification test is performed on the aged cells and basically consists of a stringently controlled 3 hour discharge which establishes the cell capacity.

---

45. Report IEEE Standard 535 "IEEE STANDARD FOR QUALIFICATION OF CLASS 1E LEAD STORAGE BATTERIES FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1979.

The aged cell Seismic withstand capability is tested on a shake-table with a representative load current flowing during the test. Any fluctuations in the cell's voltage or current indicate a weakness in the cells under test. After the Seismic test, the cells are again capacity tested with a 3 hour discharge.

The battery rack is also qualified for Seismic events. However, the rack can be qualified by analysis as well as in a shake test.

4.2.3.2 Battery Chargers

The IEEE requirements for Class 1E battery chargers are contained in the IEEE Standard 650 "IEEE Standard for Qualification of Class 1E Static Battery Chargers and Inverters for Nuclear Power Generating Stations" [46]. The battery charger must supply the continuous design dc load of the battery (which is the dc board load) and must also supply a certain current to charge the battery as well. Typically this is 10% of the batteries 8 hour ampere-hour rate:- if the battery is a 1000 Ah, then the charging current that must be provided by the charger is 100 Amperes.

Three types of battery chargers are commonly used on American Nuclear Power Plants:- The Silicon Controlled Rectifier solid state type, the controlled ferro-resonant type, and the magnetic amplifier type. The Silicon Controlled Rectifier type comprise some 75% of the chargers used and is the only type now Qualified for Class 1E use [47].

---

46 Report IEEE Standard 650 "IEEE STANDARD FOR QUALIFICATION OF CLASS 1E STATIC BATTERY CHARGERS AND INVERTERS FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1979.

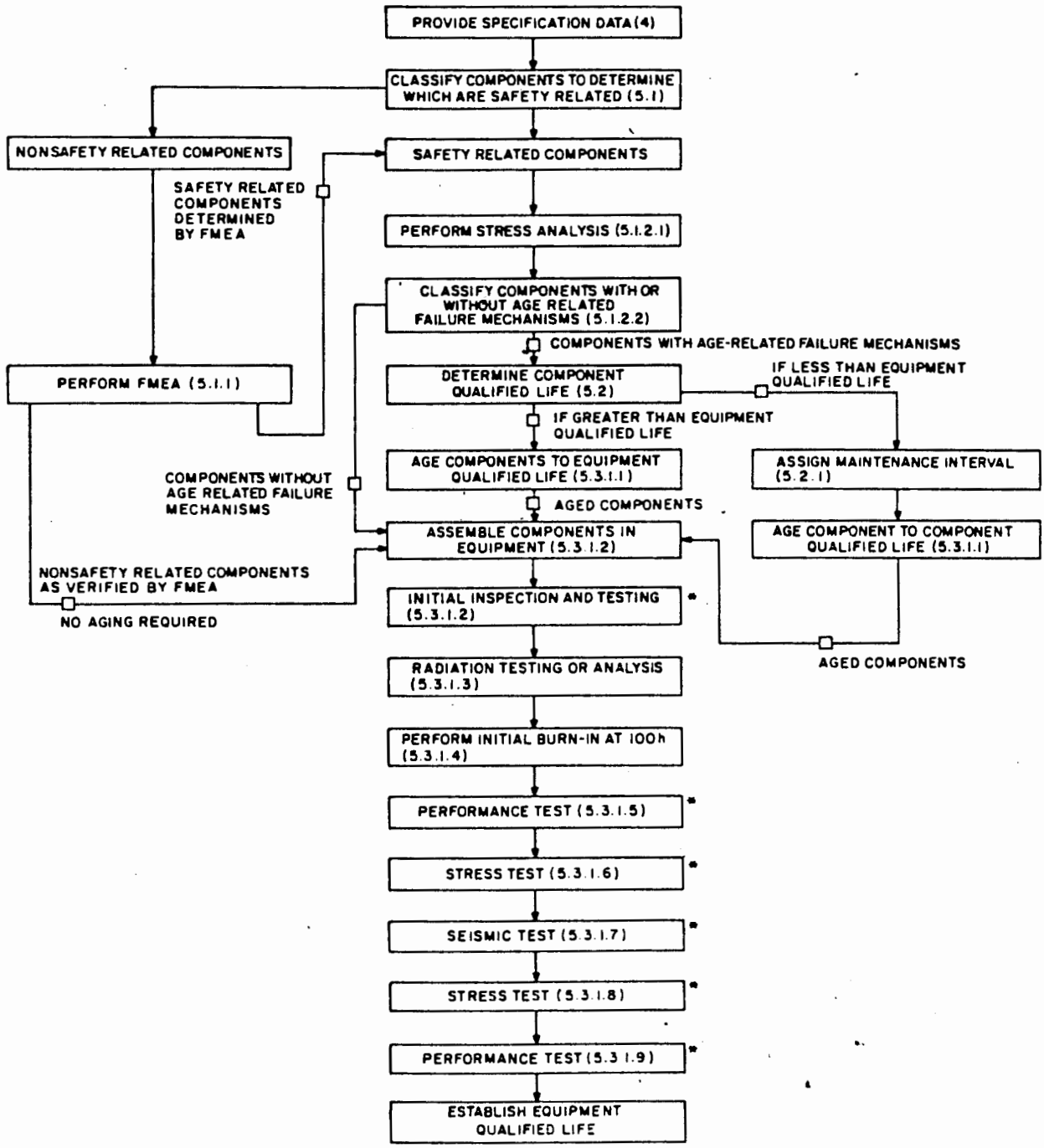
47. Gunther,W.E., Subudhi,M.,and Taylor,J.H. "OPERATING EXPERIENCE AND AGING-SEISMIC ASSESSMENT OF BATTERY CHARGERS AND INVERTERS", NUREG/CR-4564, US Nuclear Regulatory Commission, June 1986. Page 2-1.

The design of Silicon Controlled Rectifier battery chargers is not complex, but the qualification process is extensive. Figure 4.7 shows the IEEE Flowchart for Qualification of Class 1E Battery Chargers and Inverters. Essentially, the Safety-related parts are identified by Engineering Judgement and by a Failure Modes and Effects Analysis. Of the Safety-related components, those that have age-related failure mechanisms are identified and aged. All components are then assembled into the Battery Charger and the charger then undergoes the following tests in order:-

Initial functionality tests
Radiation Testing
100 Hour Burn-in test
Performance Test
Stress Test
Seismic Test
Stress Test
Performance Test.

The Performance test is done at room temperature and humidity. The Stress test is done with the temperature varying between the maximum and minimum Service temperatures, while the humidity is increased to the maximum specified in the Service conditions.

Any failures are evaluated and the design changed if necessary.



*Any failure requires analysis to determine origin: common mode or random, repair, redesign, or retest, or both, using aged components as required.

Figure 4.7 "Qualification Flowchart for Class 1E Chargers & Inverters"

4.2.3.3 Inverters

An inverter converts dc power to ac power. On Nuclear Power Plants emergency ac power is typically required for the Reactor Protection System, Feedwater System Control, and Emergency Diesel Generator Auxiliaries [48].

Four types of Inverter are commonly used:- the ferro-resonant type which is used in about 50% of American Nuclear facilities, the pulse-width modulated type, the quasi square wave, and the step wave type. The different types represent changes in the output requirements for inverters as the input requirements for computer equipment becomes more stringent [49]

Class 1E inverters are made to the same qualification program as Class 1E Battery Chargers.

4.2.3.4 Direct Current Distribution Networks

Components in the dc distribution system are designed and rated as follows:-

1 Cables

The positive and negative cables from the battery are run in separate conduits so that any insulation fault will cause an earth fault before a polarity to polarity fault. A polarity to polarity fault would cause serious damage as there is no short circuit protection in this circuit before the distribution panel. Cables are sized to carry the prospective

48. Gunther,W.E., Subudhi,M.,and Taylor,J.H. "OPERATING EXPERIENCE AND AGING-SEISMIC ASSESSMENT OF BATTERY CHARGERS AND INVERTERS", NUREG/CR-4564, US Nuclear Regulatory Commission, June 1986. Page 1-3

49. Gunther,W.E., Subudhi,M.,and Taylor,J.H. "OPERATING EXPERIENCE AND AGING-SEISMIC ASSESSMENT OF BATTERY CHARGERS AND INVERTERS", NUREG/CR-4564, US Nuclear Regulatory Commission, June 1986. Pages 2-10 and 2-16.

short circuit current and to keep the cable voltage drop acceptable even during start-up transients. A typical start-up transient would be a dc motor in a valve actuator which can draw up to 11 times the normal load current when stalled.

2 Protective devices

Fuses and circuit breakers are rated to carry the 1 minute battery discharge current but to trip at the battery short circuit current when the battery is at the minimum design state of charge. The battery protective device shall coordinate with the downstream protective devices.

3 Loads Voltage ratings

The dc loads voltage ratings should be rated for the variation range of the battery terminal voltage. At Koeberg, the 125 Volt batteries float at 131 Volts, are equalized monthly for 40 hours at 134.5 Volts, and the end-of-discharge voltage is 106.2 Volts. The dc loads must therefore have an operating voltage rating of 125 Volts, + 10%, - 15% (taking the +/-1% tolerance of the battery charger voltage regulation into account.)

4 Surge Suppression

Highly inductive loads can generate large voltage surges when de-energized:- these should be suppressed or they could cause other dc loads to malfunction.

5 Constant Power loads.

Inverters draw a constant power and the load current required is therefore inversely proportional to the

dc input voltage. The battery should be sized to accommodate these loads.

6 Battery Testing

A discharge breaker is provided to allow convenient discharge testing of the battery.

7 Cross-ties between busses.

Cross-ties between Class 1E dc busses are permitted when the new dc source has sufficient capacity to accommodate the extra load. The new dc source must not be in the redundant safety Division and must meet all the Class 1E system requirements. If a Class 1E system is cross-connected to a non-safety battery, the continued operation of the Unit is not possible as the reliability of the Engineered Safety Features is degraded by the non-Qualified non-safety battery.

4.3 Summary

The electric power supply system of a Nuclear Power Plant typically consists of:-

1. Two independent feeders from the Off-site grid network:- the one being the Generator transformer, and the other, the Auxiliary transformers. Under Normal operating conditions the Generator and Generator transformer supply all station loads via the Unit Transformer.
2. Two independent redundant Diesel Generator sets supplying Emergency power for the Engineered Safety Features if the grid network fails and the Generator fails to House Load.
3. Lead-acid batteries supplying dc power for:-

    3.1 Controlling the Breakers and Contactors in the station electrical network.
    3.2 Controlling the High Voltage yard switchgear.
    3.3 Controlling the Diesel Generator sets.
    3.4 The Reactor Protection Systems
    3.5 The Engineered Safety Feature control systems
    3.6 Controlling the Steam Turbine and Generator.

5. Trends in Electric Power Supply System Design

The accident at Three Mile Island Nuclear Power Plant caused a lot of introspection in the Nuclear industry. One of the areas that came under scrutiny was the Single Failure Criterion. The review of this lead to the increasing use of Probabilistic Risk Assessments as an improved indicator of plant safety. These Probabilistic Risk Assessments revealed that Station Blackout, that is, Loss of all ac power, was a significant threat to the safety of many existing Nuclear Power Stations.

This chapter is divided into five sections. The first discusses the review of the Single Failure Criterion, and the second describes the increasing use of Probabilistic Risk Assessments. The two major sections describe the improvements to the alternating and direct current systems at Nuclear Power Plants. The final section discusses Operator Error.

5.1 The Review of the Single Failure Criterion.

The Emergency electric power systems in Nuclear Power Plants are designed to meet the Single Failure Criterion. The loss of all ac or dc power are events that are outside the Single Failure Criterion and as such have not been analyzed [50]. The loss of all ac or dc power is possible from a Common mode failure. In the United States of America, the Advisory Committee on Reactor Safeguards has been concerned about these types of failure for over a decade and is not satisfied that the Single Failure Criterion is suitable design criterion for the Emergency Electric Power Supplies. The American Nuclear Regulatory Commission has subsequently given a higher priority to the analysis of these loss of power scenarios.

---

50. Okrent,D. "NEW TRENDS IN SAFETY DESIGN AND ANALYSIS," IAEA-CN-39/6.4, Proc. Int. Conf. on Current Nuclear Power Plant Safety Issues, IAEA, Stockholm, 20-24 October, 1980

5.2 The Use of Probabilistic Risk Analysis

The use of Probabilistic Risk Analysis increased rapidly after the Three Mile Island accident. The Risk study done by the Nuclear Regulatory Commission on the Auxiliary Feedwater systems at Three Mile Island and the resulting recommendations based on the risk study have made the industry realize the usefulness of Probabilistic Risk Assessments.

Probabilistic Risk Assessments can be used in existing plants as a safety review technique to identify plant that has a large contribution to the plant risk. In the design process for new plants, Probabilistic Risk Assessments can be used to enhance the reliability of new systems and it is expected that the Nuclear Regulatory Commission will impose regulatory requirements that go beyond the Single Failure Criterion [51].

The use of Probabilistic Risk Assessments must be accompanied by a review of the results by a well qualified professional engineer whose speciality is Nuclear reliability and safety:- the partial failure of the reactor SCRAM at Browns Ferry Unit 3 in 1980 illustrates this. The Nuclear industry has analyzed the SCRAM function in detail, but one of the initiating events they assumed to be negligible was the one that caused the incident. Further investigation uncovered serious deficiencies in the SCRAM systems. Thus, the numbers produced by a Probabilistic Risk Assessments must be tempered by professional experience.

51. Okrent,D. "NEW TRENDS IN SAFETY DESIGN AND ANALYSIS," IAEA-CN-39/6.4, Proc. Int. Conf. on Current Nuclear Power Plant Safety Issues, IAEA, Stockholm, 20-24 October, 1980

5.3 Improvements to the ac power systems.

The Nuclear industry has identified the loss of all ac power (both onsite and off-site) as a safety issue [52]. This is the so-called "Station Blackout" scenario. Probabilistic Risk Assessments has been used extensively to analyze the reliability of the ac power systems and countries have responded in different ways to the results of these studies.

5.3.1 The United States of America

The frequency of occurrence and median duration for the loss of off-site power at American Nuclear Power Plants over the period from 1968 to 1983 is given [53]:-

Cause	Number	Frequency per site-year	Median duration
Plant centered	30	0.056	0.3 hours
Grid blackout	10	0.019	0.7 hours
Severe Storm	6	0.011	2.6 hours
Totals	46	0.086	0.5 hours

The off-site power loss typically has three causes:- Plant-centered, Grid loss, and severe storms. (The number of site-years for this study was 533.)

52. Kolaczkowski,A.M., Payne,A.C. and Baranowsky,P.W. "ANALYSIS OF STATION BLACKOUT ACCIDENTS FOR LWR's", Proceedings of the International Meeting on Thermal Nuclear Reactor Safety held at Chicago, Illinois on August 29 - September 2, 1982, Volume 1, NUREG/CP-0027-V1 Part 2 of 2, page 511.

53. Reisch,F. "COPING WITH STATION BLACKOUT", Nuclear Engineering International, Volume 30, no.375, October 1985, pages 48 to 51.

American Emergency Diesel Generator failure data for unplanned demands are [54]:-

Year	Demands	Failures	Failures/demand
START PHASE			
1983	139	0	0.000/demand
1984	124	1	0.008/demand
1983	168	1	0.006/demand
LOAD-RUN PHASE			
1983	68	1	0.015/demand
1984	72	1	0.014/demand
1983	83	2	0.024/demand
3-YEAR DEMAND UNRELIABILITY			0.022/demand

Over the three years there were 22104 planned and unplanned Diesel Start demands:- the 431 unplanned start demands are few in comparison. The data for unplanned demands is sparse and this reduces the confidence level of the statistics.

54 Wyckoff,H. "THE RELIABILITY OF EMERGENCY DIESEL GENERATORS AT U.S. NUCLEAR POWER PLANTS", NSAC-108, Electric Power Research Institute, California, September, 1986.

A study sponsored by the Nuclear Regulatory Commission found that there were no dominant diesel generator failure modes (1976 to 1980 data). However, three failure modes accounted for about 17% of all diesel generator failures [55]:-

1. Dirt and moisture on relays and switches
2. Contaminated oil in the diesel speed governor and governor setpoint error.
3. Moisture in the air-start system.

Newer studies show a slightly different picture [56]. Problems with the governor accounts for about 20% of diesel failures, while each of the following systems accounts for about 10% of the diesel failures:- engine mechanical, cooling, lubrication, electric power (including generator), and instrument & control.

Although the onsite and off-site failures are independent, if they do occur simultaneously, then the impact is significant. Up to 1983, five Station Blackouts were experienced, and the longest was for 25 minutes [57].

