UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

Historical review of fire safety at NPP and application of fire PSA to Westinghouse PWR NPP in the frame of risk-informed decision making

by
Matthew Asamoah

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

ETSEIB

Historical Review of Fire Safety at NPP and Application of Fire PSA to Westinghouse PWR NPP in the frame of Risk-informed decision making.

Doctoral thesis presented by

Matthew Asamoah

For PhD. In Nuclear Engineering and ionizing radiations

July 2018

Thesis director:

Dr Javier Dies Llovera

Department of Physics, Division Nuclear Engineering

Technical University of Catalonia (UPC)

UPC ETSEIB

ACKNOWLEDGEMENT

My sincere thanks goes to my supervisor Javier Dies and Thesis Tutor Alfredo de Blas for their enormous guidance and support throughout this long Journey. Your patience, advice and warm reception during my stay and the development of this Thesis has been phenomenal.

I cannot forget Pedro Diaz for his support and technical advice. I very much appreciate effort, time and the patience. Also, thanks to Hector Hernandez for sharing his expertise, knowledge and insight.

Enric Estruch, Bern at Cirera Gerdard Revira, Antonio Gomez, Mohamed and Shaikha deserves my thanks for their various contribution to this work.

To my parents Mr/Mrs Twi Sakyi without you, I would not have reach this level. To my wife and kids, Dinah, Sammy and Joana, Thanks for the sacrifice and support. To my Barcelona family Mr/Mrs Nsiah, Kofi and vicentia.

My gratitude goes to Prof. E.H.K Akaho and Prof. B.J.B Nyarko of Ghana Atomic Energy Commission for support and encouragement.

Lastly Thanks to International Atomic Energy Agency (IAEA) for funding this PhD study in Spain

Table of Contents

LIST OF TABLES

LIST OF FIGURE

LIST OF ABBREVIATIONS

ACRS	Advisory Committee on Reactor Safeguards
AEC	Atomic Energy Commission
AESJ	Atomic Energy Society of Japan
AltNum	Alternate Number
APCSB	Auxiliary and Power Conversion Systems Branch
ATWS	Anticipated Transients without Scram
BCNum	Boundary condition Number
BCSet	Boundary Condition Set
BFN	Brown Ferry Nuclear power plant
BfS	Federal Office for Radiation Protection (Bundesamt für Strahlenschutz)
BTP	Branch Technical Position
BWR	Boiling Water Reactor
CAC	Consequence Analysis Case
CAFTA	Computer Aided Fault Tree Analysis
CCDP	Conditional Core Damage probability
CD	Core Damage
CDF	Core Damage Frequency
CFAST	Consolidated Model of Fire Growth and Smoke Transport
CFR	Code of federal Regulation
CMEB	Chemical Engineering Branch
CSN	nuclear regulatory commission of Spain
DID	Defense In Depth
DOE	Department of Energy
ECCS	Emergency Core cooling System
EOOS®	Equipment-Out-Of-Service
EPRI	Electric Power Research Institute
ET	Event Tree

ET_Seq	Event Tree Sequence
ETEvent	Event Tree Event
ETNodes	Event Tree Nodes
ETNum	Event Tree Number
EventNUM	Event Number
FDS	Fire Dynamics Simulator
FEInput	Function Event Input
FEType	function Event type
FMEA	Failure Mode and Effect Analysis
FP	Full Power
FPPs	fire protection programs
FRM	Fire Risk Matrix
FZs	Fire Zones
GDC	General Design Criterion
GL	Generic Letter
HEP	Human Error Probabilities
HFE	Fire Human Failure Events
HPos	Horizontal Position
HRA	Human Reliability Analysis
IAEA	international Atomic Energy Agency
InputNum	Input Number
INSAG	International Nuclear Safety Advisory Group.
IPEEE	Individual Plant Examination for External Events
KSFs	Key Safety Functions
KTA	Nuclear Safety Commission Germany
LARs	Licensing Amendment Requests
LLL	Lawrence Livermore Laboratory
LOCA	Lost of coolant Accident

LPSA	Living Probabilistic safety Assessment
MCDET	Monte Carlo Dynamic Event Tree
MCR	Main Control Room
MCS	Minimal cut sets
METI	Ministry of Economy, Trade and Industry
NAIIC	Independent Investigation Commission
NEA	Nuclear Energy Agency
NEI	Nuclear Energy Institute
NERG	Nuclear Engineering Research Group
NFPA	National Fire Protection Association
NPP	Nuclear Power Plant
NPR	New Production Reactor
NRA	Nuclear Regulatory Authority
NRC	Nuclear Regulatory Commission
NSC	Nuclear Safety Commission
NUREG	US Nuclear Regulatory Commission Regulation
OECD	Organization for Economic Co-operation and Development
OPSA-MEF	The Open-PSA Model Exchange Format
PDA	automatic fire detection
PEA	automatic fire suppression
PFB	fire brigade
PRA	Probabilistic Risk Assessment
PS	prompt suppression
PSA	Probabilistic Safety Assessment
PWR	Pressurized Water Reactor
QA	Quality Assurance
RATC	Risk Assessment Technical Committee
RAW	Risk Achievement Worth

RCP	Reactor Coolant Pump
RMIEP	Risk Methods Integration and Evaluation Program
RRG	Regulatory Review Group
RSS	Reactor Safety Study
SBO	Site Black Out
SECY	NRC’s Office of the Secretary
SeqNum	Sequence Number
SeqPos	Sequence Position
SNAS	School of Nuclear and allied Sciences
SNL	Sandia National Laboratories
SRP	Safety Review Plan
SSC	Structures, Systems, and Components
SSD	Safe Shutdown
TC	Technical Cooperation
TECDOC	Technical Document
UCLA	University of California at Los Angeles
UPC	Technical University of Catalonia
USNRC	United States Nuclear Regulatory Commission
UM	Unavailability Matrix
Vpos	Vertical Position
WASH	short for Washington. The AEC used WASH as a prefix for its documents
WNA	World Nuclear Agency

PREFACE

In 1961, the Government of Ghana decided to undertake the "Ghana Nuclear Reactor Project (GNRP)." This was intended to introduce nuclear science and technology into the Country and to exploit the peaceful applications of nuclear energy to foster national development. The central facility of the project was to be a research reactor designed solely for research, training and production of radioisotopes.

The long-term strategic objective of this initiative was that the research reactor would facilitate the development of manpower and promote plans for the introduction of nuclear power for electricity generation in the Country. To help realize the objective of the Ghana Nuclear Reactor Project, the Ghana Atomic Energy Commission was founded by an Act of Parliament. This dream was cut short when the first President was over thrown in 1966 and near completion of 2 MW research reactor stopped.

In 2006 the Government of Ghana wrote to IAEA about her intention to add nuclear energy to its energy mix. In view of that the School of Nuclear and Allied Sciences (SNAS) was established in 2006. SNAS is responsible for preservation, maintenance and enhancement of nuclear knowledge in Ghana and Africa through the provision of high quality teaching, research, entrepreneurship training, service and development of postgraduate programmes in the nuclear sciences and technology.

Government of Ghana in partner with IAEA Technical Cooperation (TC) programmes GHA12010 with the aim of Enhancing Human Resources Development and Nuclear Knowledge Management and GHA2002 with the aim of Human resource needs for the nuclear power programme were established. This work is based on the two TC projects upon which my study at Technical University of Catalonian (UPC) was sponsored. The 18 months sandwich fellowship programme agreement between IAEA and Nuclear Engineering Research Group (NERG) of Department of Physics and Nuclear Engineering (DFEN), School of Engineering of Barcelona (ETSEIB) Technical University of Catalonia (UPC), is structured such that six months is spent at UPC, Barcelona every year for three years.

On the other hand, the Nuclear Engineering Research Group (NERG) had established a collaborative research with the Spanish Nuclear Power Plant. Development and assessment of fire-related risk unavailability matrix. Fire-related system and key safety functions unavailability matrix and innovative tool for risk-informed decision-making at Spanish PWR NPP is developed. The Feasibility of the Development of a Fire-Related Risk Monitor from the RiskSpectrum® Fire PSA of PWR NPP has been developed. An additional work for the historical review of fire safety at Nuclear power plants in USA, Germany and Japan has been developed to make recommendations for Ghana's nuclear power programme.

The importance of fire as a potential initiator of multiple-system failures took on a new perspective after the cable-tray fire at Browns Ferry in 1975 The review have shown that the first generation Nuclear Power Plant (NPP) fire safety was not factored as high risk area that needed to be effectively assessed and quantified. This resulted in development of peculiar fire safety regulations, standards and expensive backfits. Lack of appropriate regulations and effective

methods of fire risk assessment, prescriptive, difficult and expensive retrofit regulations were instituted in USA. The alternative risk-informed performance based regulation was established in USA to resolve the challenges of the prescriptive rules. The review have revealed that both the prescriptive and risk-informed performance based approaches will not represent adequate design basis for new Nuclear Power Plants. The Japanese were pulled in the path of renew fire safety regulations and risk quantification after the Fukushima accident. It has been recognized that effective fire safety assessment, and culture, in concert with countermeasures to prevent, detect, suppress, and mitigate the effect of fires if they occur, will minimized NPP fire risk. Among the numerous recommendation the fire safety at NPP must be planned and engineered before construction begin using the state-of-the-art technology. Also, the methods of fire risk assessment must integrate the state-of-the-art deterministic and probabilistic approaches. Two methods are presented which serve to incorporate the fire-related risk into the current practices in nuclear power plants with respect to the assessment of configurations. The first method is a fire protection systems and key safety functions Unavailability Matrix (UM) which is developed to identify structures, systems, and components significant for fire-related risk. The second method is a fire zones and key safety functions (KSFs) fire risk matrix which is useful to identify fire zones which are candidates for risk management actions. The UM is an innovative tool to communicate fire risk. The Monte Carlo method has been used to assess the uncertainty of the UM. The analysis shows that the uncertainty is sufficiently bounded. The significant fire-related risk is localized in six KSF representative components and one fire protection system which should be included in the maintenance rule. The unavailability of fire protection systems does not significantly affect the risk. The fire risk matrix identifies the fire zones that contribute the most to the fire-related risk. These zones belong to the control building and electric penetrations building. The aggregation of Internal Events PSA model and Fire PSA model have shown that the Fire PSA contributes 38.4% to the Risk increase. The feasibility of developing Fire-related Risk Monitor from the FIRE PSA for the Spanish NPP was carried out. One of the main challenges is that RiskSpectrum® fire PSA has 384 fire cases and 384 CDF but in Risk Monitor one CDF is required. However, CAFTA is unable to convert a Sequential Fault Tree structure of the internal Event tree in the Fire PSA. The conversion fails to implement neither all of the sequences leading to core damage nor the Fault Tree selection of the frequency of fire. The proposal is to suppress exchange events and introduce the alignment of the consequences so that a unique result of core damage can be quantified. The detection and fire suppression Event Trees in the reference model were replaced by detection and fire extinction Fault trees. The frequency of each Fire Case of the conversion model and the reference model are quantified and the frequencies compared. The results shows that 90% of the cases are valid, however, the rest have challenges with MCS. A unique CDF of 7.65x10-7 is quantified compared with 9.83×10-6 of the reference. The conversion of the new model in CAFTA was not successful due to software incompatibility.

CHAPTER ONE

1.0 INTRODUCTION

1.1 BACKGROUND

Radiation and radioactive substances have many beneficial application ranging from Power generation to uses in medicine, industry and agriculture. Nuclear technology involves the reactions of atomic nuclei releasing energy and particles. Among the notable nuclear technologies are nuclear reactors, nuclear medicine, and nuclear Agriculture. Nuclear technology uses the energy released by splitting the atoms of certain elements. It was first developed in the 1940s, and during the Second World War to 1945 research initially focused on producing bombs by splitting the atoms of particular isotopes of either uranium or plutonium. In the 1950s attention was focused on the peaceful application of nuclear fission, notably for power generation. Today, the world produces as much electricity from nuclear energy as it did from all sources combined in the early years of nuclear power. Civil nuclear power can now boast over 16,500 reactor years of experience and supplies almost 11.5% of global electricity needs**,** from reactors in 31 countries [1]

The radiation risks that may arise from these applications to workers and the public and the environment have to be assessed and, if necessary controlled. It is generally recognized that facilities and activities dealing with radioactive materials provide many benefits but at the same time give rise to radiation risks and deleterious effects. The objective of nuclear safety is to ensure that nuclear facilities operate normally and without an excessive risk of the operating staff and the environment and prevent incidents and if they occur limit the consequences of those incidents. The overall goal of nuclear safety is to protect man and his environment by limiting the release, under any circumstances, of radioactive materials that the facility contains. Thus, ensuring the containment of the radioactive materials. The Safety Fundamentals, Fundamental Safety Principles [**2],** establish principles to ensure the protection of workers, the public and the environment, now and in the future, from the harmful effects of ionizing radiation. These principles emphasize the need to assess and control the inherent risk. Principle 5 on optimization of protection **[2**] states:

- ✓ The safety measures that are applied to facilities and activities that give rise to radiation risks are considered optimized if they provide the highest level of safety that can reasonably be achieved throughout the lifetime of the facility or activity, without unduly limiting its utilization

- ✓ "To determine whether radiation risks are as low as reasonably achievable, all such risks, whether arising from normal operations or from abnormal or accident conditions, must be assessed (using a graded approach) a priori and periodically reassessed throughout the lifetime of facilities and activities."

The optimization of protection also means using good practices and common sense to avoid radiation risks as far as is practical in day to day activities.

The engineering of nuclear facilities are designed so that the risk associated with their operation are within acceptable limits for the public and environment. There is no precise definition, however, of what constitutes an "acceptable risk"; it is basically a subjective notion. In its simplest form, risk is a possibility of loss or injury or denotes the level of uncertainty associated with an individual's given action. The acceptance of risk is generally governed by the degree to which it is considered to be relatively improbable and of limited consequence.

When one is really asking these three questions: "What can go wrong?" "How likely is it?" and "What are the consequences?" These three questions can be referred to as the "risk triplet." The traditional definition of risk, that is, probability times consequences, is fully embraced by the "triplet" definition of risk. A combination of events and/or conditions that could occur or a set of scenarios usually answers the question "What can go wrong?" The second question, "How likely is it?" can be answered in terms of the available evidence and the processing of that evidence to quantify the probability and the uncertainties involved. In some situations, data may exist on the frequency of a particular type of occurrence or failure mode (e.g., accidental overexposures). In other situations, there may be little or no data (e.g., core damage in a reactor) and a predictive approach for analyzing probability and uncertainty will be required. The third question, "What are the consequences?" can be answered for each scenario by assessing the probable range of outcomes (e.g., dose to the public) given the uncertainties. The outcomes or consequences are the "end states" of the analyses. The choice of consequence measures can be whatever seems appropriate for reasonable decision-making in a particular regulated activity and could involve combinations of end states. A risk assessment is a systematic method for addressing the risk triplet as it relates to the performance of a particular system (which may include a human component) to understand likely outcomes, sensitivities, areas of importance, system interactions and areas of uncertainty. From this assessment the important scenarios can be identified.

Safety analyses are analytical evaluations of physical phenomena occurring at nuclear power plants, made for the purpose of demonstrating that safety requirements, such as the requirement for ensuring the integrity of barriers against the release of radioactive material and various other acceptance criteria, are met for all postulated initiating events that could occur over a broad range of operational states, including different levels of availability of the safety systems. A quantitative examination of how the behavior of a system varies with alteration, usually in the values of the governing parameters. Two main types of safety assessment has been identified as deterministic safety (risk) assessment and probabilistic safety (risk) assessment. Analysis is often used interchangeably with assessment, especially in more specific terms such as ‘safety analyses. In general, however, analysis suggests the process and result of a study aimed at understanding the subject of the analysis, while assessment may also include determinations or judgments of acceptability. Analysis is also often associated with the use of a specific technique. Hence, one or more forms of analysis may be used in assessment. The formal safety analysis is part of the overall safety assessment; i.e. it is part of the systematic process that is carried out throughout the design process (and throughout the lifetime of the facility or the activity) to ensure that all the relevant safety requirements are met by the proposed (or actual) design. The important distinction is that safety analysis should be used as a documented process for the study of safety, and safety assessment should be used as a documented process for the evaluation of safety [3].

The deterministic safety assessment is an analytical procedure widely used throughout the world in the design of nuclear reactors for the purpose of generating electricity. The purpose is to ensure that the various situations, and in particular accidents, that are considered to be plausible, have been taken into account, and that the monitoring systems and engineered safety and safeguard systems will be capable of ensuring the containment of radioactive materials.

The deterministic approach is based on the two principles referred to as: leaktight barriers and the concept of defense-in-depth. Defense-in-depth consists of taking into account potential equipment failures and human errors, so that suitable preventive measures may be applied, and of making provisions for the installation of successive devices to counter such failures and limit their consequences. It consists of several successive stages (or levels), hence the term "defense-in-depth´´ and includes prevention and surveillance; protection; safeguards; and ultimate measures.

Prevention and surveillance includes all necessary measures taken to ensure that the plant is safe; items of equipment are designed with adequate safety margins and constructed in such a way that under normal operating conditions the risk of an accident occurring in the plant is kept to a minimum. Protection involves the assumption that operating incidents may occur; provisions are made to detect such incidents and to prevent them from escalating. This is achieved by designing safety systems that will restore the plant to a normal state and maintain it under safe conditions. Safeguard is presuppose that severe accidents might occur that could have serious consequences for the public and the environment. Special safety systems are therefore designed to limit the consequences to an acceptable level. Some countries make provision for a fourth level of safety consisting of what are known as ultimate measures, designed to provide protection against severe conditions under which defenses at the three levels described above prove inadequate. The fifth level ensures that consequences of significant releases of radioactive materials are mitigated.

Probabilistic Risk Assessment (PRA) is used to estimate risk by computing real numbers to determine what can go wrong, how likely is it, and what are its consequences. Thus, PRA provides insights into the strengths and weaknesses of the design and operation of a nuclear power plant.

Probabilistic safety assessment (PSA) is a comprehensive, structured approach to identifying failure scenarios, constituting a conceptual and mathematical tool for deriving numerical estimates of risk. [4] Three levels of probabilistic safety assessment are generally recognized. [**4]** Level 1 comprises the assessment of failures leading to determination of the frequency of core damage. Level 2 includes the assessment of containment response, leading, together with Level 1 results, to the determination of frequencies of failure of the containment and release to the environment of a given percentage of the reactor core's inventory of radionuclides. Level 3 includes the assessment of off-site consequences, leading, together with the results of Level 2 analysis, to estimates of public risks. 'Living' probabilistic safety assessment is a probabilistic safety assessment that is updated as necessary to reflect the current design and operational features, and is documented in such a way that each aspect of the PSA model can be directly related to existing plant information and plant documentation, or to the analysts' assumptions in the absence of such information.

The development of probabilistic analysis has resulted not only in an increase in the number of assessments carried out, but also and more importantly in expansion of their scope of application. A study published in 1989 by the Organization for Economic Co-operation and Development (OECD) Nuclear Energy Agency [**5]** entitled Probabilistic Safety Assessment in Nuclear Power Plant Management demonstrated the benefits afforded by PSA in the management of safety in nuclear power plants. The conclusions set out in the study were based in particular on the example of one utility that considered the use of PSA to be an integral part of the daily activities of its organization. The report considered that the use of PSA as an instrument of safety management in nuclear power plants offers immediate benefits to those who implement PSA techniques in the design and operation of their plants, and for all those endeavoring to enhance the safety of nuclear power plants. According to the authors, the implementation of PSA will reduce the frequencies of severe incidents and accidents and will thus be of benefit to the nuclear industry as a whole.

The early applications of risk analysis to nuclear power plants, including that presented in the draft report of the Reactor Safety Study (RSS), did not include a quantitative assessment of accidents initiated by major fires. The reason for this omission was twofold: (1) it was judged that fires were not likely to be dominant contributors to risk (RSS final report--USNRC, 1975) and (2) the state of the art in risk analysis had not yet developed an approach to covering fires. The importance of fire as a potential initiator of multiple-system failures took on a new perspective after the cable-tray fire at Browns Ferry in 1975 **[6].**

The historical developments that have characterized the importance of fire safety at nuclear power plants had gone through phenomenal research and development. The focus of this work is to assess these developments and review the assessment strategies and methodology over the years of fire safety at nuclear power plants.

1.2 JUSTIFICATION AND RELEVANCE

In nuclear power plants accidents are not desirable or welcome news under any circumstances. But history has shown that nuclear energy applications have been developed today due to some of the lessons learned from these accidents. For instance, post Chernobyl assessment emphasized the importance of designing reactor systems properly on the drawing board and implementing them correctly and maintenance. The Fukushima accident in Japan has helped to enhance the safety of reactors in the world by adopting new regulatory and safety assessment strategies. In similar measure fire accidents such as the Brown Ferry fire accident, has contributed immensely to fire safety at nuclear power plants in terms of regulations and assessment methods.

There's a cliché that says to know where you're going, you need to know where you've come from. We spend a lot of time looking at trends in culture, but we don't often look at the evolution of safety research. One area in particular that doesn't receive enough attention is the history of workplace safety. This work takes close study of several countries to see how improvements in fire safety at nuclear power plants have changed over time in order to appreciate just how far we've come. In view of that the study of historical review and observations of fire safety in NPP´s cannot be ignored, since lessons learned can push for further development in reactor safety. It will help shed light on the strengths and weaknesses in the fire safety assessment leading to enhance nuclear safety. The same way lessons learned from history can be valuable asset for future development in safety culture and assessment methods.

In recent year, Nuclear Regulatory commission (NRC) of United States published similar research on defense in depth, titled ´´Historical Review and Observations of Defense-in-Depth´´ NUREG/KM-0009 [7]. The observations and conclusions add to the timely importance of this work on fire safety.

1.3 RESEARCH OBJECTIVES

The goal of this thesis is to study and assess fire safety at Nuclear Power Plant (NPP). This will contribute to continuous safe operation and maintenance in a cost effective manner based on risk-informed decisions. The thesis is presented in three parts. The part one is the review of the historical evolution of fire safety in Nuclear Power Plants and make recommendations to embarking countries. The part two is Fire PSA and development of an innovative tool for Fire-related Risk-informed decision making. As a practical quintessential example, feasibility case study of conversion of fire PSA model to fire Risk monitor is considered in the third part.

The objectives of the first and second part of this work are:

1. To review historical fire safety at NPP and provide risk informed grounds for embarking countries to develop their NPP based on the historical analysis;
2. To develop tools to assess the risk induced by fire, as well as, an innovative way to communicative the risk to decision makers;

3. To determine the contribution of the risk increase by the aggregation of fire PSA and Internal Initiating Events PSA;

The main purpose of the third part of the project is to determine the feasibility of converting a fire PSA model to a Fire-related Risk monitor model.

The main objectives of this part are to:

- Determine whether CAFTA® (Risk Monitor quantification software) is capable of converting RiskSpectrum® Fire PSA model files into its own model;
- Identify the problems in the conversion from RiskSpectrum® fire PSA to CAFTA® and propose suitable solution; and
- Validate the conversion model in RiskSpectrum

1.4 SCOPE OF RESEARCH

The historical review of fire safety at NPP was based on documentation and records available to the public in the various countries and the international organizations such as IAEA, WINRA etc. The research is in English language, therefore, documents accessed are mainly from United States of America, Canada, Germany, United Kingdom, India, South Korea and Japan. International Atomic Energy Agency (IAEA) has been source of important documents and information from countries like China, Russia, France and many countries where many of their documentations are not in English. Ease of access to documentations from some of the countries made their choice easier for assessment as well as those with significant reportable fire safety case at the nuclear power plants. Conference papers are also a good source of information from many of the countries and provide valuable information as to the state of development in the fire safety assessment at NPP in those countries. The assessment is based on the recent available documentations and records from the various countries, international relevant organizations and the IAEA. From the above reasons, the review has been restricted to USA, Germany, Japan and International Atomic Energy Agency

A case study of Spanish Westinghouse Pressurized Water Reactor (PWR) fire Probability safety assessment (PSA) model in RiskSpectrum® is used for the feasibility study to convert to fire Risk Monitor. The Risk Monitor EOOS® has CAFTA® as the quantification software, therefore, the fire PSA model in RiskSpectrum® needed to be converted to CAFTA®. The cross platform operation of PSA model has been carried out and being developed, and the use of CAFTA to open RiskSpectrum model will contribute to that development. The challenges with the conversion of the fire PSA model to CAFTA will be addressed as far as possible.

CHAPTER TWO

2.0 SAFETY CONCEPTS IN NUCLEAR POWER PLANTS

2.1 INTRODUCTION

Brief historical review of safety from prehistoric, through the industrial revolution to this century. The basic safety concepts, applications and assessment.

2.1.1 BRIEF HISTORICAL REVIEW

Years of experience, incidents, tragedies, and education have helped evolve how people handle, control, prevent, contain, and provide safe conditions for human habitation. State intervention in man's activities to protect the health of the inhabitants goes back to prehistory. The motivation may not have been altogether altruistic; the king acted to protect his subjects because he regarded them as his property. Public health protection began for disease control. With industrialization, came the need for control of even more hazardous forces and substances. This extended protection became technological in accident analysis and response. Present efforts in controlling risk, such as from nuclear power, are a continuation of this development.

Safety, as it relates to public protection from disease, has a history extending to early history. Ruins in the Indus Valley reveal that as early as 400 B.C., building codes and sanitary engineering were in effect. The Egyptians from the middle kingdom (approximately 2000 B.C.) had bathroom and sewage facilities, as did the Incas. The Greeks formulated principles of hygiene and attempted to show a causal relationship between environmental factors and disease. Indeed, the basic text on epidemiology for 2,000 years was "Air, Waters, and Places" from the Hippocratic collection. The Romans perceived a relationship between swamps and malaria and drained many swamps. They also devised dust respirators for workers, built sewage systems, public baths and great aqueducts. Officials were empowered to destroy impure foodstuffs and regulate public baths, brothels and burial grounds. Justinian I of Byzantine, to combat one of the worst plagues in history (532 A.D.), set up quarantine posts and required certificates of health for admission to Constantinople **[5].**

While health care declined after the fall of the Roman Empire, England used the common-law concept of public nuisance to protect the public from flagrant cases of polluting the waters. In France, Germany, and Italy, tanners were prohibited from washing skins in the water supply. London, from 1309, had ordinances regulating cesspools and sewers. The Florentines forbade the sale of meat on Monday that had been slaughtered on Friday.

Houses in medieval England were usually built of timber frames filled in with wattle and daub; the roofs were thatched and chimneys as such did not exist. Within the congested walled towns the houses were built in narrow streets with over hanging upper storeys. With houses having a central hearth and straw as the floor covering a fire spread could spread very easily. William the Conqueror required all fires to be extinguished at night. The most popular method of achieving this was to use a metal cover that was put over the fire to exclude the air. This cover was called a Covert Feu which in use became Curfew.

National health legislation came into being in the 19th century primarily in the form of laws that governed the conditions of child labor and eventually prohibited it. In Germany, medical police were organized to make and enforce health and safety regulations. Both France and Germany became committed to the proposition that government had a positive duty to provide for the health, safety and welfare of workers and citizens.

The coming of industrialization intensified existing problems and created new ones. With the Clearances in England, came migration of farm labor to the cities as well as improvements in agricultural productivity to support the increasing urban population and consequent increase in communicable diseases. Smallpox was the most widespread disease in the 18th century. Peak years in London occurred between 1723 and 1796, with a periodicity of about five years. Each outbreak took over three thousand lives. In the 1740s, 75 % of London's infants died before the age of five.

The diseases of typhus and scarlet fever were also major contributors. Victorian England led the world to better health by actions improving nutrition and working conditions. The Public Health Act of 1848, established Local Boards of Health specifying educational levels of the district health officers and empowering them to enforce sanitation requirements.

The first recorded attempt to legislate for fire safety. The Mayor of London laid down that houses in the city were to be built of stone, thatched roofs were not permitted, and party walls were to be of minimum height and thickness and during summer months a tub of water was to be made available in case of fire.

2.1.2 INDUSTRIAL REVOLUTION

The other effects on safety brought by industrialization resulted from new and more powerful energy sources. Although water and wind power was used in the Middle Ages, these forces were "natural" and believed to be understood. However, the steam engine was something new. The original condensation engine was sub-atmospheric, but with Watt's invention and Carnot's theory, the quest for higher steam pressure and temperature began.

The original steam generators were simple pressure vessels that were prone to catastrophic failures and loss of life. Due to better boiler design, tube-fired boilers, and boiler inspections, the incidence of catastrophic failure is now to a rare event (about once every 100,000 vessel-years). In Great Britain in 1866, there were 74 steam boiler explosions causing 77 deaths. This was reduced to 17 explosions and 8 deaths in 1900 as a result of inspections performed by the Manchester Steam User Association. In the United States, the American Society of Mechanical Engineers established the ASME Pressure Vessel Codes with comparable reductions.

The development of steam and later the internal combustion engine made possible transportation by rail, road and air at speeds never before experienced. In all cases, the regulations, inspections, and design standards were imposed after the hazards had been exhibited by many deaths and injuries. Nuclear power has attempted, rather successfully, to anticipate the risks before they occur and avoid them through design, control and regulation. PSA is an essential analytical tool for accomplishing this result.

As regards factories, the Factories Act 1937 considerably extended the requirements as to means of escape originally contained in the Factory and Workshop Act 1901 under which District Councils had been given powers in respect of premises where more than 40 persons were employed. Following a fire in February 1956 at the Eastwood Mills, Keighley, in which eight people died, the whole question of providing fire alarms and adequate means of escape was reviewed by the Factory Inspectorate and a survey of 40,000 to 50,000 premises was carried out. The 1961 Factories Act consolidated the fire provisions contained in the Factories Acts of 1937, 1948 and 1959 - the last of which had placed the responsibility for certifying means of escape on the Fire Authority and not the District Council as provided for earlier.

2.1.3 THIS CENTURY

The discovery of nuclear fission made possible a far more concentrated energy source than ever before. Its hazards were recognized from the beginning, and for the first time, a commitment by government, to safely bring a technology on line without the deadly learning experiences that occurred to safely use earlier technologies. During World War II, experience was acquired in the operation of plutonium production and experimental reactors. Shortly after passage of the Atomic Energy Act of 1948, the Reactor Safeguards Committee was formed (1947) which was to merge with the Industrial Committee on Reactor Location Problems (1951) to become the ACRS (Advisory Committee on Reactor Safeguards). The Atomic Energy Act of 1954 made industrial nuclear power possible, and the first plant began operation at Shippingport, PA, in 1957. The risk posed by a nuclear power plant at this time was unknown, hence the Price-Anderson Act was passed to limit the financial risk.

The first report on nuclear power plant accidents, WASH-740 **[8]** was issued by Brookhaven National Laboratory (1957). The consequences predicted were unacceptable, but it was believed that the probability of such an accident was very small. This report and the technically untenable Maximum Credible Accident method in licensing gave rise, during the 1960s, to probabilistic approaches to siting (Farmer, 1967; Otway and Erdmann, 1970) and to accident analysis (Garrick et al., 1967; Salvatori, 1970; Brunot, 1970; Otway et al., 1970; Crosetti, 1971; and Vesely, 1971). The most ambitious of the pre-Reactor Safety Studies was Mulvihill, 1966, which consisted of a fault tree probability analysis followed by consequence analysis of the postulated accidents at a nuclear power plant.

2.2 REACTOR SAFETY STUDY

A letter from Senator Pastore to James Schlesinger, Atomic Energy Commission (AEC) Chairman, requesting risk information for the Price-Anderson renewal, sparked the beginning of the Reactor Safety Study (RSS) directed by Professor Norman Rasmussen of MIT. The RSS study began in September 1972 with Saul Levine, full-time staff director assisted by John Bewick and Thomas Murley (all AEC).

The use of event trees to link the system fault trees to the accident initiators and the core damage states was significant development of the study. This was a response to the difficulties encountered in performing the in-plant analysis by fault trees alone. Nathan Villalva and Winston Little proposed the application of decision trees, which was recognized by Saul Levine as providing the structure needed to link accident sequences to equipment failure.

The Reactor Safety Study was the most important development in PSA because it:

- Established a pattern for performing a PSA of a nuclear plant;

- Provided a basis for comparison;
- Identified transients and small LOCAs as the major risk contributors, rather than the previous emphasis on a large LOCAs;
- Showed that the radiological risk of a nuclear power plant is small compared with other societal risks;
- Originated the event tree for linking initiators, systems, and consequences, and introduced the fault tree to a large audience;
- Compiled a database;
- Showed that human error is a major contributor;
- Showed the impact of test and maintenance; and
- Showed the importance of common mode interactions.

The work was published as draft WASH-1400 in August 1974 and extensively reviewed. The revised report was published as WASH-1400 (FINAL) in October 1975[6]

Following the release of WASH-1400, the techniques were disseminated by the authors and interpreters through publications, lectures, and workshops. Many organizations set up in-house PSA groups, and the nucleus of the organization that had produced the Reactor Safety Study continued at the NRC.

2.3 SAFETY GOALS

The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation [2]. This applies to all facilities and activities, and for all stages over the lifetime of a facility or radiation source, including planning, siting, design, manufacturing, construction, commissioning and operation, as well as decommissioning, transport of radioactive material, management of radioactive waste and closure. This fundamental safety objective of protecting people — individually and collectively — and the environment has to be achieved without unduly limiting the operation of facilities or the conduct of activities that give rise to radiation risks. To ensure that facilities are operated and activities conducted so as to achieve the highest standards of safety that can reasonably be achieved, measures have to be taken:

(a) To control the radiation exposure of people and the release of radioactive material to the environment;

(b) To restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation;
(c) To mitigate the consequences of such events if they were to occur.

To achieve these fundamental safety objectives ten safety principles have been formulated, on the basis of which safety requirements are developed and safety measures are to be implemented.

2.3.1 SAFETY PRINCIPLES

The safety principles includes responsibility for safety, the role of governments, leadership and management for safety, justification of facilities and activities, optimization of protection, limitation of risks to individuals, protection of present and future generations, prevention of accidents, as well as emergency preparedness and response, and Protective actions to reduce existing or unregulated radiation risks.

The prime responsibility for safety must rest with the person or organization responsible for facilities and activities that give rise to radiation risks called licensee. The licensee retains the prime responsibility for safety throughout the lifetime of facilities and activities, and this responsibility cannot be delegated. This includes establishing and maintaining the necessary competences; Providing adequate training and information; as well as Establishing procedures and arrangements to maintain safety under all conditions.

The verification of appropriate design and the adequate quality of facilities and activities and of their associated equipment are the responsibility of the licensee. However, other groups, such as designers, manufacturers and constructors, employers, contractors, and consignors and carriers, also have legal, professional or functional responsibilities with regard to safety.

Safety control, storage, and transportation of radioactive material used or waste generated are the responsibility of the licensee. Provision must also be made for the continuity of responsibilities and the fulfilment of funding requirements in the long term, since radioactive waste management can span many human generations. Therefore, consideration must be given to the fulfilment of the licensee’s (and regulator’s) responsibilities in relation to present and likely future operations.

Governments must established and sustained an effective legal and governmental framework for safety, including an independent regulatory body. Governments and regulatory bodies thus have an important responsibility in establishing standards and establishing the regulatory framework for protecting people and the environment against radiation risks. However, the prime responsibility for safety rests with the licensee. In the event that the licensee is a branch of government, this branch must be clearly identified as distinct from and effectively independent of the branches of government with responsibilities for regulatory functions.

The regulatory body must have adequate legal authority, technical and managerial competence, and human and financial resources to fulfil its responsibilities. The regulatory body must be effectively independent of the licensee and of any other body, so that it is free from any undue pressure from interested parties; and demonstrate openness and transparent community involvement and/or stakeholders.

Effective leadership and management for safety must be established and sustained in organizations concerned with, and facilities and activities that give rise to, radiation risks. The administration at the highest levels in the organization has to demonstrate Leadership in safety matters. Safety has to be achieved and maintained by means of an effective management system. This system has to integrate all elements of management so that requirements for safety are established and applied coherently with other requirements, including those for human performance, quality and security, and so that safety is not compromised by other requirements or demands. The management system also has to ensure the promotion of a safety culture, the regular assessment of safety performance and the application of lessons learned from experience.

Governance of attitudes and behaviour in relation to safety of all organizations and individuals concerned must be integrated in safety culture and the management system. Safety culture includes: — Individual and collective commitment to safety on the part of the leadership, the management and personnel at all levels;
— Accountability of organizations and of individuals at all levels for safety;
— Measures to encourage a questioning and learning attitude and to discourage complacency with regard to safety.

An important factor in a management system is the recognition of the entire range of interactions of individuals at all levels with technology and with organizations. To prevent human and organizational failures, human factors have to be taken into account and good performance and good practices have to be supported.

Safety has to be assessed for all facilities and activities, consistent with a graded approach. Safety assessment involves the systematic analysis of normal operation and its effects, of the ways in which failures might occur and of the consequences of such failures. Safety assessments cover the safety measures necessary to control the hazard, and the design and engineered safety features are assessed to demonstrate that they fulfil the safety functions required of them. Where control measures or operator actions are called on to maintain safety, an initial safety assessment has to be carried out to demonstrate that the arrangements made are robust and that they can be relied on. A facility may only be constructed and commissioned or an activity may only be commenced once it has been demonstrated to the satisfaction of the regulatory body that the proposed safety measures are adequate.

Despite all measures taken, accidents may occur. The precursors to accidents have to be identified and analyzed, and measures have to be taken to prevent the recurrence of accidents. The feedback of operating experience from facilities and activities — and, where relevant, from elsewhere — is a key means of enhancing safety. Processes must be put in place for the feedback and analysis of operating experience, including initiating events, accident precursors, near misses, accidents and unauthorized acts, so that lessons may be learned, shared and acted upon. It is based on these principles that this work is undertaken so that safety will be assured at all times.

Facilities and activities that give rise to radiation risks must yield an overall benefit. The justification for facilities and activities to be considered to beneficial, then, the yield must outweigh the radiation risk to which they give rise. All the significant consequences of the operation of facilities and the conduct of activities have to be taken into account prior to assessing benefits and risk

Protection must be optimized to provide the highest level of safety that can reasonably be achieved. To determine whether radiation risks are as low as reasonably achievable, all such risks, whether arising from normal operations or from abnormal or accident conditions, must be assessed (using a graded approach) a priori and periodically reassessed throughout the lifetime of facilities and activities. Where there are interdependences between related actions or between their associated risks (e.g. for different stages of the lifetime of facilities and operation), must be identified, recognized, controlled and mitigated.

Measures for controlling radiation risks must ensure that no individual bears an unacceptable risk of harm. Justification and optimization of protection do not in themselves guarantee that no individual bears an unacceptable risk of harm. Consequently, doses and radiation risks must be controlled within specified limits. Conversely, because dose limits and risk limits represent a legal upper bound of acceptability, they are insufficient in themselves to ensure the best achievable protection under the circumstances, and they therefore have to be supplemented by the optimization of protection. Thus both the optimization of protection and the limitation of doses and risks to individuals are necessary to achieve the desired level of safety

People and the environment, present and future, must be protected against radiation risks. The application of safety standards should not be applied to only local population but also to populations remote from the facility or future population to come. This is because radiations risks may transcend national borders or generations to come and may persist for long periods of time. Thus where effects of radiation risk could span generations, the subsequent generations have to be adequately protected. Without any need for the future generations to take significant protective actions, radioactive waste must be managed in such a way to avoid imposing an undue burden on future generations.

All practical efforts must be made to prevent and mitigate nuclear or radiation accidents. When control of nuclear chain reactions fails as a result of occurrences of failures or abnormal conditions, the likelihood of harmful consequences and the failures needed to be controlled.

The primary means of preventing and mitigating the consequences of accidents is ‘defence in depth. Defence in depth is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment. The principle of defense-in-depth is implemented primarily by means of a series of barriers which would in principle never be jeopardized, and which must be violated in turn before harm can occur to people or the environment. Thus, if one level of protection or barrier were to fail, the subsequent level or barrier would be available. The independent effectiveness of the different levels of defense is a necessary element of defense in depth. The appropriate combination of effective management system and a strong safety culture, adequate site selection and the incorporation of good design and engineering features, provides defense in depth. It is enhanced by providing safety margins, diversity and redundancy, mainly by the use of design, technology and materials of high quality and reliability; Control, limiting and protection systems and surveillance features.

Arrangements must be made for emergency preparedness and response for nuclear or radiation incidents. All practical efforts to prevent and mitigate nuclear accident has also the element of likelihood of failure, therefore emergency preparedness and response plan must to be put in place to ensure that safety is assured at all times. The primary goals of preparedness and response for a nuclear or radiation emergency are:

- To ensure that arrangements are in place for an effective response at the scene and, as appropriate, at the local, regional, national and international levels, to a nuclear or radiation emergency;
- To ensure that, for reasonably foreseeable incidents, radiation risks would be minor;
- For any incidents that do occur, to take practical measures to mitigate any consequences for human life and health and the environment

The emergency response arrangements, consideration is given to all reasonably foreseeable events. Emergency plans is exercised periodically to ensure the preparedness of the organizations having responsibilities in emergency response

Lastly, Protective actions to reduce existing or unregulated radiation risks must be justified and optimized.

2.4 DEFENSE IN DEPTH

The idea of defense-in-depth originated as a military strategy, early in history, as a concept to delay the advance of the opponent by relying on multiple, layered lines of defense instead of a single strong defensive line. The applications of this idea of defense-in-depth has widely been used for non-military purposes to describe multi-layered, as well as diverse and redundant, protections, both tactical and strategic. Defense-in-depth may mean redundancy or diversity in design; that is, designing a system to remain functional although a component in the system has failed, versus trying to design components that do not fail. This concept of defense-in-depth, protection against a single failure, is engrained in the nuclear industry. In nuclear safety, defense-in-depth denotes the practice of having multiple, redundant, and independent layers of safety systems or physical barriers to protect against the occurrence, as well as the consequences, of an accident. The aim is to reduce the risk to the public from a radiological accident.

The concept of defense-in-depth appears frequently in nuclear history dating back to 1957 and WASH 740 (´´Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants") **[8]** In that document, defense-in-depth is described as: "... criteria ... that ... will require multiple lines of defense against accidents which might release fission products from the facility" and "... no hazard to the safety of the public would occur unless two additional lines of defense were also breached."

Defense-in-depth, according to NUREG/KM-0009**[7]**., has been described, discussed, and defined extensively over the years in various U.S. Nuclear Regulatory Commission's (NRC) documents including Title 10 of the Code of Federal Regulations(10CFR), NUREG reports, SECY papers, regulatory guides, Commission policy statement, Advisory Committee on Reactor Safeguards (ACRS) letters, etc. It has been at the core of the NRC's safety philosophy, and remains fundamental to the safety and security expectations of NRC's regulatory structure. Over the years, however, defense-in-depth, in the various references, has not been described, discussed or defined consistently. This is not surprising, since different authors have invoked the defense-in-depth concept in ways that best suit the particular purpose of their document.

In the NRC Strategic Plan [**9**] defense-in-depth is defined as: "... an element of the NRC's safety philosophy that employs successive compensatory measures to prevent accidents or lessen the effects of damage if a malfunction or accident occurs at a nuclear facility. The NRC's safety philosophy ensures that the public is adequately protected and that emergency plans surrounding a nuclear facility are well conceived and will work. Moreover, the philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility."

In the glossary on the NRC Website, defense-in-depth is defined as: "... an approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials. The key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defense-in-depth includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures**."[10]**

Defense-in-depth is an approach to developing and maintaining a regulatory structure comprised of multiple layers of defense that include the necessary protective features to ensure that the risk to the public is maintained acceptably low. This structure is based on layers of defense that both prevent the occurrence of adverse events and mitigate the consequences if the events were to occur. The central feature of defense in depth in relation to nuclear power plants are all safety activities; whether organizational, behavioral or equipment related, which are subject to layers of overlapping provisions, so that if a failure should occur it would be compensated for or corrected without causing harm to individuals or the public at large.

Defense-in-depth is needed to address the uncertainties in the design, construction, maintenance and operation of the nuclear facility. The general recognition is that defense-in-depth is needed to compensate for uncertainties; uncertainties regarding, for example,

- the basic design and operation of the "facility"
- knowledge in the performance of support system and components (SSCs) and operator actions under various facility conditions
- Various phenomena, etc.
- the "unknown" (i.e., unknowns events and phenomena that are unanticipated because of lack of knowledge and therefore may not be addressed in the design or operation of the facility)

2.4.1 OBJECTIVES OF DEFENCE IN DEPTH

The objective of defense-in-depth is to avert damage to the plant thereby ensuring the protection of public health and safety while maintaining an acceptably low probability of accidents and mitigation of accidents. In reviewing the various literature sources regarding the objective of defense-in-depth, the following statements are found:

- to compensate for potential human and component failures;
- to maintain the effectiveness of the barriers by averting damage to the facility and to the barriers themselves; and
- To protect the public and the environment from harm in the event that these barriers are not fully effective.

- To achieve an adequate level of safety for nuclear power plants is generally recognized to require defense-in-depth.
- The prevention of exposure of people to this radioactivity ... can be achieved ... by the use of the concept of defense-in-depth.
- [To ensure that] the probability of an accident occurring is very small.
- To protect the plant, the plant operators, and the health and safety of the public by application of a ‘defense-in-depth” design philosophy.
- Defense-in-depth concept associated with its accident prevention and mitigation philosophy.
- Defense-in-depth approach ... to ensure the protection of public health and safety.
- A defense-in-depth approach ... to prevent accident ... and to mitigate their consequences.
- To prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs.
- Incorporating defense-in-depth ... is that the facility ... tends to be more tolerant of failures and external challenges.
- To increase the degree of confidence in the results of the probabilistic risk assessment (PRA) or other analyses supporting the conclusion that adequate safety has been achieved.
- The probability of accidents must be acceptably low.
- To identify, prevent or mitigate accidents.
- Providing design feature to achieve acceptable risk.
- Be developed that establishes an approach ... [that provides for] ... balance between prevention and mitigation.
- Defense-in-depth principles that the design provides accident prevention and mitigation capability.
- An approach ... that prevents and mitigates accidents.

2.4.2 STRATEGY FOR DEFENCE IN DEPTH

The strategy for defense in depth is twofold: first, to prevent accidents and, second, if prevention fails, to limit their potential consequences and prevent any evolution to more serious conditions. Accident prevention is the first priority. From literature and historical perspective levels of defense-in-depth has been described. The idea of multiple layers or barriers is recognized, from two layers i.e. Prevent accidents and limit the consequence and prevent the evolution to more serious conditions, to four layers and five layers. The four layers structure proposal includes:

1. Prevention of accidents, protective systems to take corrective actions, and engineered safety features to mitigate the consequences.

2. Prevent initiation of incidents, capability to detect and terminate incidents, and protecting the public.

3. Protections to prevent accidents from occurring, mitigation of accidents if they occur, and emergency preparedness to minimize the public health consequences of releases if they occur.

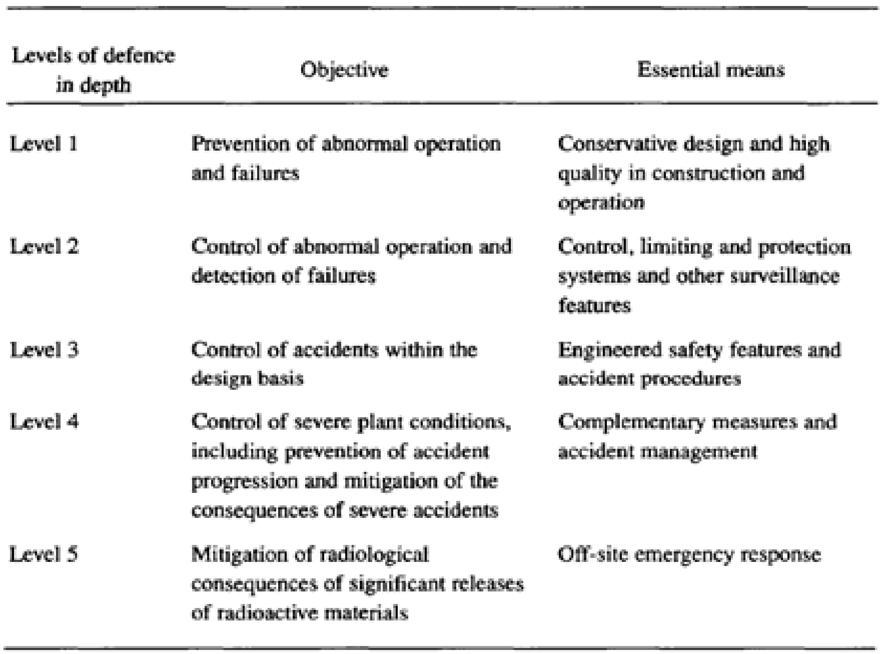
4. Superior quality in design, construction and operation, accident prevention safety systems, and consequences-limiting safety systems.

These four different descriptions of the layers of defense are similar in concept, some are just more specific in identifying how to accomplish the layer while others are more functional in what needs to be accomplished by the layer.

According to IAEA INSAG-10 **[11]**, Defense in depth is generally structured in five levels and the failure of one level, the subsequent level comes into play. The five levels, the objective and the essential means of achieving it are shown in the Table 1.1 below.

The objective of the first level of protection is the prevention of abnormal operation and system failures. If the first level fails, abnormal operation is controlled or failures are detected by the second level of protection. Should the second level fail, the third level ensures that safety functions are further performed by activating specific safety systems and other safety features. Should the third level fail, the fourth level limits accident progression through accident management, so as to prevent or mitigate severe accident conditions with external releases of radioactive materials. The last objective (fifth level of protection) is the mitigation of the radiological consequences of significant external releases through the off-site emergency response.

TABLE I.1 LEVELS OF DEFENCE IN DEPTH



Levels of defence in depth	Objective	Essential means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

Hazards such as fire, flooding or earthquakes could potentially impair several levels of defense (for example, they could bring about accident situations and, at the same time, inhibit the means of coping with such situations). Special attention is paid to such hazards, precautions are taken against them, and the plant and its safety systems are designed to cope with them. For example, protection against fire requires prevention of fires, detection of fires and the limitation of consequences by the design of fire zones and physical separation for the redundant lines of safety systems.

2.4.3 CRITERIA DETERMINING DEFENSE-IN-DEPTH

The adequacy of Defense-In-Depth (DID) can be achieved by the insights obtained through risk quantification of the elements of DID with extent practicable. The adequacy are reflected in the risk insights gained through identification of the individual performance of each defense system in relation to overall performance. It should ensure a proper balance between accident prevention and accident mitigation and the mean frequency of containment failure in the event of a severe core damage accident should be less than 1 in 100 of severe core damage accident. After conservatism consideration of the uncertainties under the adequacy of DID, severe core damage accident should not be expected on average to occur, and as well as containment performance such that severe accident are not expected to occur, as the goal for offsite consequences are expected to be met.

The rationalist approach to DID adequacy is:

- Establish quantitative acceptance criteria, such as the quantitative health objectives, core damage frequency and early large release frequency
- Analyze the system using PRA methods to establish that acceptance criteria are met
- Evaluate the uncertainty in the analysis especially those due to mode incompleteness, and determine what steps should be taken to compensate for those uncertainties

The DID adequacy is assured if the overall redundancy and diversity among the plant's systems and barriers is sufficient to ensure that risk acceptance criteria is met.

From the literature, the various recommendations for determining adequacy of defense-in-depth all use risk as the main criteria. The various guidelines propose that the elements (e.g., layers of defense) should be quantified, that risk is used to access each defense system (e.g., safety measure), that compensatory measures can be graded in order to reduce risk, that any sequence (given that all defense layers have failed) remain under a frequency consequence curve, that redundancy and diversity is sufficient to ensure risk guidelines are met, and that assessing the adequacy via a process that uses a PRA is implemented.

2.5 NUCLEAR SAFETY CULTURE

2.5.1 INTRODUCTION

Except for natural disaster any problems arising at nuclear plant originate in some way in human error. Yet the detection and elimination of potential safety bleach is effectively accomplished by human mind. For these reasons, individuals shoulder heavy responsibility beyond adherence to defined procedures. They must act in accordance with safety responsibility and develop safety culture as to prevent human error and to benefit from the positive aspects of human action. The positive human actions are influenced by culture.

"Culture…is that complex whole which includes knowledge, belief, art, morals, law, custom, and any other capabilities and habits acquired by man as a member of society." Culture is more or less the consistent patterns of thinking, feeling and behavior and these are observable in myths, symbols and artifacts. The culture focus on social structures and institutions introduce concepts of roles, status, norms, and values. [12]

However, at organizational level the culture focus on human performance in the work environment where different levels of analysis with individual differences, inter- and intra- group interactions, leadership (and management), organizational/corporate behavior and external influences. Therefore, organizational culture is a pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way you perceive, think, and feel in relation to those problems. Issues related to situational constraints and people's actual behavior have tended to be ignored.

Over the years watershed events have influenced the safety culture at commercial nuclear power plants. The Three Mile Island nuclear power plant accident was the first industry event in 1979. The event was fundamentally contributed by many challenges involving hardware, procedures, training and attitudes towards safety and regulation. In 1975, Brown Ferry nuclear power plant fire incident was a stark reminder of the hazards of internal fires to nuclear safety and attitudes towards fire safety assessment. Similarly, in 1986 Chernobyl accident highlighted the importance of properly maintaining design configuration, plant status control, line of authority for reactor safety and cultural attributes related to safety. Year 2002 discovery of degradation of the Davis-Besse nuclear power plant vessel head highlighted problems that develop when the envelopment at a plant receives insufficient attention. Most recently, the 2011 Fukushima Daiichi nuclear power plant illustrates the importance of command and control, training and resources availability for such accidents.

A theme common in these events is that problems crept in over time, often related to or a direct result of the plant culture. Had these problems been recognized, challenged and resolved, the events could have been prevented or their severity mitigated. The series of decisions and actions that resulted in these events can usually be traced to the shared assumptions, values and beliefs of the organization.

2.5.2 DEFINITION OF SAFETY CULTURE

Definitions of safety culture abound, but they variously refer to the safety-related values, attitudes, beliefs, risk perceptions and behaviors of all employees. An illustration is shown by the definitions shown below. Safety culture is defined according to NSAG-4 1991 as ´´The assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, protection and safety issues receive the attention warranted by their significance´´ **[12]**

In INSAG-3 **[13]** it was stated that Safety Culture "refers to the personal dedication and accountability of all individuals engaged in any activity which has a bearing on the safety of nuclear power plants". It was further stated to include as a key element "an all pervading safety thinking", which allows "an inherently questioning attitude, the prevention of complacency, a commitment to excellence, and the fostering of both personal accountability and corporate self-regulation in safety matters". [13]

According to the Advisory Committee on the Safety of Nuclear Installations (ACSNI) ´´The safety culture of an organization is the product of individual and group values, attitudes, perceptions, competencies and patterns of behavior that determine the commitment to and the style and proficiency of an organization's health and safety management. Organizations with a positive safety culture are characterized by communications founded on mutual trust, by shared perceptions of the importance of safety and by confidence in the efficacy of preventive measures´´. [14].

The object of safety culture is the means by which explicit attention to safety is achieved for both the organization and individuals. The manifestations of safety culture are extensive, complex and intangible, therefore, any attempt to capture the essence of it in any definition are bound to be inadequate.

2.5.3 FEATURES OF SAFETY CULTURE

The elements of safety culture for organizations and for individual in all types of activities includes;

- individual awareness of the importance of safety;
- knowledge and competence, conferred by training and instruction of personnel and by their self-education;

- Commitment, requiring demonstration at senior management level of the high priority of safety and adoption by individuals of the common goal of safety.
- Motivation, through leadership, the setting of objectives and systems of rewards and sanctions, and through individuals' self-generated attitudes.
- Supervision, including audit and review practices, with readiness to respond to individuals' questioning attitudes.
- Responsibility, through formal assignment and description of duties and their understanding by individuals.

Safety Culture has two major components: the organizational policy and managerial action, and the individual’s response in working within and benefiting by the framework. Success depends, however, on commitment and competence, provided both in the policy and managerial context and by individuals themselves.

2.5-4 TRAITS OF A POSITIVE NUCLEAR SAFETY CULTURE

Experience has shown that certain personal and organizational traits are present in a positive safety culture. The following are traits of a positive safety culture:

- Leadership Safety Values and Actions—Leaders demonstrate a commitment to safety in their decisions and behaviors.

- Problem Identification and Resolution—Issues potentially impacting safety are promptly identified, fully evaluated, and promptly addressed and corrected commensurate with their significance.

- Personal Accountability—all individuals take personal responsibility for safety.

- Work Processes—the process of planning and controlling work activities is implemented so that safety is maintained.

- Continuous Learning—Opportunities to learn about ways to ensure safety are sought out and implemented.

- Environment for Raising Concerns—a safety conscious work environment is maintained where personnel feel free to raise safety concerns without fear of retaliation, intimidation, harassment, or discrimination.

- Effective Safety Communication—Communications maintain a focus on safety.
- Respectful Work Environment—Trust and respect permeate the organization.
- Questioning Attitude—Individuals avoid complacency and continuously challenge existing conditions and activities in order to identify discrepancies that might result in error or inappropriate action.

Nuclear safety is a collective responsibility. The concept of nuclear safety culture applies to every employee in the nuclear organization, from the board of directors to the individual contributor. No one in the organization is exempt from the obligation to ensure nuclear safety is the highest priority.

The performance of individuals and organizations can be monitored and trended; therefore, performance may serve as an indicator of the health of an organization's safety culture. However, the health of an organization's safety culture could lie anywhere along a broad continuum, depending on the degree to which the attributes of safety culture are embraced. Even though safety culture is somewhat of an intangible concept, it is possible to determine whether a station tends toward one end of the continuum or the other.

2.6 NUCLEAR SAFETY ASSESSMENT

The Fundamental Safety Principles **[2]**, establishes principles for ensuring the protection of workers, the public and the environment, now and in the future, from harmful effects of ionizing radiation. These principles apply to all situations involving exposure to, or the potential for exposure to, ionizing radiation

Safety assessments are to be undertaken as a means of evaluating compliance with safety requirements (and thereby the application of the fundamental safety principles) for all facilities and activities and to determine the measures that need to be taken to ensure safety. The safety assessments are to be carried out and documented by the organization responsible for operating the facility or conducting the activity, are to be independently verified and are to be submitted to the regulatory body as part of the licensing or authorization process.

In general, 'safety assessment' is the assessment of all aspects of a practice that are relevant to protection and safety. For an authorized facility, this includes siting, design and operation of the facility. Safety assessment is the systematic process that is carried out throughout the lifetime of the facility or activity to ensure that all the relevant safety requirements are met by the proposed (or actual) design. Safety assessment includes, but is not limited to, the formal safety analysis. [15]

Safety assessment plays an important role throughout the lifetime of the facility or activity whenever decisions on safety issues are made by the designers, the constructors, the manufacturers, the operating organization or the regulatory body. The initial development and use of the safety assessment provides the framework for the acquisition of the necessary information to demonstrate compliance with the relevant safety requirements, and for the development and maintenance of the safety assessment over the lifetime of the facility or activity

The determination whether an adequate level of safety has been achieved by the facility or activity is primary purpose of safety assessment .Thus, whether the basic safety objectives and safety criteria established by the designer, the operating organization and the regulatory body in compliance with the requirements for protection and safety are met.

