Evaluation and verification of an architecture suitable for a multi-unit control room of a pebble bed High Temperature Reactor Nuclear Power Plant

H Visagie

24034002

Dissertation submitted in partial fulfilment of the requirements for the degree *Magister* in Nuclear Engineering at the Potchefstroom Campus of the North-West University

Supervisor: Dr AC Cilliers

May 2015

ACKNOWLEDGEMENTS

I am grateful for my family, namely Anelda, Reinhardt, Elske and Marnitz for their understanding, motivation and prayers. I am also thankful for Yvotte Brits from Steenkampskraal Thorium Limited for his guidance throughout the compiling of the dissertation and all the information and explanations supplied regarding the Th-100 Nuclear Power Plant (NPP).

ABSTRACT

Current regulations specify the minimum number of operators required per nuclear power plant. However, these requirements are based on the operation of large nuclear power plants, which are not inherent safe and can result in a meltdown. For newly developed small nuclear reactors, the current number of operators seems to be excessive causing the technology to be less competitive. Before the number of required operators can be optimised, it should be demonstrated that human errors will not endanger or cause risk to the plant or public.

For this study, a small pebble bed High Temperature Reactor (HTR) Nuclear Power Plant (NPP), the Th-100, was evaluated. The inherent safety features of this type of nuclear reactor include independent barriers for fission product capture and passive heat dissipation during a loss of coolant. The control and instrumentation architecture include two independent protection systems. The Control and Limitation System is the first protection system to react if the reactor parameters exceed those of the normal operational safe zone. If the Control and Limitation System fail to maintain the reactor within the safe zone, the Reactor Protection System would at that time operate and force the reactor to a safe state. Both these automated protection systems are installed in a control room local to the reactor building, protected from adverse conditions. In addition, it is connected to a semi-remote control room, anticipated as a multi-unit control room to include the monitoring and control of the auxiliary systems.

Probable case studies of human error associated with multi-unit control rooms were evaluated against the logic of the Control and Limitation System. Fault Tree Analysis was used to investigate all possible failures. The evaluation determined the reliability of the Control and Limitation System and highlighted areas which design engineers should take into account if a higher reliability is required. The scenario was expanded, applying the same methods, to include the large release of fission products in order to verify the reliability calculations. The probability of a large release of fission products compared with studies done on other nuclear installations revealed to be much less for the evaluated HTR as was expected.

As the study has proved that human error cannot have a negative influence on the safety of the reactor, it can be concluded that the first step has been met which is required, when applying for a waiver to utilise a multi-unit control room for the small pebble bed HTR NPP. Also, from the study, it is recommended that a practical approach be applied for the evaluation of operator duties on a live plant, to optimise the number of operators required. This in turn will position the inherent safe HTR competitively over other power stations.

KEYWORDS:

Control and Limitation System; Fault Tree Analysis; High Temperature Reactor Nuclear Power Plant; human error; multi-unit control room; Pebble bed; protection system; Reactor Protection System.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

1oo2	-	One out of two signals should give a reading with-in the safe zone to prevent the safety system to operate.
2oo3	-	Two out of three signals should give a reading with-in the safe zone to prevent the safety system to operate.
AVR	-	ArbeitsgemeinschaftVersuchsreaktor translated as Working Group Test Reactor
B_4C	-	Boron Carbon
EPR	-	European Pressurised Reactor
C&I	-	Control and Instrumentation also referred to as I&C
CO_2	-	Carbon dioxide
DiD	-	Defence-in-Depth and Diversity
FTA	-	Fault Tree Analysis
THTR	-	Thorium High Temperature Reactor
He	-	Helium
HMI	-	Human Machine Interface
hr	-	hour
HTR-10	-	High Temperature Test Reactor $10MW_{th}$
HTR-Modul(German)	-	High Temperature Reactor - Module
HTR-PM	-	High Temperature Gas Cooled Reactor - Pebble-bed Module
HTGR	-	High Temperature Gas Reactor
IAEA	-	International Atomic Energy Agency

INET	-	the Institute of Nuclear and New Energy Technology
INPO	-	Institute of Nuclear Power Operations
LO	-	Licensed Operators
MCR	-	Main Control Room
MW_{th}	-	Mega Watt Thermal
MW_e	-	Mega Watt Electrical
NGNP	-	New Generation Nuclear Power
NPP	-	Nuclear Power Plant
NRC	-	U.S. Nuclear Regulatory Commission
OTTO	-	Once-Through-Then-Out
PBMR	-	Pebble bed Modular Reactor
PBR	-	Pebble Bed Reactor
RPS	-	Reactor Protection System
RSS	-	Remote shut-down station
SMR	-	Small and Medium sized Reactors
STL	-	Steenkampskraal Thorium Limited
TSC	-	Technical support centre
Th-100	-	Thorium-100 Small pebble bed HTR
UK EPR	-	United Kingdom European Pressurised Reactor
U.S.	-	United States (of America)
USA	-	United States of America
y	-	Year

CHAPTER 1: INTRODUCTION

Currently various organisations are developing small nuclear plants between 25MW_e and 300MW_e. The World Nuclear Association reported (World Nuclear Association, 2012) 18 different designs in progress as at November 2012.

The current nuclear regulations are based on years of experiences on large nuclear power plants, which can have critical failures with severe consequences. This criticality led to strict minimum requirements for the control systems of Nuclear Power Plants. Design standards may vary from country to country, but when looking at the U.S. Nuclear Regulatory Commission standard (U.S. Nuclear Regulatory Commission.), a minimum of four licensed operators are required on-site per unit. Not all of these regulatory requirements are applicable for some designs, such as those with passively safe small nuclear reactors similar to the Th-100. The American Nuclear Society (American Nuclear Society, July 2010) are expecting deviations with future designs and already prepared guidelines in applying for exemptions. Cost associated with these unreasonable resource requirements creates a huge overhead cost for small nuclear power plants and can be optimised by utilising a multi-unit control room.

Considering that the new Th-100 plants, as designed by STL (Steenkampskraal Thorium Limited, 2011) are passively safe designs that can be automated, it is foreseen that an operator is able to monitor and do limited control off more than one unit safely. The utilisation of an operator for multiple units will only be allowed if it is proven to the regulator that human errors will not influence the safety of the nuclear plants.

1.1 Problem Statement

The main problem identified is that the regulator will not approve the use of a multi-unit control room if operator error, associated with the use of this multi-unit control room has the potential to negatively influence the safety of the reactor.

1.2 Research Aims and Objectives

As Travers (Travers, October 7, 2002) reported to the NRC commissioner regarding the Staff Position, current regulations do not address the possibility of more than two reactors being controlled from one control room. Applicants need to address the safety implications to demonstrate that more than two reactors can be adequately controlled from one control room.

Regarding operator staffing requirements, applicants could request an exemption from current requirements to allow an alternate level of operator staffing for modular reactors, provided they address the safety implications. This dissertation does not aim to determine nor specify the optimal number of operators required for a multi-unit control room set-up, but focus on the initial step to prove that the safety implications will not be influenced by an operator error. The research include various pebble bed nuclear reactors and there inherent safety features. The protection system of the Th-100 is examined in detail and evaluated. Probabilistic analysis of practical scenarios that can be expected when utilising a multiple unit control room is evaluated. These results are then compared to other nuclear industry reported calculations. By proving that the safety and associated control system will correctly operate regardless of whether an operator error is incurred, will allow for further motivation for reduced operators and the use of multiple unit control rooms.

1.3 Expected Outcomes and Deliverables

The hypothesis is that the safety and associated control system of a passively safe small nuclear power plant, such as the Th-100, will be able to prevent operation, malfunctions as well as critical events within the designed safety margins. This will be congruent with the Brookhaven National Laboratory expectations of future nuclear power plants stated by J. M. O'Hara, J. C. Higgens & W. S. Brown, (O'Hara, et al., September 2008) as well as the International Atomic Energy Agency (International Atomic Energy Agency, May 2005).

C. Ericson (Fault Tree Analysis - A History, 1999) reported that the Fault Tree Analysis (FTA) was adopted by the Nuclear Power industry around 1971-1980 and was used for the WASH-1400 study in 1976 to review the NPP designs to assured the public that the probability of nuclear accidents was very small. A FTA on the Th-100 reactor will be worthy deliverable, which can be compared directly with FTA done on other NPP.

1.4 Method of Investigation

The concept design of the protection and control system for the Th-100, as supplied by STL, was evaluated and further theoretical propositions were made. A detail control logic flow diagram was developed, explaining the conditions required to move between the possible four modes of operation for the reactor, namely:

- Normal operations
- Hot standby
- Hot shutdown
- Cold shutdown

Case studies were performed where a number of theoretically concurrent faults are applied to demonstrate how the protection and control system will function.

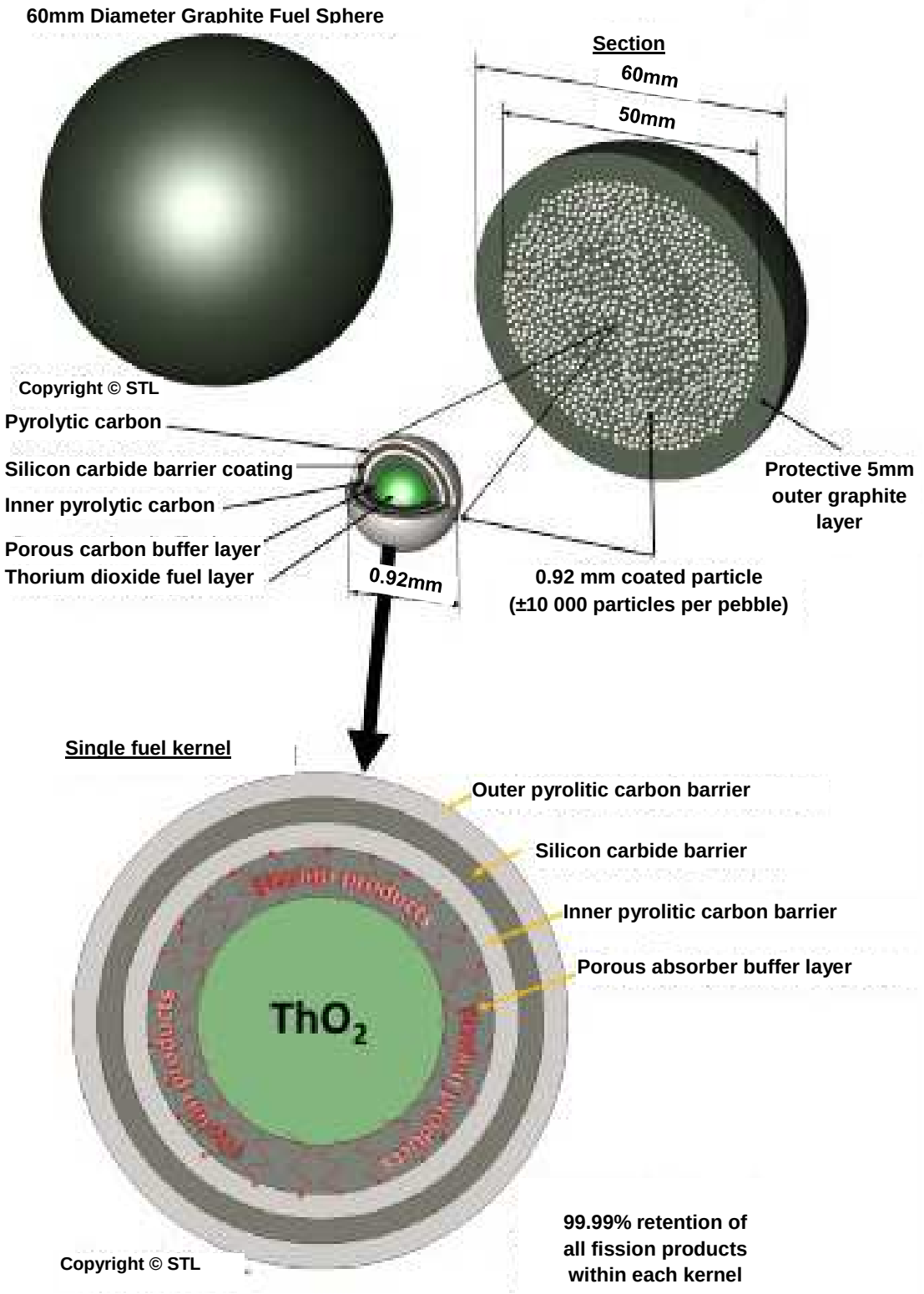
FTA was used to verify the probabilistic findings.

CHAPTER 2: LITERATURE REVIEW

2.1 Pebble Fuel

Common to all pebble bed reactors is the fuel. (AREVA NP Inc., October 2010) explained that the most common modern fuel pebbles are spheres of 60mm diameter with an inner fuelled zone containing 7 grams of uranium at 8% enrichment by weight. The fuel consist of spherical, 0.5mm diameter kernels surrounded by porous carbon, two pyrolytically deposited layers of carbon, and one layer of silicon carbide also known as TRISO particles. The layers have proven to provide a pressure boundary that confines fission products. Spend fuel is kept in storage casks on-site, while the storage facility are cooled by natural convection only. A graphical representation of the fuel as supplied by STL is shown in Figure 1.

Figure 1 - Th 100 Pebble Fuel



2.2 History of pebble bed HTR

B. K. Mcdowell, M. R. Mitchell, J. R. Nickmoloaus, R. Pugh & G. L. Swearingen, (Mcdowell, et al., October 2011) prepared a summary of the history of past and present HTGR plants for the U.S. Nuclear Regulatory Commission, since industry is currently showing interest in these developments, particularly in modular plants.

Farrington Daniels, a Professor of Chemistry at the University of Wisconsin, in 1942, first proposed gas-cooled nuclear reactors. His concepts included the use of pebble bed cores. HTGRs are defined as having characteristics of ceramic fuel, graphite moderators, and helium coolants. Based on this definition, the British CO_2 cooled reactors are excluded. Some of the HTGRs make use of graphite blocks, but the focus of this paper is on pebble bed cores.

Apart from the AVR, THTR and HTR-10 identified by Mcdowell, *et al.* (Mcdowell, et al., October 2011), research includes the HTR-Modul and NGNP (AREVA NP Inc., October 2010), PBMR (World Nuclear Association, January 2013), HTR-PM (International Atomic Energy Agency, Aug 2011) and the Th-100 (Steenkampskraal Thorium Limited, 2011). The high temperature pebble bed nuclear reactors can be categories between reactors that have reach construction phase as summarised in Table 1, and the reactors that have not yet reached construction, as summarised in Table 2.

Table 1 - Comparison of pebble bed nuclear reactors, which have reach construction phase

Reactor type	**AVR**	**THTR**	**HTR-10**	**HTR-PM**
Thermal Power:	46 MW_{th}	750 MW_{th}	10 MW_{th}	2x250 MW_{th}
Electrical Power:	15 MW_e	308 MW_e	2,5 MW_e	1x210 MW_e
Efficiency:	33%	41%	25%	42%
Power Density:	2.6 MW/m^3	6 MW/m^3	2 MW/m^3	3.2 MW/m^3
Secondary Coolant:	Steam (modern fossil steam conditions, no reheat)	Steam (modern fossil steam conditions, with reheat)	Steam	Steam
Primary System Pressure:	1.1 MPa	4 MPa	3 MPa	7 MPa
Primary Inlet Temperature:	275 °C	404 °C	250 °C	250 °C
Primary Outlet Temperature:	950 °C	777 °C	700 °C	750 °C
Years of Operation:	1967-1988	1985-1991	2000 – Still in operation	2013 – still in construction

Table 2 - Comparison of pebble bed nuclear reactors, which is yet to reach construction phase

Reactor type	**HTR-Modul**	**NGNP**	**PBMR**	**Th-100**
Thermal Power:	2x200 MW_{th}	2x250 MW_{th}	400 MW_{th}	100 MW_{th}
Electrical Power:	160 MW_e	105 MW_e	165 MW_e	35 MW_e
Efficiency:	40%	42%	41%	35%
Power Density:	3 MW/m^3		4 MW/m^3	3.8 MW/m^3
Secondary Coolant:	Steam of 530°C		Gas used in Brayton cycle	Steam
Primary System Pressure:	6 MPa		Variable to control load up to 9 MPa	4 MPa
Primary Inlet Temperature:	250°C	250°C	560°C	250°C
Primary Outlet Temperature:	700°C	>700°C still to be optimised	900°C	750°C
Design date:	1980		1990-2010	2010
Design stage:	Final design stage			Basic design

About.com **(www.about.com, 2014)** reported that on 26th April 1986, reactor four at the nuclear power plant near Chernobyl, Ukraine exploded. The Chernobyl nuclear disaster dramatically changed the world's opinion about using nuclear power. The World Nuclear Association **(www.world-nuclear.org, 2014)** reported that in Germany the support for nuclear energy was very strong in the 1970s following the oil price shock of 1974. However, this policy faltered after the Chernobyl accident in 1986, and the last new nuclear power plant was commissioned in 1989. Although the Social Democratic Party had affirmed nuclear power in 1979, they passed a resolution to abandon nuclear power within ten years in August 1986. The most immediate effect of this change of policy was the termination of research and development on the high-temperature gas-cooled reactor after some 30 years of promising work.

2.2.1 ArbeitsgemeinschaftVersuchsreaktor (AVR)

Mcdowell, *et al.* (Mcdowell, et al., October 2011) reported that the AVR, translated as Working Group Test Reactor, was one of the first reactors built in the Federal Republic of Germany. The fuel was contained in 6 cm diameter graphite pebbles. The initial core consisted of approximately 30,000 fuelled and 70,000 additional non-fuelled graphite spheres. During operation, the spheres were circulated and evaluated outside the reactor. The spheres with sufficient fuel were returned and depleted spheres with high burn-up were removed from the reactor.

The AVR operated successfully for 20 years and reached the highest temperatures of any commercial reactor to date, with temperatures of up to 1000 °C. The AVR generated 1.67 billion KWh of electricity and operated with an average availability of 66.4%.

Major tests performed on this plant included complete loss of forced cooling. This test proved that the pebble bed fuel remained below temperatures that could cause fuel failure. Temperatures were measured by instrumented graphite spheres with wires that had melting points ranging between 600 and 1280 °C.

2.2.2 Thorium High Temperature Reactor (THTR)

Mcdowell, *et al.* (Mcdowell, et al., October 2011) reported that the THTR was built by an industrial consortium in the German state of North Rhine Westphalia and was made critical in 1983. The technical performance of THTR was good, mainly due by the reliable electric drive circulators that never required a reactor shutdown.

During planned maintenance in 1988 inspections found that 35 of the 2600 hold-down bolts were defective. Technical evaluations indicated that the plant could continue to operate safely, but required a renegotiation of the risk-sharing contract between the members of the

consortium. The stakeholders decided not to restart the plant based on political considerations. Contributing to the decision not to restart the plant were the increase of financial operating losses to be borne by the utility; increases in the estimated cost of decommissioning; the fuel manufacturer ceased to manufacture the fuel pebbles; as well as the failure to secure a permanent spent fuel repository agreement; and issuance of a permanent operating licenses after the initial provisional license expired after the first 1100 full-power operating days.

2.2.3 HTR-Modul

(AREVA NP Inc., October 2010) reported that the HTR-Modul, a 2x200 MW_{th} (dual unit) modular pebble bed reactor design, was developed in Germany in the 1980s for the cogeneration of electricity, process steam and/or district heating. The concept design was reviewed and approved by German regulatory authorities, and progressed to a final design stage, but was never built.

The HTR-Modul was designed so that fuel temperature limits are not exceeded in the worst case of a complete loss of coolant. This prevents almost no release of radioactive fission products.

The HTR-Modul design formed the basis for subsequent modular PBR designs, including the South African PBMR, NGNP and the Chinese HTR-PM. The outlet temperature of the reactor is 700°C, producing steam of 530°C, which is used for electricity generation or for process applications.

The two reactor units are both housed within a single reactor building. A leak-tight reactor building is not required, due to fission product retention capability of the fuel. However the reactor building is provided with a sub-atmospheric pressure system, a pressure relief system and a filtering system. The reactor core is designed for variable loads between 50% and 100% power during normal power operation, using reflector rods to compensate for changes in reactivity.

Each reactor has a separate, independent, and dedicated reactor protection system. In the event of an accident, the safety system automatically shuts down the reactor and initiates protective actions. Two independent shutdown systems are installed. The control reflector rods consisting of six B_4C reflector rods are fully inserted by gravity. The other shutdown system consists of eighteen B_4C small balls, which are inserted by gravity into the side reflector columns when actuated. The small ball shutdown system is used for cold and long-term shutdowns. The low power density limits the fuel temperature below 1600°C under accident conditions, even without active cooling from the core. The reactor cavity can be cooled

passively preventing the exceeding design temperatures for up to 15 hours. The cavity cooler is supplied by a safety grade cooling system.

2.2.4 High Temperature Test Reactor HTR-10

Mcdowell, *et al.* (Mcdowell, et al., October 2011) reported that the HTR-10 is a 10MW_{th}, helium-cooled pebble-bed reactor, built in China at the Tsinghua University in Beijing. This reactor is similar to HTR module designs that as was discussed previously. The overall layout of a reactor vessel, a power conversion vessel, and a cross-vessel with a hot gas duct inside the cooler gas duct, is essentially the same design that has been used on several steel-vessel HTGRs and was first seen on the HTGR graphite block reactor Peach Bottom Unit 1 which operated from 1966 to 1974.

The specific Chinese governing codes and standards for the HTR-10 reactor pressure vessel could not be found by the International Atomic Energy Agency (International Atomic Energy Agency, Aug 2011) when the report was concluded. As of 2011, the power conversion vessel contains a steam generator, but plans are in place to use an intermediate heat exchanger installed in an existing cavity in the power conversion vessel with a Brayton cycle turbine; or alternatively to disassemble the steam generator and replace it with a direct Brayton cycle turbine. The indirect gas turbine could use either nitrogen or helium as a working fluid.

2.2.5 High Temperature Gas Cooled Reactor - Pebble-Bed Module

(International Atomic Energy Agency, Aug 2011) reported that the High Temperature Gas Cooled Reactor - Pebble-Bed Module (HTR-PM) is a modular High Temperature Gas Cooled Reactor (HTGR) demonstration power plant which is designed by the Institute of Nuclear and New Energy Technology (INET), Tsinghua University of China. The current HTR-PM design falls into the category of innovative small sized reactors, featuring a single 210MW electrical turbine driven by the combined two reactor modules, producing 250MW_{th} each.