The American Nuclear Regulatory Commission has identified Station Blackout as an Unresolved Safety Issue and is in the process of issuing a final rule. The objective of the rule is to reduce the risk of severe accidents occurring

---

55. Battle,R.E., Campbell,D.J. and Baranowsky,P.W. "RELIABILITY OF THE EMERGENCY AC POWER SYSTEM AT NUCLEAR POWER PLANTS." Proceedings of the International Meeting on Thermal Nuclear Reactor Safety held at Chicago, Illinois on August 29 - September 2, 1982, Volume 1, NUREG/CP-0027-V1 Part 2 of 2.

56 Wyckoff,H. "THE RELIABILITY OF EMERGENCY DIESEL GENERATORS AT U.S. NUCLEAR POWER PLANTS", NSAC-108, Electric Power Research Institute, California, September, 1986.

57. Berger,W. and Hammersley,R. "COPING WITH THE NUCLEAR STATION BLACKOUT RULE COULD PROVE EXPENSIVE", Power Engineering (USA), Volume 91, no.1, January 1987, pages 21.

as a result of station Blackout. Three areas are to be addressed [58]:-

1. Maintaining the high reliability of the electric power systems.
2. Developing procedures and training for dealing with all possible causes of Station Blackout.
3. Ascertaining that each individual plant can cope with a Blackout for an acceptable period of time.

Point three can be determined from Probabilistic Risk Assessments. For example, one Probabilistic Risk Assessment [59] indicates that the probability of total core failure is between 10^{-5} and 10^{-4} per reactor-year. The actual probability of a release of radioactivity to the environment is dependant on the type of Containment used. This Risk Assessment also indicates that the leakage of primary coolant at the Reactor Coolant Pump seals and the short service times of the dc power sources are important contributors to core damage as a result of Station Blackout.

The length of time a Nuclear Power Station can sustain a Station Blackout is dependant on the plant equipment design. Should a particular plant's Blackout coping time be less than the time determined by the Nuclear Regulatory Commission, then significant costs could be incurred in upgrading the station hardware. The estimated costs are from $200 000 to $4 million [60]. The recommended Blackout

---

58. Berger,W. and Hammersley,R. "COPING WITH THE NUCLEAR STATION BLACKOUT RULE COULD PROVE EXPENSIVE", Power Engineering (USA), Volume 91, no.1, January 1987, page 22.
59. Kolaczkowski,A.M., Payne,A.C. and Baranowsky,P.W. "ANALYSIS OF STATION BLACKOUT ACCIDENTS FOR LWR's", Proceedings of the International Meeting on Thermal Nuclear Reactor Safety held at Chicago, Illinois on August 29 - September 2, 1982, Volume 1, NUREG/CP-0027-V1 Part 2 of 2, page 514.
60. NUREG-1109 "Regulatory Analysis for the Resolution of Unresolved Safety issue A-44, Station Blackout", draft, January 1986 (referenced in Berger,W. and Hammersley,R. "COPING WITH THE NUCLEAR STATION BLACKOUT RULE COULD PROVE EXPENSIVE", Power Engineering (USA), Volume 91, no.1, January 1987.)

Coping time is from 4 to 16 hours, depending on station type [61].

Thus, the American response to the Station Blackout hazard is to firstly, for each plant, quantify the station's Blackout Coping time. Should this be less than the stations specified Coping time (as laid down by the Nuclear Regulatory Commission for different Emergency Electric Power system configurations), then the utility has two options [62]:-

1. To upgrade the equipment required to cope with a Station Blackout, that is, the dc power systems, emergency feedwater storage tank, instrument compressed air, the reactor coolant pump seal integrity without cooling, and the decay heat removal systems that are independent of ac power.

2. To upgrade the plant's ac power system configuration so that the increased reliability results in the plant complying with the Nuclear Regulatory Commission Station Blackout requirements. Typical modifications here are to add an independent power line or an extra emergency Emergency Diesel generator set.

---

61. Reisch,F. "COPING WITH STATION BLACKOUT", Nuclear Engineering International, Volume 30, no.375, October 1985, pages 48 to 51.

62 Berger,W. and Hammersley,R. "COPING WITH THE NUCLEAR STATION BLACKOUT RULE COULD PROVE EXPENSIVE", Power Engineering (USA), Volume 91, no.1, January 1987.

5.3.2 France

The French have used Diesel Generators on all their 900 MW Nuclear power units which number in excess of twenty [63].

The French Nuclear Power Stations were not designed to cope with Station Blackout initially as the event has a low probability of occurring [64]. They have subsequently identified two problems:-

1. The Reactor Primary System will lose Coolant from the Reactor Coolant Pump Seals and will result in the reactor core being uncovered. The uncovering of the core is a serious event as the Primary Fission Product Barrier, the Fuel Rod Cladding will rupture. The Secondary Fission Product Barrier, the Primary System, is already ruptured at the Primary Coolant Pump seals, and the only remaining Barrier is the Containment Building.

2. The dc system batteries can only supply the reactor instrumentation and controls for a limited time, thereafter, there will be no information on the reactor state.

The French have implemented a number of counter measures to reduce the probability of core damage resulting from a Station Blackout [65]. The Reactor Coolant Pump seal leakage is identified as a small Loss of Coolant Accident and a special system, labelled the LLS system, is installed to provide seal water (Figure 5.1).

---

63. Electricite de France. "EDF 900 MWe NUCLEAR POWER PLANTS, SHORT TECHNICAL DESCRIPTION." issued by Service d'Equipment Nucleaire Exterieur, 11-13 Avenue de Friedland, 75008 PARIS, May 1983.
64. Melcot,B. "HOW EdF BRINGS ITS PWRs TO A SAFE SHUTDOWN DURING BLACKOUT", Nuclear Engineering International, Volume 32, no.394, May 1987, pages 55-6.
65. Melcot,B. "HOW EdF BRINGS ITS PWRs TO A SAFE SHUTDOWN DURING BLACKOUT", Nuclear Engineering International, Volume 32, no.394, May 1987, pages 55-6.

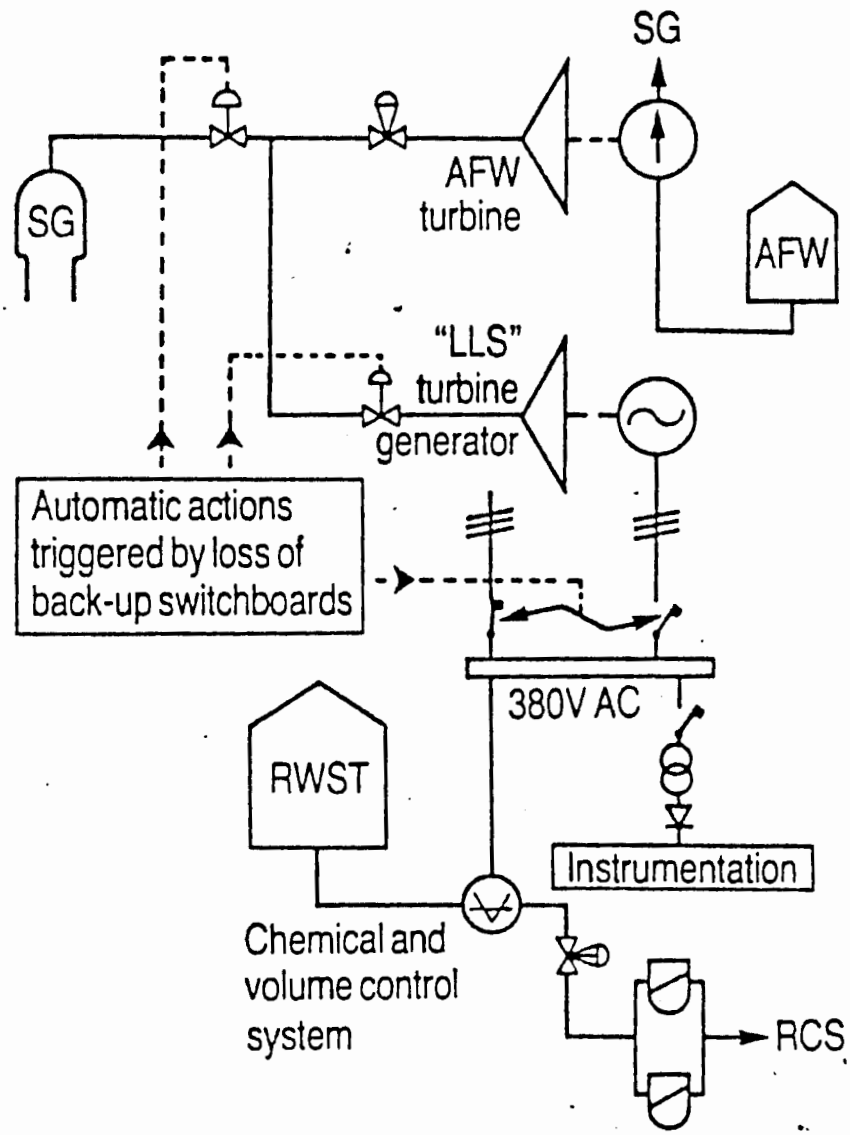


Figure 5.1 "The LLS System"

The LLS system has a small 380 Vac turbine driven generator supplied with steam from the steam generators. This ac power is used to drive a high pressure pump which forces water into the Reactor Coolant Pump seals and prevents a small Loss of Coolant Accident. The ac power is also used to supply other loads such as:- the lighting in the Unit control rooms, selected vital instrumentation, and the control system of the Auxiliary Feedwater system. Certain batteries are also charged with this power [66].

The French have developed an operating procedure "H3" to keep the plant in a safe shutdown state for a few hours until the ac power can be restored.

The sequence of events covered by the procedure "H3" are:- following a Station Blackout, the Reactor Protection System trips the reactor and the Control rods drop into the core terminating the Nuclear Fission process. The reactor coolant continues circulating even though the Coolant Pumps are not operating. The thermal gradient between the reactor core and the steam generator provides the motive force for this "natural circulation".

The heat is removed from the Steam Generators by the Auxiliary Feedwater system supplying water to the steam generator inlets:- the resulting steam is vented to the atmosphere.

At the same time, the LLS system is preventing any significant leakage at the Reactor Coolant pump seals. Once the Primary system has been cooled down to 150 deg.C and the pressure is lower than 30 Bar, the need for the Pump seal water falls away.

---

66. Electricite de France, "PWR PLANT BLACKOUT, EDF'S RESPONSE", written by M.M.Gelle, Engineering and Construction Division, January 1988.

The LLS system also provides power for the instrumentation that the Operators need to use to maintain the "Natural Circulation".

The procedure covers the restoration of power from an on-site power source. Ac power sources available are:-

1. The main off-site power source.
2. The Auxiliary off-site power source.
3. The Train (Division) A diesel generator set.
4. The Train (Division) B diesel generator set.
5. Another Unit running on house load. All French sites have more than one Unit.
6. A transportable gas turbo-generator kept at each site especially for Station Blackouts.
7. The last resort would be to take power from a Diesel Generator set in another Unit at the same site.

A "Fish plate cabinet" is provided to implement the interconnections described in points 6 and 7 above. Figure 5.2 shows the single line diagram. Thus the gas turbo-generator can be connected to any Safety related Diesel switchboard on the site, or any Diesel-generator can supply any other Diesel-generator switchboard. This is a last resort because the independence of the Safety Divisions is breached by the interconnection between them.

The French actually tested out their procedure and Blackout equipment by deliberately causing a Station Blackout at one of their 900MW plants in 1983. The test was successful.

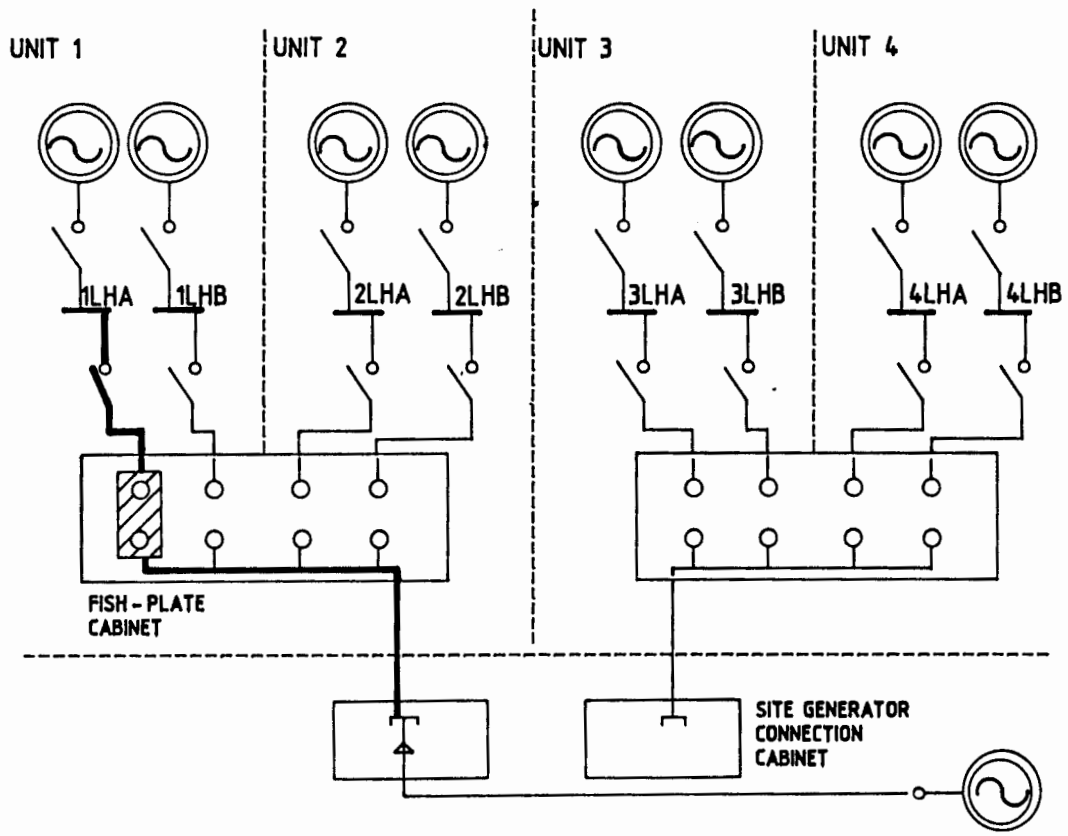


Figure 5.2 "Fish Plate cabinet used to connect external generator, or to interconnect unit diesels"

5.3.3 Britain

In Britain, the Sizewell B design has two Auxiliary Feedwater pumps driven by steam, and two Primary System charging pumps also driven by steam [67]. There are also two electrically driven pumps in each of these systems. The use of steam to power Engineered Safety System loads is to reduce the dependance on ac electric power:- thus reducing the impact of a Station Blackout. The steam driven charging pumps provide the same function as the LLS system of the French stations .

The CEGB has used gas turbines to drive the Emergency power supply generators at two of its Nuclear Power Stations [68]. The original reason for using gas-turbines was that they were supposed to be more reliable than Diesel engines. However, experience has shown that the number of failures per start attempt for gas turbines is about twice that of diesel engines.

Diesel generators are used at Sizewell B, and there are four diesel generators instead of the usual two [69]. The diesels are positioned at two separate locations ensuring physical independence.

The station batteries at Sizewell B have a 12 hour supply capability and two small diesel generators are provided for battery charging [70]. The diesel generators make the dc power independent of a Station Blackout.

---

67. Reisch,F. "COPING WITH STATION BLACKOUT", Nuclear Engineering International, Volume 30, no.375, October 1985, pages 48 to 51.
68. CASTLE,J.R. "INFLUENCE OF NUCLEAR SAFETY REQUIREMENTS FOR CEGB GAS COOLED REACTORS ON DESIGN OF THEIR ELECTRICAL AUXILIARY SYSTEMS." IEE Proceedings C (Generation, Transmission and Distribution), Volume 128, no.2, pages 117-21, March 1981.
69. George,B.V. "THE DESIGN OF THE PWR TO MEET UK REQUIREMENTS", The Nuclear Engineer, Volume 25, No.5, Sept/Oct 1984, pp. 176 to 180.
70. Reisch,F. "COPING WITH STATION BLACKOUT", Nuclear Engineering International, Volume 30, no.375, October 1985, pages 48 to 51.

Essentially, at Sizewell B, there is a four-way redundancy for systems required for shutting the plant down from power operating conditions, and a two-way redundancy for systems used when the unit is shut down for refuelling.

5.3.4 Europe

In FR Germany, the older plants usually have two redundant trains, while the newer plants have four []. The single failure criterion is met by any three of the trains so the remaining train can be tested and maintained at any time. The German standard concept for the Electric Power supplies is shown in Figure 5.3.

The Emergency Feedwater Systems and the Emergency Core Cooling Systems are located in a separate emergency building which also contains the diesel generators required for these Engineered Safety Features. The reason for the separate protected building is that the German Safety Guidelines require the safe shutdown and cooling of the reactor even when the Nuclear Auxiliary building has been destroyed by earthquakes, missiles or gas explosions.

In addition, most of the loads in the new German plants are provided with duplicate supplies to further improve the power supply reliability.