A graded approach is used in determining the scope and level of detail of the safety assessment carried out at a particular stage for any particular facility or activity, consistent with the magnitude of the possible radiation risks arising from the facility or activity.

A key component of a systematic process to verify that applicable safety requirements are met in all phases of the life cycle of a nuclear facility is safety analysis. Safety analysis incorporates both probabilistic and deterministic approaches, which complement each other. Deterministic safety analysis is the principal means of demonstrating that the dose acceptance criteria and safety goals are met with a high degree of confidence for all accidents within the design basis. Probabilistic safety analysis is the principal means of demonstrating that the safety goals are met for potential accidents both within and beyond the design basis. It identifies vulnerabilities not necessarily accessible through deterministic safety analysis alone.

2.6.1 SAFETY ASSESSMENT REQUIREMENTS

According to IAEA Safety Standards Series No. GSR Part 4 (Rev. 1) [15], the overview of the safety assessment process as indicated in figure 1.1 shows the main elements of safety assessment and verification. The process requires that systematic evaluation of all the features of the facility relevant to safety are carried out. This process includes:

(a) Preparation for the safety assessment, in terms of assembling the expertise, tools and information required to carry out the work;

(b) Identification of the possible radiation risks resulting from normal operation, anticipated operational occurrences or accident conditions;

(c) Identification and assessment of a comprehensive set of safety functions;

(d) Assessment of the site characteristics that relate to the possible radiation risks;

(e) Assessment of the provisions for radiation protection;

(f) Assessment of engineering aspects to determine whether the safety requirements for design relevant to the facility or activity have been met;

(g) Assessment of human factor related aspects of the design and operation of the facility or the planning and conduct of the activity;

(h) Assessment of safety in the longer term, which is of particular concern when ageing effects might develop and might affect safety margins, decommissioning and dismantling of facilities, and closure of disposal facilities for radioactive waste.

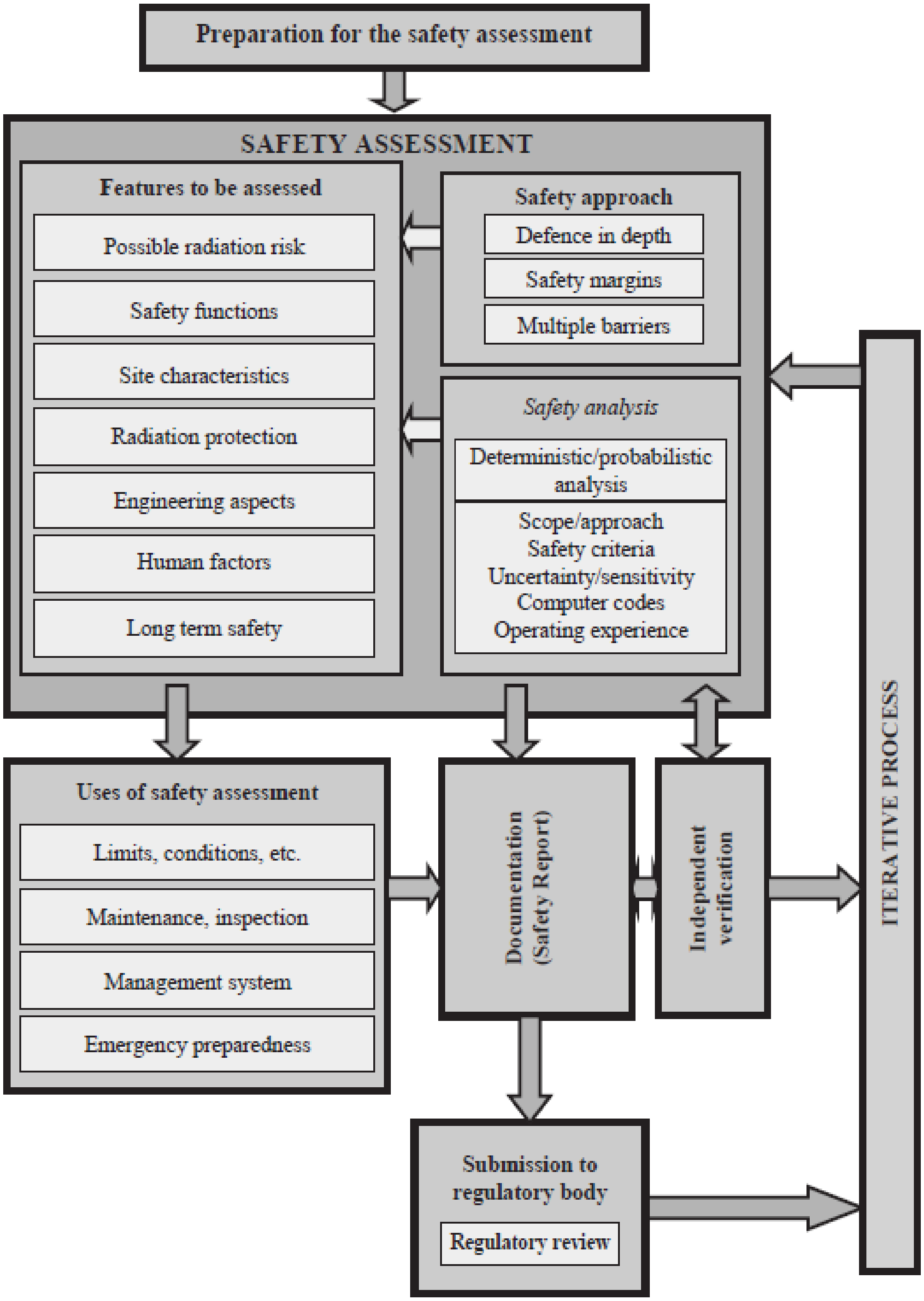


Figure 1.1 Overview of the safety assessment process [13].

The preparation stage of safety assessment is an important step for the success of the whole safety assessment program. The preparation stage ensures that there are sufficient number of people with requisite skills and expertise to carry out the work. Availability of adequate funding and necessary resources, information, data, analytical tools as well as the identification of the safety criteria are paramount to successful safety assessment. It is also necessary for assessors to have background information relating to the location, design, construction, commissioning, and operation, decommissioning and dismantling of the facility, together with any other evidence that is required to support the safety assessment.

The assessment will determine possible radiation risks, site characteristics and provisions for radiation protection. The design principles that have been applied for the facility are identified in the safety assessment, and it is determined whether these principles have been met. It is determined in the safety assessment whether requirements relating to human factors were addressed in the design and operation of a facility or in the way in which an activity is conducted. This includes those human factors relating to ergonomic design in all areas and to human–machine interfaces where activities are carried out. Evaluation of personnel competences, the associated training programs and whether the specified minimum staffing levels for maintaining safety are adequate.

CHAPTER THREE

3.0 SAFETY (RISKS) ANALYSIS

3.1 DETERMINISTIC SAFETY ANALYSIS

Deterministic safety analyses for a nuclear power plant predict the response to postulated initiating events. A specific set of rules and acceptance criteria is applied. Typically, these should focus on neutronic, thermohydraulic, radiological, thermomechanical and structural aspects, which are often analysed with different computational tools. The computations are usually carried out for predetermined operating modes and operational states, and the events include anticipated transients, postulated accidents, selected beyond design basis accidents and severe accidents with core degradation. The results of computations are spatial and time dependences of various physical variables (e.g. neutron flux; thermal power of the reactor; pressure, temperature, flow rate and velocity of the primary coolant; stresses in structural materials; physical and chemical compositions; concentrations of radionuclides) or, in the case of an assessment of radiological consequences, radiation doses to workers or the public.

Deterministic safety analyses for design purposes should be characterized by their conservative assumptions and bounding analysis. This is achieved by an iterative process in the design phase, when the limiting case(s) in terms of the minimum margin to the acceptance criteria is (are) determined for each group of postulated initiating events and sequences. To determine the limiting case for a given transient or set of transients, the consequential failures that are caused by the initiating event (internal or external) should be taken into account

In addition, an adequate set of conservative or best estimate assumptions for the initial and boundary conditions should be used. A limited number of coincident independent failures (including operator error) should also be addressed. However, the frequency of occurrence will decrease significantly as each coincident independent failure is taken into account. Only those combinations of transients whose frequency remains within the design basis should be analysed.

In a deterministic risk analysis of, for example, a nuclear power plant, the capabilities of the safety systems within the existing design would be compared with the overall safety goals of the plant (reactivity control, core cooling, retention of radioactive material within the plant and limitation of radiation exposure). Such deterministic prescriptions on the systems' design can be characterized as pre-defined rules whose fulfilment provides sufficient confidence that the safety goals are met (Berg, Fröhmel, Görtz & Schott, 1994). Thus, it is assumed that the risk related behavior of the plant can sufficiently well be described by showing compliance with these rules in a “checklist format” based on “yes” and “no” answers. The analysis results in the determination of divergences of the design and system states in the plant compared with the requirements set in the current regulations. The final result is a “safe” or “not safe” statement specific for a plant. A plant is considered safe when all possible failure event sequences leading to conditions beyond the prescribed rules can only occur at such a low probability that no precaution towards these events is required. Thus, each deterministic analysis also includes probabilistic arguments. However, comparisons of the safety of a plant relative to other plants or other types of plants fulfilling the same objective (e.g. nuclear power plants vs. coal-fired plants) are, strictly speaking, not possible. The deterministic approach for assessing safety performance thus generates only a limited insight which is necessary as basic information but not sufficient for decision-making, which is always based on relative ranking of alternative options. The only way to assure that the relative ranking is consistent is to use numbers.

3.2 PROBABILITY SAFETY ASSESSMENT

3.2.0 BACKGROUND

The development of safety design requirements for nuclear power plants in the last five (5) decades took place in a subjective, deterministic framework. Little use was made of the techniques of quantitative probabilistic risk assessment (PRA), largely because these techniques were not fully developed for analyzing nuclear power plants. It was F. R. Farmer who introduced the idea of reactor safety based on the reliability of consequence limiting equipment in the early 1960s. The first major application of PRA techniques was the Reactor Safety Study (WASH-1400**) [6]**, which demonstrated that a nuclear power plant could be analyzed in a systematic fashion by PRA techniques. Since the completion of the Study in 1975, the Nuclear Regulatory Commission (NRC) has been exploring ways of systematically applying probabilistic analysis to nuclear power plants, and the use of PRA techniques has been rapidly becoming more widespread in the nuclear community.

Contributing to these developments has been a growing appreciation of the wisdom of the strong recommendations made by the Lewis Committee to use PRA techniques for reexamining the fabric of NRC's regulatory processes to make them more rational. After the accident at Three Mile Island, these recommendations were reinforced by .the Kemenyl and Rogovin reports, which also encouraged the use of these techniques. As Lewis stated in his March 1981 Scientific American article, J "the Three Mile Island incident illustrates graphically how important it is to quantify both the probability and the consequences of an accident, and to generate some public awareness of these issues.... This is an issue that goes to the heart of many regulatory and safety decisions, where one must have some measure of the risks one is willing to accept on as quantitative a basis as the expert community can provide."[6]

Over the past years, many nuclear power plant (NPP) organizations have performed probabilistic safety assessments (PSAs) to identify and understand key plant vulnerabilities. As a result of the availability of these PSA studies, there is a desire to use them to enhance plant safety and to operate the plants in the most efficient manner practicable. PSA is an effective tool for this purpose as it assists plant management to target resources where the largest benefit for plant safety can be obtained. However, any PSA which is to be used to support decision making at NPPs must have a credible and defensible basis.

To date, probabilistic safety assessments (PSAs) have been performed for more than 200 nuclear power plants (NPPs) worldwide. Historically, PSAs have primarily been performed by regulatory bodies that have used them to gain generic risk insights (e.g. NUREG1150 **[16]**), or by licensees, who have used them for a variety of purposes including compliance with regulatory requests to support a safety case, identification and understanding key plant vulnerabilities, and analysis of the impact of proposed design or operational changes. There have also been some instances where PSAs have been used to evaluate the design of new plants. Having invested considerable resources in developing PSAs, there is a desire on the part of both licensees and regulators to use the insights derived from them to enhance plant safety while operating the nuclear stations in the most efficient manner. PSA is an effective tool for this purpose as it assists plant management to target resources where the largest benefit for plant safety can be obtained.

3.2.1 MATHEMATICS FOR PROBABILISTIC SAFETY

Nuclear power plant logical system model consist of the important components of a system and that component failure has effects on the system operability. The model treats each component as either working or not working, hence the state of the system may be represented by a logical equation composed of the states of the components. The calculation of the probability of the system is done by replacing each components Boolean state with the probability that that component will fail. The logic modelling uses the algebra of two-state variables called Boolean algebra.

Consideration are given to the meaning of probability, combining probabilities, calculating failure rates from inspection and incident data by classical and Bayes statistics. As well as treating uncertainties as distributed variables, calculating confidence intervals, and the importance of components to system operability.

3.2.2 BOOLEAN ALGEBRA

It is a branch of algebra in which the values of the variables are the true values true and false usually denoted 1 and 0 respectively. It is the algebra of two-state variables invented by George Boole to provide mathematics structure to logical reasoning. The following properties are used in the application of probabilistic safety.

Table 3.1 Properites and Comparison of Ordinary and Boolean algebra

Comparison of Ordinary and Boolean Algebra

property	Ordinary Algebra	Boolean Algebra
Commutative	$A+B=B+A$ $A*B=B*A$	same
Associative	$A+(B+C)=(A+B)+C$ $A*(B*C)=(A*B)*C$	same
Distributive	$A*(B+C)=A*B+A*C$	same
Idempotency		$A*A=A$ $A+A=A$
Completeness	$A*\overline{A}=A-A^2$ $A*1=A$	$A+\overline{A}=1$
Unity	$A+1=A=1$ $A*1=A$	$A+1=1$ $A*1=1$

Absorption	$A*(A+B)=A^2+A*B$ $A+(A*B)=A*(1+B)$	$A*(A+B)=A$ $A+(A*B)=A$
De Morgan´s theorem		$\overline{A}*\overline{B}=\overline{A+B}$ $\overline{A}+\overline{B}=\overline{A*B}$
Useful relationships	$A+(\overline{A}*B)=A+B-A*B$ $\overline{A}*(A+\overline{B})=\overline{B}+A*(B-A)$	$A+(\overline{A}*B)=A+B$ $\overline{A}*(A+\overline{B})=\overline{A}*\overline{B}$

3.2.3 MINIMAL CUT SETS AND MINIMAL PATH SETS

Boolean equations show how component failures can fail a system. For a failure analysis, a system failure event might consist of many component failure events nested together. Boolean algebra facilitates the reduction of events to a set of single-component failure events, double-component failure events, etc. The resulting single- and multiple-component events are cut sets, i.e. combinations of events, any of which could cause failure of a system. That is, a cut set is defined as a set of system events that, if they all occur, will cause system failure while a minimal cut set of a system is a cut set consisting of system events that are not a subset of the events of any other cut set. A minimal cut set is the smallest combination of component failures that can fail a system. Thus one-component minimal cut sets, if there are any, are single failures that cause system failure. Two-component minimal cutsets are pairs of components, if they occur together cause system failure. Triple-components minimal cutsets are sets of three components that, if they fail together cause system failure, and so on to higher cutsets. A minimal pathset is a smallest combination of component successes that can result in system success.

3.3 PROBABILITY AND FREQUENCY

Frequency with the dimensions of per unit time, ranges from zero to infinity and means the number of occurrences per time interval. Probability is dimensionless, ranges from zero to one, and has several definitions. The confusion between frequency and probability arises from the need to determine the probability that a given system will fail in a year. Such a calculation of probability explicitly considers the time interval and, hence, is frequency. However, considerable care must be used to ensure that calculations are dimensionally correct as well as obeying the appropriate algebra.

Three interpretations of the meaning of probability are:

1. Equation 3.1 expresses the Laplacian meaning of probability

$$\Pr obability = \frac{\text{Number of ways a result can occur}}{\text{The total number of ways all results can occur}} \tag{3.1}$$

2. von Misesian Probability

This is experimental probability determined from operating experience by counting the number of results of a particular type divided by the number of Probability trials. [5]

$$\Pr obability = \lim_{N_o \to \infty} \frac{N}{N_o} \tag{3.2}$$

Laplacian probability is calculated from geometry, von Misesian probability is approximated as the ratio of the number of times, N, which a particular result occurs to a total number of throws N_0. As N_0 becomes very large, the ratio approaches the true probability. Von Misesian probability is often called the frequency definition of probability although it does not have the dimensions of per unit time. The frequency results from the fact that N_o relates to a time interval.

3. Probability as State of Belief

As Tribus, 1969, says, all probabilities are conditional. In the example of the dice, the probabilities are conditioned on the assumption that the dice are perfect and the method of throwing has no effect on the outcome. According to deMorgan, probability refers to the belief by a mind having uncertain knowledge. This is the interpretation of probability in the Zion-Indian Point (ZIP) and some other PSAs [**5**]. Probability in this sense attempts to include all information that could affect the performance of a piece of equipment. Such information may be conveyed as a distribution whose height is proportional to confidence in the belief and whose width reflects uncertainty

3.4 COMBINING PROBABILITIES

3.4.1 Intersection or Multiplication

In an N trials experiment events A and B occur together N (A*B) times, and event B occurs N (B) times. The conditional probability of A given B can be expressed in equations 3.3 or 3.4 from 3.2

$$P(A/B) = \frac{\frac{\lim_{N_o \to \infty} N(A*B)}{N}}{\lim_{N_o \to \infty} \frac{N(B)}{N}} \qquad (3.3)$$

$$P(A/B) = \frac{P(A*B)}{P(B)} \qquad (3.4)$$

$$P(A*B) = P(A/B)*P(B) \qquad (3.5)$$

If A and B are independent, I.e. $P(A/B) = P(A)$, then equation (3.5) becomes

$$P(A*B) = P(A)*P(B) \qquad (3.6)$$

The probabilities are multiplied and this is a common approximation in PSA. The rule for combining independent probabilities in intersection is to multiply them together as shown in equation (3.7)

$$P(A*B*....N) = P(A)*P(B)*......P(N) \qquad (3.7)$$

3.4.2 Union or Addition

If events cannot occur at the same time, they are referred to as disjoint and those that can occur together are called non-disjoint. According to the von Misesian definition of probability

$$P(A_1 + A_2 + ...A_N) = \sum_{i=1}^{N} P(A_i)\text{(Disjoint)} \qquad (3.8)$$

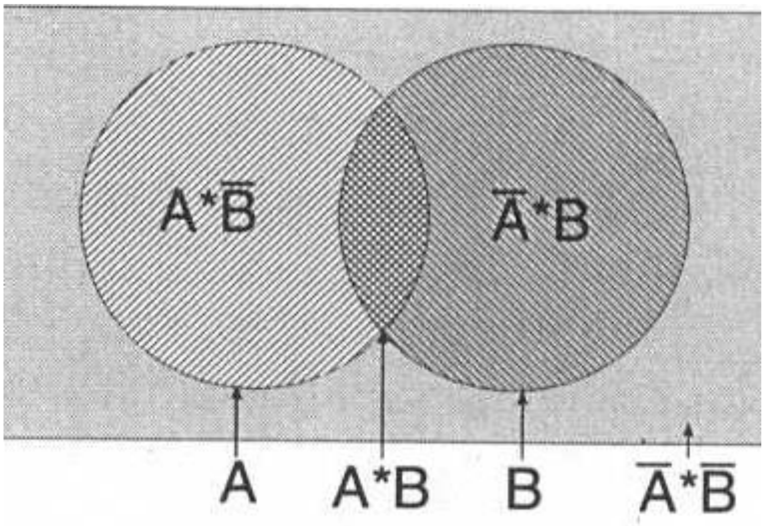


Figure 3.1 Venn diagram of sets A and B (right and left circles respectively).

From the Venn diagram Figure 3.1 the probability of each of the three segments

$P(A_1) = PA) * P(\bar{B})$ $P(A_2) = P(A) * P(B)$, $P(A_3) = P(\bar{A}) * P(B)$

Using the definition of complement these become

$P(A_1) = P(A) * [1 - P(B)]$, $P(A_2) = P(A) * P(B)$, $P(A_3) = [1 - P(A)] * P(B)$

Substituting into equation (3.8)

$$P(A + A * B + B) = P(A) * [1 - P(B)] + P(A) * P(B) + [1 - P(A)]P(B)$$

Since A+A*B=A Then simplifying the left side and expanding the right side it becomes $P(A + B) = P(A) - P(A) * P(B) + P(A) * P(B) + P(B) - P(A) * P(B)$

Simplifying it becomes

$P(A + B) = P(A) + P(B) - P(A) * P(B)$ (Non-disjoint) (3.9)

This result may be generalized to larger combinations by induction or by using de Morgan's theorem (the latter is easier to write as a computer program). The physical reason for the third term on the right of equation (3.9) is to correct for counting the overlap twice as seen in Figure 3.1. The technique of Venn diagrams is used in some PRAs to calculate mutually exclusive power states from non-mutually exclusive states.

The preceding equations can be generalized to the case of more than two events, where in general

3.4.3 M-OUT-OF-N-COMBINATIONS

The equation 3.9 can be generalized to the case of more than two events, where in general

$$P(E_1 + E_2 + ...E_N = \sum P(E) - \sum_{n=1}^{N-1} \sum_{m=n+1}^{N} P(E_n E_m) + ...(-1)^{N-1} P(E_1 E_2 ....E_N) \qquad (3.10)$$

The rth term on right –hand side of equation (3.10) contains

$$\binom{N}{r} = \frac{N!}{r!(N-r)!} \qquad (3.11)$$

Assuming that the probability of fire detector failure is P, the probability of M failed fire detectors, if the failures are independent, is P^M, and the probability of the others not failing is $(1\text{-P})^{\text{N-M}}$.

However, this must be corrected for the number of combinations of N things taken M at a time equation (3.11), where N–factorial is $N! = N*(N-1)*(N-2)........$ The combined result is given by equation 3.12 which is a binomial distribution.

$$P(N/M) = \binom{N}{M} P^M *(1-P)^{N-M} \qquad (3.12)$$

3.5 DISTRIBUTIONS

Distributions represent uncertainties. Often data are too sparse to provide a good estimate of the von Misesian probability. Confidence in the estimate may be found from knowing how the data are distributed. Distributions are of two types: discrete and continuous.

Distributions are characterized by measures of central tendency: The median is the value of x (e.g., crap scores) that divides the distribution into equal areas. The value of x at the peak. The first moment of the £ distribution*1 called the mean, average, expected or the expectation value of x is symbolized as E(x) or. The second moment about the mean is called the variance or var(x); its square-root is the standard deviation also called sigma. Thus median, mode and mean are measures of central tendency. Variance and standard deviation are measures of dispersion or uncertainty

The lower bound confidence limit is the probability that a parameter, x, is less than some value x, the upper bound confidence limit is the probability that a parameter, x, is greater than some value xt).

3. 5.1 Discrete Distributions
Poisson distribution

The Poisson distribution follows naturally from the discrete binomial distribution already introduced in the craps and the M-out-of-N problem. As *N* becomes large, the Poisson distribution approximates the binomial distribution

The Poisson distribution for observing M events in time t is given by equation (3.13)

$$P_M(t) = \frac{(\lambda * t) * \exp(-\lambda * t)}{M!} \qquad (3.13)$$

Where λ is the failure rate estimated as M/t. This model may be used if the failure rate is time dependent rather than demand dependent. As the sample size is increased further, the Poisson goes over to the Gaussian distribution which is the name commonly used by physicists and engineers for a model of many diffusion-like physical phenomena; it is called a "normal" distribution by statisticians

3.5.2 CONTINUOUS DISTRIBUTIONS
Gaussian/Normal

The Gaussian/normal is distributed1 according to equation 3.14

$$f(x) = \frac{\exp\left[-(x-\mu)^2/(2*\sigma^2)\right]}{\sigma\sqrt{(2*\pi)}} \qquad (3.14)$$

$$\begin{aligned} P(|X-\mu| \le \sigma) &= 0.693 \\ P(|X-\mu| \le 2*\sigma) &= 0.954 \\ P(|X-\mu| \le 3*\sigma) &= 0.997 \end{aligned} \qquad (3.15)$$

$$P(|X-\mu| \le k*\sigma) = 1 - 1/k^2 \qquad (3.16)$$

$$P(|X-\mu| \le k*\sigma) = 1 - 4/(9*k^2) \qquad (3.17)$$

$$f(X) = \frac{\exp\left[-(\ln(X)-\mu)^2/(2*\sigma^2)\right]}{X*\sigma\sqrt{(2*\pi)}} \tag{3.18}$$

Mean: $\alpha = \exp(\mu + \sigma^2/2)$ (3.19)

Variance: $\beta^2 = \alpha^2 * \left[\exp(\sigma^2 - 1)\right]$ (3.20)

Mode: $X_m = \exp(\mu + \sigma^2)$ (3.21)

$$\sigma^2 = \ln\left[(\beta^2/\alpha^2)+1\right] \tag{3.22}$$

$$\mu = \ln(\alpha) - \sigma^2/2 \tag{3.23}$$

Where μ is the mean, σ is the standard deviation, and x is the parameter of interest e.g. failure rate.

By integrating over the distribution, the probability of x deviating from μ by multiples of σ are given in equations 3.15. The σ , 2 σ , and 3 σ correspond to 69.3%, 95.4% and 99.7% confidence interval respectively.

3.5.3 Central Limit Theorem

The Central Limit Theorem gives an a priori reason for why things tend to be normally distributed. It says: the sum of a large number of independent random distributions having finite means and variances is normally distributed. Furthermore, the mean of the resulting distribution is the sum of the individual means; the combined variance is the sum of the individual variances [5]

3.5.3 Lognormal Distribution

The Reactor Safety Study extensively used the lognormal distribution to represent the variability in failure rates. If plotted on logarithmic graph paper, the lognormal distribution is normally distributed.

Several characteristic values of the distribution are given by equations 3.19 to 3.21 which may be solved to give equations 3.22 and 3.23.

3.5.5 Erlangian and Exponential Distributions

The Erlangian distribution is the time-dependent form corresponding to the Poisson distribution for failure events of devices operated on demand. The distribution arises frequently in reliability engineering calculations involving random failures for which $\lambda(t) = \lambda$. To derive the distribution from the Poisson distribution we recognize that the mean number of failures μ is the product of λ and time t. The probability of exactly n failures occurring in time t is then given by

$$P(n,t) = \frac{\exp(-\lambda t)(\lambda t)^n}{n!} \tag{3.24}$$

And the probability of k or fewer failures is

$$P(\leq k,t) = \sum_{n=0}^{k} \frac{\exp(-\lambda t)(\lambda t)^n}{n!} \tag{3.25}$$

Equation (3.24) permits calculation of the failure probability density f (t) for the nth failure in dt about t, given that a device has undergone n -1 prior failures. Then the system is vulnerable to failing with a hazard rate λ . Thus the Erlangian distribution follows from Eq. (3.24) as

$$f(t) = \lambda P(k-1,t) = \frac{\lambda(\lambda t)^{k-1}\exp(-\lambda t)}{(k-1)!}, k \geq 1. \tag{3.26}$$

The most important special case is for k = 1, for which the exponential distribution is obtained, with

$$f(t) = \lambda \exp(-\lambda t)$$
$$F(t) = 1 - \exp(-\lambda t)$$

The mean and variance are

$$MTTF = 1/\lambda$$
$$\sigma^2 = 1/\lambda^2$$

The exponential distribution can be used for analyzing the (first) random failure event of a device characterized by a constant hazard rate. Both the exponential and Erlangian distributions are special cases of the gamma distribution for which k is not restricted to integer values

3.6 BAYESIAN METHODS

A systematic framework for the introduction of prior knowledge into probability estimates was provided by Reverend Thomas Bayes. Indeed, Bayesian methods may be viewed as nothing more than convolving two distributions. The argument was based on what prior knowledge is acceptable, and the treatment of probabilities as random variables themselves.

Classicists believe that probability has a precise value; uncertainty is in finding the value. Bayesians believe that probability is not precise but distributed over a range of values from heterogeneities in the database, past histories, construction tolerances, etc. This difference is subtle but changes the two approaches. Bayes' methods aim to satisfy two needs: the concept of probability as degree of belief, and the need to use all available information in a probability estimate. Classicists reject all except test information. However, a Bayesian believe that prior information from related work, laboratory tests, codes, quality control, etc. should be used to decide the state of belief in something's operability. The problem is in quantifying this prior knowledge. This section develops Bayes' equation and presents results for some distributions using conjugate functions. It closes with confidence interval estimating

3.6,1 BAYES'S EQUATION

Equation 3.4 may be considered to be composed of three variables as shown in equation 3.27

$$P(A*B/E) = P(A/B*E)*P(B/E) \tag{3.27}$$

$$P(A*B/E) = P(B*A/E) \tag{3.28}$$

Where $P(A*B/E)$ is read as the probability of A and B given E. Where A, B, and E are observables and E represents the operating environment.

However, equation (3.28) is valid because A, B are commuting variables that lead to equation (3.29)

$$P(A*B/E) = P(B*A/E) = P(A/B*E)*P(B/E) = P(B/A*E)*P(A) \tag{3.29}$$

Rearranging, yields equation (3.30) which is referred to as Bayes equation

$$P(A/B*E) = \frac{P(B/A*E)*P(A/E)}{P(B/E} \tag{3.30}$$

$P(A/E)$ Is the prior probability of A given E. $P(B/A*E)$ is probability that is inferred from new data (update) and $P(A/B*E)$ is the posterior probability that results from updating the prior with new information. The denominator $P(B/E)$ serves the purpose of normalization

From completeness of the Aj´s (the components of A) and using the multiplication for intersection, equation (3.31) is obtained

$$P(B/E) = \sum_i P(B*A_i/E \qquad (3.31)$$

$$P(B/E) = \sum_i P(B/A_i*E)*P(A_i/E \qquad (3.32)$$

$$P(A/B*E) = \frac{P(B/A*E)*P(A/E)}{\sum_i P(B/A_i*E)*P(A/E)} \qquad (3.33)$$

$$P(A/B*E) = \frac{P(B/A*E)*P(A/E)}{\int P(B/A_i*E)*P(A_i/E)*dA} \qquad (3.34)$$

Bayes equation may be written as the more useful equation (3.33), for discrete A_i, and as equation (3.34) for continuous A's over the domain of A. The two equations show that the updated probability is just the product of the prior and the new information. If the entire set of conditional probabilities becomes known, the calculation of the posterior becomes straightforward. It is often used in probabilistic risk assessments of nuclear systems to update the probability density function representing the failure rate of a component or the frequency of an event of interest.

3.7 THE ROLE OF PSA IN NPP SAFETY MANAGEMENT

Probabilistic Safety Assessment (PSA) is an established technique to numerically quantify risk measures in nuclear power plants. It is also referred to as Probabilistic Risks Assessment (PRA) especially in United States of America. Therefore, PSA and PRA are used interchangeably in this work. PSA consist of a huge model of the nuclear power plant, in which all safety relevant systems, involving thousands of components, are modelled in terms of their reliability and are logically linked together to determine to overall likelihood of core melt accidents.

PSA seek to determine what undesired scenarios can occur, with which likelihood, and what the consequences could be. In addition, it can generate indirect information such as the importance of individual risk contributors.

In the nuclear industry, PSA is required to fulfil the following principal objectives:

- Provide an estimate of the core damage frequency (CDF) and identify the major accident sequences;
- Identify those components or plant systems whose unavailability significantly contribute to the core damage frequency;
- Identify any functional, spatial and human induced dependencies within the plant configuration which contribute significantly to the core damage frequency;
- Provide a computerized model of the nuclear power plant;
- Rank the accidence sequences and components according to their relative importance;
- Evaluate the plant operating experience;
- Evaluate the plant technical specification and limiting condition of operation
  Support decisions on backfitting and design modifications.

The analysis is done using a logical and systematic approach that makes use of realistic assessments of the performance of the equipment and plant personnel as a basis for the calculations. This in principle has the potential to produce an understanding of the inherent risk of operating the plant over a much wider range of conditions than the traditional deterministic methods which generally define what is assumed to be a bounding set of fault conditions. Furthermore, the adoption of conservative assumptions relating to plant and system performance is an accepted approach to addressing uncertainty when performing these deterministic analyses. PSA considers a much broader range of faults and takes integrated approach at the plant as a whole. It looks at system inter-dependencies and uses realistic criteria for the performance of the plant and systems, which leads to more risk informed decision making. The PSA, therefore, is a useful tool for safety management and its use can increase the level of safety by providing information not available from the evaluation of a limited set of design basis events.

However, while the PSA can be seen, in principle, to provide a broader perspective on safety issues than the deterministic approaches, the application of sound engineering principles has been demonstrably successful in achieving a high level of safety. Besides, while PSA is a very powerful tool to support decision making, its weaknesses and limitations need also to be acknowledged. Therefore, it is unlikely that PSA can be the sole decision making tool. Consequently, a consensus seems to be being reached that an integrated approach that uses deterministic engineering principles and probabilistic methods is the appropriate approach to decision making at nuclear power plants. For example, the NRC policy states that ´´The use of PRA technology should be increased in all regulatory matters to the extent supported by the state of the art in PRA methods and data, and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy´´ [**17**]. That is indicative of a trend towards a modern risk informed approach to safety regulation in which the PSA is used to provide one of the inputs to decisions concerning safety.

3.7.1 PROJECT MANAGEMENT FOR PSA

The management scheme for PSA project is established by the selection of methods, procedures and personnel. This involves the organization of team that perform the PSA, the training of the team, preparation of a PSA project schedule, the estimation and securing of the necessary funds, and establishment of quality assurance procedures and peer review procedures.

The PSA study is usually commissioned by either the plant designer, or the operator or the regulator. The operating organization always participate as a source of operational knowledge, as well as beneficiary of the insight obtained.

Identification of design weakness or procedural weakness can be corrected or improved less expensively when the PSA process is performed as early as possible in lifetime of the plant than the plant is in operation. It is possible to start PSA in any of the stages in the lifetime of the plant. The model and documentation is maintained in clear, traceable systematic and transparent manner. In this way it can be effectively used to support the review, application and the future upgrade of the PSA.

3.8 PROBABILISTIC SAFETY ASSESSMENT (PSA) TASKS AND METHODS

PSA involves the development of several sets of accident sequences models and determining their outcome. In view of that, several sets of models are developed and analyzed.

The accident sequences development and analysis can be broken down into two sets of models, those relating to the plant systems and those related to the containment.

The plant-system models generally consist of event trees, which depict initiating events and combination of system success and failures, and fault trees which depict ways in which the system failures represented in the event trees can occur. These models are analyzed to evaluate the frequency of each accident sequence.

The containment models represent the events occurring after the accident but before the release of radioactive material from containment to the environment. They deal with the physical processes induced in the containment as well as the transport and deposition of radionuclides within containment. The assessment covers the response of the containment to these processes, including possible failures modes, and evaluate the releases of radionuclides to the environment.

3.8.1 INITIAL INFORMATION COLLECTION

Probabilistic safety assessments are broad, integrated research requiring large amounts of information from deterministic safety assessment. The information that is required depends on the scope of the analysis and falls into three broad categories: 1. Plant design, site, and operation information. 2. Generic and plant-specific data. 3. Documents on PSA methods.

3.8.2 SYSTEM ANALYSIS

The frequencies of plant damage and public consequence are calculated using plant logic combined with component fragilities. This task involves the definition of accident sequences, an analysis of plant systems and their operation, the development of a data base for initiating events, component failures, and human errors; and an assessment of accident-sequence frequencies. It constitutes a major portion of the risk assessment and hence is divided into the several subtasks discussed below. Although the subtasks are presented sequentially, the performance of the plant-system and accident-sequence analysis requires considerable iteration. The results of this analysis-the frequencies of accident sequences and insights into their causes--constitute the products of a level 1 PRA. They are also used in the subsequent tasks of more-extensive risk assessments. Event and fault trees are constructed to identify the accident sequences and the damage that may result from an earthquake.

The quantification of accident sequences involving fires follows the general methodology for event trees and fault trees. Special attention must be paid to intersystem dependencies introduced by fire. Although early analysis based on simple system reliability models indicated low accident probability, more recent estimates employing sophisticated plant and system-level models give higher risk. These estimates tend to be dominated by the effects of interactions that increase the probability of successive failures in an accident chain

3.9 EVENT-TREE DEVELOPMENT

The event-tree is combinations of initiating events and the successes or failures of systems-to be analyzed and the development subtask delineates the various accident sequences. A graphical depiction of a sequence of events and consequence are described logically. This activity includes an identification of initiating events and the systems response to each initiating event. The scope of the event tree depends on the extent of the analysis.

Systems that only serve to mitigate, but do not contribute to the prevention of a core-melt accident may not be included in a level I PRA. The analysts developing the event trees should consult with those familiar with the analysis of physical processes inside the containment to define system dependences arising from interactions related to the physical phenomena induced by the accident. Separate event trees are generally constructed for each [18]

Quantification of the risk associated with a commercial nuclear power plant requires the delineation of a large number of possible accident sequences. Because nuclear systems are complex, it is not feasible to write down by inspection a listing of important sequences. A systematic and orderly approach is required to properly understand and accommodate the many factors that could influence the course of potential accidents.

Using information from the accident sequence initiating event analysis, system event trees that display the combinations of plant system failures that can result in core damage are constructed for each initiating event group. An individual path through such an event tree (an accident sequence) identifies specific combinations of system successes and failures leading to (or avoiding) core damage. As such, the event tree qualitatively identifies what systems must fail in a plant in order to cause core damage.

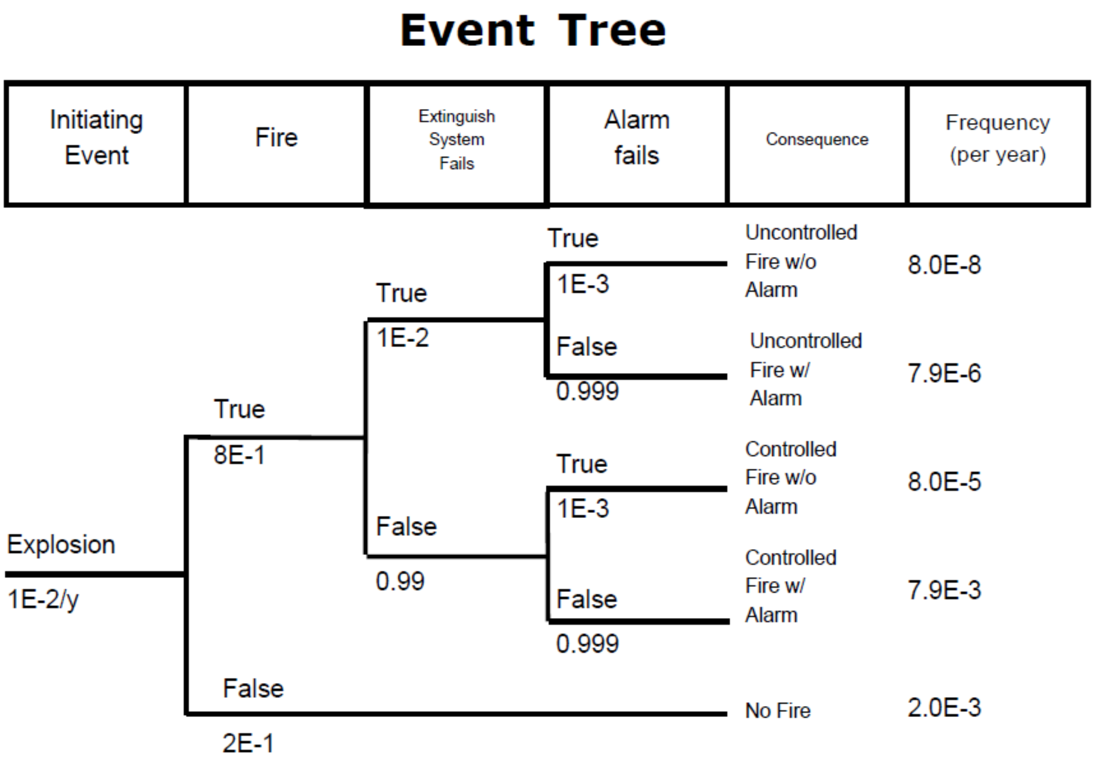
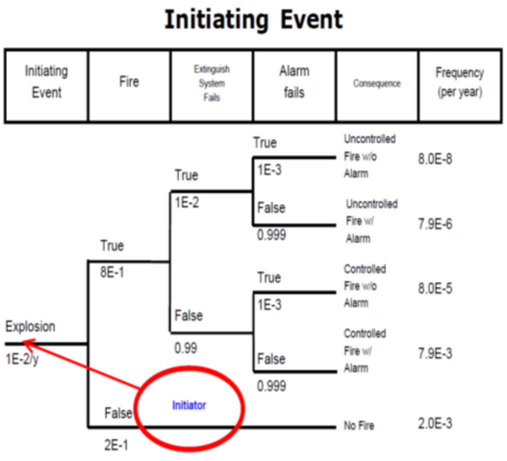


Figure 3.2a. Typical example of an Event Tree



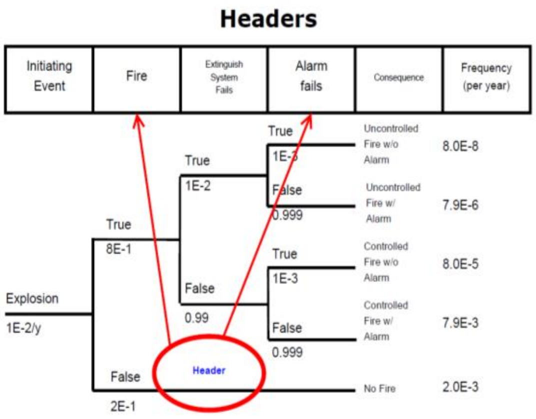


Figure 32b

figure 3.2c

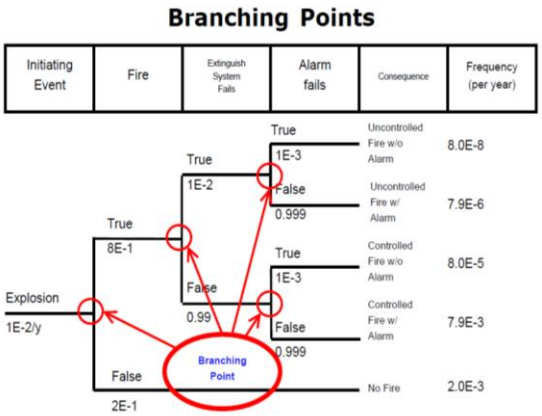


Figure 3.2d

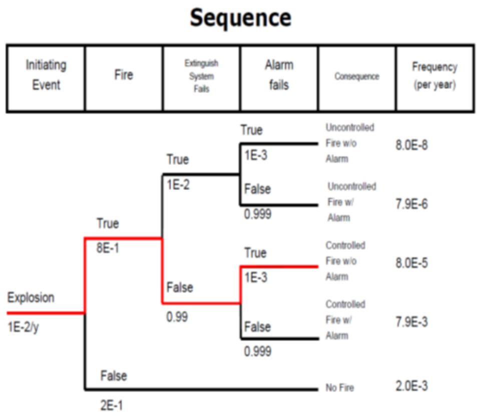


Figure 3.2e

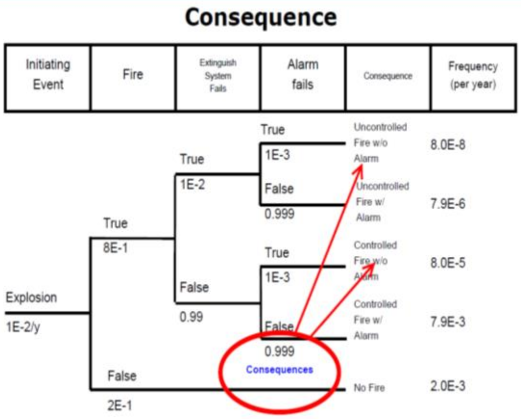


Figure 3.2f

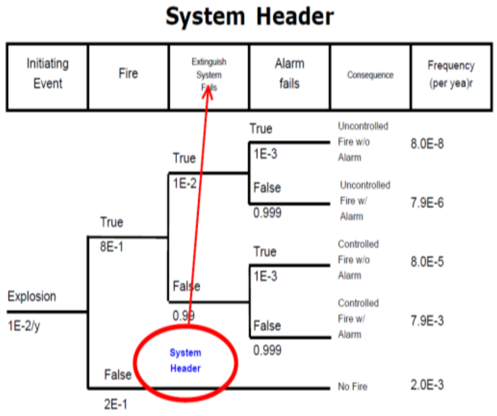


Figure 3.2g

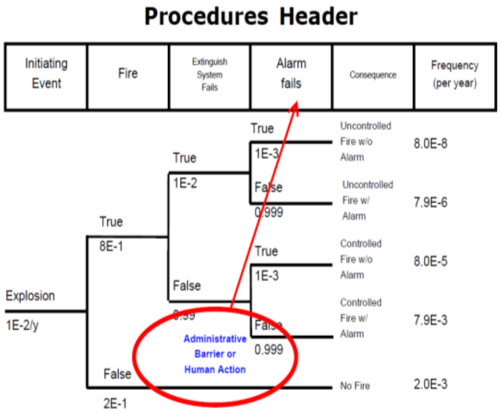


Figure 3.2h

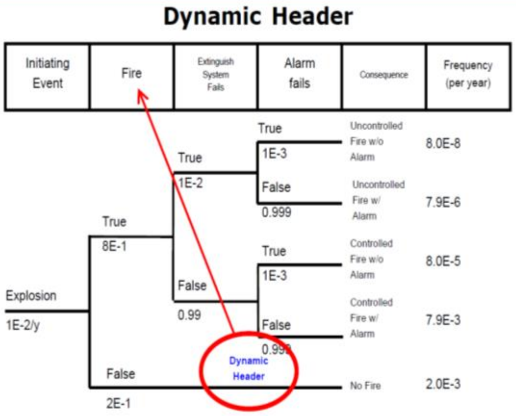


Figure 3.2i

The graphical logical representation of the event trees consist of initiating events, headers, branches, sequences and consequences as shown in a sample event tree in figure 3.2a-e. The headers comprise of system header, procedure header and dynamic header. Safety functions or barriers may be engineering (systems, containment) or administrative (regulations, procedures, organization) as shown in figure 3.2.f-h. Other factors have to be considered such as dynamics: gas burning, physical variables evolution; Human: personnel trained or near the accident scene; Environmental: conditions at the accident site or in rooms

An Initiating Event is defined as a significant departure from normal conditions that may lead to undesired consequences such as, for instance, a gas leak, falling objects, fire start etc. An initiating event may lead to one or more undesired consequences depending on the success or failed condition of barriers or safety functions. They are complex systems designed so that one or more barriers separate dangerous processes from undesired consequences; Systems are put in place to mitigate events that depart from stable operation. An initiator may lead to different consequences with different probability depending on the working state of the barriers and mitigating systems.

There are two types of initiators: internal and external. Internal initiators results from failures within the plant or the plant´s support utilities. For example, vessel rupture, human error, cooling failure, loss of feedwater, condenser vacuum, instrument air, and loss of offsite power are internal events. Earthquakes, tornados, fires (external or internal), and floods (external or internal) constitute external initiators. The external initiators may trigger an internal events. Event trees can be used to analyze either type of initiator.

Given the initiator, the sequence must show what operational systems or actions are involved in responding to the initiator and generally ordered in time sequence. A support system must enter the sequence before the affected systems in order for a support system failure to fail the systems it supports. These mitigating systems are not necessarily equipment, they may be human actions. Exceptions to time sequencing the events arise from the need to introduce dependencies by manipulating the branching probabilities according to preceding events

The headers specifies events for which the probability of failure (or success) must be specified to obtain the branching probabilities of the event tree as shown in figure 3.2 (d). However, for complex system events of failure may require fault tree or equivalent methods to calculate the branching probability using component probabilities. In some cases, the branching probability may be obtained directly from failure rate data suitably conditioned for applicability, environment and system interactions.

3.10 FAULT TREE MODEL

According to NUREG 0492 a fault tree analysis can be simply described as an analytical technique, whereby an undesired state of the system is specified (usually a state that is critical from a safety standpoint), and the system is then analyzed in the context of its environment and operation to find all credible ways in which the undesired event can occur. The fault tree itself is a graphic model of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired event. The faults can be events that are associated with component hardware failures, human errors, or any other pertinent events which can lead to the undesired event. A fault tree thus depicts the logical interrelationships of basic events that lead to the undesired event-which is the top event of the fault tree.

It is important to understand that a fault tree is not a model of all possible system failures or all possible causes for system failure. A fault tree is tailored to its top event which corresponds to some particular system failure mode, and the fault tree thus includes only those faults that contribute to this top event. Moreover, these faults are not exhaustive-they cover only the most credible faults as assessed by the analyst.

It is also important to point out that a fault tree is not in itself a quantitative model. It is a qualitative model that can be evaluated quantitatively and often is. This qualitative aspect, of course, is true of virtually all varieties of system models. The fact that a fault tree is a particularly convenient model to quantify does not change the qualitative nature of the model itself.

A fault tree is a complex of entities known as "gates" which serve to permit or inhibit the passage of fault logic up the tree. The gates show the relationships of events needed for the occurrence of a "higher" event. The "higher" event is the "output" of the gate; the "lower" events are the "inputs" to the gate. The gate symbol denotes the type of relationship of the input events required for the output event. Thus, gates are somewhat analogous to switches in an electrical circuit or two valves in a piping layout.

Fault Trees is Logic models of safety functions that are required to mitigate an initiating event, as established by the success criteria developed in sequence analysis. The failure of the system is the top event that represents failure to comply with the success criterion of the system. Thus, the fault tree is a graphic model of the various parallel and sequential combinations of faults that result in the top event.

The methodology proceeds in a step-by-step deductive way breaking down the top event to find all of the credible ways in which the undesired event can occur. The analysis stops at basic events where further decomposition is not possible or worthwhile. The Basic event is probability that a component fails to perform its intended task during an accident.

CHAPTER FOUR

4.0 HISTORICAL REVIEWS OF NUCLEAR POWER PLANT FIRE SAFETY

4.1 INTRODUCTION

Since its inception, fire has been a vital part of humankind's existence and survival. Numerous attempts has been made to prevent, control and mitigates the devastative effects of fires over all these years. The great fire of Rome in 64 AD caused devastation due to narrow streets, tall buildings, combustible building materials, and common walled buildings. Emperor Nero created a new urban plan by creating wider streets, restrictions on the height of houses; no common walls of buildings and homes that were constructed with fire resistant materials such as stone instead of wooden pillars. Similarly, in September1666, the 13th King Charles II of England issued a proclamation in which the walls of all new buildings were to be of brick or stone; the main streets were to be widened to prevent fire spread; and the existing narrow alleyways were to be considerably reduced. In 1631 the United States of America the first American building code issued in Boston Massachusetts by John Winthrop, Governor of Boston, outlawed the building of wooden chimneys and thatched roofs of homes as each of these were found to cause more fires and dangerous fires throughout the community.

In the course of history and experiences with fire disasters laws and regulations were developed to prevent and control domestic and industrial fire around the globe. Fire detection, suppression and control systems were developed such as fire alarm system, fire detectors, and automatic fire sprinkler system. For example, First Automatic Sprinkler System was patented by Philip W. Pratt of Abington, MA in 1872 **[19]**

Despite the numerous fire disasters, human error, weak fire laws enforcement, system and equipment failures continued to cause billions of dollars in damages and fatalities. For instance, in 1953 General Motors Plant Fire the Building was only 20% sprinkled, there were no fire walls or partitions, and no roof vents, and unprotected steel roof trusses. Fire started when a cutting torch ignited conveyor drip pan oil and spread quickly through the open room. Smoke, heat, and fire were trapped in the building due to no roof vents. Fire hose streams only penetrated 75 feet into the 866 feet wide building. Roof trusses failed quickly and allowed melted roof asphalt to fuel the fire. This resulted in code changes by restrictions on roof tar build up; Separation of hazardous operations; Sprinkler requirements in Industrial buildings; Fire coating for steel frame trusses; Automatic fire doors and NFPA 204-Guide for Smoke and Heat Venting.

In nuclear energy front, from 1945 attention was given to harnessing this energy in a controlled fashion for naval propulsion and for making electricity. Since 1956 the prime focus has been on the technological evolution of reliable nuclear power plants. These nuclear power plants were also treated as an industrial complex. Hence, industrial fire regulations and laws were applied. Similar fate befell the nuclear industry, for example The Windscale fire of 10 October 1957 was the worst nuclear accident in Great Britain's history, ranked in severity at level 5 out of a possible 7 on the International Nuclear Event Scale. The two piles had been built as part of the British atomic bomb project **[20**]. Windscale Pile No. 1 was operational in October 1950 followed by Pile No. 2 in June 1951. The fire burned for three days and there was a release of radioactive contamination that spread across the UK and Europe **[21]**. The effect was not only damage caused by the fire but also radiological effects.

Years of experience, incidents, tragedies, and education has helped evolve how people handle, control, prevent, contain, and provide safe conditions with fire. Agencies such as the National Fire Protection Association (NFPA), the International Code Council (ICC), Underwriter's Laboratories (U.L.), as well as many others have been monumental in the development of codes and regulations that limit the devastating effect that fire creates.

In the 28 years of United States Atomic Energy Commission (AEC) existence, the total losses from all accident causes, including fires, explosions, electrical materials, radiation/decontamination incidents, materials losses, transportation incidents, acts of nature, and miscellaneous causes amounted to just under $68 million. Of this total, fires accounted for 60%. The cumulative loss ratio for the entire period was 2.0 per $100 of property values. For fire alone, the ratio was 1.2 per $100 of value **[22]**

This research looks at historical assessment and observations of nuclear power plants fire safety. The historical assessment will be based on fire safety regulations, fire safety protection programs, and fire safety assessment methods from the perspective of United State of America, Germany, Japan and International Atomic Energy Agency (IAEA). Review of nuclear power plant fire safety regulations from the perspective of regulatory bodies is considered.

4.2 HISTORICAL REVIEW OF FIRE SAFETY AT NPP IN USA

4.2.1 FIRE SAFETY REGULATIONS EVOLUTION

The May 11, 1969 Rocky Flats plutonium facility fire **[22]** marks a dividing line in the history of AEC fire protection program. The fire started from the spontaneous ignition of plutonium briquettes in storage box in a glove box line and spread to involve combustible shielding materials in the box and the conveyer lines.

The post Rocky Flats fire lessons learned led to three steps of major importance to be taken. As described in the AEC General Manager´s letter of December 16, 1969, to the Chairman of the congressional joint Committee on Atomic Energy. [22]

These led to an initiation of physical upgrading program, Organizational changes and Insurance Survey program. In addition to the three programs, the directive covering the fire protection requirements of the AEC was changed to more clearly spell out the performance nature of the system. The new definition and the goals of the ¨improved risk¨ were spell out and became the fire protection standard.

With the development of commercial NPP in the USA, Westinghouse designed the first fully commercial PWR of 250 MWe, Yankee Rowe, which started up in 1960. While the boiling water reactor (BWR) was developed by the Argonne National Laboratory, and the first one, Dresden-1 of 250 MWe, designed by General Electric, was started up earlier in 1960. A prototype BWR, Vallecitos, ran from 1957 to 1963. The AEC continued to use the fire requirement guides developed for the research facilities and as applied to other industrial facilities to commercial nuclear power plants.

The NRC was created on January 19, 1975, by the Energy Reorganization Act, which abolished the Atomic Energy Commission (AEC) and replaced it with the NRC, the Energy Research and Development Administration, and the Energy Resources Council. The latter two agencies later became part of the U.S. Department of Energy (DOE), which was created on October 1, 1977.

When the U.S. nuclear industry designed (and built, in many cases) the current generation of commercial NPPs, the NRC stated its fire protection requirements in terms of broad performance objectives for the design and location of systems, structures, and components important to safety; the use of noncombustible and heat-resistant materials; and the provision of fire detection and suppression systems. No detailed implementation guidance existed to determine whether a plant's fire protection program met these objectives, and the NRC staff relied upon compliance with local fire codes and insurance underwriter ratings to determine acceptability.

The governing regulatory guidance until 1975 for fire protection in nuclear power plants was based on the General Design Criteria 3(GDC-3) to 10 CFR50 Appendix A **[23]**. In January 1975, NRC inherited its regulatory roles from AEC. In March 22, NRC were confronted with the fire at Browns Ferry Nuclear (BFN) station, which caused damage to the electrical circuits including safety related cables.

The fire at the Browns Ferry Nuclear (BFN) Power Plant, Unit 1, on March 22, 1975, was a pivotal event that brought fundamental change to fire protection and its regulation in the U.S. nuclear power industry and all over the globe. The BFN fire began when a worker used a candle to inspect for air leakage during the installation of temporary penetration seals on fire-barrier cable trays. A ventilation-induced differential pressure between the plant cable spreading room and the Unit 1 reactor building was being used as the driving force for smoke from the candle. The movement of smoke toward and through the seal would indicate a crack in a temporary penetration seal. During this inspection, the candle flame set the temporary polyurethane penetration seal material on fire when it was sucked into the crack. The fire quickly spread to the cables on both sides of the penetration and burned uncontrollably for almost 8 hours [6]. During the fire, the control room received numerous erroneous instrument readings and spurious indications of systems starting and stopping (of course, at the time, the operators did not know if they were real or not). In large part, the continued burning resulted from reluctance on the part of plant operators to apply water to the fire for fear of shorting out vital electrical safety systems. Once water was applied, the fire was quickly brought under control. The fire damaged over 1,600 electric cables, routed in 117 conduits and 26 cable trays; of the affected cables, 628 were important to safety and rendered all of the Unit 1 and many of the Unit 2 emergency core cooling systems (ECCS) inoperable. Figure 4.1 shows BFN cable trays with cables damaged by the fire. Although the BFN fire disabled a significant number of plant safety systems, the operators successfully brought the reactor from power operation to a safe shutdown condition. However, the loss of multiple safety systems resulted in significant difficulties in achieving a safe shutdown state. Operators had to initiate a number of untested recovery actions to restore plant systems and achieve a stable reactor condition.

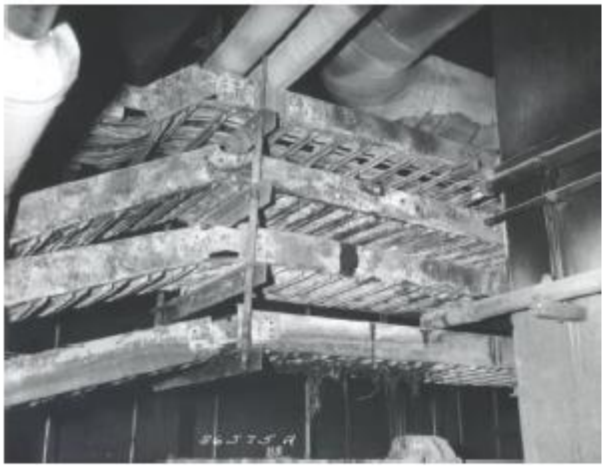


Figure 4.1 Brown Ferry cable trays after the fire, showing damaged cables [24]

In May 1976, the NRC issued BTP APCSB 9.5-1, “Guidelines for Fire Protection for Nuclear Power Plants” [25], which incorporated the recommendations from the Browns Ferry fire special review team and provided technical guidelines to assist licensees in preparing their FPPs. As part of this action, the staff asked each licensee to provide an analysis dividing the plant into distinct fire areas and demonstrating that redundant success paths of components required to achieve and maintain safe-shutdown conditions for the reactor were adequately protected from fire damage. However, the guidelines of APCSB 9.5-1 applied only to those licensees that filed for a construction permit after July 1, 1976.