In February 2008 the implementation plan and the budget for the HTR-PM project was approved by the State Council of China. The demonstration nuclear power plant is being constructed in Rongcheng, Shandong Province, China. The construction of the plant is scheduled to be completed by the end of 2013. Li (Li, April, 2014) reported that construction re-started in 2012, after the Fukushima accident and it will be connected to the grid in 2017.

The main motivation for developing HTGR nuclear is that the high heat that is generated can substitute the current fossil fuel boilers and generate process heat which is used in industry, thus saving a substantial amount of fossil fuels and resulting in less environmental pollution.

2.2.6 New Generation Nuclear Plant (NGNP)

The designers of the NGNP (AREVA NP Inc., October 2010) uses the detail designs of the HTR-Modul, as discussed above as a reference plant. Areas where the HTR-Modul does not align with new generation requirements would be addressed as part of routine design activities if the design were deployed in the United States of America. A few substantive areas where the HTR-Modul deviates from the NGNP requirements are identified below.

The reactor outlet temperature for a PBR deployment would be optimised during design as the current outlet temperature of 700°C is below the range specified in the NGNP requirements. Operating experience has demonstrated PBR technology with temperatures up to 950°C.

An alternative cavity cooling design is proposed that would extend the duration of passive heat removal to meet NGNP expectations, beyond the current 15 hours. A preliminary heat balance of the reference design indicates net cycle efficiency for electricity production of approximately 40%. Efficiency, reliability and cost comparisons will determine whether the required 42% efficiency will be met.

The HTR-Modul under adverse conditions can return to criticality at temperatures below 100°C, due to an insufficient negative temperature coefficient of reactivity. Considering the impacts, a power increase from 200 MW_{th} to 250 MW_{th} is considered realistic and achievable.

The use of a shared turbine fed from both HTR-Modul reactors is recommended for consideration for plants with the primary mission of electricity production. Larger steam turbines are more efficient and installation cost of a single large turbine is less than installing two smaller turbines. An alternative design is considered to be a reliable solution where the requirement for completely passive residual heat removal is being addressed.

2.2.7 PBMR

The Pebble Bed Modular Reactor (PBMR) was in the process of being developed by a consortium in South Africa. It was based on German expertise and aimed for maximised safety and efficient economics. The PBMR designs would have a direct-cycle (Brayton cycle) gas turbine generator and thermal efficiency of approximately 41% to produce 165 MW_e, although the Demonstration Plant was designed for a conventional steam turbine. The helium coolant leaves the core at 900°C. Power can be adjusted by changing the system pressure. Unfortunately the development has ceased due to lack of funds and customers.

2.2.8 Th-100

The Th-100 is a Thorium fuelled gas cooled pebble bed reactor producing 100 MW_{th}. Steenkampskraal Thorium Limited (Steenkampskraal Thorium Limited, 2011) claims that this Generation IV Reactor can be built and commissioned within the next 5 to 10 years.

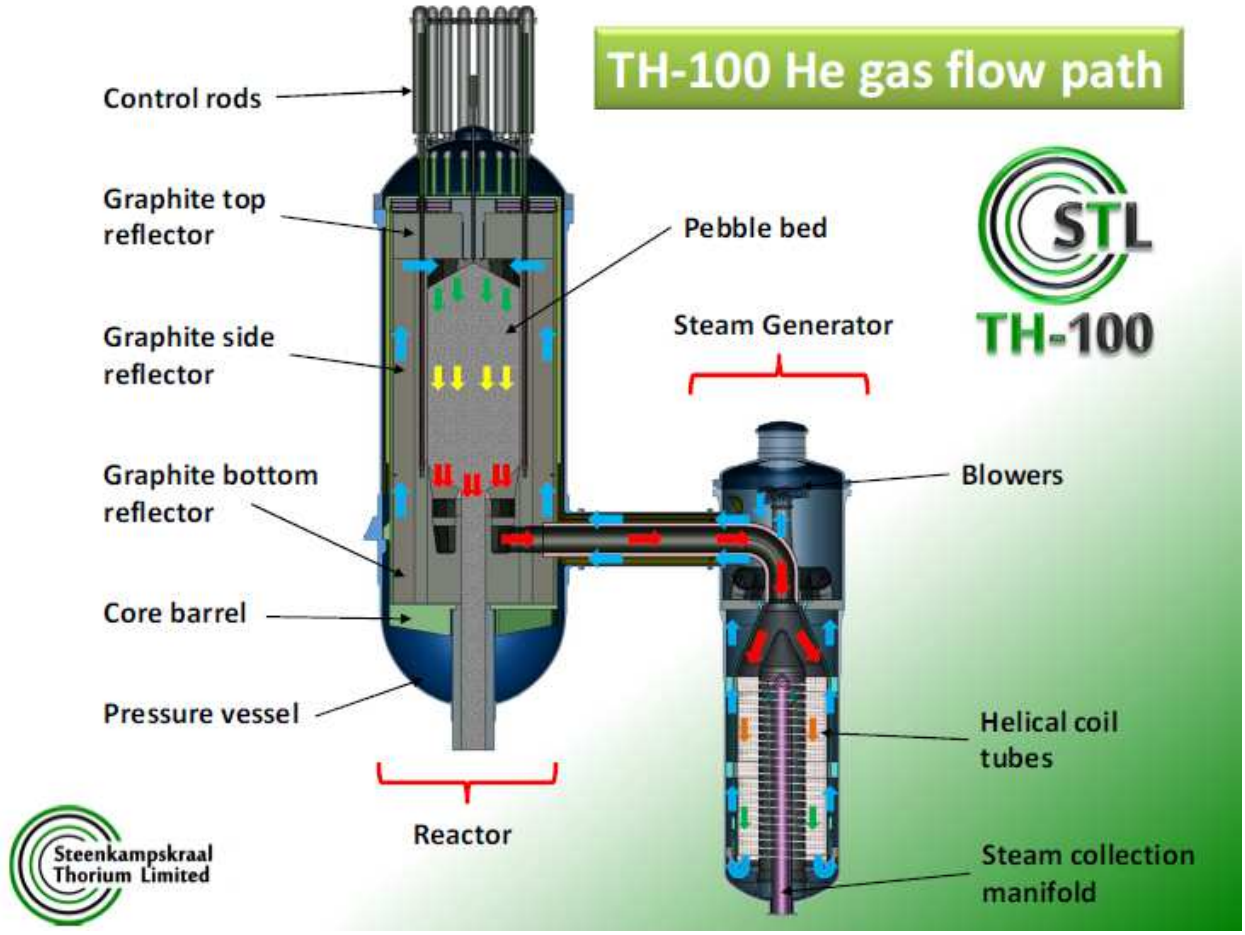
The reactor features a Once-Through-Then-Out (OTTO) Thorium fuel cycle, thereby simplifying the layout. The high temperature steam produced can be used for producing power via a steam turbine ($35MW_e$), or it can be used for process heat in industry plants.

The Th-100 exhibits the following characteristics:

- Fully ceramic fuel elements, which cannot melt, even in an extreme accident which may result in the total loss of active cooling;
- Use of coated thorium fuel particles (TRISO) effectively retaining the fission products within the fuel and allowing for very high burn-up of the fuel;
- Use of helium as coolant, which is both chemically and radiologically inert and does not influence the neutron balance. It allows for very high coolant temperatures during normal operation; dust is periodically removed,
- He is continually purified.
- The reactor core has a low power density and can tolerate a loss of forced cooling events and a total loss of the decay heat removal capability providing a very robust design with high heat capacity rendering the reactor thermally inert during all operational and control procedures;
- Very strong negative temperature coefficients contribute to the excellent inherent safety characteristic of these reactors;
- Efficient retention of fission products in the coated particle fuel in normal operation allows for a clean helium circuit; resulting in low levels of contamination of the coolant gas, low release of radioactivity, and extremely low radiation dose values to the operation staff;
- Efficient retention of fission products in the coated particles under extreme accidents results in a reactor without catastrophic release to the environment under these conditions.
- The fission product release is protected by multiple independent barriers, namely silicone carbide fuel kernels, the pressure vessel and a containment building.

The physical layout can be seen with courtesy of STL in Figure 2.

Figure 2 – Physical layout of the Th-100



Reitsma (Reitsma, August 2013) reported that the development philosophy of the Th-100 is to simplify without compromising safety where possible. This has led to that where possible existing proven technology will be used. This has the advantage that the plant characteristics has well known behaviour and should be easier to license. For example the thermal power is extracted from the He gas stream via a proven stainless steel helical coil steam generator. The electricity can be produced by adding an off-the-shelf steam turbine. All components consist of small size and modular construction resulting in a relative low cost solution. The largest components are small enough for road transport. This allows for mass production at a lower cost and ensures better quality assurance. The pressure vessel is rated at 4MPa only, which ensures there is various manufactures across the globe, with competitive associated cost and reduce lead times.

2.3 Reduction of operating staff in coal power stations

Parker (Parker, February 2013) identified that in reducing control room operator attendance requirements, coal power stations were able to reduce their operating costs. Options identified to accomplish this goal range from simply centralising the supervision of common plant functions to establishing fully unattended control rooms monitored by roving operators.

The example, at Stanwell Power Station in Queensland, is considered. In the mid-1990s, a new operational philosophy was introduced, enabling increased levels of plant process protection, sequence automation, and instrument redundancy to maintain automatic operation. Total staff levels were approximately half of what typically was required, and a unique operating arrangement led to the introduction of "unattended operation" as normal practice. The station won an international award in 1995 for innovative operation and automation. Today, Stanwell operates four units nightly with only two roving operator/maintainers.

The outcomes at Stanwell subsequently influenced the automation requirements specified for both new plant and rehabilitation projects throughout Australia. These requirements included the introduction of single-push-button start-up for supercritical coal-fired units, highly responsive plant performance, high-reliability control and protection, advanced alarm management, and provision for reduced and flexible attendance operation. On many rehabilitation projects involving control system replacements, instrumentation and actuation levels were raised and control rooms were redesigned and, in some cases, centralised.

Unattended operation describes the arrangement where all operators may leave the control room for plant monitoring or routine maintenance. A tablet device is carried to receive any significant alarms and advice. Operator recall alarms and lights are also located around the plant and are activated if physical presence in the control room is required.

2.4 Licensing requirements

The American Nuclear Society (American Nuclear Society, July 2010) focused on operator staffing for Small and Medium sized Reactors (SMRs). It is assumed that Small and Medium Sized Reactors (SMRs) have the potential to require a much smaller staff per reactor than existing large reactors. Staffing levels are foreseen to be reduced as long as safety is not compromised. The inherently safe designs eliminate the need for a plant operation staff of the magnitude employed at current NPPs. The new designs are typically more automatic, and thus require less human intervention. Therefore the number of Licensed Operators (LOs) in a multi-modular SMR facility will be less than in an equivalent large reactor.

The reduced staffing is not in line with current regulations and the specific requirements are accomplished with the approval of exemption requests to current regulations until the regulations are updated to accommodate the new SMR designs.

The current regulations require for a single-unit 10-MW_e Toshiba 4S reactor plant to maintain four LOs per shift on-site. This translates into a combined operating staff of 40 to 80 personnel under current requirements. This level of staffing is excessive, considering the size and simplicity of the plant as well as the minimal operator intervention foreseen for either normal operation or accident response.

The current regulations do not consider NPPs with more than three units nor controlled from a single multiple unit control room. The staffing requirements for a NuScale design plant with twelve modules, extrapolated from the requirements, result in staffing numbers far in excess of those believed necessary to safely operate the reactors.

It should be noted that under no circumstances should the level of qualification of the LOs be reduced for the SMRs. Safe operation of smaller reactors continue to require extensive training and testing for the operating staff, in line with existing U.S. Nuclear Regulatory Commission (NRC) and Institute of Nuclear Power Operations (INPO) requirements. Other industry experience demonstrates that staffing can be reduced as automation and simplicity are increased; however it is associated with increased training and experience of the operating staff.

While formal requests for the new SMR designs have yet to be issued, the calculated probability of a significant release and potential for off-site radiation consequences can be expected to be lower than those for both advanced reactor designs and current-generation reactors. The reasons for this are the following:

- The simple, passive features should result in a lower calculated probability of core damage than current□generation plants.
- The capability of the containment structure and its passive nature cooling capability provide a reliable barrier to release for those designs that rely on containments.
- The radionuclide inventory has orders of magnitude less than that used in the current large reactors in use.

Even when multiple modules of an SMR design are combined in one facility to have a cumulative capacity comparable to a large plant of the GEN III/III+ designs, the above factors suggest that the number of LOs may be less than would be currently required. Simplicity of

operation allows for additional collateral duties for LOs without compromising essential safety functions.

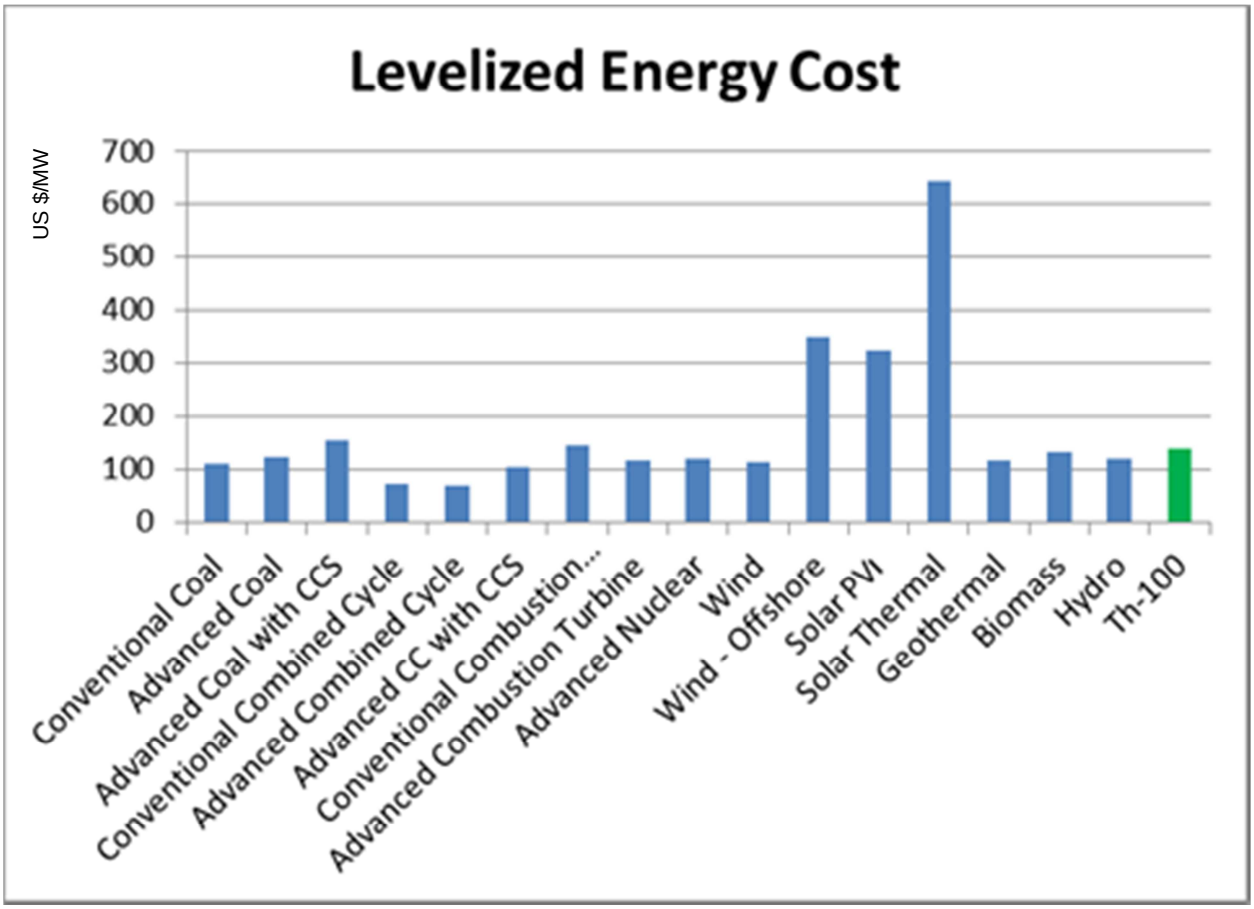
2.5 Drive for Multi-Unit Control Room

Hixson (Hixson, Aug 2011) reported that small modular reactors (SMRs) are part of a new generation of nuclear power plants being designed all over the world. The objective of these SMRs is to provide a flexible, cost-effective energy alternative.

A 25-megawatt reactor is 1/64 the size and complexity of a standard large 1.6 Giga Watt reactor from Westinghouse or AREVA.

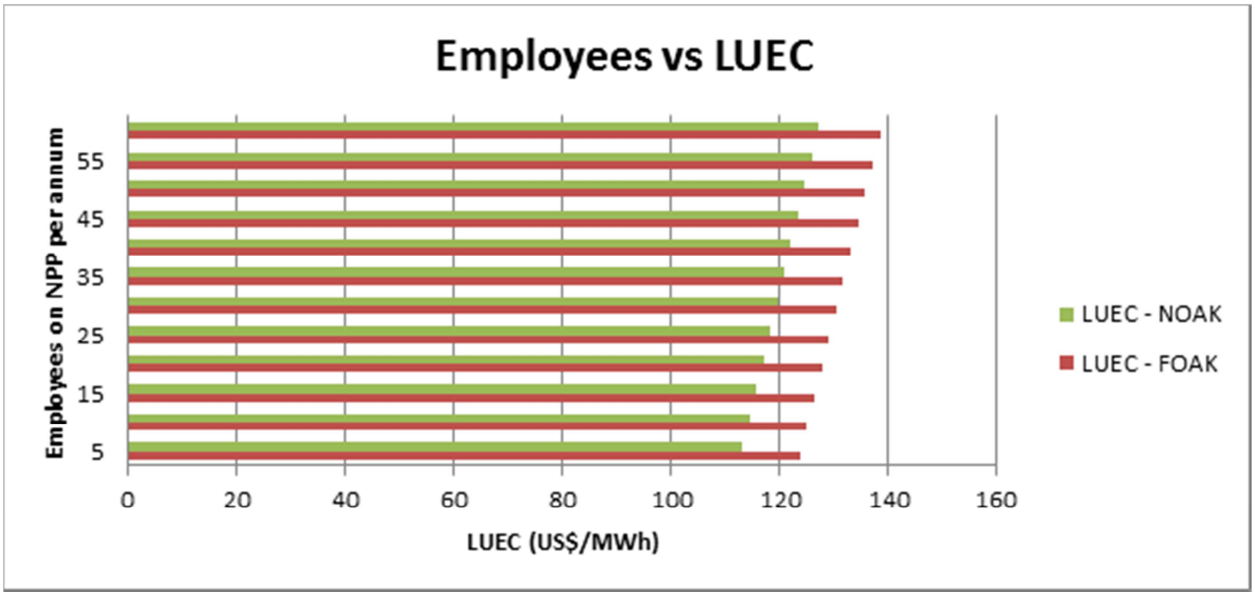
Courtesy of STL, the following figure compares the different technologies. This cost comparison is based on the use of six operators on a five shift roster for the Th-100 NPP.

Figure 3 – Levelised unit electricity cost for different technologies



However, if the operator numbers can be reduced the clean, passively safe nuclear energy of the Th-100 can compete with the established power generation methods, such as coal. This is shown in Figure 4, also supplied by STL.

Figure 4 - Levelised unit electricity cost vs. operators employed



FOAK: First of a kind (Is expensive mainly due to engineering cost)

NOAK: Number of a Kind (Due to optimisation cost less than the first of a kind)

2.5.1 Multi-Unit Control Room Proposed for NuScale

A press release by GSE Systems, Inc. (GSE Systems Inc, 2012, October 5) stated that the entity plans to build the world's first prototype of a 12-unit nuclear power plant operated from a single common control room. This simulator will be used by NuScale Power LLC for the development and demonstration operational concepts prior to construction. This simulator will be used to validate the multi-unit control room concept to the Nuclear Regulatory Commission, which is responsible for approving the SMR design.

2.6 Human factors

O'Hara *et al.* (O'Hara, et al., September 2008) identified, amongst others, to meet the Generation IV design goals that human error in operations and maintenance should be managed. For economy, safety and reliability, designs have to minimize human errors. In particular, designs may incorporate error tolerance features to minimize human errors and the consequences of any errors. Safety reviews will have to specifically address error tolerant design activities and features. This requires the development of comprehensive approaches to error tolerance. For new designs with no operating experience, it is especially important to have a good risk analysis, to define risk-important human actions, and then to address those actions in all aspects of the design.

G. A. Boy & K. A. Schmitt, (Boy, et al., 2012) reflected that despite all possible training and experience, people are always subject to failure, i.e., they commit errors. Communication, cooperation and coordination among team members may fail. Designing for safety is a real issue that deserves extreme attention. The current answer to protect people from the failure of safety–critical systems is grounded in the development of software-intensive systems. It is an easy way to generate protections but the accumulation of software layers increases automation, and thus system complexity and consequently perceived complexity that in turn can generate new types of safety issues. Safety–critical systems deserve clean and understandable solutions.

Human operators' vigilance tends to decrease when they do not have much to do. This is why human operators need to be kept in the control loop to maintain reasonable continuous situation awareness. Z. Yong, M. HaiYing, J. Jianjun & Z. Li (Zhou, et al., 2012) found that with the introduction of computer and digital technologies, NPPs may negatively impact human cognition and behaviour. Typical human factors issues which may degrade operators' cognitive performance were evaluated. The results demonstrated that the "interface management tasks" exerted the greatest impact upon operators' cognitive reliability and secondly the "workload transition".

The primary tasks performed by nuclear power plant operators are process monitoring and control. However, in digital control rooms, the interface is computer-based. Operators do not interact directly with the plant. To perform the monitoring and control task, operators must actively interact with the computerised interface, and are required to perform interface management tasks including searching for data, navigating through displays, configuring interfaces, scaling windows, etc. Interface management draw cognitive resources away from the primary task and thereby make it resource limited. Secondly, interface management tasks often distract operators' attention, and interfere with their limited memory buffer. The distraction or interruption may cause a waste of cognitive resources. Thirdly, since the allowed response time under accident conditions is limited, managing the interface can increase operators' time pressure, and finally lead to attention narrowing or reduction in working memory capacity.