In Germany, Belgium and Switzerland, additional diesel driven feedwater pumps have been provided [72]. These are located in a special building some distance from the reactor building.

---

71. Simon,M. "REDUNDANCY PROVES ITS WORTH IN FR GERMANY," Nuclear Engineering International, Volume 32, no.394, May 1987, pages 57.
72. Reisch,F. "COPING WITH STATION BLACKOUT", Nuclear Engineering International, Volume 30, no.375, October 1985, pages 48 to 51.

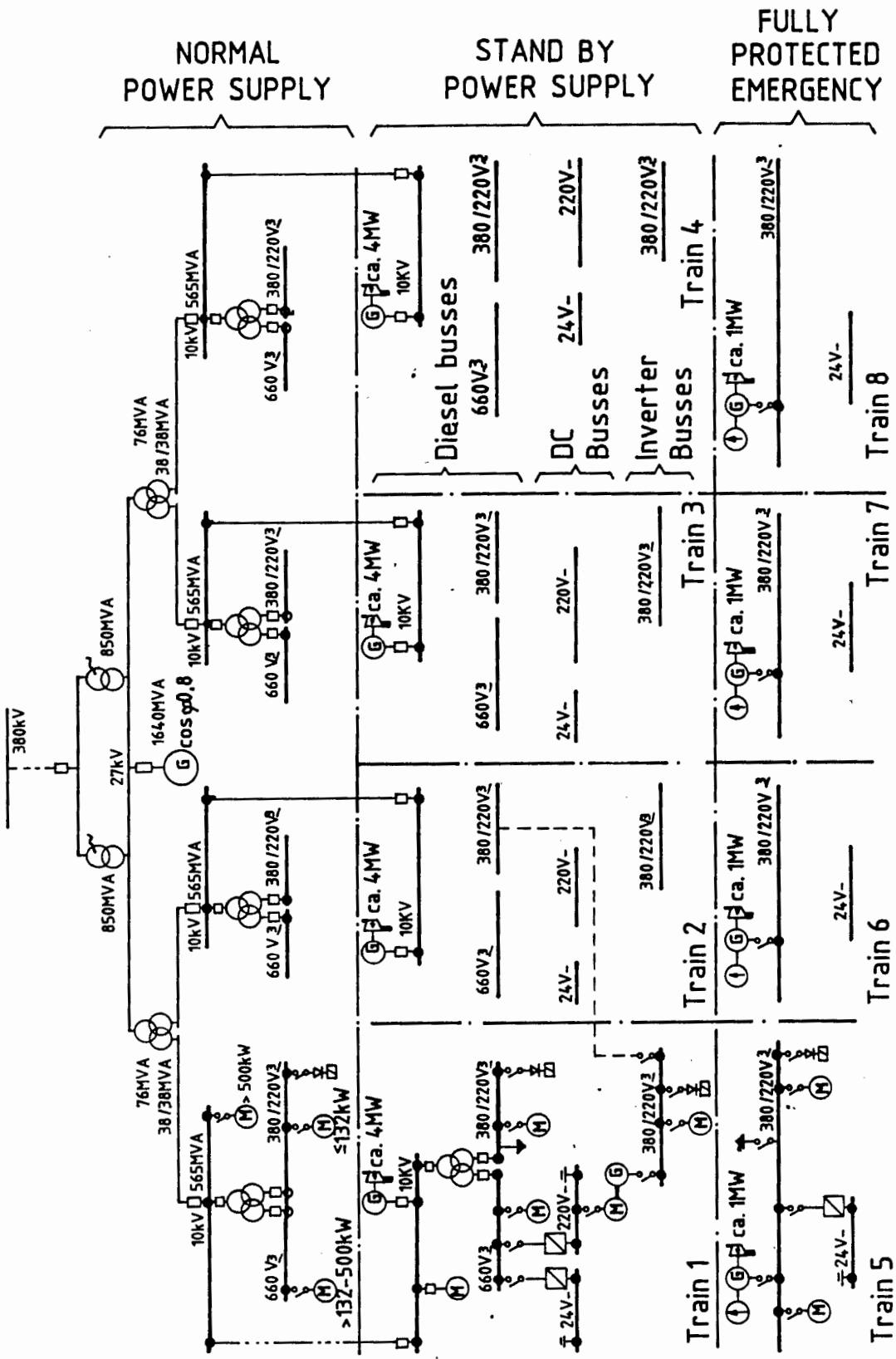


Figure 5.3 "The German Electric Power Supply system

5.3.5 South Africa

In South Africa, ESKOM follows the French Nuclear program closely:- ESKOM reviews all plant modifications implemented by the French for applicability to Koeberg Nuclear Power Station. Thus, ESKOM has a Blackout Working Party and the author sat in this Working party for a time.

The Blackout Working Party commissioned the ESKOM corporate Probabilistic Risk Assessment group to perform a Probabilistic Risk assessment for Station Blackout at Koeberg Nuclear Power Station [73]. The results indicate that Koeberg meets the Atomic Energy Corporations requirements as laid down in the LBG1 document [74].

A recommendation of the Risk study is that Medium Voltage Breakers have the manual closing facility re-installed (it was removed at ESKOM's request when the station was built). The Risk study ignored the effect of battery failure and assumed that in the event of battery failure, the Medium Voltage Breakers could be opened and closed manually.

The study indicates that the Unit trip is a significant initiating event for a Station Blackout and the recommendation here is that Unit trips be reduced. The success rate of House loading is also an important factor and the recommendation is that this is tested to maintain a high success rate.

At present, Koeberg has none of the French Blackout modifications in place and the above study addresses the present plant state. The ESKOM Blackout committee is

---

73. ESKOM, Nuclear Engineering Division, Report 1124602 "Loss of Electric Power Supplies", March 1989.

74. Atomic Energy Board of South Africa "LICENSING OF NUCLEAR INSTALLATIONS: A GUIDE TO THE REQUIREMENTS FOR SAFETY ASSESSMENT", document no. LBG/1, issue 3, May 1979.

therefore of the opinion that no further modifications are necessary.

The author believes that the French Blackout modifications are well thought out, and their implementation at Koeberg will require minimal extra plant as an extra Diesel Generator is already installed along with a special switchboard that can connect the extra Diesel to any of the four Emergency Medium Voltage Switchboards.

The only extra equipment required is the LLS turbo-generator and the Low Voltage LLS switchboard. The re-supply of a Blackout Unit from a houseloaded unit via the High Voltage Switchyard is essentially covered by a procedure, while the last resort of breaching the Safety System independence by connecting a Emergency Diesel from another unit to the Emergency busbars of the Blackout Unit is achieved by overiding the interlocks on the extra Diesel switchboard. All these actions need to be covered by a procedure which could be based on the French H3 procedure.

The advantage of installing the LLS turbo-generator is that in the event of a Blackout, the Primary pump seals will not be damaged immediately. The commercial implications are that once the cause of the Blackout has been rectified, the Unit can return to operation if the power was restored before any Primary Pump Seal damage occurred.

5.4 Improvements to the dc power systems.

The main components in the dc power systems are:- batteries, battery chargers, inverters, and the dc power distribution system.

5.4.1 Batteries

A study sponsored by the Nuclear Regulatory Commission in the United States of America to evaluate the use of lead-acid batteries in Nuclear Power Plants found several issues affecting the life of cells [75].

The most common age-related stress mechanism in lead-acid cells using lead-calcium alloys is the corrosion of grids in the plates and the corrosion of the top conductors. The acid corrodes the lead to lead-dioxide which causes a 21% volume growth:- this leads to a number of failure modes.

1. The grids in the plate swell and can cause poor contact between the grid and the active material in the plate.

2. The plates may swell to such an extent that the container cracks:- a cell without electrolyte is useless.

The corrosion of the lead is enhanced by high temperatures which can result from overcharging, a high current ripple in the cell, or high ambient temperatures. An increase in ambient temperature from 25 deg.C to 35 deg.C can reduce the cell life by as much as 50%.

---

75. Edson,J.L. and Hardin,J.E. "AGING OF CLASS 1E BATTERIES IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS," NUREG/CR-4457, United States Nuclear Regulatory Commission, July 1987, page 30.

The problem with cells that are weakened by this swelling and weakening is that they may still be able to supply their design power but the seismic withstand capability may be seriously impaired. Tests on old batteries have confirmed this. Thus the latest revision of IEEE Std 535-1986 "IEEE Standard for Qualification of Class 1E Lead Storage Batteries for Nuclear Power Generating Stations" requires that seismic qualification take place with aged cells. Some manufacturers have qualified their new range of cells to 15 years.

Operating experience in the United States of America indicates that:-

1. Low Specific Gravity of cells accounted for 27% of the battery-related events reported to the Nuclear Regulatory Commission.

2. Errors by personnel in operating, maintaining and testing batteries accounted for 21% of the battery-related events reported to the Nuclear Regulatory Commission.

3. Wearout failure of cells peaks between 6 and 11 years of operation

The implication of the above points is that lead-acid cells are not being looked after as well as they should be. Low Specific Gravity can only occur if the cell terminal voltage is incorrect and the cell is discharging. The large number of personnel errors indicates an under-estimation of the care needed to ensure long cell life:- the early failures could be a result of the lack of care in maintaining and operating the cells.

Thus there is a need to develop better techniques of monitoring the state of lead-acid cells in Nuclear Power

Plants, particularly cell state of charge, and the Seismic withstand ability of old cells.

In 1986 the author was part of a literature search conducted by the Design & Specification Group at Koeberg Nuclear Power Station. The aim was to find useful papers and articles on lead acid batteries. One of the most useful papers found, in the author's opinion, is one by D.Berndt of VARTA Batterie AG [76].

The state of charge of cells on float charge is not easy to determine as the only true indicator of cell state of charge is a qualification discharge. The use of the cell Specific Gravity is problematic as discussed previously.

Berndt proposes a statistical method that evaluates the whole battery of cells. The cell terminal voltages are measured with the battery at Float charge conditions and the distribution is plotted. Figure 5.4 shows the distribution for over 300 cells in 12 batteries used by the German Federal Postal Administration. The terminal voltages have a Normal Distribution with a Standard deviation of 4 mV.

If one cell was faulty then it would show up on the Normal Distribution as being outside the Normal Distribution. Berndt also puts forward that if several cells were outside the Normal Distribution, then the battery as a whole is not fully charged.

The use of Specific Gravity measurements is only needed to investigate weak cells because the acid density cannot fall while the cell terminal voltage is correct.

---

76. Berndt,D. "STATIONARY LEAD ACID BATTERIES, OPERATIONAL CONDITIONS, FUTURE ASPECTS," presented at Symposium on Standby & Uninterruptable Power Supplies, organized by South African Institute of Electrical Engineers and The Association of Municipal Electricity Undertakings of South Africa, 17 to 18 September 1986, paper I1.

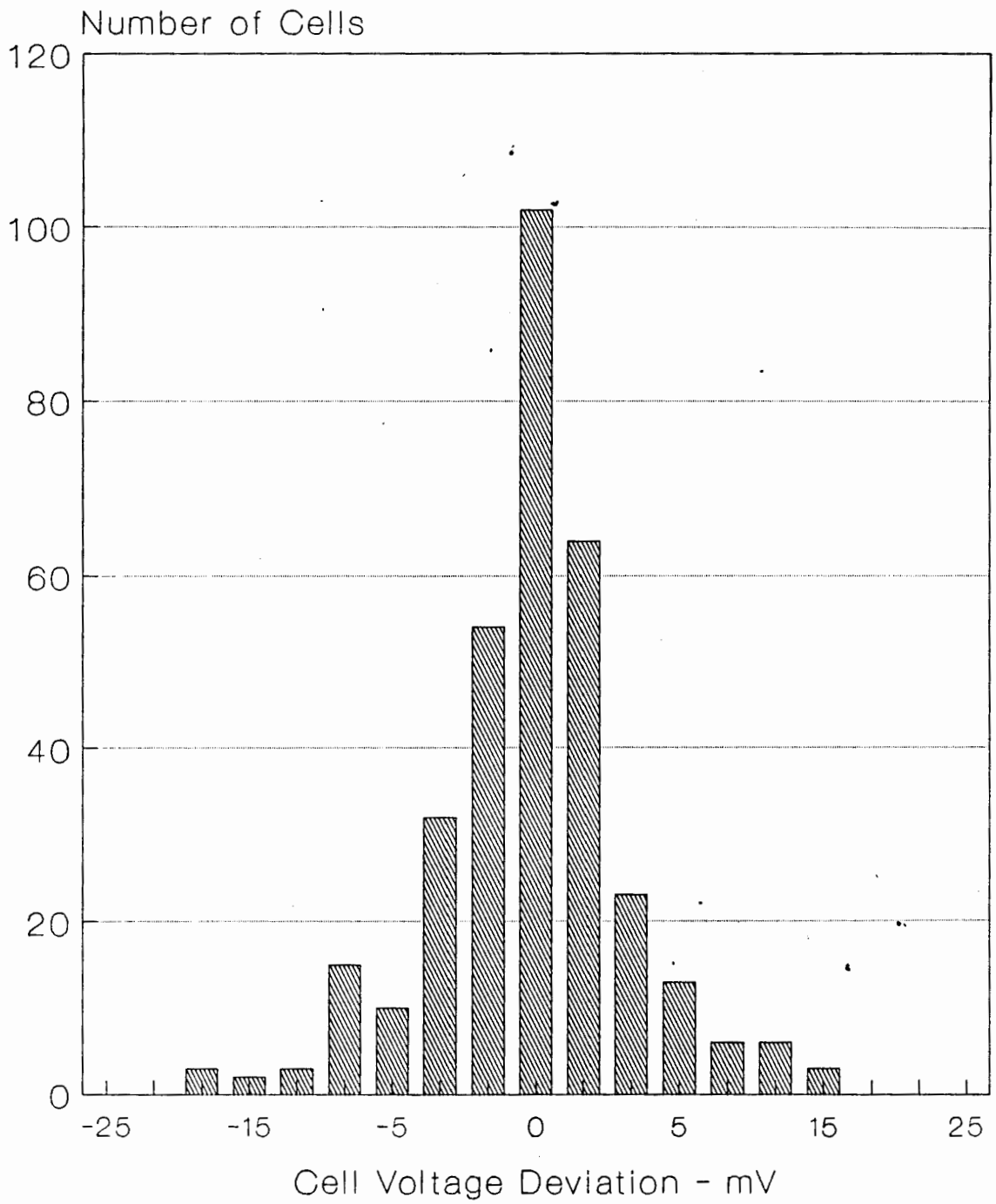


Figure 5.4 **"Terminal Voltage Distribution for 300 Lead-acid cells"**

The IEEE recommended maintenance is not as sophisticated as this and the author expects many users of batteries to utilize Berndt's method because it is so simple and gives information about individual cells and the battery as a whole.

Interestingly, Berndt goes on to describe sealed lead-acid cells. He concludes that due to the cell internal processes, the simple method proposed above cannot be used to monitor the state of charge of sealed lead acid cells. As the cells are sealed, no Specific Gravity measurements are possible, and the only way to test sealed cells is to discharge them. Thus, the use of sealed cells is not possible in Nuclear plants, unless two battery banks are used so that each can be discharged periodically while the other supports the loads.

The use of Lead-acid batteries has had a long and involved history at Koeberg Nuclear Power Station [77]. After the initial installation of the batteries in 1982, some problems were experienced with cells not being properly charged. Near the end of 1982, certain cells were still undercharged, and the float voltage was increased from 2.20 V/cell to 2.22 V/cell. Electricite de France in France were experiencing similar problems at the time.

The batteries did not recover and in mid 1983, a large number of batteries failed their discharge tests. The Contractor replaced cells and the batteries were eventually fit for use in 1984 when the Unit was started up for the first time.

In early 1985, during a forced outage, several batteries failed their discharge tests and new cells were ordered from France.

---

77. Morley,M "KOEBERG BATTERIES", KOEBERG Computer Reference 201124R, 28 October 1986.

In mid 1985, it came to light that Electricite de France were replacing certain batteries after as little as 3 years and they had a general policy to replace all cells after 5 years.

The author's involvement started in July 1986 when a Battery Working Group was formed to address a number of issues:-

1. The effect of temperature on cell life.
2. The effect of current ripple on cell life.
3. The advisability of deep discharges.
4. The suitability of the battery charging regime.
5. The world experience with lead-acid batteries.

1. Temperature

A higher temperature increases the cell capacity and corrosion rate, and lowers the cell open-circuit voltage [78]. Typically, an increase in temperature from 20 deg.C to 30 deg.C halves battery life [79].