In September 1976, in an effort to establish defense-in-depth FPPs, without significantly affecting the design, construction, or operation of existing plants that were either already operating or well past the design stage and into construction, the NRC modified the guidelines in APCSB 9.5-1 and issued Appendix A to APCSB 9.5-1 [25]. This guidance provided acceptable alternatives in areas where strict compliance with APCSB 9.5-1 would require significant modifications. Additionally, the NRC informed each licensee that the staff would use the guidance in Appendix A to analyze the consequences of a postulated fire within each area of the plant and asked licensees to provide results of the fire hazards analysis for each unit and the technical specifications for the present fire protection systems.

Thanks to the review of fire hazards analysis using the Appendix A to APCSB 9.5-1[25], the staff of NRC realized that additional guidance on the management and administration of FPPs was necessary. In August 1977, GL77-02 “Nuclear Plant Fire Protection Functional Responsibilities, Administrative Controls and Quality Assurance” [26], was issued. This guidelines provided criteria to review specific elements of a licensee´s FPP, including organization, training, and combustible and ignition source control, firefighting procedures, and quality assurance (QA).

By early 1980, most operating plants had completed their analyses and implemented much of the FPP guidance and recommendations specified in Appendix A to the BTP. In most cases, the NRC found the licensees’ proposed modifications resulting from these analyses to be acceptable. In some instances, however, technical disagreements, such as the requirements for fire brigade size and training, water supplies for fire suppression systems, alternative or dedicated shutdown capability, emergency lighting, qualifications of penetration seals used to enclose places where cables penetrated fire barriers, and the prevention of reactor coolant pump (RCP) oil system fires, were raised. Some licensees opposed the wholesale adoption of these specified fire protection recommendation. After extensive deliberations, and given the generic nature of some of the disputed issues, the commission resolved that a rulemaking was necessary to ensure proper implementation of the NRC´s fire protection requirements.

Consequently, in November 1980, the NRC published the “Fire Protection” rule, 10 CFR 50.48, which specified broad performance requirements, as well as Appendix R to 10 CFR Part 50, which contained detailed regulatory requirements for resolving the disputed issues.

The proposed rule, and the application of appendix R to all plants licensed before January 1, 1979, including those for which the staff had previously agreed that the fire protection features met the provisions of Appendix A to APCSB 9.5-1 [25] were analyzed. The commission decided that only 3 of the 15 items in Appendix R were of such safety significance that they should apply to all plants licensed before January 1, 1979, including those whose fire protection features met the provisions Appendix A. These three items are fire protection of safe-shutdown capability (including alternative or dedicated shutdown systems), emergency lighting, and the Reactor Coolant Pump (RCP) oil system.

Appendix R to 10 CFR Part 50 and 10 CFR 50.48 became effective on February 17, 1981; but, the rule provided exemption process. A licensee can request an exemption if the required fire protection feature to be exempted would not enhance fire protection safety in the facility, or if a modification to meet regulatory requirements might be detrimental to overall safety. The NRC approved many plant specific alternative methods to achieve the underlying purpose of the regulation based on exemptions at about 60 nuclear power plants.

This progression, the broad provisions of the General Design Criteria (GDC), the detailed implementing guidance, the plant-by-plant review, and finally the issuance and backfit of the fire protection regulation and the prescriptive requirements of Appendix R created a complex regulatory framework for fire protection in U.S. nuclear power plants licensed before 1979 and resulted in the issuance of additional guidelines, clarifications, and interpretations, primarily as generic letters. The NRC did not require plants licensed after January 1, 1979, to meet the provisions of Appendix R unless directed to do so in specific license conditions. The NRC typically reviewed these plants using the guidelines of SRP Section 9.5.1, “Fire Protection Program”, which subsumed the criteria specified in Appendix R. In July 1981, the NRC issued a major revision to the SRP for use in the review of new license applications. This revision included SRP Section 9.5.1 with Branch Technical Position (BTP) CMEB 9.5-1, “Fire Protection for Nuclear Power Plants” **[25**], as an update to the earlier fire protection Branch Technical Positions (BTPs).

0n 23 October 1987, despite all the efforts of regulations, a fire occurred at the problem-plagued Fort St. Vrain Nuclear Power plant which forced the plant to shut down but there were no injuries and no radiation was released. The fire was caused by a hydraulic relief valve that blew and spewed hydraulic oil which got ignited. However the lessons learned help in the development and implementation of regulations.

The approach to fulfil compliance to licensing requirements, the achievement of nuclear safety goal, and performance objectives continued from the mid of 1970. This approach was cooperatively processed with the same recognition and needs in regulation and Utilities. In 1992, the NRC opened it position in a paper titled "Elimination of Requirements Marginal to Safety," July 24, 1992 (SECY92.263) **[27**]. The SECY paper that transmitted the final amendment to 10 CFR 50, Appendix J to add a performance-based option to the containment leakage testing rule. In 1993 Regulatory review Group (RRG) was formed to achieve a continuing regulatory improvement. Later on, both SECY94-090 ´´Institutionalization of Continuing Program for Regulatory Improvement, May 18, 1994´´and SECY96.134 ´´Options For Pursuing Regulatory Improvement in Fire Protection Regulations for Nuclear Power Plants´´ were published. In October 1996 the commission recognized modification and amendments in the some part of Appendix R for the regulatory improvement, and revision of 10CFR50.48 to accommodate the performance-based and risk-informed approach. SECY97-127 Development of a Risk-Informed, Performance-Based Regulation for Fire Protection at Nuclear Power Plants issued in June 1997 accelerated its direction towards a new rulemaking plan.

With intense and multiple effort by NRC, Utilities and the research institutions, in 1997, constituted a task force team to investigate and analyze the situation of the fire protection plan and program in nuclear power sites. It endeavored to develop guidelines and applicable methodologies with EPRI, and supported the nuclear power sites to introduce techniques and methodologies

In SECY-98-058, “Development of a Risk-Informed, Performance-Based Regulation for Fire Protection at Nuclear Power Plants,” dated March 26, 1998 **[28**], the NRC staff proposed to the Commission that the staff work with NFPA and the industry to develop a performance-based, risk-informed consensus standard for fire protection for nuclear power plants.

The intense regulatory improvement activities, a number of fire tests, systematic analysis for the operating experience, pilot experiments and overall analysis for the IPEEE **[29**] results executed by individual plant were implemented with the same intents and insights by regulation, utilities and research institutes.

The NRC´s "PRA Policy Statement” (60 FR 42622, August 16, 1995) **[17]** formalized the Commission's commitment to risk-informed regulation through the expanded use of PRA. The PRA Policy Statement states, in part, ´´The use of PRA technology should be increased in all regulatory matters to the extent supported by the state of the art in PRA methods and data, and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy¨ **[17].**

Consequently, on February 9, 2001, the performance-based fire protection standard for the Light Water Reactor was published and promulgated as an American National standard. Thus, the National Fire Protection Association (NFPA) published in 2002 of NFPA 805, “Performance-Based Standard for Fire Protection for Light-Water Reactor Electric Generating Plants” (2001 Edition) **[30**]. This is the upgrade of the American standard NFPA 803, which is the standard that covers the protection of LWRs from the consequences of fire, including safety of on-site personnel, protection of property and continuity of production. The NFPA 803 published in 1977 has been used as fire protection regulation, containing prescriptive requirements with deterministic methodology. However, performance-based approach relies upon measurable (or calculable) outcomes (i.e., performance results) to be met but provides more flexibility as to the means of meeting those outcomes

Subsequently, the NRC in July 2004, amended 10CFR 50.48, “Fire Protection,” to permit existing reactor licensees to voluntarily adopt the fire-protection requirements contained in NFPA 805 as an alternative to existing deterministic fire-protection requirements.

In May 27, 1988, a change in NRC policy to establish a retention period for records that licensees must maintain was added. Text clarifications were effected to clarify that holders of an operating license must have a fire protection plan. In June 20, 2000, change in policy to amend fire protection requirements to remove the requirement that penetration seal materials be noncombustible. The requirement was amended to add paragraph (c) so that a plant can adopt “Performance-Based Standard for Fire Protection for Light-Water Reactor Electric Generating Plants” (2001 Edition**)** **[30],** which provides a performance-based alternative to the existing prescriptive requirements. The introductory text to (f) was also amended accordingly to incorporate NFPA 805.

In 2000, the NRC implemented the Reactor Oversight Process, where safe-shutdown capability of licensees were inspected. The inspectors observed that many licensees had not upgraded or replaced Thermo-Lag 330-1 fire barrier material or had not provided the separation distance between redundant safe-shutdown success paths necessary to satisfy the requirements in Section III.G.2 of Appendix R to 10 CFR Part 50. Some licensees compensated for the lack of or degraded fire barriers by relying on operator manual actions that had not been reviewed and approved by the NRC through the exemption process in 10 CFR 50.12, “Specific Exemptions.” Other licensees misinterpreted Section III.G.1 to allow the use of operator manual actions in lieu of the means specified in Section III.G.2, although redundant safe-shutdown success paths were in the same fire area.

In 2001, the Electric Power Research Institute (EPRI) and NEI performed a series of cable functionality fire tests to advance the nuclear industry’s knowledge of fire-induced circuit failures, particularly the potential for spurious equipment actuations initiated by hot shorts. On the final report NEI considered “Spurious Actuation of Electrical Circuits Due to Cable Fires: Results of an Expert Elicitation” (Report No. 1006961) in May 2002 [31]. NEI considered the results of the testing in preparing an industry guidance document for circuit analysis, NEI 00-01, “Guidance for Post-Fire Safe-Shutdown Circuit Analysis” (Revision 2 issued May 2009) **[32**].

The lack of knowledge of the potential for certain types of circuit failure mechanisms led to the variety of interpretation with respect to circuit analysis. The cable fire tests performed by EPRI/NEI significantly increased the knowledge available to the industry and the NRC with respect to fire-induced circuit failures and their potential to cause multiple spurious actuations that could affect safe shutdown after a fire. The NRC staff resumed inspection of fire-induced safe-shutdown circuits in January 2005. The NRC staff issued RIS 2005-30, “Clarification of Post-Fire

Safe-Shutdown Circuit Regulatory Requirements” **[33],** to clarify regulatory requirements related to post-fire safe shutdown circuit analysis and protection. Revision 2 of this regulatory guide provides the current guidance on how a licensee may disposition circuit analysis issues. The enforcement discretion for circuit-related findings provided in EGM 98-002 ends 6 months following the issuance of this regulatory guide, as described in EGM 09-002, “Enforcement Guidance Memorandum—Enforcement Discretion for Fire Induced Circuit Faults,” dated May 14, 2009 **[34]**.

The commission´s fire protection requirements and guidelines consist of rules, generic communications, staff guidance, and her related documents. The current version of the 10 CFR 50.48, fire protection was issued January 1, 2008 and the recent industry and regulatory issues have prompted the NRC to update this comprehensive guide to provide additional clarification of regulatory expectations with respect to FPPs.

The overall maturity of fire protection regulations, the many years of nuclear plant operating experience, the improvement of analysis methodologies, and the opportunity to incorporate these benefits in the original plant design provide the bases for enhanced fire protection in new reactor designs.

4.2.2 NPP FIRE PROTECTION REVIEW IN USA.

The concept of fire protection in the United States of America entails the use of echelons of administrative controls, fire protection systems and features, and safe-shutdown capability. The primary objectives of fire protection programs (FPPs) at U.S. nuclear plants are to minimize both the probability of occurrence and the consequences of fire. To meet these objectives, the FPPs for operating nuclear power plants are designed to provide reasonable assurance, through defense-in-depth, that a fire will not prevent the performance of necessary safe-shutdown functions, and that radioactive releases to the environment in the event of a fire will be minimized. Nuclear power plant facilities take a defense-in-depth approach to protect against fires by creating multiple independent and redundant layers of protection to compensate for potential human and mechanical failures. Nuclear energy facilities have comprehensive fire protection systems, equipment and procedures to ensure safety as well as programs to manage combustible materials and ignition sources.

4.2.2.1 FIRE PROTECTION PROGRAM BEFORE 1975

During the initial implementation of the U.S. nuclear reactor program, regulatory acceptance of FPPs at nuclear power plants was based on the broad performance objectives of GDC 3 in Appendix A to 10 CFR Part 50. Appendix A establishes the necessary design, fabrication, construction, testing, and performance requirements for structures, systems, and components (SSCs) important to safety. GDC 3 addresses fire protection requirements and specifies, in part, that (1) SSCs important to safety must be designed and located to minimize the probability and effects of fires and explosions, (2) noncombustible and heat-resistant materials must be used wherever practical, and (3) fire detection and suppression systems must be provided to minimize the adverse effects of fires on SSCs important to safety. However, given the lack of detailed implementation guidance for this GDC during this early stage of nuclear power regulation, the level of fire protection was generally considered acceptable if the facility complied with local fire codes and received an acceptable rating from its fire insurance underwriter. Thus, the fire protection features installed in early U.S. nuclear power plants were very similar to those installed in conventional fossil-fuel power generation stations.

When the AEC was formed in 1947, it inherited the programs and facilities of the war time Manhattan Engineering District which had a crash program to develop an Atomic bomb. Many of the buildings were both substantially built and provided with automatic fire protection, this was generally the exception, rather than the rule.

The AEC continued the program of Universities and private corporation operation of the facilities, with the AEC personnel functioning as program and contract managers. Each field office had established a separate safety section by 1960 which includes professional fire protection engineers.

As result of the experience and background of the first generation of AEC fire engineers led to AEC´s first fire protection requirements goal, specifically stated as the improved risk´´ level of protection. While the fire protection deficiencies of the inherited buildings had not been cured, the fire protection system was able to respond quickly and proved its worth during the two Paducah fires.

By February 1, 1971 studies of the safety organizations within AEC were completed. A system of internal management audit of fire safety program were instituted at each major facility. Field office audits and in-depth inspections in the fire safety areas was strengthened. This deterministic approach of fire safety survey program was instituted by allowing independent fire safety inspections through insurance association and factory mutual research. The staff and the industry had system-based tools for considering fire risk, rather than today's more detailed, component-based information

Fire protection standards were instituted with definitive objectives such as ``to obtain and maintain a level of fire protection adequate to ensure that fires and related perils will not results in hazardous exposures of the public and employees.´´ **[22]**

Fire Research program at Lawrence Livermore Laboratory (LLL) was leader in early smoke test, using the Bureau of standards smoke chamber, and much of the work conducted by Gaskill is applicable today. Other laboratory in-house research resulted in computer design of Sprinkler heads, carbon microspheres as an extinguishing agent, high rack storage, and cooling tower protection systems.

Union Carbide´s Oak Ridge facilities developed a fire protection system for cable trays, consisting of bagged vermiculite placed on the trays.

Thus the AEC, which had been charged with regulation and promotion of the nuclear power industry, was replaced by the NRC (which inherited only the regulatory function) and DOE (which inherited the promotional function).

4.2.2.2 NRC FIRE PROTECTION PROGRAM

When the NRC was created, regulation of the nuclear power industry was based primarily on a set of deterministic rules. Those rules, including the ones related to fire safety, relied heavily on the design requirements for large, nonnuclear industrial facilities. They did not rely on quantitative safety evaluations, such as probabilistic risk assessments (PRAs). The NRC did not publish the first PRA, WASH-1400, “Reactor Safety Study—An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants,” **[6]** until October 1975.

Fire Protection Program for Nuclear Power Facilities Operating Prior to and after January 1, 1979 were based on defense-in- depth principles and the use of deterministic safety approach. The objectives were to: prevent the fire from starting; detect rapidly, control and extinguish promptly the fires that occur; and to provide protection for structures, systems, and components important to safety so that a fire that is not promptly extinguished by the fire suppression activities will not prevent the safe shutdown of the plant.

4.2.2.3 AN OVERVIEW OF DETERMINISTIC FIRE PROTECTION

The 1975 fire at one of the Brown Ferry Reactor in Alabama prompted the establishment of the deterministic fire requirements. The fire protection plan of every plant was to meet the requirements to outline the overall fire protection program. The fire protection system as well as the means to ensure safe reactor shutdown in the event of fire was paramount. The goal of the established plant fire protection program is to ensure that one of the several sets of safe shutdown systems will remain free of fire damage.

The safe shutdown equipment are separated by a barrier that protect one set from fire for 3hours and are at least 20 feet (6.1m) apart. In addition to that the safe shutdown equipment have automatic fire suppression and detection systems.

The approach to fire protection involves a multi-layered concept of defense-in-depth. The defense-in-depth fire protection concept involves prevention of fire starting; rapidly detection and control; and extinguishing promptly those fire that do occur. The last approach is mitigation by protecting the reactor’s ability to safely shutdown if a fire is not promptly extinguished. The overall fire protection of the USNRC can be summarized in the figure 4.2 below

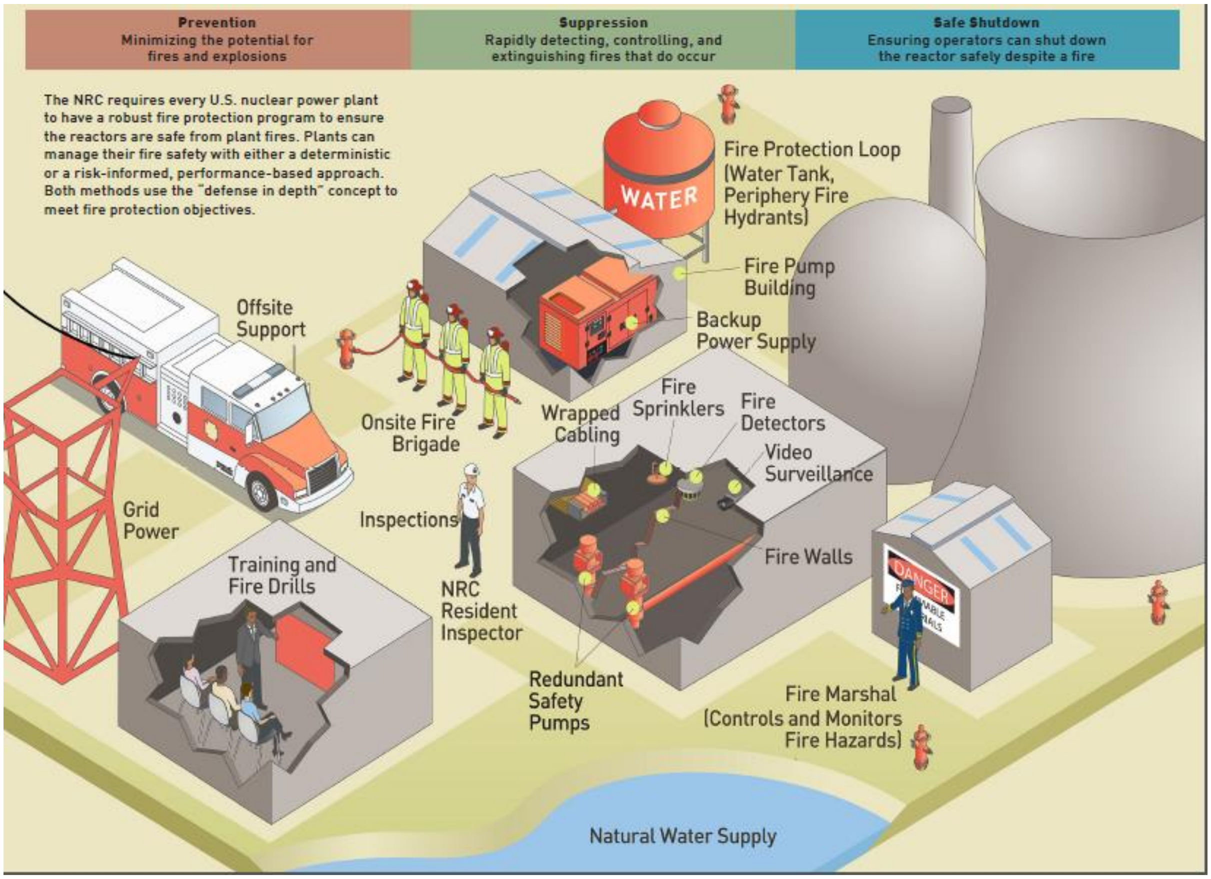

Prevention
Minimizing the potential for fires and explosions
Suppression
Rapidly detecting, controlling, and extinguishing fires that do occur
Safe Shutdown
Ensuring operators can shut down the reactor safely despite a fire
The NRC requires every U.S. nuclear power plant to have a robust fire protection program to ensure the reactors are safe from plant fires. Plants can manage their fire safety with either a deterministic or a risk-informed, performance-based approach. Both methods use the "defense in depth" concept to meet fire protection objectives.
WATER
Fire Protection Loop (Water Tank, Periphery Fire Hydrants)
Fire Pump Building
Backup Power Supply
Offsite Support
Onsite Fire Brigade
Wrapped Cabling
Fire Sprinklers
Fire Detectors
Video Surveillance
Grid Power
Inspections
Fire Walls
Training and Fire Drills
NRC Resident Inspector
DANGER
Redundant Safety Pumps
Fire Marshal (Controls and Monitors Fire Hazards)
Natural Water Supply

Figure 4.2 Summarized fire Protection program a typical NPP by USNRC [35]

PREVENTION: Combustibles and potential fire initiators are kept out of the plant as much as possible to reduce the chances of a fire. The prevention activities involves: fire marshal, NRC Inspectors, and training and drills. The fire marshals are NPP staff that monitor fire hazard such as the storage of combustibles and control ignition sources as well as metal cutting and welding. With the introduction Probabilistic Risk Analysis (PRA), gathering and recording of data on fire hazards at plant was instituted.

The NRC inspections are carried out by the resident inspectors on daily on plant activities and perform specific fire safety inspections every three months. Regional NRC inspectors inspect the plant's fire protection approach in depth every 3 years. Engineers and technical staff from NRC headquarters review plant changes to ensure that fire safety is maintained based on acceptable criterion.

The staff of the NPP are trained on fire safety through regular drills on responding to possible fires. The staff are also trained on mapping out the types of fire hazards at the plant and location of firefighting equipment in the event of a fire.

FIRE SUPPRESSION

Fire suppression involves rapid detection, control and extinguishing fires that are not prevented. The fire suppression system involves automatic fixed sprinklers, fire detection, onsite fire Brigade offsite support and fire protection loops. The fire protection loops involves fire pumps building and peripheral fire hydrants which pumps unlimited water from natural water supply such as Lakes, rivers and ocean.

According to Sandia National Laboratories' (SNL) Report by S.P. Nowlen **[36]**, fire incident data base provides insights into the detection and suppression of nuclear plant fires. These insights are associated with both the methods of fire suppression most commonly employed, and the time typically required to suppress fires.

For example, in the report for the nuclear power industry, by far the majority of fires are manually detected and manually suppressed. Manually detected fires outnumber automatically detected fires by approximately 5 to 1. Nearly all of the fires reported in the SNL data base have been suppressed by manual actions and in only a relatively few fires have automatic suppression systems played a role [Sandra]. These observations can be attributed to a number of factors.

First, the current USNRC regulations require the installation of automatic fire detection and fire suppression systems only in plant areas containing redundant trains of safety equipment. In practice, relatively few plant areas will meet this criteria, and thus, relatively few areas in most plants will be protected by such systems. (The implementation of fire protection varies widely between utilities. In practice one will find plants with extensive automatic detection systems and several fixed fire protection systems, while in other plants, one will find very few such systems installed.

Another related factor is that all nuclear power plant sites in the US are required to have, on site, manual fire response teams. These teams may be comprised of personnel drawn from plant security, maintenance, and operation staffs, or may be personnel dedicated to fire protection activities. This requirement tends to increase the reliance of utilities on their personnel to represent the first line of fire defense for most plant areas.

A third factor which tends to increase the ratio of manually to automatically detected and suppressed fires is that many fires are either caused by personnel actions or occur as a result of test and maintenance operations during which personnel are present in the immediate area. These fires are typically handled quickly by the personnel on the scene before any automatic measures might have become involved.

A final factor, is that plants, on occasion, have been reluctant to implement automatic fire suppression system due in large part to a significant history of adverse spurious fire suppression system actuation incidents. Nuclear power plants must be concerned with the continued safe operation of the reactor safety systems, and in some cases, it has been judged that an automatic fire protection system might represent a greater hazard that did the perceived fire hazard.

SAFE SHUTDOWN

Using installed equipment and procedures that reasonably ensure the reactor can shut down safely if a plant fire is not prevented or rapidly suppressed. The safe shutdown feature include backup power supply, redundant safety pumps, separation and fire walls, and wrapped cabling.

If the plant loses power from the transmission grid, reliable alternative power sources referred to as backup power such as diesel generators power equipment to safely shut down the plant. Plants also have diesel-powered fire pumps to supply firefighting water.

Redundant Safety Pumps are multiple sets of different pumps that can provide cooling water to keep the nuclear fuel safe. Fire protection programs separate these pump sets to keep them from being damaged by a single fire.

Fire walls separate sets of safety equipment, including pumps, into areas that would be impacted by a single fire. The walls are typically concrete or concrete block with fire-resistant sealant protecting the openings for pipes and cables.

Fire-resistant material protects cables for redundant safe-shutdown components located in one fire area. This material will have been tested to last 1 to 3 hours, depending on the application.

FIRE PROTECTION RESEARCH EFFORTS

The effectiveness of the Appendix R requirements in ensuring the availability of the plant's safety –related functions during a fire depended on the appropriateness of certain underlying assumptions. The assumption regarding redundant equipment separation (e.g., Electric cables); automatic suppression system; automatic fire detection systems; fire shield, barriers, and cable coatings; the flammability of older electric cable insulation; fire effects on safety-related equipment other than cables; and the use of low flame-spread cables in new installations. This called for research to ascertain and verify these assumptions.

The NRC started looking at research to ensure rapid improvement in fire protection knowledge and insights. The NRC started sponsoring a considerable number of research on fire-related issues. The first phase of NRC research span 1975-1987, which began with the Fire Protection Research Program (FPRP) and Other Fire-Safety-Related Activities. The next, 1987-1993, constitute Fire Research Program Conducted between Completion of the FPRP and Completion of the Risk Methods Integration and Evaluation Program (RMIEP). After the completion of RMIEP followed the 1993-1998 fire research. During this period, the NRC and the nuclear industry undertook projects to better understand issues identified through a number of paths, including inspection results, operational experience, fire PRA results, and fire research results. The results of those projects have benefited industry and NRC programs by improving the PRA method used for the NUREG-1150 and RMIEP PRAs and enhancing the data available to support its applications.

The goal of the Fire Protection Research Program (FPRP) 1975-1987 was to confirm the correctness of the underlying assumptions in Appendix R requirements. The research have shown that the effectiveness of redundant equipment separation for a small room where the effects of hot gas layers could become significant, a separation of 20 feet (6.1m) was not in itself sufficient to ensure that cabling so separated from the source of fire would remain undamaged. However, the additional test confirmed that the separation with the support of automatic fire detection and suppression the redundant equipment will remain undamaged.

The experimental program of the automatic fire suppression system have shown that all the suppressants; carbon dioxide, halon, and water-based sprinklers system could effectively contain fully developed cable tray fire when installed according to existing general industry practices. The test found that direct water spray suppression was the most effective system for extinguishing and preventing reignition of all fire sizes cable types and tray configuration. For gaseous system, the test showed that prolong soak times (15 to 20 minutes) at full concentration where necessary to ensure that deep-seated cable fires could be extinguished.

In 1983, the NRC significantly expanded the objectives of the FPRP to include developing test data and the analytical capabilities needed to determine NPP fire +risk, determining fire effects on control room equipment and operations, and determining the effects of suppression system actuation on safety equipment.

Arguably the most notable part of the above threefold program was the 25 large-scale fire tests (the "Fire Model Validation Tests") conducted by SNL. These tests collected data from fires with a range of fuels, fire intensities, fire locations, and ventilation conditions. The data supported fire model improvements programs as documented in NUREG/CR- 4681, "Enclosure Environment Characterization Testing for the Base Line Validation of Computer Fire Simulation Codes," issued March 1987 **[37]**; NUREG/CR-4527, "An Experimental Investigation of Internally Ignited Fires in Nuclear Power Plant Control Cabinets," Part I: "Cabinet Effects Tests," Volume 1, issued April 1987 [38]; and Part II: "Room Effects Tests," Volume 2, issued November1988 **[39].**

4.2.3 NPP FIRE SAFETY ASSESSMENT METHODS REVIEW IN USA

4.2.3. 1 EARLIER ATTEMPT TO NUCLEAR POWER PLANT RISK QUANTIFICATION

The early designers of nuclear reactors could not assure reactor safety through a quantitative, probabilistic approach, and AEC instead relied on deterministic design safety where probability were estimated qualitatively through engineering judgment. The probabilistic representation of risk associated with nuclear reactors have long thought by Government, industry and academia, to be useful to be quantified. The risk quantification approach would provide statistical frequencies estimating the probability of accident occurring. The U.S. Atomic Energy Commission (AEC) welcomed the early attempts at creating these quantification with much skepticism. The AEC were skeptic on risk quantification approach even though as the AEC support research to improve quantitative approaches to reliability and risk assessments, its regulatory staff were reluctant to accept the idea that probability analysis had matured enough to evaluate quantitative risk for reactor. This perhaps reflected a concern about the uncertainties inherently associated with PSA results, and that the analysis has a significant degree of subjectivity, since many of the inputs are based on judgment.

Nevertheless, in 1972, the AEC launched WASH-1400, The Reactor Safety Study, led by Norm Rasmussen of the Massachusetts Institute of Technology (MIT). WASH-1400 represented a watershed event for the development and use of risk assessment in the nuclear industry. The first report of WASH-1400 was produced in 1974. A team of over 50 contractors and AEC staff worked over 3 years to produce a draft of WASH-1400 in 1974. After Congress transferred authority to regulate nuclear power plants from the AEC to the newly established NRC in 1974, the NRC published the final report in October 1975. WASH-1400 demonstrated that PRA could offer new, important, and actionable insights that benefit reactor safety **[6]**. The goal of WASH-1400 was to identify every single accident sequence that matters and evaluate its probability and estimate the

Core Damage (CD) frequency or the probability of release into the containment into the offsite environment. The safety community did not think that such analysis was possible and had no confidence that all the possibilities could work out because of lack of the supporting data. The historical development of PRA in USA is summarized in Figure 4.3 below

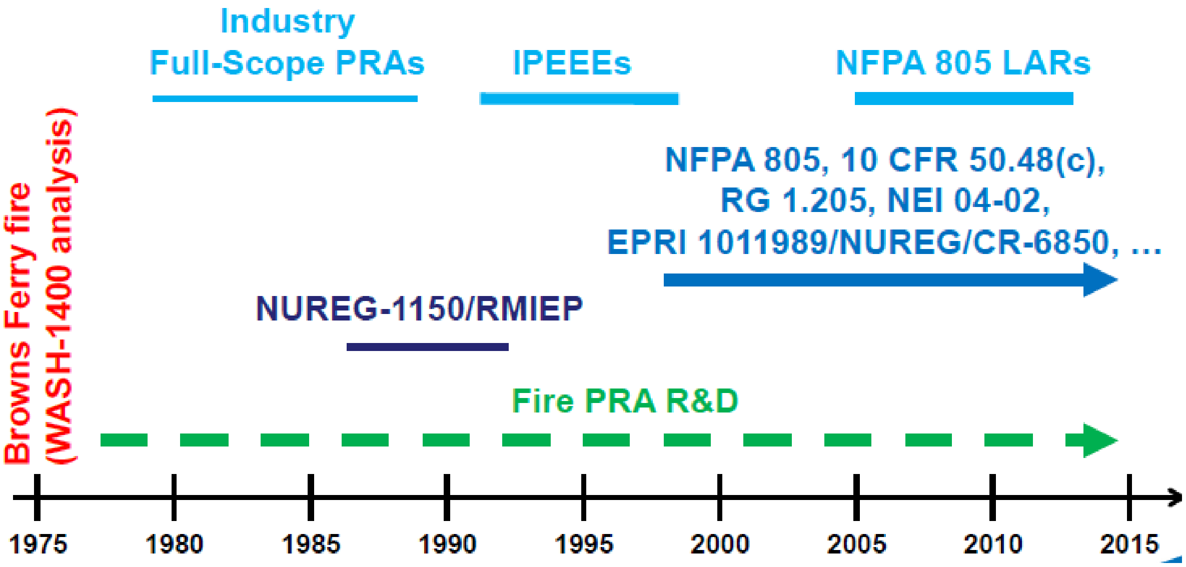


Figure 4.3 summarized historical review of fire safety at NPP in USA

4.2.3.2 THE IMPACT OF WASH-1400 ON REACTOR RISK QUANTIFICATION

In April 1977 NRC assembled a panel of seven experts to review WASH-1400. The group is chaired by Professor Hall Lewis of department Physics at University of California. The group was known as “Lewis Committee’’ and their report known as “Lewis Report”. The Lewis Committee focused on understanding WASH-1400 and its applicability to nuclear power plants regulation, as well as scrutinizing the models used. The terms of reference of the review group was to provide an advice and information on the final report of the Reactor Safety Study, WASH-1400. This advice and information will assist the Commission in establishing policy regarding the use of risk assessment in the regulatory process, in improving the basis for the use of such assessments. It will also clarify the achievements and limitations of the Reactor Safety Study.

The Lewis Committee praised the usefulness of fault trees. However, while praising WASH-1400, the Committee also criticized the overly optimistic executive summary which overstated the implications of main report. The following issues were raised in the Lewis Committee Report on WASH-1400:

- The accuracy of the weather (dispersion) model was suspect.
- Unrealistic evacuation schemes were overly optimistic and could have led to a favorably lower fatality rate.
- Earthquakes, fires, and human error were not considered appropriately when determining overall risk.
- Accidents were considered only for the case of the plant running at full power.

Finally the WASH-1400 'the Reactor Safety Study' studied only internal events at full power. Subsequently, industry and NRC studies to include external events such as fire, earthquake and flooding. PRA related to fire became of much interest after the 22 March, 1975 Brown Ferry nuclear power plant fire. This fundamentally changed how the NRC dealt with fire protection at U.S. nuclear power plants.

4.2.3.3 FIRE SAFETY ASSESSMENT AFTER BROWN FERRY FIRE ACCIDENT

Historically, Probabilistic Safety Assessments (PSA) were originally developed in order to calculate the probability of external events such as an aircraft falling onto a given target. PSA techniques were subsequently used to develop scenarios for hypothetical accidents that might result in severe core damage, and to estimate the frequency of such accidents. The first study of this kind carried out in the United States was published in 1975 (Rasmussen report) and provided the first assessment of the potential risk of core damage for two power reactors.

The early applications of risk analysis to nuclear power plants, including that presented in the draft report of the Reactor Safety Study (RSS), did not include a quantitative assessment of accidents initiated by major fires [21]. The reason for this omission was twofold:

(1) It was judged that fires were not likely to be dominant contributors to risk (RSS final report--USNRC, 1975) and (2) the state of the art in risk analysis had not yet developed an approach to covering fires.

The original quantification of core-damage risk at an NPP (WASH-1400, October 1975) only included events initiated by plant system and component faults, where the cause of failure was internal to the failed items (such events are called "internal events"). It did not include events initiated by earthquakes, floods, and fires, where the cause of failure is external to the failed items (such events were called "external events"). However, because of the fire at BFN in March 1975, the first fire PRA was performed in 1975 as a supplement to WASH-1400.8 Its results provided a quick estimate of the risk implications of that fire, indicating that the CDF associated with the BFN fire was about 20 percent of the CDF due to the non-fire-related events that were addressed in the main body of the WASH-1400 study. It also recommended the development of a more detailed fire PRA method using improved models and data.

Consequently, when internal events were later quantified for six additional NPPs, three quantifications also included events caused by fires. The quantifications that included fire risk were Peach Bottom Unit 2 and Surry Unit 1, under the NUREG-1150 program, and LaSalle Unit 2, under the RMIEP program, NUREG/CR-4832, "Analysis of the LaSalle Unit 2 Nuclear Power Plant: Risk Methods Integration and Evaluation Program (RMIEP)," Volume 9: "Internal Fire Analysis," issued January 1990 [40]. The basic framework of the fire-risk quantification method applied in NUREG-1150 and RMIEP studies represented a milestone that has since become the accepted framework for conducting a "state-of-the-art" NPP fire-risk analysis. The framework is based on the full internal events PRA, with its event trees and fault trees providing consistency with respect to the internal events analysis, including the full gamut of random, test, and maintenance-related unavailabilities. This same framework is used in the currently recommended (2008) method presented in NUREG/CR-6850 (EPRI 1011989), "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities," issued September 2005 [41].

Also, the early applications of risk analysis to nuclear power plants was purely based on deterministic approaches. The analyst was to determine how well the defense in depth approaches of fire prevention, suppression and mitigation are working.
In a nuclear facility, as in any industrial plant, risk assessment distinguishes between the potential hazards that might be encountered in the absence of any protective measures, and the residual risks that will still remain despite the measures taken. The problem lies in assessing the latter, since there is no way of ensuring that they have been completely eliminated. The insight to the latter is provided by PSA methodology providing potential initiators of multi-system failures.

The importance of fire as a potential initiator of multiple-system failures took on a new perspective after the cable-tray fire at Browns Ferry in 1975. Although various experts have disagreed as to how close that fire came to an accident resulting in core damage and a major release of radioactive material, it is clear that its impact was extensive when measured in terms of the failure of redundant and diverse safety-related systems. It is not surprising, therefore, that risk analyses performed after the Browns Ferry fire have tended to include fires in the quantification of risk.

More so, one of the first attempts at numerically estimating the risks due to fires appeared in the final report of the Reactor Safety Study, published later in the same year (1975) as the Browns Ferry fire. An estimate was made of the conditional probability of core melt given the specific damage state induced in the Browns Ferry systems by the fire (USNRC, 1975). The unconditional frequency of fire-induced core melt, calculated by averaging out the observed frequency of the Browns Ferry type of fire over the experience of U.S. commercial nuclear power plants, was found to be 1×10^{-5} per reactor-year, which is about 20 percent of the total core-melt probability estimated in the Reactor Safety Study. Kazarians and Apostolakis (1978) **[24**] performed the same type of calculations under different assumptions and concluded that the frequency of core melt could be higher by a factor of 10. Both of these analyses appropriately point out that the results apply only to the specific circumstances of one particular fire and should not be construed as an estimate of the total contribution of fires to risk.

A more detailed risk analysis of fires was included in the USA´s Clinch River Breeder Reactor (CRBR) Risk Assessment Study (1977) **[5**]. A failure modes and effects analysis was used to identify important fire locations for a wide variety of combustibles, including cables, oil, and sodium. Its estimate of the frequency of fire-induced core melt, 5×10^{-7} per reactor year,

4.2.3.4 RESEARCH AND DEVELOPMENT IN THE FIRE RISK ASSESSMENT METHODOLOGY

Fire safety assessment slowly evolve as history proceeds, changing from the use of deterministic, qualitative research methods to more quantitative PRA-informed methods. The NRC formalized this trend toward the increased use of quantitative methods in NPP regulations to complement the deterministic approach and supports the NRC's traditional defense-in-depth philosophy.

A number of research activities for U.S. nuclear regulatory commission for various aspect of fire risk for light- water reactor has been carried out. Gallucci's doctoral dissertation work (1980) **[42]** at Renssenlaer Polytechnic institute, nuclear plant data were analyzed and categorized in the HTGR study. The source of data extended beyond licensee event reports to include insurance company records, and therefore the sample size was somewhat larger. The result was a more complete data base, particularly with regard to fires during construction. Gallucci (1980) developed a risk-analysis methods and applied it to a representative design for large BWR. The probabilistic aspects of fire propagation were modeled in terms of an event tree that explicitly models various stages of ignition, detection, suppression, and propagation. The frequency of core damage due to fires was estimated to be about 2 x 10^{-4} per reactor-year, with an upper bound of about 1 x 10^{-3} per reactor-year. In this study, three types of combustibles at each of 11 plant locations were analyzed in the quantification of risk. **[5]**

Apostolakis, Kazarians, and Siu **[43]** in project carried out at University of California at Los Angeles made advancements in the risk analysis of major fires. Specific advancements in this work include the development of a physical model for fire propagation and suppression, a method for propagating uncertainties through this model, and the use of Bayes' theorem in estimating plant-specific and location-specific fire-occurrence frequencies. Using the advances resulting from Apostolakis et.tal research, the Zion, Indian Point, and Big Rock Point plants studies have included detailed analyses of fire-induced accident sequences.

Also, in parallel with the FPRP, the NRC sponsored a project to develop a fire PRA methodology at UCLA, with supplemental efforts at RPI and BNL. The resulting methodology was used to conduct a number of industry-sponsored fire PRAs, including those at Zion and Indian Point, which then received intensive NRC-sponsored reviews at BNL and SNL. Those industry-sponsored fire PRAs were thus the first to apply the UCLA-developed framework, which was later used in NRC-sponsored fire PRAs, including the RMIEP (LaSalle) and the plants in NUREG-1150, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants **[24, 16**]. A number of industry-sponsored PRAs, including those at Zion (1981) and Indian Point (1982), used the UCLA-developed approach, which showed that fire could be an important contributor to CDF and risk because of its potential to act as a failure mechanism affecting multiple trains of equipment.

For example, the Apostolakis team developed and demonstrated an approach that integrated the predictions of a deterministic computer model for fire behavior (i.e., COMPBRN, developed by N. Siu at UCLA **[44]** into the assessment. The team accomplished this integration through the use of a competing-risks framework that computed the probability of fire damage to equipment (including electrical cables) as the outcome of a "race" between two simultaneous processes, fire growth and fire suppression. For instance, Rensselaer Polytechnic Institute (RPI) developed a methodology for evaluating the probability for loss of NPP safety functions because of fire. It established a framework for investigating fire scenarios that modeled fire development through its stages of ignition, detection, propagation, and suppression. RPI applied the methodology to a generic, or representative, boiling-water reactor (i.e., the plant characteristics assumed did not represent any specific plant) and obtained conservative estimates of core-damage probabilities from postulated fires. The RPI study also discussed variations in the methodology for application to specific plants.

During the period of 1993-1998 after completion of RMIEP, Inspection results, operational experience, fire PSA results and fire research results have benefited industry and NRC programs.

These helped to better understand issues identified through a number of paths in the research conducted. The results of these projects was beneficial by improving the PSA methods leading to the development of the NUREG-1150 and RMIEP PSA’s and enhancing the data available to support its application.

The research activities resulted in further recommendation work to include tests to investigate the smoke effects on higher voltage alternating current (AC) equipment, such as switchgears. This has become imperative because the research work carried out tests predominantly involved low-voltage direct current (DC) digital circuits and showed that, in addition to the immediate effects of airborne smoke, a possible latent effect exists from the buildup of soot-like deposits on digital microelectronic circuits. These deposits could cause circuit failures even well after the fire is extinguished, including during the venting and purging period. Data of these failures needed to be included in Fire PRA of the nuclear power plants.

Furthermore, to support the policy of increased use of PRA in regulatory, in 1998, the RES staff initiated a new part of its fire research program to address gaps in the ability to perform realistic fire PRAs. After organizing expertise in PSA, fire-risk analysis, fire protection and fire safety from NRC offices, other Government agencies, Universities, nuclear industry groups and several NPP licensees, four tasks were identified. The four tasks were: [24]

1. Tools for Circuit Failure Mode and Likelihood Analysis.
2. Tools for Fire Detection and Suppression Analysis.
3. Fire Modeling Toolbox
4. Experience from Major Fires

As work progressed on the initial tasks, it was decided that the requantification effort would be merged with work then underway by EPRI to improve fire PRA methods and data. This cooperative combined requantification resulted in the development of the joint NRC/EPRI fire-risk methodology described in NUREG/CR-6850 (EPRI 1011989) [**41**]. The NRC published details of the data search, fire testing, and improved fire PRA method in NUREG/CR-6834, “Circuit Analysis—Failure Mode and Likelihood Analysis,” issued September 2003 [**45**]. The tools for fire detection and suppression analysis task resulted in development of the fire detection and suppression method recommended in NUREG/CR-6850 (EPRI 1011989**)[41**] that includes the use of historical evidence regarding fire duration gleaned from fire events, combined with the use of fire brigade response times demonstrated by unannounced fire drills.

Experience from major fires task was to gain new methodology insights from actual NPP fire incidents worldwide. The review concluded that the overall structure of current fire PRA methods can appropriately capture the dominant factors involved in a fire incident. However, the review identified several areas of potential improvement to current methods. One improvement would more realistically consider the effects of smoke propagation on plant operators and fire fighters, which could lead to event sequences otherwise considered very unlikely. The review also identified a few factors that fell outside the scope of current fire PRAs, including the occurrence of multiple initial fires or secondary fires, multiple simultaneous initiating events, and turbine blade ejection events that could simultaneously result in fires caused by significant releases of flammable lubrication oil and hydrogen, mechanical damage from blade debris (such as severance of pipelines), and flooding (e.g., damage to water lines containing river water). The detailed results and insights were published in NUREG/CR-6738, "Risk Methods Insights Gained from Fire Incidents," in September 2001 **[46].**

The insights provided the confidence that no significant revisions were needed to the general fire PRA approach currently being used and that improvements could be incorporated through more readily accomplished changes to specific fire PRA elements.

The National Fire Protection Association (NFPA) publication in 2002 of NFPA 805, "Performance-Based Standard for Fire Protection for Light-Water Reactor Electric Generating Plants" (2001 Edition) **[30];** and the NRC's subsequent July 2004 amendment of 10 CFR 50.48, "Fire Protection," to permit existing reactor licensees to voluntarily adopt the fire-protection requirements contained in NFPA 805 as an alternative to existing deterministic fire-protection requirements called for Improving Fire Modeling—Verification and Validation. In May 2007, "Verification and Validation of Selected Fire Models for Nuclear Power Plant Applications," NUREG-1824 (EPRI 1011999) **[47]** was issued.

Risk-informed involves the use of quantitative risk assessment (QRA) evaluation tools and techniques (e.g., event trees, fault trees) in conjunction with traditional fire protection engineering methods and deterministic fire modeling tools. This quantitative information provides input for making informed decisions regarding fire and explosion risk impacts and cost-effective strategies for risk reduction.

Performance-based fire protection is a quantitative, probabilistic measure of fire protection success based on functional performance requirements derived from specific scenario and risk tolerance criteria. Performance is evaluated by response effectiveness, online availability and operational reliability, within an event tree risk model on a conditional probability basis.

In 2001, EPRI and RES embarked on a cooperative project to improve the state of the art in fire-risk assessment to support the new risk-informed environment in fire protection. The report developed a process for identification and inclusion of post fire human failure events (HFEs), a methodology for assigning quantitative screening values to these HFEs and the initial considerations of performance-shaping factors and related fire effects that may need to be addressed in developing best-estimate human error probabilities (HEPs). However, the description of the methodology to develop these best-estimate of HEPs, given the performance-shaping factors the fire-related effects was not detailed.

In 2007, EPRI and RES developed explicit guidance for estimating HEPs for HFEs under fire-generated conditions, building on the existing human reliability analysis (HRA) methods. The progress regarding development and testing of that fire HRA methodology includes addressing the range of fire procedures used in existing plants, the range of strategies for MCR abandonment, and the potential impact of fire-induced spurious electrical effects on crew performance. A detailed fire HRA scoping quantification approach to allow derivation of more realistic HEPs than those in the screening approach have been developed.

In October 2007, the NRC issued NUREG-1852, “Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire,” [48] which addresses the unique aspects of fire and associated operator manual actions. The report suggested a criteria for determining whether operator manual actions—proposed by operating plants for use in achieving and maintaining hot shutdown are feasible and can be performed reliably in response to fire.

In 2008, an industry report addressing early lessons learned from efforts to support the implementation of NFPA 805 [30] stated that, the current fire PRAs being developed in consistent with NUREG/CR-6850 have more systematic modeling conservatism than the more mature internal events PRA evaluations. In 2010, the Nuclear Energy Institute (NEI) provided a report supporting its view that fire PRAs performed using EPRI 1011989/NUREG/CR-6850 and its supplement are conservative [41]. The report stated clearly that it has become evident to the industry practitioners that:

• The manner in which fires are characterized does not conform to operating experience;

• The level of quantified risk is overstated, as compared to operating experience; and

• There is an unevenness in the level of conservatism in the results that can mask key risk insights and result in inappropriate decision-making.

In 2011, an ACRS report on the current state of NFPA 805 implementation **[49, 50**] first cautioned about generalized labels, stating:

“…contentions that the basic fire analysis concepts and methods are ‘immature’ are an over-simplification. The guidance in NUREG/CR-6850 consolidates advancements in fire analysis methods and knowledge that have evolved over the last 25 years. In some cases, those advancements are rather substantial.”

Furthermore, in 2013, NEI’s letter to NRC **[50, 51**], identified a number of impediments to the advancement of risk informed regulations, specially referring to the ‘’chilling effects’’ of issues arising in the implementation of NPFA 805, including:

“…untested PRA fire methods laced with conservatisms in the required fire-risk analyses… [resulting in] fire PRAs … not consistent with operating experience.”

It is recognized that fire PRA concerns continue to shape industry and NRC discussions aimed at improving risk-informed regulation and that fire PRA is likely to play a major role in NRC’s ongoing Level 3 PRA project [50 52], it is believe that the effort to document the understanding of maturity and realism of the current fire PRAs is timely and a continuous process.

4.3 HISTORICAL NPP FIRE SAFETY EVOLUTION IN GERMANY

4.3.1 NPP FIRE SAFETY REGULATIONS EVOLUTION

In the early designs of nuclear power plants in Germany fire events were not identified according to its actual risk for nuclear safety as happened in United States. Though, in the early years of the design and operation of nuclear power plants, design and regulations have always considered fire safety to some extent. However, nuclear specific requirements and standards related to fire protection were not fully developed. Regular industrial fire protection standards were adopted and only somewhat altered to ensure that radiological release was kept within the plant. Nuclear power plants had to meet applicable building codes and standards - the same which were used for other types of industrial facilities and even for office complexes. These non-nuclear regulations contain national and international industrial standards, laws and ordinances for building constructions as well as for fire brigade management and equipment, and ordinances regarding the work place safety. In addition, usually general design criteria and/or safety criteria had described general requirements for fire prevention, detection and response.

However, the fire at the Browns Ferry nuclear power plant in 1975 and the development of the general defense-in-depth concept for nuclear power plants have resulted in an improved fire protection strategy. This calls for fire safety regulations as an integral part of nuclear power plants safety regulations in order to protect the health and safety of the public from the potential consequences which a fire may have on nuclear safety.

In Germany the legal basis for the licensing of nuclear power plants and other nuclear installations is the Atomic Energy Act and the mandate for preparing nuclear safety standards is given to the KTA (Nuclear Safety Standards Commission) which was founded in 1972. The KTA has restrictive procedures to definitely ensure consensus principles and was not in a position to approve comprehensive fire safety relevant standards until 1975.

The commission of the KTA consist of 50 members. Representatives of 5 groups with 10 persons each, who met in former times three time a year, nowadays only once a year. The groups are (1) the manufacturers and vendors of nuclear facilities, (2) the operators/utilities of nuclear facilities, (3) the state licensing authorities and the federal authorities that supervise them, (4) the safety reviewing and advisory organizations and last but not least (5) the other authorities, organizations and institutions dealing with or involved in nuclear technology. The 50 members are nominated for a period of 4 years, the board consists of 5 persons, one of each group. The principle is that the partners cooperate as equal partners and make their decision by consensus. All decisions which are directly related to the establishing of standards must be agreed to by five-sixths of the members who participate in the individual full session of the KTA. This procedure shall ensure that no one of the five groups can be outvoted when a decision has to be taken. Each standard is first published as a draft standard and the public is invited to comment on it within a period of 3 months. Comments received are discussed and taken into account, as appropriate, before then the final version is established and published by the German Federal Minister of the Interior in Federal Gazette **[53].**

The preparation of the safety standards is not done by the 50 members of the KTA, but by working groups and supervising subcommittees. They are supported by a scientific technical secretariat. The working group members are experts in the fields of interest and are nominated by the different institutions and companies belonging to the 5 groups of the KTA. The members of the subcommittees are nominated by their institutions, but in addition officially appointed by the KTA. Subcommittees have to supervise and coordinate the activities of the working groups which report to them. The draft standards prepared by the working groups are reviewed by the subcommittees before submission to the KTA. If necessary, the drafts are referred back to the working group and further discussion is initiated. Subcommittees generally have also to review comments received from the public after the publication of the draft standard and generally have to prepare the final version of the standard. It can be said that developing a KTA safety standard is rather complicated and slow.

In November 1975, ´´the fire protection in Nuclear Power Plants´ standard KTA 2101 was established by KTA. It has three parts namely; Part 1: Basic Principles; Part 2: structural Elements; Part 3: Mechanical and Electrical Components,

The commission decided to establish uniform fire protection requirements for nuclear power plants and to harmonize the different licensing activities in the various fields and responsibilities involved. The need for the promulgation of this standard was greatly influenced by the Brown Ferry nuclear power fire accident in the United States in March 1975.

However, the issue of fire protection in addition to its nuclear implication is an important part of different conventional building laws, which in Germany are per definition independent state laws. Therefore, these independent state laws unlike the Atomic Energy Act, are not governed by federal laws. Hence, time consuming discussions have been necessary to harmonize the different strategies between different authorities to reach consensus.

It took a decade before KTA 2101.1 "Basic Principles of Fire Protection in NPPs" (December 1985) **[53]** was published as valid safety standard. The theoretical concept for the combination of plant-internal and –external events with consequential and related fires, which was drafted in KTA 2101.1, was absolutely new and had to be explained during many discussions. For a fire protection engineer it was at that time strange to think about design principles for fires in combination with other extremely seldom events.

KTA 2101.1, ´´Fire protection in Nuclear Power Plants; Part 1: Basic Principles" treat all relevant issues such as basic design-philosophy including the special protection of safety relevant features, the overall-postulate of fires in case of the existence of burning material and the consideration of consequential and unrelated fires with plant-internal and -external events as well as basic design requirements for structural and equipment related fire protection measures and operational fire protection measures and tests and inspections.

With reference to structural measures, it states that basically incombustible construction material shall be used, that fire zones shall be created inside the structures and that the fire resistance rating of walls and ceilings of fire zones shall be at least 90 minutes. Special considerations are included for closures of openings in fire qualified walls and ceilings.

Also, requirements for equipment related fire protection measures refer to the special situation inside containment, the design principles for fire alarm and fire suppression systems, for smoke and heat removal as well as for fire protection measures for ventilation systems and off-gas systems.

With reference to the issue of tests and inspections for example details for tests prior to the granting of a construction or assembly license are to be seen as well as for the supervision of the construction and for tests prior to the commissioning of the NPP and after major repairs and modifications are stipulated by KTA 2101.1 fire protection in NPP basic principle standard.

In November 1976 there was an additional KTA-decision to complement the safety standard set KTA 2101, ´´Fire Protection of Nuclear Power Plants" by the standard KTA 2102, which should deal with, ´´Rescue Routes in Nuclear Power Plants" which is a very important fire protection issue to ensure primarily personnel safety as indicated in conventional building laws, but could not be materialized. This was not possible due to the fact that five-sixths of the members who participate in the individual full session of the KTA could not agree. Therefore, the harmonization of different states laws is time consuming at the different strategies between different authorities to reach the goals.

KTA 2102 was published as draft safety standard in June 1990. Comments especially from representatives of the German official body, responsible for life and health of working people in general, have led to a revision of the paper, for which the commission of the KTA was asked for official approval as safety standard in 1992. Up to now no 5/6 consensus was possible within the commission of the KTA in order to publish it as a valid safety standard. Especially since 1992 the operators of the German nuclear power plants argue about the question whether it makes sense to integrate issues of the conventional building code in nuclear safety standards. In this context it is worthwhile to know that in Germany in the sphere of influence of conventional building laws there is an inventory protection for the owners of a building, which does not exist in nuclear facilities where normally the actual state of science and technology form the basis for licensing procedures. This is also the reason why KTA 2101.2 was not published as official safety standard up to now.

After years of deliberations the second edition KTA 2101.1 was issued in December 2000, revised in 2005 and the latest edition was issued in November 2015.

Moreover, the provisions on structural elements; mechanical and electrical components; KTA 2101.2 and KTA 2101.3 were finalized and issued in December 2000. The revised versions were issued in November 2015. Apparently these standards provide the technical detailed designs for fire safety and needed time.

The updates in German nuclear fire safety standards of the German Safety Standards Commission is to enhance and harmonize all the three parts of KTA 2101 which are interrelated. The structures are harmonized to provide the fundamental requirements in part 1 and the technical details for design and operation of structures, systems and components with respect to fire safety in part 2 and 3 accordingly, avoiding duplications.

Major goals of the update of KTA 2101, Parts 1 to 3 were the following: [**54**]

- Updating requirements to the actual state-of-the-art:
  - corresponding to the most recent, also non-nuclear standards and norms,
  - providing specific compliance with requirements regarding the fire brigade,
  - considering low power and shutdown plant operational states better and more systematically,
  - addressing the fire hazard analysis explicitly and in a systematic way,

  - considering nuclear specific deviations from non-nuclear standards and norms with regard to escape and rescue routes,
  - Covering event combinations of fires and other anticipated events more systematically as a lesson learned from the Fukushima Dai-ichi reactor accidents in 2011.
- Compliance with the (new) “Safety Requirements for NPP” [34] in respect of the following aspects:
  - Better consideration of the defense-in-depth concept, including specific compliance with requirements for the safety demonstration, in particular requiring a fire protection concept (sometimes in the international framework also called fire protection program) and a systematic and comprehensively documented deterministic fire hazard analysis (FHA) being kept up to date,
  - a more systematic approach and outline of the standards covering nuclear specific requirements and deviations from non-nuclear standards and norms,
  - a systematic and comprehensive consideration of event combinations of fires with other anticipated event that have to be assumed, either occurring as consequence of the initial event or if their occurrence at the same time has to be accounted for due to their occurrence frequency and the extent of damage. In this context, the following event combinations have to be considered:
    - Combinations of causally related events:
    - Fire and consequential event,
    - Anticipated event and consequential fire,
    - Fire and independently occurring anticipated event.

Sections of KTA 2101.1 have been formulated more precisely or new requirements have been added for consistency with international requirements, in particular from IAEA and WENRA.

A section on applications of the standard provides precise guidance on the goals of the standard KTA 2101.1. One of the most important changes section ´´3.3 Combinations of Fires with other Anticipated Events´´ **[54]** in the standard affects the protection against combinations of fires and other anticipated events.

For KTA2101.2 the update follows the demands of the KTA (General Assembly), in particular for:

- Adapting references and definitions to up-to-date standards and codes,
- Updating and enhancing the requirements in order to make them consistent to up-to-date national as well as international standards and codes,
- Updating in particular the technical requirements for structural components to the state-of-the-art,
- Harmonizing this part of the standard KTA 2101 with the other two parts, KTA 2101.1 and KTA 2101.3.

In the KTA 2101.2 **[53**], specific requirements for structural components are provided. This covers in detail the followings topics:

  - Design of structural fire protection means,

- Location and accessibility of nuclear power plant buildings,
- Fire compartments and fire sub-compartments
- Structural elements enclosing fire Compartments and fire Sub-compartments (fire barriers),
- Escape and rescue routes,
- Ventilation systems, heat and smoke removal systems and components

In an informative appendix (Appendix A) a simplified validation approach for determining the fire resistance rating of structural elements is provided.