Advanced automation and computer systems execute the greater part of the operational task. The role of operator has changed from an active controller to a passive observer. During normal operating situations, operators may face prolonged periods of low workload. However, in accident conditions, especially when the operator must simultaneously assume manual control due to automation failure, workload increases dramatically. The sudden transitions between extreme low workload and critical high workload can cause cognitive cost and performance degradation. Firstly, the low workload state is immediately subsequent to the high workload state, may make the short-term memory buffer continue to be overloaded even after the

workload shift decreases. Secondly, sudden workload transition can induce psychological stress, and result in shrinkage of cognitive resources. Thirdly, although operators are capable of maintaining performance across workload transitions by using various adaptive methods such as effort regulation or changing resource allocation strategy, adaptation to workload transitions itself will consume mental resources, and may result in fatigue after-effects. Besides, the inappropriate resource allocation strategy can also reduce the available cognitive resources.

2.7 Architectures

Abu-Khader (Abu-Khader, 2009) summarised that the general safety objective for nuclear power plants are to protect the individual, society and the environment by establishing and maintaining effective measures against radiological hazards. The power control system is a vital control system for a nuclear reactor which directly concerns the safe operation of a nuclear reactor.

Y. S. Suh, J. Y. Keum & H. S. Kim, (Suh, et al., 2011) describe the following tactics to withstand single failures:

- Self-diagnostic: The system is implemented to detect infinite loop, memory corruption, overflow, underflow, and divide by zero.
- Heartbeat: The heartbeat is similar to a watchdog timer and can be implemented between two systems.
- Defence-in-depth: The architecture includes the non-safety control systems, Reactor Protection system as well as the Reactor Limitation system, alarm systems, plant monitoring and control systems.
- Diversity: Diverse the safety and non-safety systems as well as the alarm and monitoring systems.
- Redundancy: A 2-out-of-3 voting logic is used in the decision processors of the safety systems and a hot-standby is used in the non-safety systems. The networks are redundant.
- Independence: A gateway is established between the safety and non-safety systems and separated dedicated safety data links for the safety function are provided. The use of fibre optic data links satisfied an electrical isolation requirement.

S. H. Chang, S. S. Choi, J. K. Park, G. Heo & H. G. Kim, (Chang, et al., 1998) describe an advanced HMI which is proposed specifically for Korean operators. The design goals for the proposed HMI are to reduce operators' physical/mental workload and eliminate human errors that can affect plant safety and availability as much as possible.

The following recommendations are applicable to this dissertation:

- Monitoring and control functions should be digital utilising microprocessors, and a redundant operator work station should be provided to accommodate the failure of an operator work station.
- Separate hardware and software should be used for monitoring and control functions in a work station to avoid data communication bottlenecks and to maintain simple control system designs. However, monitoring and control functions should be closely linked in view of interaction with operators.
- Control of safety systems should be separated from that of non-safety systems using different hardware and software.
- Spatially dedicated hardwired switches should be equipped for essential functions such as reactor trip and safety injection to shut down a plant safely, in the case of complete failure of digital control.

Maillart (Maillart, 1999) reported on the Control and Instrumentation (C&I) architecture of the European Pressure Reactor (EPR). It constitutes a number of systems that act individually or as part of multiple lines of defence. Safety functions are allocated to the different systems in such a way that the total combination of systems will achieve the anticipated safety integrity target. Independence and diversity are evaluated when combining the contributions of the individual systems derive the global safety integrity. The control room systems are characterised by the following:

- Centralised main control room (MCR) equipped with:
    - Computerised operator workstations,
    - Safety control area comprising of the set of safety classified control means, to be used in case of the failure of the main operator workstations and as the means for the safety demonstration concerning the human–machine interface,
    - Shift supervisor workstation,
    - Plant overview panel providing a common overview of the state of the plant to the control room staff;
- Remote shut-down station (RSS) to be used in the case of unavailability of the main control room, allowing access to the cold shut-down; a superposition of the loss of the MCR and of an accident is not assumed regarding the extremely low probabilistic value;
- Technical support centre (TSC), being the place (separated from the main control room) for external experts advising the operators in case of an accident.

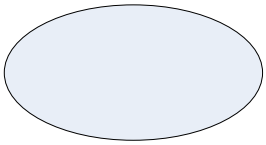
EDF Energy (EDF Energy, 2013) reported on the UK EPR digital C&I system. The concept of "Defence-in-Depth and Diversity" (DiD) ensures the effectiveness of the protective barriers by identifying the threats to their integrity and by providing successive lines of defence to protect them from failure. The C&I architecture relies on three main lines of defence:

- Preventive line, whose goal is to control the main plant parameters within their expected operating range and control potential deviations. It includes hazards protection.
- Main line of protection called safe path C&I safety features, providing a back-up in case of loss of the Protection System used to prevent core melt functions to protect against hazards.
- Risk reduction line used to prevent core melt in case of common cause failure of digital C&I systems preventing the main line of protection to operate and mitigate the consequences of severe accidents with a dedicated C&I system.

2.8 Fault Tree Analysis

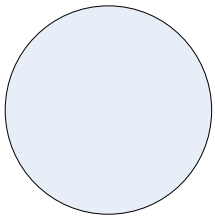
Fabrycky (Fabrycky, 2006) defined reliability as the ability of a system to perform its intended mission when operating through a planned mission scenario or series of scenarios, in a realistic operational environment. The Fault Tree Analysis (FTA) can be effectively applied in the early phases of design to focus and delineate potential problems. It is recommended to use the FTA for complex systems, which are highly software intensive. The FTA symbols that were used in this study are defined in Figure 5 below.

Figure 5 – Fault Tree Analysis format and symbols

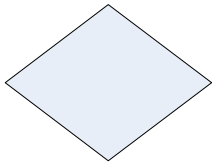


Top level event

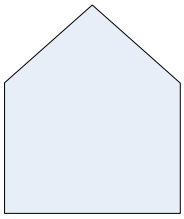
Intermediate fault event



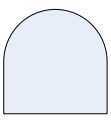
Basic / Lowest level failure event



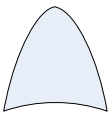
Undeveloped event (can be analyzed with a separate fault tree)



Input event



AND Logic gate



OR Logic gate

In order to evaluate a fault tree in a qualitative and quantitative manner the process explained by W. E. Vesely, F. F. Goldberg, N. H. Roberts & D. F. Haasl, (Vesely, et al., 1981) is followed. The minimal cut sets are defined as the smallest combination of component failures which, if they all occur, will cause the top level event. The different minimal cut sets indicates the importance of certain safety factors and can be qualitatively interpreted. For a quantitative evaluation the failure rates of each term in the minimum cut set is required. The FTA pictogram can be expressed in Boolean algebra. Boolean reduction techniques, such as the idempotent law and law of absorption can be used to cancel redundancies.

The idempotent law states:

$X \cdot X = X$

$X + X = X$

The law of absorption states:

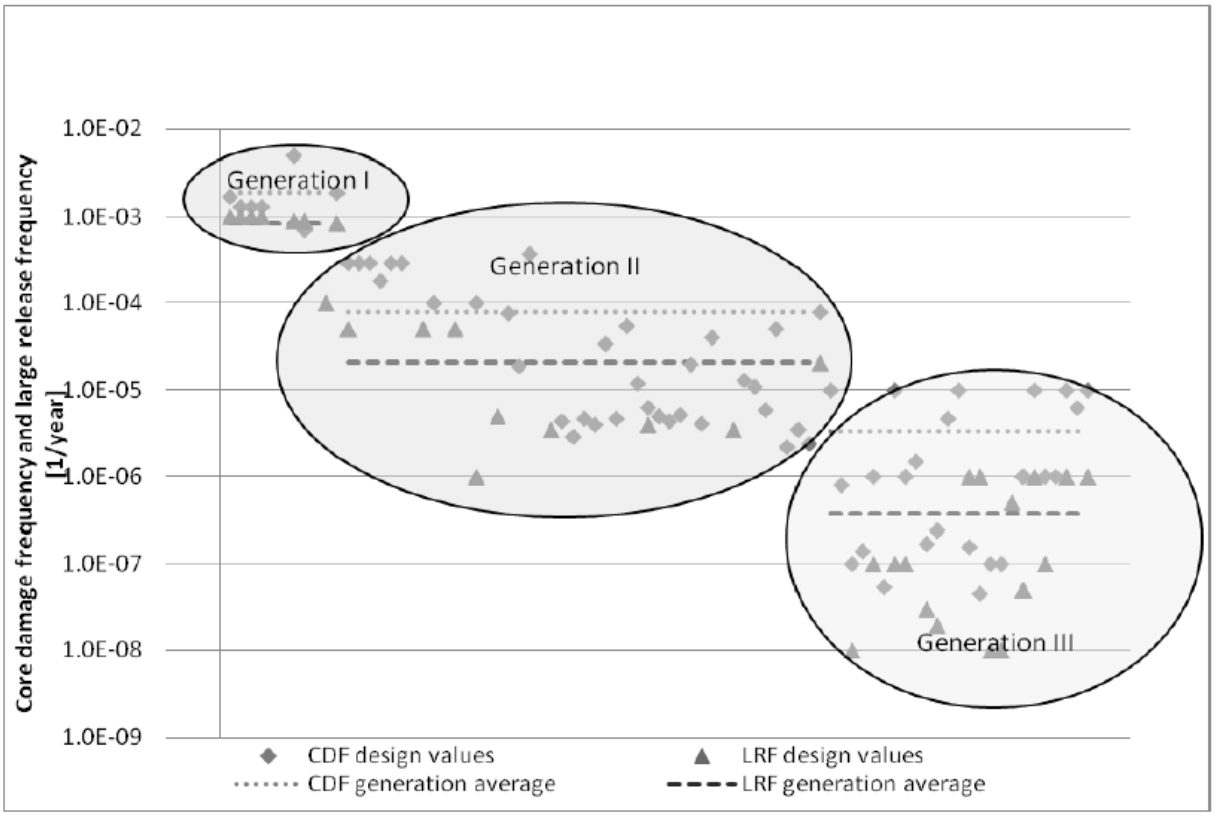
$X \cdot (X + Y) = X$

$X + X \cdot Y = X$

IAEA (INTERNATIONAL ATOMIC ENERGY AGENCY, 1988) compiled a comprehensive reference list, which can be used for this particular study. The probability of a failure is calculated over a one year period.

Figure 6 prepared by (NEA, 2010) using the sources supplied from (IAEA, 2004) shows a quantitative comparison to nuclear installations and will be used to verify the overall reliability.

Figure 6 – Evolution of core damage frequency and large release frequency for existing (Generation I and II) and for future reactors (Generation III/III+)



2.9 Summary of Literature Review

From the literature reviewed the following has been succinctly emphasised:

- There is a drive to develop and install SMR in the USA.
- Pebble bed reactors are some of the oldest concept nuclear reactors.
- Various types of plants have been built and successfully been operated.
- The safety of the plant has proven that even without forced cooling, the core will not melt down.
- Various modern developments are on-going and are currently being implemented.
- Other industries have adopted reduced operating staff to safe operating cost.
- The current nuclear licensing does not cater for SMRs and multi-unit control rooms.
- Various associations expressed the need for reduced operators in SMR designs.
- A SMR designer is promoting a twelve-in-one multi-unit control room.

In conclusion, the operating expenditure needs to be optimised for a new small pebble bed reactor to be considered an economical competitive against other technologies. As emphasised by several of the above sources, the use of a multiple-unit control room, is a practical and viable solution, however, as with all nuclear installations, the safety cannot be compromised.

To evaluate the safety requirements a further study was completed on the human factors as well as C&I architectures. Risk analysis is required for designs with no operating experience, as humans will make errors, regardless of their training or experience. Although automation is used to address human short comings it also adds to the complexity of the system and may degrade operators' cognitive performance.

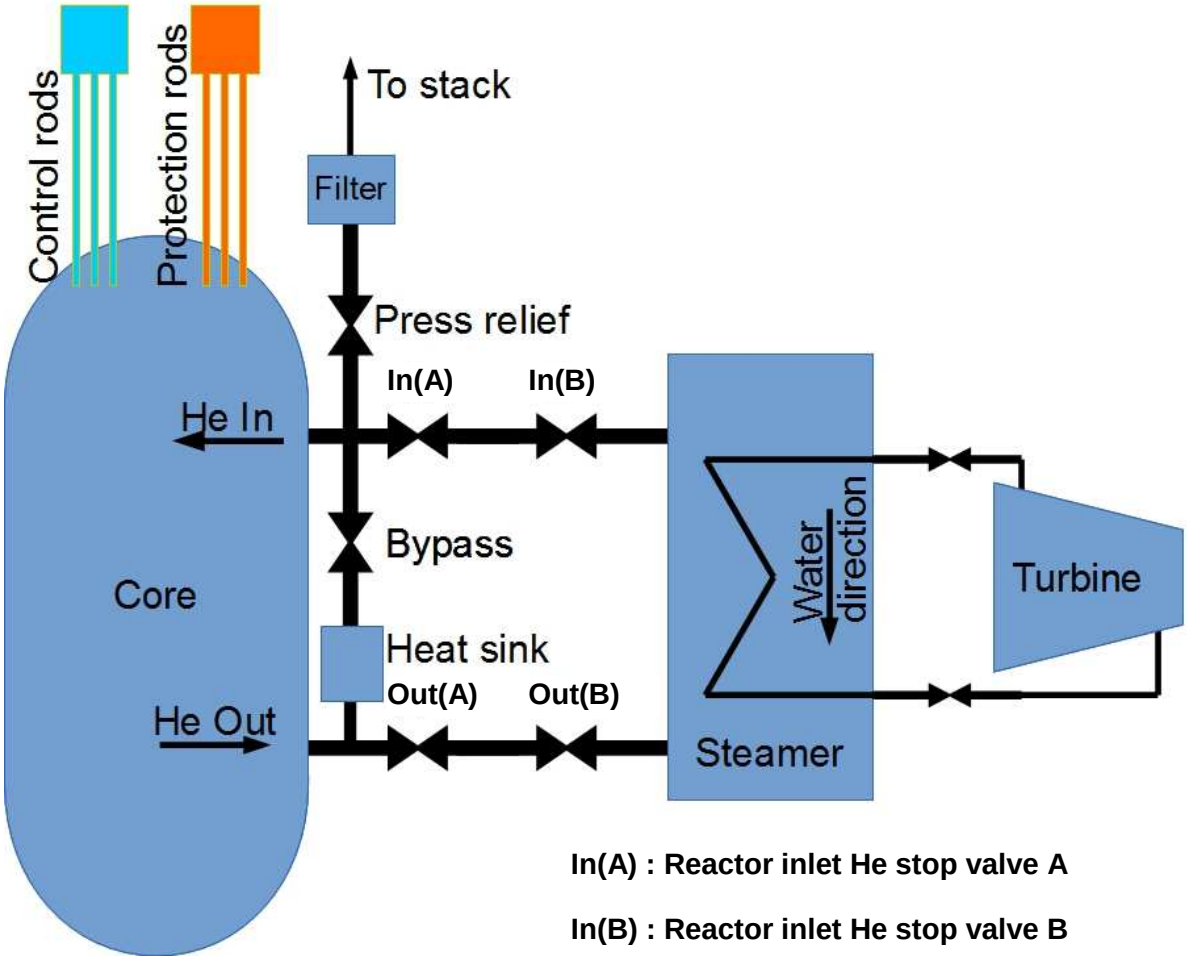
To prevent radiological hazards, the architecture of most nuclear power plants evaluated uses the concept of Defence-in-depth, diversity as well as redundancy.

The FTA is identified to proof the reliability of the Th-100 through various scenarios. The result can be verified against studies done on other NPP.

CHAPTER 3: CONCEPT ARCHITECTURE

The concept architecture discussed in this chapter was based on the Th-100, but similarities may be found when evaluating other pebble bed HTRs. Figure 7 indicates the single line architecture that has been used for this dissertation. Although the Th-100 is designed to withstand extreme accidents which may result in total loss of active cooling, the addition of a bypass system with an external heat sink is included in this evaluation. Double isolation is obtained by doubling the reactor inlet and the reactor outlet valves.

Figure 7 - Single line architecture of the Th-100



In(A) : Reactor inlet He stop valve A

In(B) : Reactor inlet He stop valve B

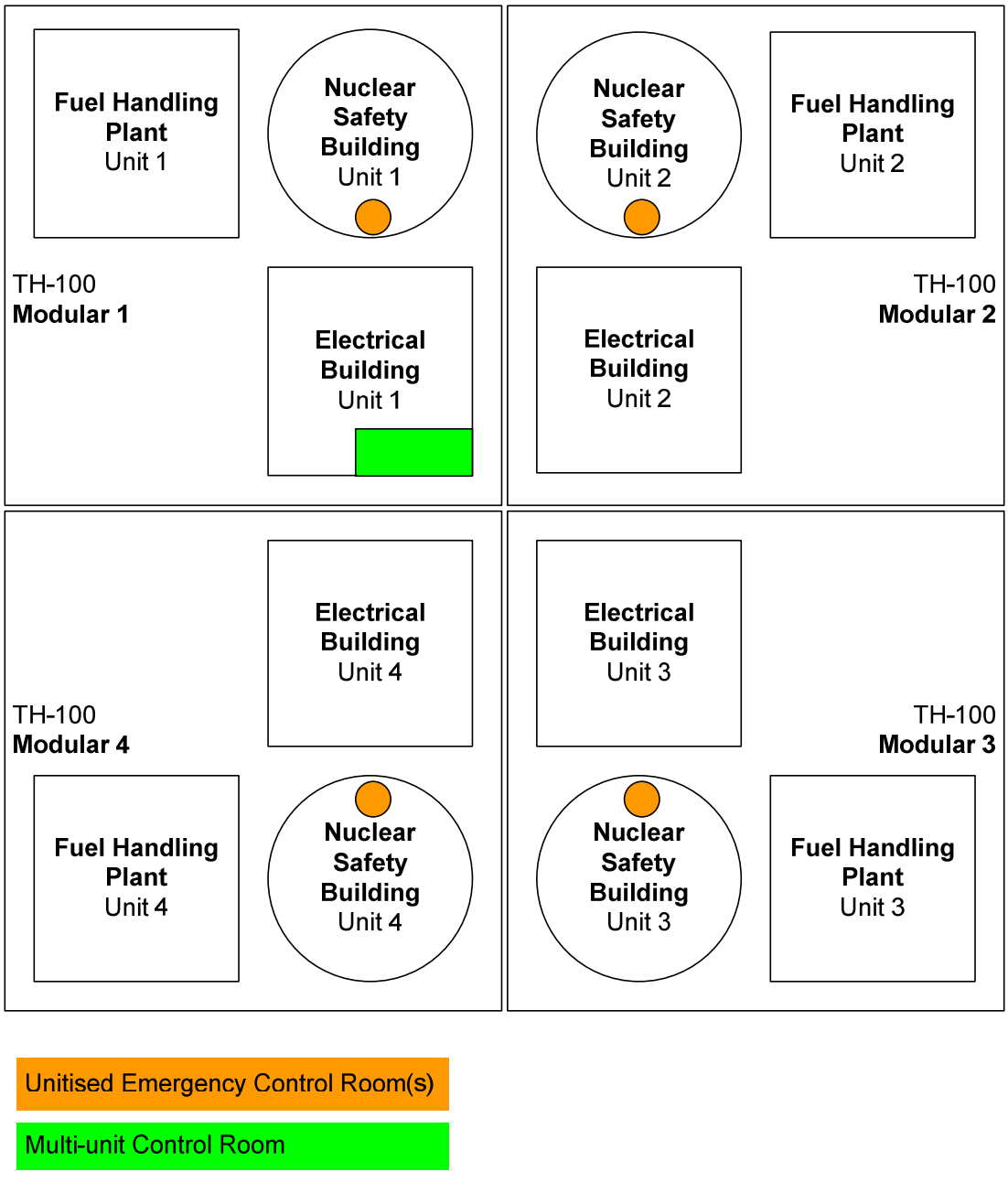
Out(A) : Reactor Outlet He stop valve A

Out(A) : Reactor Outlet He stop valve B

3.1 Control rooms

The control systems for one reactor are distributed over two control rooms, the Emergency Control Room as well as the Main Control Room. For a multi-unit control room set-up, the Main Control Room is foreseen to be shared with a number of reactors situated in close proximity of all the reactors that are being monitored. An Emergency Control Room will however remain in a special area within the nuclear safety building concrete structure of each reactor. By analysing the physical modular layout of a typical Th-100 nuclear power unit, the logical starting point will be to install a cluster of four units and to install a four-in-one multi-unit control room in a central location. One of the possible proposals can be seen in Figure 8.

Figure 8 – Proposed cluster of Th-100



The different control rooms which are being used in the Th-100 are discussed as follows:

3.1.1 Emergency Control Room

As mentioned each reactor has its own dedicated Emergency Control Room and is situated in a special area within the nuclear safety building concrete structure. This Emergency Control Room is designed such that flooding, lightning storms, earthquakes or certain airplane attacks cannot cause failure of systems installed within this area. A 10 hour battery back-up is provided for the critical systems. All the related safety information is displayed and consists of the following:

- Control and Limitation System
- Reactor Protection System

Although the protection system is designed in such a manner that it will automatically return the reactor to a safe-state if required, it is foreseen that expert operators will manage the Emergency Control Room during events which require intensive operating. These events include, but are not limited to the following events:

- Making the reactor critical (Light-up)
- Shut down of the reactor
- Emergency incidents

In case both the emergency control room as well as the main control room is manned the emergency control room actions will take preference.

3.1.2 Main Control Room

The Main Control Room is not situated within the nuclear safety building and can be situated on a semi-remote area, away from the nuclear reactor, since it will be connected with redundant fibre optic cables to the control systems that enhance the monitoring and control of the bill of plant areas. In the Main Control Room the Human System Interface is duplicated for all the systems installed in the Emergency Control Room, namely the Reactor Protection System and the Control and Limitation System , as well as for the following additional systems:

- Turbine Generator Control System
- Emergency Diesel Generator Control System
- Heating Ventilation and Air-Conditioning System
- Fuel Handling and Waste Control System
- Electrical Power Supplies

- Nuclear Auxiliary
- Fire Alarm Systems
- Intrusion Detection System
- Communication Systems

3.2 Control Sub-systems

The following sub-systems are essential to the reactor control systems:

3.2.1 Neutron Flux Measurement

As the primary indication of the state of the nuclear reactor, the neutron flux is measured over a range of 10 decades in both for the axial and azimuthal distribution. Three redundant channels exist with each containing a source range, intermediate range and an at power range. The source range is measured in two azimuths, whereas the intermediate range and the *at power* range are measured in three azimuths. These sensors are located in the concrete of the primary cavity and calibration and testing of detectors are done with neutron sources. Calorimetric – instrumentation tests are verified with periodically performed power balances of the primary system.