2. Current Ripple

Excessive current ripple through a Lead-acid battery results in a loss of life:- the analogy is that every cycle of the ripple is a small charge-discharge cycle. As a lead-acid battery only has a finite number of full charge-discharge cycles, the cumulative effect of the ripple charge-discharge cycles is a loss of life. Current ripple can cause extra heating of cells which accelerates the loss of electrolyte. At Koeberg Nuclear Power Station, the specified maximum ripple is 5% of the Ampere-hour

78. "THE WILLARD STORAGE BATTERY", Willard, P.O.Box 4025, Port Elizabeth, 6014, RSA, Form 6750, April 1982.
79. Boettger,K., Engineer, AEG company, verbal communication, 1986.

rate, that is, 50 Amperes for a 1000 Amp-hour battery [80]. Measurements of the ripple current indicate that the actual ripple currents at Koeberg Nuclear Power Station are less than 1% of the battery Ampere-hour rates:- batteries feeding inverters have a slightly higher figure of 3%.

3. Magnitude of Maintenance Discharges

A one-hour discharge test is used to qualify the batteries for service at Koeberg Nuclear Power Station. (The batteries are designed to supply the dc loads for one hour at the minimum temperature of 15 deg.C). This discharge is roughly 30% of the battery capacity. The effect of discharges of different magnitude was investigated with respect to battery life.

The disadvantages of deep discharges are that these use up some of the batteries finite number of charge-discharge cycles. The advantage of deep discharges is that it reduces the amount of rhombic Lead-dioxide in the Positive plate by converting it to tetragonal Lead-dioxide [81]. The significance of this is that the tetragonal form has a specific weight capacity which exceeds that of the rhombic form by 150 to 300%. The tetragonal form has a lower self discharge rate due to its lower final charge potential.

Thus, in float charge applications, the occasional deep discharge of lead-acid batteries is beneficial as the impact on the finite number of charge-discharge cycles is small, and the capacity of the positive plate is maintained.

---

80. Koeberg Nuclear Power Station, Specification for Lead-acid Batteries, Ref. Maintenance Manual 315 "LEAD ACID BATTERIES".

81. Dasoyan, M.A. and Aguf,I.A. "CURRENT THEORY OF LEAD ACID BATTERIES", Technicopy, Stonehouse, England, 1979 pages 146 to 165.

4. Battery Charging

The battery charging regime consists of a float voltage with a monthly equalizing charge. The float voltage is 2.22 V/cell and the equalizing voltage is 2.28 V/cell. Initially the equalizing charge was for 18 hours, but this was increased to 40 hours in 1986 to combat the gradual discharge of the batteries.

This did improve the battery performance on float charge, however, many batteries were approaching their fifth year of operation and the decision was taken to replace all old batteries on Unit 1. These batteries had not had the best commissioning and had been undercharged at 2.20 V/cell [82]:- this can lead to sulphation and low specific gravities. High electrolyte concentrations can speed up the self discharge process and result in undercharging [83]. There is evidence that this may have occurred in some of the cells at Koeberg Nuclear Power Station [84]. The Unit 2 batteries had been commissioned with more care and some of these have given six years operation before being replaced.

The current policy for Unit outages is to perform a 10 hour deep discharge test and then Boost charge the batteries to 2.6 V/cell. This has to be done off-load as the dc system loads are not rated for these high voltages. As the Unit outages occur yearly, this Boost charge can only happen yearly.

---

82. ESKOM Surveillance Report RSV/86/002/VD/927, Koeberg Nuclear Power Station Computer Ref. 192341R, dated 18 July 1986.

83. Dasoyan, M.A. and Aguf,I.A. "CURRENT THEORY OF LEAD ACID BATTERIES", Technicopy, Stonehouse, England, 1979 page 346.

84. ESKOM Memorandum from Engineering Investigations Manager to Power Station Manager, Koeberg Nuclear Power Station, Ref. OT243,Acc.No,309590, dated 23 April 1987.

A flowchart (Figure 5.5) has been developed to allow a battery that fails the one hour qualification test to be "cycled". This cycling is done to re-form the active material on the plates and to remove any sulphation.

Boost charging at 2.6 V/cell has the additional advantage of circulating the electrolyte which eliminates any stratification of the electrolyte. With this in mind, Koeberg Nuclear Power Station has specified air electrolyte agitators for all new cells:- this is expected to increase the life of the batteries as the charging is more efficient when the electrolyte is stirred.

Koeberg Nuclear Power Station has built a "Battery Hospital" which is essentially a suitably ventilated room with a large automated battery charger. The "Battery Hospital" is used to commission new battery banks for installation during outages:- this ensures a properly commissioned battery as there is plenty of time to form the cells by cycling the battery a few times.

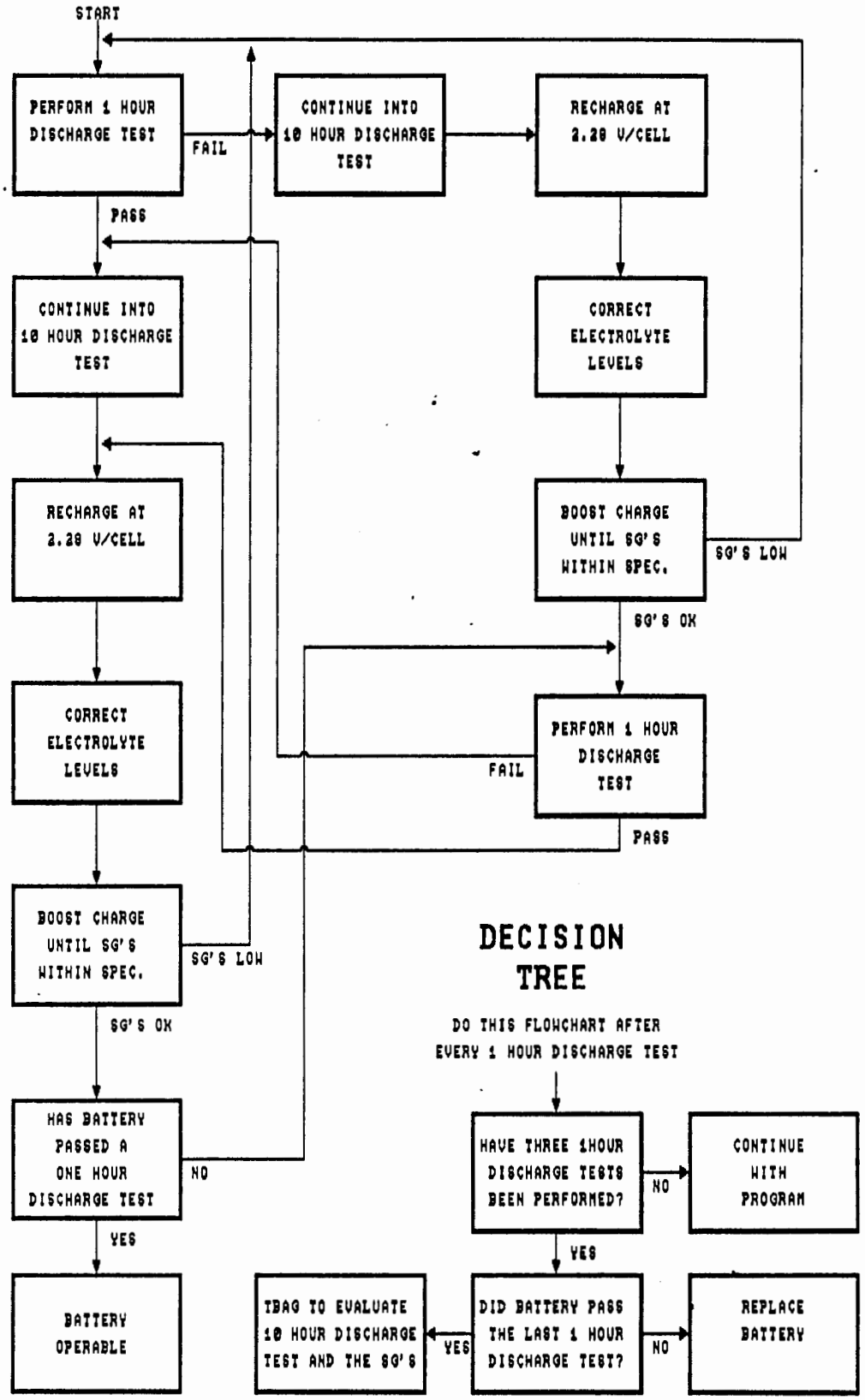


Figure 5.5 "Maintenance Flowchart for Charging Lead-acid Batteries"

5. World Experience

The author produced an ESKOM report on "Representative Stationary Battery Experience" in September 1987 [85]. The purpose of the report is to provide a summary of the operational experience gained by various stationary battery users in North America and Europe.

The USA and Canadian experience with stationary lead acid batteries is summarized as follows [86]:-

1. Most applications rely on the use of pasted alloy plate cells.
2. Operating restrictions require careful control of charging voltage, battery environment, and purity of water and sulphuric acid.
3. The relatively low frequency of power failures and the use of emergency diesel generators result in infrequent and short discharges for most cells.
4. Cell failure at old age is usually related to a small number of mechanisms, most often involving corrosion or sulphation.
5. Many cell failures result from misuse or abuse during installation or operation.
6. One of the largest users, the Bell System, has developed its own design after unsatisfactory performance by calcium alloy cells.
7. A Bell System survey illustrates that even for the same cell type, wide variations in operating life can occur between manufacturers or even between generations of cells produced by the same manufacturer.

---

85. Smyth,T.P. "Representative Stationary Battery Experience", Design & Specification Group, Koeberg Nuclear Power Station, Report DSG-550-002, Sept 1987.
86. Friedman E J et al "ELECTROTECHNOLOGY VOL 3, Stationary Lead acid Batteries, "Applications and Performance", Ann Arbor Science Publishers Inc;, Michigan, 1980

8. Subtle changes in cell design, fabrication, materials or operation can have considerable impact on performance.
9. The Bell survey clearly indicates three classes of cell performance (a) those of short life (7 years); (b) those of moderate life (11 years); and (c) those of long life (greater than 15 years).
10. Proper selection of initial, float and equalization voltage have a strong influence on cell operation and life.
11. Calcium alloy cells are most often chosen for applications where infrequent discharges are expected. Tubular or Plante cells are chosen for less reliable circumstances.
12. Strict maintenance, monitoring and reporting procedures are required for batteries used in critical dc systems in Nuclear power facilities.

The British Post Office uses Plante cells and since 1972, emergency batteries have not been used as a filtering element for the battery charger:- filtering is more economically provided by capacitors integrated into the module. The batteries are found to be more reliable on float charge when they are not used as a filtering element.

The float voltage is carefully selected and provided by a well-filtered charger:- the cell plates do not corrode, no equalizing charge is needed and the cell condition is gauged from the colour of the cell electrodes.

Cell maintenance comprises of a float voltage measurement, electrolyte level correction and electrode colour examination.

The CEGB use Plante cells in all their power plants and obtain a service life of 25 years in Nuclear plants. As no

discharge tests are possible during Nuclear plant operation, only specific gravity measurements and visual inspections are done.

Future plants will, however, use tubular cells as they are more economic and the installation will have a redundant capacity in excess of 100%.

The Swiss Post office uses tubular cells and has carefully optimized the cell floating voltage. This regime eliminates equalizing charges and periodic discharge/ charge cycles: a cell life of 15 years can be expected.

Swiss Nuclear plants use both plants and tubular cells and have achieved battery lifes of 10 and 9 years respectively. The cell manufacturers are involved in the battery maintenance and the manufacturer Electrona suggest a cell life of up to 19 years when used with a very well filtered battery charger.

The West German Post office use both Plante and tubular cells and expects 15 years of service from both types.

The West German Nuclear plants use mainly Plante cell types and achieve 20 years battery lifetimes. Batteries are equalized annually at 2.6 to 2.7 V/Cell and the cells are dismantled and cleaned annually. The average battery room temperature is 15 deg.C.

The French experience is summarized as:-

"The life of the Plante batteries is at least 20 years, while the Ironclad (tubular) lead batteries have much shorter lives. The Ironclad batteries, with higher capacity than the Plante, have shown faster corrosion, particularly for those units installed since 1960. Those

units coupled with inverters have corroded at a much faster rate. This aging phenomenon is characterized by a substantial loss of capacity. The discharge curves significantly decrease below the minimum value specified by the manufacturers".

"In addition to the normal aging, the lead-acid batteries have shown frequent corrosion on the top of the plates, resulting in a slow reduction in the size of their cross sections. Fracturing of the plates has also occurred. It should be noted that these failures did not seem to occur on all cells of the same battery, even though they are all subjected to the same charge and discharge currents and are in the same environment. These failures are very serious because they occur without any warning or apparent visual signs or changes in characteristics, eg. specific gravity".

"In summary, the two years of observations and analysis indicate that the corrosion of the cells occurs where perchlorate ions are formed. The analysis also shows that the corrosion is more pronounced when an inverter is part of the circuit" [87].

The American and European usage and trends of Lead-acid cells is summarized in Figure 5.6 [88]:-

87. Friedman E J et al "ELECTROTECHNOLOGY VOL 3, Stationary Lead acid Batteries, "Applications and Performance", Ann Arbor Science Publishers Inc;, Michigan, 1980

88. Friedman E J et al "ELECTROTECHNOLOGY VOL 3, Stationary Lead acid Batteries, "Applications and Performance", Ann Arbor Science Publishers Inc;, Michigan, 1980.

Feature	U.S.	Canada	U.K.	France	Switzerland	Germany
Most common cell type	Lead calcium alloy, flat plate grid	Lead antimony alloy, flat plate grid	Plante	Tubular	Tubular	Tubular Plante
Typical Size Amp-hours	1200-1600	1000-1500	Up to 2200	No info.	No info.	Up to 10 000
Expected life Years	Calcium:20 Antimony:18 Tubular:22 Manchester:25	No info.	Plante:25	No info.	Tubular:15	Plante:25-30 Tubular:15
Trend for future use	Further use of calcium alloy	More use of calcium design	Increased use of tubular	No info.	Increased use of tubular	Increased use of tubular

Figure 5.6 "American & European usage of Lead-acid cells"

5.4.2 Battery Chargers and Inverters

An assessment of the aging of battery chargers and inverters used in Nuclear Power Plants was prepared for the United States Nuclear Regulatory Commission [89].

The most significant problem in the design of chargers and inverters is the use of electrolytic and oil-filled capacitors. Plant failure histories as reported to the Nuclear Regulatory Commission show that these types of capacitor have a useful life of 4 to 6 years. The report recommends the use of capacitors with higher voltage and temperature ratings to reduce the stress on the component. Of note is that the Pulse-width modulation type of inverter uses a smaller filtering capacitor and may not be as susceptible to capacitor failure.

Other design and fabrication issues are:-

1. The use of surge suppression equipment is essential on the inputs to chargers and inverters.

2. The use of natural convection cooling is not sufficient as many charger and inverter failures are attributed to overheating. The use of Forced Cooling is recommended.

3. Zener reference diodes are not stable enough for use as voltage references.

4. Transformer internal temperatures are higher than anticipated and the use of Class B insulation has resulted in premature transformer failures. The use of Class H insulation is recommended to ensure reliable service from Safety related transformers.

---

89. Gunther,W.E., Subudhi,M.,and Taylor,J.H. "OPERATING EXPERIENCE AND AGING-SEISMIC ASSESSMENT OF BATTERY CHARGERS AND INVERTERS", NUREG/CR-4564, US Nuclear Regulatory Commission, June 1986.

5. The detection of a battery charger failure on some plants only occurs when the low voltage alarm on the dc busbars is activated:- when the battery is at the end of its useful discharge. This is undesirable. In France, one of the most serious incidents occurred in this way:- the charger on the main control battery failed and the battery gradually ran down without the operators being aware of it. The consequence was that the Engineered Safety Feature equipment was operating spuriously as the various control relays dropped out at random due to the very low control voltage. A modification was installed to immediately detect charger output failure and to trip the switchboard in the event of the battery voltage reaching the minimum board voltage:- no control at all is better than spurious, unpredictable action.

The failure of battery chargers and especially inverters can have a significant impact on the plant:- for example, the reactor can trip, the safety injection systems can be actuated, or the Emergency Core Cooling Systems may be inhibited.

For both the Reactor Protection System and the Emergency Core Cooling Systems the failure of inverters has the greatest contribution to the system unreliability. The failure of battery chargers is the third greatest contributor to the Emergency Core Cooling Systems unreliability.

The testing of the Diesel Generator sets results in large voltage and frequency variations in the power applied to the battery chargers which stresses the charger components unnecessarily and could cause early failure. Battery chargers and inverters should be given additional attention during construction and commissioning to ensure

that they are not prematurely aged by electrical or physical stresses.

The addition of a second battery charger which will significantly increase the reliability of the dc systems. A typical example is shown in Figure 5.7 [90]:- Battery chargers 31 and 32 both supply battery number 3. However, to save costs, a common battery charger is shared between batteries 1 and 2 as the second charger.

Plant data indicates that at least 30% of charger and inverter failures are age related and a significant improvement in the equipment performance can be made by reducing these failures. This is supported by a more recent report [91]. Chargers and inverters have a burn-in period of about 2 years operation and a wear-out period after 4 to 6 years operation.

The ambient temperature of chargers or inverters has a "dramatic" effect on the reliability of the equipment:- overheating is identified as a major contributor to aging related failures. Components affected included capacitors, transformers and semiconductors.