The requirements for design of structural fire protection means; location and Accessibility of nuclear power plant buildings; fire compartments and sub-compartments; structural elements enclosing fire compartments; escape and rescue routes; and ventilation systems, equipment for heat and smoke removal were included in KTA 2101.2. This accomplish the initially intended standard KTA 2102, which should deal with, ´´Rescue Routes in Nuclear Power Plants".

The recent update of KTA 2101.3 (2015-11) [54] follows the demand of modifications prepared by the KTA (General Assembly), in particular for:

- adapting references and definitions to up-to-date standards and codes,
- updating and enhancing the requirements in order to make them consistent to up-to-date national as well as international standards and codes,
- updating in particular the technical requirements for extinguishing systems according to the state-of-the-art,
- reviewing the requirements for heat and smoke removal systems, in particular with respect to access and escape routes,
- including precise technical requirements for storage of pressurized gas cylinders, and
- Harmonizing this part of the standard KTA 2101 with the other two parts, KTA 2101.1 and KTA 2101.2.

Moreover, the following general adaptations have been considered:

- Moving more general requirements from KTA 2101.3 to KTA 2101.1 or KTA 2101.2 or more technical requirements from KTA 2101.1 to KTA 2101.3 as far as suitable and avoiding duplications,
- Enhancing and harmonizing the wording of performance based requirements between the three parts of KTA 2101 and considering other fire protection standards and codes,
- Deleting definitions as well as requirements from this standard, if already well-established and regulated in the non-nuclear fire related building codes and standards.

The structure of the contents in the part 3 of the standard KTA 2101 has been slightly adapted accordingly resulting in the following main paragraphs: Fundamentals; Scope; Definitions; Fire Protection Measures for Mechanical Components and Systems; Fire Protection Measures for Electrical Facilities and Arrangements; Facilities for Fire Detection and Fire Alarm; Facilities for Fire Suppression; and Ventilation Systems, Facilities for Smoke and Heat removal.

The Federal Office for Radiation Protection (Bundesamt für Strahlenschutz – BfS) publishes several laws and regulations on nuclear safety and radiation protection. ´´The safety Requirements for Nuclear Power plants´´ **[55]** issued as of 22 November 2012 and Federal Gazette (BAnz AT 30.03.2015 B2.) on 24 January 2013. The amended and revised version was published on the 3 March 2015

Section of the requirement for safety demonstration indicates that deterministic methods as well as the probabilistic safety analysis shall be applied to demonstrate that technical safety requirements are fulfilled. This shows that probabilistic Safety assessment can be used to supplement deterministic approaches to demonstrate the fire safety of the nuclear power plants. Though, no standard on the use of PSA has been issued, but internationally accepted and locally developed guides are used.

4.3.2 NPP FIRE PROTECTION REVIEW IN GERMANY

The fire safety standard was developed after construction of the first generation of Germany Nuclear power Plants in accordance with the worldwide progress of safety culture and industrial fire protection requirements for NPPs. Three ´´generations´´ of NPPs can be distinguished in Germany with regards to the fire protection concepts at the start of operation.

The fire protection measures of the first generation of NPPs were designed according to the general fire safety requirements for buildings and industrial plants. They were not subjected to requirements derived from nuclear safety as a result of non-recognition of fire as nuclear safety risk. The fire protection concepts of the first generation NPPS are characterized by the following features:

- Design according to conventional fire protection requirements
- No physical separation of safety systems´ redundancies
- High importance of fire extinguishing

The second generation plants were under construction when the significance of fire protection measures for nuclear safety was recognized. This resulted in substantial improvement of the fire protection concept before completion, whereas the oldest plants undergone upgrade after the beginning of commercial operation. Their fire protection were characterized by:

- Partial physical separation of safety systems´ redundancies
- Fire barriers for areas or rooms with high fire loads
- Stationary fire extinguishing system in areas with safety related system or higher fire loads

The third generation of plants were designed and constructed according to the safety standard KTA 2101. They are featured by the following characteristics:

- Designed according to KTA 2101 safety standards
- Physical separation of safety systems´ redundancies
- All fire barriers with a fire resistance rating of 90 minutes
- Stationary fire extinguishing systems in compartment with high fire loads.

Consequently, two main aspects of fire protection concepts has been developed:

- In the parts of the plants fire protection is based on upgraded passive, active and administrative fire protection measures
- Independent emergency systems in separate buildings provide for the functions lost due to a fire damaging more than one redundancy

In this context, the importance of independent emergency systems in the case of large fire is more considerable for the first plant generation. **[54]**

Incidents and accidents have shown that fires at nuclear power plants cannot be precluded. Combustible materials, such as lubricants or cable insulations, and potential ignition sources are contained in the plant. Consequently, measures for the minimization of fire loads and ignition sources form part of the preventive measures of fire protection in these plants. However, fire protection measures should not be viewed in isolation; they should rather be examined with respect to their interaction with other measures for design requirements. This means that individual fire protection measures, e.g. preventive and/or firefighting measures, need to be harmonized such that the global aims of fire protection are achieved, taking into consideration the requirements of operation and safety.

The concept of defense-in-depth has been applied in KTA 2101 fire safety protection at nuclear power plants standard. The fire protection defense-in-depth as shown in Figure 4.4 consist of:

- operational fire protection measures,
- structure related fire protection measures,
- equipment related fire protection measures, and
- manual firefighting capabilities

The effective implementation of quality assurance (QA), periodic preventive inspections, and preventive maintenance, approach minimize the fire risk and raise the efficiency of the entire fire protection defense-in depth concept.

Figure 4.4 shows the measures of the entire fire protection defense-in-depth concept, their interaction and their effects to the nuclear protection goals and the radiological safety objectives respectively the equipment and materials to be protected.

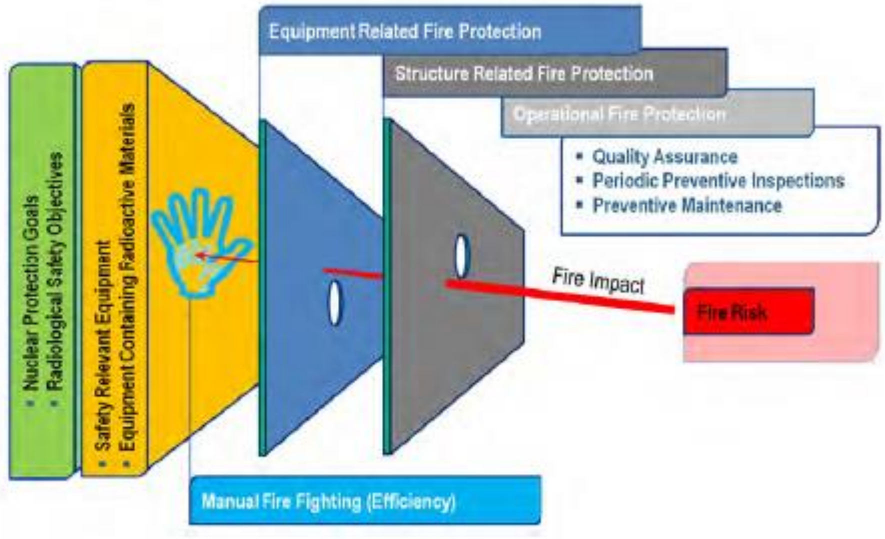

Equipment Related Fire Protection
Structure Related Fire Protection
Operational Fire Protection
▪ Quality Assurance
▪ Periodic Preventive Inspections
▪ Preventive Maintenance
Fire Impact
Fire Risk
▪ Nuclear Protection Goals
▪ Radiological Safety Objectives
▪ Safety Relevant Equipment
▪ Equipment Containing Radioactive Materials
Manual Fire Fighting (Efficiency)

Figure 4.4 Fire protection defense-in-depth concept in Germany [56]

The purpose of fire protection in non-nuclear industrial plants is to protect operating personnel and to preserve and maintain production and capital goods. These overall objectives of fire protection also apply to nuclear facilities. However, regarding nuclear facilities, they have to be supplemented by a further overall objective of protection with a higher priority: ensuring nuclear safety. For this purpose, it must be ensured that a fire will not affect safety related systems and plant components to the extent that they are no longer capable of fulfilling the required safety related functions

Hence, the development of comprehensive fire protection concepts is to ensure that the fire protection measures selected in each individual case for respective nuclear facilities are not only suitable but also consider safety related boundary conditions. The nature of protection objectives in Germany is to have different priorities in different areas of the plant.

The safety relevance of individual buildings or compartment areas of a nuclear facility can differ, depending on the arrangement of the safety related systems or radioactive materials. For instance, areas of the plant important to safety are given priority to fire safety. At the plant the nuclear protection objective is primarily of importance only in those buildings in which components for shut-down of the reactor and removal of residual heat are located. The protection objectives are applied in the reactor auxiliary building although does not contain such systems, it does contain system for treatment of contaminated wastes. Apart from the turbine and the generator, the turbine hall also contains systems of feedwater and /or steam circuit, as well as, the cooling systems. However, as these are of minor importance in terms of safety, no nuclear protection has to be taken into consideration for this building. It be observed that the availability of escape routes and exclusion of smoke, such as they apply to rooms intended for permanent occupation are not absolute but only conditional and their relevance is coupled to fulfillment of other safety requirements.

In the Federal Republic of Germany, nuclear power plants are provided with engineered safety systems such that in case of fire which inhibit the habitability of the control room and multiple redundant switchgear, the objective is to shut the plant down safely and to keep it in shutdown state. The escape root ease the safe evacuation in the control room and the essential functions of the control room could be replaced.

Nuclear power plant in the Federal Republic of Germany, two different methods are possibly used to demonstrate that the nuclear protection objective has been achieved. The first method is used to demonstrate that the fire protection measures are suitable to limit the fire to its inception phase or to a physically restricted area, without any relevant consequences. The second method is used to demonstrate that even a fire would not give rise to any inadmissible nuclear consequences.

Passive fire protection measures are given priority in nuclear power plants. This involves the minimization and enclosure of fire loads, minimization of the development of smoke and the measures for prevention of expected ignition sources in the areas of exposed combustible materials. For instance the structural separation of various redundancies of the safety system, is given priority over active measures such as firefighting. However, conventional building code requirements are fulfilled by installing stationary fire extinguishing systems, as well as mobile firefighting systems for the plant fire brigade.

In nuclear power plants, stationary fire extinguishing systems mainly use water as a fire extinguishing agent and gas extinguishing systems are used to lesser extent. However, in some plants of special design such as fast breeder reactor, or thorium high temperature reactor, the use of water may be restricted for plant specific reasons. In such cases, gas (e.g. CO_2 or halon) or even inertization (helium, argon, and nitrogen) is used for firefighting purposes.

Regarding gas extinguishing systems, the $C0_2$ and halon systems have become the state of the art, with halon having certain advantages over $C0_2$ as far as fire protection alone is concerned.

In the event of a fire, great importance is attached to early activation of countermeasures. As it cannot always be assumed that plant personnel can detect a fire in its inception phase, at least the fire detection equipment should be automated.

In nuclear power plants, in the past, activation of stationary fire extinguishing systems, and in particular of deluge sprinklers, was in general not automated. The reasons included the potential effects of an erroneous activation of these systems with respect to their availability and to the safety of the plant. Events in some countries involving the erroneous activation of automatic fire extinguishing systems have led to a controversial discussion over the last couple of years on the necessity of automatic activation in the Federal Republic of Germany.

In general, the issue of spray deluge sprinkler systems has somewhat eased, at least in the Federal Republic of Germany, since sprinkler systems are also considered to be suitable for the fighting of cable fires. Sprinkler systems release smaller amounts of water, so erroneous activation will not produce any serious negative consequences.

What is likely to emerge in the future is broader use of sprinkler systems, which would mean fast firefighting when required and a limitation in the amount of water in erroneous activations.

The former version of KTA 2101.3 included the requirement that "…as far as the fire detection and alarm systems must be designed against earthquakes, safety standard KTA 2201.4 shall be applied. It is permissible to alternatively assume that the fire detection and alarm facility stays available after an earthquake, provided, it is proven that the support structure of the fire alarm board retains it stability during earthquakes and it is ensured that any failed components in the fire alarm control center and the corresponding local control centers can, if required, be replaced (e.g., by exchanging the modules) or repaired at short notice."

In the actual version of KTA 2101.3, a recommendation and a requirement for design are being distinguished. It is recommended that the fire detection and alarm systems should be designed against earthquakes according to KTA 2201.4, if they are located in building areas which need to be seismically designed according to their safety relevance and if the seismic intensity I exceeds I = VI (EMS-98). The requirement is that the fire detection and alarm systems shall be designed against event combinations of fires and other anticipated events if their function after an event combination has to be ensured according to KTA2101.1, par.3.3.

Seismically designed fire detection and alarm systems are available and represent state-of-the-art systems.

4.3.3 NPP FIRE SAFETY ASSESSMENT METHODS REVIEW IN GERMANY

Operational Experience and characteristics of nuclear power plants have shown that fire can be a safety significant hazard. In view of that, the regulators expect the licensees to justify their arrangements for identifying how fires can occur and spread, assessing the vulnerability of plant and structures, determining how the safe operation of a plant is affected, and introducing measures to prevent a fire hazard developing and mitigate against its effects if it should nevertheless develop.

Most of the engineering work in designing fire protection measures in German nuclear power plants has been performed on a deterministic basis. Moreover, the use of deterministic fire risk analysis is the practice in Germany to review the fire protection state of operating NPP. The probabilistic approach provides different insights into design and availability of systems and components supplementing the results from deterministic safety analyses It should be underlined that these reviews have led to comprehensive backfitting and upgrading measures including structural fire protection measures (e.g. fire barriers) as well as the active fire detection, alarm and extinguishing features and administrative fire protection measures (for manual firefighting) resulting in significant improvements in fire safety, in particular in case of a NPP built to earlier standards **[57].**

Deterministic Fire safety analysis was addressed in 1977 in the safety criterion 2.7 ‘’ Fire and Explosion protection’’ of the Safety Criteria for Nuclear power Plants (s (BMI, 1977) [**59].** In the 1994 guidelines on incident requiring that protective measures against fires be taken by means of plant engineering was issued (BMI, 1994) [59]. Three nuclear safety standards defining and prescribing the basic deterministic requirements, namely, fire safety measures regarding structural plant components, mechanical, and electrical components as described in safety standard KTA 2101 **[59**]. Accordingly, the deterministic basic requirements describe, in the design principles, structural and equipment-related fire protection measures against building internal and external fires, operational fire protection measures as well as tests and inspections are elaborated.

The plant internal fire hazard is considered in the deterministic safety status analysis as part of the Plant Safety Review (PSR) in order to determine if the goal oriented requirements outlined in the regulatory framework are met.

Methods to analyze existing plants systematically regarding the adequacy of their existing fire protection equipment can be deterministic as well as probabilistic. Fire risk assessment has become an integral part of PSA and, at international level, fires have been recognized as one of the major contributors to risk of nuclear power plants. In Germany, it is recognized that probabilistic approach of fire safety analysis provides different insights into design and availability of systems and components and supplements the results from deterministic analyses. Thus, probabilistic considerations have been taken into account for decision making on a case-by-case basis and recommended in the frame of comprehensive fire risk periodic safety reviews.

For fire risk assessment in Germany, a qualitative or quantitative screening process is proposed to identify critical fire zones followed by a quantitative event tree analysis in which the fire induced hazard state frequency will be determined. The models proposed have been successfully applied in complete and partial fire risk studies for German nuclear power plants.

A state-of-the-art methodology for Fire PSA has been developed and successfully applied for a German NPP. The state-of-the-art approach for performing Fire PSA has been developed in Germany, which has been exemplarily and completely applied to a German NPP with boiling water reactor (BWR) of the type BWR-69 for full power (FP) operation [59]. This methodology is based on a combined multi-step qualitative and quantitative screening approach applying a comprehensive database specifically developed for the application within the frame of Fire PSA. The approach being applied enables to automatically perform several analytical steps of the Fire PSA. Some of the automatisms, e.g. the calculation of compartment specific fire occurrence frequencies or the probabilities of fire propagation to adjacent and further compartments, have been successfully implemented in the database. Standardized input data files have been provided for other applications of the Fire PSA database, e.g. for determining fire induced core damage frequencies by means of the simulation code CRAVEX.

For example, Isar 1 BWR nuclear power plant had completed the fire PSA [61]. The quantitative screening process was applied to approximately 500 rooms, in reactor building, turbine building, switchgear building, emergency diesel room, and service water intake structure. 172 critical rooms were identified and analyzed. The relation of local fire frequencies was calculated using Berry´s method. The fire induced hazard state frequency of about $6.3X10^{-7}$/a for the whole plant resulted mainly from 14 single rooms and 7 room pairs (calculation including fire spreading analysis) [61]

The Germany regulatory body issued PSA methods guide; (FAK PSA, 2005a) **[59**] and PSA data (FAK PSA, 2005b) **[59]** in performing the periodic safety review. The guide contains reference listings of initiating events for NPP with PWR and BWR respectively, which must be checked plant specifically with respect to applicability and completeness. The listings includes plant internal fires and detailed instructions for the analysis of plant internal fires, fire frequencies and unavailability of fire detection and alarm features as well as data. These technical documents have been developed by a working group of technical experts from nuclear industry, research centers, universities, authorities and technical support organizations chaired by the BfS (Bundesamt für Strahlenschutz, Federal Office for Radiation Protection).

The task of fire PSA within the in advance defined global boundary is to determine the annual frequency of fire induced core damage states of the NPP. The set of all the compartments is the starting point of the fire analysis. The spatial plant partitioning is performed in the way that all compartments characterize the global analysis boundary and that no compartment overlap. In this case, the annual frequency of fire induced core damage states of the plant results from the sum of all compartment related annual frequencies of fire induced core damage states.

The assumption is that compartments with a low fire load density do not impact the fire PSA results. The screening process eliminate these compartments before starting the detailed compartments and specific scenario analysis. The fire induced core damage frequencies of all the remaining compartments are determined in a first step using simplified and conservative assumptions

The Fire PSA database has not yet been completely adapted from full power plant modes to low power and shutdown modes; and investigations are being carried out as to which data have to be changed or added for these states.

Further development focuses on fire induced cable failures and circuit faults, which are broadly discussed on an international level with USA leading the discussion **[**59]. In this context, a cable failure mode and effect analysis (FMEA) for all the PSA related cables has been developed **[59]** and tested for a fire compartment, which had been identified as significant in the frame of the Fire PSA. This leads to the requirement to enlarge the Fire PSA database considering additional data needed for a cable FMEA and/or combining the compartment inventory matrix with the cable database of the FMEA. The activities for implementation of the cable FMEA approach in the Fire PSA methodology are ongoing.

A further development covers the characteristics of compartments and components for supplementing the automatic data supply, such as data on the room heights for fire simulations with the zone model CFAST or the description of the ventilation systems for assessing smoke propagation. This is a simplified fire effects analysis within the screening by standardized fire simulations.

Improved Modelling and Assessment of the Performance of Firefighting Means in the Frame of a Fire PSA has been carried out to assess the performances of the firefighting means to be applied in a nuclear power plant. An integrated deterministic and probabilistic safety analysis (IDPSA) was carried out to assess the performances of the firefighting means to be applied in a nuclear power plant. The tools used in the analysis are the code FDS (Fire Dynamics Simulator) for fire simulation and the tool MCDET (Monte Carlo Dynamic Event Tree) for handling epistemic and aleatory uncertainties [60].

The analysis was performed in two parts. The first steps of the analysis focused on the performances of the crew members in charge of firefighting and made extensive use of the tool MCDET and its Crew module. The aleatory uncertainties taken into account relate to the timings of human actions to be applied for firefighting and to whether actions are successfully performed or not.

It is important to note that statistical national database exist for Fire PSA. In particular, data on compartment specific as well as component specific fire occurrence frequencies. However, reliability data of fire protection features has to be further improved and expanded. Moreover, the human influence has to be considered carefully and analyze in holistic manner.

The use of internationally available generic data (e.g. for fire occurrence frequencies), mainly from the U.S. and France, is not always appropriate for application within Fire PSA for German plants due to differences in design, inspection and maintenance. However, the German data being presently available do not always allow providing a verified database because only a very small amount of approx. 30 fire events had to be obligatory reported to the national supervisory authorities. Therefore, the OECD FIRE Database Project which was started by OECD/NEA in 2003 to collect fire event data and meanwhile comprises more than 340 fire events from twelve NEA member countries (OECD, 2009) may supplement performing Fire PSA for German NPP by further input data.. First test applications of this database with up to the end of 2008 in total 343 fire events have been successfully performed [59].

4.4 HISTORICAL NPP FIRE SAFETY EVOLUTION IN JAPAN

4.4.1 NPP FIRE SAFETY REGULATIONS REVIEW

During the final stage of world war II United States dropped nuclear bomb on two Japanese cities, Hiroshima and Nagasaki, on August 6, 1945.The two bombings killed at least 129000 people and the after effect still persist. However, in 1954 United States passed the Atomic Energy Act, for peaceful application of atomic energy. Despite the catastrophic effect of the atomic bomb in Japan, in 1954, a legislation was passed to use atomic energy for peaceful purposes. The following year, Japan’s Atomic Energy Basic Law went into effect, limiting the nation’s pursuit of fission power to peaceful purposes only but putting the country on the path to serious nuclear power development. Japan initially turned to Great Britain for help with civilian nuclear power. Japan’s first reactor was Tokai 1, a British-designed Magnox reactor (CO_2 cooled and graphite moderated, using natural, un-enriched uranium as fuel). It was rated at 166 MW. Construction began in early 1961 and was completed in late 1965. The unit operated at the Tokai station until March 1998. Magnox nuclear technology proved a dead end, both in Britain and Japan. The Japanese soon shifted their attention to U.S.-designed light water reactors, both boiling water designs and pressurized water reactors. Fukushima Daiichi 1, for example, was a General Electric boiling water reactor. Construction started in 1967 and the plant went into commercial service in late 1970. By the end of the 1970s the Japanese industry had largely established its own domestic nuclear power production capacity. According to the WNA, the first indigenous Japanese plants had performance problems, with capacity factors averaging below 50%. The country embarked on a program to improve nuclear performance and brought the plants up to world standards by the mid-1980s **[62].**

In Japan, the regulatory framework was defined by a hierarchy of legal and regulatory documents: national laws, regulations (or Ministerial Orders and Ordinances), and regulatory guides issued by the Nuclear Safety Commission (NSC). The NSC regulatory guides consist of Level I and Level II guides. Level I guides establish requirements that are comparable to the design basis requirements in NRC regulations for nuclear power plants. Level II guides provide additional guidance in specific technical areas, but most Level II guides are not available in English. The NSC regulatory guides are not regulatory requirements or legally binding. However, indications are that in practice licensees would comply with these guides as though they constituted requirements.

The national laws and regulations (or Ministerial Orders and Ordinances) do not contain design requirements and specific safety standards for nuclear power reactors. There are three general guides namely; Reviewing Safety Design of Light Water Nuclear Power Reactor Facilities (L-DS-I.0); Regulatory Guide for Reviewing Nuclear Reactor Site Evaluation and Application Criteria (L-ST-I.0); Evaluating Safety Assessment of Light Water Reactor Facilities (L-SE-I.0). These three guides and some supporting Level I guides were considered to provide design basis requirements. The safety design guide (L-DS-I.0) was issued in 1970 and revised in 1977, 1981, 1990 and 2001. The siting guide (L-ST-I.0) was issued in 1964 and revised in 1990. The “requirements” of these two guides were in effect at the time of the construction permit of Fukushima Daiichi Nuclear Power Plants (from 1966 to 1972 for units 1-6). [63, 64]

The safety evaluation guide (L-SE-I.0) was initially issued in 1990 and revised in 2001. The stated purpose of this guide is to provide “the basis of the judgment for adequacy of the design to ensure safety at the plants. Review related to the application for the establishment license (includes the application of alteration of an establishment license) of the individual light water nuclear power reactor were issued under these laws and regulations in ministerial ordinances.

Regulatory Guide for Reviewing Fire Protection of Light Water Nuclear Power Reactor Facilities (L-DS-I.03) was part of regulatory guide for design. This guide provides that design of nuclear power plants incorporate provisions to prevent occurrence of fires, to detect/extinguish fires should they occur and to mitigate the consequences from plant fires. A fire protection program is required for plant operation. But there is not guidance given on the fire protection program. The guide requires that the function of the fire protection systems not be severely affected by a major earthquake and design take into consideration of earthquake induced fires. The detail analysis and safety assessment of the fires were not provided under the regulatory guide. Therefore fire hazard analysis were not a regulatory requirement. Japanese regulatory requirements apparently did not specifically address beyond design basis events such as station blackout (SBO) events, Anticipated Transients Without Scram (ATWS) and terrorist attacks.

Japanese Nuclear regulatory body does not have inspection rules on the fire protection systems of operating nuclear power plants. Nuclear regulatory inspectors do not inspect fire protection matters. Fire protection systems inspections are inspected by Fire Defense Department under the Fire Defense Law in Japan. This legal framework includes nuclear power plants.

A severe accident at TEPCO's Fukushima Daiichi Nuclear Power Station, triggered by the devastating natural events of 11 March 2011, and taught Japan and the world many important lessons on nuclear safety issues including fire safety.

One of the most significant actions taken in Japan post-Fukushima to improve its nuclear safety management and regulation is the creation of a new nuclear regulatory body, the Nuclear Regulation Authority (NRA). On the September 19, 2012, one and half year after the Fukushima accident the new Nuclear Regulatory Authority (NRA) was inaugurated. The main aim of NRA was to carry out a complete review of safety guidelines and regulatory requirements to formulate a set of new regulations to protect people and the environment. On July 8, 2013, the new regulatory requirements for commercial power reactors got into force.

The new regulatory requirements were developed taking into account the lessons-learnt from the accident at Fukushima Daiichi Nuclear Power Station. The lessons that were identified in the reports of the National Diet's Nuclear Accident Investigation Commission, the Government's Nuclear Accident Investigation Committee and the Independent Investigation Commission on the Fukushima Daiichi nuclear accident, considered the harsh natural conditions unique to Japan. The regulations were in line with the consistency with the safety standards and guidelines of the International Atomic Energy Agency (IAEA). So-called "safety myth" had critically impeded efforts for nuclear safety in Japan before the accident at Fukushima Daiichi nuclear Power Plant, however, more stringent regulations have been developed with an underlying assumption that severe accidents could occur at any moment.

Based on a concept of "Defense-in-Depth", essential importance was placed on the third and fourth layers of defense and the prevention of simultaneous loss of all safety functions due to common causes. The third layer of defense involves equipment related to fire safety protection and the fourth layers of defense consist of structures related to fire safety protection. The operational fire protection constitute operational measures such as periodic preventive inspections, preventive maintenance and quality assurance. In this regard, the previous assumptions on the impact of earthquakes, tsunamis and other external events such as volcanic eruptions, tornadoes and forest fires were re-evaluated, and countermeasures for nuclear safety against these external events were decided to be enhanced. Furthermore, it is required to take countermeasures against internal fires and internal flooding, and to enhance the reliability of on-site and off-site power sources to deal with the possibility of station blackout (SBOs). Enhance countermeasures against events other than natural phenomena that may trigger common cause failures are strict and thorough measures for fire protection, countermeasures against internal flooding, and reinforcement of power supply systems to prevent power failure. Strict and thorough measures against fires have been reinforced or newly introduced in new regulation. Example of measures for fire protection is the requirement for the use non-combustible materials for cables installed in SSCs with safety functions and whose non-combustibility are confirmed by verification tests

4.4.2 NPP FIRE PROTECTION REVIEW IN JAPAN

The fire accident in Browns Ferry Nuclear Power Plant in 1975 in the US triggered detailed regulations to be formulated for fire protection in nuclear power plants (NPPs) in Japan. "Examination Guide for Safety Design of Light Water Nuclear Power Reactor Facilities" was amended in 1977 in addition of "Guideline 5: Design Consideration against fire", and "Examination Guide for Fire Protection of Light Water Nuclear Power Reactor Facilities" was established in 1980. This guideline, based on the principal policies of "shut down the reactor" and "prevent uncontrolled release of radioactive materials" to ensure NPP safety as a whole, employed multi-barrier concept comprising of countermeasures for fire prevention, fire detection and extinguishment, and mitigation of fire effects.

In the 1980, the nuclear safety commission had issued ‘’The review Guide for the Fire Protection of light Water Type Power Generation Nuclear Reactor Facilities’’ which required the utility companies necessary items for fire protection measures to be included in their safety analysis report in the application for established permission of the nuclear power plants **[65]**

Fires in Japanese nuclear power plant is very seldom event. For the earlier 27 years of operation experience only four events were reportable. However, the electric utilities have operated their thermal plant long time before the first introduction of nuclear power plants. The fire protection management was a major concern of the utility companies, since the thermal power plants have storages of large quantities of highly combustible fuel, either coal or oil, which are the subject of the fire protection Law. Hence, they have established administrative guidelines based on the legal requirement.

However, the practices in fire protection management usually vary for individual nuclear power stations. The organization of fire protection management for nuclear power station consist of (1) fire protection management committee; (2) Fire protection management organization; and (3) self Defense fire brigade system. The committee is chaired by the station General Manager and the vice-chairman is the deputy general manager. The other member of the committee are the managers of the individual organizations and the fire protection Administrator of the station. The mandate of the committee is to review:

- modification of the fire protection plan of the station
- maintenance / management of the fire protection facilities of the station
- organization of self-defense fire brigade
- Education and training on fire protection and
- Other matters

The committee is held twice a year or anytime requested by the chairman as necessary.

The fire protection management systems are incorporated effectively into the overall management systems of the nuclear power plants. The fire protection management consist of the fire protection administrator, nominated deputy to support and responsible person in charge of fire protection who is responsible for individual subjective items for fire protection. Within the protection zone, including the reactor building, the auxiliary building, turbine building, and etc. fire protection is generally administered by the chief supervisor for operation. Outside of the protection zone including main administration building, general information building, modification work office, main building of the power station, etc. are divided by room base classification and responsible persons are defined. Also, detailed inspection list for facilities is defined.

In Japan, the fire prevention and fire protection are divided in two parts, active and passive. The passive methods involves separation and division into fire compartments and fire cells. This incorporated in the engineering design layouts.

The active fire protection includes fire alarm system, automatic and manual firefighting systems, automatically activated fire dampers and fire barriers. These systems are well connected and placed at areas where reactor safety systems are in place in order to protect them from internal fires. The active and passive fire prevention and fire protection systems are combined in such a way that the goals of the installation are reached.

The passive fire prevention involves the limitation of the load as well as separation and isolation of a fire if and when they occur. The division of the plant into compartments and fire cells follow the division of the reactor safety functions. For items not important to safety the division is done in such a way that fire can be isolated in the smallest possible area considering the layout of the buildings. The fire alarm systems cover the whole plant i.e. all rooms where a fire can start are supervised by a fire alarm system common for the unit.

Effective and updated fire suppression system are in place, therefore when the fire occur both automatic and manual system are activated, should the other fire prevention measures failed.

In Japan, strict check of possibility of fire by well-equipped detection system and routine administration of utility themselves and high level of education for utility staffs and positive culture of preventing fire by them has resulted in minimal fire occurrences.

4.4.3 NPP FIRE SAFETY ASSESSMENT METHODS REVIEW IN JAPAN

According to the Japanese Government report to the IAEA Ministerial Conference on Nuclear Safety in June 2011 after the Fukushima Nuclear Power Station accident, lesson 27: Effective use of probabilistic safety assessment (PSA) in risk management. The report stated that ‘’PSA has not always been effectively utilized in the overall reviewing processes or in risk reduction efforts at nuclear power plants. While a quantitative evaluation of risks for quite rare events such as a large scale tsunami is difficult and may be associated with many uncertainties even within PSA, Japan has not made sufficient efforts to improve the reliability of the assessments by explicitly identifying the uncertainties associated with these risks. Considering the knowledge and the experiences regarding uncertainties, the Japanese government will further actively and swiftly utilize PSA while developing improvements to safety measures including effective accident management measures based on PSA’’.[58] This is an indication that safety assessment has mainly been based on deterministic methodology and hence the sluggishness in development of the Probabilistic methodology.

In the past in Japan, PSA has been implemented to evaluate the validity of Accident Management strategies and the quantitative safety of NPPs in the Periodic Safety Review (PSR). Furthermore, the Nuclear Safety Commission (NSC) issued draft safety goals in terms of public risk and determined performance objectives in terms of core damage frequency and containment failure frequency. The NSC and regulators launched discussions for implementing risk-informed regulation

The importance of probabilistic Risk Assessment has been highlighted not only for internal events but also for external events following the Fukushima Daiichi NPP accident in Japan. The following reflections through the past PRA activities and also with light of the Fukushima Daiichi NPP accident experiences.

- Severe accident countermeasure based on PRA are not updated since 2002.
- Slow progress is shown in the assessment of actual plants based external events PRA
- There are lack of initiatives for enhancing safety beyond the level required by laws and regulations. That is, there should be more in-house PRA utilization for continuous plant safety improvement.

Table 4.1 The PRA initiatives in Japan **[66**].

PRA Initiatives	
Late 1980s	PRA research
1982	Decision by NSC (Implementation of Accident management AM)
1992	Notice by MITI (future plan of AM
1994	Utilities’ release of the report on AM (PRA overview)
1997 ~	Utilities’ release of the internal at-power PRA results in PSR
2001 ~	Utilities’ release of the internal shutdown PRA results in PSR
2002	Utilities release of the report on AM completion (all plants)
2009 ~	Use of PRA in determining maintenance significance
2013 ~	PRA is being carried out to draw out a severe accident scenario according to the New Regulatory Requirement

From the table it be seen that not much was done on PRA as far as possible in terms of fire PRA.

The new regulatory framework is to encourage utilities voluntary initiatives in view of important roles to be played by the utilities in continuous improvement. These utilities voluntary initiatives is supported by many technical standards regarding PRA and risk-informed activities published and prepared under Atomic Energy Society of Japan (AESJ). The standards for internal fire PRA was published in June 2014 (AESJ-SC-P008:2013).The internal fire PRA standard covers in-site fire caused by failure of components and human errors. It is planned to hold discussion over the revision of PRA implementation standards concerning internal floods/internal fire accompanying an earthquake. It is also planned to develop an integrated implementation standards for the combinations of external events after clearly defining the consequential event and the combined event.

Improvement of the PRA implementation standards is expected to lead to deeper understanding of the plant safety against all the external hazards and the establishment of appropriate measures against individual hazards. To facilitate the use of PRA, government and nuclear industry are actively working on the preparation of regulatory guidelines and industry standards and considering the application of risk-informed approaches to actual plants. It is recognized that continuous monitoring of risks depending on changing plant conditions, ‘’risk monitoring’’ in future risk-informed applications should be developed.

Currently in Japan, many utilities already have risk monitoring systems, or are under consideration for the systems introducing as the effective tools for the continuous plant safety improvements. However, fire risk monitor has not been developed yet.

4.5 INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA)

The International Atomic Energy Agency (IAEA) was established in Vienna in 1957 as an agency of the United Nations. The Statute of the IAEA, approved by 81 nations, based on three pillars: nuclear verification; safety and security; and the transfer of technology. The International Atomic Energy Agency was the world's center for cooperation in the nuclear field, the Agency works with its Member States and multiple partners worldwide to promote the safe, secure and peaceful use of nuclear technologies.

The IAEA has identify Fire hazard as a major contributor to a plant's operational safety risk; the international nuclear power community (regulators, operators, designers) have been studying and developing tools for defending against this hazard.

In view of that, substantial efforts have been undertaken worldwide to effectively implement advances in fire safety at both new and existing nuclear power plants. The agency initiated program on fire safety to assist in these efforts. The program was intended to provide assistance to member states in improving fire protection and assessment in the nuclear power plants. The IAEA program is aimed at development of guidelines and good practices, the promotion of advanced fire safety assessment techniques, the exchange of state of the art information between practitioners, the provision of engineering safety advisory services, and training in the implementation of internationally accepted practices.

During the period 1993–1994, the IAEA task concentrated on fire safety and fire protection of operating plants with the main focus on the development of guidelines and good practice documents. The first task was the development of a Safety Guide which formulated specific requirements for the fire safety of operating nuclear power plants. Several good practice documents [67, 68] providing advice on fire safety inspection were developed to assist in the implementation of this Safety Guide. These documents were published in the IAEA NUSS Series as Safety Practices. These publications address all technical aspects of fire safety inspection at nuclear power plants (NPPs) including fire protection measures and firefighting capability [69], fire protection system organization, management and procedural control [70], and evaluation of fire hazard analysis [71].

In the period 1995–1996 the task concentrated on the development of good practices in the preparation of fire safety analysis. Two documents providing advice on the preparation of systematic fire safety analysis at NPPs were published under the Safety Report Series: “Preparation of Fire Hazard Analyses for Nuclear Power Plants” [72] and “Treatment of Internal Fires in Probabilistic Safety Assessment for Nuclear Power Plants” [73].

The IAEA task on fire safety for 1997–1998 includes tasks aimed at promoting a systematic assessment of fire safety related events and disseminating the essential insights from this assessment.

The first fire safety Standard at NPP was issued in 1979 by the IAEA Safety series No SG-50-D2. This was four years after the historic Brown Ferry NPP fire accident, which caused the need to recognize fire at NPP as a safety concern. The guide was restricted to fire protection of items important to safety, leaving the aspects of fire protection not related to safety in nuclear power plants to be decided upon the basis of the national practices and regulations. This publication was revised in 1992 and has been superseded by NS-G-1.7 ´´ Protection against internal fires and Explosions in Design of Nuclear Power Plants´´ Safety Guide NS-G-1.7 is a revision of an earlier Safety Guide, Safety Series No. 50-SG-D2. This and other Safety Guides recommend how to meet the design requirements established in Safety Standards Series No. NS-R-1, Safety of Nuclear Power Plants: Design. Its technical content is based on the most recent operating experience and has been extended to cover the design of plants in relation to internal explosions. The appendices provide guidance for the design and upgrading of fire detection and suppression systems.

Fire Safety Guide of the Operation of Nuclear Power Plants provides recommendations on how to meet the requirements for achieving and maintaining fire safety in the management and operation of a nuclear power plant throughout its lifetime. It covers topics including fire prevention, control of combustible materials and ignition sources, manual firefighting, training and quality assurance. The requirements for fire safety are established in Safety Standards Series No. NS-R-2, Safety of Nuclear Power Plants: Operation. The guidelines are provided concerning organization and responsibilities, periodic updating of the fire hazard analysis, modifications relating to fire safety, inspection, maintenance and testing of fire safety features, records and documentation, the adoption of a formal policy for fire safety, and specific responsibilities and authorities of staff in relation to fire safety.

The subsequent publications as shown in Table 4.2, were based on guidelines for deterministic fire safety assessment; ranging from inspections, firefighting, data gathering, fire hazard analysis and evaluations, to upgrading of fire safety.

Table 4.2 Historical IAEA publications on Fire Safety at Nuclear Power Plants

	Title	Type of document	Year of publication
1	Fire protection in Nuclear Power Plants	Safety Series No SG-50-D2 (rev 1)	1979 1992
2	Inspection of fire protection measures and fighting capability at NPP	Safety Series No 50-P-6	1994
3	Guidelines for multipurpose data systems for NPP	TECDOC-756	1994
4	Fire Hazard analysis for WWER NPP	TECDOC-778	1994
5	Evaluation of fire hazard analyses for NPP	Safety Report series No 50-P-11	1995
6	Assessment of the overall fire safety arrangements at NPP	Safety Series No 50-P-9	1996
7	Treatment of internal fires in PSA for NPP	Safety Report Series No 10	1998
8	Preparation of fire hazard analysis for NPP	Safety Report Series No 8	1998
9	IAEA &OECD- incident Reporting system (IRS) Reporting guidelines		1998
10	Organization and conduct of IAEA fire safety Review at NPP	Services series No 2	1998
11	Upgrading of fire safety in NPPs	TECDOC- 1014	1998
12	Root cause Analysis for fire safety related Events	TECDOC-1112	Sept.1999
13	Use of operational experience in fire safety assessment of NPP	TECDOC-1134	Jan 2000
14	Safety of NPP operation	Safety standard Series No NS-R-2	2000
15	Safety of NPP: Design,	Safety Standard Series No NS-R-1	2000
16	Fire Safety in the operation of NPP	Safety Standard Series No NS-G.2.1	2000

17	Operational safety performance indicators for NPP	TECDOC-1141	May 2000
18	Experience gained from fire in NPP: Lessons learned	TECDOC-1421	2004
19	Protection against internal fires and Explosions in Design of NPP	Safety Standard Series No NS-G-1.7	2004

The first publication on probabilistic fire safety assessment was in 1998 in the Safety report Series No. 10. The assessment approach has not changed but complementation of the Deterministic approach with the PSA methods. This Safety Report provides information on good practices in conducting probabilistic safety assessment (PSA) for fires in land based nuclear power plants. It has been developed in response to the increasing attention being given to PSA worldwide and is intended to facilitate the implementation of the risk based approach to fire safety assessment for both new and operating nuclear power plants.

In early 2001, the activities of IAEA on PSA in general have included the preparation of IAEA-TECDOC-1101, Framework for a Quality Assurance Program for Probabilistic Safety Assessment; IAEA-TECDOC-1106, Living Probabilistic Safety Assessment (LPSA); and IAEA-TECDOC-1135 (jointly with OECD/NEA) on Regulatory Review of PSA Level 1. These publications are all aimed at improving the quality of the PSAs so that they can support decision making efficiently and reliably.

However, National regulations or standards for fire protection may require approaches that differ from the recommendations given in the IAEA Safety Guide. A compromise may in this case have to be found on the basis of engineering judgment.

Member States that operate NPPs have played an important role in the effort to improve fire safety by circulating their experience internationally — this exchange of information can effectively prevent potential events. When operating experience is well organized and made accessible, it can feed an improved fire hazard assessment on a probabilistic basis. The practice of exchanging operational experience seems to be bearing fruit: serious events initiated by fire are on the decline at plants in operating States. However, to maximize this effort, means for communicating operational experience need to be continuously improved and the pool of recipients of operational experience data enlarged.

CHAPTER FIVE

OBSERVATIONS AND RECOMMENDATIONS

This chapter reviews the fire safety regulations, protection and methods of assessment in the United States of America, Federal Republic of Germany and Japan. This is the observations and recommendations after the historical review of fire safety at the Nuclear Power Plants in chapter four. For each of the countries, sections will be devoted to Regulations, fire safety protection and methods of fire safety assessment and subsections on peculiar aspects for each country.

5.0 OBSERVATIONS IN USA NPP FIRE SAFETY REGULATION

5.1.1 Earlier Regulations Development before USNRC Formation

The Atomic Energy Commission (AEC) of United States of America inherited the fire protection regulations and practices of the facilities and the programs of the Corps of Engineers Manhattan Engineering District which had created the atomic bombs of World War II. Building on the early weapons work, the AEC came to encompass major new programs, including operation of the nation’s multi-discipline national laboratories, the development and regulation of peaceful uses of atomic energy and extensive research in many Physical and biological sciences. Some of these old buildings have fire protection deficiencies.

The billions of dollars of investments in these facilities were challenged by fire incidents. Thus in the 28 years of AEC existence the total losses from all accidents causes, including fires, explosions, electrical, material handling, radiation/decontamination incidents, material losses , transportation incidents, acts of nature, and miscellaneous causes, amounted to just under $68 million. Fire accounted for 80% of this total. This called for enhancement of fire safety programs which were mainly based on deterministic approach and the performance in fire protection was especially noteworthy and bears recording, notwithstanding limited scientific knowledge.

The high-quality level of experienced personnel of the first-generation of the AEC fire protection engineers led to the first AEC fire protection requirements specifically stated that the ´´improved risk´´ level of protection was the AEC goal. The improved risk protection implies that professional fire protection engineering judgment (with full benefit of past experience) has been used to obtain the highest economically justifiable level of industrial loss prevention. The success of the fire protection engineers was partly based on the sharing of their experiences. Most importantly, annual meetings facilitated the dissemination and coordination of fire protection activities.

After the Rocky Flats fire, lessons learned led to an initiation of physical upgrading program, organizational changes and insurance survey program. The fire protection requirement of AEC was changed to more clearly spell out the performance nature of the system. The new definition and the goals of the ´´improved risk´´ were spell out and became the fire protection standard. The most evident characteristics of an improved risk property is the existence of reliable, automatic fire extinguishing system throughout all the buildings of combustible construction or contents.

It is recognized that insurance played a critical role in paying for loss of materials and property. The recommendation is that effective and financially reliable insurance companies must be developed to ensure that losses in Ghana's nuclear power program due to inevitable fire outbreaks can be insured.

5.1.2 The 1975 Brown´s Ferry Cable Fire and development of the Appendix R Requirements

For the nuclear industry, there was initially little recognition on the part of plant designers that fires could represent a threat to safe plant operations. It was only after the severe cable tray fire at the Brown's Ferry reactor site in 1975 that the operational importance of fire safety was fully recognized. As a result of this incident, the USNRC instituted a new set of fire safety requirements which specifically addressed these unique concerns. The implementation of these requirements for most commercial nuclear power plants requires significant plant modifications. In most cases, as backfits, the modifications were often expensive undertaking as well. The implementation of the fire protection requirements has been a difficult process which has often placed USNRC and the nuclear utilities in harsh adversarial roles. This was largely from the fact that the USNRC requirements were very prescriptive and straight jacket for every nuclear power station no matter the peculiar circumstances which resulted in numerous exemptions applications.

This provides a great and important lesson for Ghana's nuclear power program to ensure that regulations, requirements and guidelines on fire protection of nuclear installations must be planned and engineered from the start of these projects to avoid expensive retrofits. By recognizing the lessons gained from the past experience of U.S.A, Ghana can avoid many of the limitations in regulations that resulted in fire continuing to represent a significant risk contributor for commercial nuclear reactors in U.S.A. In the many cases, the dominant fire risk scenarios identified in the risk assessments could have been eliminated or, at least, had their importance significantly reduced through design engineering modification. However, when addressed through retrofit, it is almost inevitable that some level of the residual risk remains.

It is recommended that the current USNRC fire safety regulations (i.e. Appendix R to 10CFR50) will not represent an adequate design basis for Ghana's nuclear power program because the regulations were specifically developed as retrofit rules, they do not represent the appropriate design consideration for a new reactor. It is recognized that those USNRC rules which apply to the reactor sites at that time were specifically written as retrofit requirements. These regulations were in two parts. First, Appendix R to 10CFR50 provides the regulations which apply to all reactor sites licensed prior to January 1, 1979. Second, Section 9.5-1 of the Standard Review Plan (SRP) describes the criteria for evaluation of fire safety for reactors licensed after that date. Even the provisions set forth in the SRP recognize that all of the plants at the time had already initiated construction by the time the guidelines were established, and hence, certain desirable factors might not be achieved.

In general, the Appendix R requirements specify alternate methods for fire protection, through separation, redundant trains of plant safety equipment. Because these requirements were to be applied as a retrofit, they specifically allow for the housing of redundant safety systems within a single fire area. The most controversial, and least restrictive, of the alternative redundant train separation criteria identified in Appendix R was the so-called Twenty-Foot Separation Criteria by which:

- redundant equipment must be separated by 20-feet of horizontal space with no intervening combustibles; and
- Area must be protected by automatic fire detection and suppression systems.

However, Appendix R also allows for the consideration of case by case exemptions to these requirements, and allows for the use of alternative provisions shown to provide an "equal level of protection."

The prescriptive nature of the fire regulations to plants build earlier made implementation difficult and complex. This led to a number of exemption request and utilities resistance to Appendix R often quiet strong, leading to attempted law suit to strike down provisions of Appendix R. Since the institution of Appendix R, the nuclear industry in the U. S. has struggled with the interpretation and implementation of these requirements. As a result, the deadline for Appendix R compliance submittals was extended from March 1981 to July 1982. By December 1982, about 500 exemption requests had been submitted to the USNRC, and 225 of these requests were denied. The clarification of NRC staff position In October 1983, based on the results of the exemption request reviews and Appendix R compliance inspection results, the nuclear industry appealed. This appeal was rejected by the nuclear regulatory commission. As a result 38 reactor units submitted new exemption requests, and 15 units submitted new alternative safe shutdown implementation plans. The completion of the initial review of all utility Appendix R implementation documentation took almost a decade and only ended by the end of 1989.

The above scenarios of this prescriptive requirement of fire protection is not a pleasant experience and that prayers in the nuclear industry must learn a lessons to avoid it. Therefore, all new comer countries like Ghana must plan and engineered the fire protection system using the state-of-the-art technology and methods. This will in future help to avoid expensive retrofits.

5.1.3 Development of fire safety regulations for newly design power reactors

Earlier in July 1981, the USNRC issued Section 9.5.1 of the Standard Review Plan (SRP Revision 3). This document describes those fire safety provisions intended to apply to all reactors licensed after January 1, 1979. In general, the SRP reiterates the Appendix R requirements. In certain areas, the requirements are expanded somewhat, but the differences are relatively minor. When the first draft of the retrofit requirements were issued in Branch Technical Position (BTP) CMEB 9.5-1, this document was accompanied by a companion Appendix A, which provided a draft version of fire safety regulations to be applied to a new reactor site. The differences between Appendix R and the SRP are far less significant than were the differences between the retrofit rules of the original BTP 9.5-1 and its associated Appendix A guidelines for new plants.

In 1990, the USNRC staff policy statement [74] on the evolutionary Advance Light water Reactor (ALWR) designers to ensure safe shutdown is achieved assuming that all equipment in any area is rendered inoperable by fire and that reentry into the fire area for repair and operator action is not possible. This calls for the need for remote safe shutdown capabilities when re-entry into the fire area for repair and operator action is not possible. The planning and engineering of new production reactor must take all probably scenarios into account. However, this must be balanced with cost and benefit analysis in the regulations by applying goal setting regulation rather than prescriptive regulations.

It is obviously comprehensible that the current Appendix R fire safety requirements do not represent an adequate basis for the design and implementation of fire safety for the new reactors. The policy of the NRC staff implies that the new guidelines will specifically disallow the use of physical segregation or passive protection of redundant safety equipment within a single fire area as an adequate means of fire hazard mitigation. Instead, redundant safety equipment will be required to be housed in separate fire areas which are bounded all sides by three hour rated barriers.

It was recognized that significant additional risk reduction be achieved through expansion of the NRC policy statement on the new reactors. The USNRC staff policy position represents a purely deterministic criterion. As such, it will not address the residual risk associated with random equipment failures or outages in the redundant safety trains. As currently stated, the staff position requires that a reactor must be designed so that safe-shutdown conditions can be reached assuming that all equipment in a single fire area might be rendered inoperable by a fire and that reentry into the fire area for recovery actions is not possible. The additional consideration of any possible single active component failure in other plant equipment outside of the fire area due to nonfire related causes (e.g., random failure, maintenance outages, sabotage, personnel errors, etc.) would significantly reduce the likelihood of any risk significant core damaging fire scenarios remaining. Therefore, for new reactor construction for new comer country like Ghana both deterministic and probabilistic regulation approach to NPP fire safety is highly recommended.

The recommended extension is not intended to acquire that all safety system be designed in a three –train configuration. The recommended extension directed at protection of general safety functions and the overall ability of the plant to achieve a safe shutdown state, rather than protection of any one given plant safety system. The primary impact of the additional constraint is likely to be on the plant support systems rather than on the front-line safety systems because even in a one-or two-train plant many alternate methods of achieving safe shutdown are typically available (for example high pressure injection versus depressurization and low pressure injection in a LWR plant). However, it is the plant support systems, such as the electrical power and service water systems, which may require three-train availability. Even in the case of electrical power, a true three-train system would not be required because offsite power and two 100% diesel generators could be configured to provide three way segregation so long as appropriate isolation and switching capability are provided.

The intent of the enhanced criteria is to ensure that the designers consider that, in addition to fire induced damage, any one active component might either fail on demand or might be unavailable due to a service outage. It is not intended that the single failure necessarily applied to full system failure unless a single component failure might render a redundant system inoperable.

The use of a more rigorous fire safety design criteria such as that outlined in SECY-90-016-[74], the regulatory requirements, including the additional probabilistic constraint can be expected to significantly reduce the likelihood that risk-important fire scenarios will remain unaddressed by future reactor designs. As described earlier, for the operating commercial nuclear reactors, many of the dominant fire risk scenarios involve cases in which the segregation of redundant safety system equipment within a single fire area has been used as a means of fire protection. The use of the above criteria would eliminate most of these plant vulnerabilities.

However, the use of a fire PSA as a design definition tool will represent a departure from the traditional application of risk assessment as a design review tool. This means that the fire PSA takes a higher level of importance than that which is typical of past confirmatory review risk assessments. The degree to which potential design weaknesses are identified and evaluated in the fire PSA would become a critical consideration. This is not considered optimal because the overall level of uncertainty in a typical PSA is significant, and because differences in analysis methodology can significantly impact the level to which plant vulnerabilities are identified. Notwithstanding, even with conservatism and uncertainty, insights from PSA can be profitable.

But, if the confirmatory role of fire PRA will be raised to a higher level of quality assurance, then significant additional overhead burden will be placed on the fire PSA in that the data bases, fire models, and expert judgment factors utilized in the analysis must be scrutinized. With the growing levels of the maturity of fire PSA methodology, accumulation of data for fire PSA and experiences gained from the operation of the NPP, Ghana can use the insights from PSA for design review purposes.

5.1.4 Performance-based standard for Fire Protection

The 1995 PRA Policy Statement states, in part, the use of PRA technology should be increased in all regulatory matters to the extent supported by the state of the art in PRA methods and data, and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy. The subsequent publications of the NRC and NFPA, “Performance-Based Standard for Fire Protection for Light-Water Reactor Electric Generating Plants” (2001 Edition), brought new alternative approach in nuclear power plant fire protection regulations.

On July 16, 2004 the Nuclear Regulatory Commission amended 10 CFR Part 50.48 “Fire Protection” to add a new subsection, 10 CFR 50.48(c), that established acceptable fire protection requirements. The change to 10 CFR 50.48 endorses, with exceptions, the National Fire Protection Association’s 805, “Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants – 2001 Edition,” as a voluntary alternative for demonstrating compliance with 10 CFR 50.48 Section (b) and Section (f**)[30].**

The prescriptive fire protection requirements predating the July 16 2004 Amendment to 10 CFR 50.48 were established well before the emergence risk-informed, performance-based analytical techniques.

The Risk-informed, performance-based standard for fire protection at Nuclear Power Plants include the benefit of probabilistic risk assessment for fires and reflect insights into fire risk evident from the significant body of operating experiences developed through risk based assessment. This fire protection rule would allow flexibility and facilitate the use of alternate approaches to meet the fire safety objectives. This may reduce the need for many exemption requests as discussed in subsection 5.1.2.

More so, the Nuclear Energy Institute (NEI), representing the nuclear industry, championed the use of risk-informed, performance-based processes for fire protection at NPP. This adoption of optional fire protection licensing basis is effective and comprehensive, without placing an unnecessary burden on licensees pursuing risk-informed, performance-based initiatives. The composition of the NFPA 805 Technical committee on nuclear facilities, comprising nuclear plant licensees, the NRC, insurers, equipment manufacturers, and subject matter experts, made this fire protection standard effective and comprehensive. Though NFPA 805 provides many of the tools and processes necessary for risk-informed, performance-based fire protection, additional guidance and clarification is warranted. The implementing guidance is intended to provide that additional guidance and clarification for effective, comprehensive implementation without undue burden on licensees.

As stated in 10 CFR 50.48 (c) (3) (I), any licensee’s adoption of a risk-informed, performance-based program that complies with the rule is voluntary. Compliance with this rule may be adopted as an acceptable alternative method for complying with either 10 CFR 50.48 (b), for plant licensed to operate before January 1, 1979, or the fire protection license conditions for plants licensed to operate after January 1, 1979, or 10 CFR 50.48 (f), plants shutdown in accordance with 10 CFR 50.82(a)(1).

NFPA 805 is related to other fire protection requirements and codified as 10 CFR 50.48(c). The new rule was placed deliberately in this location to show how it relates to existing fire protection requirements. The new rule establishes alternative requirements that a licensee may voluntarily adopt instead of continuing to comply with its current fire protection licensing basis. Over the period of 2008-2013, 20 units have submitted Licensing Amendment Requests (LARs) to make use of this change to the NFPA 805. They have an average reported fire CDF of about 4E-5/reactor-year (ry) and an average contribution to total CDF of about 70%.[36]

However, the recommendation for new comer country like Ghana is not to use alternative prescriptive requirement or risk-informed, performance-based as adopted by NRC but rather move towards an integrated approach that combines the insights provided by the deterministic approach and those from the probabilistic approach with any other requirements in making decisions on a safety issue for a nuclear facility or in deciding on the priorities for the activities to be carried out by the regulatory body.

5.2.0 OBSERVATION ON NPP FIRE PROTECTION IN USA

The fire protection programs were inherited by the US Atomic Energy commission (AEC) from the war time Manhattan Engineering district. The fire protection program at that time was based on general fire code for homes and industrial establishments. Many of the buildings were both substantially built and provided with automatic fire protection as an exception rather than the rule. This continued into the initial commercial power plants. The recommendation is that Ghana should not thread on that path by continuing to apply general fire code for homes and industrial establishment to the nuclear power plants. Unique and applicable fire safety regulations should be established for the nuclear power program

By February 1, 1971, a system of internal management procedures and audit were instituted to strengthened fire safety programs at the nuclear power plants. The deterministic approach of inspection by independent fire safety inspectors was instituted to prevent financial and material loses to fires. This was an indication that internal fire safety measures and programs were not adequate, and therefore, efforts of external inspectors will help develop and strengthened any measures identified. This led to the development of system-based tools for considering fire risk. The external inspectors approach should be encouraged so that internal management procedures and audit are not relaxed on alter of complacency.

The fire research programs resulted in the development of the fire protection tools and systems such as the design of sprinkler heads, and carbon microsphere as an extinguishing agent.

The NRC inherited the fire protection programs from the AEC which were purely based on deterministic methods and approaches. During that time nuclear power industry fire safety rules relied heavily on the design requirements. The March 22, 1975 Brown ferry nuclear power plants fire accident which coincided with the establishment of the NRC resulted in further and far reaching development and clear path of the NPP fire protection programs

5.2.1 THE NRC FIRE PROTECTION PROGRAM

The NRC nuclear power plants fire protection program provide fire safety assurance through a defense-in-depth philosophy. The first element of consideration was the comprehensive identification and analysis of fire and explosion hazards. The objective is to prevent the fires and explosion from starting. The next element is the organization and staff positions responsible for the management and implementation of the fire protection program. Commitment, requiring demonstration at senior management level of the high priority of safety and adoption by individuals of the common goal of safety. The fire prevention program consist of administrative policy, procedures, and the practices for training of general plant personnel, control of fire hazard, inspections; testing and maintenance of fire protection systems and features; control of plant modification; control of fire system outages and impairments; and fire protection program quality assurance.

The fire protection elements also consist of installation of automatic fire detection, alarm and suppression systems, including fire water supply and distribution systems. The purpose is to detect, rapidly control and extinguish promptly those fires that do occur. In addition to the automatic detection and suppression, manual suppression capability including portable fire extinguishers, standpipes, hydrant hose stations, local fire brigade and external fire department are in place to provide the needed additional defense-in-depth.