3.2.2 Core Monitoring

The core monitoring system receives the process information from the field instruments, regarding pressures, temperatures and flows. These values are placed in a model to compare it with theoretical heat and mass balance equations and the model is also updated with the neutron flux measurements. Any measurement that does not align with the theoretical values is highlighted as a problem area. If the problematic measurement is confirmed to be correct, the system also generates alarms to indicate that a probable leak is occurring in the system.

3.2.3 Rod Position Control and Monitoring

The nuclear reactivity is mainly controlled by the control rods position. These rods absorb free neutrons and thus reduce the reactivity within the nuclear reactor. Various control rods are distributed throughout the reactor, ensuring that all areas within the reactor have approximately the same neutron flux. It is essential to be able to control the position of the eleven control rods as a group, as well as the seven shutdown rods as a group. The hardware should also be monitored to determine, with certainty, the exact position of each rod. The control system is not able to extract the control rods if the Reactor Protection System requires the rods to be inserted.

3.2.4 Post-Accident & Event Recording & Monitoring

All critical signals are stored long term. This information assists in investigations.

3.3 Control Systems

The main focus on this dissertation is the Control systems applicable to the safety of the reactor, and consists of the following two independent systems:

- Control and Limitation System
- Reactor Protection System

As mentioned both these control systems are able to be accessed from either the unitised emergency control room or the shared main control room.

The Control and Limitation System is set to maintain the reactor with-in the safe normal limits, and thus the Reactor Protection System is only required to operate once the Control and Limitation has failed. The Control and Limitation has the ability to control the final elements in much the same way as the Reactor Protection System, however the Reactor Protection System takes precedence.

3.3.1 Control and Limitation System

The Control and Limitation System use set-points from the operators and control the nuclear reactor accordingly. The operators' instructions can either be local to the Emergency Control Room, by means of the dedicated emergency control panel; or remote from the Main Control Room. Local operation takes precedence, however it is expected that the Emergency Control Room remains unmanned during normal operations. The automated limitation control is set-up to avoid any unsafe limitations.

3.3.1.1 Control and Limitation Logic

The logic of the Control and Limitation System, as explained above is designed to keep the reactor within the safe margins. The Control system has four possible operational conditions for the reactor, namely:

- Normal operations
- Hot standby
- Hot shutdown
- Cold shutdown

Normal operation is where sufficient sensors (2oo3 or 1oo2) for each measurement area have healthy readings. This operation mode of the automatic controls will then control different control loops within safe limits to meet the operator selected set points.

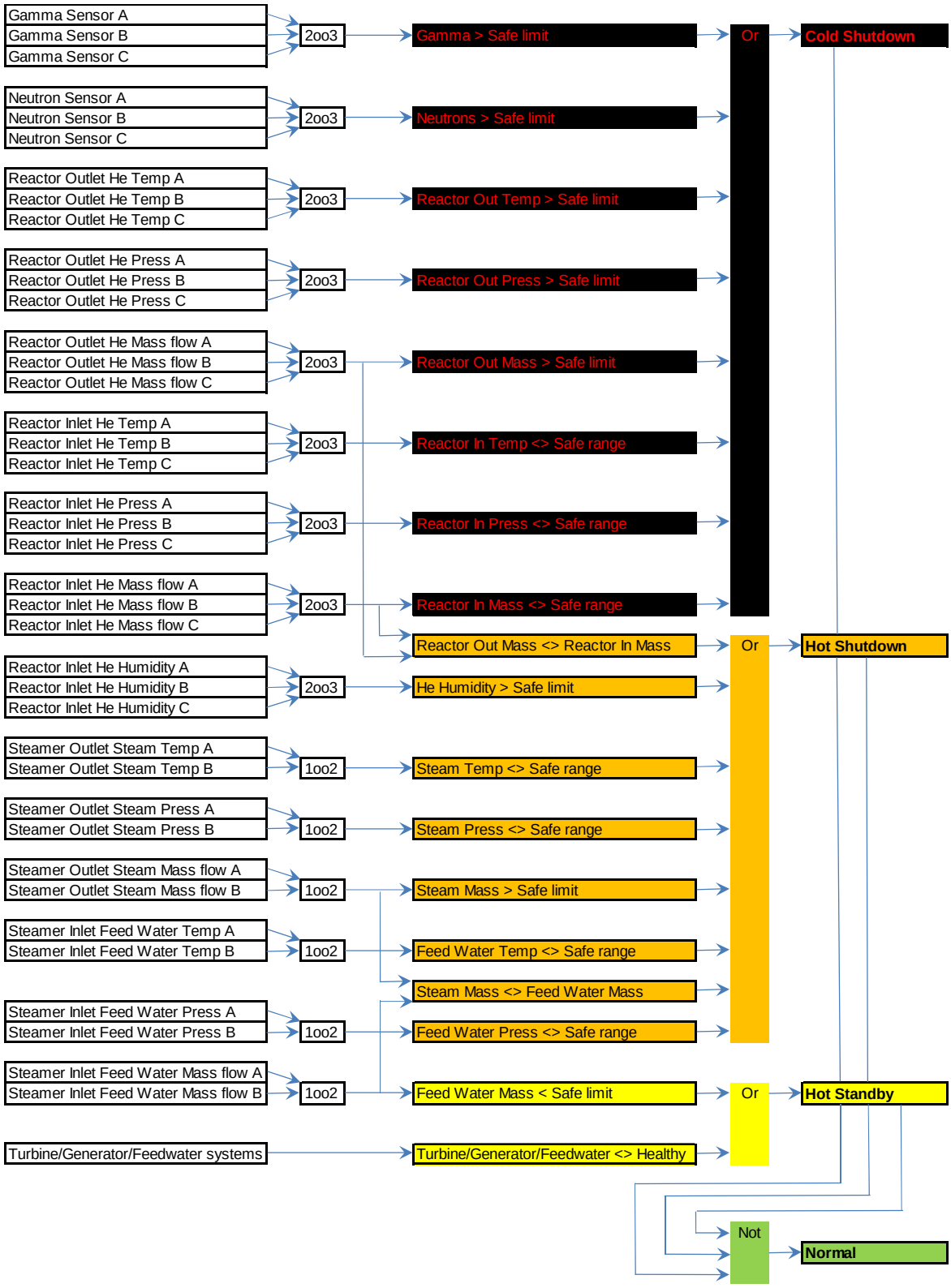
Hot standby is caused by a fault on the secondary (non-nuclear) side of the power plant, normally a turbine trip, which causes the inefficient removal of heat from the steamer. The turbine steam is bypassed directly to the condenser, while simultaneously the control rods are inserted to reduce reactivity of the nuclear reactor. The system may return to normal operation mode as soon as the fault on the secondary side has been resolved.

Hot shutdown mode is caused when there is a leak on the steamer. Since the pressure of the helium is normally higher than the steam cycle it is highly unlikely to occur but is vital as steam which enter the nuclear reactor, will change the properties of the reactor and chemical reactions may occur as the fuel pebbles mix with water. It also prevent contamination of the secondary side, although helium gas tends not to carry radiation. To prevent the negative consequences, the steamer is quickly isolated both on the primary side as well as on the secondary side. The reactivity is reduced to the minimum by fully inserting the control rods and the Helium gas is kept circulating by opening the steamer bypass system. The passive heat sink associated with the bypass is designed for this specific worst case scenario. Once the leak has been identified and closed-off, the system can be altered from hot shutdown mode to hot standby, where the steam generator is put in service again in parallel with the open bypass. If all systems prove to be correct, the secondary systems can be commenced, the bypass closed and the system can continue in normal operation mode.

Cold shutdown mode is activated as soon as the second sensors of any area on the nuclear reactor indicate a reading that is not within the safe margins (2oo3). Any sensor failing is also interpreted to be out of the safe margin. This is a critical situation and the nuclear reactor will be shut down immediately by dropping both the control rods as well as the protection rods. The system cannot be re-started easily after the fault(s) have been identified and corrected. The light-up procedure is required to re-activate the nuclear plant.

The control logic from the field inputs to determine the operation mode is represented in Figure 9 below.

Figure 9 – Th-100 NPP Control Logic from input to determine operational mode



The control outputs are controlled, depending on the identified operation mode of the Control and Limitation System. The outputs are represented in Table 3.

Table 3 - Th-100 NPP Control Logic output with reference to the operational mode

	Cold Shutdown	Hot Shutdown	Hot Standby	Normal
Control Rods	Fully inserted	Fully inserted	Slowly inserted fully	Controlling as per power requirements
Protection Rods	Fully inserted	Fully extracted	Fully extracted	Fully extracted
Reactor Outlet He Stop Valve A Reactor Outlet He Stop Valve B	Open Open	Quick close Quick close	Open Open	Open Open
Reactor Inlet He Stop Valve A Reactor Inlet He Stop Valve B	Open Open	Quick close Quick close	Open Open	Open Open
Steamer He Bypass Valve	Close	Quick Open	Close	Close
Steamer Outlet Steam Stop Valve	Open	Quick close	Open	Open
Steamer Inlet Feed Water Stop Valve	Open	Quick close	Open	Open

3.3.2 Reactor Protection System

The Reactor Protection System (RPS) is required to monitor and process variables essential to the safety of the Th-100 reactor and the environment; to detect events and to automatically initiate protective actions. In the case of an event, the reactor protection system shuts down the reactor and actuates the protective actions required for mitigation. The RPS has three separate and redundant channels configured in such a way to satisfy physical and electrical independence and separation requirements. Two-out-of-three (2oo3) logic is used.

In the case of abnormal events, the protection system implements the automatic and manual actuation of safety systems and the relevant monitoring functions necessary to reach a controlled state by a reactor emergency shutdown and to commence the safety systems:

- Reactivity control;
- Residual heat removal;
- Primary helium blower mass flow control;
- Blow down steam at the secondary system;
- Isolation of the primary and secondary systems;
- Limitation of radioactive releases at the site boundary to an acceptable limit and maintaining integrity of the primary and secondary systems;

The RPS includes the data acquisition and automation of the:

- Reflector rods;
- Primary helium blower;
- Primary system isolation valves;
- Secondary system isolation valves;
- Steam generator relief valves

The RPS is designed to ensure that fulfilment of its safety functions are assured in the event of accidents occurring simultaneously with a postulated equipment failure or unavailability due to maintenance.

3.3.2.1 Reactor Protection Logic

The protection logic of the Reactor Protection System, is designed to operates only if and when the Control and Limitation System fails to keep the reactor within the safe margins.

Each of the critical field sensors is installed in triplicate. These three sensors are compared with each other and at least two of the three switches need to be reading a safe, healthy signal. This is called a 2-out-of-3 (2oo3) system. The critical sensors are as follows:

- Neutron measurement
- Gamma measurement
- Pressure of the nuclear reactor coolant
- Humidity of the nuclear reactor coolant
- Inlet temperatures of the nuclear reactor coolant
- Outlet temperatures of the nuclear reactor coolant
- Mass flow of the nuclear reactor coolant

The combined signal from the 2oo3 system is forwarded to two separate trains. Each one of these trains has its own independent controllers that decide whether the safety systems should operate.

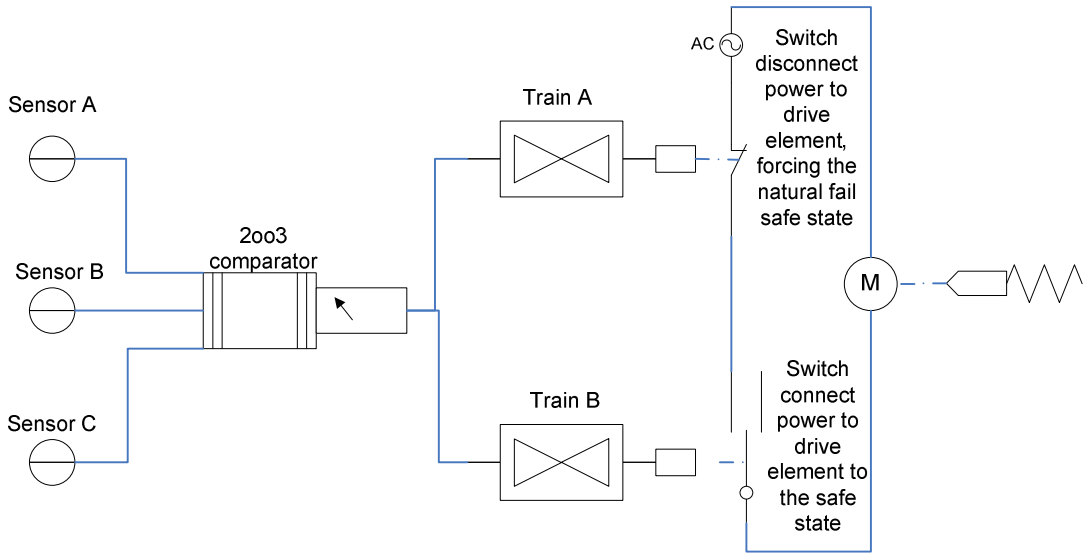
When train A activates the protection, it cuts the supply from the control element, which entails that the control element reverts back to the fail-safe position, by making use of gravity or a spring loaded control element.

When train B activates the protection it drives the control element, to the fail-safe position. Thus regardless of a malfunction of either train A or train B, the plant always returns to the fail-safe position. The fail-safe protection control elements are as follows:

- Control rods
- Shutdown rods
- Primary helium blower
- Primary system isolation valves
- Secondary system isolation valves
- Steam generator pressure relief valves

The protection logic is represented in Figure 10 as shown below.

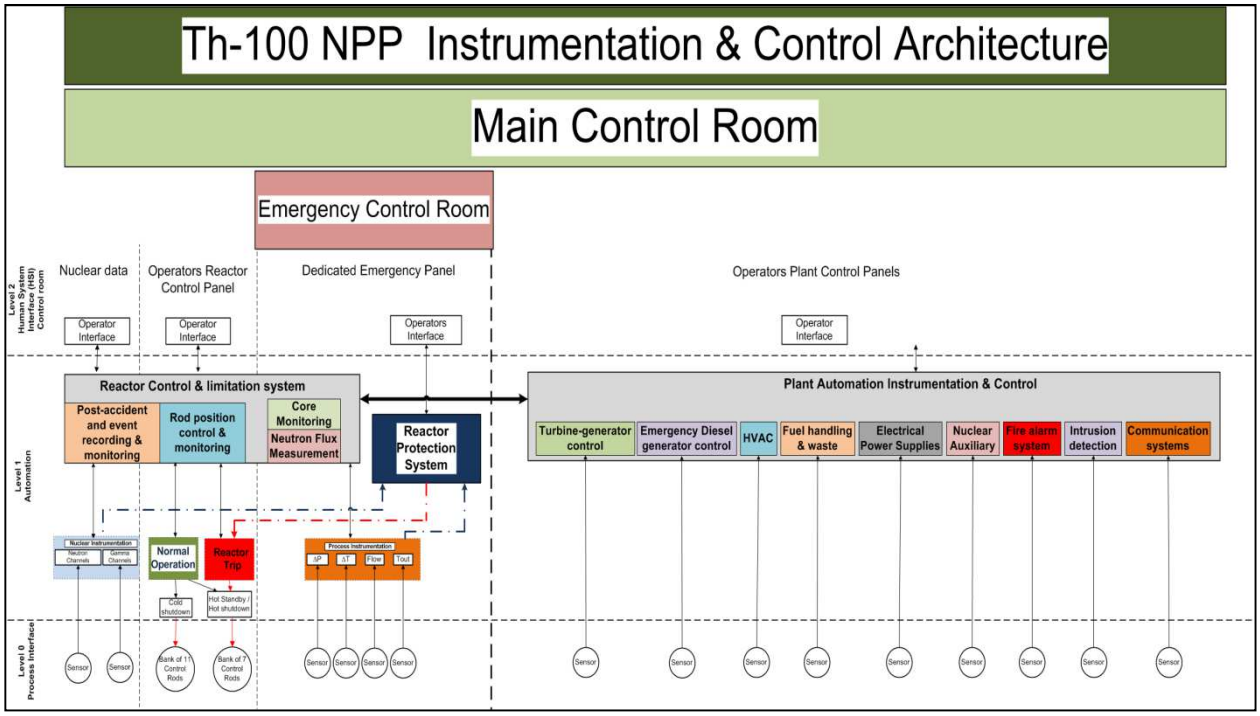
Figure 10 – Th-100 NPP Protection Logic



3.4 Instrument & Control Architecture Overview

A high level representation of the instrumentation and control architecture is depicted in Figure 11, below. Redundancy is specifically not shown, in order to keep the figure easily understandable.

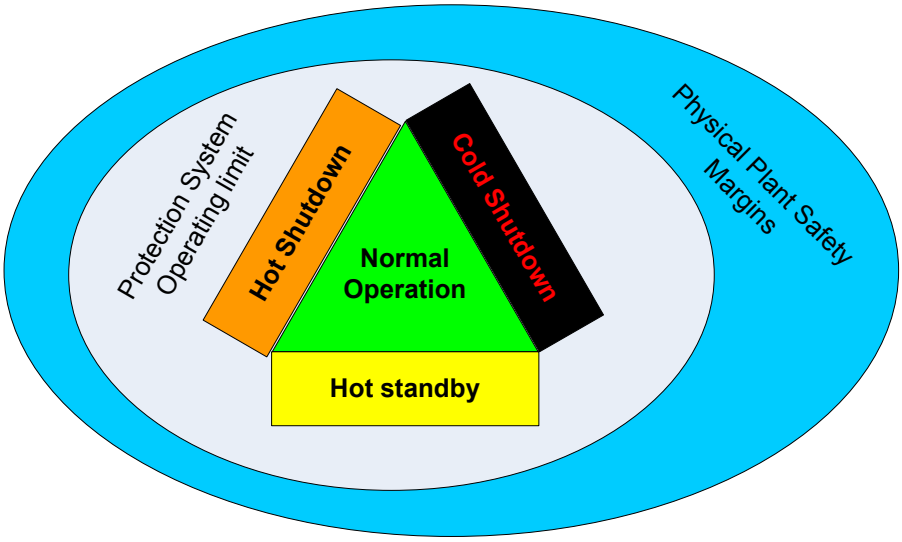
Figure 11 – Th-100 NPP Instrument & Control Architecture



CHAPTER 4: ARCHITECTURE EVALUATION

From the previous chapter it is apparent that the Control and Limitation System and the Reactor Protection System are separate independent systems. The Reactor Protection System is designed to make the reactor safe in case the Control and Limitation System is unable to control it within the pre-defined safety envelope and will keep the reactor with-in the physical plant safety margins. The different safety margins are represented in Figure 12 below. The four operating modes, normal operation, hot standby, hot shutdown and cold shutdown are part of the Control and Limitation System.

Figure 12 – Designed safety margins



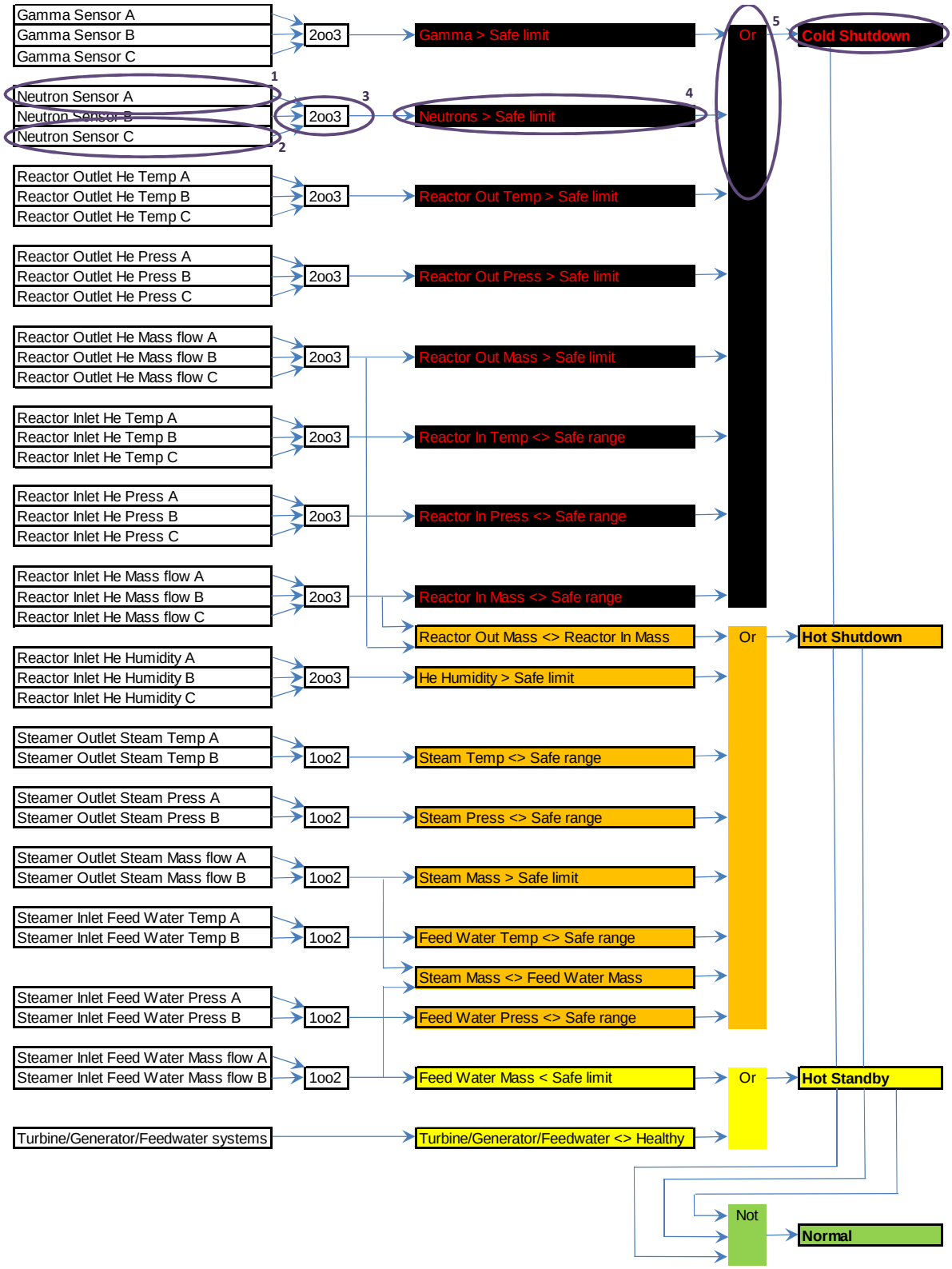
The evaluation of the architecture needs to start at the Control and Limitation System and its ability to keep the nuclear reactor with-in the pre-defined states, as this is the first line of defence. Various possible events can be developed.