The Seismic withstand capability of aged chargers and inverters is impaired in some instances by weak cabinet mountings, printed circuit board supports, connectors, and oil filled capacitors.

A 12-year old Safety-related inverter and battery charger where tested for the United States Nuclear Regulatory Commission [92]. The main assessment of the equipment

---

90. Young,R.A. "ADDITIONAL ELECTRICAL DESIGN CONSIDERATIONS EMPLOYED AT DIABLO CANYON NUCLEAR POWER PROJECT," IEEE Power Engineering Society Summer Meeting (Text of A Papers), Portland, ORE, USA, 18-23 July 1976, pages A76 438-2/1-6.

91. Muhlheim,M.D. and Murphy,G.A. "CAUSES AND EFFECTS OF VITAL INSTRUMENTATION AND CONTROL POWER SUPPLY BUS FAILURES," Nuclear Safety, Volume 28, No.1, January - March 1987, pages 90-7.

92 Gunther,W.E. "TESTING OF A NATURALLY AGED NUCLEAR POWER PLANT INVERTER AND BATTERY CHARGER", NUREG/CR-5192, United States Nuclear Regulatory Commission, September 1988.

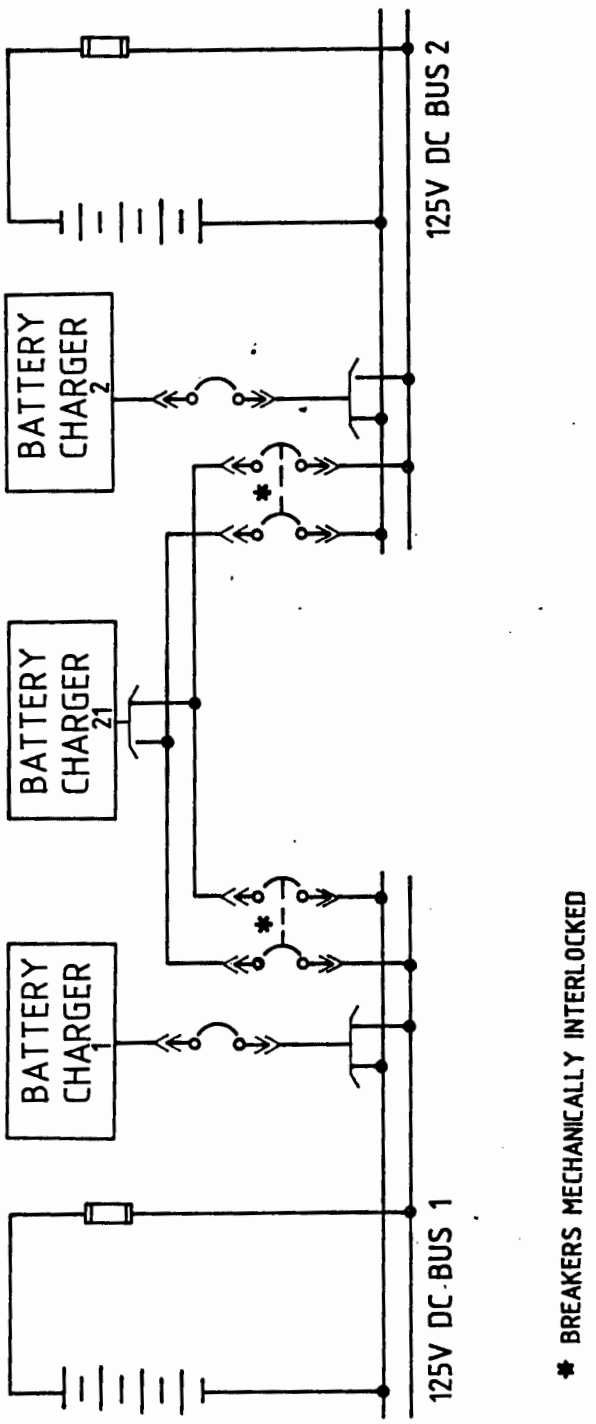


Figure 5.7 "An Additional Charger increases Reliability"

after testing, was that it had not aged substantially. The two main recommendations are:-

1. Temperatures of the internal panel as well as key components be monitored to detect overheating:- overheating usually precedes component failure.

2. The inverter was tested with one or more of the input and output filter capacitors disconnected and was found to be functional. The report recommends that each capacitor be individually fused and alarmed:- therefore the failure of one capacitor in the filter bank will not trip the inverter. The alarm signals the inspection of the remaining capacitors.

Periodic testing is identified as a problem in some plants [93]:- only a few plants do capacity tests on their inverters and chargers. The importance of these items of equipment makes periodic testing essential.

The documentation of failure causes is poor and could be because the maintenance staff are not familiar with the equipment or because time is limited. To improve the reliability of equipment, the failure modes are necessary.

From the failure data available, personnel errors account for about 15% of the total failures documented. As with batteries, the improvement of operating and maintaining the equipment will improve the performance levels considerably.

Thus, personnel training should be improved in the operating and maintenance arenas, and key components used in battery chargers and inverters should be subject to a regular performance testing to detect imminent failure.

---

93 Gunther,W.E., Subudhi,M.,and Taylor,J.H. "OPERATING EXPERIENCE AND AGING-SEISMIC ASSESSMENT OF BATTERY CHARGERS AND INVERTERS", NUREG/CR-4564, US Nuclear Regulatory Commission, June 1986.

Some of these tests could be done while the equipment is on load. Detailed guidelines for a Battery Charger and Inverter Maintenance program are given in a Nuclear Regulatory Commission study [94].

Failures of fast-acting fuses used in inverters and battery chargers to protect the semiconductors is a cause for concern. The failures are attributed to thermal stresses. This is to be investigated at a later stage and could have a significant impact on Nuclear plants due to the extensive use of fuses in safety related electrical equipment. A recent paper indicates that fuse and breaker failures contribute 23% and 6% respectively to inverter failures [95].

To illustrate the performance of battery chargers and inverters, the failure distribution for the Vital Instrumentation & Control Power supplies are given. These power supplies have batteries, battery chargers and inverters to provide ac power (Figure 5.8).

---

94 Gunther,W.E., Lewis,R. and Subudhi,M. "DETECTING AND MITIGATING BATTERY CHARGER AND INVERTER AGING", NUREG/CR-5051, United States Nuclear Regulatory Commission, August 1988.

95 Muhlheim,M.D. and Murphy,G.A. "CAUSES AND EFFECTS OF VITAL INSTRUMENTATION AND CONTROL POWER SUPPLY BUS FAILURES," Nuclear Safety, Volume 28, No.1, January - March 1987, pages 90-7

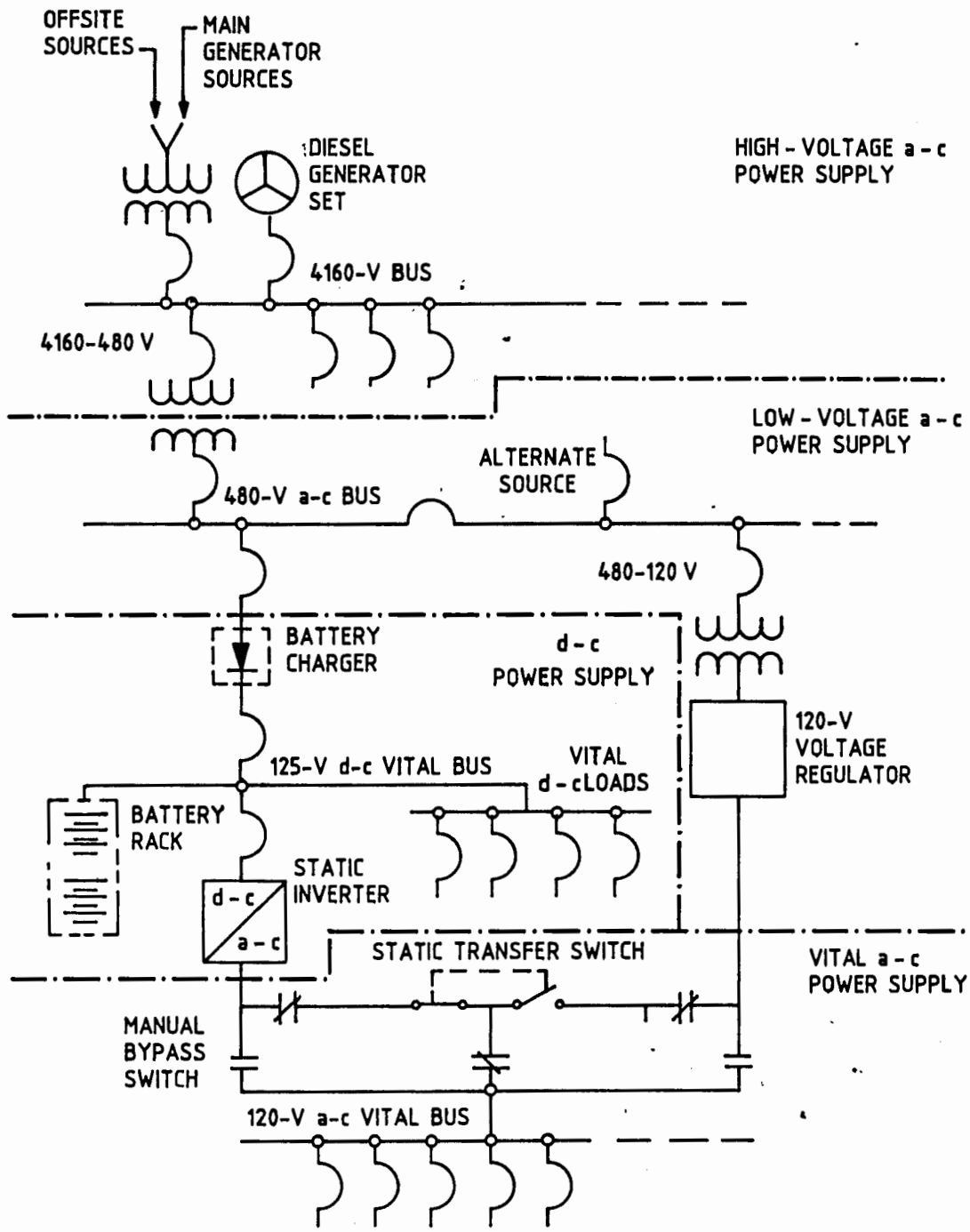


Figure 5.8 "Typical Vital Instrumentation & Control power supply system"

The main causes of Vital Instrumentation & Control Power Supply failure in the United States of America is inverter failure with human error a close second. The figures are [96]:-

Failure Mode	Failure Distribution
Inverter failures	43%
Human Errors	35%
Battery Charger failures	7%
Miscellaneous causes	15%

The inverters are the most complex equipment in the Vital Instrumentation & Control power supplies and these have the highest failure rate. The battery chargers are not as complex and have a better reliability. The batteries are the simplest of all and are not a significant cause of power supply failure.

In West German Nuclear plants, the Vital Instrument and Control systems are powered by 24 Volts dc and not the typical ac of French and American plants [97]. The 24 Volts dc is supplied by batteries and safety related inverters are therefore not required. This leads to an improvement in power supply reliability as there are fewer components in the power supply chain.

96. Muhlheim,M.D. and Murphy,G.A. "CAUSES AND EFFECTS OF VITAL INSTRUMENTATION AND CONTROL POWER SUPPLY BUS FAILURES," Nuclear Safety, Volume 28, No.1, January - March 1987, pages 90-7.

97. Simon,M. "REDUNDANCY PROVES ITS WORTH IN FR GERMANY," Nuclear Engineering International, Volume 32, no.394, May 1987, pages 57.

5.4.3 Direct Current System Layout

The Battery Working Group at Koeberg Nuclear Power Station met with representatives of the battery manufacturer and the main electrical contractor to discuss future maintenance and operation of the batteries. The proposals of the several Electricite de France power stations were discussed.

The outcome of the discussions was that a Voltage-dropping diode system (as used on ESKOM's distribution sub-stations) would be used on all batteries located away from the main plant at Koeberg Nuclear Power Station. A schematic of this system is shown in Figure 5.9:- the voltage monitor switches in blocks of voltage dropping diodes to keep the load voltage constant when the input voltage is raised for Boost charging. Typical dc systems are those in the Chlorine plant and the Demineralized water plant:- these applications are not important to Nuclear safety.

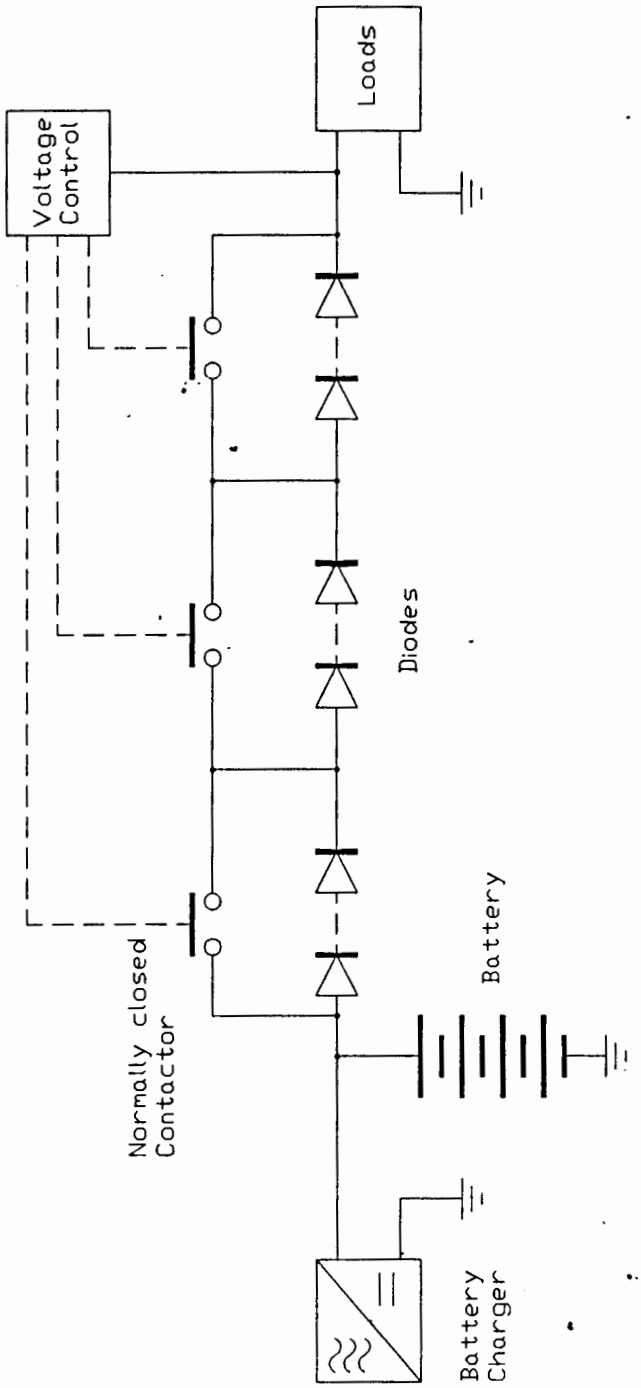


Figure 5.9 "ESKOM Voltage Dropping Diode System"

Direct current systems that are located inside the main plant (some are Safety related) are to be supplied from additional batteries which allow the system batteries to be Boost charged. The author played a significant role in the development of this design. The schematic is shown in Figure 5.10:- the additional battery is the same size as the largest battery in the Division and voltage range, and can be switched so that it supplies the dc system switchboard. The system battery can then be charged, or cycled if necessary, from the additional battery charger. The interconnections need to have mechanical interlocks to ensure the independence of the dc systems.

The author produced a cost benefit analysis for the modification [98] and demonstrated that the modification offers a probable saving of R46 million for an initial outlay of R3.5 million. This is because a battery failure will not cause a forced outage as the dc system can be supplied from the additional battery until the new battery is bought and commissioned. Without the modification, a failed safety related battery that has to flown out from France will result in a forced outage of at least three months. The loss of earnings from the sale of electricity for a single day amounts to over R1 million.

The additional benefits are that a failed Safety Related battery has much less impact on the station safety.

The Voltage dropping diode system does not have the same cost benefit when applied to the main station batteries as the failure of a battery leads to a Forced Outage with the associated loss of electricity sales.

At present, the decision to implement this modification at Koeberg Nuclear Power Station has not been finalized.

---

98. Smyth,T.P. "COST BENEFIT ANALYSIS FOR AUXILIARY BATTERY MODIFICATION", Design & Specification Group, Koeberg Nuclear Power Station, File DSG-241-0002, June 1988.