The USNRC Appendix R fire safety regulations specifically state that fire suppression systems must be installed such that the actuation of the system will not adversely impact plant safety system. Research and experience have shown that adverse fire suppression effects, and potential for significant risk impact on plant safety system exist. It is recommended that the anticipated new reactor program, fire risk analysis include consideration of potential fire suppression induced equipment damage, and that the new reactor design include provisions for the management of fire suppressants following either advertent or inadvertent release.

Fires and fire suppression systems can also compound the problem of access control through induced failure of the access control system. For new production reactor, the plant designers and the plant operations staff must recognize that the requirements of plant security and plant operations can be in conflict. A proper balance must be achieved which both ensures plant security, and yet will not inhibit the ability of plant operators to respond to emergencies, including fires. This balance should be considered and engineered on the particular plant design which will determine which areas of the plant may require unimpeded access in the event of a plant emergency and at the same time catering for security needs. The security and safety balance challenge can be solved to greater extent when considered at planning stages and appropriately engineered in both construction and operation.

The USNRC has developed a number of requirements for the design of control room ventilation systems to ensure the habitability of the control room in the event of a plant accident. These include the protection of ventilation system components and power sources, the ability to isolate the control room from all external inputs, and requirements to provide emergency air supplies within the control room for the use of plant operators. In terms of fires safety, two different concerns apply, namely, the protection of the control room environment from both internal and external fires.

A review of control room habitability requirements [36] revealed that the current requirements for the isolation of the control room in the event of a plant accident were considered adequate to deal with the potential for smoke to be introduced into the control room due to a fire in some other part of the plant. However, it was also found that the necessity and capability of a control room smoke purging systems were not adequately covered in the existing guidance.

Regulatory Guide 1.120 (RG 1. 120) [75] and BTP CMEB 9.5-1 [76] specify that the method for combustion products removal should be established during the initial stages of the plant design and that the use of the normal ventilation system is acceptable for smoke removal if it is “available and capable. ” However, RG 1.120 and the BTP do not provide a basis for evaluating the smoke removal capability.

Often new comer country, it is recommended that the ventilation system for the main control room, and possibly for other vital plant areas, in particular the remote shutdown station, be designed so as to support combustion products removal. However, it should also be recognized that a fire of sufficient size will overwhelm even a well-designed smoke removal system. Procedures should be established for the abandonment of the main control room in the event that an uncontrolled fire occurs. Further, emergency air supplies, which include eye irritation protection, should be available for all of the plant operating staff in the control room.

The operating experience of commercial nuclear power plants includes numerous transformer failures which have resulted in severe fires [36]. Many of these fires have also resulted in significant challenges to operational safety.

For new production reactors special considerations should be given to the selection and placement of plant transformers. In summary, oil-filled transformers should not be used inside of the primary plant structures, all external transformers should be spatially separated from primary plant structures, and redundant transformers should be segregated from each other by missile and fire barriers. All large transformers should be provided with fixed fire protection systems, and these systems should be clearly identified and located so as to minimize the potential for multiple spurious fire suppression system actuations to induce a common-cause loss of off-site power.

The issue of control system interactions associated with control room fire scenarios has been observed to be problematic. The concern focusses on the potential for a control room fire to induce multiple spurious actuations and equipment failures prior to the transfer of control to the remote shutdown station. The recommendation is that the anticipated fire risk analysis (PRA) include consideration of potential multiple spurious actuation and component failures during control room fire. The identified vulnerabilities can likely be resolved through the inclusion of fire barriers and train segregation within the control panel complex.

The specific concern associated with the issue of smoke control and manual firefighting effectiveness focus on the fact that most commercial nuclear power plants place a high level of relevance on the ability of on-site personnel to provide for fire suppression. Both the Appendix R and the Standard Review Plan (SRP) requirements include provisions for the staffing and training of manual fire response teams at all operating reactor sites. However, these requirements ensure only minimal training for firefighting personnel. For example, if only the minimum standards of training are implemented, plant personnel assigned to the fire response teams may never receive live-fire training. It is a good practice that the plants have included at least one qualified plant operator on each manual fire response team. This is an important and prudent consideration as it is vital for the manual fire response teams to recognize the operational importance of a given fire area or a given component in that area. This will help to ensure that potentially significant collateral damage induced by suppression efforts is minimized in responding to a fire situation.

Finally, from the USNRC experiences and documented reports [36] it is recommended for new comer countries like Ghana that the new production Reactor (NPR) design consider the following factors:

- Provisions should be made for the management of water in all areas where water is expected to be used as a fire suppressant. This should include water from either fixed suppression systems or manual hose stations.

- Provisions should be made to manage gaseous suppression agents following discharge. This should include consideration of appropriate ventilation discharge paths and administrative procedures for the venting of suppression agents and fire products from the fire area.
- Floor penetration seals should be water tight for areas in which water is likely to be employed as a fire suppressant, including manually applied water.
- Cable and conduit penetrations into electrical cabinets should be sealed to prevent water intrusion in any area in which water is likely to be used as a fire suppressant, including manually applied water.
- Electrical conduits should be examined for the potential to channel water to sensitive components and sealed if necessary. In particular, conduits which pass form one fire area to another should be examined.
- C02 discharge nozzles should not be located near components sensitive to freezing such as integrated circuits, circuit breakers, motor control centers, and relays. (Based on a the accumulated experience of the fire protection community, a distance of at least 10 feet (3.048 m) is generally considered adequate to mitigate the immediate cooling effects of gaseous discharge.)
- Multiple gaseous storage tanks should be used for multiple suppressant systems rather than a single large storage tank to service many systems. (One incident has occurred in which a plant's entire suppressant inventory was discharged into a single fire area.)
- Placement of fire protection system control panels should ensure that a multiple safety system vulnerability is not created through the potential for common mode failures to occur in multiple actuation control panels (for example, from fire induced damage or from a steam line break).
- Suppression system design should consider the significance of potential inadvertent actuation induced equipment damage. Designs must consider a balance between fast response and inadvertent actuation likelihood. (For example, automatic deluge sprinklers are the most likely type of suppression system to be spuriously actuated. The use of a wet pipe or pre-action system would reduce the likelihood of spurious actuation though might increase system response times.)
- Suppressant system actuation switches should be clearly marked, including a clear description of the protected area or equipment, and should be protected from inadvertent actuation due to casual contact. (Incidents have occurred in which personnel have accidentally set off systems not realizing they were manipulating an actuator handle, and in which personnel have set off several systems because they were uncertain as to which system provided coverage to a specific fire area.)
- Single smoke detectors should not be used as the sole criteria for the initiation of fire suppressant discharge (at the least, multiple detection logic or cross zoning should be employed, or an alternate detector type should be employed, particularly in areas of high humidity, high dust levels, or potential steam leak areas).
- Administrative procedures are needed to ensure that routine plant maintenance activities do not inadvertently set off fixed fire suppression systems. (For example, welding or cutting operations might require that smoke detectors be deactivated, and a fire watch be

posted. Procedures should also ensure that fire protection systems are properly restored upon completion of work.)

- Fire hazards analyses and fire risk analyses should consider fire suppressant discharge, either inadvertent or advertent, as a source of equipment failure.
- All plant personnel should be trained in the use of hand-held fire extinguishers, and should be made aware of fire emergency procedures.
- Fire protection systems in diesel generator areas will require special consideration. These systems should be seismically qualified to ensure that spurious actuation during a seismic event will not occur. Diesel generator cooling systems and combustion gas intakes should not be compromised by the actuation of gaseous suppression systems. Generator support equipment (control panels, wiring, junction boxes, fuel supplies, motor control centers, etc.) should be protected from water intrusion induced damage. The design should ensure that common mode failure of multiple generators cannot occur due to fire suppression efforts (either manual or fixed systems).
- The plant design should consider the potential for a seismic event to induce the actuation of fire protection systems. This introduces the potential for common cause failures of multiple safety systems and may require that the fire protection systems in certain critical plant areas be seismically qualified to prevent spurious actuation. In one case in particular, scenarios involving the failure of both off-site and on-site power source have been postulated at operating reactors. However, the concerns also extend to other plant areas and systems.

5.2.2 NRC FIRE PROTECTION RESEARCH EFFORTS OUTCOME

Under the leadership of USNRC fire protection program (FPRP), a number of individual efforts involving both analytical and experimental, associated with broad range of NPP fire safety issues have been performed.

Research on fire source characterization is associated with the identification of potential fire initiation sources and the characterization of the burning behavior of these sources. Detection and suppression system effectiveness includes consideration of the degree of additional safety afforded by such systems, and the adequacy of the general industry guidelines for system implementation in nuclear power plant applications. Room effects issues are associated with the mechanisms for the transport of fire products (heat, smoke, etc.) within the room of fire origin. Equipment response issues are associated with the effects of a fire environment on the operability of plant components. The final area, room-to-room fire effects, is associated with the potential adverse effects of a fire beyond the room of origin. These effects include fire spread through barriers, the management of fire products and fire suppression agents, manual fire brigade accessibility issues, and spurious suppression system operation in uninvolved areas.

As a result of the USNRC- sponsored fire safety research efforts a number of insights into fire behavior, fire mitigation strategies, fire induced equipment damage, and fire analyses have been realized. These insights serves as critical lessons for countries planning to embark on nuclear power project especially those in sub-Sahara. Based on these insights, it is recommended that the following factors be considered in the design, construction and operation of new production reactors:

- Despite the use of low flame spread cables, fires in cable installations should be anticipated and appropriate mitigation measures put in place. The FMRC cable selection protocol report provides a sound engineering approach to cable selection and fire protection.
- Water is considered the most effective suppressant for application to cable installations.
- Gaseous suppression agents, $C0_2$ and Halon, can be effectively employed against cable fires. However, designs must allow for the maintenance of suppressant concentrations for up to 15 minutes to ensure effective suppression of deep seated fires. (Halon is not expected to be used as a fire suppressant due to its ozone depleting properties.)
- Severe fires have been observed during the testing of electrical control panel fire behavior, even when low flame spread cables were installed. Control panel designs should recognize this potential by maintaining safety train segregation and by providing appropriate fire barriers to subdivide panel installations (such as in the main control room and the remote shutdown area). These segregation provisions should include the consideration of cable routing paths, particularly cables routed above the electrical panels themselves.
- For cable tray installations, local flame barriers and fire retardant coatings can reduce, but not eliminate, cable fire hazards. For new reactors, such measures should not be relied upon as the sole means of providing protection to redundant trains of safety equipment from the damaging effects of a single fire. Segregation into separate fire areas should be the preferred method for achieving protection for redundant safe shutdown capability.
- During testing, component (cable) damage has been observed due to hot layer effects alone, even when these components (cables) were separated in accordance with the Appendix R spatial separation requirements. The preferred method for the protection of redundant safe shutdown equipment from the damaging effects of a single fire should be segregation into separate fire areas as defined by three-hour-rated fire barriers on all sides.

If properly designed and installed, carbon dioxide and Halon suppression systems will eventually extinguish even deep seated fires such as those encountered with cable installations. However, the maintenance of proper concentrations of suppression agents for sufficient periods of time is critical to prevent re-ignition.

Gaseous suppression agents applied during a fire permit enclosure temperatures to remain higher than do water based suppression systems. Sensitive control circuitry may experience loss of function and/or calibrations shifts during extended exposures at even relatively mild temperature elevations.

Cable and ventilation duct wall penetration seals can allow hot gases and flame to pass through prematurely under conditions of positive pressure differential if the seal system is such that air passages are incorporated, even though such penetration seal systems may pass standard U. S. fire barrier qualification tests.

Testing has shown that cables can fail at temperatures well below the material ignition temperatures. Electrical cabinet fires which consumed all of the available combustible materials within approximately 15 minutes of ignition were observed for both IEEE-383-74 rated low flame spread cables and for nonrated cables. For the nonrated cables, full involvement cabinet fires can be electrically initiated as a result of a low intensity (less than 15 Ampere) simulated electrical fault.

The deterministic criteria of the Appendix R guidelines do not address the residual risk associated with probabilistic events such as multiple faults, multiple spurious operations, and multiple random equipment failures.

Manual firefighting and operator control and recovery actions may be severely hampered by the rapid development of a thick toxic smoke layer during cable fires, even in very large rooms having high forced ventilation rates. Standard approaches to the design of industrial ventilation systems, including those installed in current nuclear power plants, do not include the consideration of smoke removal as a design constraint. Therefore, these ventilation systems cannot be expected to provide effective combustion products removal, and may, in fact, aggravate the spread of combustion products to nonfire areas.

Research has shown that Chlorides released during PVC cable insulation fires were observed to become bound to smoke particulate which was subsequently deposited on surfaces throughout a fire enclosure. These chlorides, when combined with water, can form a highly corrosive and electrically conductive deposit.

5.3.0 OBSERVATIONS FOR NPP FIRE SAFETY ASSESSMENT METHODOLOGY-USA

The deterministic fire safety assessment methodology has been used from the early development of nuclear power plants. Initially, this method was based mainly on inspections, components and system analyses, have gone through research and development to the use of computer-based programs. A progressive development of deterministic methods of fire was directed towards how well the defense-in-depth approaches of fire prevention, suppression and mitigation are adequate. A key element of the safety analysis for a nuclear power plant is the demonstration that defense-in-depth is adequate, and deterministic safety analyses play a vital role in this demonstration. This method continue to lead the fire risk assessment at NPP.

5.3.1 PROBABILISTIC RISK ASSESSMENT (PRA)

The first attempt to estimate quantitatively risk due to fire appeared in the final report of the Reactor Safety Study in 1975. A more detailed quantitative risk analysis of fire in USA, was in the Clinch River Breeder Reactor risk assessment report. Specific advancement were made by development of physical model for fire propagation and suppression of fire at NPP. Advancement of fire risk analysis methods has resulted in widespread development of detailed fire probabilistic risk assessment at nuclear power plants. The Fire PRA models are maintained and frequently exercised to help ensure safe reliable, and cost-effective operation of NPP.

Fire PRA has achieved sufficient credibility and value with the nuclear industry. The USA federal regulation was amended to allow implementation of the risk-informed, performance-based protection standard NFPA 805; as an alternative to the traditional prescriptive fire protection requirements.

In 1998, the NRC issued a regulatory guide1.174 [77] providing a framework for using PRA to support risk-informed changes to the plant license basis. This regulatory guide along with continued advancement in PRA methods and data, supported a growing interest and actual implementation of the risk-informed applications by NPP operators

The fire PRAs developed in the early 1990s tended to be treated as ‘‘single use analyses’’ to support response to Generic Letter 88-20 Supplement 4 [78]. They tended not to be maintained current with the as-operated plant and with the methodological advancements occurring over the years. So, the 2004 amendment of the fire protection regulation (10 CFR 50.48 [61]) to allow implementation of NFPA 805, as well as the growing interest in other risk-informed applications, spurred a new wave of detailed fire PRA development at most U.S. nuclear power plants. These most recent analyses are generally being performed with the guidance of NUREG/CR-6850 [41], a significant advance from the previous methodology [63], and the fire PRA consensus standard (Part 4 to the ASME/ ANS-RA-Sb-2013 [47]).

The Fire Risk Re-quantification study has resulted in the state-of-the-art methods, tools, and data for fire PRA for commercial NPPs. The documented methods are intended to support future applications of fire PRA, including risk informed regulatory application.

The objective is to consolidate recent research and development activities into a single state-of-the-art fire PRA methodology. This will provide a structural framework for the overall analysis as well as specific recommended practices to address key aspects of the analysis. The approach is to develop the fire PRA methodology document involving a consensus process design to fully debate and build consensus on past methodological issues.

The methodological issues raised in the past fire risk analyses, including Individual Plant Examination of External Events (IPEEE) fire analysis have been addressed to the extent allowed by the current state-of-the-art and the overall project scope.

5.3.2 RISK-INFORMED, PERFORMANCE-BASED APPROACH

Over the years there have been a considerable movement in the nuclear power industry from prescriptive rules and practices towards broadened use of risk information to supplement decision-making.

In the area of fire protection, this movement is evidenced by numerous initiatives by the U.S. Nuclear Regulatory Commission (NRC) and the nuclear community worldwide. In 2001, the National Fire Protection Association (NFPA) completed the development of NFPA 805, “Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants 2001 Edition” [30]. Effective July 16, 2004, the NRC amended its fire protection requirements to permit existing reactor licensees to voluntarily adopt fire protection requirements contained in NFPA 805 as an alternative to the existing deterministic fire protection requirements [75]. In addition, there is significant recent emphasis on risk-informed decision-making under the current 10 CFR 50 Appendix R rule concerning changes to the plant’s fire protection licensing basis, requests for exemption or deviation, and the evaluation of inspection findings.

The Risk-informed methodology has gained a lot of acceptance in the sense that it can assist management decision makers by providing a structured, consistent method to quantify risk, evaluate risk reduction alternatives, and perform cost/benefit analysis. As a starting point the decision makers must understand the concept of risk, risk-based program motivation, risk methodology, and project management issues.

The risk-informed, performance-based approach fire protection validity base steps follow appraisal, analysis, performance and assessment. The appraisal start with program objectives and risk tolerance; whilst analysis seek loss scenarios development, initiating event likelihood and exposure profile modeling. Then, fire protection system (FPS) performance success probability leads to assessment of risk estimation and comparison with risk tolerance. The final step involving cost/benefit analysis of risk reduction alternatives.

5.3.3 MATURITY AND REALISM OF FIRE PRA

Fire PRA has been described as being less matured and less realistic than internal Events PRA. On the other hand, in a PRA context, the concept of realism addresses the degree to which an analysis represents the technical and organizational system relevant to the decision problem. The analytical methods, models, tools, and data of a less mature discipline could, but need not, produce unrealistic analysis results. Conversely, a more mature discipline could, for practical reasons, employ technology with known weaknesses, only requiring that the weaknesses be understood and appropriately addressed in the decision making process.

Fire PRA, as with PRA in general, is aimed at identifying risk-significant scenarios and quantifying their likelihoods and consequences. In practice, the analytical resources of U.S. fire PRAs are typically focused on scenarios leading to core damage and large, early release. To accomplish this, the analysis, as indicated by past and current guidance, is iterative [65, 66]. Potentially important scenarios are identified, conservatively assessed, and passed on to more detailed analysis stages if they meet certain screening criteria. The intent is that the overall results of the analysis be sufficiently realistic for the purposes of the study; there is no guarantee that the analyses of non-contributing scenarios, some of which may be important contributors to intermediate end states (e.g., loss of specified safety functions but not core damage), are realistic.

The fire PRA maturity and realism issues are often raised together. Although, they are related, they are actually separate. The concept of maturity addresses the relative state of development of a technical discipline. On the other hand, in a PRA context, the concept of realism addresses the degree to which an analysis represents the technical and organizational system relevant to the decision problem. The analytical technology (i.e., methods, models, tools, and data) of a less mature discipline could, but need not, produce unrealistic analysis results. Conversely, a more mature discipline could, for practical reasons, employ technology with known weaknesses, only requiring that the weaknesses be understood and appropriately addressed in the decision making process. PRA results and insights are increasingly used in regulatory applications as well as NPP operations. These applications ranges from the approval of changes to plant licensing basis, the assessment of the significance of inspection findings. Thus, from plant-specific to industry-generic issues in the assessment of safety issues affecting more than one plant, and the determination as to whether new regulatory requirements should be imposed on industry. So far as, the method has an increasingly both industry and regulatory applications, it cannot be said to be non-realistic. However, the conservatism weaknesses needed to be addressed through research and development. Of course, the practitioners of a less mature discipline might consciously use conservative (and potentially unrealistic) assumptions in an attempt to compensate for weaknesses in the current state of knowledge – the extent and appropriateness of this practice is a key controversy in ongoing U.S. fire PRA applications.

Fire PRA, as with PRA in general, is aimed at identifying risk-significant scenarios and quantifying their likelihoods and consequences. In practice, the analytical resources of U.S. fire PRAs are typically focused on scenarios leading to core damage and large, early release. To accomplish this, the analysis, as indicated by past and current guidance, is iterative [41]. Potentially important scenarios are identified, conservatively assessed, and passed on to more detailed analysis stages if they meet certain screening criteria. The intent is that the overall results of the analysis be sufficiently realistic for the purposes of the study; there is no guarantee that the analyses of non-contributing scenarios, some of which may be important contributors to intermediate end states (e.g., loss of specified safety functions but not core damage), are realistic.

Several analyses raised concerns regarding model input and calculated consequences, however, if the steps and acceptance criteria set out in PRA guides, these weaknesses can be minimized if not cured.

Qualitatively comparing the U.S.A. and international precursor description with the fire PRA results, it appear that the fire PRA are doing reasonably well with respect to realism. Most of the important scenarios identified by the fire PRA appear to have basis in operating experiences.

The current fire PRA framework and approach remains largely as described by Apostolakis et al. [43] and the PRA Procedures Guide, NUREG/CR-2300 [18]. However, in the years since the initial applications of this methodology (e.g., the early 1980’s Indian Point PRA), considerable work has been performed to improve the realism of specific modeling elements. In the late 1990’s, NRC/RES initiated a fire PRA research program whose efforts were guided by a structured identification and evaluation of potential problem areas. [79] Using results from that program and parallel industry activities, RES and EPRI jointly developed NUREG/CR-6850 (EPRI 1011989) and Supplement 1 to that document.10, 11 these documents provide the principal technical guidance available for current U.S. fire PRAs.

According to Siu et tal [80] based on the results of analysis of available information, the fire PRA is in an intermediate-to-late stage of maturity (albeit less mature than internal events), and that the quantitative results of current fire PRAs, as performed using current guidance, may be conservative (to an uncertain degree). Some of the observed conservatisms may arise from practical modeling choices made to reduce analysis effort, and others are likely due to limitations in current fire PRA technology and guidance.

From a qualitative standpoint, it can observed that current fire PRAs compare well with operating experience. Most of the important scenarios identified by the fire PRAs appear to have a basis in past precursor events (U.S. and international), and most of the precursor events represent, at a high level, scenarios involving fire sources and induced plant transients typically included in fire PRAs.

As a potential realism concern, it can be noted that some fire PRAs identify yard fires as being important risk contributors – this result does not seem to be consistent with operational experience. We also note that current fire PRA technology does not address some notable features of a number of precursor events, including multiple fires, multiple hazards, and non-proceduralized recovery actions. Nevertheless, the fire PRA methodology is recommended for new production reactors and the notable features of multiple fires multiple hazards and non-proceduralized recovery actions will be well addressed with time and intense research. For NPR, it is recommended that a full-scope PRA be performed, including the consideration of fire as an event initiator. It is further recommended that a methodology, such as that employed in the NUREG- 1150 analyses, which utilizes the full internal events fault trees as the basis for analysis be utilized.

5.3.4 INADEQUENCIES IN CURRENT ANALYTICAL FIRE MODELS

It has been observed that significant questions of computational accuracy and overall code adequate remain unresolved for the computer fire simulation models which are currently used to support the assessment of fire risk for the U.S. commercial nuclear power plants. For new production reactors it recommended that an improved fire analysis model be assembled using currently available time modelling capabilities. This model must address the unique needs of a nuclear plant risk assessment and should be benchmarked by comparison to enclosure fire test data which is gathered as part of the USNRC, IAEA and global fire protection research activities.

5.3.5 UPDATING OF FIRE EXXPERIENCE DATA BASES

It has been recognized that one of the fundamental input used in the analysis of fire risk is experience based on the information on the frequency and impact of actual fire related incidents. In particular, new comer countries will depend on the commercial nuclear industry who have logged significant base of experience with both actual fire incidents and incidents involving the advertent or inadvertent actuation of fire suppression systems. It is recommended that these data bases be updated and /or formalized for use by new production reactors in the analysis of fire risk

5.3.6 USE OF EXPERT JUDGMENTS IN QUANTIFCATION ANALYSIS

In the analysis of fire risk methodology, some of the most significant sources of uncertainty is that associated with the use of expert judgments. For new production reactors it is recommended that procedure is be formalized for the incorporation of such judgments in new production reactor fire risk assessment. It is expected that formalizing of the existing methodologies will be required to comply with the stringent new production reactors quality assurance requirements.

Similarly, the available data on the vulnerability of plant equipment to fire induced damage is very sparse. For new production reactors it is recommended that NPR specific component vulnerability data be gathered. This data will be needed to support equipment damage assessments as a part of the fire risk assessment.

5.4.0 OBSERVATION AND RECOMMENDATIONS ON GERMANY NPP FIRE SAFETY

5.4.1 Observations on Germany nuclear power plant fire regulations

The development of nuclear power plants which was started in the early of 1960 were regulated by the Basic law and the Atomic Energy Act of 23 December 1959. This is followed by the general and administrative regulations and the nuclear power plants safety criteria promulgated as at October 21, 1977. Reactor safety commission (RSK) guidelines and Nuclear Safety Commission (KTA) standards were the order of nuclear safety laws in Germany.

The fire protection regulation of the building code governed the construction of the earlier nuclear power plants. The main objective of the Basic law, the primary requirement, is to ensure that life and physical integrity of persons are protected. That also means that a fire shall not have any consequence to the life of an individual: This implies that both for persons who are close to the fire in the NPP and those, who are far away from the NPP fire but could be affected by the fire.

In Germany, the NPP fire protection law developed out of the Basic law through the Atomic Energy Act. The general administrative regulations to the NPP safety criteria and the Reactor Safety commission guidelines, were purely deterministic. In all these levels of the laws and the building code the deterministic approach of the industrial fire safety were applied.

From the historical review it has been observed that, it took a decade instead of the planned five years for the KTA2101.1 ´´Basic principles of fire protection in NPP´´ to be published as a valid fire safety standard from the date of the establishment of the Nuclear Safety Commission (KTA).This only form the first part of the nuclear safety standard. The other two parts; Structural elements, mechanical and electrical components were published in December 2000. It took a decade and half to reach consensus on this parts which contains the technical details of the standard KTA 2101. During the eighties the velocity for progress was influenced by the conflicts between existing atomic and conventional requirements, during the nineties it was the conflict between acceptance and rejection of nuclear power in general, also within the different groups of authorities with nuclear responsibilities.

It is an important feature of German technical legislation and has long lasting tradition that technical safety standards are developed by commissions which are appointed by Ministers of the Federal Government rather than by governmental agencies or by private institutions. Such commissions were the model for the formation of the German Nuclear Safety Standards Commission, the KTA, It belongs to the realm of the public law and is indeed neither a governmental agency nor a private organization, like the German Standards Institute (the DIN) or the American Society of Mechanical Engineers (the ASME) or the American Nuclear Society (the ANS). Therefore, it is recommended that Ghana develop it nuclear safety standard not along the line of KTA which is non-governmental and non-political. Rather the nuclear regulatory Authority adopts applicable well developed international standard with the involvement of Professionals, civil society and all identified stakeholders.

The Germany Nuclear power plants fire safety standards and regulations are goal oriented and not prescriptive, like what pertain in USA. Therefore, the formulation of the standards are based on consensus and needed all relevant players on board. As high as, not less than 80% of the membership of the full section of the members of the commission must approve the draft standards. The goal oriented standards and regulations are recommended for Ghana provided the needed technical expertise are available to apply the appropriate acceptance criteria and judgment.

However, as high as, 80% of the membership of the full section is on the high side and cause unnecessary delays in the formation of these standards

The membership of the commission is fair representation of the five identified relevant groups and not only a membership representation, but rather ten members from each. This approach might have challenges in Ghana because the membership to be drawn from the manufacturers and vendors of nuclear facilities are unavailable in the country. The large numbers for the commission is understandable because of the opposition and nuclear energy politics in Germany. However, consensus with stakeholders and interested groups as well as depending on the experiences of other countries will go a long way to develop a fire safety standards at nuclear power plants.

Therefore, finding a consensus on a technical aspects on behalf of the elaborating safety standards is sensible especially when commercial markets are no more closed and open for everybody. However, it is necessary that to find consensus is not too long. To be able to realize this it is necessary generally to restrict on the basic principles and not concentrate on detailed requirements. Such requirements should be left into the responsibility specific licensing and supervising process.

Also, it has been observed that the implementing organizations own the regulations when consensus is reached, making implementation smooth, and no need to further explain or clarify the standards like the norm in USA NRC regulations implementation.

There were overlapping issues in KTA 2101.1, KTA2101.2, and KTA2101.3, for Basic Principles, Structural elements, and Mechanical and electrical Components parts respectively. Updates were carried out to harmonize all the three parts of the KTA 2101 ´´Fire protection in Nuclear Power Plants´´. The requirements of the standard were updated to the actual state-of-the-art, most recent knowledge in the field, and non-nuclear standards and norms. The updates also cover lessons learned from the Fukushima Dai-ichi nuclear power plant accident and sections have been formulated more consistency with international requirements especially IAEA and WENRA. All these updates were aimed at making the fire safety standard at Nuclear Power Plants in Germany a living document and up-to-date. Though, the thoughts of the future of nuclear power plants in Germany is derailing the efforts in the development a living document and up-to-date state-of-the-art nuclear power plant fire safety standards and regulation through research and development.

In the Federal Republic of Germany, probabilistic safety assessment is used to supplement the deterministic safety assessment to demonstrate safety of nuclear power plants including fire safety. This is documented in the safety requirements rules and regulation of Nuclear Safety and Radiation Protection. However, regulatory guide are provided for PSA applications based on international and local experiences and no standards are published yet.

5.5.0 OBSERVATION AND RECOMMENDATION ON GERMANY NUCLEAR POWER PLANT FIRE PROTECTION

In Germany, Nuclear power plants (NPP) are protected against internal and external fires by a fire protection defense-in-depth concept including the following precautionary measures: operational, structural and equipment related fire protection measures as well as manual firefighting. The fire protection measures are designed in consideration of fires to be expected (from fire loads permanently and temporarily present together with potential ignition sources) in order to prevent a violation of both the protection goals of public law and the nuclear protection goals / radiological safety objectives in case of internal and external fires

The fire protection in the NPPs have evolved through the use of building and industrial code to the use of the KTA 2101 nuclear power plants fire safety standard. Thus, the earlier nuclear power plants built based on the buildings and industrial code have been upgraded to support the nuclear safety objectives. By the upgrade resulted in addition of partial physical separation of safety systems´ redundancies and fire barriers for areas or rooms with high fire loads. These were absent during the initial construction as a result of lack policy and recognition of fire risk to the safety systems of the plants. However, in situations where the separation and fire barriers are not feasible adequate fire protection systems, measures are put in place to protect safety relevant systems and equipment. This is achieved by utilization of operational fire protection through Quality assurance (QA), periodic preventive inspections and preventive maintenance. Germany nuclear power plants have been to greater extent successful in decreasing fire risk, and even if fires do occur they are promptly and decisively brought under control.

Thus, passive fire protection are developed and implemented to ensure prevention of occurrence of incipient fires through fast and reliable fire detection and suppression. In case failure occurs, through fast and reliable prompting system and limitation of fire spread to other areas, the fire is brought under control by efficient active firefighting.

5.5.1 FIRE DETECTION AND ALARM SYSTEMS

The fire detection and alarm systems are designed against earthquakes. Seismically designed fire detection and alarm systems are available and represent the state-of-the-art systems. It is alternatively permissible to assume that fire detection and alarm facilities stays available after earthquake, and failure of components in the fire alarm control center be replaced by exchanging the modules or repaired at short notice

5.5.2 FIRE EXTINGUISHING SYSTEMS

Suitability of stationary fire extinguishing systems in fire extinguishing areas typical for nuclear power plants has been changed as a result of the availability of various new fire extinguishing systems with gas, water, foam or combinations of extinguishing agents as extinguishing media.

It has been observed that, water extinguishing systems with both normal nozzles and fine nozzles are not suitable in switch gear building with more than 1000 V, but the fine nozzles can partly be suitable for transformers in closed-off rooms. However, the normal and fine nozzles water extinguishing systems are mostly suitable in large assemble of cables: partitioned off in cable ducts or channels, cable wells and cable rooms. But normal nozzles are not suitable in rooms with data processing and electronics.

Sprinklers systems are suitable for fuel-oil containing components and systems partitioned off areas. The Sprinkler is suited as fire protection of equipment, provided, the remaining fire loads are individually protected by a fire extinguishing system for Large assemblies of cables and cable transition points: not partitioned off. Slow triggering behavior; additional measures against smoke dissipation might be required in case of Rooms with electronic data processing and electronics.

Heavy foam are not suitable in most areas except, at transformers and fuel-oil containing components and systems, where Foam must be applied with sufficient adhesion to be effective with regard to fire extinguishing.

To sum up the fire extinguishing effects of the various stationary extinguishing systems, it may be stated that sprinkler and spray deluge sprinkler systems are suitable without any restriction for cable distributors, transformers and oil containing systems and components. Gas extinguishing and sprinkler systems may also be used without restriction for oil containing systems and components. For data processing and other electronic and switchgear compartments, they are considered suitable with certain restrictions; for example, the sluggish activation behavior of sprinklers or excess pressure build up problems, as well as personnel protection problems in the case of $C0_2$.

In conclusion, fire protection measures need not be specified in a single approach, but rather, the concept be related to aspects as well as the great variety of possible fire protection measures. Fire protection can only be an efficient tool if plant specific fire concepts are developed for future perspective to new nuclear facilities, as well as, in retrospect, to older facilities. For positive and enhanced development of fire protection systems, it is appropriate to document, evaluate and make available to planners of facilities the experiences gained from the frequency of fire inceptions and the reliability and efficiency of fire protection systems. As far as operating nuclear power plant facilities are concerned, it is absolutely appropriate to check at regular intervals whether the assumptions on which the original fire protection concepts was based still holds and relevant, in spite of possible changes in the plant conditions.

5.6.0 OBSERVATIONS ON SAFETY ASSESSMENT METHODS IN GERMANY

Historically, most of the engineering work in designing NPP fire protection features in Germany has been performed on deterministic basis. The use of deterministic fire safety analysis is the current practice in Germany to review the fire protection states of the operating NPP. This method has been used to satisfy regulatory requirement. It has been used to justify the arrangement for identifying how fire occur. The arrangement involves the following:

- Identification of how fire can occur and spread,
- Assessing the vulnerability of plants equipment and structures
- Determining how the safe operation of plants is affected
- Introduction of measures to prevent a fire hazard from developing and propagating
- Mitigation of its effect.

The effective utilization of the deterministic method ensure and guarantee the adequate degree of the defense-in-depth of the fire protection systems and programs. The successful and effective implementation of the deterministic methodology of fire safety at NPP have led to comprehensive backfitting and upgrading measure. More importantly, for the NPP built to earlier standards, structural fire protection measures as well as active fire detection, alarms, extinguishing features, and administrative fire protection measures have resulted in significant fire safety.

It has been observed that, the probabilistic approach provides different insight into design and availability of systems and components. It supplements the results from deterministic analysis and enhance the understanding of fire risk. The recommendation is that the state-of-the-art integration of deterministic and probabilistic methods fire safety assessment should be adopted so that the weakness and the strengths of each the methods is complemented

5.6.1 GERMANY NPP FIRE PSA

The Probabilistic Safety Assessment (PSA) has been taken into account for decision making on a case-by-case basis for fire protection at the Germany NPP. It has been accepted as risk-informed supplementary tool for deterministic fire safety assessment. The state-of-arts approach PSA has been developed in Germany.

In 2005, Germany issued a regulatory guide for PSA for performing Periodic Safety Review (PSR). The guide contains reference listings of initiating events for NPP with PWR and BWR. The plants internal fires are included. Detailed instructions for the analysis of plant internal fires, fire frequencies, and unavailability of fire detection and alarm system as well as data.

The fire PSA was tasked to determine the annual frequency of fire induced core damage states (FCDF) of the NPP within the in advance defined global analysis boundary. The set of all compartments is the starting point for fire analysis. An established screening process is done to screen out compartments with low fire load density which do not impact the fire PSA results. The screening process to identify critical fire compartments is an important first step within the fire risk assessment.

The screening analysis should not be too conservative so that an unmanageable number of fire scenarios remains for the detailed quantification analysis. Two ways are identified for the screening: namely, qualitative screening and screening by frequency.

Qualitative screening allows the determination of critical fire compartments with a limited effort, whilst, screening by frequency, critical fire compartment are identified by means of a simplified event trees analysis. The success of effective screening is dependent on quality of data for the analysis. The uncertainty associated with this analysis needs to be taken into consideration.

The partitioning of the NPP into compartments is an important step in performing fire PSA. In the frame of this step of the analysis it is a major task to make available all data and information necessary to calculate the compartment related frequency. In no small way will appropriate data reduce the uncertainty associated with the analysis. Inadequate database with result in aleatory uncertainty and therefore, the questions of database needed to be addressed. It is recommended that Ghana establishes a formalized system of gathering, processing, and storing data relating to safety including fire.

5.6.2 FIRE PSA DATABASE IN GERMANY

Performing a qualitative fire risk assessment, a comprehensive database must be established which include fire initiating frequencies, reliability data for all the active fire protection systems. This means detailed information on fire barriers and their elements. Potential ignition sources, fire detection and extinguishing systems, and firefighting capabilities.

Plant specific data are applied as far as feasible, however, generic reliability data have been used as an additional unavailable plant specific data. Nevertheless, the use of international available generic data (e.g. for fire occurrence frequency), mainly the USA and France, is not always appropriate within fire PSA. This is because Germany plants have differences in design, inspection and maintenance.

The international effort, for OECD, fire database project, is in the right direction to minimized uncertainty associated with the PSA analysis. The real data from across the globe will help promote the realism of the fire PSA analysis and uncertainty associated with it can be minimized if not eliminated. The database project will provide the basis for juxtaposition of the data from difference plants in a given country or from different continent. The harmonization of methods and procedure of gathering the data will lead to effective utilization of resources and efforts and the database will provide easily available information for new comer countries. However, the use of this data must take into consideration the effect of environmental conditions under which the data was taken or is going to be used for the analysis. Without harmonization and formalization of methods and procedures adopted for the acquisition of the data from different countries the application of the data will be problematic.

5.7.0 OBSERVATIONS ON JAPAN FIRE SAFETY REGULATIONS AT NPP

In Japan, the regulatory framework is defined by a hierarchy of legal and regulatory documents: national laws, regulations (or ministerial orders and ordinances), and regulatory guides issued by NSC.

Reactor design requirements and safety criteria are contained in the NSC regulatory guides. The NSC regulatory guides are not regulatory requirements or legally binding. However, in practice licensees would comply with those guides as though they constituted requirements. This show that safety culture is well developed at Japanese Nuclear Power Plants. Thus, safety issues are taken as a culture and people are not mandated legally to do so. Yet, a culture can be broken at will if it does not go with punitive measure. No wonder the report by the National Diet of Japan Fukushima Nuclear Independent Investigation Commission (NAIIC) is very straightforward in its findings: that the fundamental causes of the disaster are to be found in the ingrained conventions of Japanese culture where reflexive obedience, reluctance to question authority, devotion to sticking with program, groupism and insularity. This should be a great lesson for Ghana that disadvantage in our culture should not affect the safety culture that is demanded by nuclear industry.

The NSC level 1 guides establishes requirements that are comparable to the design basis requirements of US. NRC regulations for NPP. The safety assessment is within the scope of design basis analyses. However, laws and standards for fire protection for domestic and industrial establishments were applied to the nuclear power plants in Japan, notwithstanding the peculiar radiations safety and the experiences of NPP fires in other countries like U.S.A. The laws and standards for fire protection for domestic and industrial establishments should not be adopted wholesale for NPP, rather the adoption should be done based on peculiar safety circumstances of NPP and the experiences of other countries in the nuclear industry.

Lessons learned after the accident at Fukushima Daiichi nuclear power station in 2011 resulted in the improvement in nuclear safety management, laws and regulations. Legally independent Nuclear Regulatory Authority was formed to regulate all nuclear activities in Japan.

5.7.1 NUCLEAR REGULATORY AUTHORITY (NRA) JAPAN

The Nuclear Regulatory Authority (NRA) Japan was established to provide for regulations and management of activities and practices for peaceful use of nuclear materials or energy. The NRA has formulated a set of new regulations to protect people and the environment from the harmful effects of radiation. The regulatory authority and its regulation are based on internationally accepted standards and guidelines of the International Atomic Energy Agency (IAEA) and other developed regulatory authority like NRC. The attention has been shifted from Japan hierarchy of legal and regulatory system. Ghana has taken a similar path by establishment of the independent Nuclear Regulatory Authority to provide for regulation and management of activities and practices for the peaceful use of nuclear materials or energy

The new fire safety regulations at the nuclear power plants are based on defense-in-depth concept. The importance is placed on equipment and structures for fire protection and countermeasures to prevent failures. In view of that, simultaneous loss of all safety functions due to common caused failures are prevented because of multiple countermeasures to prevent failure. This has caused for re-evaluation of countermeasures against internal fires and flooding. Particularly, the regulation require enhanced countermeasures to ensure the reliability of on-site and off-site power sources to deal with the possibility of station blackout (SBO). The SBOs were assumed to have no chance of happening before Fukushima accident, and looking at the earthquake prone nature of Japan, the regulation is in the right direction.

All these regulatory requirements are to strengthen the highly successful fire safety measures and ensure legally mandated enforcement.

The internationally recognized concept of performance-based requirement where operators' select concrete alternative measures to comply with fire safety requirement based on the characteristics of the facilities has been established by NRA.

5.8.0 OBSERVATIONS ON NPP FIRE PROTECTION IN JAPAN

The experiences of utilities in thermal power plants fire protection and safety culture have influenced the fire safety practices in the nuclear power plants. Effective and concrete fire protection management systems are in place at all the plants. This was evident in the number of fire, minor though reportable, incident at the nuclear power plants. At almost 50 unit power plants in the first 28 years had reported only four (4) fire incidents in 1967, 1977, 1985 and 1988. Between 1988 and 2001 three incidents are reported.

Fire protection at NPPs in Japan has been basically taken according to "Examination Guide for Fire Protection of Light Water Nuclear Power Reactor Facilities". A more specific guideline for actual design has been established in JEAG 4607, "Fire protection guideline for NPPs" by the Japan Electric Association with a commitment by Ministry of Economy, Trade and Industry (METI). Similarly, this specifies undertaking fire protection design by combining appropriately three countermeasures as; fire prevention, fire detection and extinguishment, and mitigation of fire effects, corresponding to the safety significance of the function requirements.

5.8.1 FIRE PREVENTION

Apart from high level of education for the utility staffs, positive fire safety culture and intention of preventing fire, the following measures below are identified for fire prevention at NPP in Japan.

- Use noncombustible or fire retardant materials
- Take preventive countermeasures against igniferous or flammable materials (prevention of leakage and leak expansion, consideration for layout, ventilation, and restriction of accumulation etc.)
- Prevent overheat due to over-current in electric equipment
- Prevent fire due to natural phenomenon (thunder, earthquake etc.)

5.8.2 FIRE DETECTION AND EXTINGUISHMENT

The fire safety at NPP in Japan has been impacted by integration of the well maintained, well-equipped fire detection and extinguishing systems, and routine administration of the utilities themselves. Notwithstanding, the following measures are taken:

- Allocate fire detectors and extinguishing systems appropriately (design, test, calibrate and inspection, etc.)
- Take countermeasures against failures, malfunction of equipment and/or operator
- Secure extinguishing function against natural phenomenon (earthquake, freezing, typhoon, etc.)

Mitigation of the fire effects by ensuring safe shutdown, alternative shutdown capability during control room fire and reactor safety at all times. The number of fire events with generating fire or smoke is only nine events as at 2001, which means fire protection has been appropriately taken.

5.9.0 OBSERVATION ON FIRE RISK ASSESSMENT METHODS IN JAPAN

Nuclear Power Plant fire risk assessment in Japan has been mainly based on deterministic methods. This involves the analytical evaluation of physical fire related phenomena occurring at the nuclear power plant through hazard analysis. The purpose is to demonstrate that fire safety and other safety requirements such as fire prevention, suppression and mitigation, put in place in the defense-in-depth approach of fire protection are fulfilled. Both best estimate and conservative approaches have been used in the deterministic method.

5.9.1 FIRE PRA AND RISK-INFORM METHODS

There has been sluggishness in the development of fire probabilistic risk assessment in Japan. Unlike other countries where research and data have been developed for PRA methods that of Japan had been slow. Though, Seismic PRA and other internal events PRA has been developed and recognized that PRA bring addition insight in the safety assessment at the nuclear power plants. This can be attributed to the non-availability of local database to create a realistic fire PRA model and legally enforced requirements. The complacency on the part of the utilities for their fewer recorded fire incidents.

However, the March 11, 2011 Fukushima Daiichi site accident has rekindled the interest and regulations to use PRA methods and standard procedures for fire PRA. Hence further development for seismic PRA to include other external hazards, including combinations of these hazards. Therefore, seismically induced fires and flooding are examples that typically need to be accounted for in a seismic PSA.

The Atomic Energy Society of Japan (AESJ) is at the forefront of the development of fire PRA standards. The implementation of internal fire PRA standard is under discussion at the fire PRA subcommittee of the Risk Assessment Technical Committee (RATC).

The scope of the internal fire PRA standard include fire source inside the site and fire source outside the site. Thus, inside fire caused by failure of components and human error. Also, the in-side fires caused by in-side equipment damage induced by external events such as earthquake. The fire source outside of the site caused by external events such as earthquake and the fire then spread to the site.

The standards being developed does not cover in-site fire caused by in-site equipment damaged by external events such as earthquake or flooding. The standard include the fire induced initiating events and/or loss of mitigation system and focuses on the thermal effects only. In the scope of the standard physical and chemical phenomena of the fire such as component failure due to micro-particle of smoke, and components mechanical damage due to explosion is not considered. Further discussions and enhancement to involve all these excluded issues by AESJ needed to be addressed. In addition, the discussions on the internal fire PRA standard should include a requirement providing detailed methods on circuit analysis, human error at the fire cases, and fire influenced analysis.

Finally, Japanese database for the flooding, seismic and internal fire needed to be established or enhanced. Development of methods and preparation of studies aiming to obtain realistic risk assessments, neither too optimistic nor too much conservative, is a key issue. These more realistic evaluations would provide a better view on the real problems and also a better view on the interest of safety improvements.

5.10 CONCLUDING REMARKS

The impart of fire at first generation nuclear power plants on radiological consequence as a result of Core Damage was not recognized and appropriately catered for until the Brown Ferry Nuclear Power site accident in 1975. The Brown Ferry accident resulted in strict prescribed regulations in United States of America, aside the home and industrial fire safety regulations. Similar recognition of radiological risk that can be triggered by Fire resulted in regulations and standards in Germany and other places. In Japan there were no specific strict prescriptive regulations for the NPP, this is because Japan had good fire safety culture for their industrial complexes including the NPPs. However, after the Fukushima nuclear accident Japan recognized to need to regulate all aspect of nuclear safety including fire and that resulted in formation of the Nuclear Regulatory Authority. The prescriptive fire safety regulation in USA resulted in difficult and expensive retrofits causing many NPPs applying for exemptions.

Fire protection program were instituted to protect safety related components, structures and systems. The program involves administrative, prevention, suppression and mitigation measures, Preventive measures such as Combustibles and potential fire initiators are kept out of the plant as much as possible to reduce the chances of a fire. The prevention activities involves: fire marshal, Inspectors, and training and drills. The NPP staff monitor fire hazard such as the storage of combustibles and control ignition sources as well as metal cutting and welding.

Fire suppression involves rapid detection, control and extinguishing fires that are not prevented. The fire suppression system involves automatic fixed sprinklers, fire detection, onsite fire Brigade offsite support and fire protection loops

The early designers of Nuclear Reactors could not ensure safety through the quantitative probabilistic approach. Nuclear Reactor safety was assured based on deterministic approach. The Fire-related nuclear reactor safety was assured based on deterministic approach. The analyst determine how well the defense in depth approaches of fire prevention, suppression and mitigation are working.

The importance of fire as a potential initiator of multiple system failures took a new perspective after the cable tray fire at Brown Ferry in 1975. Fire safety assessment slowly evolved with time changing from deterministic qualitative methods to quantitative PSA methods as alternative method or supplementary method.

Fire PSA had evolved growing in realism and maturity as compared with Internal Event PSA. Insights from Fire PSA had been applied in Risk-informed, Performance based approach as alternative to Prescriptive regulation. The growing use of PSA in risk-informed decision making at NPP operations and maintenance has gained recognition.

Therefore, the next chapter of this Thesis will be devoted to Fire PSA and its use in Risk-informed application at Spanish PWR NPP.

CHAPTER SIX

FIRE PSA AND ITS USE IN RISK INFORMED APPLICATION

6.0 INTRODUCTION

With the increasing maturity of the fire PSA, there is growing confidence in applying the methodology in Risk-informed decision- making at Nuclear Power Plants. The insight from PSA has contributed to risk –informed decision making in both operations and regulatory activities. Given the broad spectrum of equipment and activities covered at nuclear power plants, the regulations can be strengthened and resources can be allocated to ensure that they are focused on the most risk-significant equipment and activities, and to ensure a consistent and coherent framework for regulatory decision-making.

The applications of PSA beyond the Individual Plant Examination of External Events (IPEEE) process, a comprehensive effort to resolve comments and concerns was still needed. As a result of NRC's review of licensee submittals and based on their experience with the IPEEE program, the NRC raised a number of technical issues regarding Fire Induced Vulnerability Evaluation (FIVE) and the Fire PSA Implementation Guide [82]. While the applied methods were deemed acceptable for accomplishing the objectives of the IPEEE, it became clear that they would need upgrades to support future Risk-Informed/Performance-Based (RI/PB) applications in fire protection.

Both the NRC Office of Nuclear Regulatory Research (RES) and the Electric Power Research Institute (EPRI) were active in the development of methods for fire risk analysis during the 1990s, EPRI, in particular, developed methods to support its utility members in the preparation of responses to Generic Letter 88-20, Supplement 4, ''Individual Plant Examination of External Events (IPEEE)''. This effort produced the Fire Induced Vulnerability Evaluation (FIVE) Method [83] and the Fire PSA Implementation Guide [1.5]. FIVE was reviewed by the NRC and approved (with certain conditions [29]) for use in the IPEEE program. The Fire PSA Implementation Guide was reviewed by the NRC during the IPEEE process and, following resolution of several issues, was ultimately accepted by NRC as meeting the IPEEE goals. Virtually every U.S. nuclear utility used one or both of these documents to perform their IPEEE fire analyses.

This resulted in the EPRI/RES Fire Risk Requantification program. The principal objective was to develop a technical basis and methodology that will clarify issues affecting application of Fire risk methods. The project culminated in the joint EPRI/RES publication of the state-of-the-art Fire PSA methodology NUREG/CR-6850. It serves as an upgrade and a revision to the EPRI Fire PSA Implementation Guide [41], develop insights on strengths and weaknesses of the Fire PSA models and results; and provide specific insights on the elements of a Fire PSA expected to form the basis for Risk-informed, Performance-Based (RI/PB) applications in fire protection.

This chapter treats the overview of fire PSA methodology, insights and observation in section 6.1. Section 6.2 discusses the process for Risk-informed decision making and overview of decision making. The section 6.3 is the development and assessment of fire-related risk unavailability matrix. Fire-related system and key safety functions unavailability matrix and innovative tool for risk-informed decision-making at Spanish PWR NPP. 6.4 Understanding and assessing the impact of other risk assessment on the Unavailability Matrix.

6.1 OVERVIEW OF FIRE PSA METHODOLOGY

The fire PSA methodology described in NUREG/CR-6850 [41] follows a process that in principle, similar to the methods documented in the EPR Fire PSA Implementation Guide [84], NUREG-1150 [16], and NUREG-4840 [85]. Methodological issues raised in past fire risk analyses, including the Individual Plant Examination of External Events (IPEEE) fire analyses; have been addressed to the extent allowed by the current state-of-the-art. This methodology has brought a lot of confidence in the application and usage at almost all NPP around the globe for fire risk-informed decision-making.

The Fire PSA methodology has been described by a flow chart in Figure 6.1. Certain tasks may need refinement after conduct of one or more of the subsequent tasks. This makes the Fire PSA iterative. It may also be appropriate to incorporate only limited detail in the first pass through an analysis task, deferring the pursuit of additional detail pending the results of a later task. For example, the number of components and circuits credited in Tasks 2 and 3 is likely to be revised after attempts at screening in Tasks 4 and 7.

The qualitative screening in Task 4, the fire PSA component selection in Task 2 can be reviewed so that Fire-induced model can appropriately be modelled. Similarly, after quantitative screening-1 (Task 7A), the Task 2 Fire PSA component selection can be reviewed further. There is potential for feedback loops at virtually every stage of analysis, each potentially returning to almost any earlier stage of analysis. Analyst judgment is needed to ensure that an appropriate overall analysis process is followed.

6.1.2 DESCRIPTION OF EACH TECHNICAL TASK FOR THE OVERALL FIRE PSA

1. TASK 1: Plant Boundary Definition and Partitioning

2. TASK 2: Fire PRA Component Selection

3. TASK 4: Qualitative Screening

5. TASK 5: Plant Fire-Induced Risk Model

6 TASK 6: Fire Ignition Frequency

7. TASK 7: Quantitative Screening

8. TASK 8: Scoping Fire Modeling

9. TASK 9: Detailed Circuit Failure Analysis

10. TASK 10: Circuit Failure Mode Likelihood Analysis

11. TASK 11: Detailed Fire Modeling

12. TASK 12: Post-Fire Human Reliability Analysis

13. TASK 13: Seismic Fire Interactions

14. TASK 14: Fire Risk Quantification

15. TASK 15: Uncertainty and Sensitivity Analyses

16 TASK 16: Fire PRA Documentation

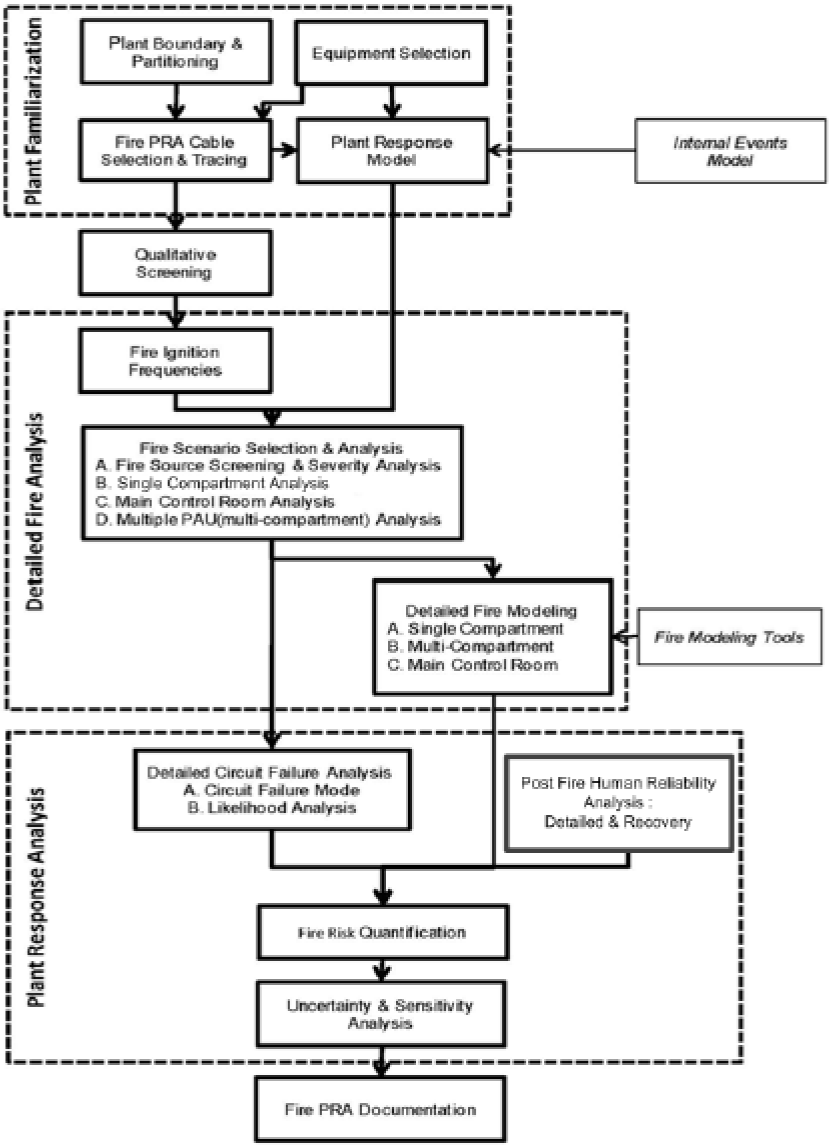

Plant Familiarization
Plant Boundary & Partitioning
Equipment Selection
Fire PRA Cable Selection & Tracing
Plant Response Model
Internal Events Model
Qualitative Screening
Detailed Fire Analysis
Fire Ignition Frequencies
Fire Scenario Selection & Analysis
A. Fire Source Screening & Severity Analysis
B. Single Compartment Analysis
C. Main Control Room Analysis
D. Multiple PAU(multi-compartment) Analysis
Detailed Fire Modeling
A. Single Compartment
B. Multi-Compartment
C. Main Control Room
Fire Modeling Tools
Plant Response Analysis
Detailed Circuit Failure Analysis
A. Circuit Failure Mode
B. Likelihood Analysis
Post Fire Human Reliability Analysis :
Detailed & Recovery
Fire Risk Quantification
Uncertainty & Sensitivity Analysis
Fire PRA Documentation

Figure 6.1 The Fire PSA methodology described by a flow chart [41]

1. PLANT BOUNDARY DEFINITION AND PARTITIONING (TASK 1)

The first step in a Fire PSA[11] is to define the physical boundary of the analysis, and to divide the area within that boundary into analysis compartments. For the purposes of a Fire Probabilistic Risk Assessment (PSA), the plant is divided into a number of fire compartments. The analysis then considers the impact of fires in a given compartment, and fires that might impact multiple compartments. This procedure establishes the process for defining the global plant analysis boundary and partitioning of the plant into fire compartments. The product of this task will be a list of plant fire compartments in the nuclear power plant under analysis.

The objectives of the partitioning task are to (1) define the global plant analysis boundaries relevant to the Fire PSA, and (2) divide the plant into discrete physical analysis units (fire compartments). The fire compartments form the fundamental basis of the subsequent Fire PSA. That is, the Fire PSA will initially consider fire threats to safe shutdown primarily in the context of the defined fire compartments. The results of the Fire PSA will be presented in terms of the risk contribution for fires confined to a single compartment and for fires that impact multiple adjacent compartments.

A fire compartment is a well-defined enclosed room, not necessarily with fire barriers. Fire compartments generally fall within a fire area, and are bounded by non-combustible barriers where heat and products of combustion from a fire within the enclosure will be substantially confined. Boundaries of a fire compartment may have open equipment hatches, stairways, doorways or unsealed penetrations. The term fire compartment is defined specifically for fire risk analysis and maps plant fire areas and/or zones, defined by the plant and based on fire protection systems design and/or operations considerations, into compartments defined by fire damage potential [41]. For example, the control room complex or certain areas within the turbine building may be defined as a compartment.

2. FIRE PSA COMPONENT SELECTION (TASK 2).

The selection of components that are to be credited for plant shutdown following a fire is a critical step in any Fire PSA. Components selected would generally include any and all components credited in the 10 CFR 50 Appendix R post-fire SSD analysis. Additional components will likely be selected, potentially including any and all components credited in the plant's internal events PSA. Also, the proposed methodology would likely introduce components beyond either the 10CFR 50 Appendix R list or the internal events PSA model. Such components are often of interest due to considerations of combined spurious actuations that may threaten the credited functions and components.