4.1 Case study 1: Cold Shutdown

In Case study 1 the demand load increases and the operator(s) need to increase power on all running units. A neutron excursion alarm is received on a specific unit, however the demand for extra power is again emphasised from the grid controller at the same time and the operator(s) increases accidently not only the stable units, but also the unit which has the high neutron alarm.

Referring to Figure 9, Figure 13 shows that as soon as the second neutron sensor is not reading a value within the safe margin, the Control and Limitation System will change the operating mode to cold shutdown mode.

Figure 13 – Th-100 NPP Control Logic for Case 1

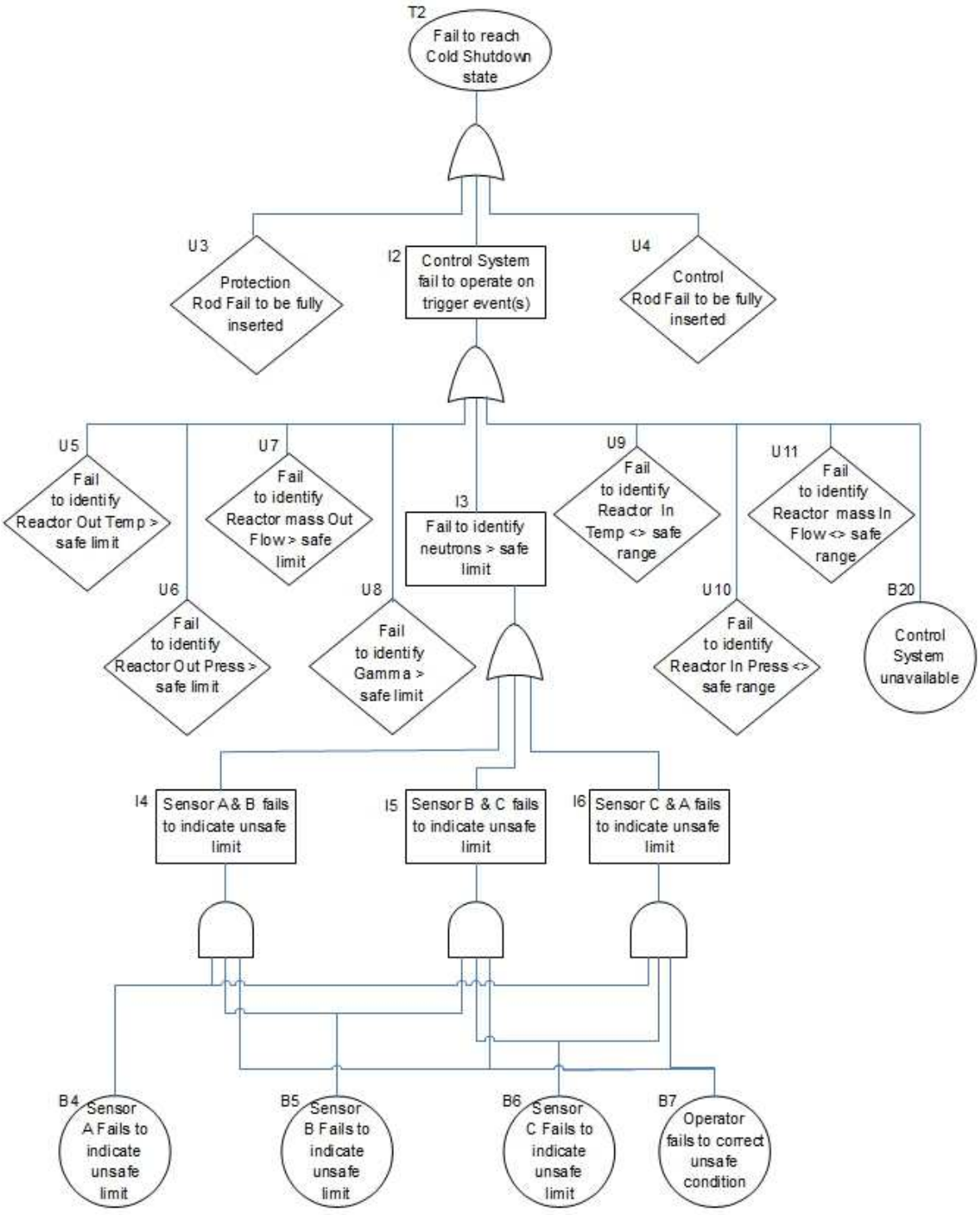


Referring to Table 3, both the control rods and the protection rods will be fully inserted, which will shut down the reactor, thus overriding the wrong operator instruction to increase the unstable reactor.

4.1.1 Develop FTA: Failure to reach Cold Shutdown State

A further investigation to why the Control and Limitation system will not reach a cold shutdown state when it is required is done by using the FTA. Figure 14 indicates all the events that need to occur, to prevent the Control and Limitation System to successfully protect the plant from an unsafe condition such as explained in Case Study 1.

Figure 14 - Fault Tree Analysis: Fail to reach cold shutdown



Referring to Figure 14, it is evident that the top level event can be written, by using Boolean algebra as follows:

$$T2 = U3 + I2 + U4 \qquad \text{Equation 4.1}$$

$$I2 = U5 + U6 + U7 + U8 + I3 + U9 + U10 + U11 + B20 \qquad \text{Equation 4.2}$$

$$I3 = I4 + I5 + I6 \qquad \text{Equation 4.3}$$

$$I4 = B4 \cdot B5 \cdot B7 \qquad \text{Equation 4.4}$$

$$I5 = B5 \cdot B6 \cdot B7 \qquad \text{Equation 4.5}$$

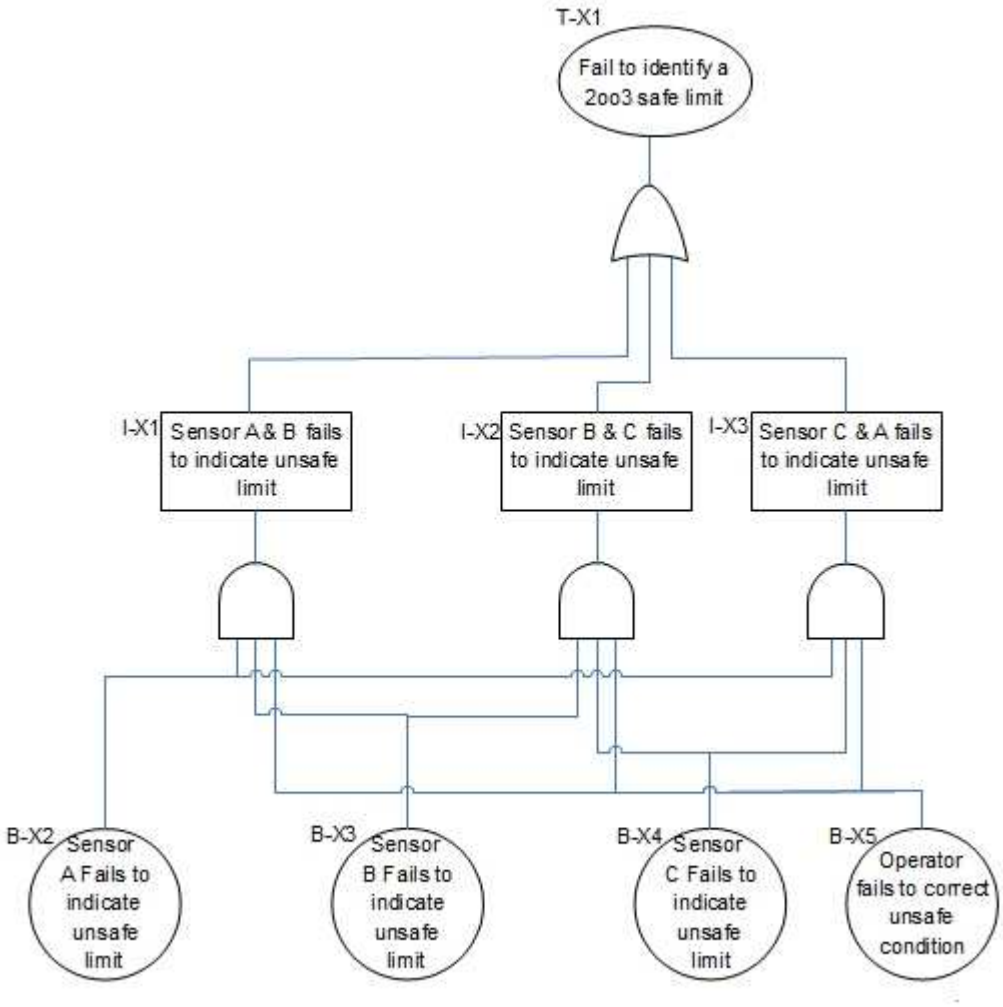
$$I6 = B4 \cdot B6 \cdot B7 \qquad \text{Equation 4.6}$$

By using top down substitution, Equation 4.1 - 4.6 can be manipulated to form the minimum cut set expression for T2, the top level event.

$$T2 = U3 + U4 + U5 + U6 + U7 + U8 + U9 + U10 + U11 + B20 + (B4 \cdot B5 \cdot B7) + (B5 \cdot B6 \cdot B7) + (B4 \cdot B6 \cdot B7) \qquad \text{Equation 4.7}$$

All the measurements which are required to identify the need to go into a cold shutdown mode are deemed critical and thus have been put into a 2oo3 configuration. To evaluate the undeveloped terms U3-U11 a general FTA is developed for a 2oo3 measurement system, as can be seen in Figure 15.

Figure 15 - Fault Tree Analysis: Fail to identify a 2oo3 safe limit



Without the detail designs being available and thus the failure rates of each specific type of the sensor used, a typical sensor failure rate will be used for each of the undeveloped cases U3-U11. It can be assumed that the probability of failure to identify that the neutrons is out of the safe limits as depicted in I3, Figure 14, will be in the same range for all the undeveloped cases where the system fails to identify the safe limits as depicted in T-X1, Figure 15. Thus mathematically it can be stated:

$$I3 \approx U5 \approx U6 \approx U7 \approx U8 \approx U9 \approx U10 \approx U11 \approx T\text{-}X1. \qquad \text{Equation 4.8}$$

4.1.2 FTA Qualitative evaluation: Failure to reach Cold Shutdown State

Form the minimum cut set expression for the top event, Failure to reach cold shutdown state, T2, as shown in Equation 4. 7, the following one termed minimum cut sets are derived.

$M1 = U3$ (Protection Rods fail to be fully inserted) Equation 4.9

$M2 = U4$ (Control Rods fail to be fully inserted) Equation 4.10

$M3 = B20$ (Control system unavailable) Equation 4.11

With the assumption that the all the sensors have about the same failure rate all of the remaining multi termed cut sets will be similar to:

$M4 = (B4 \cdot B5 \cdot B7)$ Equation 4.12

Equation 4.12 can be interpreted as the probability of the sensor failure multiplied by itself and multiplied by the human factor.

Qualitatively the single term cut sets (M1 – M3) has a bigger influence on allowing the system to fail and is discussed first. With reference to Equation 4.9-4.10, if a probability of failure needs to be lowered it is recommended to the designers to split the control rods and the protection rods into different banks and size these rods that only three of the four bank of rods is required to stop the nuclear reactions. With reference to Equation 4.11, (Seiji, et al., 2001) reports that Hitachi is in the process of researching and developing technologies to support next generation supervisory and control systems and that the current equipment which are deployed are achieving high reliability. The minimum quantitative requirements will need to be specified in the detail designs. The multi termed cut sets shows the effectiveness of having a 2oo3 configuration.

4.1.3 FTA Quantitative evaluation: Failure to reach Cold Shutdown State

For a quantitative evaluation the failure rates of each term in the minimum cut set is required. Using Equations 4.4-4.6, Equation 4.3 can be written as follows:

$I3 = (B4 \cdot B5 \cdot B7) + (B5 \cdot B6 \cdot B7) + (B4 \cdot B6 \cdot B7)$ Equation 4.13

It has been explained that for the basic design phase the probability of sensor failure is equal to all the sensors. Thus by using Equation 4.8, Equation 4.7 can be written as follows:

$$T2 = U3 + U4 + (I3) + (I3) + (I3) + (I3) + (I3) + (I3) + B20 + (B4 \cdot B5 \cdot B7) + (B5 \cdot B6 \cdot B7) + (B4 \cdot B6 \cdot B7)$$ Equation 4.14

And Equation 4.13 can be reduced to:

$$I3 = (B_{sensor} \cdot B_{sensor} \cdot B_{Human}) + (B_{sensor} \cdot B_{sensor} \cdot B_{Human}) + (B_{sensor} \cdot B_{sensor} \cdot B_{Human})$$

$$I3 = 3 \times (B_{sensor} \cdot B_{sensor} \cdot B_{Human}) \qquad \text{Equation 4.15}$$

According to Equation 4.13 is the last three terms of Equation 4.14 also equal to I3, thus Equation 4.14 can be reduced to:

$$T2 = U3 + U4 + (I3) + (I3) + (I3) + (I3) + (I3) + (I3) + B20 + (I3)$$

$$T2 = U3 + U4 + B20 + 8 \times (I3) \qquad \text{Equation 4.16}$$

Substituting Equation 4.15 into Equation 4.16 reveals:

$$T2 = U3 + U4 + B20 + 8 \times (3 \times (B_{sensor} \cdot B_{sensor} \cdot B_{Human}))$$

$$T2 = U3 + U4 + B20 + 24 \times (B_{sensor} \cdot B_{sensor} \cdot B_{Human}) \qquad \text{Equation 4.17}$$

The IAEA (INTERNATIONAL ATOMIC ENERGY AGENCY, 1988) reports the following mean failure rates:

- Control rods fail to be inserted (U4) of 2.0×10^{-7}/hr equates to 1.8×10^{-3}/y
- Controller general fails (B20) of 7.1×10^{-7}/hr equates to 6.2×10^{-3}/y
- Indicating instrument electronic general faulty measurement (B_{sensor}) of $7.7\text{x}10^{-7}$/hr which equates to 6.8×10^{-3}/y

For B_{human} a human error potential of 0.1 can be considered with regard to the recommendation of the Health and Safety Executive report (Health and Safety Executive, 2012) which state that it is valid in most cases.

With an absence of a failure rate for protection rods the same value is used as the control rods. This is a valid assumption as both the control rods and the protection rods work on the same principle.

$$U3 \approx U4 \qquad \text{Equation 4.18}$$

The top event (T2), fail to reach cold shutdown, can be quantitatively be calculated, with failure rates assigned to all the terms of Equation 4.17 as follows:

$$T2 = U3 + U4 + B20 + 24 \times (B_{sensor} \cdot B_{sensor} \cdot B_{Human})$$

$$T2 = 2 \times U4 + B20 + 24 \times (B_{sensor} \cdot B_{sensor} \cdot B_{Human})$$

$$T2 = 2 \times (1.8 \times 10^{-3}) + (6.2 \times 10^{-3}) + 24 \times \left((6.8 \times 10^{-3}) \cdot (6.8 \times 10^{-3}) \cdot 0.1\right)$$

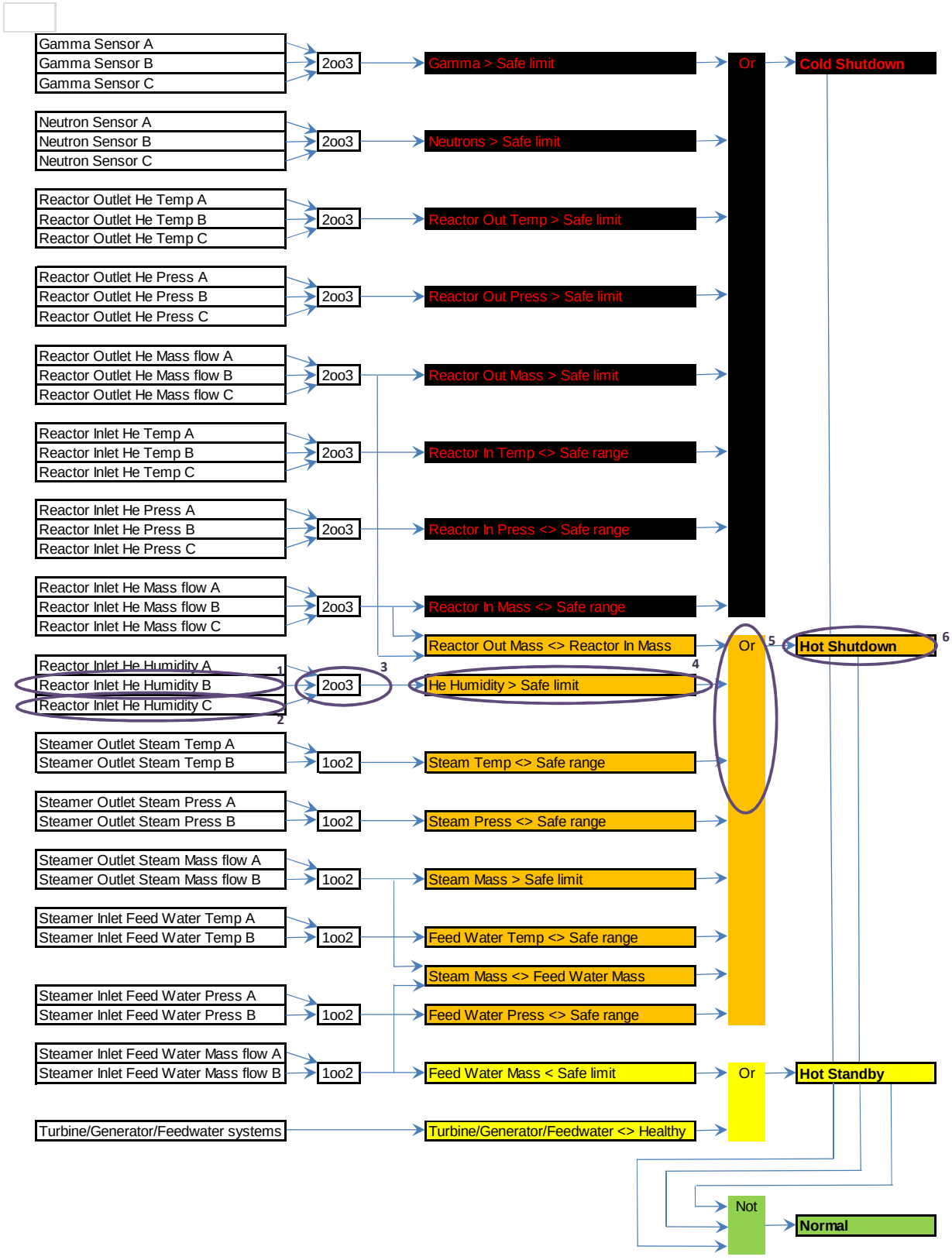
$$T2 = 9.8 \times 10^{-3} \qquad \text{Equation 4.19}$$

4.2 Case study 2: Hot Shutdown

In Case study 2 the reactor inlet Helium Humidity sensor B demonstrates a high value, greater than the safe limit. The operator suspects that the reading is erroneous as it is not in-line with the other two sensors, sensors A and C, and the operator dispatches a maintenance crew to inspect. The maintenance crew accidently identify the wrong sensor and disconnect the reactor inlet Helium Humidity sensor C to recalibrate it in the workshop. When a sensor is disconnected the Control and Limitation System as well as the Reactor Protection System assume the worst case situation and also interpret a high value for the helium humidity sensor.

Referring to Figure 9, Figure 16 demonstrates that as soon as the second humidity sensor reads a value greater than the safe margin, the Control and Limitation System will change the operating mode to hot shutdown mode.