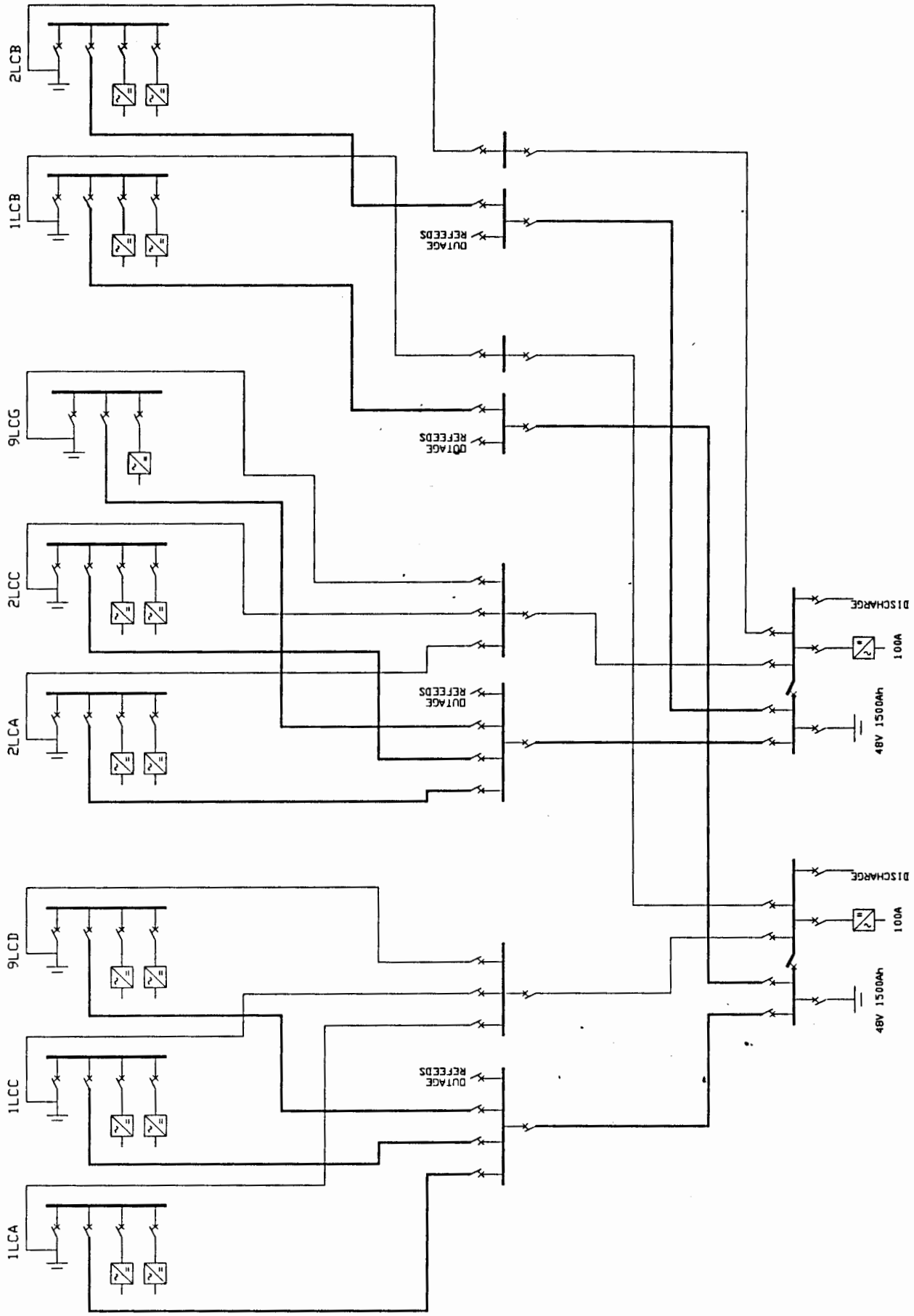


Figure 5.10 "ESKOM Auxiliary Battery System"

5.5 Operator Error.

The high incidence of Human Error leading to loss of power is cause for concern:- the systems should be designed in such a way as to minimize operator error. As a guide, typical figures used for Operator Error in Probabilistic Risk studies are [99]:-

Type of Operation	Fraction of Operations not completed Correctly
Complicated, non-routine	1 in 4
Non-routine, other duties at same time.	1 in 10
Routine, requires care	1 in 100
Routine, simple	1 in 1000
Simplest possible operation	1 in 10 000

These figures apply to Normal operating conditions and the message is that the more complex the action, the higher the probability is that the operator will make a mistake. This is the reason the configuration of the dc systems at Nuclear Power Plants are kept simple:- a complex interconnected system would result in more operating errors.

There are two schools of thought on the way to increase the reliability of Nuclear Power Stations:- the one is to reduce the complexity and therefore the number of plant items, and the other, to add more redundant equipment to assure the functionality of the safety systems.

---

99 Whittingham,R.B. "HUMAN FACTORS IN RELIABILITY AND SAFETY - A PRAGMATIC APPROACH", Nuclear Safety and Reliability Assessment Course organized by the Atomic Energy Corporation of South Africa and the University of Cape Town, Pretoria, 24 June to 5 July, 1985.

1. The first approach is illustrated by the Westinghouse Advanced Pressurized Water Reactor design [100]:- to increase the plant reliability, Westinghouse are altering the reference plant design wherever possible to simplify licensing, construction, operation, and maintenance. Thus, the building volume has been reduced by 55%, there are 60% fewer valves, 50% fewer large pumps, 60% less pipe, 50% less heat exchangers, and 80% fewer control cables.

   Furthermore, the plant is passively safe, that is, the shutdown systems will carry out their functions indefinitely without any operator intervention. Fewer components coupled with a passively-safe design will lead to a more reliable plant and to lower capital costs:- a 40% saving over present day plants is estimated. The cost is estimated to be $762 million for a 600MW (electric) plant.

2. The second approach is illustrated by the British Sizewell B Nuclear Power Station:- instead of the usual two safety trains, the Sizewell B design calls for four [101]. Thus there are four high head safety injection pumps, six main feedwater pumps, four auxiliary feedwater pumps, and four diesel generators. The electrical network is complex as there are four independent safety trains and approximately twice as much equipment as in a two train plant. The Probabilistic Risk Assessments of the design indicate that the frequency of a large uncontrolled release of radioactivity to the environment is less than 10^{-7} per reactor per year.

---

100. "600-MWe APWR FORECAST TO COST $762 MILLION," Nuclear News, October 1988.

101. George,B.V. "THE DESIGN OF THE PWR TO MEET UK REQUIREMENTS", The Nuclear Engineer, Volume 25, No.5, Sept/Oct 1984, pp. 176 to 180.

Typical figures for Operator Error in Emergency situations are [102]:-

Time since incident	Fraction of Operations not completed Correctly
Within 1 minute	1 in 1
After 5 minutes	9 in 10
After 30 minutes	1 in 10
After some hours	1 in 100

The significance of these figures is that an emergency situation at a Nuclear Power Station must be detected automatically. The necessary Engineered Safety feature actions must be initiated automatically as the operator cannot be relied upon to make decisions in the first 5 minutes.

102 Whittingham,R.B. "HUMAN FACTORS IN RELIABILITY AND SAFETY - A PRAGMATIC APPROACH", Nuclear Safety and Reliability Assessment Course organized by the Atomic Energy Corporation of South Africa and the University of Cape Town, Pretoria, 24 June to 5 July, 1985.

5.6 Summary of Trends

The trends noted in the Emergency electric power supply systems at PWR Nuclear Power Plants are:-

1. The use of Probabilistic Risk analysis is increasing as it provides quantitative information on design weaknesses.

2. The main improvements to the ac power systems are to reduce the impact of a Station Blackout. The main Station Blackout modifications are:-

   2.1 The addition of an extra diesel generator or a gas turbo-generator.
   2.2 The addition of equipment to protect the Primary pump seals.
   2.3 For new plants, the Engineered Safety Features consist of four redundant Safety trains rather than the usual two of the older plants.

3. The improvements to the dc power systems are to increase the reliability of power supply. The main areas of concern are:-

   3.1 Overheating of batteries leading to early failures.
   3.2 Poor battery monitoring techniques leading to undercharged cells.
   3.3 Overheating of Battery chargers and Inverters leading to early failures.
   3.4 The lack of periodic testing and monitoring of Battery chargers and Inverters.
   3.5 The large percentage of the failures of Batteries, Battery chargers and Inverters attributed to Operator Error.

6. Recommendations for Utilities

The information presented in the previous chapter is used to formulate recommendations for Existing Nuclear Power Plants, and for Future Nuclear Power Plants. The recommendations are written in a straight-forward manner in the interests of brevity and clarity.

6.1 Actions for Existing Utilities

Existing utilities should justify all modifications with a cost benefit analysis as it may be cheaper to improve the maintenance of equipment rather than to implement modifications.

The recommendations for existing utilities resulting from the trends noted in the previous chapter are:-

6.1.1 Station Blackout

The utility should perform a Probabilistic Risk Assessment to quantify the risk of a Station Blackout. The results of the study should indicate if and where any improvements are needed in the ac or dc electric power systems. Typical modifications to the ac systems would be the addition of additional generating equipment like a diesel or steam driven generator. Modifications to the dc systems could be extra battery chargers, or extra batteries.

The utility should keep a history record of all failures of Engineered Safety Feature equipment and of the grid network so that the Risk Assessment can be validated from time to time.

Once the mechanisms for coping with a Station Blackout are in place, a detailed procedure is necessary to minimize

operator error. For example, the French have a complete procedure "H3" which covers their Blackout coping systems.

6.1.2 Diesel Generators

Utilities should pay particular attention to the maintenance of the engine governor as the failure of this item is the most significant of all diesel failure modes.

6.1.3 Batteries

High battery temperature caused by overcharging, high ripple current, or a high ambient temperature has a marked effect on battery life:- utilities should ensure that the battery chargers are tested regularly so that the batteries are correctly charged. The temperature of the battery rooms should be kept at or below 25 deg.C:- air conditioning should be installed if necessary.

Operating history in the United States of America indicates that cells are not being maintained as well as they should be. The non-intrusive battery monitoring method proposed by Berndt should be used to monitor the condition of the batteries:- the need for maintenance will be determined by the battery condition.

The initial commissioning of Lead-acid batteries is very important as it determines the behavior and life of the batteries.

Batteries should be given "deep" rejuvenating discharges at every outage and batteries that are out of specification should be "cycled".

The use of a gas bubbler system on the batteries to ensure full charge should be considered:- the agitation of the

electrolyte should eliminate electrolyte stratification and the resulting false Specific Gravity measurements.

6.1.4 Battery Chargers and Inverters

Large Electrolytic and Oil filled capacitors should be replaced every 4 to 6 years as these are the most significant cause for equipment failure.

A temperature survey of Chargers and Inverters should be performed as overheating has been identified as the major contributor to aging failures. The addition of forced cooling may be required.

Immediate detection of battery charger failure is required as the battery will be discharged by the time the low board voltage alarm is activated. Furthermore, an automatic trip of the entire dc board is necessary once the voltage drops below the board minimum:- this is to eliminate spurious control relay operation at low voltages. Spurious, unpredictable operation is worse than no automatic control at all.

Periodic testing and Condition monitoring of Battery Chargers and Inverters is necessary. The documentation of failure causes is necessary to establish areas needing improvement. Temperature monitoring of key components for overheating is a good indicator of impending failure. Fuse failures should be documented:- the manufacturer of the fuses should be included in the records so that any correlation can be identified.

Operating and maintenance procedures for the Vital Instrumentation & Control Power supplies should be improved to reduce the large proportion of failures attributed to human error.

6.2 Actions for Power plants being designed.

Simple design changes can have a marked effect on the lifetime performance of a Nuclear Power Plant. These changes are most easily effected at the design stage.

The recommendations based on the contents of this thesis for the design of various equipment are:-

6.2.1 Station Blackout

The design process for modern Nuclear Power Stations usually involves a Probabilistic Risk study. This study should address the Station Blackout event. One method to reduce the impact of Station Blackout is to use Steam to power Engineered Safety Feature equipment:- thus the power sources are diversified which leads to independence and a lower risk of Common Mode failure. Another method to reduce the impact of Station Blackout is to have more redundant power sources:- use four diesel generators or extra battery banks. The Probabilistic Risk study will dictate the exact combinations of equipment that meet the Licensing Authorities requirements.

6.2.2 Diesel Generators

The historical failure modes of Diesel Generators should be examined closely and the design changed accordingly. The engine governor is the main cause of diesel generator failure and the design of this item should be improved. Other significant failure modes are detailed in Section 5.3.1.

6.2.3 Batteries

The life of Lead-acid batteries can be extended by keeping the battery room temperature below 25 deg.C and by ensuring that well filtered battery chargers and inverters are used. Furthermore, an air bubbler system which agitates the electrolyte will eliminate electrolyte stratification and assure full charge of the cells.

The initial commissioning of Lead-acid batteries is very important as it determines the behavior and life of the batteries. Therefore when the new plant is commissioned, the batteries must not be neglected:- the commissioning and maintenance procedures should be in place to control the work.

Diversification of battery types should lead to system reliability improvements as each type has different failure modes and frequencies. Thus Nickel Cadmium cells could be used in one Safety train while Lead-acid cells are used in the other.

6.2.3 Battery Chargers and Inverters

The design of battery chargers should call for fewer Electrolytic and Oil filled Capacitors. Pulse width modulation techniques could be used in the inverters or battery chargers to eliminate the need for large filtering capacitors. Where a large filtering capacitor bank is used, each capacitor should be individually fused and alarmed:- the failure of a capacitor will not trip the Inverter, but the operators will be aware that the inverter needs maintenance. Surge suppression equipment is recommended on the inputs to Chargers and Inverters.

Natural cooling should not be used in this equipment as aging is accelerated by high temperatures. The

qualification specification should call for the temperatures of all major components to be measured under operating conditions:- this provides the reference values for Condition based maintenance of the equipment.

During construction and commissioning, care should be taken to ensure that Chargers and Inverters are not prematurely aged by electrical or physical stresses.

The operation of the equipment should be kept simple:- operator error is a significant failure mode for Chargers and Inverters.

6.2.4 Vital Instrumentation & Control Power supplies

The inverters are the main cause of Vital Instrumentation & Control power supply failures:- this is understandable as they are complex items of plant. The West German approach which eliminates the need for inverters is therefore attractive. Their approach is to power the Vital Instrumentation & Control equipment with 24 dc. The overall power supply system is therefore simpler and a reduction in operator error can be expected. Operator error is the second highest cause of Vital Instrumentation & Control Power supply failure.

To conclude, the standard PWR Nuclear Power Plant designed in 1970 utilized a dual Safety train concept. With the increased use of Probabilistic Risk Analysis, the Station Blackout Scenario became a significant Safety concern for these plants.

Several responses to reduce the impact of Station Blackout were implemented, and essentially took the form of extra power sources such as diesel, steam-turbine or gas-turbine generators, or an increase in the number of redundant Safety trains for the newer designs.

The specific combinations of additional or modified equipment is dictated by the Probabilistic Risk Assessments, and is specific to each plant configuration.

The loss of all alternating current power sources is not the only important electrical accident, the direct current systems are also vital to plant reliability.

Lead-acid batteries are used to provide direct current power:- new cell designs are qualified more stringently, especially for Seismic withstand capability. Direct Current equipment failure mode history allows new equipment to be designed to be more reliable, and guides the application of Condition Based maintenance.

Finally the significant contribution that Human Error makes to equipment and system failure should lead to designs that are more user-friendly, and should reduce this source of plant unreliability.

7.0 References

"600-MWe APWR FORECAST TO COST $762 MILLION," Nuclear News, October 1988.

"CHERNOBYL: THE SOVIET REPORT," Nuclear News, October 1986.

"CODE OF FEDERAL REGULATIONS, Chapter 10, ENERGY", Published by the Office of the Federal Register, National Archives and Records Service, General Services Administration, United States of America, January 1981.

"THE WILLARD STORAGE BATTERY", Willard, P.O.Box 4025, Port Elizabeth, 6014, RSA, Form 6750, April 1982.

Atomic Energy Board of South Africa "LICENSING OF NUCLEAR INSTALLATIONS: A GUIDE TO THE REQUIREMENTS FOR SAFETY ASSESSMENT", document no. LBG/1, issue 3, May 1979.

Battle,R.E., Campbell,D.J. and Baranowsky,P.W. "RELIABILITY OF THE EMERGENCY AC POWER SYSTEM AT NUCLEAR POWER PLANTS." Proceedings of the International Meeting on Thermal Nuclear Reactor Safety held at Chicago, Illinois on August 29 - September 2, 1982, Volume 1, NUREG/CP-0027-V1 Part 2 of 2.

Berger,W. and Hammersley,R. "COPING WITH THE NUCLEAR STATION BLACKOUT RULE COULD PROVE EXPENSIVE", Power Engineering (USA), Volume 91, no.1, January 1987.

Berndt,D. "STATIONARY LEAD ACID BATTERIES, OPERATIONAL CONDITIONS, FUTURE ASPECTS," presented at Symposium on Standby & Uninterruptable Power Supplies, organized by South African Institute of Electrical Engineers and The Association of Municipal Electricity Undertakings of South Africa, 17 to 18 September 1986, paper I1.