This task provides the procedure for creating the Fire PSA Component List. This list serves as the basis for those components modeled in the Fire PSA, and it is the key source of information for which corresponding cables need to be identified and located for the Fire PSA. As such, the Fire PSA Component List, Fire PSA Model, and corresponding cable identification are iterated upon to ensure an appropriate correspondence among these three items. The product of this task is a list

[1] Probabilistic Safety Assessment (PSA) and Probabilistic Risk Assessment (PRA) are used interchangeably to means same in this work

of the equipment to be included in the Fire PSA and for which corresponding cables need to be identified and located for the nuclear power plant under analysis.

3. FIRE PSA CABLE SELECTION (TASK 3).

This task provides instructions and technical considerations associated with identifying cables supporting those components selected in Task 2. In previous Fire PSA methods (such as EPRI FIVE and Fire PSA Implementation Guide) this task was relegated to the Safe Shutdown (SSD) analysis and its associated databases. Conducting a Fire PSA in accordance with this procedure necessitates an analysis of fire induced circuit failures beyond that typically conducted during original Fire PSAs. The task provides methods and instructions for conducting the first phase of circuit analysis–selecting Fire PSA cables (Task 3). The purpose of Task 3 is to identify for all Fire PSA components the circuits/cables3 associated with the components and the routing[2]/plant location of the identified circuits/cables. These relationships can then be used to determine the Fire PSA components potentially affected by postulated fires at different plant locations.

The Fire PSA Cable List identifies the circuits/cables needed to support proper operation of equipment contained in the Fire PSA Equipment List. Essential electrical power supplies are also identified during this task. The Fire PSA Cable List might also include Associated Circuits. Associated Circuits are cables that are not necessarily directly linked to a component, but have the potential to cause improper operation of a component as a result of certain failure modes associated with fire-induced cable damage.

The Fire PSA Cable List is not simply a list of cables. It also establishes, for each cable, a link to the associated Fire PSA component and to the cable’s routing and location. These relationships provide the basis for identifying potential equipment functional failures at a fire area, fire compartment, or raceway level.

4. QUALITATIVE SCREENING (TASK 4)

This task according to the methodology identifies fire analysis compartments that can be shown to have little or no risk significance without quantitative analysis. Fire compartments may be screened out if they contain no components or cables identified in Tasks 2 and 3, and if they cannot lead to a plant trip due to either plant procedures, an automatic trip signal, or technical specification requirements. This procedure describes the criteria for qualitatively screening the fire compartments defined in Task 1

From Task 1, Plant Partitioning, a set of fire compartments is identified for the Fire PSA. These compartments are subjected to a series of screening analyses that will determine the relative fire risk associated to each. Qualitative screening is the first of such screening analyses. It is not intended to assign risk values to particular fire compartments. It is intended, however, to identify those fire compartments where, according to pre-determined criteria, the fire risk is expected to be

[2] The term “circuit” and “cable” are often used interchangeably for fire-related circuit analyses. A circuit is comprised of electrical components, subcomponents, and cables/connection wire. Within the context of fire induced equipment failures, it is understood that circuit selection or circuit identification refers to the identification of cables that connect all the related components and subcomponents of a complete circuit.

relatively low or nonexistent compared to others. This task assumes that the risk (i.e., CDF and/or LERF) associated with the fire scenarios where a controlled manual plant shutdown may be attempted as a precautionary measure and no other Fire PSA components are affected is low

5. FIRE-INDUCED RISK MODEL (TASK 5)

This task is a logic model that reflects plant response following a fire. Specific instructions have been provided for treatment of fire-specific procedures or preplans. These procedures may impact availability of functions and components, or include fire-specific operator actions (e.g., self-induced-station-blackout). The task describes the procedure for developing the Fire PSA Model to calculate CDF, CCDP, LERF, and CLERP for fire events. The procedure addresses the process of implementing temporary or permanent changes to the Internal Events PSA to quantify fire-induced CDF, CCDP, LERF, and CLERP, and for developing special models to address FEPs. The procedure also addresses the transition from temporary changes to permanent changes to the Internal Events PSA Model during the development of the Fire PSA Model.

The primary objective of this task is to provide an approach that allows the user to configure or modify the Internal Events PSA model to quantify fire-induced CDF, LERF, CCDP, and CLERP. There are at least two different PSA modeling approaches that have evolved in the PSA field. These two models, in the evolution of PSA methodology development efforts have come to be known as the "Fault Tree Linking Approach" and "Event Trees with Boundaries Approach". There is a number of different PSA software products available in the industry market designed around these two approaches. The approach described in this procedure is based on standard state-of-the-art PSA Practice, and is intended to be applicable for any PSA methodology or software product.

6. FIRE IGNITION FREQUENCIES (TASK 6)

This task describes the approach to develop frequency estimates for fire compartments and scenarios. Significant changes from the EPRI FIVE method have been made in this task. The changes generally relate to use of challenging events, considerations associated with data quality, and increased use of a fully component based ignition frequency model (as opposed to the location/component-based model used, for example, in FIVE[3]). The purpose of the fire frequencies task is to describe the procedure for estimating the fire-ignition frequencies associated with fire ignition sources. Generic ignition frequencies that can be specialized to plant conditions in terms of plant characteristics and plant fire event experience are provided. Uncertainties in the generic frequencies are also provided in terms of 5th, 50th, and 95th percentiles.

This task estimates fire-ignition frequencies and their respective uncertainties for different compartments (e.g., main control room and RHR pump room) and ignition sources (e.g., CCW Pump A and three vertical segments of a motor control center (MCC)). A generic set of fire ignition frequencies for various generic equipment types (ignition sources) typically found in certain plant locations was developed as a starting point. It should be noted that when analyzing historical event data it could not be determined whether or not electrical equipment (e.g., cables and electrical

[3] Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, NUREG-1150, U.S. NRC, Washington, DC, 1990.

cabinets) employ thermoset or thermoplastic insulation and/or jackets. Therefore, all the events for any given ignition source type were combined and the resulting frequencies should be used for both types of cable insulation and jacket material.

7. QUANTITATIVE SCREENING (TASK 7)

A Fire PSA allows the screening of fire compartments and scenarios based on their contribution to fire risk. This approach considers the cumulative risk associated with the screened compartments (i.e., the ones not retained for detailed analysis) to ensure that a true estimate of fire risk profile (as opposed to vulnerability) is obtained.

The purpose of procedure is to provide the user an approach to quantify the Fire PSA Model using the procedure provided in Task 5, and to screen out fire compartments based on quantitative criteria. This procedure develops the bases for the quantitative screening criteria and provides specific methods for implementing the screening process. The primary objective of this task is to provide the user an approach to quantify the Fire PSA Model developed in Task 5, and to screen out fire compartments based on quantitative screening criteria. It is emphasized that the screening criteria are meant to be applied as part of the Fire PSA Model building and quantifying process. The screening criteria are not the same, nor should they be confused with, the acceptance criteria for applications of the Fire PSA Model. For example, the screening criteria herein are not directly correlated to the delta-CDF and delta-LERF criteria used in Regulatory Guide 1.174 [86] for the acceptability of making permanent changes to the plant. The screening criteria are intended to complement the RG 1.174 criteria and to allow for the use of fire PSA results in a RG 1.174 application, but they are also intended to serve the broader objectives of a typical fire PSA.

8. SCOPING FIRE MODELING (TASK 8)

This step provides simple rules to define and screen fire ignition sources and fire scenarios in an unscreened fire compartment. Scoping fire modeling is the first task in the Fire PSA framework where fire modeling tools are used to identify ignition sources that may impact the fire risk of the plant. Screening some of the ignition sources in the room, along with the application of severity factors to the unscreened ones, may reduce the compartment fire frequency previously calculated in Task 6.

The purpose of this task is to screen out those fixed ignition sources that do not pose a threat to the targets within a specific fire compartment, and to assign severity factors to unscreened fixed ignition sources. It must be noted that only those ignition sources should be considered in this task that were included in establishing the fire ignition frequency in Task 6. All other potential ignition sources that were screened out in Task 6 should neither be addressed in this task. With this task, the level of effort for detailed fire propagation analysis may be reduced. Furthermore, applying severity factors may reduce the compartment frequency calculated in Task 6, resulting in some compartments being screened before detail fire modeling studies are conducted.

9. DETAILED CIRCUIT FAILURE ANALYSIS (TASK 9)

This task provides an approach and technical considerations for identifying how the failure of specific cables will impact the components included in the Fire PSA SSD plant response model.

Fire PSA methodology necessitates an analysis of fire induced circuit failures beyond that typically conducted during original Fire PSAs

The cable failure modes of particular interest here include shorts-to-ground and hot shorts. Open circuit failures[4], [4]as the initial cable failure mode, will typically not be considered in this procedure. However, an open circuit condition resulting from the predicable operation of a circuit protection device (e.g., circuit breaker and fuse) in response to fire-induced short circuits will be considered with regard to its impact on the operation of the component(s) affected by the cable under consideration.

An Equipment Failure Response Report[5] is a consolidated list of possible component responses resulting from fire damage to the cable. This aspect of the circuit analysis is fundamentally a deterministic study and does not include failure mode probabilities. However, the results of this task will serve as the basis for estimating the likelihood of specific equipment functional failures at a compartment or scenario level.

10. CIRCUIT FAILURE MODE LIKELIHOOD ANALYSIS (TASK 10).

This task considers the relative likelihood of various circuit failure modes. This added level of resolution may be a desired option for those fire scenarios that are significant contributors to the risk. The methodology is as a result of benefits from the knowledge gained from the tests performed in response to the circuit failure issue.

This task provides methods and instructions for conducting the third phase of circuit analysis – circuit failure mode likelihood analysis for Fire PSA cables. Task 10 estimates the probability of hot short cable failure modes of interest, which in turn can be correlated to specific component failure modes. The methods and techniques for deriving circuit failure mode probability estimates are based on limited data and experience. Consequently, this area of analysis is not yet a mature technology, and undoubtedly further advances and refinements will come with time. Nonetheless, the methods and techniques presented represent the current state of knowledge and provide a reasonable approach for establishing first-order circuit failure mode probability estimates, albeit with relatively high uncertainty tolerances.

Task 10 is intended to provide a probabilistic assessment of the likelihood that a cable will experience one or more specific failure modes (e.g., short-to-ground, intra-cable conductor-to conductor short, inter-cable conductor-to-conductor short, etc.). The results of this assessment are entered into the Fire PSA Database, allowing generation of equipment failure reports, including the estimated likelihood of the failure modes of concern

11. DETAILED FIRE MODELING (TASK 11).

This task describes the method to examine the consequences of a fire. This includes consideration of scenarios involving single compartments, multiple fire compartments, and the main control room. Factors considered include initial fire characteristics, fire growth in a fire compartment or

[4] Within the context of this procedure, "open circuit failure" refers to the loss of continuity due to direct physical damage to the conductor (e.g., melted wire).

across fire compartments, detection and suppression, electrical raceway fire barrier systems, and damage from heat and smoke. Special consideration is given to turbine generator (T/G) fires, hydrogen fires, high-energy arcing faults, cable fires, and main control board (MCB) fires.

There are considerable improvements in the method for this task over the EPRI FIVE and Fire PSA Implementation Guide in nearly all technical areas.

In the preceding tasks, the analyses were organized around compartments, assuming that a fire would have widespread impact within the compartment. In Task 11, for those compartments found to be potentially risk-significant (i.e., unscreened compartments), a detailed analysis approach is provided. As part of the detailed analysis, fire growth and propagation is modeled and possibility of fire suppression before damage to a specific target set is analyzed.

The detailed fire modeling process generally follows a common step structure, but the details of the analyses often vary depending on the specifics of the postulated fire scenario. This task provides separate procedures for three general categories of fire scenarios: fires affecting target sets located inside one compartment; fires affecting the main control room (MCR); and fires affecting target sets located in more than one fire compartment (multi compartment fire analysis).

Task 11 provides final estimates for the frequency of occurrence of fire scenarios involving a specific fire ignition source failing a predefined target set before fire protection succeeds in protecting the target set. This result is combined in the final quantification steps that follow this task, with the CCDP/CLERP given failure of the target set to estimate the CDF/LERF contribution for each fire scenario. The CCDP/CLERP may include modified human error probabilities based on fire scenario specifics.

Task 11 encompasses the final stages of analysis of the physical fire behaviors associated with fire scenarios in unscreened compartments. A fire scenario in the Fire PSA context begins with initiation of a fire and ends with either safe shutdown of the reactor or a core-damage event. Task 11 is concerned only with the analysis of the physical fire scenario; that is, those aspects of the analysis related to the fire ignition, fire growth, propagation, target set damage, and fire detection and suppression.

12. POST-FIRE HUMAN RELIABILITY ANALYSIS (TASK 12)

This task considers operator actions for manipulation of plant components. The analysis task procedure provides structured instructions for identification and inclusion of these actions in the Fire PSA. The procedure also provides instructions for estimating screening human error probabilities (HEPs) before detailed fire modeling results (e.g., fire growth and damage behaviors) have been developed. Estimating HEP values with high confidence is critical to the effectiveness of screening in a Fire PSA. This report does not develop a detailed fire HRA methodology. There are a number of HRA methods that can be adopted for fire with appropriate additional instructions that superimpose fire effects on any of the existing HRA methods, such as SHARP, ATHEANA, etc. This would improve consistency across analyses i.e., fire and internal events PSA.

This Task evaluate the impact of fire scenarios on the human actions addressed in the base PSA study (i.e., the Internal Events PSA[6] or original Fire IPEEE analysis) used to create the Fire PSA

Model, as well as how to identify and quantify new actions to be performed as part of the plant fire mitigation plans and procedures. Evaluating the reliability for these human actions supports the Fire PSA Model for calculating such metrics as CDF, CCDP, LERF, and CLERP for fire-induced initiating events. The initial quantification of these metrics makes use of screening probabilities for human failure events (HFEs) where appropriate. As necessary, more detailed best estimate analyses of some human actions will be [5]needed to obtain more realistic assessments of fire risk.

Task 12 addresses a process for performing both screening and detailed analysis of post-fire human actions identified in accident sequences initiated by a fire. The main focus is to foster the process for assessing the impact of location-specific fires on the human actions taken in response to a fire-induced initiating event, thus preventing core damage and mitigating releases. This task procedure covers three essential elements of most human reliability analysis (HRA) studies.

• Identification of the HFEs to be included in the Fire PSA.

• The assignment of screening human error probabilities for the identified HFEs to assist in focusing the modeling and fire risk analysis to those scenarios and human actions most important to the overall risk results.

• Considerations for the detailed best-estimate quantification of the more important HFEs to properly consider the fire effects on human performance.

13. SEISMIC-FIRE INTERACTIONS ASSESSMENT (TASK 13)

This task is a qualitative approach to help identify the risk from any potential interactions between an earthquake and fire. This Task does not provide a methodology for developing models and quantifying risk associated with fires caused by a severe seismic event. This is, due to a combination of limitations in the state of the art, and the perceived low level of risk from these fires. The low risk is based on the low frequency of an earthquake that can initiate a challenging fire and degrade various plant fire protection defense-in-depth elements, and the general seismic ruggedness of the NPPs as part of their design basis. This task is gaining prominence after Fukushima accident in Japan and a lot of work are being done to provide a methodology for developing models and quantifying risk associated with fire caused by a severe seismic event.

14. FIRE RISK QUANTIFICATION (TASK 14).

This section describes the procedure for performing fire risk quantification. This procedure provides the user a general method for quantifying the final Fire PSA Model to generate the final fire risk results.

Task 7, Quantitative Screening, it is expected that a number of fire compartments or fire scenarios will be screened out from the formal fire quantification results (i.e., not added into the calculated total plant fire-related CDF and LERF). It is expected that as a minimum, total plant CDF and LERF estimates will be provided by summing all the CDFs and LERFs for the unscreened fire

[5] Internal Event PSA is the probabilistic Safety Analysis of internal event that can cause Core Damage.

compartments/scenarios. The significant contributors to the plant CDF and LERF should also be provided. In addition, it is also expected that the nature (e.g., type of sequences) of the screened out compartments/scenarios are at least identified and as a check of the cumulative screening criteria discussed in Task 7, it is recommended that the screened CDFs and LERFs also be summed separately to provide a perspective on the total residual risk from the screened compartments/scenarios. It should be emphasized that these screened portions of the results represent various levels of analysis (for instance, some may only involve fire scoping modeling; others may involve both detailed fire modeling and some detailed circuit analysis

15. UNCERTAINTY AND SENSITIVITY ANALYSES (TASK 15)

This task describes the approach to follow for identifying and treating uncertainties throughout the Fire PSA process. The treatment may vary from quantitative estimation and propagation of uncertainties where possible (e.g., in fire frequency and non-suppression probability) to identification of sources without quantitative estimation, where knowledge of a quantitative treatment of uncertainties is beyond the state-of-the-art. The treatment may also include one-at-a-time variation of individual parameter values to determine the effect on the overall fire risk (sensitivity analysis).

The purpose is to describe an approach for identifying and treating uncertainties throughout the Fire PSA process and identifying sensitivity analysis cases. It also prescribes a review for the identified uncertainties among the Fire PSA analysts to establish an integrated approach of addressing the effects of these uncertainties on the results of the analysis.

Many of the inputs that make up CDF and LERF estimates are uncertain (e.g., fire frequencies, extent of fire growth, equipment failure probabilities, operator action probabilities, etc.). Since many of these inputs are commonly treated as the result of random processes in the PSA, the core damage events and large early release events are modeled as possible results of a set of interacting random processes, specifically, those involving a fire that causes a plant transient, the response of mitigating systems to the transient including fire effects, and the associated actions of human operators. Hence, the occurrences of core damage and large early release events are also, therefore, treated as random events.

16. FIRE PSA DOCUMENTATION (TASK 16)

This procedure provides the general Practice considered necessary for documenting the Fire PSA and its results. The objective of this task is to ensure there is adequate documentation of the Fire PSA to allow review of the Fire PSA development and its results, as well as to provide a written basis for any future uses of the Fire PSA.

6.1.3 INSIGHTS AND OBSERVATION

There has been significant improvement over the previous methods and the following insights and observation are recognized [41]:

- The addition of spurious operation faults to the post-fire Safe Shutdown (SSD) response model holds the potential to substantially alter the existing perspectives on fire risk. The limited depth and completeness of the demonstration studies completed to date means that quantitative insights into the general magnitude of fire risk, and the impact of such fault modes on fire risk, have not yet been developed. However, the demonstration studies did involve fire risk scenarios where the dominant cutsets involved two or more spurious operations. These scenarios would likely not have been captured in risk studies conducted using earlier analysis procedures. The ultimate risk significance of these effects remains to be seen.

- The incorporation of high-energy arcing faults as a failure mode for high-energy electrical switching equipment (e.g., switchgears) could lead to some shifts in the perception of the relative risk importance of these fire ignition sources. Based on the best evidence to date, arcing faults in such equipment, while relatively rare occurrences, hold the potential for significant fire-induced damage in very little time. Hence, fire suppression features (either fixed or involving the fire brigade) may not be effective at preventing the initial damage. Depending on the plant-specific configuration and proximity of the critical damage targets to the faulting component, this could imply the existence of risk-important fire scenarios that would not have been identified in fire risk analyses based on earlier analysis methods and assumptions.
- The Fire PSA method documented here includes substantial changes compared to previous Fire PSA methods (e.g., NUREG-1150, FIVE, and the EPRI Fire PSA Implementation Guide). Fire risk analyses based on a direct application of these earlier methods may be of limited usefulness, even as a starting point for an updated analysis. Fire vulnerability assessments conducted under the Individual Plant Examination of External Events (IPEEE) program have not adequately addressed many of the factors now considered important (e.g., spurious actuations and proper treatment of fire severity). Note that plant-specific data collected under the earlier methods should be applicable to this methodology.
- It has generally been presumed that use of a post-fire SSD response model that credits (and therefore includes) only those components, systems, and functions credited in the deterministic 10 CFR 50 Appendix R safe shutdown analysis will lead to conservative risk estimates. The experience gained through the study shows that this presumption may not necessarily be true. Consideration of multiple concurrent spurious actuations is beyond the current design basis for most plants. The 10 CFR 50 Appendix R post-fire SSD component list was developed accordingly. Multiple spurious actuations involving non-Appendix R components may hold the potential to compromise 10 CFR 50 Appendix R SSD functions. The failure to include these functional dependencies could result in optimism in the Fire PSA SSD model. Crediting systems and components beyond the plant’s existing safe shutdown strategy could offset the impact of these failure modes.
- Selection and tracing of the components and cables, and to a lesser extent the analysis of their fire-induced failure modes, continues to present the biggest challenge in terms of estimating the resources needed to conduct the Fire PSA. In some cases, more than half of the resources needed for implementing the methodology documented in the report was directed to cable and component selection, analysis of the credited systems and function, and routing of the credited cables and components. Note that introducing spurious operation fault modes into the post-fire plant SSD response model involves substantial use of resources, but is not the driving factor. Rather, increasing the depth and rigor pursued in

the component and cable selection task leads to additional burden in component and cable tracing, and supporting circuit analyses. The 10 CFR 50 Appendix R SSD components carry some level of analysis pedigree that carries over to the Fire PSA. However, consideration of multiple concurrent spurious actuations may need additional analysis of even the Appendix R components. When crediting components beyond the Appendix R SSD list, the supporting cable failure mode and effects analyses should be performed at the same order of rigor and depth as those performed for the 10 CFR 50 Appendix R systems and components.

- A Fire PSA is a multidisciplinary project that needs expertise and knowledge that rarely reside in one person. A team of people who collectively provide all of the necessary expertise is needed to ensure quality and control cost.

6.2 A PROCESS FOR RISK-INFORMED DECISION-MAKING

The use of PSA results in decision-making has been addressed in Regulatory Guide 1.174, which describes an integrated risk-informed decision-making process that was specifically developed to provide guidance to licensees on how to use risk information in a licensing submittal to change the licensing basis of a plant

Final Policy Statement on the Use of Probabilistic Risk Assessment (PRA) Methods in Nuclear Regulatory Activities [1], the U.S. Nuclear Regulatory Commission increasingly made use of risk information in a number of its activities, including licensing actions and oversight activities. Regulatory Guide 1.174, for example, provides guidance to a licensee on the use of PRA in license amendment requests [86]. The philosophy expressed in that document had been adapted for use in other regulatory applications

In GAO-04-415, "Nuclear Regulation—NRC Needs to More Aggressively and Comprehensively Resolve Issues Related to the Davis-Besse Nuclear Power Plant's Shutdown," issued May 2004 [87], the U.S.

Government Accountability Office (GAO) made the following recommendation with respect to the areas of risk evaluation, communication, and their use in the decision-making:

- Improve the U.S. Nuclear Regulatory Commission's (NRC's) use of probabilistic risk assessment (PRA) estimates in decision making by (1) ensuring that the risk estimates, uncertainties, and assumptions made in developing the estimates are fully defined, documented, and communicated to NRC decision makers; and (2) providing guidance to decision makers on how to consider the relative importance, validity, and reliability of quantitative risk estimates in conjunction with other qualitative safety-related factors

Following this a process has been created for reactor-based risk-informed decision making, although it is considered that the basic steps can be followed for other risk-informed applications.

The process supplements the existing risk-informed decision-making processes (e.g., that given in Regulatory Guide (RG) 1.174 [86]; MD 8.3, "NRC Incident Investigation Program," issued March 27, 2001 [88]; and LIC-401, "NRR Reactor Operating Experience Program," issued May 17, 2005 [89]

To be effective in communicating risk-informed decisions, it is important to consider early in the process the stakeholders who need to be informed and involved, as well as who will be impacted, and to build in communication steps that encourage discussion and clarification throughout the process. This enables analysts and decision makers to be more effective in communicating the results during and at the end of this risk-informed process. Placing emphasis on communication during the process helps identify topics that require clarification and focuses attention on ensuring that all participants share an understanding of the subject, objective, terms, and assumptions at hand; this encourages discussion and prevents misunderstandings among team members and therefore enables everyone to stay on track. This is especially important when working with multidisciplinary teams that include both risk analysts and analysts from other (e.g., engineering and licensing) disciplines.

6.2.1 OVERVIEW OF THE DECISION MAKING PROCESS

Figure 6.2 outlines the new process to be followed for risk-informed decision-making. The figure depicts three different areas— a) technical activities (information gathering and analysis), b) the risk-informed decision-making process itself (Steps 1 - 4), and c) communication of the decision (Steps 5 - 7).

The first three steps in this process are common to other risk-informed decision-making processes. To support these steps, information gathering and technical analyses are performed. Step 4 (i.e., integrate assessment results) is also part of the risk-informed decision-making process in RG 1.174 [83]. However, RG 1.174 only briefly discusses this important step. Therefore, additional guidance for documenting assessment results is provided[6]. Steps 5 - 7 have been separated to highlight the importance of communicating the decision and to emphasize the need to use recently developed guidance for risk communication [90, 91]. Feedback loops (e.g., Step 6 to Step 3) reflect the potential need for additional analyses to clarify initial results or answer questions that were not previously considered.

Underlying all steps in the process is the need for documentation. In order to make the results of this risk informed decision-making process traceable and comprehensible, and to assist in its consistency, a series of templates has been developed to formalize the form and format of such documentation.

[6] U.S. Nuclear Regulatory Commission, "Integrated Risk-Informed Decision-Making Process for Emergent Issues", LIC-504, December 2005, ADAMS accession number ML052060376.

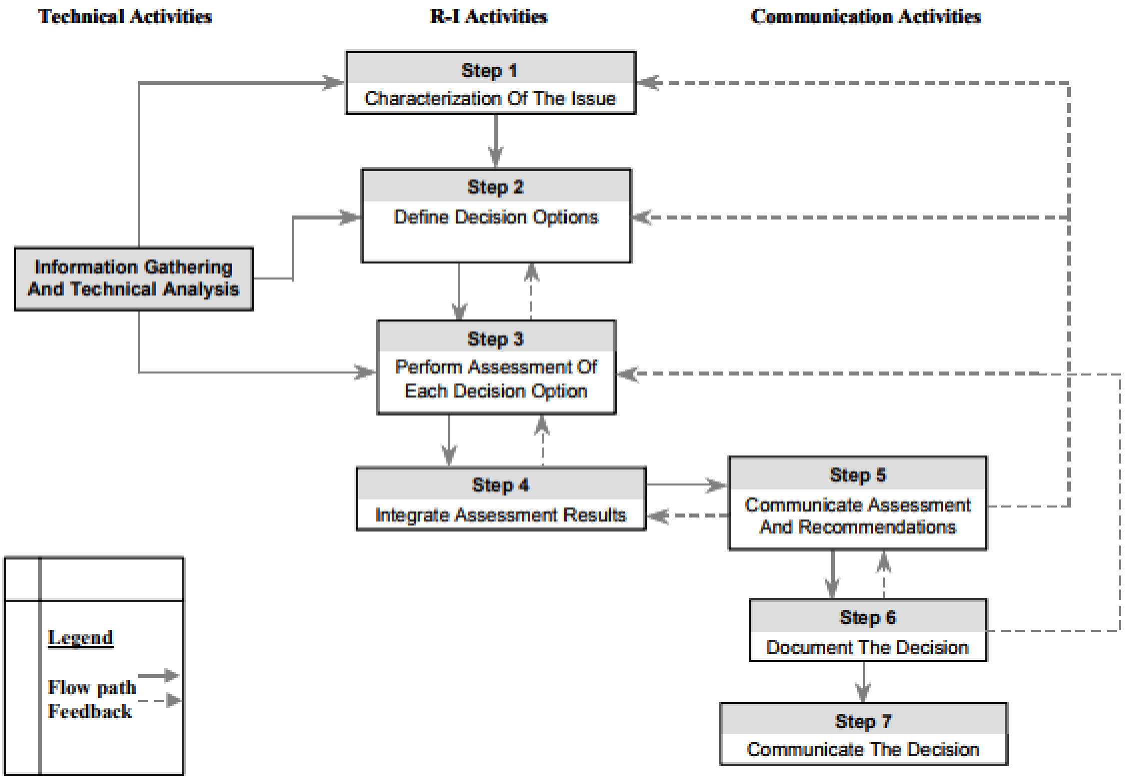


Figure 6.2 RISK-INFORMED (R-I) DECISION MAKING PROCESS [92]

A framework to provide for communicating the preferred decision option selected by the integration team to decision makers. Decision makers typically need information presented in summary format for rapid assessment and ease of understanding the impacts and complexity of an issue. Decision makers need narrative descriptions that provide qualitative insight into causes, uncertainties, assumptions, and affected outcomes for a given situation. Less information is needed regarding the details of numerical results, statistical methods, and analyses. This background information must be available, but it should be presented after the recommendations in step 5.

In view of the need of providing a summary format and a narrative descriptions that provide qualitative insight for risk-informed decision making, Fire-Related Systems and Key Safety Functions Unavailability Matrix has been developed. This was as a result of the Development and assessment of fire-related risk unavailability matrices to support the application of the maintenance rule in a PWR nuclear power plant

6.3 FIRE-RELATED SYSTEMS AND KEY SAFETY FUNCTIONS UNAVAILABILITY MATRIX

The Nuclear Engineering Research Group (NERG) in collaboration with a Spanish Pressurized Water Reactor (PWR) Nuclear Power Plant (NPP) applied the Probabilistic Safety Assessment (PSA) methodology to risk-informed decision making. The purpose of this Fire PSA related research activity is to develop tools for risk-informed decision making. The objective of the project was to develop an Unavailability Matrix (UM) for Fire Protection Systems (FPSs) and Key Safety functions (KSFs). It also presents innovative methods to incorporate fire-related risk into the current assessment of plant configurations. The method identify structures, systems and components significant for Fire- related risk. The method also identify Fire Zones (FZs) which are potential candidates for risk management actions. The methods are restricted to the use of the Fire PSA of the NPP. The NPP PSA team provided technical guidance throughout the development of the methods. The outcome of the methods are matrix structures assessed by means of risk criteria. This work has been published in a peer review journal by the NERG [93] and methodology describe in the next sections.

6.3.1 MATRICES DELINEATION. SELECTION OF REPRESENTATIVE BASIC EVENTS

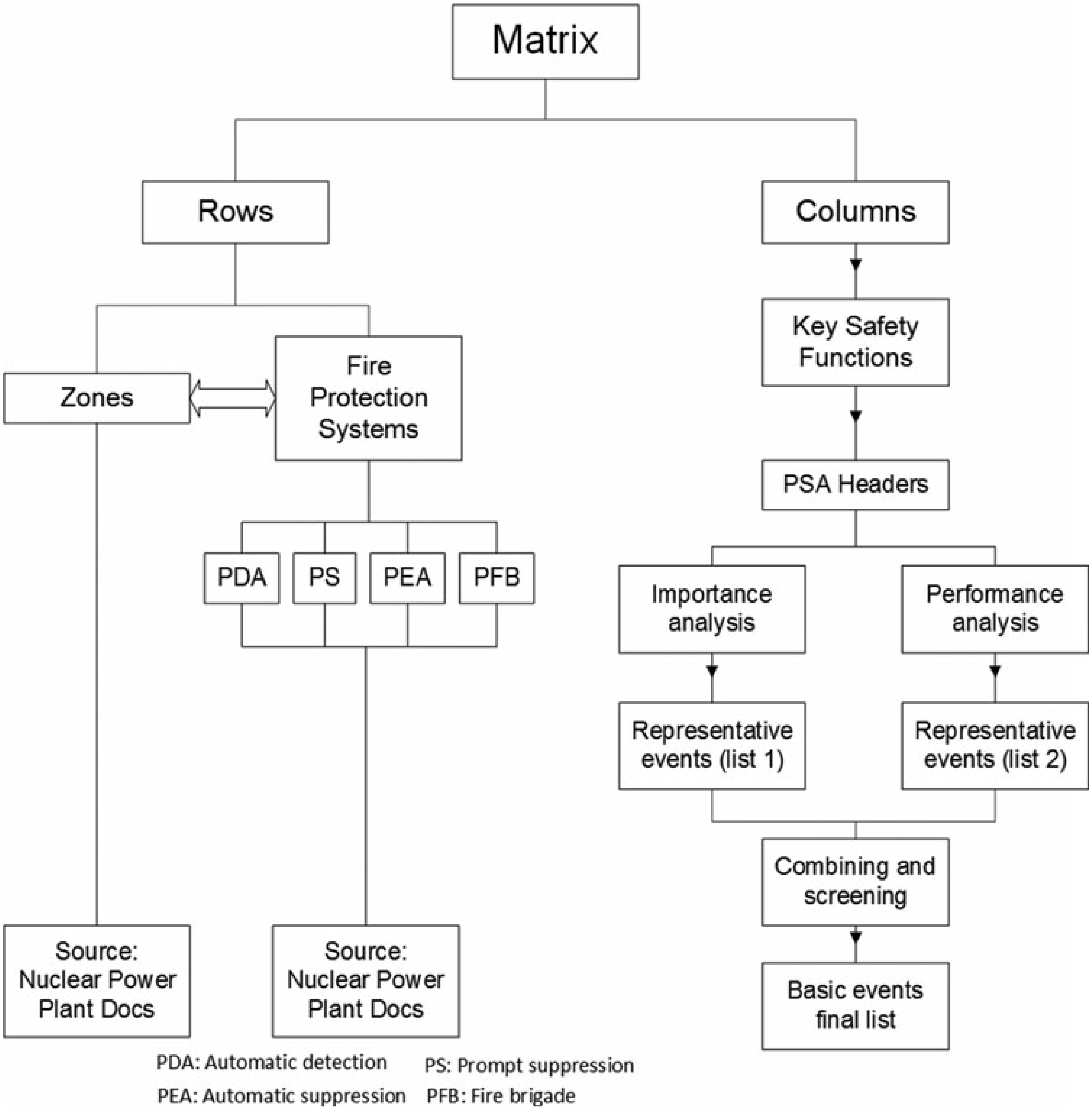
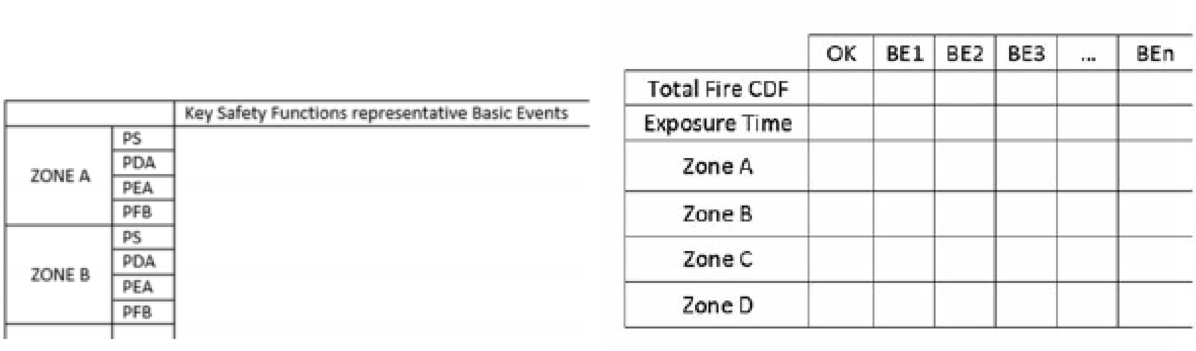


Figure 6.3 Methodology followed to delineate the unavailability matrix [93]

The rows of the UM matrix host all the FPSs within the scope of the fire PSA. Likewise, the rows of the Fire Risk Matrix (FRM) contain all the Fire Zones (FZs) analyzed in the fire PSA detailed analysis. Columns host KSFs' representative basic events for both UM and FRM. A screening analysis was carried out for the purpose of selecting basic events which are significant to and exclusively represent one of the KSFs. Figure 6.3 shows the methodology followed to select the elements to be introduced in the UM.

The fire PSA detailed analysis includes four generic types of Fire Protection Systems (FPSs): prompt suppression (PS), automatic detection (PDA), automatic suppression (PEA), and fire brigade (PFB) [3]. Each generic type of FPS is linked to several specific FPSs of the plant [41, 94]. The Fire Zones are introduced into the UM for simplicity and traceability purposes. In the matrix, each zone contains the fire protection systems which makes it easy to know which function (detection or suppression) is unavailable. The UM contains 167 FPSs [93].



		Key Safety Functions representative Basic Events
ZONE A	PS	
	PDA	
	PEA	
	PFB	
ZONE B	PS	
	PDA	
	PEA	
	PFB	

	OK	BE1	BE2	BE3	...	BEn
Total Fire CDF						
Exposure Time						
Zone A						
Zone B						
Zone C						
Zone D						

Figure 6.4. Unavailability Matrix layout with FPSs [93]

6.3.2 SCREENING OF KEY SAFETY FUNCTIONS (KSFS') REPRESENTATIVE EVENTS

Key Safety Functions (KSFs'): Subcriticallity (S), Core Cooling (C), Heat Sink (H), and RCS Inventory (I) related to Fuel Matrix and Fuel Clad were assessed. Similarly, Reactor Coolant Systems (RCS) Integrity (P), Heat Sink (H), and RCS Inventory (I) that are related to Reactor Coolant Systems (RCS) were also selected as well as pressure boundary and Containment Building Integrity (Z) related to containment vessel.

The KSFs analyzed in both matrices are: subcriticality (S), core cooling (C), heat sink availability (H), reactor coolant system (RCS) integrity (P), RCS inventory (I), electricity supply (E). The subcriticality KSF is equal to the reactivity control fundamental safety function. The core cooling, heat sink availability, and RCS inventory KSFs have to be maintained in order to ensure the removal of heat from the core fundamental safety function. The RCS integrity KSF is associated with the confinement of radioactive materials fundamental function. Containment integrity is not included as a key safety function because the fire PSA used in the analysis is level 1. Electricity supply has been included in the KSFs list because the failure to accomplish this function could jeopardize all the three fundamental safety functions, either together or separately

The performance of safety systems and safeguards ensures the accomplishment of the KSFs' acceptance criteria. Systems and safeguards are modelled in the PSA by virtue of Fault Trees. The accomplishment of KSFs during an accident sequence ensures the Plant does not suffer any negative consequence. Safety systems and safeguards' Fault Trees consequently are the headers of the PSA model. The headers represent the state of KSFs in the scope of PSA.

The screening analysis for selecting KSFs' representative basic events is based on a risk importance analysis. The importance analysis has been applied to the Boolean equations of unavailability of the internal events' mitigation headers. All those basic events whose risk achievement worth (RAW) [91] importance measure is greater than a specific value are selected for further analysis. The screening RAW value is set to10. The screening value is more restrictive than that for other applications where the plant's CDF is evaluated because the quantity of basic events evaluated in a header is much smaller than the quantity of basic events evaluated in the Boolean equation for the plant's CDF. The NPP support team agreed with the screening value. The basic events selected from all the headers analysis are merged in a new list which includes all the basic events selected by means of the importance analysis. This is referred to as representative events (list 1) in Figure 6.3

A list of qualitatively chosen basic events is added to the importance analysis list. This is referred to as representative events (list 2) in Figure 6.3. The SSCs represented by these qualitatively chosen basic events are considered to be important regarding the accomplishment of a KSF. The procedure used to choose those basic events in list 2 is the so-called performance analysis in Figure 6.3. The performance was carried out by the NPP support team.

An exclusivity analysis is applied to the final list of basic events in order to screen out: all the repeated basic events (leaving one representative in the list); basic events representing more than one KSF. Besides, a single representative basic event is chosen from all those basic events related to components whose unavailability has exactly the same risk impact on the performance of an SSC (for instance, components in series in the same train or symmetric components).

The final matrices include 29 KSF representative basic events. Both matrices have a column to represent the scenario in which all the KSF representatives are in normal state. The dimension of the UM is 168 × 30, whereas the dimension of the FRM is 43 × 30 (i.e. the fire PSA assesses 41 zones [93]).The FRM includes a row to present the exposure time to reach an accumulated increment of Core Damage Probability (CDP) of 1.0E-06. Figure 6.3 shows the definitive layout of both matrices.

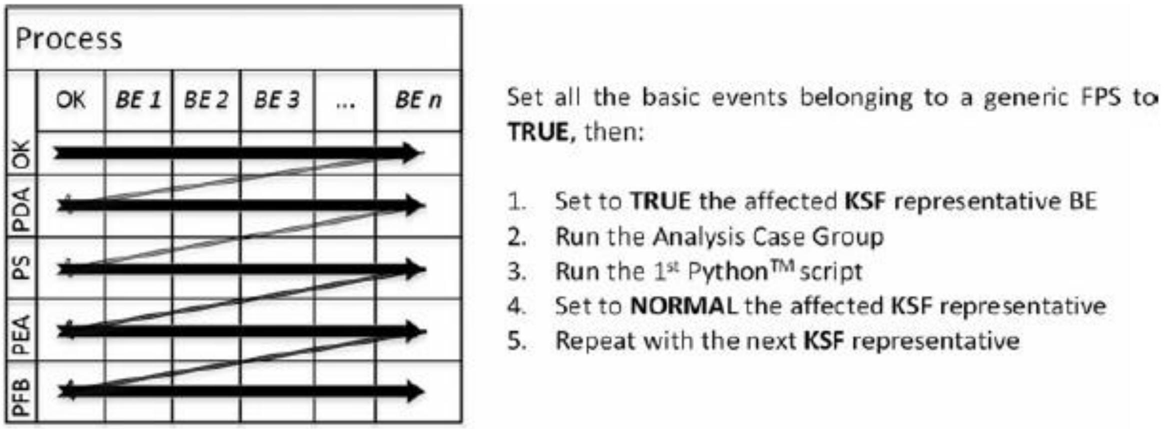
6.3.3 MATRICES QUANTIFICATION IN RISKSPECTRUM

The fire PSA RiskSpectrum ® model of the Spanish NPP provides the Core Damage Boolean equation for each fire analysis case, and each FZ included in the analysis. However, it does not evaluate Boolean equation for the Core damage frequency (CDF) of the whole plant. The CDF of the whole plant is the risk measure used in the UM. Therefore, the CDF of the plant is quantified by means different to RiskSpectrum ® Equation (5.1) is used to calculate the plant's CDF associated with each element of the UM.

$$CDF_{Zi,s,k} = \sum_{z}(dCDF_{z,OK,k}) - dCDF_{zi,OK,k} + dCDF_{zi,s,k} \qquad 6.1$$

Equation (5.1) has three degrees of freedom: the zone (z), the FPS (s), and the KSF (k). The acronym dCDF refers to the CDF related to a FZ. So to say, a dCDF is a single and specific value of CDF, independent from other dCDFs, which is solely associated with fires postulated in a specific FZ. Each dCDF is considered as the contribution of a FZ to the CDF of the plant. In average conditions 2, the overall CDF of the plant is in fact the result of the summation of all the dCDFs. In consequence, the first term of Equation (5.1), which is the summation of the dCDFs of all the FZs in the PSA, is equal to the CDF of the plant as long as no FPS is set unavailable. In a case where one FPS is unavailable, the contribution of the FZ affected by the unavailability of the FPS has to be subtracted from the first term. The dCDF of the affected FZ, computed with the unavailable FPS set to TRUE, is added as the third term of the Equation (1). All the Equation (5.1) terms have to be assessed with the specific KSF representative basic event in TRUE state when assessing the unavailability of a KSF. The outcome of Equation (6.1) is the CDF of the plant restricted to the unavailability of an FPS and/or the unavailability of a KSF representative basic event.

The risk measure assessed in the FRM is the contribution of each FZ (i.e. dCDF) to the NPP's fire CDF when SSCs representative of KSFs are unavailable. These dCDFs are used in the terms of Equation (6.1) (i.e. dCDFz, OK, k). Both matrices are then calculated using the same methodology.



Set all the basic events belonging to a generic FPS to **TRUE**, then:

1. Set to **TRUE** the affected **KSF** representative BE
2. Run the Analysis Case Group
3. Run the 1st Python™ script
4. Set to **NORMAL** the affected **KSF** representative
5. Repeat with the next **KSF** representative

Figure 6.5 Quantification procedure in RiskSpectrum [93]

The objective of the quantification in RiskSpectrum ® is to obtain all the FZs' contributions to plant's fire CDF (dCDFs in Equation (6.1)). The procedure shown in Figure 6.5 is followed. It is a pivoting quantification process whose pivots are the four generic types of FPSs. Two hundred and sixty RiskSpectrum runs have been carried out to obtain all those dCDFs.

6.3.5 FINAL MATRICES CALCULATION AND COMPLETION

The calculation of the UM elements is completed using two Python^{TM} scripts. The first script translates RiskSpectrum ® results' files into proper text files adapted for the second script. The second script performs two tasks. The first task is to generate an ancillary matrix called dCDF matrix which contains all the dCDFs computed with RiskSpectrum ®. The layout of the dCDF matrix is similar to that of the UM. The second task is to calculate the UM elements by means of Equation (5.1) and the data stored in the dCDF matrix. Both are provided in text files and are translated to an Excel ® worksheet to facilitate the treatment of data.

The risk assessment criteria similar to what is proposed by the Spanish regulatory body for the assessment of findings [9] is applied to evaluate the matrix. These criteria are based on the concepts of exposure time (TE) and ΔCDP of the situation assessed (see Equation (6.2))

$$\Delta CDF \bullet \left(\frac{T_E}{365}\right) = \Delta CDP \qquad 6.2$$

ΔCDF is the difference between the CDF of each matrix element (CDF$_a$ i.e. the CDF of the plant restricted to the unavailability of an FPS and /or the unavailability of a KSF representative basic event) and the plant's reference fire CDF. The ΔCDP threshold to differentiate between insignificant and significant risk is set to 1.0E-06, in compliance with other criteria that utilized this figure 6.9. The metric used to evaluate the risk is the TE needed to reach the ΔCDP threshold. Table 6.1 shows both the qualitative levels of risk criteria and the risk assessment quantitative criteria. The quantitative risk criteria presented in column 3 of Table 6.1 are the result of isolating CDF$_a$ from the criteria in column 2. The plant's reference fire CDF is used for that purpose. The value of the plant's reference fire CDF is roughly 9.83E-06 (1/r × y)

Table 6.1 Risk assessment qualitative and quantitative criteria and color code.

Color	Qualitative criteria	Quantitative criteria	CDFa (1/rxy) criteria
Green	Very low	ΔCDF*(7/365)<1.0E-06	CDF$_a$<6.20E-05
Yellow	Low/moderate	ΔCDF*(7/365)>1.0E-06	6.20E-05<CDF$_a$<1.31E-04
Orange	High	ΔCDF*(3/365)>1.0E-06	1.31E-04<CDF$_a$<1.0E-03
Red	Very high	ΔCDF$_a$>1.0E-03	CDF$_a$>1.0E-03

Table 6.2 Risk significant fire protection systems and key safety functions representatives.

Description	Risk	System	KSF
Motor pump	Yellow	AFW	Heat sink
Vital electric bar A	Yellow	Electric supply	Electricity supply
Pneumatic valve	Yellow	SSWS	Heat sink
Control room suppression	Yellow	FPS	
Retention valve	Orange	HPSI	RCS inventory
Vital electric bar B	Orange	Electricity supply	Electricity supply
DC bar	Red	Electricity supply	Electricity supply

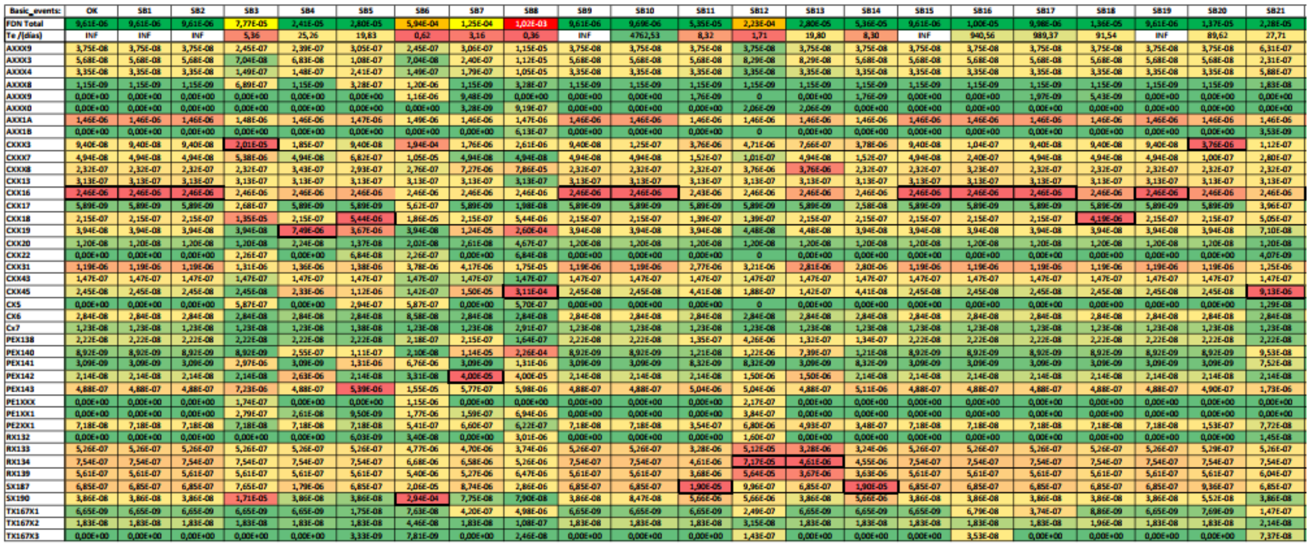
The risk criteria are divided into four qualitative levels: very low (green), low or moderate (yellow), high (orange), and very high risk (red) as shown in Figure 6.7. The fire-related risk is significant for the yellow level and above. For the very low region of risk, the ΔCDP threshold of 1.0E-06 is not reached after seven days of operation under the situation assessed (see column 2 of Table 6.1). No corrective actions are needed to fix the situation assessed. If the situation is the consequence of maintenance, the maintenance can last as much time as needed. For the low or moderate region of risk, the ΔCDP threshold of 1.0E-06 is reached after three days, and before seven days, of operation under the situation assessed. Corrective actions should be taken to fix the situation assessed before seven days have passed. If the situation is the consequence of maintenance, the maintenance can last as many as seven days. For the high region of risk, the ΔCDP threshold of 1.0E-06 is reached before three days of operation under the situation assessed. Corrective actions should be taken to fix the situation assessed at most before three days have passed. If the situation is the consequence of maintenance, the maintenance could last three days at most. To enter the very high region of risk, the CDF of the situation assessed has to be higher than 1.0E-03. This is an unacceptable situation. Corrective actions should be taken immediately after the situation triggers and the plant may have to be shutdown. The situation cannot be consequence of an online maintenance. An online maintenance associated with such a high value of CDF cannot and will not be allowed.

6.3.6 THE RESULTANT UNAVAILABILITY MATRIX

The Unavailability Matrix had 79% of elements belonging to the very low risk region (green) as shown in figure 6. 7. The situations described by the elements in the green region are not a safety concern and do not require corrective actions as long as the plant takes a suitable time to return to normal operation. The fire-related risk significant matrix elements (yellow or above, see Table 6.2) are mainly localized in six columns (KSF representatives) and one row (FPS). The matrix elements of these six columns and one row are all belonging to a significant level of fire-related risk. Besides, there is a small quantity of isolated combinations of unavailability whose fire-related risk is significant. These isolated combinations are the only noticeable impact of the unavailability of FPS aside from the yellow row. The unavailability of FPSs, apart from the yellow row and those isolated combinations, does not significantly affect the matrix results and, so, the fire-related risk. The fire-related risk significant combinations of unavailability are mostly influenced by the unavailability of KSF representatives.

The FPSs associated with isolated combinations of unavailability whose fire-related risk is significant belong to the auxiliary, control, and auxiliary feedwater buildings. New statements and/or restrictions taking into account those SSCs and FPSs related to the significant isolated combinations of unavailability and the SSCs and FPSs in Table 6.2 should be included in the maintenance rule.

This Unavailability Matrix becomes an important decision-making tool based on the risk information that color codes in the matrix present. Immediately, the matrix is presented to decision-makers, they do not border much on green and yellow areas, but rather concentrate their efforts, energy and resources on the red areas to ensure safety of the plant,



Basic_events:	OK	SB1	SB2	SB3	SB4	SB5	SB6	SB7	SB8	SB9	SB10	SB11	SB12	SB13	SB14	SB15	SB16	SB17	SB18	SB19	SB20	SB21
FDN Total	9,61E-06	9,61E-06	9,61E-06	7,77E-05	2,41E-05	2,80E-05	5,94E-04	1,25E-04	1,02E-03	9,61E-06	9,69E-06	5,35E-05	2,23E-04	2,80E-05	5,36E-05	9,61E-06	1,00E-05	9,98E-06	1,36E-05	9,61E-06	1,37E-05	2,28E-05
Te /(dias)	INF	INF	INF	5,36	25,26	19,83	0,62	3,16	0,36	INF	4762,53	8,32	1,71	19,80	8,30	INF	940,56	989,37	91,54	INF	89,62	27,71
AXXX9	3,75E-08	3,75E-08	3,75E-08	2,45E-07	2,39E-07	3,05E-07	2,45E-07	3,06E-07	1,15E-05	3,75E-08	3,75E-08	3,75E-08	3,75E-08	3,75E-08	3,75E-08	3,75E-08	3,75E-08	3,75E-08	3,75E-08	3,75E-08	3,75E-08	6,31E-07
AXXX3	5,68E-08	5,68E-08	5,68E-08	7,04E-08	6,83E-08	1,08E-07	7,04E-08	2,40E-07	1,12E-05	5,68E-08	5,68E-08	5,68E-08	8,29E-08	8,29E-08	5,68E-08	5,68E-08	5,68E-08	5,68E-08	5,68E-08	5,68E-08	5,68E-08	2,31E-07
AXXX4	3,35E-08	3,35E-08	3,35E-08	1,49E-07	1,48E-07	2,41E-07	1,49E-07	1,79E-07	1,05E-05	3,35E-08	3,35E-08	3,35E-08	3,35E-08	3,35E-08	3,35E-08	3,35E-08	3,35E-08	3,35E-08	3,35E-08	3,35E-08	3,35E-08	5,88E-07
AXXX8	1,15E-09	1,15E-09	1,15E-09	6,89E-07	1,15E-09	3,28E-07	1,20E-06	1,15E-09	3,28E-07	1,15E-09	1,15E-09	1,15E-09	1,15E-09	1,15E-09	1,15E-09	1,15E-09	1,15E-09	1,15E-09	1,15E-09	1,15E-09	1,15E-09	1,83E-08
AXXX9	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	1,16E-06	9,48E-09	0,00E+00	0,00E+00	0,00E+00	1,76E-09	0	0,00E+00	1,76E-09	0,00E+00	0,00E+00	1,97E-09	5,43E-09	0,00E+00	0,00E+00	0,00E+00
AXXX0	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	3,28E-09	9,19E-07	0,00E+00	0,00E+00	0,00E+00	2,06E-09	2,06E-09	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00
AXX1A	1,46E-06	1,46E-06	1,46E-06	1,48E-06	1,46E-06	1,47E-06	1,49E-06	1,46E-06	1,47E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06
AXX1B	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	6,13E-07	0,00E+00	0,00E+00	0,00E+00	0	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	3,53E-09
CXXX3	9,40E-08	9,40E-08	9,40E-08	2,01E-05	1,85E-07	9,40E-08	1,94E-04	1,76E-06	2,61E-06	9,40E-08	1,25E-07	3,76E-06	4,71E-06	7,66E-07	3,78E-06	9,40E-08	1,04E-07	9,40E-08	9,40E-08	9,40E-08	3,76E-06	1,12E-07
CXXX7	4,94E-08	4,94E-08	4,94E-08	5,38E-06	4,94E-08	6,82E-07	1,05E-05	4,94E-08	4,94E-08	4,94E-08	4,94E-08	1,52E-07	1,01E-07	4,94E-08	1,52E-07	4,94E-08	2,40E-07	4,94E-08	4,94E-08	4,94E-08	1,00E-07	2,80E-07
CXXX8	2,32E-07	2,32E-07	2,32E-07	2,32E-07	3,43E-07	2,93E-07	2,76E-07	7,27E-06	7,86E-05	2,32E-07	2,32E-07	2,32E-07	3,76E-06	3,76E-06	2,32E-07	2,32E-07	3,23E-07	2,32E-07	2,32E-07	2,32E-07	2,32E-07	2,32E-07
CXX13	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07
CXX16	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,43E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06
CXX17	5,89E-09	5,89E-09	5,89E-09	2,68E-07	5,89E-09	5,89E-09	5,62E-07	5,89E-09	1,98E-08	5,89E-09	5,89E-09	5,89E-09	5,89E-09	5,89E-09	2,58E-08	5,89E-09	5,89E-09	5,89E-09	5,89E-09	5,89E-09	5,89E-09	3,96E-07
CXX18	2,15E-07	2,15E-07	2,15E-07	1,35E-05	2,15E-07	5,44E-06	1,86E-05	2,15E-07	5,44E-06	2,15E-07	2,15E-07	1,39E-07	1,39E-07	2,15E-07	2,15E-07	2,15E-07	2,15E-07	2,15E-07	4,19E-06	2,15E-07	2,15E-07	5,05E-07
CXX19	3,94E-08	3,94E-08	3,94E-08	3,94E-08	7,49E-06	3,67E-06	3,94E-08	1,24E-05	2,60E-04	3,94E-08	3,94E-08	3,94E-08	4,48E-08	4,48E-08	3,94E-08	3,94E-08	3,94E-08	3,94E-08	3,94E-08	3,94E-08	3,94E-08	7,10E-08
CXX20	1,20E-08	1,20E-08	1,20E-08	1,20E-08	2,24E-08	1,37E-08	2,02E-08	2,61E-08	4,67E-07	1,20E-08	1,20E-08	1,20E-08	1,20E-08	1,20E-08	1,20E-08	1,20E-08	1,20E-08	1,20E-08	1,20E-08	1,20E-08	1,20E-08	1,20E-08
CXX22	0,00E+00	0,00E+00	0,00E+00	2,26E-07	0,00E+00	6,84E-08	2,26E-07	0,00E+00	6,84E-08	0,00E+00	0,00E+00	0,00E+00	0	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	4,07E-09
CXX31	1,19E-06	1,19E-06	1,19E-06	1,31E-06	1,36E-06	1,38E-06	3,78E-06	4,17E-06	1,75E-05	1,19E-06	1,19E-06	2,77E-06	3,21E-06	2,81E-06	2,80E-06	1,19E-06	1,19E-06	1,19E-06	1,19E-06	1,19E-06	1,19E-06	1,25E-06
CXX43	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07
CXX45	2,45E-08	2,45E-08	2,45E-08	2,45E-08	2,33E-06	1,12E-06	1,42E-07	1,50E-05	3,11E-04	2,45E-08	2,45E-08	4,41E-08	1,88E-07	1,42E-07	4,41E-08	2,45E-08	2,45E-08	2,45E-08	2,45E-08	2,45E-08	2,45E-08	9,13E-06
CX5	0,00E+00	0,00E+00	0,00E+00	5,87E-07	0,00E+00	2,94E-07	5,87E-07	0,00E+00	5,70E-07	0,00E+00	0,00E+00	0,00E+00	0	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	1,29E-08
CX6	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	8,58E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08
Cx7	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,38E-08	1,23E-08	1,23E-08	2,91E-07	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08
PEX138	2,22E-08	2,22E-08	2,22E-08	2,22E-08	2,22E-08	2,22E-08	2,18E-07	2,15E-07	1,64E-07	2,22E-08	2,22E-08	1,35E-07	4,26E-06	1,32E-07	1,34E-07	2,22E-08	2,22E-08	2,22E-08	2,22E-08	2,22E-08	2,22E-08	2,22E-08
PEX140	8,92E-09	8,92E-09	8,92E-09	8,92E-09	2,55E-07	1,11E-07	2,10E-08	1,14E-05	2,26E-04	8,92E-09	8,92E-09	1,21E-08	1,22E-06	7,39E-07	1,21E-08	8,92E-09	8,92E-09	8,92E-09	8,92E-09	8,92E-09	8,92E-09	9,53E-08
PEX141	3,09E-09	3,09E-09	3,09E-09	2,97E-06	3,09E-09	1,31E-06	6,76E-06	3,09E-09	1,31E-06	3,09E-09	3,09E-09	8,32E-09	8,32E-09	3,09E-09	8,32E-09	3,09E-09	3,09E-09	3,09E-09	3,09E-09	3,09E-09	3,09E-09	7,52E-08
PEX142	2,14E-08	2,14E-08	2,14E-08	2,14E-08	2,63E-06	2,14E-08	3,31E-08	4,00E-05	4,00E-05	2,14E-08	2,14E-08	2,14E-08	1,50E-06	1,50E-06	2,14E-08	2,14E-08	2,14E-08	2,14E-08	2,14E-08	2,14E-08	2,14E-08	2,14E-08
PEX143	4,88E-07	4,88E-07	4,88E-07	7,23E-06	4,88E-07	5,39E-06	1,55E-05	5,77E-07	5,98E-06	4,88E-07	4,88E-07	5,04E-06	5,04E-06	4,88E-07	5,11E-06	4,88E-07	4,88E-07	4,88E-07	4,88E-07	4,88E-07	4,90E-07	1,73E-06
PE1XXX	0,00E+00	0,00E+00	0,00E+00	1,74E-07	0,00E+00	0,00E+00	1,15E-06	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	2,17E-07	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00
PE1XX1	0,00E+00	0,00E+00	0,00E+00	2,79E-07	2,61E-08	9,50E-09	1,77E-06	1,59E-07	6,94E-06	0,00E+00	0,00E+00	0,00E+00	3,84E-07	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00
PE2XX1	7,18E-08	7,18E-08	7,18E-08	7,18E-08	7,18E-08	7,18E-08	5,41E-07	6,60E-07	6,22E-07	7,18E-08	7,18E-08	3,54E-07	6,80E-06	4,93E-07	3,48E-07	7,18E-08	7,18E-08	7,18E-08	7,18E-08	7,18E-08	1,53E-07	7,72E-08
RX132	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	6,03E-09	3,40E-08	0,00E+00	3,01E-06	0,00E+00	0,00E+00	0,00E+00	1,60E-07	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	1,45E-08
RX133	5,26E-07	5,26E-07	5,26E-07	5,26E-07	5,26E-07	5,26E-07	4,77E-06	4,70E-06	3,74E-06	5,26E-07	5,26E-07	3,28E-06	5,12E-05	3,28E-06	3,24E-06	5,26E-07	5,26E-07	5,26E-07	5,26E-07	5,26E-07	5,29E-07	5,26E-07
RX134	7,54E-07	7,54E-07	7,54E-07	7,54E-07	7,54E-07	7,54E-07	6,68E-06	6,58E-06	5,26E-06	7,54E-07	7,54E-07	4,61E-06	7,17E-05	4,61E-06	4,55E-06	7,54E-07	7,54E-07	7,54E-07	7,54E-07	7,54E-07	7,54E-07	7,54E-07
RX139	5,61E-07	5,61E-07	5,61E-07	5,61E-07	5,61E-07	5,61E-07	5,40E-06	5,27E-06	6,47E-06	5,61E-07	5,61E-07	3,68E-06	5,64E-05	3,67E-06	3,63E-06	5,61E-07	5,61E-07	5,61E-07	5,61E-07	5,61E-07	5,61E-07	6,04E-07
SX187	6,85E-07	6,85E-07	6,85E-07	7,65E-07	1,79E-06	6,85E-07	2,06E-05	8,74E-06	2,86E-06	6,85E-07	6,85E-07	1,90E-05	9,96E-07	6,85E-07	1,90E-05	6,85E-07	6,85E-07	6,85E-07	6,85E-07	6,85E-07	9,36E-07	6,85E-07
SX190	3,86E-08	3,86E-08	3,86E-08	1,71E-05	3,86E-08	3,86E-08	2,94E-04	7,75E-08	7,90E-08	3,86E-08	8,47E-08	5,66E-06	5,66E-06	3,86E-08	5,66E-06	3,86E-08	3,86E-08	3,86E-08	3,86E-08	3,86E-08	5,52E-08	3,86E-08
TX167X1	6,65E-09	6,65E-09	6,65E-09	6,65E-09	6,65E-09	1,75E-08	7,63E-08	4,20E-07	4,98E-06	6,65E-09	6,65E-09	6,65E-09	2,49E-07	6,65E-09	6,65E-09	6,65E-09	6,79E-08	3,74E-07	8,86E-09	6,65E-09	7,69E-09	1,47E-07
TX167X2	1,83E-08	1,83E-08	1,83E-08	1,83E-08	1,83E-08	1,83E-08	4,46E-08	1,83E-08	1,08E-07	1,83E-08	1,83E-08	1,83E-08	3,15E-08	1,83E-08	1,83E-08	1,83E-08	1,83E-08	1,83E-08	1,96E-08	1,83E-08	1,83E-08	2,14E-08
TX167X3	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	3,33E-09	7,81E-09	0,00E+00	2,46E-08	0,00E+00	0,00E+00	0,00E+00	1,43E-07	0,00E+00	0,00E+00	0,00E+00	3,53E-08	0,00E+00	0,00E+00	0,00E+00	0,00E+00	7,37E-08

7

Figure 6.6 Typical section of the Unavailability Matrix [94]

6.3.7 UNCERTAINTY ANALYSIS

The purpose of this analysis is to evaluate the uncertainty associated with the development and quantification of the UM. The goal is to conclude whether the tool is robust and the results provided are trustworthy enough. The target of the analysis is to estimate the mean and the 95 percentile of the UM matrix elements so as to compare them with the point estimate values.