Figure 16 – Th-100 NPP Control Logic for Case 2



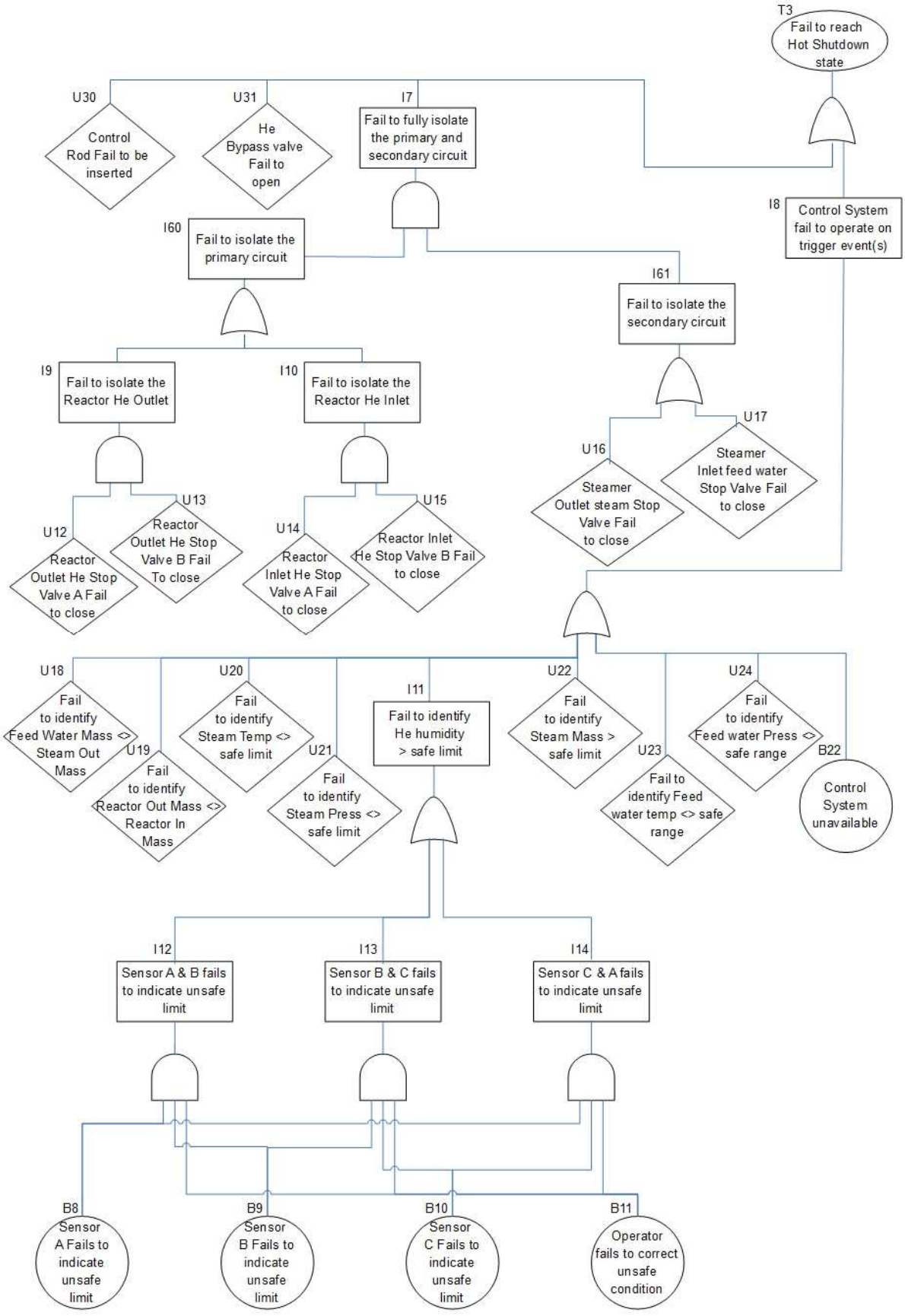
Referring to Table 3 the Control and Limitation System is protecting the reactor from water ingress as a probable tube leak within the steamer is being experienced. The steamer is quickly isolated both from the primary (reactor) side as well as from the secondary (turbine and feed water) side. The secondary side can be stopped almost immediately, but the nuclear reactor cannot, therefore a bypass system with a heat sink is opened allowing the helium to continue to circulate throughout the reactor. This continuous circulation ensures the reactor does not overheat. The control rods are fully inserted to reduce the reactor power and to reduce the heat dissipated at the heat sink.

The control rods are inserted at a rate, which will limit the amount of xenon poisoning. As there are low limits of xenon poisoning the reactor will be able to quickly run full load once the fault(s) has been corrected.

4.2.1 Develop FTA: Failure to reach Hot Shutdown State

A further investigation to why the Control and Limitation System will not reach a hot shutdown state when it is required is done by using the FTA. Figure 17 indicates all the events that need to occur, to prevent the Control and Limitation System to successfully protect the plant from an unsafe condition as for example explained in Case Study 2.

Figure 17 - Fault Tree Analysis: Fail to reach hot shutdown



Referring to Figure 17, it is evident that the top level event can be written, by using Boolean algebra as follows:

$$T3 = I7 + I8 + U30 + U31 \quad \text{Equation 4.20}$$

$$I7 = I60 \cdot I61 \quad \text{Equation 4.21}$$

$$I60 = I9 + I10 \quad \text{Equation 4.22}$$

$$I9 = U12 \cdot U13 \quad \text{Equation 4.23}$$

$$I10 = U14 \cdot U15 \quad \text{Equation 4.24}$$

$$I61 = U16 + U17 \quad \text{Equation 4.25}$$

$$I8 = U18 + U19 + U20 + U21 + I11 + U22 + U23 + U24 + B22 \quad \text{Equation 4.26}$$

$$I11 = I12 + I13 + I14 \quad \text{Equation 4.27}$$

$$I12 = B8 \cdot B9 \cdot B11 \quad \text{Equation 4.28}$$

$$I13 = B9 \cdot B10 \cdot B11 \quad \text{Equation 4.29}$$

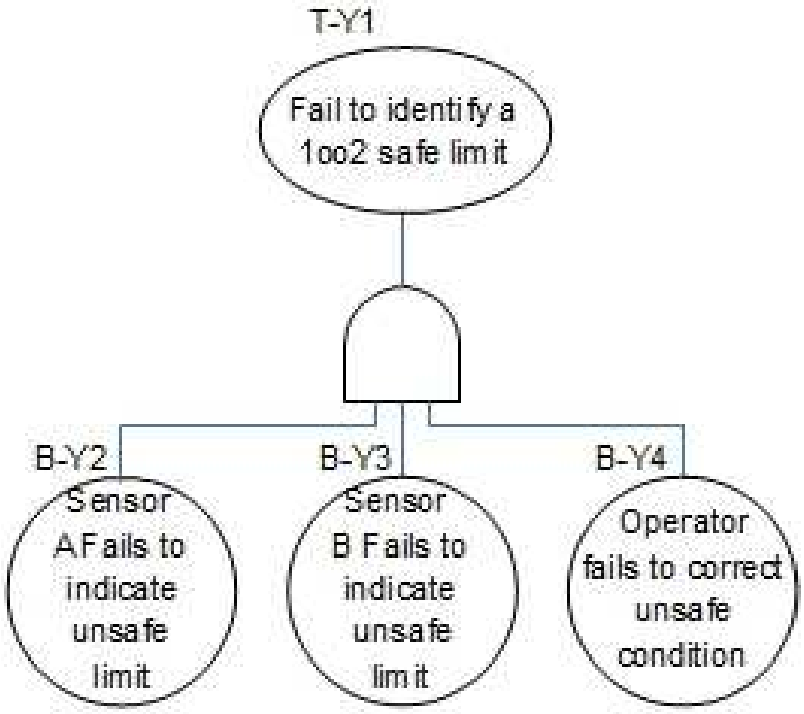
$$I14 = B8 \cdot B10 \cdot B11 \quad \text{Equation 4.30}$$

By using top down substitution, Equation 4.20-4.30 can be manipulated to form the minimum cut set expression for T3 the top level event.

$$T3 = (U12 \cdot U13 + U14 \cdot U15) \cdot (U16 + U17) + U18 + U19 + U20 + U21 + B8 \cdot B9 \cdot B11 + B9 \cdot B10 \cdot B11 + B8 \cdot B10 \cdot B11 + U22 + U23 + U24 + B22 + U30 + U31 \quad \text{Equation 4.31}$$

To evaluate the undeveloped terms U20-U24 a general FTA is developed for a “Fail to identify a 1oo2 safe limit” system, as can be seen in Figure 18.

Figure 18 - Fault Tree Analysis: Fail to identify a 1oo2 safe limit



Without the detail designs being available and thus the failure rates of each specific type of the sensor(s) used, a typical sensor failure rate will be used for each of the undeveloped cases U20-U24. All of these cases have the same configuration and it can be assumed that all of them concur to the probability of failure to identify the unsafe condition as depicted in the typical 1oo2 configuration as shown in Figure 18. Thus mathematically it can be stated:

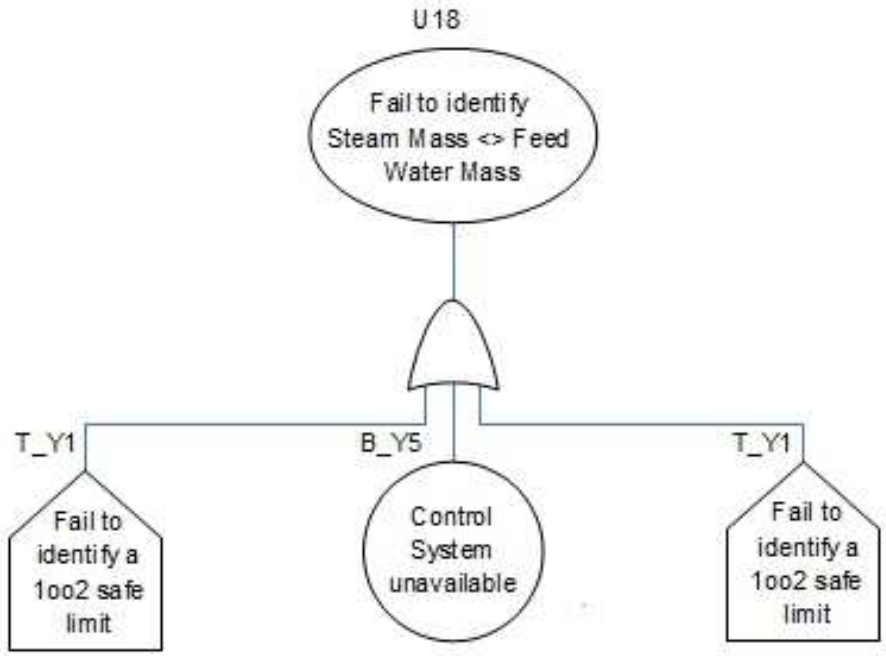
$U20 \approx U21 \approx U22 \approx U23 \approx U24 \approx T\_Y1.$ Equation 4.32

The top level event (T_Y1) can be written, by using Boolean algebra as follows:

$T\_Y1 = B\_Y2 \cdot B\_Y3 \cdot B\_Y4$ Equation 4.33

To evaluate the undeveloped term U18 a FTA, as shown in Figure 19, is developed “Fail to compare two 1oo2 safe limits” system. “Fail to identify a 1oo2” as shown in Figure 18 has been used as input.

Figure 19 - Fault Tree Analysis: Fail to compare two 1oo2 safe limits



Referring to Figure 19, it is evident that the U18 can be written, by using Boolean algebra as follows:

$$U18 = T\_Y1 + B\_Y5 + T\_Y1$$

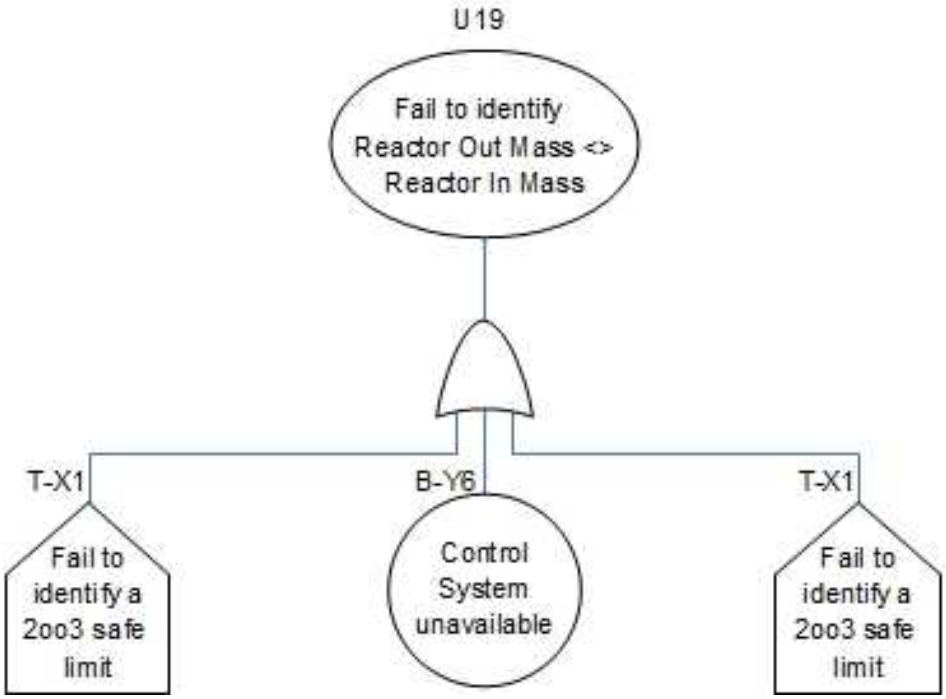
$$U18 = 2 \times T\_Y1 + B\_Y5 \qquad \text{Equation 4.34}$$

Substituting Equation 4.33 in 4.34 reveals:

$$U18 = 2 \times (B\_Y2 \cdot B\_Y3 \cdot B\_Y4) + B\_Y5 \qquad \text{Equation 4.35}$$

To evaluate the undeveloped term U19 a FTA, as shown in Figure 20, is developed termed “Fail to identify a 2oo3 safe limit” system. The detail of the input term can be viewed in Figure 15.

Figure 20 - Fault Tree Analysis: Fail to compare two 2oo3 safe limits



Referring to Figure 20, it is evident that the U19 can be written, by using Boolean algebra as follows:

$$U19 = T\_X1 + B\_Y6 + T\_X1$$

$$U19 = 2 \times T\_X1 + B\_Y6 \qquad \text{Equation 4.36}$$

Using Equation 4.8 and Equation 4.13, Equation 4.36 simplifies to:

$$U19 = 2 \times \big((B4 \cdot B5 \cdot B7) + (B5 \cdot B6 \cdot B7) + (B4 \cdot B6 \cdot B7)\big) + B\_Y6 \qquad \text{Equation 4.37}$$

Using Equation 4.32, the top event as described in Equation 4.31 simplifies to:

$$T3 = (U12 \cdot U13 + U14 \cdot U15) \cdot (U16 + U17) + U18 + U19 + T_{Y1} + T_{Y1} + B8 \cdot B9 \cdot B11 + B9 \cdot B10 \cdot B11 + B8 \cdot B10 \cdot B11 + T_{Y1} + T_{Y1} + T_{Y1} + B22 + U30 + U31$$

$$T3 = (U12 \cdot U13 + U14 \cdot U15) \cdot (U16 + U17) + U18 + U19 + 5 \cdot T_{Y1} + B8 \cdot B9 \cdot B11 + B9 \cdot B10 \cdot B11 + B8 \cdot B10 \cdot B11 + B22 + U30 + U31 \qquad \text{Equation 4.38}$$

Substituting Equation 4.33 in 4.38 reveals:

$$T3 = (U12 \cdot U13 + U14 \cdot U15) \cdot (U16 + U17) + U18 + U19 + 5 \cdot (B\_Y2 \cdot B\_Y3 \cdot B\_Y4) + B8 \cdot B9 \cdot B11 + B9 \cdot B10 \cdot B11 + B8 \cdot B10 \cdot B11 + B22 + U30 + U31 \qquad \text{Equation 4.39}$$

The term U18 is calculated in Equation 4.35 and thus Equation 4.39 becomes:

$$T3 = (U12 \cdot U13 + U14 \cdot U15) \cdot (U16 + U17) + (2 \times (B\_Y2 \cdot B\_Y3 \cdot B\_Y4) + B\_Y5) + U19 + 5 \cdot (B\_Y2 \cdot B\_Y3 \cdot B\_Y4) + B8 \cdot B9 \cdot B11 + B9 \cdot B10 \cdot B11 + B8 \cdot B10 \cdot B11 + B22 + U30 + U31$$

Equation 4.40

The term U19 is calculated in Equation 4.37 and thus Equation 4.40 becomes:

$$T3 = (U12 \cdot U13 + U14 \cdot U15) \cdot (U16 + U17) + (2 \times (B\_Y2 \cdot B\_Y3 \cdot B\_Y4) + B\_Y5) + (2 \times \big((B4 \cdot B5 \cdot B7) + (B5 \cdot B6 \cdot B7) + (B4 \cdot B6 \cdot B7)\big) + B_{Y6}) + 5 \cdot (B\_Y2 \cdot B\_Y3 \cdot B\_Y4) + B8 \cdot B9 \cdot B11 + B9 \cdot B10 \cdot B11 + B8 \cdot B10 \cdot B11 + B22 + U30 + U31$$

Equation 4.41

It is assumed for this basic design all similar equipment has the same failure rates meaning:

$$B_{sensor} = B4 = B5 = B6 = B8 = B9 = B10 = B\_Y2 = B\_Y3$$

Equation 4.42

$$B_{Human} = B7 = B11 = B\_Y4$$

Equation 4.43

$$B_{CPU} = B22 = B\_Y5 = B\_Y6 = B20$$

Equation 4.44

$$B_{Valve} = U12 = U13 = U14 = U15 = U16 = U17$$

Equation 4.45

Using Equation 4.42-4.45 the top event as described in Equation 4.41 can be reduced further:

$$T3 = (B_{Valve} \cdot B_{Valve} + B_{Valve} \cdot B_{Valve}) \cdot (B_{Valve} + B_{Valve}) + (2 \times (B_{sensor} \cdot B_{sensor} \cdot B_{Human}) + B_{CPU}) + (2 \times \big((B_{sensor} \cdot B_{sensor} \cdot B_{Human}) + (B_{sensor} \cdot B_{sensor} \cdot B_{Human}) + (B_{sensor} \cdot B_{sensor} \cdot B_{Human})\big) + B_{CPU}) + 5 \cdot (B_{sensor} \cdot B_{sensor} \cdot B_{Human}) + B_{sensor} \cdot B_{sensor} \cdot B_{Human} + B_{sensor} \cdot B_{sensor} \cdot B_{Human} + B_{sensor} \cdot B_{sensor} \cdot B_{Human} + B_{CPU} + U30 + U31$$

$$T3 = (4 \cdot B_{Valve} \cdot B_{Valve} \cdot B_{Valve}) + 3 \cdot B_{CPU} + 16 \cdot (B_{sensor} \cdot B_{sensor} \cdot B_{Human}) + U30 + U31$$

Equation 4.46

4.2.2 FTA Qualitative evaluation: Failure to reach Hot Shutdown State

Form the minimum cut set expression for the top event, Failure to reach Hot Shutdown state, T3, as shown in Equation 4. 46, the following one termed minimum cut set is derived.

$$M11 = 3 \times (B_{CPU})$$

Equation 4.47

$$M12 = U30$$

Equation 4.48

$$M13 = U31$$

Equation 4.49

With the remaining multi termed cut sets:

$$M14 = 16 \times (B_{sensor} \cdot B_{sensor} \cdot B_{Human})$$

Equation 4.50

$$M15 = 4 \times B_{Valve} \cdot B_{Valve} \cdot B_{Valve}$$

Equation 4.51

Qualitatively the single term cut sets (M11 – M13) has a bigger influence on allowing the system to fail and is discussed first. With reference to Equation 4.47 and 4.49, it is clear that the both the control system hardware as well as the He Bypass valve requires a very high availability. The control rods, as shown in Equation 4.4.8 also requires a high availability and can be split in separate control rod banks to increase their availability if required.

Equation 4.50-4.51 show the how the designers have catered to increase the availability of instruments and overcome valves that is prone to passing.

4.2.3 FTA Quantitative evaluation: Failure to reach Hot Shutdown State

For a quantitative evaluation the failure rates of each term in the minimum cut set is quantified as follows:

The IAEA (INTERNATIONAL ATOMIC ENERGY AGENCY, 1988) reports the following mean failure rates:

- Control rods fail to be inserted (U30) of 2.0×10^{-7}/hr equates to 1.8×10^{-3}/y
- A motorised valve failing to open (U31) of $1.0\text{x}10^{-5}$/hr which equates to a probability of a failure of $8.8\text{x}10^{-2}$/y
- A motorised valve failing to close (B_{Valve}) of $1.0\text{x}10^{-5}$/hr which equates to a probability of a failure of $8.8\text{x}10^{-2}$/y
- Controller general fails (B_{CPU}) of 7.1×10^{-7}/hr equates to 6.2×10^{-3}/y
- Indicating instrument electronic general faulty measurement (B_{sensor}) of $7.7\text{x}10^{-7}$/hr which equates to 6.8×10^{-3}/y

For B_{Human} a human error potential of 0.1 can be considered with regard to the recommendation of the Health and Safety Executive report (Health and Safety Executive, 2012) which state that it is valid in most cases.

The top event (T3), fail to reach hot shutdown, can be quantitatively be calculated, with failure rates assigned to all the terms of Equation 4.46 as follows:

$$T3 = 4 \times (8.8\text{x}10^{-2})^3 + 3 \times (6.2 \times 10^{-3}) + 16 \times (6.8 \times 10^{-3})^2 \cdot 0.1) + 8.8\text{x}10^{-2} + 1.8 \times 10^{-3}$$

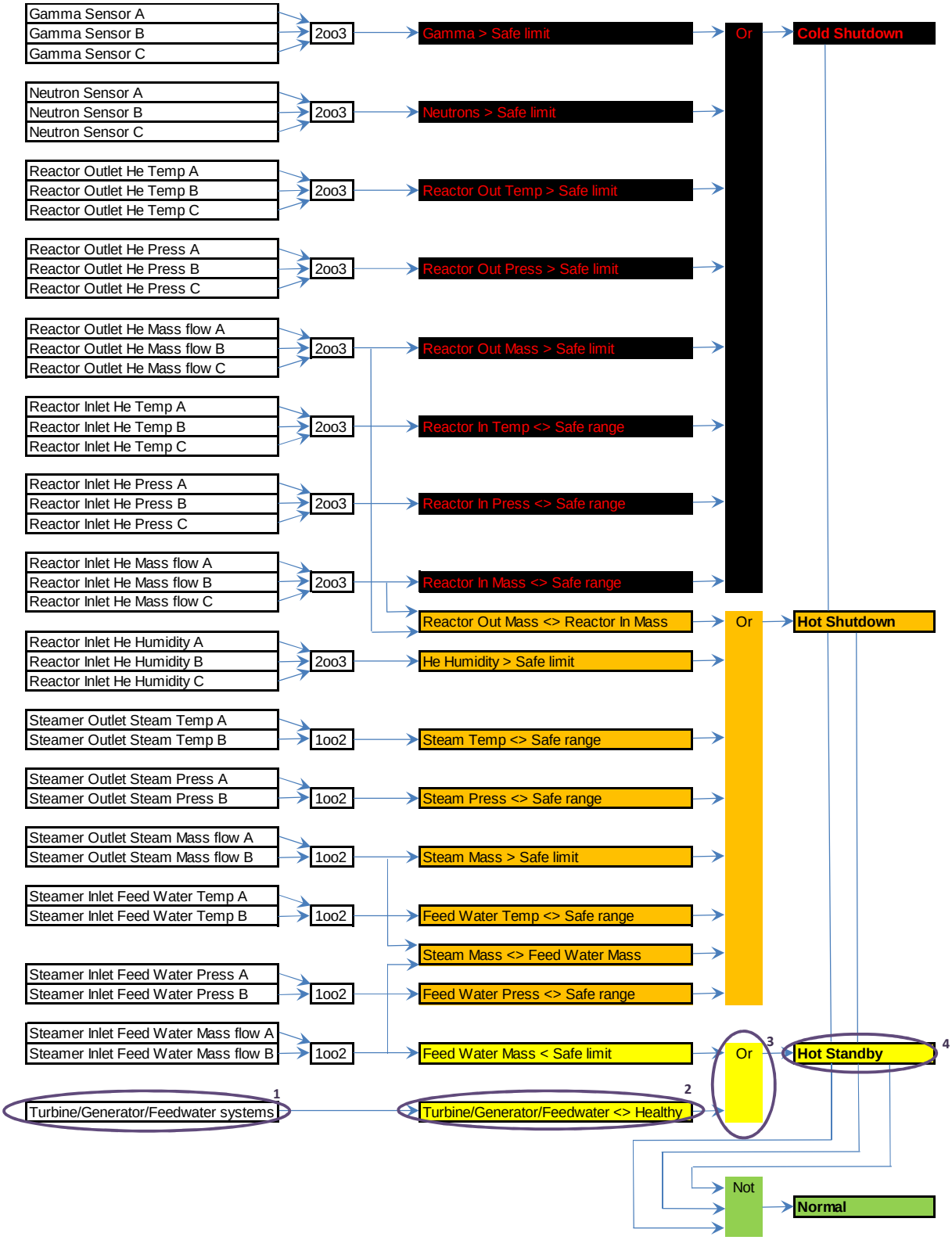
$$T3 = 1.1 \times 10^{-1} \qquad \text{Equation 4.52}$$

4.3 Case study 3: Hot Standby

In Case study 3 abnormal high ambient temperatures are being experienced and the operator(s) need to reduce loads on all the running units to compensate for the less efficient condensers. The operator(s) start reducing the loads of the units one by one starting at unit 1 and continue chronologically. However before all the units' outputs could be reduced one turbine tripped due to high condenser levels and the Turbine/Generator/Feedwater healthy signal is lost at the Control and Limitation System.