Boettger,K., Engineer, AEG company, verbal communication, 1986.

Boikess,R.S. and Edelson,E. "CHEMICAL PRINCIPLES", Harper & Row, New York, 1978.

CASTLE,J.R. "INFLUENCE OF NUCLEAR SAFETY REQUIREMENTS FOR CEGB GAS COOLED REACTORS ON DESIGN OF THEIR ELECTRICAL AUXILIARY SYSTEMS." IEE Proceedings C (Generation, Transmission and Distribution), Volume 128, no.2, pages 117-21, March 1981.

Chu, T., Yoon, W.H., and Fitzpatrick, R.G. "AN ANALYSIS OF LOSS OF OFF-SITE POWER WITH A PWR AT SHUTDOWN", Transactions of American Nuclear Society (USA), Vol.55, 15-19 Nov., 1987, pp 452-3.

Daniels,G.H. "ELECTRICAL SYSTEM DESIGN FOR FUTURE AGR POWER STATIONS", IEE Proceedings C (Generation, Transmission and Distribution), Volume 128 no.2, March 1981, pages 123-8.

Dasoyan, M.A. and Aguf,I.A. "CURRENT THEORY OF LEAD ACID BATTERIES", Technicopy, Stonehouse, England, 1979.

Edson,J.L. and Hardin,J.E. "AGING OF CLASS 1E BATTERIES IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS," NUREG/CR-4457, United States Nuclear Regulatory Commission, July 1987.

Electricite de France, "PALIER-900," Information brochure, June 1982.

Electricite de France, "PWR PLANT BLACKOUT, EDF'S RESPONSE", written by M.M.Gelle, Engineering and Construction Division, January 1988.

Electricite de France. "EDF 900 MWe NUCLEAR POWER PLANTS, SHORT TECHNICAL DESCRIPTION." issued by Service d'Equipment Nucleaire Exterieur, 11-13 Avenue de Friedland, 75008 PARIS, May 1983.

ESKOM Memorandum from Engineering Investigations Manager to Power Station Manager, Koeberg Nuclear Power Station, Ref. OT243,Acc.No,309590, dated 23 April 1987.

ESKOM Surveillance Report RSV/86/002/VD/927, Koeberg Nuclear Power Station Computer Ref. 192341R, dated 18 July 1986.

ESKOM, Nuclear Engineering Division, Report 1124602 "Loss of Electric Power Supplies", March 1989.

IAEA-TECDOC-390 "SAFETY ASSESSMENT OF EMERGENCY ELECTRIC POWER SYSTEMS FOR NUCLEAR POWER PLANTS", subtitled "A manual on the use of IAEA Safety Series No.50-SG-D7: Emergency Power Systems at Nuclear Power Plants", issued by the International Atomic Energy Agency, Vienna, 1986.

Friedman E J et al "ELECTROTECHNOLOGY VOL 3, Stationary Lead acid Batteries, "Applications and Performance", Ann Arbor Science Publishers Inc;, Michigan, 1980

George,B.V. "THE DESIGN OF THE PWR TO MEET UK REQUIREMENTS", The Nuclear Engineer, Volume 25, No.5, Sept/Oct 1984, pp. 176 to 180.

Gunther,W.E. "TESTING OF A NATURALLY AGED NUCLEAR POWER PLANT INVERTER AND BATTERY CHARGER", NUREG/CR-5192, United States Nuclear Regulatory Commission, September 1988.

Gunther,W.E., Lewis,R. and Subudhi,M. "DETECTING AND MITIGATING BATTERY CHARGER AND INVERTER AGING", NUREG/CR-5051, United States Nuclear Regulatory Commission, August 1988.

Gunther,W.E., Subudhi,M.,and Taylor,J.H. "OPERATING EXPERIENCE AND AGING-SEISMIC ASSESSMENT OF BATTERY CHARGERS AND INVERTERS", NUREG/CR-4564, US Nuclear Regulatory Commission, June 1986.

Koeberg Nuclear Power Station, Specification for Lead-acid Batteries, Ref. Maintenance Manual 315 "LEAD ACID BATTERIES".

Kolaczkowski,A.M., Payne,A.C. and Baranowsky,P.W. "ANALYSIS OF STATION BLACKOUT ACCIDENTS FOR LWR's", Proceedings of the International Meeting on Thermal Nuclear Reactor Safety held at Chicago, Illinois on August 29 - September 2, 1982, Volume 1, NUREG/CP-0027-V1 Part 2 of 2.

Melcot,B. "HOW EdF BRINGS ITS PWRs TO A SAFE SHUTDOWN DURING BLACKOUT", Nuclear Engineering International, Volume 32, no.394, May 1987, pages 55-6.

Morley,M "KOEBERG BATTERIES", KOEBERG Computer Reference 201124R, 28 October 1986.

Muhlheim,M.D. and Murphy,G.A. "CAUSES AND EFFECTS OF VITAL INSTRUMENTATION AND CONTROL POWER SUPPLY BUS FAILURES," Nuclear Safety, Volume 28, No.1, January - March 1987, pages 90-7

Nielsen,D. "AUXILIARY POWER SYSTEM FOR THE DIABLO CANYON NUCLEAR PLANT," IEEE Power Engineering Society Summer Meeting (Text of A Papers), Portland, ORE, USA, 18-23 July 1976, pages A76 300-4/1-5.

Okrent,D. "NEW TRENDS IN SAFETY DESIGN AND ANALYSIS," IAEA-CN-39/6.4, Proc. Int. Conf. on Current Nuclear Power Plant Safety Issues, IAEA, Stockholm, 20-24 October, 1980

Regulatory Guide 1.32 "Criteria for Safety-related Electric Power Systems for Nuclear Power Plants," United States Nuclear Regulatory Commission, Washington, D.C. 20555.

Regulatory Guide 1.53 "Application of the Single Failure Criterion to Nuclear Power Plant protection system," United States Nuclear Regulatory Commission, Washington, D.C. 20555.

Regulatory Guide 1.6 "Independence between redundant stand-by (onsite) power sources and between their distribution systems," United States Nuclear Regulatory Commission, Washington, D.C. 20555.

Regulatory Guide 1.75 "Physical independence of Electric Systems," United States Nuclear Regulatory Commission, Washington, D.C. 20555.

Regulatory Guide 1.9 "Selection, Design and Qualification of Diesel-Generator Units used as Standby (Onsite) Electric Power Systems at Nuclear Power Plants," United States Nuclear Regulatory Commission, Washington, D.C. 20555.

Reisch, F. "TECHNICAL NOTE: SWEDEN'S DECEMBER 1983 GRID COLLAPSE AND THE NUCLEAR POWER PLANT'S RESPONSE", Nuclear Safety, Vol.26, No.2, March/April 1985, pp 153-6.

Reisch,F. "COPING WITH STATION BLACKOUT", Nuclear Engineering International, Volume 30, no.375, October 1985, pages 48 to 51.

Report IEEE Standard 308 "IEEE STANDARD CRITERIA FOR CLASS 1E POWER SYSTEMS FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1980.

Report IEEE Standard 323 "IEEE STANDARD FOR QUALIFYING CLASS 1E EQUIPMENT FOR NUCLEAR POWER GENERATING STATIONS",The Institute for Electrical and Electronic Engineers, New York, USA, 1983, page 10, sect.4 para.2.

Report IEEE Standard 379 "IEEE STANDARD APPLICATION OF THE SINGLE FAILURE CRITERION TO NUCLEAR POWER GENERATING STATION CLASS 1E SYSTEMS",The Institute for Electrical and Electronic Engineers, New York, USA, 1977

Report IEEE Standard 387 "IEEE STANDARD CRITERIA FOR DIESEL-GENERATOR UNITS APPLIED AS STANDBY POWER SUPPLIES FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1977.

Report IEEE Standard 450 "RECOMMENDED PRACTICE FOR MAINTENANCE, TESTING, AND REPLACEMENT OF LARGE LEAD STORAGE BATTERIES FOR GENERATING STATIONS AND SUBSTATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1980.

Report IEEE Standard 484 "IEEE RECOMMENDED PRACTICE FOR INSTALLATION DESIGN AND INSTALLATION OF LARGE LEAD STORAGE BATTERIES FOR GENERATING STATIONS AND SUBSTATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1981.

Report IEEE Standard 485 "IEEE RECOMMENDED PRACTICE FOR SIZING LARGE LEAD STORAGE BATTERIES FOR GENERATING STATIONS AND SUBSTATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1983.

Report IEEE Standard 500 "RELIABILITY DATA",The Institute for Electrical and Electronic Engineers, New York, USA, 1977.

Report IEEE Standard 535 "IEEE STANDARD FOR QUALIFICATION OF CLASS 1E LEAD STORAGE BATTERIES FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1979.

Report IEEE Standard 603 "IEEE STANDARD CRITERIA FOR SAFETY SYSTEMS FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1980.

Report IEEE Standard 650 "IEEE STANDARD FOR QUALIFICATION OF CLASS 1E STATIC BATTERY CHARGERS AND INVERTERS FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1979.

Report IEEE Standard 650 "IEEE STANDARD FOR QUALIFICATION OF CLASS 1E STATIC BATTERY CHARGERS AND INVERTERS FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1979. Appendix B, page 22.

Report IEEE Standard 765 "IEEE STANDARD FOR PREFERRED POWER SUPPLY FOR NUCLEAR GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1983.

Report IEEE Standard 946 "IEEE RECOMMENDED PRACTICE FOR THE DESIGN OF SAFETY RELATED DC AUXILIARY POWER SYSTEMS FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1985.

Simon,M. "REDUNDANCY PROVES ITS WORTH IN FR GERMANY," Nuclear Engineering International, Volume 32, no.394, May 1987, pages 57.

Smyth,T.P. "COST BENEFIT ANALYSIS FOR AUXILIARY BATTERY MODIFICATION", Design & Specification Group, Koeberg Nuclear Power Station, File DSG-241-0002, June 1988.

Smyth,T.P. "Representative Stationary Battery Experience", Design & Specification Group, Koeberg Nuclear Power Station, Report DSG-550-002, Sept 1987.

Tudor representative, verbal communication, February 1987.

United States of America, Military Document Ref.MIL HDBK 217 "RELIABILITY DATA".

Westinghouse Training manual "PLANT SYSTEMS ENGINEER", prepared for ESKOM, 1985

Whittingham,R.B. "HUMAN FACTORS IN RELIABILITY AND SAFETY - A PRAGMATIC APPROACH", Nuclear Safety and Reliability Assessment Course organized by the Atomic Energy Corporation of South Africa and the University of Cape Town, Pretoria, 24 June to 5 July, 1985.

Winkler,B.C. "QUANTIFICATION OF SAFETY STANDARDS," Nuclear Safety and Reliability Assessment Course organized by the Atomic Energy Corporation of South Africa and the University of Cape Town, Pretoria, 24 June to 5 July, 1985.

Wyckof,H. "LOSS OF OFF-SITE POWER EXPERIENCE AT U.S. NUCLEAR POWER PLANTS-ALL YEARS THROUGH 1984", Proceedings of the American Power Conference, Chicago,Il,USA, 22-24 April 1985, pp 791-6.

Wyckoff,H. "THE RELIABILITY OF EMERGENCY DIESEL GENERATORS AT U.S. NUCLEAR POWER PLANTS", NSAC-108, Electric Power Research Institute, California, September, 1986.

Young,R.A. "ADDITIONAL ELECTRICAL DESIGN CONSIDERATIONS EMPLOYED AT DIABLO CANYON NUCLEAR POWER PROJECT," IEEE Power Engineering Society Summer Meeting (Text of A Papers), Portland, ORE, USA, 18-23 July 1976, pages A76 438-2/1-6.

8.0 Bibliography

"IAEA SAFETY GUIDE No. 50-SG-D7", International Atomic Energy Agency, Vienna, 1982.

Berger, W.E. and McCauley, T.M. "MONITORING CHANGES IN THE AC/DC AUXILIARY POWER SYSTEM", Trans. of the American Nuclear Society (USA), Vol.54, suppl. 1, 1987, pages 139-41.

Dasgupta, S. and Murphy,J.J. "DEGRADED OR LOSS OF VOLTAGE PROTECTION OF CLASS 1E AUXILIARY POWER SYSTEMS IN A NUCLEAR POWER PLANT", IEEE Transactions on Nuclear Science, Vol.NS-26, No.1, February 1979.

Electricite de France. "EDF 1300 MWe NUCLEAR POWER PLANTS, SHORT TECHNICAL DESCRIPTION." issued by Service d'Equipment Nucleaire Exterieur, 11-13 Avenue de Friedland, 75008 PARIS, June 1983.

Killen, T.S. and Damar,R.M. "STANDARDIZED ELECTRICAL AUXILIARY SYSTEM FOR SNUPPS", IEEE Trans. on Power Apparatus & Systems, Vol. PAS 96, no.5,Sept/Oct 1977, pp 1602-7.

Koepfinger, J.L. and Khunkhun, K.J.S. "PROTECTION OF AUXILIARY POWER SYSTEMS IN A NUCLEAR POWER PLANT", IEEE Trans. on Power Apparatus and Systems, Vol.PAS-98, No.1, Jan/Feb 1979.

Masche,G. "SYSTEMS SUMMARY OF A WESTINGHOUSE PWR NUCLEAR POWER PLANT", Westinghouse Electric Corporation, August 1973.

Nielsen,D. "AUXILIARY POWER SYSTEM FOR THE DIABLO CANYON NUCLEAR PLANT," IEEE Power Engineering Society Summer Meeting (Text of A Papers), Portland, ORE, USA, 18-23 July 1976, pages A76 300-4/1-5.

Reisch,F. and Fransson,R. "RECENT DEVELOPMENTS IN POWER SUPPLY NEEDS", Nuclear Engineering International, Vol.25, no.294, January 1980, pp39-42.

Rice, B.M. et al, "IEEE 603-308 AD HOC COMMITTEE REPORT", IEEE Transactions on Nuclear Science, Vol.NS-26, No.1, February 1979, pp 871-887.

9.0 Drawing Credits

Figure 2.1 Adapted from: Masche,G. "SYSTEMS SUMMARY OF A WESTINGHOUSE PWR NUCLEAR POWER PLANT", Westinghouse Electric Corporation, August 1973.

Figure 2.2 Adapted from: Electricite de France. "EDF 900 MWe NUCLEAR POWER PLANTS, SHORT TECHNICAL DESCRIPTION." issued by Service d'Equipment Nucleaire Exterieur, 11-13 Avenue de Friedland, 75008 PARIS, May 1983.

Figure 2.3 Adapted from: Electricite de France. "EDF 900 MWe NUCLEAR POWER PLANTS, SHORT TECHNICAL DESCRIPTION." issued by Service d'Equipment Nucleaire Exterieur, 11-13 Avenue de Friedland, 75008 PARIS, May 1983.

Figure 2.4 Sourced from: Electricite de France. "EDF 900 MWe NUCLEAR POWER PLANTS, SHORT TECHNICAL DESCRIPTION." issued by Service d'Equipment Nucleaire Exterieur, 11-13 Avenue de Friedland, 75008 PARIS, May 1983.

Figure 2.5 Adapted from: CGEE Alsthom CONSULTANT Training Documentation, 1987.

Figure 2.6 Adapted from: CGEE Alsthom CONSULTANT Training Documentation, 1987.

Figure 2.7 Adapted from: Electricite de France. "EDF 900 MWe NUCLEAR POWER PLANTS, SHORT TECHNICAL DESCRIPTION." issued by Service d'Equipment Nucleaire Exterieur, 11-13 Avenue de Friedland, 75008 PARIS, May 1983.

Figure 2.8 Adapted from: Electricite de France. "EDF 900 MWe NUCLEAR POWER PLANTS, SHORT TECHNICAL DESCRIPTION." issued by Service d'Equipment Nucleaire Exterieur, 11-13 Avenue de Friedland, 75008 PARIS, May 1983.

Figure 2.9 Adapted from: Electricite de France. "EDF 900 MWe NUCLEAR POWER PLANTS, SHORT TECHNICAL DESCRIPTION." issued by Service d'Equipment Nucleaire Exterieur, 11-13 Avenue de Friedland, 75008 PARIS, May 1983.

Figure 3.1 Sourced from: Report IEEE Standard 650 "IEEE STANDARD FOR QUALIFICATION OF CLASS 1E STATIC BATTERY CHARGERS AND INVERTERS FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1979.

Figure 3.2 Sourced from: Winkler,B.C. "QUANTIFICATION OF SAFETY STANDARDS," Nuclear Safety and Reliability Assessment Course organized by the Atomic Energy Corporation of South Africa and the University of Cape Town, Pretoria, 24 June to 5 July, 1985.

Figure 3.3 Author's original.

Figure 3.4 Author's original.

Figure 3.5 Author's original.

Figure 3.6 Author's original.

Figure 3.7 Author's original.

Figure 3.8 Author's original.