The only uncertainty-related data available for the development of the uncertainty analysis are the cumulative distribution functions and the probability density functions of the dCDFs used to compute the UM matrix elements. RiskSpectrum ® provides both functions in a discrete manner, and their analytical expressions are unknown.

The Monte Carlo method is used to carry out the uncertainty analysis because it suits the available data. The Monte Carlo method is sequentially applied to each matrix element. The flow chart from Figure 4 shows the Monte Carlo methodology used to apply the uncertainty analysis. The discrete cumulative distribution functions of the dCDFs are adjusted to segmented linear regressions. Random seeds between 0 and 1 are used to obtain random point estimate values of the dCDFs for each simulation. A simulation corresponds to the execution of Equation (1) for one UM matrix

[7] For confidentiality the details of the Unavailability Matrix cannot be shown. The because of large nature of the details are shown by zooming the potions of the matrix to show the details

element. The mean and the 95 percentile of a matrix element are computed after running the desired number of simulations.

The Monte Carlo methodology presented in Figure 6.4 is executed using a Matlab ® script. The script provides the uncertainty parameters (i.e. Mean and 95 percentile) for all the matrix elements in a matrix layout equal to that of the UM.

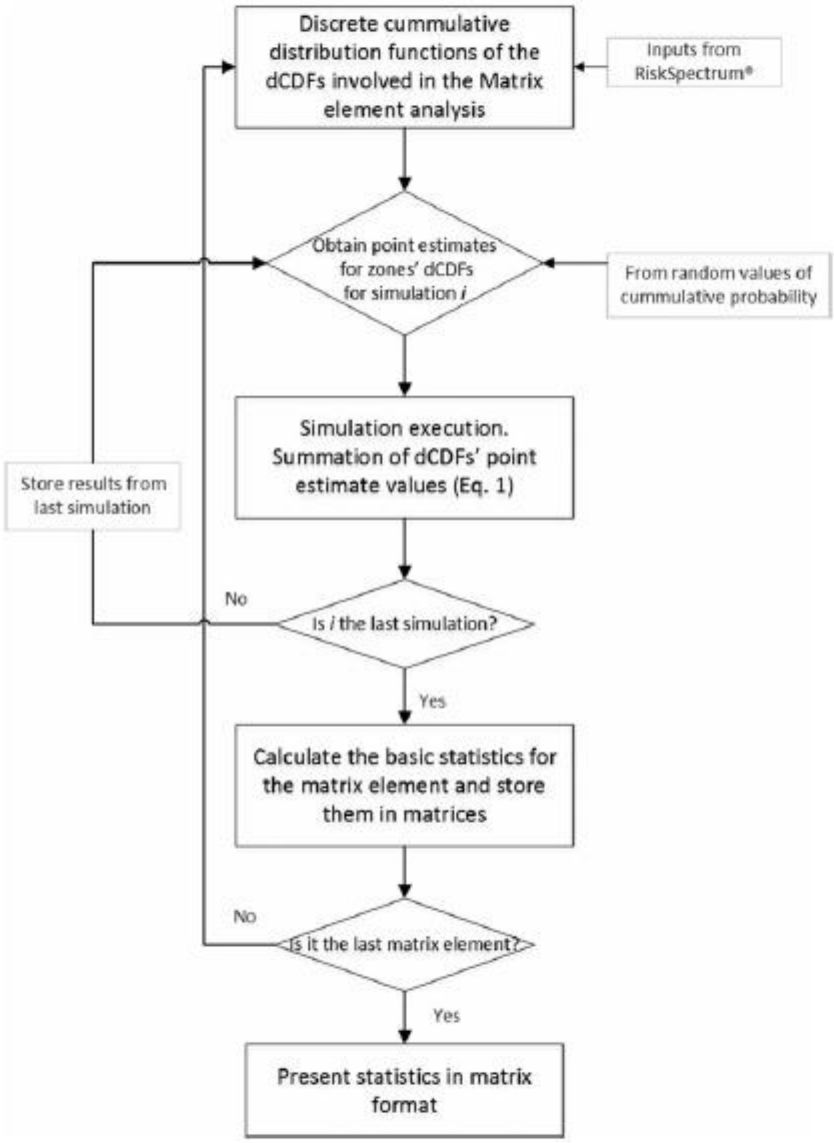

Discrete cummulative distribution functions of the dCDFs involved in the Matrix element analysis
Inputs from RiskSpectrum®
Obtain point estimates for zones' dCDFs for simulation *i*
From random values of cummulative probability
Simulation execution. Summation of dCDFs' point estimate values (Eq. 1)
Store results from last simulation
No
Is *i* the last simulation?
Yes
Calculate the basic statistics for the matrix element and store them in matrices
No
Is it the last matrix element?
Yes
Present statistics in matrix format

Figure 6.7 Monte Carlo methodology [93]

The Matlab ® script has been satisfactorily validated by comparison of results with RiskSpectrum ®'s uncertainty analysis algorithm for a specific made-up case. RiskSpectrum ®'s uncertainty analysis is also based upon the Monte Carlo method [95]. A sensitivity analysis has been performed to decide that 10,000 is the optimal number of simulations to be carried out per matrix element, executing the Matlab ® script.

6.3.8 RESULTS AND CONCLUSIONS OF THE UNCERTAINTY ANALYSIS

The 95 percentile of the NPP's fire CDF is the representative figure of the uncertainty associated with the development and quantification of the UM. However, the Monte Carlo method slightly overestimates the fire CDF. The comparison between mean values and point estimate values yields that the former are greater than the latter. Therefore, part of the difference between the 95 percentile values and the point estimate values belongs to overestimation, not to uncertainty.

Four hundred twenty-seven elements of the UM ascend to the directly superior risk category when evaluating the 95 percentile results instead of the point estimate values. Four hundred twenty-seven elements constitute the 8.5% of the whole matrix. No matrix element ascends to a two times superior risk category. Three hundred and four of these 427 elements belong to two columns whose point estimate values are near the threshold between two risk categories. The point estimate values of the rest of ascending elements, which belong to different columns, are also near the threshold between two risk categories. The difference between the 95 percentile value and the point estimate value is roughly one to two orders of magnitude lower than the point estimate values for the majority of matrix elements.

The conclusions regarding the risk category of matrix elements when assessing the 95 percentile instead of point-estimate values are virtually the same. From the 8.5% of the matrix elements which ascend to the directly superior risk category, 74% (314) are already considered as risk significant. Besides, the small difference between the 95 percentile value and the point estimate value, and the overestimation fact, shows that the uncertainty associated to the matrix analysis is low [96]. The uncertainty analysis demonstrates that the UM is a robust tool. The results obtained are trustworthy enough as to be used in risk-informed decision making processes. The driving factors are the assessment of those principles of integrated decision making that play the most significant role in the decision (i.e., defense-in-depth philosophy is maintained, sufficient safety margin is maintained, any changes to risk are small and consistent with regulatory requirement. Further research will be devoted to the use of sensitivity analyses in the assessment of model and assumption uncertainties for the risk significant cases.

6.4 UNDERSTANDING AND ASSESSING THE IMPACT OF OTHER RISK ASSESSMENT.

In making an integrated decision, the decision maker needs to consider elements such as definition of the decision, identify the regulatory requirements risk-informed analysis etc. When the risk-informed analysis element is considered, the uncertainties associated with the risk analysis (i.e., the results) need to be addressed so that the robustness of the conclusions of the risk analysis is understood and appropriately considered in the decision. The need to understand the results of the risk assessment in detail is required to identify the sources of uncertainty that are relevant to the decision. It is important to assess the results generated by combining results from PSA model for different hazard groups (E.g. Internal Initiating events, internal fires, seismic events, etc.). In this work the aggregation of results from Internal Events PSA model and the fire PSA model is considered.

NUREG-1855 states that the results from different PSAs (i.e., Fire PSA, Internal Events PSA, External Events PSA, Internal Floods PSA, and others) can be aggregated. The contributions from different PSAs can be aggregated for the operational states and the risk groups are different amongst PSAs. Some issues have to be taken into account though. For instance, the level of detail and precision may be different when combining different PSA models. Nevertheless, different uncertainty levels do not prevent the aggregation of CDFs of different Risk contributors as long as the different sources of conservatism are identified

The results of the fire PSA model and the results of Internal Events PSA model have been aggregated. An Unavailability matrix containing the aggregation of both Internal Events and the fire PSA have been computed. The only difference would be the aggregation of the corresponding contribution of Internal Events PSA to all the matrix elements. This contribution is restricted to Unavailability of KSFs for FPSs are not assessed in the Internal Events PSA.

It has been considered convenient to apply the criteria of Table 6.1. Limits of risk to the set of the two probabilistic analyzes. A new matrix is generated to consider the combination of risk of the elements of internal events PSA and the fire PSA. The values of the matrix have been calculated as

$$CDF_{i,j}^{set} = CDF_{i,J}^{fire} + CDF_{i}^{internal} \qquad 6.3$$

The subscript i represents the unavailability of some fire protection system of some room. The subscript j represents the unavailability of some safety function by changing the status to True of a representative Basic Event.

$$\Delta CDF_{i,j}^{set} = CDF_{i,j}^{set} - CDF_{0,0}^{set} \geq 0 \qquad 6.4$$

The subscripts 0, 0 refer to the nominal CDF value. In nominal state all Basic Events of the PSA database are in a state Normal and no changes have been made to it. If in addition the superscript is "Set", its value is the sum of the nominal of Fire CDF and nominal Internal CDF.

Table 6.3 Colors according to risk, with equivalence to values of the CDF of the (Internal +Fires) PSA matrix

color	Condition imposed	Condition translated to the matrix
Green	ΔCDF*7/365<1E-6	CDF < 7.22E-05
Yellow	ΔCDF*7/365>1E-6	7.22E-05 <CDF <1.42E-04
Orange	ΔCDF*3/365>1E-6	1.42E-04 <CDF< 1E-03
Red	CDF> 1E-03	CDF>1E-03

Table 6.3 shows the equivalence between the increased in CDF required for it to be in a certain range and the value or range of values of $CDF_{i,j}$ that delimit each strip of the matrix CDF Fire and Internal together. The same formula is used as in Equation 6.5 adapted to the fact of having two PSA evaluated jointly.

$$CDF_{i,j}^{set} > CDF_{0,0}^{set} + \frac{365}{7} \bullet 10^{-6} \qquad 6.5$$

The nominal value of the Fire PSA is 9.836E-6, the nominal value of the internal Events PSA is 1.019E-5, and the sum of the two ($CDF_{0,0}^{set}$) is 2.003E-05.

It is important to keep in mind that two different probabilistic analyzes are being added with origins of sequences of different accidents, and different degrees of uncertainty.
Only 51 new simulations would had to be run in the end (1 simulation per KSF representative). RI regions' limits would have to be reassessed to include the contribution of the Internal Events PSA. The first analysis to be done after the creation of the new Matrix would be the comparison of the Fire Matrix and the Aggregation Matrix. The purpose would be to see whether the inclusion of Internal Events PSA modifies the look of the Matrix, so to say, whether there are more important Basic Events from the point of view of RI. The analysis of which PSA contributes the most to the CDFs in the Matrix elements could be performed afterwards. To do so, the fact that each Matrix element is different, in terms of Risk, would have to be taken into account in order to weight the values and obtain a unique result for the whole Matrix. This result would highlight whether Fire PSA or Internal Events PSA contributes the most to the aggregated Matrix. Thus, the importance of the Fire PSA in the overall CDF of the plant could be assessed.

6.4.1 RESULTS OF THE AGGREGATION MATRIX

Results from the new joint matrix show most elements of the array assigned risk levels yellow-orange-Red. Altogether, there are more Basic Events in risk levels yellow-orange-red in the case of fire alone. List of Basic Events that cause a substantial change in risk in all the scenarios in which a fire control system is unavailable according to their level of risk increase (or color band):

- Yellow color band: 1BMxxxxxAS, 1TBxxxxxxS*, 1VKxxxxxxO*, 1VMxxxxxxA*, xREPKTDIBE*, 1BMxxxxxAR*, 1VMxxxxxAA*, 1VRxxxxxxA*, 1BMxxxxxAR*, 1VRxxxxxxC*
- Orange color band: 1VRxxxxxxA, 1BHCAxxxAF*, 1VNxxxxxxA*
- Red color band: 1BLBCxGxBF, 1BHCAxxxAF*

Basic Events with an asterisk are those that have changed the group of color. There is no Basic Event that has jumped more than one level of risk. That means that all the yellows marked with asterisks before they were significant for the risk, the oranges with an asterisk before were yellow and the red with an asterisk before was orange. There have not been green jumps to orange / red or yellow to red.

New Basic Events and the safety functions they represent:

- 1TBxxxxxxS: TURBO-PUMP 36P01 FAILURE TO START
  - L1+L2: INSUFFICIENT FLOW OF A.A.A. to GV'S (< 380 gpm)
  - L4: LOSS OF THE FLOW TO GVs B or C
  - L6: FAILURE OF SECONDARY HEAT EXTRACTION
- 1VKxxxxxxO: MOTOR VALVE OF CONTROL VCF-3602 FAILURE A REMAIN OPEN:
  - L1+L2: INSUFFICIENT FLOW OF A.A.A. to GV'S (< 380 gpm)
- 1VMxxxxxxA: MOTORIZED VALVE VM-3078 FAILURE TO THE OPENING:
  - L1+L2: INSUFFICIENT FLOW OF A.A.A. to GV'S (< 380 gpm)
  - L4: LOSS OF THE FLOW TO GVs B or C
- xREPKTDIBE: FAILURE TO ENERGIZE RELI TDI TRAIN B:
  - B2: FAILURE TO RECOVER ELECTRICAL ENERGY EXTERIOR
- 1BMxxxxxAR: MOTORIZED PUMP 11P01A FAILURE IN OPERATION:

    - F3: "FEED & BLEED" FAILURE (REACTOR SHOTS AND TURBINE)
    - U1+U2: HIGH PRESSURE INJECTION SYSTEM FAILURE A COLD BRANCHES
- 1VMxxxxxAA: VALV. MOTORIZED VM-1410A FAILURE AT OPENING:
    - U2: FAILURE OF THE HIGH PRESSURE INJECTION SYSTEM A COLD BRANCHES
- 1VRxxxxxxA: VALV. RETENTION 15004 FAILURE AT OPENING:
    - F3: "FEED & BLEED" FAILURE (REACTOR SHOTS AND TURBINE)
    - U2: FAILURE OF THE HIGH PRESSURE INJECTION SYSTEM A COLD BRANCHES
- 1BMxxxxxAR: MOTORIZED PUMP 14P01A OPERATING FAILURE
    - D2: INJECTION AND RECIRCULATION TO COLD BRANCHES
    - U2: FAILURE OF THE HIGH PRESSURE INJECTION SYSTEM A COLD BRANCHES
    - W: LOSS OF REFRIGERATION IN RHR MODE
- 1VRxxxxxxC: VALV. RETENTION 43002 FAILURE TO CLOSURE
    - Z2: INSUFFICIENT REFRIGERATION IN TRAIN OF Essential Service Water (ESW)

It has been observed the appearance of numerous Basic Events causing Increases in the level of risk. Even so it is unknown for the moment if the Fire PSA had values very close to the limit of the yellow strip and the inclusion of the Internal PSA had little importance in the changes, or otherwise or if its inclusion has had strong repercussions. For this reason, the proposal is to analyze which of the PSA has most influenced the CDF increases

The values presented in the aggregated Fire and Internal matrix can be understand as described in Equation 6.6.

$$CDF_{i,j}^{set} = CDF_{0,0}^{set} + \Delta CDF_{i,j}^{set} \qquad 6.6$$

The values of the matrix are the sum of the nominal value plus an increase (provided by the disabling of safety functions and / or fire protection system). . Thus, Equation 6.7 is obtained; from equation 6.3.

$$CDF_{i,j}^{set} = CDF_{i,j}^{fire} + CDF_{j}^{\text{int}ernal} \qquad 6.3$$

If i = j = 0, then

$$CDF_{0,0}^{set} = CDF_{0,0}^{fire} + CDF_{0}^{\text{int}ernal}$$

Therefore

$$\Delta CDF_{i,j}^{set} = \Delta CDF_{i,j}^{fire} + \Delta CDF_{j}^{\text{int}ernal} \qquad 6.7$$

That is, the increase is in turn the sum of the increments given by two different PSA. It is considered interesting to estimate what PSA (Fire or Internal) contributes more CDF increase to the joint matrix.

$$\Delta CDF_{i,j}^{fire} \underset{>}{\le} \Delta CDF_{j}^{\text{int}ernal} \tag{6.8}$$

Taking into consideration the importance of greater conservatism which is associated with an analysis such as the Fire PSA. To a certain level, conservative bias will be reduced by the development of detailed models and corresponding guidance for the analysis of external hazards, fires, and LPSD that will provide a similar level of rigor to the one currently used in internal events at-power PRAs. However, a higher level of uncertainty does not preclude the aggregation of results from different risk contributors; but it does require that sources of conservatism having a significant impact on the risk-informed application be recognized.

To ensure this conservatism, we want to give a numerical descriptive value. The methodology developed proposes to provide a value of 0 to 1, or from 0% to 100%. This value tends to 0% when the increases provided by the Internal PSA are greater than the increments provided by the Fire PSA. If the increase in risk of each situation is mostly caused by the Fire PSA, the numerical value end tends to 100%. When the two increase the risk in the same measure the value would be 50%, half between the two extremes.

Equation 6.9 is the formula that has the above properties described.

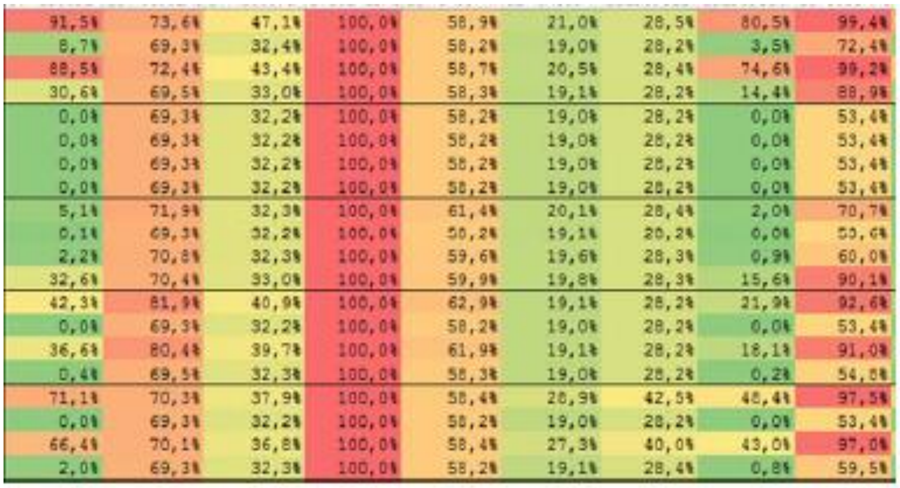
$$\text{Representative value} = \frac{\Delta CDF^{fires}}{\Delta CDF^{set}} \tag{6.9}$$

A representative increase cannot be drawn from the Fire matrix or the joint matrix either. A new matrix is built as a first step, matrix of representative values, with the formula of Equation 6.10. The Elements of this matrix are identified with the acronym vri, j.

$$Vr_{i,j} = \frac{\Delta CDF_{i,j}^{fire}}{\Delta CDF_{i,j}^{set}} = \frac{\Delta CDF_{i,j}^{fire}}{\Delta CDF_{i,j}^{fire} + \Delta CDF_{j}^{\text{int}ernal}}$$

$$== \frac{CDF_{i,j}^{fire} - CDF_{0,0}^{fire}}{(CDF_{i,j}^{fire} - CDF_{0,0}^{fire}) + (CDF_{j}^{\text{int}ernal} - CDF_{0}^{\text{int}ernal})} \tag{6.10}$$

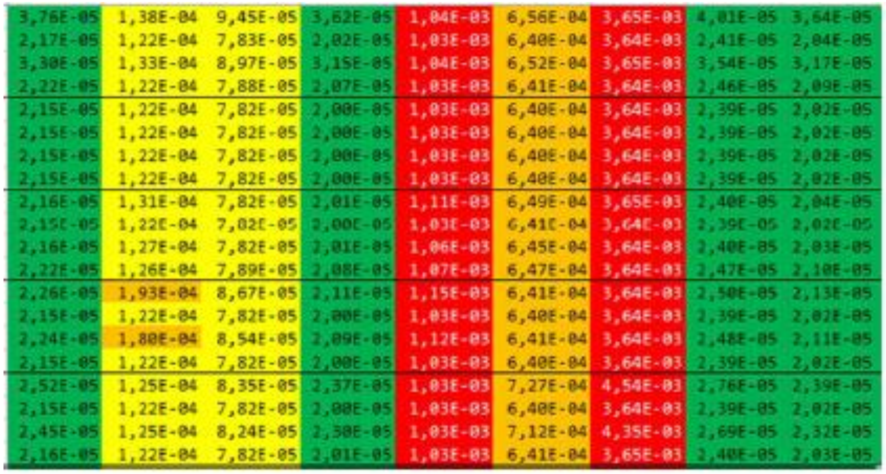
From this point you get a matrix that describes each element of the joint matrix. A sample of example can be seen in figures 6.8 and 6.9 below



91,5%	73,6%	47,1%	100,0%	58,9%	21,0%	28,5%	80,5%	99,4%
8,7%	69,3%	32,4%	100,0%	58,2%	19,0%	28,2%	3,5%	72,4%
88,5%	72,4%	43,4%	100,0%	58,7%	20,5%	28,4%	74,6%	99,2%
30,6%	69,5%	33,0%	100,0%	58,3%	19,1%	28,2%	14,4%	88,9%
0,0%	69,3%	32,2%	100,0%	58,2%	19,0%	28,2%	0,0%	53,4%
0,0%	69,3%	32,2%	100,0%	58,2%	19,0%	28,2%	0,0%	53,4%
0,0%	69,3%	32,2%	100,0%	58,2%	19,0%	28,2%	0,0%	53,4%
0,0%	69,3%	32,2%	100,0%	58,2%	19,0%	28,2%	0,0%	53,4%
5,1%	71,9%	32,3%	100,0%	61,4%	20,1%	28,4%	2,0%	70,7%
0,1%	69,3%	32,2%	100,0%	58,2%	19,1%	28,2%	0,0%	53,6%
2,2%	70,8%	32,3%	100,0%	59,6%	19,6%	28,3%	0,9%	60,0%
32,6%	70,4%	33,0%	100,0%	59,9%	19,8%	28,3%	15,6%	90,1%
42,3%	81,9%	40,9%	100,0%	62,9%	19,1%	28,2%	21,9%	92,6%
0,0%	69,3%	32,2%	100,0%	58,2%	19,0%	28,2%	0,0%	53,4%
36,6%	80,4%	39,7%	100,0%	61,9%	19,1%	28,2%	18,1%	91,0%
0,4%	69,5%	32,3%	100,0%	58,3%	19,0%	28,2%	0,2%	54,8%
71,1%	70,3%	37,9%	100,0%	58,4%	28,9%	42,5%	48,4%	97,5%
0,0%	69,3%	32,2%	100,0%	58,2%	19,0%	28,2%	0,0%	53,4%
66,4%	70,1%	36,8%	100,0%	58,4%	27,3%	40,0%	43,0%	97,0%
2,0%	69,3%	32,3%	100,0%	58,2%	19,1%	28,4%	0,8%	59,5%

Figure 6.8 Fragment of the comparative matrix of increments

In Figure 6.8 we can observe the risk levels of the fragment



3,76E-05	1,38E-04	9,45E-05	3,62E-05	1,04E-03	6,56E-04	3,65E-03	4,01E-05	3,64E-05
2,17E-05	1,22E-04	7,83E-05	2,02E-05	1,03E-03	6,40E-04	3,64E-03	2,41E-05	2,04E-05
3,30E-05	1,33E-04	8,97E-05	3,15E-05	1,04E-03	6,52E-04	3,65E-03	3,54E-05	3,17E-05
2,22E-05	1,22E-04	7,88E-05	2,07E-05	1,03E-03	6,41E-04	3,64E-03	2,46E-05	2,09E-05
2,15E-05	1,22E-04	7,82E-05	2,00E-05	1,03E-03	6,40E-04	3,64E-03	2,39E-05	2,02E-05
2,15E-05	1,22E-04	7,82E-05	2,00E-05	1,03E-03	6,40E-04	3,64E-03	2,39E-05	2,02E-05
2,15E-05	1,22E-04	7,82E-05	2,00E-05	1,03E-03	6,40E-04	3,64E-03	2,39E-05	2,02E-05
2,15E-05	1,22E-04	7,82E-05	2,00E-05	1,03E-03	6,40E-04	3,64E-03	2,39E-05	2,02E-05
2,16E-05	1,31E-04	7,82E-05	2,01E-05	1,11E-03	6,49E-04	3,65E-03	2,40E-05	2,04E-05
2,15E-05	1,22E-04	7,82E-05	2,00E-05	1,03E-03	6,41E-04	3,64E-03	2,39E-05	2,02E-05
2,16E-05	1,27E-04	7,82E-05	2,01E-05	1,06E-03	6,45E-04	3,64E-03	2,40E-05	2,03E-05
2,22E-05	1,26E-04	7,89E-05	2,08E-05	1,07E-03	6,47E-04	3,64E-03	2,47E-05	2,10E-05
2,26E-05	1,93E-04	8,67E-05	2,11E-05	1,15E-03	6,41E-04	3,64E-03	2,50E-05	2,13E-05
2,15E-05	1,22E-04	7,82E-05	2,00E-05	1,03E-03	6,40E-04	3,64E-03	2,39E-05	2,02E-05
2,24E-05	1,80E-04	8,54E-05	2,09E-05	1,12E-03	6,41E-04	3,64E-03	2,48E-05	2,11E-05
2,15E-05	1,22E-04	7,82E-05	2,00E-05	1,03E-03	6,40E-04	3,64E-03	2,39E-05	2,02E-05
2,52E-05	1,25E-04	8,35E-05	2,37E-05	1,03E-03	7,27E-04	4,54E-03	2,76E-05	2,39E-05
2,15E-05	1,22E-04	7,82E-05	2,00E-05	1,03E-03	6,40E-04	3,64E-03	2,39E-05	2,02E-05
2,45E-05	1,25E-04	8,24E-05	2,30E-05	1,03E-03	7,12E-04	4,35E-03	2,69E-05	2,32E-05
2,16E-05	1,22E-04	7,82E-05	2,01E-05	1,03E-03	6,41E-04	3,65E-03	2,40E-05	2,03E-05

Figure 6.9 Levels of importance of the fragment of the comparative matrix of increments

It is important to note that a simple average, rows, columns, or general, of the new representative value matrix would not be representative of the set. An example Basic Event can be highlighted to illustrate the problematic for the Basic Event 1VExxAxxAS (fourth Basic Event in the illustrations 2 and 3) the increase is entirely provided by the Fire PSA, the Internal PSA does not provide any increase

($\Delta CDF^{fire}_{1vB1A19AS} = 0$). This Basic Event is at one end of the possible values which can give the formula for the calculation of vri, j, but by observing its level of risk in Illustration 3 is clear that it has low impact of the Basic Event in the plant (green risk level). To get an average representative of the whole matrix, a methodology has been developed that allows ponder the importance of each element of the matrix.

A new auxiliary matrix has been created, the matrix of relative errors. Their elements are called eri, j. The matrix has dimensions from row 1 and the column 1 to the end of the rows and columns of the joint FDN matrix. It is therefore omitted the plant states that either do not have any problem with the suppression of fire (row 0) or have no safety function of partially or totally unavailable (column 0).

$$\text{Relative error}_{\text{i, j}}= er_{i,j} = \frac{CDF_{i,j}^{set} - CDF_{0,0}^{set}}{CDF_{0,0}^{set}} \qquad 6.11$$

Being $CDF_{0,0}^{set}$ the nominal value, or base, of the joint matrix. With the matrix of relative errors can be observed in a descriptive way the importance that has an element of the joint matrix. A relative error of 0 means that no there is a difference, and a relative error of 1 means that the joint FDN of the case is the double that of the nominal.

A new matrix, weight matrix, has been calculated with a weight factor (wi, j) customized for each element of the matrix using the auxiliary matrix of the matrix using the auxiliary matrix of relative errors. The denominator of the weight factor is the sum of all the elements of the matrix of relative errors.

$$w_{i,j} = \frac{er_{i,j}}{\sum_i \sum_j er_{i,j}} \qquad 6.12$$

With the weight matrix you can relate an element of the matrix, that is, a couple fire protection system - safety function, with its importance relative within the matrix. The information provided by the weight matrix is the same as the matrix of relative errors, but the weight matrix is focused on achieving the final representative value and it is not possible to read it qualitatively as the matrix of relative errors. For example the column of the Basic event (1VExxAxxAS), its weight is very close to zero in the large most elements.

A last matrix has been generated, the matrix of representative values weighted, whose elements are vrpi, j. This matrix is simply a

$$vrp_{i,j} = vr_{i,j} \cdot w_{i.j} \qquad 6.13$$

The total sum of all the elements of the representative value matrix weighted is the final representative numerical value object of this methodology.

$$\text{Representative value} = \sum_i \sum_j vrp_{i,j} = \sum_i \sum_j (vr_{i,j} - w_{i,j})$$

$$= \sum_i \sum_j \left(vr_{i,j} \cdot \frac{er_{i,j}}{\sum_i \sum_j er_{i,j}} \right) = \frac{1}{\sum_i \sum_j er_{i,j}} \sum_i \sum_j \left(vr_{i,j} \cdot er_{i,j} \right) \qquad 6.14$$

The total sum of all the elements of the representative value matrix weighted is the final representative numerical value object of this methodology. It can be seen in the equation of the final representative value, that the use of matrix of weights can be ignored

The result of applying the methodology to the case study gives as a value representative 38.4%. Therefore the Internal PSA has more influence in the increase in risk. This shows that fire PSA contributes 38.4% to increase in risk and it compares well with work done by USNRC, IPE/IPEEE and NFPA 805. The figure 6.10 below shows the comparison of ratio of fire CDF to internal events CDF for earlier IPEEE and recent NFPA 805 estimates.

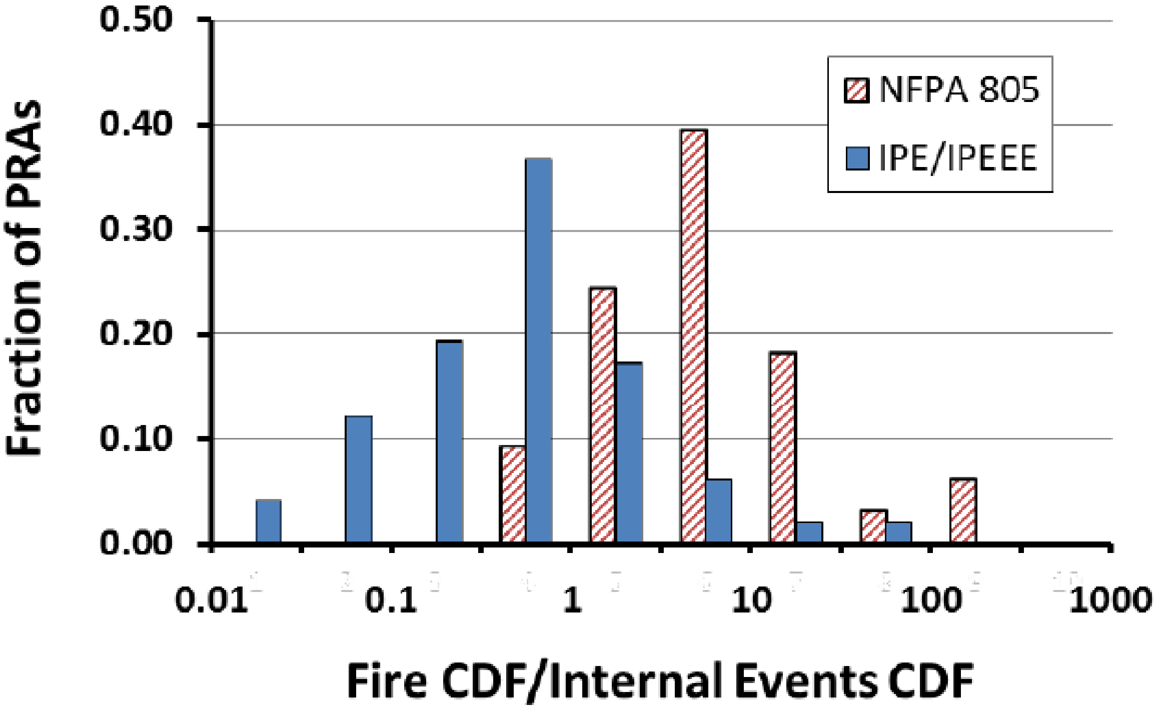


Figure 6.10 Ratio of Fire CDF to internal events CDF: comparison of IPE/ IPEEE and NFPA 805 estimates [97]

According to Siu et. tal, (2016) [97], in the IPE/IPEEE studies, fire is an important contributor for many plants. In the recent LAR submittals, fire is a major or even dominant contributor for most plants. In the Indiana Point 2 (1982) NPP the percentage % of fire contribution to total CDF is 38%. The summary of the statistics from representative sample of NFPA 805 LARs % of contribution to total CDF ranges from 35% -95%.The possible explanations to figure 6.10 for dominance of fire in the analysis for IPE/IPEEE and NFPA 805 change include: a) the numerous plant changes made since the IPE/IPEEE studies were preferentially effective for non-fire related initiators, b) the IPEEE studies underestimated the importance of key issues addressed in the recent studies, or c) the recent fire PRA results are indeed conservative.

6.5 CONCLUDING REMARKS

Fire Risk-informed decision making is very important for effective and efficient means of using financial resources, man hours and performance delivery to ensure safe operation and safety at Nuclear Power Plants. The use of clearly documented Fire PSA methodology as described by NUREG/CR-6850 has brought confidence in the Fire risk assessment process as the methodology mature.

Although a communication plan is not required for every regulatory activity, it is likely the issues addressed in the risk-informed process will generate enough interest and impact that the technical staff and decision makers would benefit from a plan to convey the process and its outcomes to internal and external stakeholders

The Fire Risk Unavailablity Matrix had been created as an innovative tool for communicating Fire risk in the frame of Risk-informed decision making process. Therefore, there is the need to develop real time fire risk assessment and risk-informed decision making tool at the nuclear power plants operations. Real time risk assessment tool referred to as Risk Monitor has been developed for Internal Events PSA. The next chapter is devoted to the feasibility study of developing Fire-Related Risk Monitor from the RiskSpectrum ® Fire PSA. This will contribute to real time Risk-informed decision making and risk communication processes.

CHAPTER SEVEN

FEASIBILITY OF THE DEVELOPMENT OF A FIRE-RELATED RISK MONITOR FROM THE RISKSPECTRUM® FIRE PSA OF PWR NPP

7.0. BACKGROUND AND SIGNIFICANCE OF THE PROJECT

It was only after the severe cable tray fire at the Brown's Ferry reactor site in 1975 that the operational importance of fire safety was fully recognized. As a result of this incident, the USNRC instituted a new set of fire safety requirements (referred to as prescriptive requirements) which specifically addressed these unique concerns. The implementation of these requirements for most commercial nuclear power plants requires significant plant modifications. In most cases, as backfits, the modifications were often expensive undertaking as well.

In order to overcome the difficulties from the prescriptive and deterministic regulations, risk-informed and performance-based analyses were recently introduced into a fire protection engineering practice. Risk-informed, performance-based fire protection is an integration of decision analysis and quantitative risk assessment with a defined approach for quantifying the performance success of Fire Protection Systems (FPS). An internal fire analysis that is called as a fire PSA is performed to estimate the contribution of potential internal fires to an overall plant CDF and to identify the vulnerabilities of a safe shutdown capability after such fires.

Fire PSA has been developed through research, updates and reviews over the years. The maturity of the NPP fire PSA is intermediate as compared with the internal events PSA. The CDF is quantified per reactor year, however, PSA is maintained as a living PSA that is regularly updated to reflect the current design and operation of the plant. The current state-of-the-art research is geared towards evaluation of the instantaneous risks so that risk-informed decision are taken in real time.

A Risk Monitor is one of the specific applications of a Living PSA and is a real-time analysis tool used to determine the point-in-time risk which is based on the actual plant configuration defined in terms of the Plant Operational Mode. According to IAEA Risk Monitor is defined as "a plant specific real-time analysis tool used to determine the instantaneous risk based on the actual status of the systems and components. At any given time, the Risk Monitor reflects the current plant configuration in terms of the known status of the various systems and/ or components – for example, whether there are any components out of service for maintenance or tests. The Risk Monitor model is based on, and is consistent with, the Living PSA. It is updated with the same frequency as the Living PSA. Risk monitor has been developed for Internal Events PSA as risk informed decision-making tool. The Risk Monitor is used by the plant staff in support of operational decisions. [98].

Collaboration research project has been established between Nuclear Engineering Research Group (NERG) at the Physics Department of Technical University of Catalonia (UPC) and a Spanish NPP. The project is a Risk Monitor of Fire Probability Safety Assessment (PSA) of Pressurized Water Reactor (PWR) of Westinghouse Nuclear Power Plant (NPP). This research and development project is a voluntary initiative of the Spanish Nuclear Power Plant to show that its

Fire protection systems are in compliance with the regulatory standard and current areas of research.

The project is the development of FIRE Risk Monitor related to FIRE PSA of a Spanish Nuclear Power Plant. The goal is to develop Fire Risk Monitor to quantify the instantaneous risk triggered by the possibility of fire occurring at any plant area. Risk Monitors are now used routinely to provide risk information for use by plant operators in managing plant safety. The main reason for developing Risk Monitors has been to produce a PSA tool to generate risk information for use in the day to day management of operational safety. Risk Monitors are being used to provide an input into maintenance planning to ensure that these activities are scheduled in such a way that high peaks in the risk are avoided wherever possible and the cumulative risk is low. They provide information on which components should be returned to service before particular maintenance activities are carried out and which of the remaining operational components are the most important to ensuring plant safety during specific maintenance outages.

Although, the PSA model in Risk Monitor is based on Living PSA model, it is important to realize that the Living PSA may not be directly usable as a Risk Monitor PSA. The aim of the Risk Monitor is to provide an estimate of the point-in-time risk for the current plant configuration and environmental factors whereas the Living PSA provides an estimate of the average risk so that it uses average initiating event frequencies and maintenance unavailabilities, and usually takes account of the exposure time to different initiating events as the plant passes through the different Plant Operational States modelled in the PSA. Hence, the Living PSA model needs to be reviewed for any average or assumed conditions in the model to ensure that an accurate point-in-time risk is calculated for all configurations.

The software to be used for the Risk Monitor have different capabilities from that used for the Living PSA. In particular, the two software packages may handle NOT logic differently and may have different ways of handling house events that change value during event sequences. In addition, the Risk Monitor require the event tree/ fault tree model developed in the Living PSA to be replaced by a large fault tree model (referred to as a Top Logic model). The conversion from the PSA to the Risk Monitor needs to address these incompatibilities.

The Risk Monitor will be developed from the FIRE PSA model developed using RiskSpectrum® code which had been peer reviewed. The Fire PSA model and the fire analysis support data for the development of the Fire Risk Monitor were provided by the PSA team at the nuclear power plant. The Fire PSA is maintained as a Living PSA by regularly updated to reflect the current design and operation of the plant.

7.1.0. OBJECTIVE AND RESEARCH CONTENTS OF THE PROJECT

The main objective of this project is to:

- Convert the Fire PSA model to a Risk Monitor-suitable model
- Identify the main problems that may arise.
- Propose solution and solve to the extent possible,

The scope of the project is to:

- Determine whether CAFTA® (quantification software) is capable of converting RiskSpectrum® files into its own models
- Convert the model in CAFTA®.
- Validate the model in CAFTA®
- Create a new thermometer for the Fire PSA.

Project can be divided in three principal milestones:

1. Conversion of the RiskSpectrum® Fire PSA Model to a suitable CAFTA PSA model. Then determine whether the software is capable of converting RiskSpectrum® files into its own files.
2. Creation of a risk Monitor model from quantification model. Creation of a fire thermometer and mitigation events- Validate, if needed.
3. Introduction of fire related equipment into Risk Monitor.

This chapter has been arranged with the following sections: Description of the fire PSA model in RiskSpectrum ® Code; CAFTA the Risk Monitor Conversion code; Conversion of fire PSA model to CAFTA-Intended solution to conversion challenges and proposal solution; Methodology for the new conversion model-Creation of fire case fault trees and creation of fire cases internal event trees; Validation of the Conversion model in RiskSpectrum; Conversion of the conversion model to CAFTA and Conclusion.

7.2.0 Description of the Fire PSA Model

There are numerous source of fire Probabilistic Risk Assessment (PRA) methodological guidance used by the nuclear power industry. In Spain the methodology used in the United States of America has been adopted. The NUREG/CR-6850[41] and its supplemental documents provides industry consensus requirements for fire PRA used for risk informed decision-making in the USA. The NUREG/CR-6850 standard has been used around the globe for fire Probabilistic Risk Assessment (PRA) or fire Probabilistic Safety Assessment (PSA) as preferred in some jurisdictions. It has been developed in response to the increasing attention being given to PSA worldwide and is intended to facilitate the implementation of the risk based approach to fire safety assessment for both new and operating nuclear power plants

Additionally, the international Atomic Energy Agency Safety Report Series No. 10 ‘’TREATMENT OF INTERNAL FIRES IN PROBABILISTIC SAFETY ASSESSMENT FOR NUCLEAR POWER PLANTS’’ [73] documents a broad international consensus of fire PSA good practice. This Safety Report provides information on good practices in conducting probabilistic safety assessment (PSA) for fires in land based nuclear power plants. It also provide useful guide in developing fire PSA for NPP.

This fire PSA model was developed based on the fire PRA methodology described in the NUREG/CR-6850 [41]. The detailed tasks described in the methodology was followed. However, seismic fire interactions are not considered. The probability of fire induced by seismic interaction does not pose a potential fire risk.

The process can be organized into three tasks: plant boundary and partitioning, screening (qualitative and quantitative), scoping fire modeling (detailed scenario analysis) and fire risk quantification.

7.2.1 PLANT BOUNDARY AND PARTITIONING

The partitioning task begins with plant areas of potential interest to fire PSA. All plant areas associated with normal operation, emergency operation and power productions are included in the boundary definition and analysis. The intent was for the analysis boundary to encompass all areas with the potential to contribute significantly to fire risk. The analysis boundary divided and subdivided into fire compartments. Each compartment was defined such that there is high confidence that the effects of fire originating within the compartment will not significantly propagate into an adjacent compartment. All credible ignition sources within the analysis boundary are then identified, and the initial analysis to estimate fire occurrence frequency for easy ignition sources is carried out. Fire scenarios are then defined such that the collection of scenarios is then defined such that the collection of scenarios encompasses all potentially significant fire risk contributors within the analysis boundary.

Compartments in which fire would neither cause an initiating event nor degrade accident mitigation are qualitatively screened from further consideration. Fire scenarios are defined for the remaining (Unscreened) compartments, starting was a very conservative scenarios definition and successively refining the levels of modeling realism commensurate with risk significance of the compartment.

The global plant boundary are divided into plant fire areas based on the report from plant Fire Hazard Analysis (FHA). The FHA identify fire zones within the areas. The fire areas defined in the regulatory context satisfies compartments in the context of fire PRA. The fire zones are defined in the context of a fixed fire protection system. The fire zones are often delimited by taken into account the fire protection system present in each area. The fire zone is not necessary bounded by fire barriers.

7.2.2 INIATING EVENTS CAUSED BY FIRE

The analysis of a fire depends on the building and zone the fire takes placed, the type of fire, the specific origin the fire is postulated in and the internal events fire could cause. If the fire is initiated in an area that contain cooling pipes can cause Loss of Coolant Accident or in an area that contain critical cables can cause loss of off-site power. Fire initiated events identified are medium, small and very small Loss Of Coolant Accident (LOCA), loss of off-site power, turbine and reactor trip loss of condenser vacuum and Feedwater Loss.

Similarly, main Feedwater steam line Rupture inside containment, inadvertent safety injection, Loss of safeguard bar 9A and components services water Loss among other are identified.

7.2.3 IDENTIFICATION OF HAZARD SOURCES AND FIRE SOURCE CATEGORIZATION

The enhance information regarding potential fire source, the fire barrier quantification status of credited partitions and fire protection features are provided by fire protection expert.

The fire hazard analysis also provide significant information on the fire source and categorization. For the purpose of this model the fire at the plant are classified into two categories: cut and welding Fires, and others. The others are fire from Fire sources identified include diesel generator fires, electric motor fires, electrical cabinet fires, transformer fires, hydrogen tank fires and yard transformer. The ventilation system such as air conditioning units, chillers, fan motor, air filter, damper etc. can initiate fires. High voltage transformers are significant source of fire.

As part of the approach, potentially important fire scenarios are identified through a consideration of the fire hazard (ignition sources and fuel) in each of the fire areas and of the plant equipment (including electrical cables) that may be damaged by fire. The fire initiated scenarios are of particular interest involving the triggering of a plant transient (an initiating event) and the degraded response of plant systems and operators. The fire sources can be fixed such as the pumps, diesel generators, main station transformers and turbine generators, may contain combustibles liquids as fuel and for lubrication. Some of the fire sources are transient such as welding and cutting.

7.2.4 QUALITATIVE AND QUANTITATIVE SCREENING ANALYSIS

The state-of-the-art methodology for fire PSA has been developed and applied to this Spanish NPP. The methodology was based on combined multi-step qualitative and quantitative screening approach. The method applies a comprehensive database specifically developed for the application within the frame of the fire PSA

Screening analysis eliminates items from further consideration based on their negligible quantities. The fire compartments were analyzed and screen out compartments that are shown to have little or no risk significance without quantitative analysis. Through this qualitative screening fire compartment which contain no components or cables and cannot lead to a plant trip due to either plant procedure an automatic trip signal or technical specification requirements were screened out. The fire compartments that contain no safety related component or cables were screened out before quantitative screening process were done.

The quantitative screening analysis was done based on the contribution of fire compartments and scenarios to the fire risk. The approach considers the cumulative risk associated with the screened comportments.

If a screening approaches provides the results of the each compartments frequency at a particular power mode exceeding a specific threshold, a detailed analysis is carried out for estimating these frequency considering all the available information and data.

Each compartment is analyzed with respect to fire specific aspect. If the results of this analysis show that no fire impairing nuclear safety can occur under the boundary conditions of plant mode being analyzed, the compartment is excluded from further analysis for this plant mode.

The systematic analysis of the entire plant compartment are performed in two different ways: qualitative and quantitative screening. Critical fire component can be identified within the frame of qualitative or a quantitative process. The qualitative screening allows the determination of critical fire compartments based on and applying appropriate selection criteria.

In the frame of quantitative screening by frequency, critical fine compartments are identified by means of a simple event free analysis based on the detailed knowledge of the plant specific situation.

7.2.5 HAZARD OCCURRENCE FREQUENCY SCENARIOS-PLANT SPECIFICATION FIRE EVENT

The analysis model is based on the assumptions that fire frequencies remain constant over time and the total ignition frequency is the same equipment for the same equipment type, regardless of the differences in quantity and characteristics off the equipment. Similarly, the likelihood of fire ignition is same across an equipment type. For example, pumps are assumed to have the same fire ignition frequency regardless of the size, usage level, and the working environment.

The fire frequency associated with a compartment is quantified. Compartment level frequency is calculated from the sum of all frequencies $\lambda_{IS,\,J}$ associated with the ignition sources present in the compartment. The ignition source frequencies $\lambda_{IS,\,J}$ are estimated from the following equation:

$$\lambda_{IS,J} = \lambda_{IS} W_L W_{IS,J,L} \qquad 7.1$$

Where:

$\lambda_{IS,J}$ = Plant-level fire frequency associated with ignition source IS

W_L = Location weighting factor associated with the ignition source

$W_{IS,J,L}$ = Ignition source weighting factor reflecting the quantity of the ignition source type present in compartment J of location L.

Based on the data and methodology presented in NUREG/CR-6850[41] of Spanish NPP the fire frequency $\lambda_{IS,J}$, for electrical cabinet and the cabinet and the potential transient fire sources are estimated to be 7.20 E-05/year and 4.80E-04/year respectively

An estimation of fine occurrence frequency for each ignition source is developed for all credible ignition sources. Fire ignition source including electrical cabinet, pumps, transformers and cutting and welding can occur at various plant locations due to maintenance activities. For the purpose of this model fire sources has been grouped into cutting and welding and others.

7.3.0 DETAILED DESCRIPTION OF THE MODEL

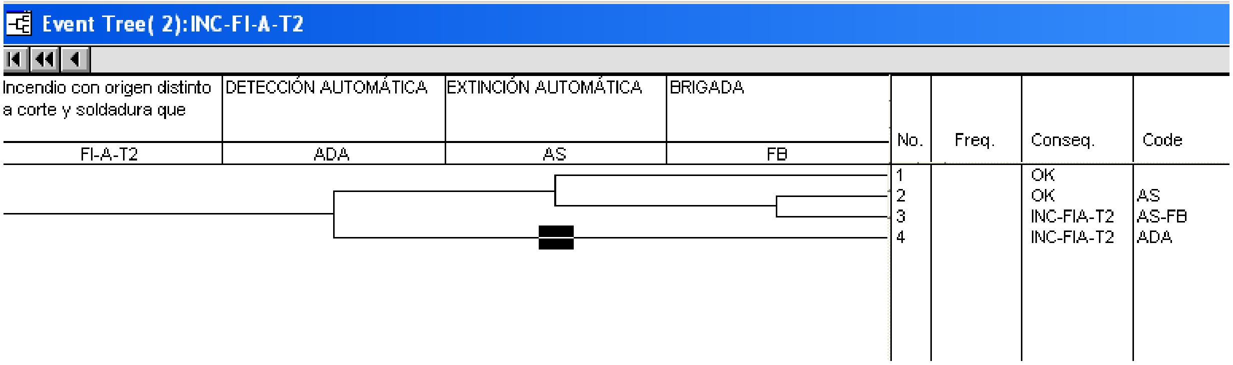
All potential significant fire scenarios risk contribution within the analysis boundary is defined. The compartments in which fire would neither cause an initiating event nor degrade accident mitigation are qualitatively screened from further consideration. Fire scenarios are defined for the unscreened compartment, commencing with very conservative scenarios definition and consecutively, referring the levels of modeling realism commensurate with risk significance of the component. All ignition sources within the compartment are conservatively assumed to fail all targets in the compartment with no credit given to suppression.

A fire progression event tree is utilized iteratively for the fire scenario definition. The fire progression event tree is used to model the entire fire progression including the growing set target failure that occurs as a function of time. It includes probabilistic modeling of the progression and the suppression. The degree of detailed of the fire progression event tree depends on the risk significant of the fire scenarios. High risk scenarios uses a less resolute fire progress event tree.

7.3,1 FIRE SCENARIOS TREES

The detailed fire modeling involves analysis of fire growth and propagation, equipment damage, fire detection and fire suppression. The methodology takes into account the interactions among prompt direction, prompt suppression and fire brigade response

The fire PSA is modeled using fire detection and suppression Event trees which introduces the probability of the suppressing a fire before it causes an internal event or core damage. The initiating events of these trees are either cut and welding fires or other fires. The sequential Headers are prompt detection, automatic suppression and fire brigade. A typical fire event tree is shown in the figure 7.1 (a) and Figure 7.1 (b) for other fires, and cut and welding respectively. The consequence of the event tree can be okay, where the initiated fire does not cause any risk and extinguished. Or the consequence could also initiate other internal event leading to core damage indirectly or directly.



Event Tree(2):INC-FI-A-T2

Incendio con origen distinto a corte y soldadura que	DETECCIÓN AUTOMÁTICA	EXTINCIÓN AUTOMÁTICA	BRIGADA
FI-A-T2	ADA	AS	FB

No.	Freq.	Conseq.	Code
1		OK	
2		OK	AS
3		INC-FIA-T2	AS-FB
4		INC-FIA-T2	ADA

Figure 7.1 (a) Event tree for a typical fires other than cut and welding

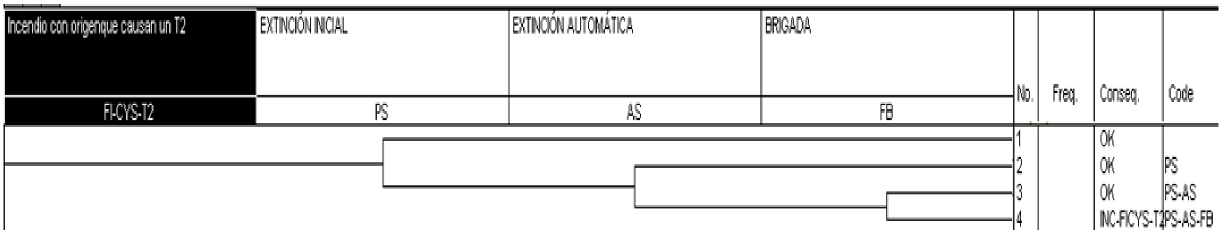


Figure 7.1 (b) Event tree for typical fire from cut and welding

The FIRE PSA Fire detection and suppression Event Trees which introduce the chance of suppressing a fire before it causes an Internal Event or CD. Usually each detection and suppression Event Tree is related to an Internal Event. The negative consequence(s) of these Trees is the no suppression of the fire and, thus, the occurrence of the Internal Event. The accident sequences of the Internal Events are delineated in other Event Trees who's Initiating Events are linked to the Consequences of the detection and suppression Trees (Fig 6.2). The fire Event Trees delineate the possibility of non-suppression of a fire before it causes core damage or triggers an internal event.