Referring to Figure 9, Figure 21 shows as soon as the Turbine/Generator/Feedwater healthy signal is lost and the Control and Limitation System will change the operating mode to hot standby mode.

Figure 21 – Th-100 NPP Control Logic for Case 3

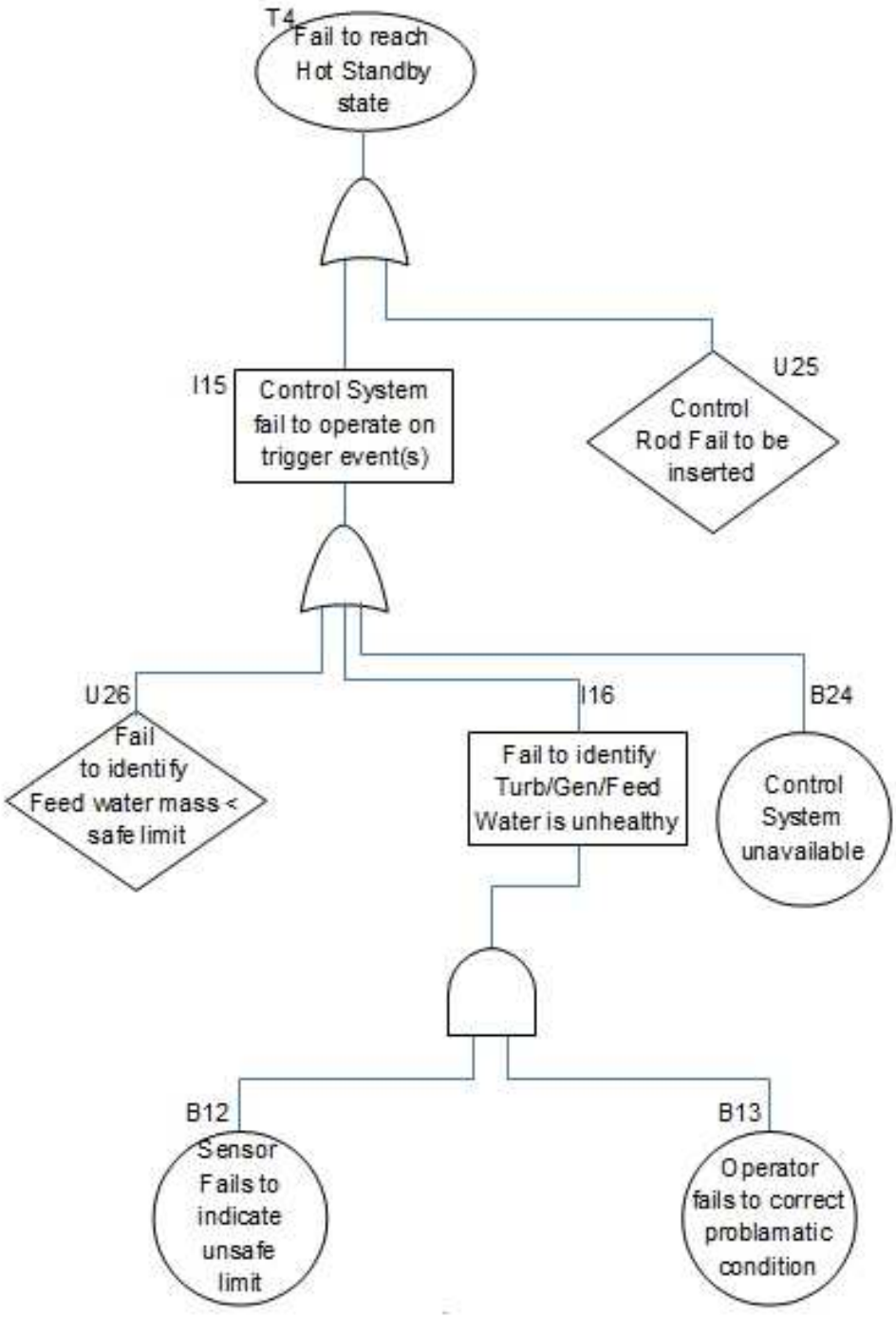


Referring to Table 3, the control rods will be fully inserted, at a slow rate to limit xenon poisoning, thereby enabling the quick run-up as soon as the fault(s) have been cleared on the Turbine/Generstor/Feedwater system.

4.3.1 Develop FTA: Failure to reach Hot Standby State

A further investigation to why the Control and Limitation system will not reach a hot standby state when it is required is done by using the FTA. Figure 22 indicates all the events that need to occur, to prevent the Control and Limitation System to successfully protect the plant from an unsafe condition typically as explained in Case Study 3.

Figure 22 - Fault Tree Analysis: Fail to reach hot standby



Referring to Figure 22 the top level event can be written, by using Boolean algebra as follows:

$$T4 = I15 + U25$$ Equation 4.53

$$I15 = U26 + I16 + B24$$ Equation 4.54

$$I16 = B12 \cdot B13$$ Equation 4.55

By using top down substitution Equation 4.53-4.55 can be manipulated to form the minimum cut set expression for T4 the top level event.

$$T4 = U26 + B12 \cdot B13 + B24 + U25$$ Equation 4.56

The undeveloped terms U26 has already been evaluated by the FTA "Fail to identify a 1oo2 safe limit" system, as can be seen in Figure 18. Referring to Equation 4.33 it is clear that

$$U26 = T\_Y1 = B\_Y2 \cdot B\_Y3 \cdot B\_Y4$$ Equation 4.57

It is assumed for this basic design all similar equipment has the same failure rates meaning:

$$B_{sensor} = B12 = B\_Y2 = B\_Y3$$ Equation 4.58

$$B_{Human} = B13 = B\_Y4$$ Equation 4.59

$$B_{CPU} = B24$$ Equation 4.60

Using Equation 4.58-4.60 the top event(T4) as described in Equation 4.56 can be simplified as follows:

$$T4 = B_{sensor} \cdot B_{sensor} \cdot B_{Human} + B_{sensor} \cdot B_{Human} + B_{CPU} + U25$$ Equation 4.61

4.3.2 FTA Qualitative evaluation: Failure to reach Hot Standby State

Form the minimum cut set expression for the top event, Failure to reach Hot Standby state, T4, as shown in Equation 4.61, the following one termed minimum cut sets are derived.

$$M21 = B_{CPU}$$ Equation 4.62

$$M22 = U25$$ Equation 4.63

With the remaining multi termed cut sets:

$$M23 = B_{sensor} \cdot B_{Human}$$ Equation 4.64

$$M24 = B_{sensor} \cdot B_{sensor} \cdot B_{Human}$$ Equation 4.65

Qualitatively the single term cut sets (M21 – M22) has a bigger influence on allowing the system to fail and is discussed first. With reference to Equation 4.62, it is clear that the control system hardware requires a very high availability. With reference to Equation 4.63, if a probability of failure needs to be lowered it is recommended to the designers split the control rods into three different banks of which two is required to bring the reactor to hot standby. The difference between a single sensor and a 1oo2 combination can be clearly seen comparing Equation 4.64 and Equation 4.65.

4.3.3 FTA Quantitative evaluation: Failure to reach Hot Standby State

For a quantitative evaluation the failure rates of each term in the minimum cut, T4, as shown in Equation 4.61 set is required.

The IAEA (INTERNATIONAL ATOMIC ENERGY AGENCY, 1988) reports the following mean failure rates:

- Control rods fail to be inserted (U25) of 2.0×10^{-7}/hr equates to 1.8×10^{-3}/y
- Controller general fails (B_{CPU}) of 7.1×10^{-7}/hr equates to 6.2×10^{-3}/y
- Indicating instrument electronic general faulty measurement (B_{sensor}) of $7.7\text{x}10^{-7}$/hr which equates to 6.8×10^{-3}/y

For B_{Human} a human error potential of 0.1 can be considered with regard to the recommendation of the Health and Safety Executive report (Health and Safety Executive, 2012) which state that it is valid in most cases.

$$\mathrm{T4} = (6.8 \times 10^{-3}) \cdot (6.8 \times 10^{-3}) \cdot (0.1) + (6.8 \times 10^{-3}) \cdot (0.1) + (6.2 \times 10^{-3}) \ + 1.8 \times 10^{-3}$$

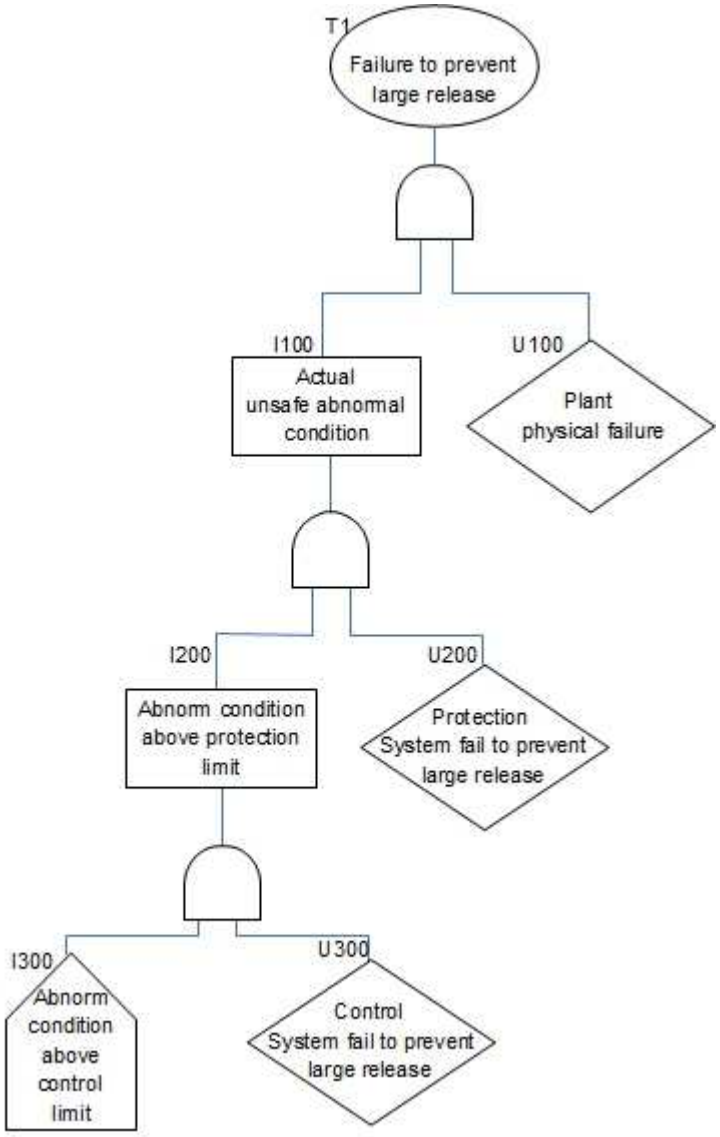
$$\mathrm{T4} = 8.7 \times 10^{-3} \qquad \text{Equation 4.66}$$

CHAPTER 5: ARCHITECTURE VERIFICATION

Thus far the control and limitation system evaluations showed how it should operate, what can cause that it does not operate as it should, qualitative evaluations showed how it can be made more reliable and quantitative evaluations showed what failure rates can be expected. To verify these findings it needs to be compared with similar studies, however these studies are not easily obtained. There is however a large number of studies which has been done comparing the different nuclear power plants probabilities of core damages and large radiation releases, as summarised in Figure 6. If the methods of chapter 4 are expanded to determine the probability of a possible catastrophic disaster it can be compared to these studies and if found that it is better than the majority of class III reactors it can be assumed that the findings of chapter 4 are verified.

With reference to Figure 12, which displays the different safety margins, a FTA, as shown in Figure 23 is developed, showing the different safety margins, which will prevent a large release of radiation.

Figure 23 – General Fault-tree analysis indicating the safety margins

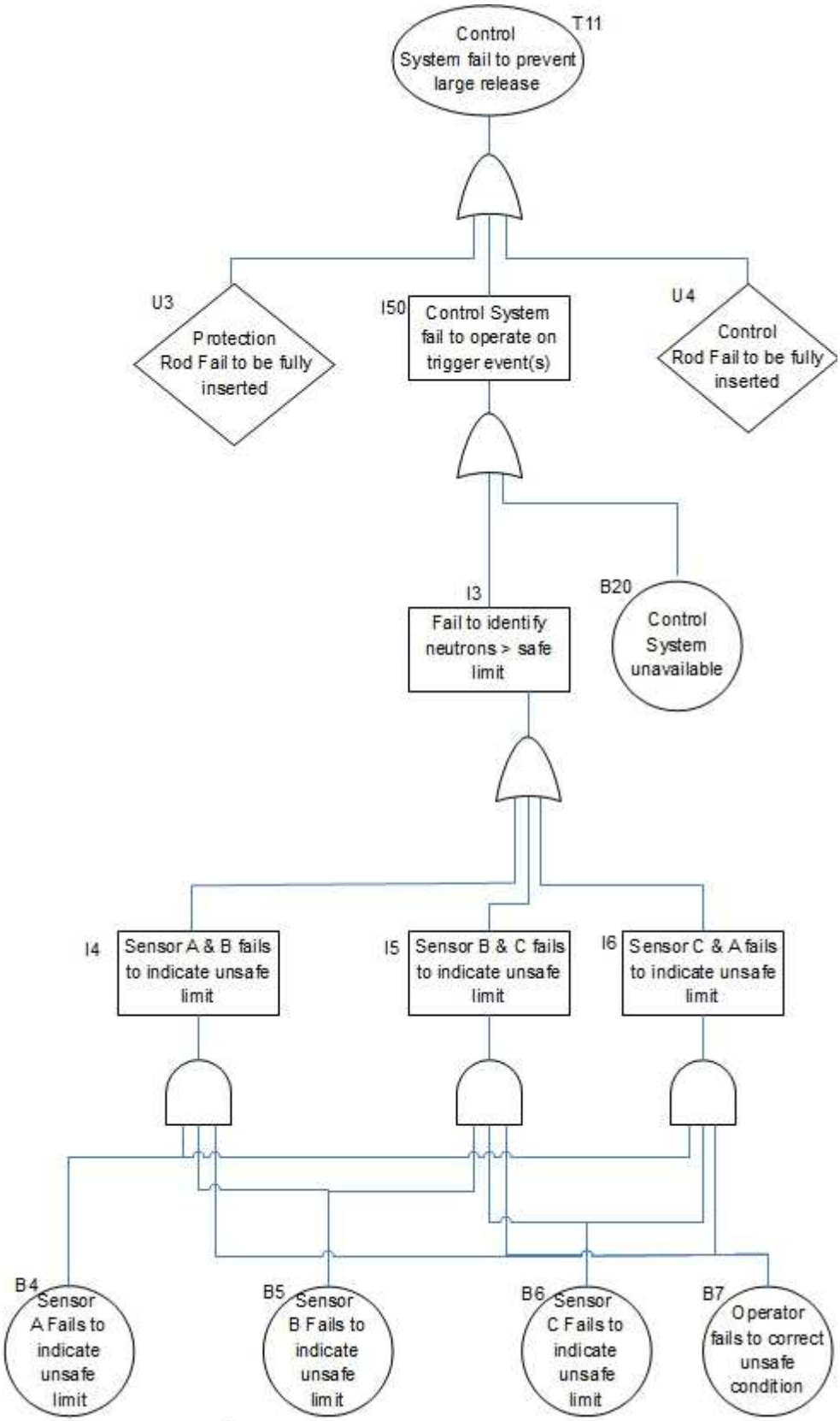


To evaluate Figure 23, the undeveloped events U300, Control and Limitation System fail to prevent a large release, as well as U200, Reactor Protection System fail to prevent a large release, needs to be developed.

5.1 Control and Limitation System failure to prevent a large release

For U300, Control and Limitation System fail to prevent a large release, as shown in Figure 23 the FTA look very similar to what has been done in Chapter 4.1 Case study 1:Cold Shutdown, as can be seen in Figure 24.

Figure 24 – Control and Limitation System fail to prevent a large release



Referring to Figure 23 the top level event, T11 – Control and Limitation System fail to prevent a large release of radiation, can be written by using Boolean algebra as follows:

$$T11 = U3 + I50 + U4 \quad \text{Equation 5.1}$$

$$I50 = I3 + B20 \quad \text{Equation 5.2}$$

$$I3 = I4 + I5 + I6 \quad \text{Equation 5.3}$$

$$I4 = B4 \cdot B5 \cdot B7 \quad \text{Equation 5.4}$$

$$I5 = B5 \cdot B6 \cdot B7 \quad \text{Equation 5.5}$$

$$I6 = B4 \cdot B6 \cdot B7 \quad \text{Equation 5.6}$$

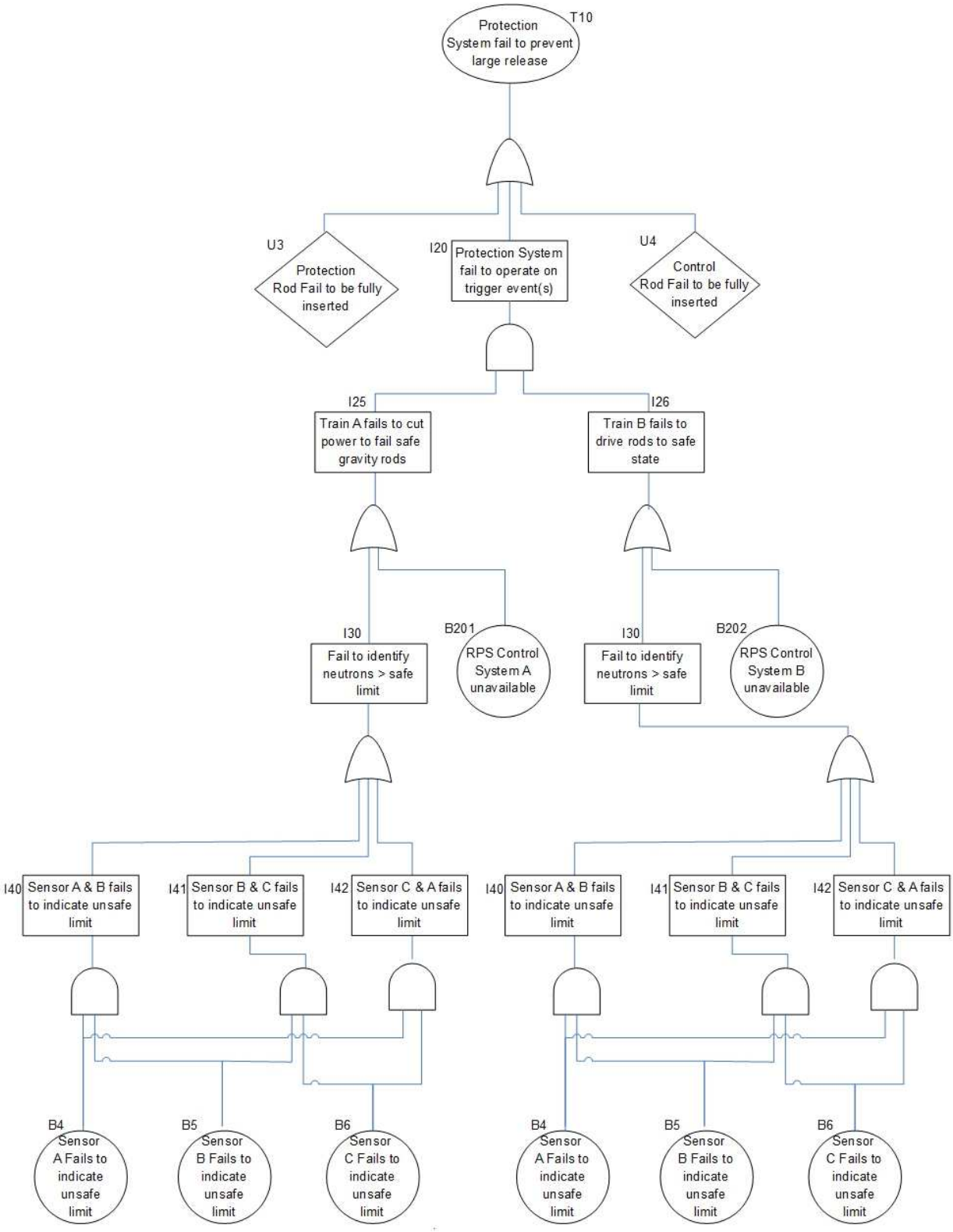
By using top down substitution, Equation 5.1-5.6 can be manipulated to form the minimum cut set expression for T11 the top level event.

$$T11 = U3 + (B4 \cdot B5 \cdot B7 + B5 \cdot B6 \cdot B7 + B4 \cdot B6 \cdot B7) + B20 + U4 \quad \text{Equation 5.7}$$

5.2 Reactor Protection System failure to prevent a large release

For U200, Reactor Protection System fail to prevent a large release, as shown in Figure 23, the FTA is developed according to Figure 10 – Th-100 NPP Protection Logic and is shown in Figure 25.