Figure 3.9 Sourced from: Report IEEE Standard 603 "IEEE STANDARD CRITERIA FOR SAFETY SYSTEMS FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1980.

Figure 3.10 Sourced from: Report IEEE Standard 603 "IEEE STANDARD CRITERIA FOR SAFETY SYSTEMS FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1980.

Figure 3.11 Sourced from: Report IEEE Standard 603 "IEEE STANDARD CRITERIA FOR SAFETY SYSTEMS FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1980.

Figure 3.12 Sourced from: Report IEEE Standard 603 "IEEE STANDARD CRITERIA FOR SAFETY SYSTEMS FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1980.

Figure 3.13 Sourced from: Report IEEE Standard 603 "IEEE STANDARD CRITERIA FOR SAFETY SYSTEMS FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1980.

Figure 4.1 Sourced from: Electricite de France. "EDF 900 MWe NUCLEAR POWER PLANTS, SHORT TECHNICAL DESCRIPTION." issued by Service d'Equipment Nucleaire Exterieur, 11-13 Avenue de Friedland, 75008 PARIS, May 1983.

Figure 4.2 Adapted from: Electricite de France. "EDF 900 MWe NUCLEAR POWER PLANTS, SHORT TECHNICAL DESCRIPTION." issued by Service d'Equipment Nucleaire Exterieur, 11-13 Avenue de Friedland, 75008 PARIS, May 1983.

Figure 4.3 Sourced from: Report IEEE Standard 387 "IEEE STANDARD CRITERIA FOR DIESEL-GENERATOR UNITS APPLIED AS STANDBY POWER SUPPLIES FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1977.

Figure 4.4 Sourced from: Report IEEE Standard 765 "IEEE STANDARD FOR PREFERRED POWER SUPPLY FOR NUCLEAR GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1983.

Figure 4.5 Sourced from: Report IEEE Standard 946 "IEEE RECOMMENDED PRACTICE FOR THE DESIGN OF SAFETY RELATED DC AUXILIARY POWER SYSTEMS FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1985.

Figure 4.6 Sourced from: Edson,J.L. and Hardin,J.E. "AGING OF CLASS 1E BATTERIES IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS," NUREG/CR-4457, United States Nuclear Regulatory Commission, July 1987.

Figure 4.7 Sourced from: Report IEEE Standard 650 "IEEE STANDARD FOR QUALIFICATION OF CLASS 1E STATIC BATTERY CHARGERS AND INVERTERS FOR NUCLEAR POWER GENERATING STATIONS", The Institute for Electrical and Electronic Engineers, New York, USA, 1979.

Figure 5.1 Sourced from: Melcot,B. "HOW EdF BRINGS ITS PWRs TO A SAFE SHUTDOWN DURING BLACKOUT", Nuclear Engineering International, Volume 32, no.394, May 1987, pages 55-6.

Figure 5.2 Sourced from: Electricite de France, "PWR PLANT BLACKOUT, EDF'S RESPONSE", written by M.M.Gelle, Engineering and Construction Division, January 1988.

Figure 5.3 Sourced from: Reisch,F. and Fransson,R. "RECENT DEVELOPMENTS IN POWER SUPPLY NEEDS", Nuclear Engineering International, Vol.25, no.294, January 1980, pp39-42.

Figure 5.4 Adapted from: Berndt,D. "STATIONARY LEAD ACID BATTERIES, OPERATIONAL CONDITIONS, FUTURE ASPECTS," presented at Symposium on Standby & Uninterruptable Power Supplies, organized by South African Institute of Electrical Engineers and The Association of Municipal Electricity Undertakings of South Africa, 17 to 18 September 1986, paper I1.

Figure 5.5 Author's original.

Figure 5.6 Sourced from: Friedman E J et al "ELECTRO-TECHNOLOGY VOL 3, Stationary Lead acid Batteries, "Applications and Performance", Ann Arbor Science Publishers Inc;, Michigan, 1980

Figure 5.7 Adapted from: Young,R.A. "ADDITIONAL ELECTRICAL DESIGN CONSIDERATIONS EMPLOYED AT DIABLO CANYON NUCLEAR POWER PROJECT," IEEE Power Engineering Society Summer Meeting (Text of A Papers), Portland, ORE, USA, 18-23 July 1976, pages A76 438-2/1-6.

Figure 5.8 Adapted from: Muhlheim,M.D. and Murphy,G.A. "CAUSES AND EFFECTS OF VITAL INSTRUMENTATION AND CONTROL POWER SUPPLY BUS FAILURES," Nuclear Safety, Volume 28, No.1, January - March 1987, pages 90-7

Figure 5.9 Author's original.

Figure 5.10 Author's original.

A. APPENDIX A "A Summary of 10CFR50 For Electrical Engineers"

The Nuclear Regulatory Commission of America lays down the requirements for Nuclear Power Plants in the United States of America and the details of the licensing procedure and license requirements are published in the American Code of Federal Regulations Title 10 - "Energy" Part 50 - "Domestic licensing of production and utilization facilities". [103] (The short form reads 10CFR50.) As the document is a legal one, it has many parts and spells out the requirements in precise terms. As an electrical designer, many sections of 10CFR50 are of no immediate concern, but the sections that are important are:-

10CFR50.34	"Contents of Applications; technical information"
10CFR50.36	"Technical Specifications"
10CFR50.48	"Fire Protection"
Appendix A	"General Design Criteria for Nuclear Power Plants"

A.1 Technical Information

The form and content of the technical part of the license application are laid down in 10CFR50.34 "Contents of Applications; technical information". The applicant must submit a Preliminary Safety Analysis Report before the Construction permit can be issued and a Final Safety Analysis Report before the Operating License can be issued.

---

103. "CODE OF FEDERAL REGULATIONS, Chapter 10, ENERGY", Published by the Office of the Federal Register, National Archives and Records Service, General Services Administration, United States of America, January 1981.

A.1.1 The Preliminary Safety Analysis Report

As the name implies, the Preliminary Safety Analysis Report must present all information necessary for the Nuclear Regulatory Commission to be able to ascertain the impact of the plant on public health and the environment. The Preliminary Safety Analysis Report must therefore have a description of the proposed site of the Nuclear Power Plant and an appraisal of the site in terms of the site evaluation factors laid down in 10CFR100 "Reactor site criteria". Briefly, these factors are:- the characteristics of the reactor design, such as the quantity of radio-active material, the design standards, and the safety features provided to limit the release of radio-active material; the population density around the reactor site; and the physical characteristics of the site, such as the seismic stability of the area.

The Preliminary Safety Analysis Report must also contain a summary description of the design and operating features of the proposed power plant, and the preliminary design of the power plant. The preliminary design must contain the design bases of the plant and, to ensure a common framework, the Nuclear Regulatory Commission provide their minimum design requirements in Appendix A of 10CFR50 "General Design Criteria for Nuclear Power Plants." The materials, general arrangement and approximate dimensions are also included so that the Nuclear Regulatory Commission can ascertain whether the final plant conforms to the original design bases.

A major portion of the Preliminary Safety Analysis Report concerns the performance of the structures, systems and components of the power plant in terms of the safety of the public:- the analysis should detail the safety margins during normal and transient operation; the adequacy of the safety related structures, systems, and components; and the functioning of the Emergency Core Cooling Systems

during all credible loss-of-coolant accidents. Any plant conditions or variables that are likely to be important parts of the plant's specifications should be identified at this stage so that these parameters can be verified before the operating license is issued. Furthermore, the applicant's preliminary emergency plans should be detailed:- the Nuclear Regulatory Commission's recommendations are contained in Appendix E of 10CFR50 "Emergency planning and preparedness for production and utilization facilities."

Further points that should be included in the Preliminary Safety Analysis Report are:- the proposed organization and training of the power plant staff and the technical qualification of the license applicant to build and operate the proposed power plant. Where more than one plant is to built on one site, the license applicant must give details of how the continued safe operation of the operating units will be maintained during the construction of further units. Also required is information about the proposed Quality Assurance Program to be applied to the design, manufacture and construction of the power plant. The Nuclear Regulatory Commission's requirements in this respect are laid down in Appendix B of 10CFR50 "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants."

Finally, the Preliminary Safety Analysis Report should contain information regarding any Research and Development work needed to establish the safe functioning of any component, structure or system. The Nuclear Regulatory Commission will not issue an operating license unless it is satisfied that all safety issues are resolved.

Thus, the Preliminary Safety Analysis Report contains all the information required by the Nuclear Regulatory Commission so that it can determine whether or not the proposed plant will significantly affect the safety and

health of the public. Once the Nuclear Regulatory Commission is satisfied that the proposed plant is safe, a Construction permit is issued.

A.1.2 The Final Safety Analysis Report

When the plant is built, or nearly complete, the Nuclear Regulatory Commission requires a Final Safety Analysis Report to be submitted which will be used to finally determine the overall safety of the Nuclear Power Plant. The Final Safety Analysis Report essentially contains the same information as the Preliminary Safety Analysis Report, but in greater detail and with the plant as-built information.

Thus the Final Safety Analysis Report contains all the plant siting information and shows that the plant conforms to all the relevant site evaluation factors. The plant is described and analyzed in detail complete with the design bases, the justification for the bases, and evaluations showing the successful operation of the various safety functions. In particular and in relation to the electrical design, 10CFR50.34(b) calls for discussions involving the instrumentation & control systems, the electrical systems, and power conversion schemes where any of these affect the plant safety.

The final quantities and nature of radio-active material in the plant is listed, and the manner in which the release of radio-active material is controlled and limited is also given. The amount of radiation the plant operators and the public will be exposed to is also dealt with here:- the limits are set out in 10CFR20 "Standards for protection against radiation."

Again, the major portion of the Final Safety Analysis Report concerns the effect of the plant on the public

health and the environment:- and so, much attention is paid to the analysis and evaluation of the design and performance of the plant systems, structures and components - particularly those associated with the safe shut-down of the reactor and the containment of radio-activity. The Emergency Core Cooling Systems are analyzed and evaluated for all postulated Loss of Coolant Accidents (LOCA's), and where any Research and Development was required to verify the performance of safety related equipment, the results are given now.

The Final Safety Analysis Report must also present details of the organizational structure, the technical qualifications of the license applicant, and the details of the Operator re-qualification program:- the guide-lines for Operator re-qualification are contained in 10CFR55 "Operator's licenses" Appendix A "Requalification programs for Licensed operators of Production and Utilization Facilities." The continued training of Nuclear plant operators is important as this minimizes the possibility of operator error in an accident situation. The Nuclear Regulatory Commission requires details of the administrative controls to be used to assure the safe operation of the plant and the requirements in this regard are laid down in Appendix B of 10CFR50 "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants."

In addition to the administrative controls, the Nuclear Regulatory Commission require plans for pre-operational testing and initial operation of the new equipment. Furthermore, plans for normal operation, surveillance, maintenance and periodic testing as well as plans for emergencies (as set out in Appendix E of 10CFR50), are required. The operating technical specifications as described in 10CFR50.36 are required as part of the license:- if any of the specified criteria are violated

then various actions are laid down, the most stringent being to immediately shut the reactor down completely.

Finally, as in the Preliminary Safety Analysis Report, where more than one plant is to built on one site, the license applicant must give full details of how the continued safe operation of the operating units will be maintained during the construction of further units.

A.1.3 The Physical Security Plan

The Nuclear Regulatory Commission require a satisfactory Physical Security Plan in addition to the Final Safety Analysis Report before an Operating license can be issued. The main purpose of the Physical Security Plan is to prevent sabotaging of the Nuclear reactor or theft of radio-active material.

A.1.4 The Safeguards Contingency Plan

The Nuclear Regulatory Commission also require a Safeguards Contingency Plan:-this is a documented plan with specific responses to various physical security breaches. The Nuclear Regulatory Commission requirements for the Physical Security Plan and the Safeguards Contingency Plan are laid down in 10CFR73 "Physical protection of Plants and Materials."

Thus the Final Safety Analysis Report in conjunction with the Physical Security Plan and the Safeguards Contingency Plan contains sufficient information to allow the Nuclear Regulatory Commission to finally ascertain the safety of the new Nuclear Power Plant. If the Nuclear Regulatory Commission is satisfied with all facets of the power station design, construction, commissioning and

operational structure, an Operating License will be issued.

A.2 General Design Criteria

Appendix A "General Design Criteria for Nuclear Power Plants" of 10CFR50 contains the Nuclear Regulatory Commission's requirements for the design of Nuclear power generating stations. I shall discuss those General Design Criteria applicable to electrical design in some detail, and pass over the other criteria with a short summary.

Appendix A of 10CFR50 contains fifty-five General Design Criteria.

The first five General Design Criteria are overall requirements and lay down conditions for:- Quality Control; protection against natural phenomena (earthquakes, hurricanes, tsunami, etc.); fire protection; protection against accident phenomena (the effects of postulated accidents such as Loss of Coolant Accidents, missiles from the turbines and pipe-whip effects); and for the sharing of structures, systems and components between Units at multiple Unit sites.

The following ten General Design Criteria give the Nuclear Regulatory Commission's guidelines for the prevention of radio-active release by utilizing multiple Fission Product Barriers. Hence the General Design Criteria give requirements for:- the reactor design and operational characteristics; the instrumentation and control equipment used to keep the reactor in a safe operating condition; the design of the Containment structure; the design, inspection and testing of the Electric power supplies; and for the Unit Control Rooms.

The rest of 10CFR50 Appendix A has:- ten General Design Criteria giving requirements for the reactor protection and reactivity control systems; seventeen General Design Criteria applicable to the Fluid systems; eight General Design Criteria applicable to the reactor Containment structure; and the final five concern the control of Nuclear fuel and radio-active material.

Now, the General Design Criteria applicable to Electric power systems are General Design Criteria 17 and 18. The General Design Criterion 17 calls for two main sources of electric power:- onsite and offsite. These power sources should be designed so that the systems important to safety will always be available. The capacity and configuration of these power sources should be such that the Fission Product boundaries remain intact during all possible operational conditions, and that the reactor core is cooled and reactivity contained for all postulated accident conditions.

The batteries and distribution systems of the onsite electric power supplies should have sufficient independence, redundancy, and testability so that they fulfill their safety functions even with a single failure occurring.

The electric power from the offsite transmission network should be supplied by two physically independent circuits which are designed and located so as to minimize the chances that they will fail simultaneously. The Nuclear Regulatory Commission allow a common switchyard and a common right of way for the two independent feeders. Again, each of the offsite power sources must be available independently of whether the other one fails, or all onsite the power sources fail. One of the offsite electric power sources should be available in a few seconds following a Loss of Coolant Accident to ensure the containment of radio-active material.

Appendix A draws the designer's attention to the facts that neither a generator trip, nor an offsite power loss, nor any onsite power losses, shall cause the loss of any of the remaining power supplies.

General Design Criteria 18 gives the requirements for the inspection and testing of the electric power systems. The electric power systems important to safety should be designed so that periodic inspection and testing of the wiring, insulation, connections, and switchboards can be carried out. The purpose of these inspections and test are to ensure that the electric power systems remain as reliable as possible. Both the systems as a whole, and the parts there-of are tested periodically under conditions that mimic the design operating state as closely as possible. Examples of system components are relays, switches and busbars; and system examples are the reactor protection system, and the electric power transfer systems between the offsite, onsite and intra-unit power sources and sinks.

A.3 Plant Technical Specifications

The third section of 10CFR50 that is important to the electrical designer is 10CFR50.36 "Technical Specifications". The technical specification of a Nuclear Power Station contains the safety limits for those process parameters of the plant which, if exceeded, would significantly increase the chances of a radio-active release occurring. The Operating License therefore has a clause that instructs the plant operators to immediately shut the reactor down if any safety limit is exceeded and the Nuclear Regulatory Commission must sanction the continued operation of the plant before the start-up of the plant.

The technical specification also contains limiting safety system settings for the automatic protection systems:- these are the limits for those variables controlled by the automatic protection systems such as the Reactor Protection System. That is to say, that the automatic protection system must never allow the controlled variable to exceed the limiting safety system setting for that variable. Should an automatic protection system not function as required during normal operation, then the technical specification requires appropriate action or even reactor shut-down. The purpose of the limiting safety system setting is to prevent a safety limit being exceeded. This is a serious condition requiring much investigation before the plant can operate again. A transgression of a limiting safety system setting, however, is resolved by the plant operator and he decides when to start up the plant again. The Nuclear Regulatory Commission nevertheless requires all information about the incident and the justification for plant re-start.

The plant specification contains the limiting conditions for operation:- these are the minimum functional or performance levels that can be tolerated in equipment important to safety. Again, the reactor may have to be shut down if a limiting condition for operation is exceeded.

Surveillance requirements are included in the plant specification:- these are to make sure that the equipment important to safety is functioning correctly so that the plant does not exceed any safety limits and remains within the operational limiting conditions. The surveillance requirements apply to testing, calibration and inspection.

The final part of the technical specifications provide for administrative controls such as procedures and recordkeeping which are needed to operate the plant safely.