Figure 25 – Reactor Protection System fail to prevent a large release



Referring to Figure 25 the top level event, T10 – Reactor Protection System fail to prevent a large release of radiation, can be written by using Boolean algebra as follows:

$$T10 = U3 + I20 + U4$$ Equation 5.8

$$I20 = I25 \cdot I26$$ Equation 5.9

$$I25 = I30 + B201$$ Equation 5.10

$$I26 = I30 + B202$$ Equation 5.11

$$I30 = I40 + I41 + I42$$ Equation 5.12

$$I40 = B4 \cdot B5$$ Equation 5.13

$$I41 = B5 \cdot B6$$ Equation 5.14

$$I42 = B4 \cdot B6$$ Equation 5.15

By using top down substitution, Equation 5.8-5.11 can be manipulated to form

$$T10 = U3 + (I30 + B201) \cdot (I30 + B202) + U4$$ Equation 5.16

Making use of the distributive law ($X+Y \cdot Z=(X+Y) \cdot (X+Z)$) Equation 5.16 can be simplified as:

$$T10 = U3 + I30 + (B201 \cdot B202) + U4$$ Equation 5.17

Substituting Equation 5.12-5.15 in Equation 5.17, the top level event(T10) can be expanded as follows:

$$T10 = U3 + B4 \cdot B5 + B5 \cdot B6 + B4 \cdot B6 + (B201 \cdot B202) + U4$$ Equation 5.18

5.3 Determining the Probability of a large release for the Th-100

With reference to Figure 23, the top level event, T1 Failure to prevent a large release of radiation, can be written by using Boolean algebra as follows:

$$T1 = I100 \cdot U100$$ Equation 5.19

$$I100 = I200 \cdot U200$$ Equation 5.20

$$I200 = I300 \cdot U300$$ Equation 5.21

Where U300, Control and Limitation System fail to prevent a large release is shown in Equation 5.7, thus:

$$U300 = T11 = U3 + (B4 \cdot B5 \cdot B7 + B5 \cdot B6 \cdot B7 + B4 \cdot B6 \cdot B7) + B20 + U4$$

Equation 5.22

U200, Reactor Protection System fail to prevent a large release is shown in Equation 5.18, thus:

$$U200 = T10 = U3 + B4 \cdot B5 + B5 \cdot B6 + B4 \cdot B6 + (B201 \cdot B202) + U4$$

Equation 5.23

By using top down substitution, Equation 5.19-5.23 can be manipulated to form the minimum cut set expression for T1 the top level event.

$$T1 = I300 \cdot (U3 + (B4 \cdot B5 \cdot B7 + B5 \cdot B6 \cdot B7 + B4 \cdot B6 \cdot B7) + B20 + U4) \cdot (U3 + B4 \cdot B5 + B5 \cdot B6 + B4 \cdot B6 + (B201 \cdot B202) + U4) \cdot U100$$

Equation 5.24

For a quantitative evaluation the failure rates of each term in the minimum cut, T1, as shown in Equation 5.24 set is required.

The IAEA (INTERNATIONAL ATOMIC ENERGY AGENCY, 1988) reports the following mean failure rates:

- Control rods fail to be inserted (U3=U4) of 2.0×10^{-7}/hr equates to 1.8×10^{-3}/y
- Indicating instrument electronic general faulty measurement (B4=B5=B6) of $7.7\text{x}10^{-7}$/hr which equates to 6.8×10^{-3}/y
- Controller general fails (B20=B201=B202) of 7.1×10^{-7}/hr equates to 6.2×10^{-3}/y

The Health and Safety Executive report (Health and Safety Executive, 2012) reports the following mean failure rates:

- Human error (B7) potential of 0.1 can be considered
- Catastrophic failure rate of a spherical pressure vessel (U100) = 4×10^{-6}/y

The term I300 which state that the abnormal condition exist, which has the potential to cause a catastrophic failure is unknown and implies that there are a large number of the fuel kernels that have been damaged inside various fuel pebbles. This event is very unlikely and although the probability is unknown it should be less than 1, causing Equation 5.24 to be simplified as follows:

$$T1 < (1) \cdot (U3 + B4 \cdot B5 \cdot B7 + B5 \cdot B6 \cdot B7 + B4 \cdot B6 \cdot B7 + B20 + U4) \cdot (U3 + B4 \cdot B5 + B5 \cdot B6 + B4 \cdot B6 + (B201 \cdot B202) + U4) \cdot U100$$ Equation 5.25

With estimated values for all terms of Equation 5.25 the probability of reaching a failure where a large radiation release is present can be calculated as follows:

$$T1 < (1) \cdot ((1.8 \times 10^{-3}) + (6.8 \times 10^{-3}) \cdot (6.8 \times 10^{-3}) \cdot (0.1) + (6.8 \times 10^{-3}) \cdot (6.8 \times 10^{-3}) \cdot (0.1) + (6.8 \times 10^{-3}) \cdot (6.8 \times 10^{-3}) \cdot (0.1) + (6.2 \times 10^{-3}) + (1.8 \times 10^{-3})) \cdot ((1.8 \times 10^{-3}) + (6.8 \times 10^{-3}) \cdot (6.8 \times 10^{-3}) + (6.8 \times 10^{-3}) \cdot (6.8 \times 10^{-3}) + (6.8 \times 10^{-3}) \cdot (6.8 \times 10^{-3}) + ((6.2 \times 10^{-3}) \cdot (6.2 \times 10^{-3})) + (1.8 \times 10^{-3})) \cdot (4 \times 10^{-6})$$

$$T1 < 1.5 \times 10^{-10}$$ Equation 5.26

5.4 Summary of results

Although both qualitative and quantitative evaluations have been done for all the different failure modes of the Control and Limitation System, it is only the combined effects of the Control and Limitation System, the Reactor Protection System and the plant's physical characteristics that are compared to previous studies on other nuclear power stations. The quantitative evaluation of the combined effects has a probability of a large release to occur that meets the requirements of a Generation IV system, if it is better than the Generation III nuclear power stations as shown in Figure 6. This means that the probability of a large release should be less than $1x10^{-8}$.

The final results in Chapter 5 originated from the evaluations in Chapter 4. Therefore, the summary includes the findings of Chapter 4.

The Control and Limitation System has three possible protection modes apart from the normal safe operations, namely Cold shutdown, Hot shutdown and Hot standby. The typical case studies presented for each possible protection mode, clearly show that the operator has the option to correct the situation before the Control and Limitation System takes control. However, once the unsafe limit has been reached, the operator is unable to intervene further.

For the Cold shutdown it was determined that since all protections are a similar 2oo3 configuration, all possible events where the system fails to identify the unsafe condition is of the same magnitude and the combined effect of the probability of failure to reach Cold shutdown is calculated to be 9.8×10^{-3} (see Equation 4.19). From this evaluations it have been identified that if the probability of failure needs to be lowered, design-engineers are recommended to split the control rods and the protection rods into different banks and size these rods that only three of the four bank of rods are required to stop the nuclear reactions.

The relative low probability of the Control and Limitation System to not reach Hot shutdown when required, is determined in Equation 4.52 to be 1.1×10^{-1}. From this figure, 80% is contributed to the fact that the single bypass valve needs to open. This low value clearly indicates the need that the core should be designed to have an internal passive heat sink which will allow heat generated by the core to be dissipated, without having it to be transferred via a steamer bypass system to an external heat sink. In this case where no bypass is installed, the probability of failure to reach Hot shutdown is reduced to a more favourable figure of 2.4×10^{-2}. If an external heat sink that is activated through a bypass system is required, it is recommended to have an alternative bypass valve installed parallel to the existing valve. With two parallel bypass valves the probability of failing to reach Hot shutdown is calculated at 3.2×10^{-2}.

The probability of failure of the Control and Limitation System to reach Hot standby is calculated in Equation 4.66 to be 8.7×10^{-3}. This figure is in-line with the failure to reach Cold shutdown. This value is determined predominately by the availability of the control system as well as the single control rod bank.

To verify the findings, similar evaluations to Chapter 4 have been done in Chapter 5 regarding the probability of an event that will have a large release of radiation. The probability is a function of the Control and Limitation System that requires a malfunction to prevent a shutdown. It also necessitates the Reactor Protection system malfunction to prevent physical damage to the plant. From the developed FTA, as shown in Figures 23 to 25, it is clear that the operator can only influence any event before the unsafe event reached the Control and Limitation System's safe limits. The Reactor Protection System will only be utilised if the Control and Limitation System malfunctions and is fully automated and no operator is thus able to influence the working of the system. The critical scenario will only occur if the Control and Limitation System, the Reactor Protection System and the physical pressure vessel fail. The probability of causing a large release of radiation is determined in Equation 5.26 to be less than 1.5×10^{-10}. Comparing this result to Figure 6 it is clear that the Th-100 is better equipped to prevent large releases of radiation than any other Generation III nuclear power plant.

In conclusion the architecture, as conceptually explained in Chapter 3 and evaluated in detail in Chapter 4, has been verified in Chapter 5.

CHAPTER 6: CONCLUSION

6.1 Establishing the need

Various small nuclear plants are currently being developed world wide. Although pebble bed High Temperature Reactor Nuclear Power Plants are of the oldest nuclear concepts, its inherent safety features still interest new developers. The unique fuel pebbles which contain 0.5mm diameter kernels surrounded by porous carbon, two pyrolytically deposited layers of carbon and one layer of silicon carbide, have proven to provide a pressure boundary that confines the fission products to the kernels. Even in the worst scenario where the complete loss of force cooling has been tested, operational proof was obtained that the core temperature remains below the fuel failure temperature and thus, the nuclear fission products retain within the fuel pebbles.

As developers continue to modernise the design of Nuclear Power Plants, it is necessary that new designs are competitive to other available power plants. The current nuclear industry is predominately Light Water Reactors, which has a high power density core, meaning that more power can be generated per nuclear core. Yet, this design still requires extremely high safety features as a nuclear meltdown is possible. The inherent safe HTR has a much lower power density core and requires multiple nuclear reactors to generate the same amount of electricity as produced by a single Light Water Reactor. For new HTR power Plants to remain competitive with other technologies, the reducing of operators is now being investigated.

Some of the coal power industries have already implemented the use of a multi-unit control room successfully. Thus, research focusing on the optimal number of operators that are required for the battery of HTR plants was the next logical step. Unfortunately, no applicable literature could be found on the topic and no method could be identified to verify a proposed alternative number of operators. The difficulties to establish the optimal number of operators and to prove the new concept of multi-unit control rooms within the nuclear industry are also evident in the laborious efforts of NuScale, the developers of a new multi-unit small Light Water Reactor. A full scale multi-unit control room simulator has been developed for the NuScale concept.

The U.S. Nuclear Regulatory Commission (NRC) is well aware that current regulations which has evolved over the years concerning large Light Water Reactors, do not address the possibility that more than two reactors are being controlled from one control room. Thus the safety implications of having a multi-control room will have to be investigated, before the

reduction of staff can be evaluated. The evaluation and verification of the architecture suitable for a multi-unit control room for a pebble bed High Temperature Reactor Nuclear Power Plant, will form the basis of an application to reduce the number of operators, which is to be submitted to prove that an operator error will not influence the safety implications.

6.2 Proof that the need is addressed

It is assumed that this dissertation will form the basis for the application to the NRC to relax operator requirements. Therefore, the following vital information is to be considered as set out below.

6.2.1 Brief summary on the history of HTR plants

It was Prof Farrington Daniels that first proposed the pebble bed gas cooled nuclear reactor concept in 1942. For years, both the AVR and the THTR reactor operated successfully. However, the Chernobyl accident in 1986, which also used carbon as a moderator, has stopped research and development of similar power plants. Various HTR plants were designed based on the proven concepts, but only the Chinese were able to build a 2.5 MW_e test reactor in 2000 and subsequently a 210 MW_e power plant construction was started in 2012.

6.2.2 Fault Tree Analysis – Evaluation method

The nuclear industry is known to prefer the Fault Tree Analysis (FTA) to calculate the probability of failures that could occur. Subsequently, FTA is also used to compare the various nuclear power plants with one another. The qualitative and quantitative evaluations done on the architecture also supplied valuable feedback for the design engineers.

6.2.3 Th-100 Architecture

The Th-100 has been identified as a typical pebble bed High Temperature Reactor Nuclear Power Plant. The literature study in Chapter 2 includes public information regarding the safety system associated with the design such as:

- Ceramic fuel elements which cannot melt in extreme accidents where total loss of cooling is present;
- Fission product retention within the fuel kernels;
- Helium coolant which is both chemically and radiological inert;
- Passive decay heat removal capability;
- Strong negative temperature coefficients; and

- Independent barriers protect fission products release, namely silicone carbide fuel kernels, the pressure vessel and a containment building.

The information pertained in Chapter 3 is based on concept designs of Steenkamp Kraal Limited at the time and include details regarding the safety thereof, below:

- A control room (The Emergency Control Room) with 10 hour battery back-up, which can withstand flooding, lightning storms, earthquakes and certain airplane attacks which contains the two independent automated protection systems called the Control and Limitation System as well as the Reactor Protection System;
- A control room (The Main Control Room) situated in a semi-remote area, which are foreseen to be shared with different nuclear units and auxiliary systems and duplicate the monitoring and control via the two automated protection systems of the Emergency Control Room;
- The Control and Limitation system is set to maintain the reactor with-in the safe normal limits;
- The Reactor Protection System will operate once the Control and Limitation System failed to keep it within safe limits and takes precedence above the Control and Limitation System;
- Various sensors are used to determine if the state of the reactor and the concept 1oo2 and 2oo3 are explained;
- The Control and Limitation Systems use the sensors to determine which one of the following states are operated, namely the Normal operations, the Hot standby, the Hot shutdown or the Cold shutdown; and
- For the Reactor Protection System, the input sensors are shared with the Control and Limitation System. However, the fail-safe concept and the application of the two independent trains are explained with the activation of reactor controls.

A theoretical control logic based on the proposed architecture has been developed to explain in detail how the Control and Limitation System should operate. Chapter 4 deals with the evaluation of the architecture that was developed for a multi-unit control room and is based on the control logic of the Control and Limitation System. Probable case studies, typical in a multi-unit control room associated with human error were introduced. In none of the cases the operator was able to intervene after the unsafe limits have been reached. Qualitative and quantitative evaluations highlighted areas which could be designed to be more reliable. An

example involves that the control rods are to be split in different banks, where three of the four operating banks will be able to shut down the reactor.

The suitability of the architecture for a multi-unit control room has been confirmed and verified in Chapter 5, where the probability of an event that will have a large release of radiation has been calculated by applying the same methods as in Chapter 4. Although the improbable event of the fission products not being retained within the fuel kernels was assumed to be already in action and no containment building was used in the calculations, the results was in the order of 10^{-10}. On the other hand, other independent studies have revealed that the best Generation III+ plants has a probability of a large release which is in the order of 10^{-8} . Thus it can be assumed that the evaluation in Chapter 4 has been verified.

6.2.4 Conclusion: Proof that the need is addressed

The need was identified to prove that the safety implications will not be influenced by an operator error when operating from a multi-unit control room. Apart from the inherent safety features of a HTR which was highlighted, the detail architecture has been discussed, evaluated and verified. The typical case studies clearly indicate that the operator cannot influence the protection system, once the unsafe limits have been reached. With the assumption that this dissertation will form the base document of an application to the NRC to relax the operator requirements, all reliability figures for the Control and Limitation System has already been calculated.

6.3 Recommendations

The evaluation and verification of an architecture suitable for a multi-unit control room of a pebble bed High Temperature Reactor Nuclear Power Plant revealed that operator errors do not affect the protection systems negatively. In future, research could focus on the identification of the optimal number of operators that would be needed for such power plants. Then again, the verification of such findings could be problematic as no previous research and case studies have been conducted on the recommended topic. Also, in future a more practical approach could be followed where the first unit should be manned as per regulations. Studies can be conducted on the operators to investigate their work load and from these results a reduction can be motivated and permission be requested for testing on a live unit. This process should be ongoing to optimise the number of operators. Once the HTR power plant cost has been reduced, there could be no justification for continuing to build fossil fuel power plants that increase pollution or erect nuclear plants that are inherently unsafe.

BIBLIOGRAPHY

Abu-Khader, Mazen M. 2009. Recent advances in nuclear power: A review. 2009, Vols. Progress in Nuclear Energy 51 (2009) 225–235, doi:10.1016/j.pnucene.2008.05.001.

American Nuclear Society. July 2010. *Interim report of the American Nuclear Society President's special committee on small and medium sized reactor (SMR) generic licensing issues .* July 2010.

AREVA NP Inc. October 2010. *Pebble Bed Reactor Assessment Executive Summary.* October 2010. Technical Data Record. Document No.: 12 - 9155160 - 000.

Boy, Guy A. and Schmitt, Kara A. 2012. Design for safety: A cognitive engineering approach to the control and management of nuclear power plants. 2012, Vols. Annals of Nuclear Energy 52 (2013) 125–136, http://dx.doi.org/10.1016/j.anucene.2012.08.027.

Chang, Soon Heung; Choi, Seong Soo; Park, Jin Kyun; Heo, Gyunyoung; Kim, Han Gon. 1998. Development of an advanced human–machine interface for next generation nuclear power plants. 1998, Vols. Reliability Engineering and System Safety 64 (1999) 109–126, PII: S0951-8320(98)00073-8.

EDF Energy. 2013. The UK EPR digital I&C system. *http://www.neimagazine.com/.* [Online] April 2013.

Fabrycky, Benjamin S. Blanchard & Wolter J. 2006. *System Engineering and Analysis.* Fourt Edition. Mew Jersey : Pearson Prentice Hall, 2006. ISBN 0-13-186977-9.

GSE Systems Inc. 2012, October 5. *World's First Control Room Simulator for a Multi-Unit Nuclear SMR Uses Technology from GSE Systems.* Sykesville (Baltimore) : s.n., 2012, October 5.

Health and Safety Executive. 2012. *Failure Rate and Event Data for use within Risk Assessments (28/06/2012).* 2012. PCAG chp_6K Version 12 – 28/06/12.

Hixson, Lucas W. 6 Aug 2011. Nuclear Microreactors (SMRs—small modular reactors). *www.enformable.com.* [Online] 6 Aug 2011.

IAEA. 2004. *Status of advance light water reactor designs.* Vienna : Internation Atomic Energy Agency, 2004. TECDOC-1391.

INTERNATIONAL ATOMIC ENERGY AGENCY. 1988. *COMPONENT RELIABILITY DATA FOR USE IN PROBABILISTIC SAFETY ASSESSMENT.* Vienna : s.n., 1988. IAEA-TECDOC-478.

International Atomic Energy Agency. May 2005. *Innovative small and medium sized reactors: Design features, safety approaches and R&D trends. Final report of a technical meeting.* s.l. : International Atomic Energy Agency, May 2005. IAEA-TECDOC-1451.

—. Aug 2011. *Status report 96 - High Temperature Gas Cooled Reactor - Pebble-Bed Module (HTR-PM).* Vienna, Austria : International Atomic Energy Agency, Aug 2011.

Maillart, Herve´. 1999. Design of the I&C for the European pressurised water reactor. 1999, Vols. Nuclear Engineering and Design 187 (1999) 135–141, PII: S0029-5493(98)00260-X.

Mcdowell, B K; Mitchell, M R; Nickmoloaus, J R; Pugh, R; Swearingen, G L October 2011. *High Temperature Gas Reactors: Assessment of Applicable Codes and Standards.* Richland, Washington 99352 : Pacific Northwest National Laboratory, October 2011. Prepared for the U.S. Nuclear Regulatory Commission under an Interagency Agreement with the U.S. Department of Energy Contract DE-AC05-76RL01830. PNNL-20869.

NEA. 2010. *Comparing nuclear accident risk with those from other energy sources.* s.l. : Nuclear Energy Agency - Organisation for economic co-operation and development, 2010. NEA No. 6861 ISBN 978-92-64-99122-4.

O'Hara, John M, Higgens, James C. and Brown, William S. September 2008. *Human Factors Considerations with Respect to Emerging Technology in Nuclear Power Plants.* s.l. : Brookhaven National Laboratory, September 2008.

Parker, Don. February 2013. Plant Automation Advancements: The Australian experience. February 2013.

Steenkampskraal Thorium Limited. 2011. Steenkampskraal Thorium Limited: Reactor safety. *http://www.thorium100.com/.* [Online] 2011. http://www.thorium100.com/.

Suh, Yong Suk, Keum, Jong Yong and Kim, Hyeon Soo. 2011. Developing architecture for upgrading I&C systems of an operating nuclear power plant using a quality attribute-driven design method. 2011, Vols. Nuclear Engineering and Design 241 (2011) 5281–5294, doi:10.1016/j.nucengdes.2011.09.027.

Travers, William D. October 7, 2002. *LEGAL AND FINANCIAL POLICY ISSUES ASSOCIATED WITH LICENSING NEW NUCLEAR POWER PLANTS.* s.l. : NRC, October 7, 2002. SECY-02-0180.

U.S. Nuclear Regulatory Commission. *Code of Federal Regulations, Title 10, "Energy,".* 10 CFR § 50.54 in combination with 10 CFR § 50.47.

Vesely, W. E.; Goldberg, F. F.; Roberts, N. H.; Haasl, D. F. 1981. *Fault Tree Handbook.* Washington : U.S. Nuclear Regulatory Commission, 1981. NUREG-0492.

World Nuclear Association. January 2013. Advanced Nuclear Power Reactors. *http://www.world-nuclear.org/.* [Online] World Nuclear Association, January 2013. http://www.world-nuclear.org/.

—. 2012. Small Nuclear Power Reactors. *http://www.world-nuclear.org/.* [Online] November 2012.

Zhou Yong; Mu HaiYing; Jiang Jianjun; Zhung Li. 2012. Investigation of the impact of main control room digitalization on operators cognitive reliability in nuclear power plants. 2012, Vols. Work 41 (2012) 714-721, DOI: 10.3233/WOR-2012-0231-714.