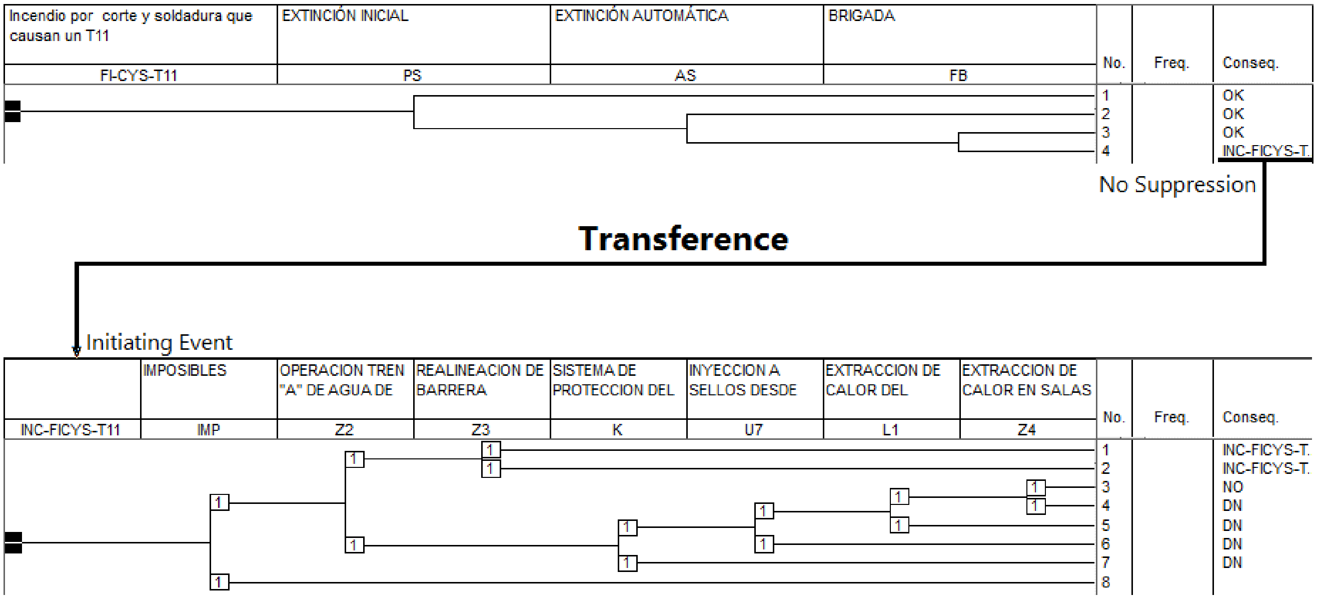


Figure 7.2: The Fire accident event tree linked to an internal event tree to trigger core damage.

7.3.2 INTERNAL EVENT/FAULT TREES

The internal event PSA model is a logical model in terms of event and fault trees. The model is a combination of the initiating events as compared to external event such as tornados and seismic events, component failures and human failures event that leads to core damage. The component failures are of causes internal to the component themselves and not from external cause.

The internal event PSA logic model combines both event tree and fault trees for component failures linked. The fault trees were built using logic gates, basic events and house events. The fault tree is subdivided between several fault tree pages which are bound together using transfer gates. The basic event is an event for which there is no further fault tree structure developed. Each basic event bears a unique ID making it possible to use the basic event in several fault tree branches.

The gate is an event in fault tree with logical operator in its definition and bears a unique ID. The dominant gate used are the AND-gate, OR-gate, NAND-gate, NOR-gate etc. In the AND-gate the output from the gate is TRUE if all the inputs to the gate are TRUE, whilst in the OR-gate the output from the gate is TRUE if at least one input form the gate is TRUE. In the NAND-gate (NOT AND) the output from the gate is TRUE if at least one input to the gate is FALSE, whilst in the NOR-gate (NOT OR) the output from the gate is TRUE if all the inputs to the gate are FALSE.

A link to a gate in another part of the fault tree is referred to as transfer gate. A logical switch referred to as house event are used to switch ON or OFF branches in the fault tree and thereby getting different versions of the fault tree without changing it explicitly. The house event is a special type of basic event. Its status is not in terms for the house event itself, unless it is set using a state value. The status of the house event is set in the boundary condition sets defined for the analysis.

Exchange events are used to replace one basic events or a whole fault free branch using top gate. The exchange is activated by a house event set to TRUE or FALSE in a boundary condition set.

A boundary condition set is a powerful mechanism for changing the logic in the fault trees and event trees as well as component reliabilities for analyses of special conditions. A number of boundary conditions are set to be applied where running the analysis to avoid having to change the model explicitly.

The boundary condition set (BCSet) are used to absolutely specify TRUE OR FALSE logical values for house events, basic events or gates. A BCSet can also include other BCSets. The BCSets are activated in an analysis case, an initiating events or for a function event.

The analysis case BCSet are boundary conditions specified and that are applied in analysis case you are running. The BCSets are declared in the initiating events and the boundary conditions are applied in events trees that use the initiating event. Function events are used to declare one BCSet for each input. The conditions in the BCSet are applied in all downstream branches from the function events in the events trees where the function events are used. BCSet are used in modeling of a component differently under different conditions or switch ‘ON’ or ‘OFF’ some branches in the fault tree structure and there by obtain different version of the same fault tree without changing it explicitly. BCSets are created for the analysis cases so that each case can be analyzed independently. Of specific interest are fire initiated scenarios involving the triggering of a plant transient and the degraded response of the plant systems and operators. The fire cases frequencies are quantified by estimating the frequency of fire initiation, the conditional probability of fire-induced damage to critical equipment given the fire, and the conditional probability of core damage given the specified equipment damage

7.4.0 FIRE PSA QUANTIFICATION

Potentially important fire scenarios are identified as part of the approach through a consideration of fire ignition sources and fuels in each plant areas and of the plant equipment that may be damaged by a fire.

The method of quantifying the fire-induced core damage frequency is expressed by the following equation: [45]

$$CDF = \sum_i \lambda_i \sum_j P_{ed,j/i} \sum_k P_{CD,k/i,j} \qquad 7.2$$

Where λ_i is the frequency of the fire scenario I

$P_{ed,j/i}$ Is the conditional probability of damage to critical equipment set j given the occurrence of fire scenario *I*

$P_{CD,k/i,j}$ Is the conditional probability of core damage due to plant response scenario k given fire scenario I and damage to critical equipment set j

The first term quantifies the first layer of defense-in-depth (prevent fires from being ignited). The second term addresses the issues of fire growth, detection, suppression and component damageability and thus quantifies the second and third layers of defense in depth (detect and extinguish any occurring fires rapidly to limit damage and prevent spreading of those fires that have not been extinguished to minimize potential fire effects on key plant systems and functions). The third term addresses the unavailability of equipment unaffected by the fire and /or operator failures.

The final fire risk result are obtained by quantifying the final fire PSA model. The final core damage frequency (CDF) are quantified for each fire scenario. The fire scenarios screened out are not added into the calculated total plant fire related CDF. The total plant CDF are estimated by swimming all the CDF for the unscreened fire scenarios/cases. The fire scenario frequencies are used to quantify CDF for each fire ignition event. The fire scenario frequencies are combined with the appreciate Conditional Core Damage Probability (CCDP) value to quantity the CDFs

384 fire scenarios/cases have been identified and the CDF's of these cases referred to as consequence analysis case (CAC) are evaluated

7.4.1 QUANTIFICATION OF CDF AND RESULTS

The fire PSA model was designed using RiskSpectrum ® PSA code. The model contains all the parameters of Internal Event PSA, internal event trees, fault trees, headers and basic events. The successful screening process ensured that only those fire scenarios with potential to cause either an internal Event or core damage are introduced into the analysis. The initiating events of the fire

PSA are however diverse fire scenarios. From the operational experiences two categories are identified in this case: cut and welding fires and others.

After partitioning and fire zoning, qualitative and quantitative screening analysis as described in subsection 4.1 and 4.4 respectively, 384 areas are identified. In these areas fire can be initiated and affect safety cables and equipment. The fire cases/ scenarios in these areas are referred to as consequence analysis cases. The consequence analysis cases are grouped into fire zones for analysis.

The fire PSA adapt this division and introduce into the risk analysis the concept of zones and buildings. The fire accident progression, and the consequences of the fire depends on the origin and the type of fire. Thus, fire originating from control building, where control and protection cables could be affected is not the same effect as fire in the Auxiliary Building.

Therefore, the analysis of the fire rest on the following variables: building and the zone where the fire take place, the specific origin (inside the zone) of the fire, the type of fire, and the internal Events the fire could cause.

The fire PSA model included a consequence analysis case for each of the combination of the variables stated above, provided it is plausible going through the screening analysis. Each consequence analysis case is associated with a Boundary Condition Set (BC Set). Each BC Set imposes the plant conditions of specific case and activates a House event. The House event is mainly linked with the headers of the detection and suppression Events trees associated with each case.

The quantification of zones' CDF is carried out by MCS Analysis Cases. An MCS Analysis Case obtains an MCS Boolean equation by means of adding the Boolean equations of different Consequence Analysis Cases. All the Consequence Analysis Cases associated to a zone are merged in the MCS Analysis Cases of the FIRE PSA. There is an MCS Analysis Case per fire zone. The total Core Damage Frequency caused by Fire initiators is the sum of the Fire CDFs of the zones.

The FIRE PSA Model provided by the NPP contains 384 Consequence Analysis Cases which represent all the possible fire cases Plant could suffer (thus, only the ones that have gone through the screening analysis). The plant is divided in 6 buildings and 41 zones. The FIRE PSA Model consequently contains 41 MCS Analysis Cases. The buildings taken into account in the analysis are: Auxiliary systems building, turbine, containment, electric penetrations, Auxiliary Feedwater, and Control. The results in terms of CDF provided by the FIRE PSA model [87, 91] is shown in Table 7.1 below.

Table 7.1. The results in terms of CDF provided by the FIRE PSA model [93, 98]

BUILDING	CDF(y^{-1})
Auxiliary	1.60E-06
Turbine	3.16E-08

Containment	1.88E-06
Electric Penetrations	6.18E-07
Auxiliary FeedWater	7.36E-07
Control	4.97E-08
TOTAL	9.83E-06

In the Fire PSA model 384 consequence analysis cases (CAC) of Fire Events trigger internal Events which results in 384 core damage frequency (CDF). A single CDF is evaluated using a formula outside the RiskSpectrum quantification software. However, in the conversion model single CDF is required by the quantification software CAFTA for the determination of the risk level in the Risk Monitor software.

7.5.0 CONVERSION OF FIRE PSA MODEL TO CAFTA

Computer Aided Fault Tree Analysis (CAFTA) System Version 5.3 is a computer program for developing reliability models of large complex systems, using fault tree and event tree methodology. CAFTA is a trademark of the Electric Power Research Institute, Inc. and is designed to meet the many needs of reliability analysts while performing fault tree/event tree analysis on a system or group of systems. It includes:

- Fault Tree Editor for building, updating and printing fault tree models
- Event Tree Editor for building, updating and printing event tree models
- Reliability Database for storing the basic event, failure rate and gate information used in the models.
- Cutset Editor which is a valuable tool for reviewing and analyzing cutset results
- Evaluating processors to generate cutsets and to calculate individual gate probabilities

If a file format is recognized by CAFTA then that file is displayed under the correct file folder in the Project Window. For example, fault tree files which end in a .CAF file extension are placed under the Fault Tree folder and event tree files which end in an .ETA file extension are placed under the Event Tree folder. Typically, a Reliability Database is used for a single project but other databases can also be included and utilized within a single project. Some research work has been carried out using CAFTA for analysis in Spain [99].

The nuclear regulatory commission of Spain (CSN) had developed a computer tool to convert CAFTA models into the variant of the OPSA-MEF format [99]. RiskSpectrum model unlike CAFTA can be converted directly to OPSA-MEF format. The challenge is that no attempt has been made to convert RiskSpectrum model to CAFTA and vice versa. There has been effort to standardized PSA codes so that cross platform analysis and verification can be achievable in the foreseeable future. The CAFTA software has specific tool to convert files from RiskSpectrum but yet to convert a full large model.

One of the motivation of this work is that should the conversion from RiskSpectrum to CAFTA fail, it becomes one of the starting points to achieve that goal in the future. Nevertheless, the conversion from CAFTA to RiskSpectrum via OPSA-MEF have been achieved. The reverse process from RiskSpectrum to OPSA-MEF is possible. But conversion from OPSA-MEF to CAFTA has not been possible.

The problems are usually caused by different behavior of the modelling features in RiskSpectrum and CAFTA. Among these, the following must be highlighted.

∗ Distributions of basic events parameters. Distribution parameters are different in RiskSpectrum and CAFTA, so special care must be taken in the conversion process.

∗The format of the post processing rules is not the same in both codes. Not all the rules allowed by CAFTA's Qrecover program have been translated. Only the most common, significant rules have been translated.

∗ Boundary conditions do not work in the same way in CAFTA and RiskSpectrum. In CAFTA, BCs can be defined as follows:

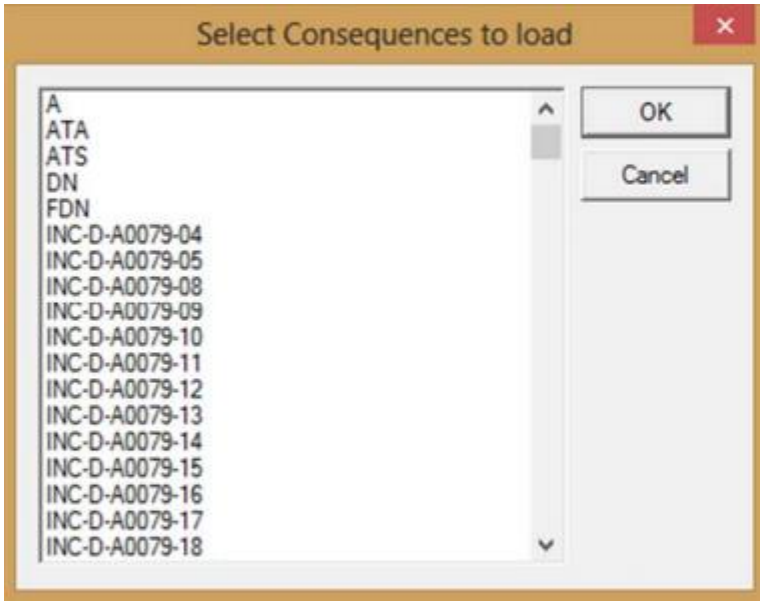
• At model level

• At sequence level. These BCs over write the model level BCs.

•At header level. Usually BCs defined in one header are applied also to the following header, although this behavior can be changed through user defined options in the PRAQuant file. Header level BCs overwrite the two previous types of BCs.

The major difference at sequence (or analysis) level is that BC sets are applied after obtaining the Boolean equation desired. At header level: BC Sets are applied when obtaining the Boolean equation. Besides, in RiskSpectrum those BCSets that must be applied throughout the whole Event Tree are introduced in the Initiating Event. The BCSets only apply to the header where they are allocated in for the rest of headers.

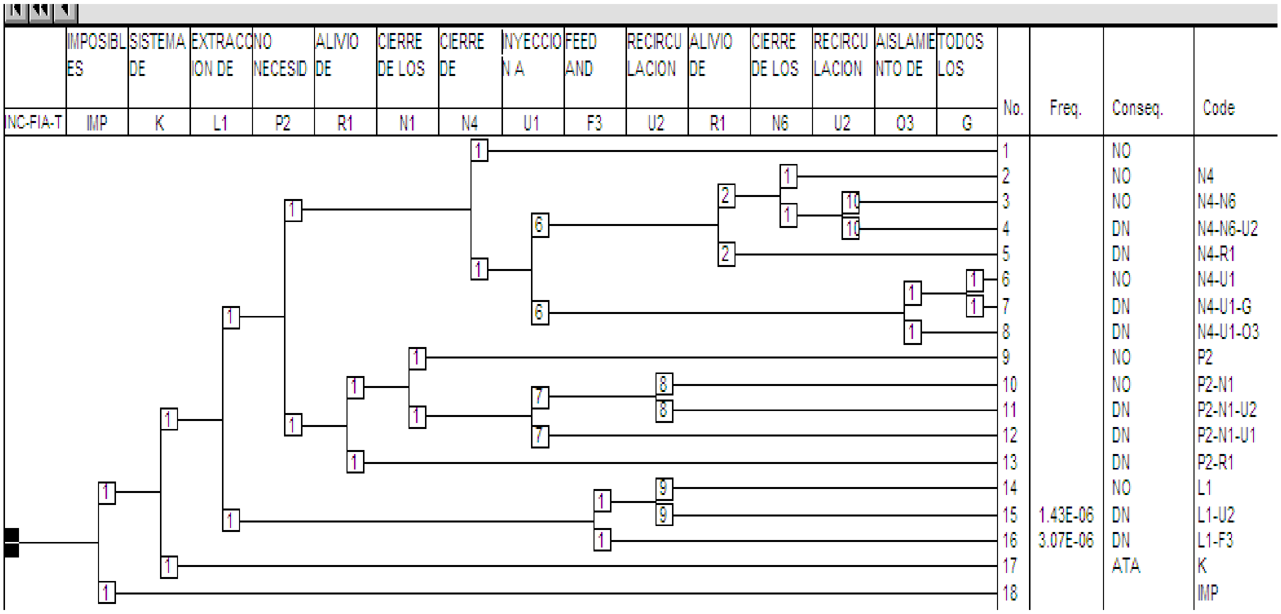
The first attempt is to convert the RiskSpectrum® Fire PSA model in CAFTA. In the process CAFTA code requested the selection of consequence (s) or sequence (s) to be included in the conversion model as shown in figure 7.3. In this case ´FDN´ (CDF- Core Damage Frequency) internal consequence can be selected directly, as it is seen in figure 7.3. However, in the case of Fire PSA the first issue is how to select as many as 384 consequences representing the fire cases assessed to obtain a single CDF. More so, the model to be obtained will still be problematic even when it is possible to load the 384 consequences, for the risk monitor requires a single CDF value, not 384 CDF. Nevertheless, the selection of 384 consequence cases result in a crash of CAFTA software.



A
ATA
ATS
DN
FDN
INC-D-A0079-04
INC-D-A0079-05
INC-D-A0079-08
INC-D-A0079-09
INC-D-A0079-10
INC-D-A0079-11
INC-D-A0079-12
INC-D-A0079-13
INC-D-A0079-14
INC-D-A0079-15
INC-D-A0079-16
INC-D-A0079-17
INC-D-A0079-18

Figure 7.3: Consequences input screen of CAFTA

In view of the fact that we cannot actually assess the potential conversion of the RiskSpectrum Fire PSA due to the challenge of crashing of the CAFTA software after selecting 384 consequences cases. One consequence analysis case, for example, INC-D- A0079-08, is selected to evaluate the potential conversion from RiskSpectrum® to CAFTA. It is observed that, for the example in question, there are nine (9) sequences of CD (Core Damage) for Internal Event tree of the fire PSA in RiskSpectrum® that lead to Core damage as indicated in figure 7.4, but conversion in CAFTA shows five (5) sequences leading to CD as shown in Figure 7.5



No.	Freq.	Conseq.	Code
1		NO	
2		NO	N4
3		NO	N4-N6
4		DN	N4-N6-U2
5		DN	N4-R1
6		NO	N4-U1
7		DN	N4-U1-G
8		DN	N4-U1-O3
9		NO	P2
10		NO	P2-N1
11		DN	P2-N1-U2
12		DN	P2-N1-U1
13		DN	P2-R1
14		NO	L1
15	1.43E-06	DN	L1-U2
16	3.07E-06	DN	L1-F3
17		ATA	K
18			IMP

Figure 7.4: Internal Event tree in RiskSpectrum ® showing sequences of events that leads to CD

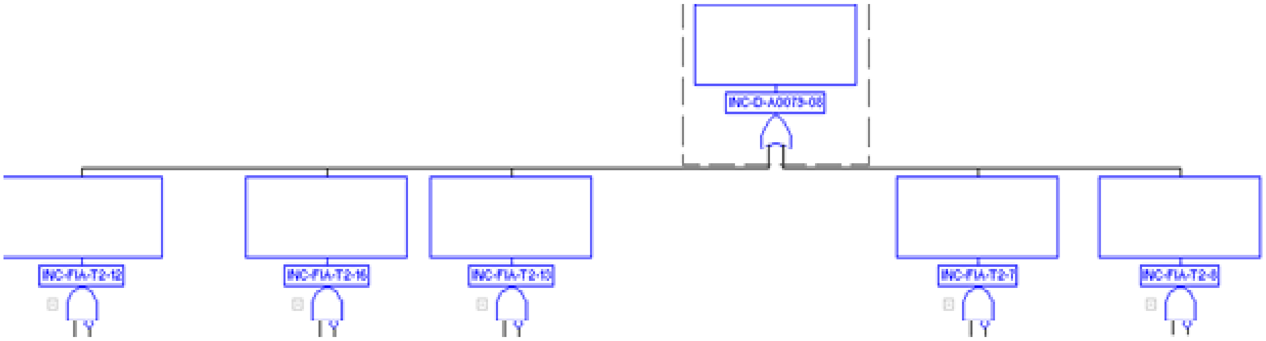


Figure 7.5. The sequences of internal Event tree for INC-D-A0079-08 selected by CAFTA after conversion

When another Fire case for example INC-D-A0079-04, but with the similar internal event tree as the previous one shown in Figure 7.5, is selected to convert in CAFTA, it is observed that CAFTA randomly selected eight (8) out of nine (9) of the sequence that leads to CD as shown in Figure 7.6 below.

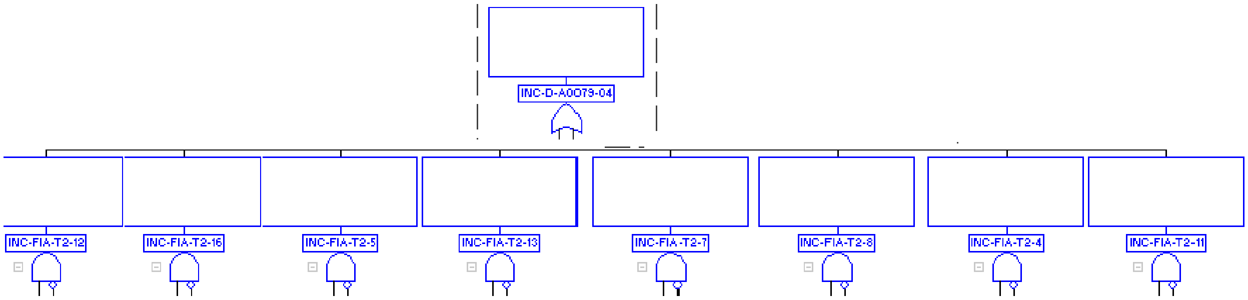


Figure 7.6. The sequences of internal Event tree for INC-D-A0079-04 selected by CAFTA after conversion

Also, some of the headers leading to CD were randomly selected as shown in figure 7.7 below. The headers that lead to CD for sequence No 12 as indicated in figure 7.4 are INC-F1A-T2, P2, N1 and U1. But from Figure 7.7, the headers which are the input of the AND-gate had U1 missing out in the conversion in CAFTA.

It is observed that CAFTA is unable to show a Fault Tree Sequential structure of the internal Event tree in the Fire PSA. Conversion presents several flaws:

- Some of the accident sequences carrying core damage are not integrated in the CAFTA model. That is, information is lost in the conversion.

- The initiating event of the internal Events Tree is not well integrated. In the RiskSpectrum® model the consequences of some event trees are the initiating events of other event trees. In the conversion CAFTA does not include all sequences that lead to a result which causes the triggering of the initiating internal event. It seems that the software chooses one of the sequences randomly. Furthermore, the Fault Tree providing frequency of the fire (the fault tree equivalence of the fire scenarios event tree described in fig 7.1(a) & (b)) is not transferred to CAFTA conversion model under any circumstances.

In brief, none of sequence of the fire scenarios tree was converted and the conversion fails to implement neither all of the sequences leading to core damage nor the Fault Tree (equivalent of the fire case event trees) selection of the frequency of fire.

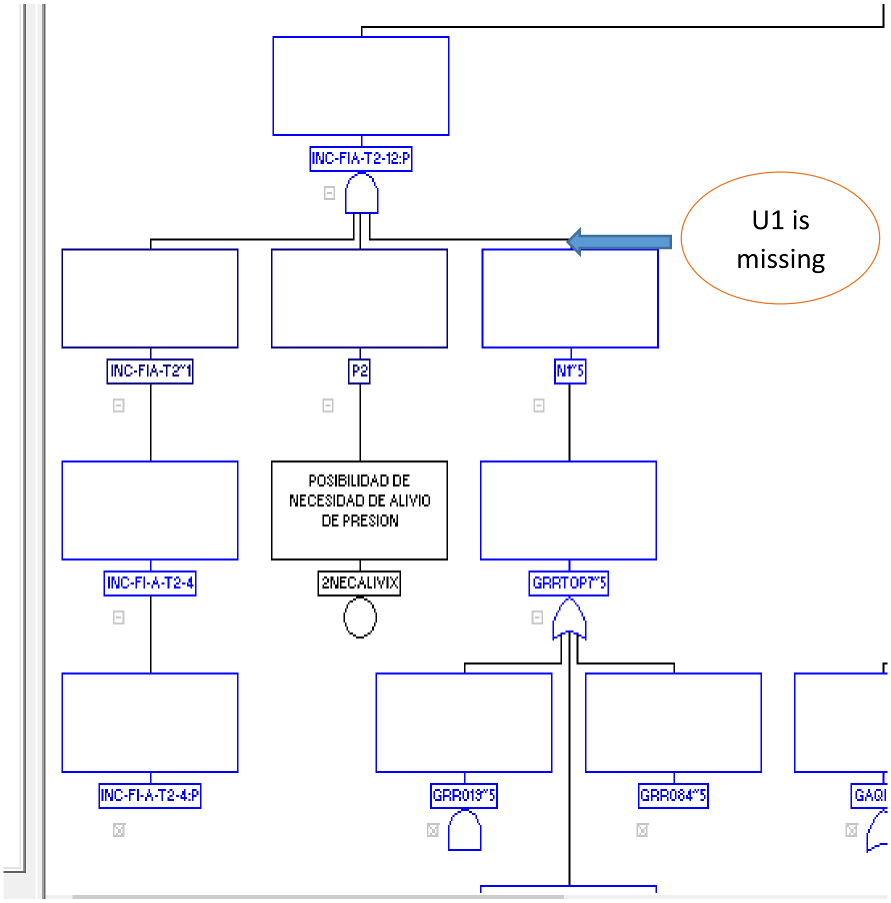


Figure 7.7: Example of consequence fire case INC-D-A0079-08 translated by CAFTA

7.5.1. INTENDED SOLUTION TO THE CONVERSION CHALLENGES

The conversion of event trees in the current Fire PSA model in CAFTA results in loss of information. The accident sequences are not well integrated and arbitrary selection of sequences need to be address. Besides, the treatment of Fire PSA by Risk Monitor would be complicated since the Fire PSA provides 384 CDF values instead of a unique CDF value. Any proposed solution to change the original Fire PSA model in order for it to be convertible with CAFTA and adapt it to the Risk Monitor must take into account the following characteristics:

- It must be capable of delivering a unique result without any friction between the different cases of fire.

- It should facilitate the integration of all accident sequences leading to core damage to prevent loss of information.

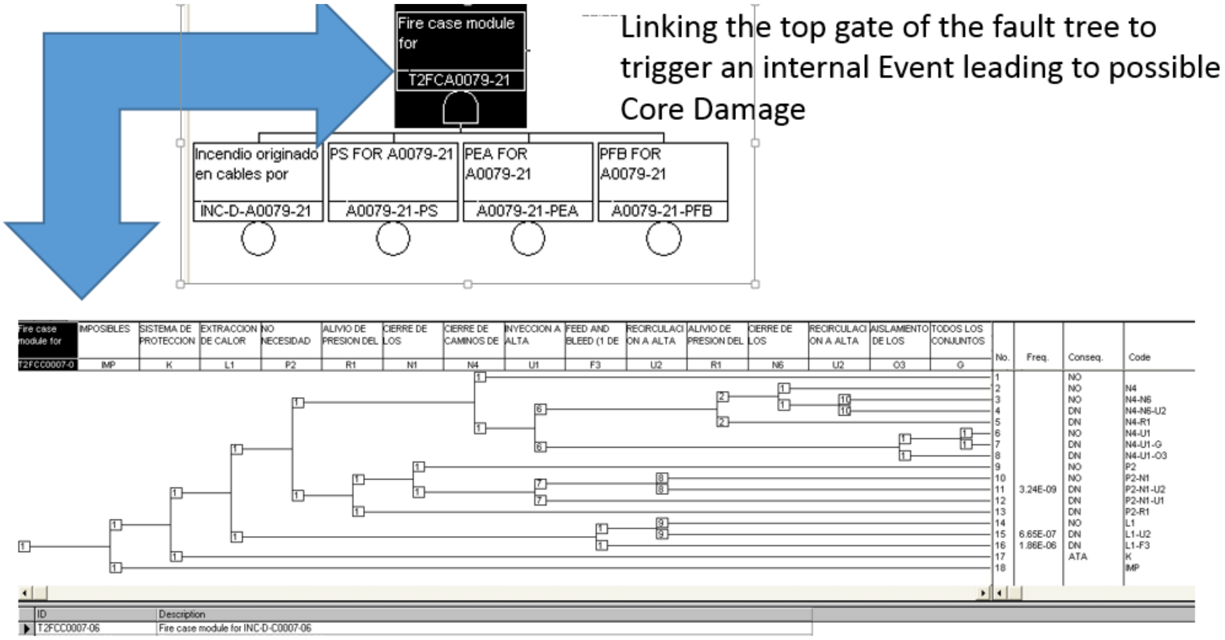
- It should facilitate the integration of fire frequencies as initiating Event frequency in the internal event trees in translating the conversion.

7.5.2. PROPOSAL

The proposal is based on the modification of the base Fire PSA model (referred to as reference model) in RiskSpectrum® for it to be suitable for Risk Monitor purposes and for it to be converted to CAFTA (see features above). The proposal is characterized by two important features:

- Replacement of detection and fire suppression Event Trees, by detection and fire extinction Fault trees. As many as 384 Fault Trees created should have equivalent internal event Trees to be linked with as initiating events. For each fire case fault tree, the basic events (prompt suppression/automatic fire detection (PS/PDA), automatic fire suppression (PEA) and fire brigade (PFB)) are introduced. The target of Fault Trees is to easily enter each fire case specific probabilities without the need for Exchange Events. Furthermore, these fault trees are perfectly suited to the change in philosophy of evaluating a single value Core Damage Frequency (CDF). An illustration as shown in figure 7.8 show that the top gate of the fault tree is linked to the corresponding internal event tree of the analyzed case.

- Change the orientation of the consequences so that one unique result can be quantified. The proposal is to introduce the alignment of the consequences so that a unique result of core damage associated with internal event trees, which in turn are related to the different fire cases (384) analyzed in the PSA, can be quantified. This implies having to create as many internal Event trees as cases. The Top gate of the Fault Trees would be linked to the initiating events of the internal Event trees, becoming the initiating event of the internal event sequences.



Linking the top gate of the fault tree to trigger an internal Event leading to possible Core Damage

No.	Freq.	Conseq.	Code
1		NO	
2		NO	N4
3		NO	N4-N6
4		DN	N4-N6-U2
5		DN	N4-R1
6		NO	N4-U1
7		DN	N4-U1-G
8		DN	N4-U1-O3
9		NO	P2
10		NO	P2-N1
11	3.24E-09	DN	P2-N1-U2
12		DN	P2-N1-U1
13		DN	P2-R1
14		NO	L1
15	6.65E-07	DN	L1-U2
16	1.86E-06	DN	L1-F3
17		ATA	K
18			IMP

ID	Description
T2FCC0007-06	Fire case module for INC-D-C0007-06

Figure 7.8: Linking the top gate of the fire initiation, detection and suppression fault tree to trigger an internal event tree.

The model resulting from these changes would be appropriate for a Risk Monitor. Once the changes are implemented all the specific fire cases could be validated in the reference model. Modified model results would be validated with the reference model to verify the appropriateness of the new modeling.

7.6.0 METHODOLOGY

The development of a new alternative quantification method for a fire PSA in RiskSpectrum is achieved by changing the orientation of the consequences as a unique result of CDF associated with Events trees of internal events is presented. The procedure is described as follows: the creation of database, enter the fire basic events in RiskSpectrum, development of fire fault trees in RiskSpectrum, create analysis case event trees for the internal events and linked the fire fault tree and the analysis case internal event trees. A database is created for all the 384 fire analysis cases in Microsoft Excel® to ensure that all cases are appropriately entered in RiskSpectrum. The database contains list of all the fire cases and their identification codes for the reference Fire PSA model. A corresponding list of new identification code for the fire basic events: Prompt Suppression PS; Automatic fire detection PDA; Automatic fire suppression PEA; and fire Brigade PFB; for all the fire consequence analysis cases. It also contain a list of updated probabilities for the basic events. This database serves as quality control measure. All the Fire case basic events are entered in RiskSpectrum and re-checked with the database in Excel. Creation of fault trees from the Fire event trees for all the 384 CAC is followed. The next stage is the creation of Event trees for the internal events using Microsoft Access Query 2007® utilizing access database of RiskSpectrum. The top gate of the fault tree is linked to the corresponding internal event tree as the initiating event of the internal event trees to trigger an internal event. One fire consequence analysis Case (CAC) with as many Internal Event trees as fire cases assessed is created. Summary of the procedure is shown in the flow chart in figure 7.9 and detailed description in the sections 7.6.1, 7.6.2, 7.6.3, and 7.6.4.

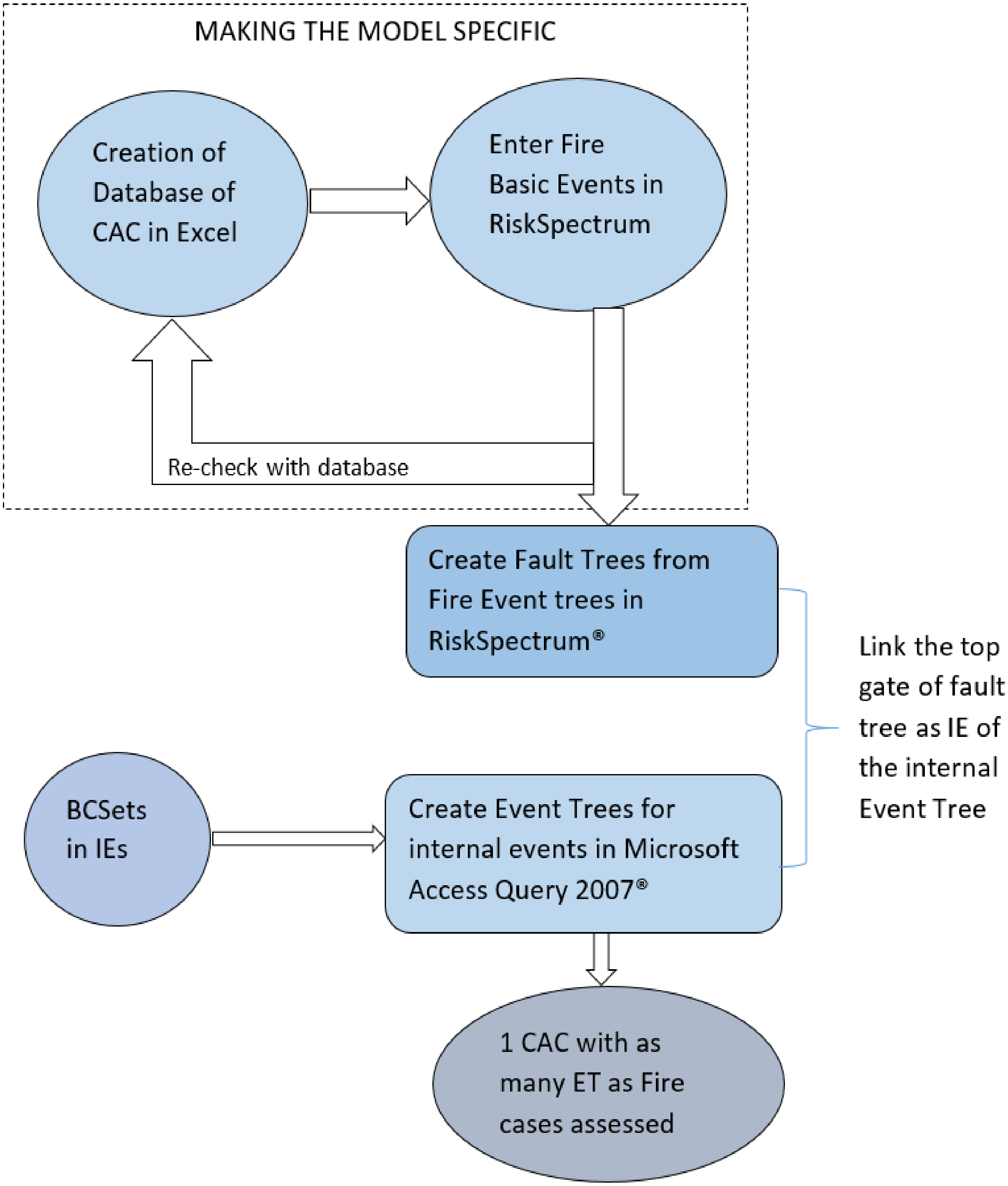

MAKING THE MODEL SPECIFIC
Creation of Database of CAC in Excel
Enter Fire Basic Events in RiskSpectrum
Re-check with database
Create Fault Trees from Fire Event trees in RiskSpectrum®
Link the top gate of fault tree as IE of the internal Event Tree
BCSets in IEs
Create Event Trees for internal events in Microsoft Access Query 2007®
1 CAC with as many ET as Fire cases assessed

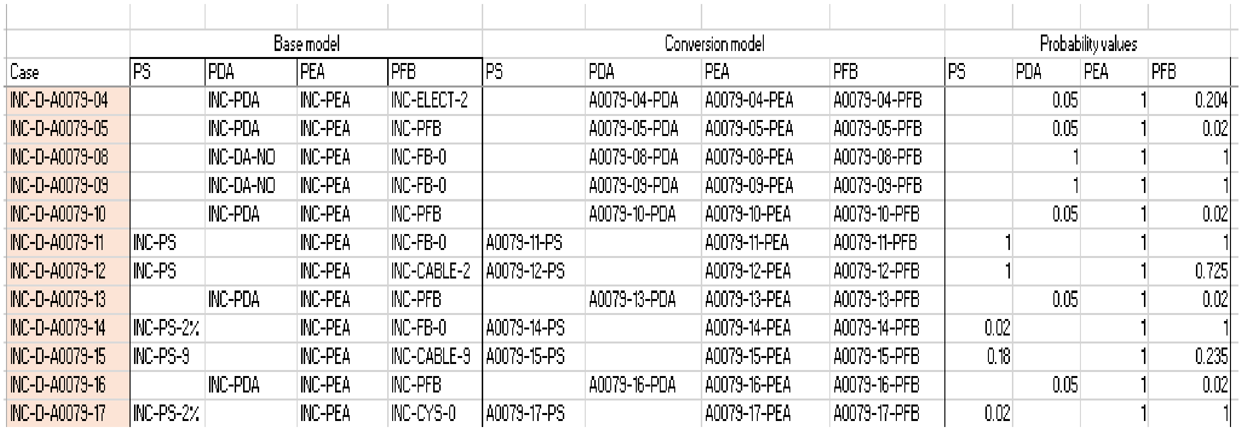
Figure 7.9: The flow chart of the method of the proposed solution

7.6.1 CREATION OF DATABASE

A database to relate reference model FPS basic events to conversion model FPS basic events was created in Microsoft excel ®. The database includes the specific basic events used in the reference model and the new basic events of the conversion model per fire analysis case. The purpose of the database is to ensure that all data related to the fire protection system basic events are entered appropriately and serves as quality control measure.

The first column of figure 7.10 indicate the fire CAC ID and the base model columns represents the corresponding basic events IDs in the reference. The conversion model columns represents the equivalent basic Events IDs and the probability values columns shows the corresponding basic events probabilities. The conversion model column consist of independent IDs for the basic events for each fire analysis case and along the row is the IDs for each fire basic event. The probability values column is a list of updated probabilities of each basic event per fire analysis case.

The probabilities or failure rates are the same, but changing the IDs to have one basic event per FPS. There are IDs PS/PDA, PEA, and PFB for the Basic Events for each Consequence Analysis Case in the reference model representing prompt suppression/automatic fire detection, automatic fire suppression and fire brigade respectively. These codes are added as suffix to the IDs of the reference fire cases to represent the IDs for the Basic Events in the conversion model. For example, the Fire Protection System (FPS) INC-D-A0079-04 with basic event codes, PDA, PEA and PFB, becomes A0079-04-PDA, A0079-04-PEA, and A0079-04-PFB respectively as the new basic events for aforementioned case, as shown in the figure 7.10 below.



	Base model				Conversion model				Probability values			
Case	PS	PDA	PEA	PFB	PS	PDA	PEA	PFB	PS	PDA	PEA	PFB
INC-D-A0079-04		INC-PDA	INC-PEA	INC-ELECT-2		A0079-04-PDA	A0079-04-PEA	A0079-04-PFB		0.05	1	0.204
INC-D-A0079-05		INC-PDA	INC-PEA	INC-PFB		A0079-05-PDA	A0079-05-PEA	A0079-05-PFB		0.05	1	0.02
INC-D-A0079-08		INC-DA-NO	INC-PEA	INC-FB-0		A0079-08-PDA	A0079-08-PEA	A0079-08-PFB		1	1	1
INC-D-A0079-09		INC-DA-NO	INC-PEA	INC-FB-0		A0079-09-PDA	A0079-09-PEA	A0079-09-PFB		1	1	1
INC-D-A0079-10		INC-PDA	INC-PEA	INC-PFB		A0079-10-PDA	A0079-10-PEA	A0079-10-PFB		0.05	1	0.02
INC-D-A0079-11	INC-PS		INC-PEA	INC-FB-0	A0079-11-PS		A0079-11-PEA	A0079-11-PFB	1		1	1
INC-D-A0079-12	INC-PS		INC-PEA	INC-CABLE-2	A0079-12-PS		A0079-12-PEA	A0079-12-PFB	1		1	0.725
INC-D-A0079-13		INC-PDA	INC-PEA	INC-PFB		A0079-13-PDA	A0079-13-PEA	A0079-13-PFB		0.05	1	0.02
INC-D-A0079-14	INC-PS-2%		INC-PEA	INC-FB-0	A0079-14-PS		A0079-14-PEA	A0079-14-PFB	0.02		1	1
INC-D-A0079-15	INC-PS-9		INC-PEA	INC-CABLE-9	A0079-15-PS		A0079-15-PEA	A0079-15-PFB	0.18		1	0.235
INC-D-A0079-16		INC-PDA	INC-PEA	INC-PFB		A0079-16-PDA	A0079-16-PEA	A0079-16-PFB		0.05	1	0.02
INC-D-A0079-17	INC-PS-2%		INC-PEA	INC-CYS-0	A0079-17-PS		A0079-17-PEA	A0079-17-PFB	0.02		1	1

Figure 7.10: A Typical Data base table showing the fire case in reference model and the conversion model

.

7.6.2 CREATION OF FIRE CASE FAULT TREES

The new basic Events are introduced into the RiskSpectrum fire PSA model. The data entered is re-checked with the excel data base to ensure all data entered are correct as a quality control measure. These new basic Events are used in the creation of the fault trees for all the fire CAC. Instead of sequential treatment of the fire events in the event tree, the failure sequence are described in the new fire fault trees. The success sequence paths are not treated in the fault tree because their consequences are not needed for this analysis.

Fire suppression event trees for fires with origin other than cutting and welding activities are converted to fault tree as shown in the example in figure 7.11. Similarly, fire suppression event trees for fires originating from welding and cutting activities are converted to fault Trees as shown in the example in Figure 7.12

The quantification of non-suppression frequency of the new fault tree and the Event tree from which it is created shows that same results are obtained. This convincingly shows that the fault tree created is equivalent to the Event Tree from which it was converted.

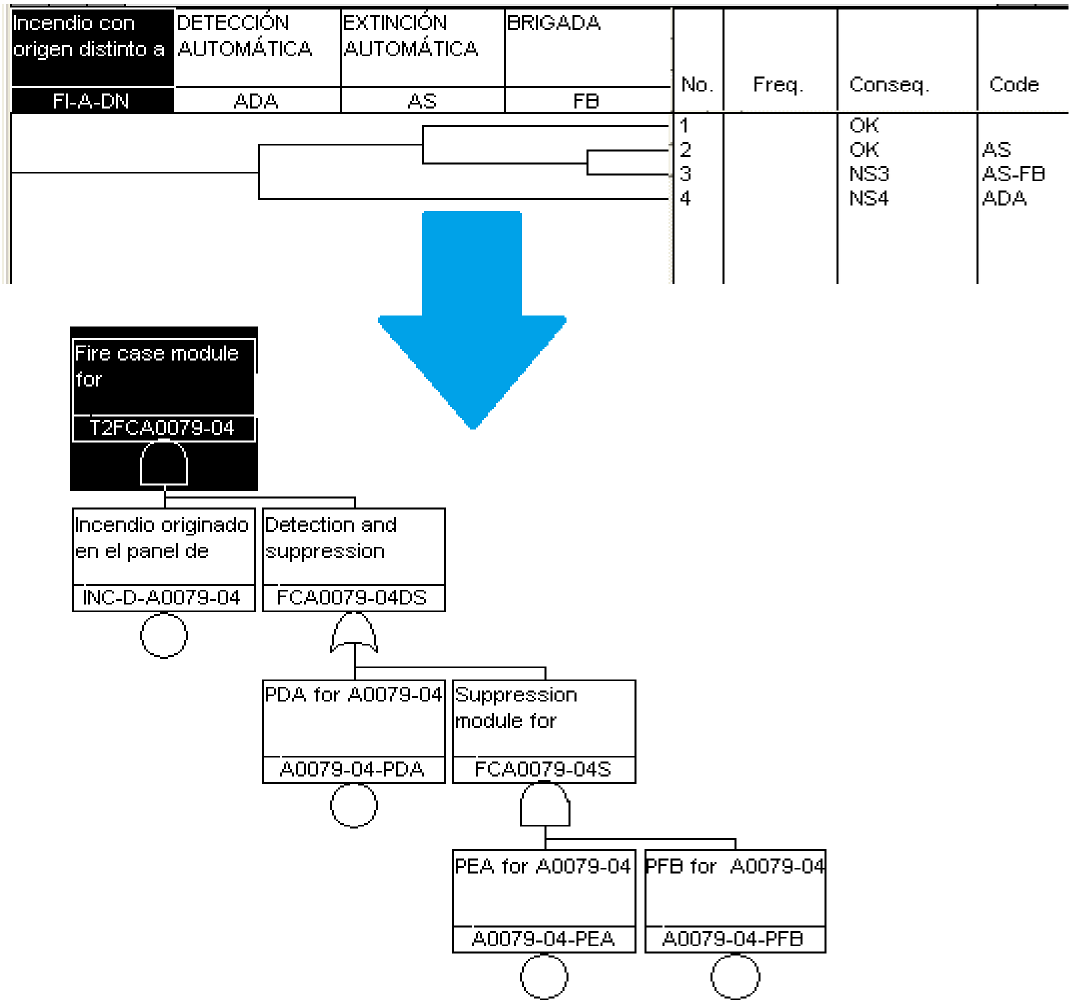
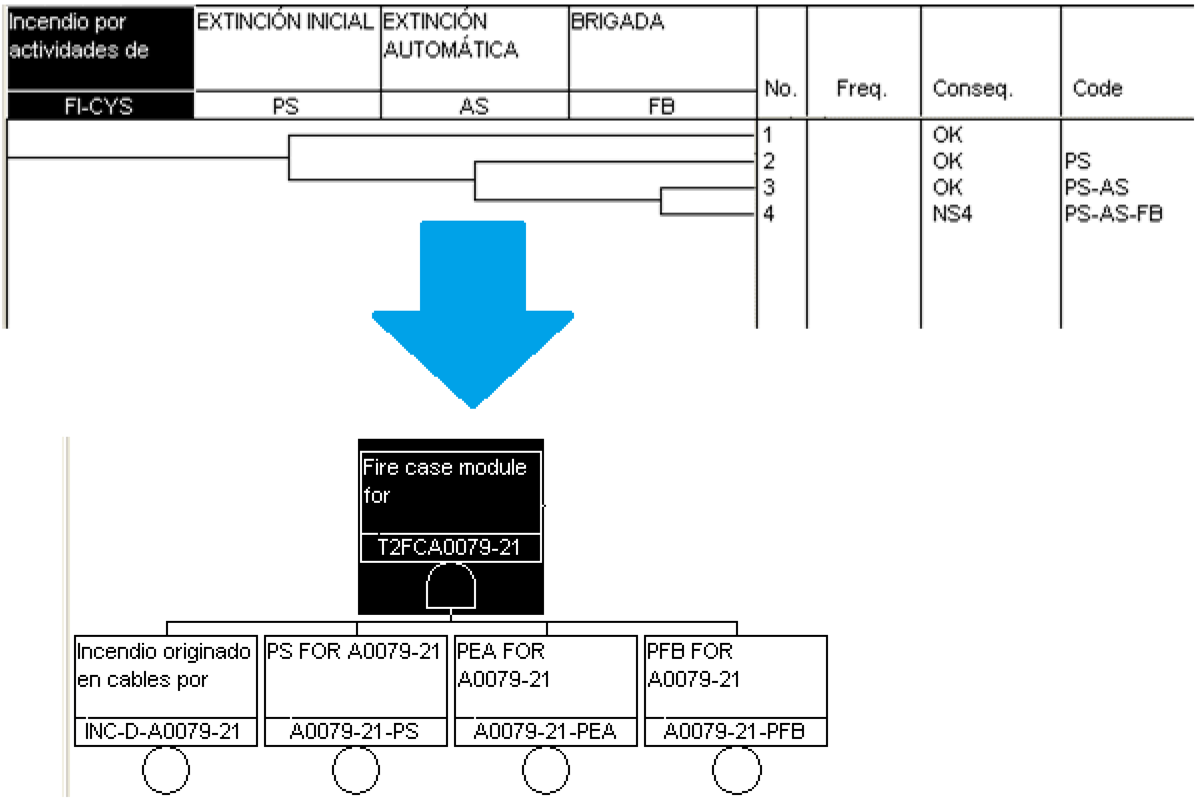


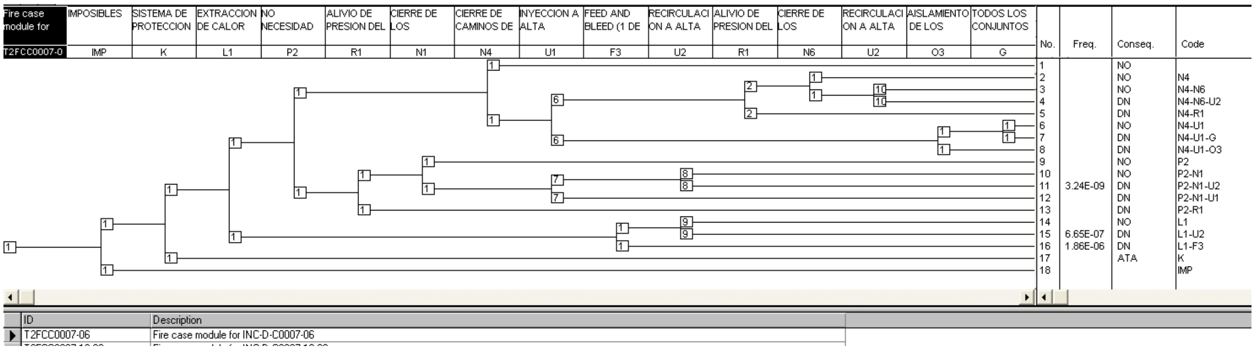
Figure 7.11. Example of Event Tree for fires with origin other than cutting and welding converted to fault tree



Incendio por actividades de	EXTINCIÓN INICIAL	EXTINCIÓN AUTOMÁTICA	BRIGADA	No.	Freq.	Conseq.	Code
FI-CYS	PS	AS	FB				
				1		OK	
				2		OK	PS
				3		OK	PS-AS
				4		NS4	PS-AS-FB

Figure 7.12. Example of Event Tree of fire originating from welding and cutting converted to fault tree

A Fault tree is created for each of the consequence analysis cases in the model. Their purpose is to provide the frequency values for no suppression/fire progression scenarios. These frequency values are linked to the Internal Events' event trees headers as Initiating Events which consequently lead to a possible core Damage (CD) as shown in the figure 7.13. As many as the number of fire analysis cases had their corresponding internal Events´ event trees created using Microsoft Access Query 2007®.



Fire case module for	IMPOSIBLES	SISTEMA DE PROTECCION	EXTRACCION DE CALOR	NO NECESIDAD	ALIVIO DE PRESION DEL	CIERRE DE LOS	CIERRE DE CAMINOS DE	INYECCION A ALTA	FEED AND BLEED (1 DE	RECIRCULACI ON A ALTA	ALIVIO DE PRESION DEL	CIERRE DE LOS	RECIRCULACI ON A ALTA	AISLAMIENTO DE LOS	TODOS LOS CONJUNTOS
T2FCC0007-0	IMP	K	L1	P2	R1	N1	N4	U1	F3	U2	R1	N6	U2	O3	G

No.	Freq.	Conseq.	Code
1		NO	
2		NO	N4
3		NO	N4-N6
4		DN	N4-N6-U2
5		DN	N4-R1
6		NO	N4-U1
7		DN	N4-U1-G
8		DN	N4-U1-O3
9		NO	P2
10		NO	P2-N1
11	3.24E-09	DN	P2-N1-U2
12		DN	P2-N1-U1
13		DN	P2-R1
14		NO	L1
15	6.65E-07	DN	L1-U2
16	1.86E-06	DN	L1-F3
17		ATA	K
18			IMP

ID	Description
T2FCC0007-06	Fire case module for INC-D-C0007-06

Figure 7.13: Typical Example of an internal event tree for which the fault tree top gate can be linked as initiating event.

7.6.3. CREATION OF FIRE CASES INTERNAL EVENT TREES

The Internal Events' trees associated with the fire consequence analysis cases are created. The creation of these event trees is by replicating the internal Events' Trees who's initiating Events are the top gate of the fire CAC fault trees. These internal events include; S1-medium Lost of Coolant Accident (LOCA); S2- small LOCA; S3- very small LOCA; T2- Turbine and Reactor Trip; T3- Loss of condenser vacuum; T8- Inadvertent safety injection; etc. The RiskSpectrum ® software is capable of duplicating Event trees, but the process is cumbersome and time consuming. The objective is to replicate the internal event trees in the fire PSA model, without any change in sequence and data. The only change is the assigning of unique Identification code to each internal event tree replicated. As many as fire consequence analysis cases are created. Looking at the time and the number of internal events´ trees to be created, it is not prudent to use RiskSpectrum.

In view of that Microsoft Access Query was used for the creation of the internal Event trees conveniently and as fast as possible from the PSA model access database. Microsoft Access is a database management system on which several Microsoft products are built with graphical interface and software development tools. Microsoft Access store data in its own format and can also import or link directly to data stored in other application databases. The Microsoft Access query is a request for data results for action on data, or for both. It can be used to perform calculations, to combine data from different tables, or even to add, change, or delete table data. The Microsoft Access query 2007 version was used.

The changes can be done in Microsoft Access Query and the outcome can be shown graphically in RiskSpectrum. It can be verified in RiskSpectrum whether the exact replicate of the internal Event tree has been made. Event trees associated to an internal event such as T2, S2, T3, etc. are replicated with as many T2 new event trees as fire cases which leads to T2, but given each a unique Identification (ID) code.

7.6.3.1 CREATION OF UNIQUE IDENTIFICATION CODE FOR THE EVENT TREES

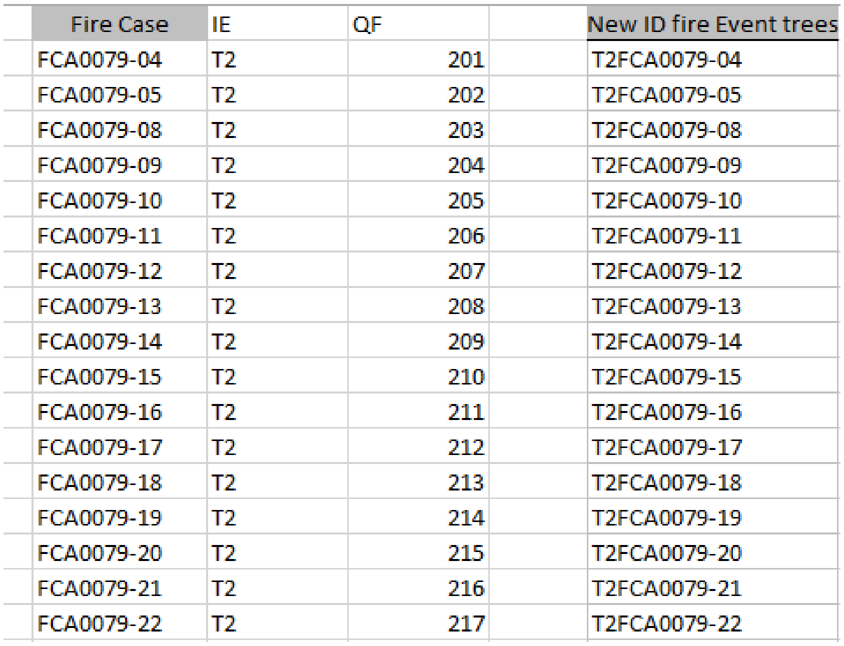
A unique new IDs are created for the replicated event trees in a way to help set an easy criteria for their selection in access query. An excel spread sheet is used for creation of the ID codes as shown in Table 7.1. The new unique ID for the internal event trees is represented by the fire consequence analysis case (CAC) code of the new model, but starting with the code of the type of internal Event associated to, such as T2, S3, T3, T4, T7, TV, T8, T9A, T9B, T10, TS and T11. For example XXFCA0093-06-A, where XX is S2, T2, T4, TV etc. like T2FCA0079-04. This is done to ensure that all fire CAC associated with any particular internal Event having the same event tree can be selected together.

Similarly, a unique Identification codes are created for the Boundary Cut Sets (BCSet) for all the consequence Analysis Cases top gate. A boundary condition set (BCSet) is used to explicitly specify TRUE or FALSE logical values for house events, basic events or gates. The BCSet is required for the top gate of the fire CAC fault tree which is the initiating Event of the internal event trees to be created.

For simple selection criteria, the BCSet IDs are designed so that the type of internal event associated to such as T2, S3, T4, etc. are added as prefix to the CAC ID of reference model. This

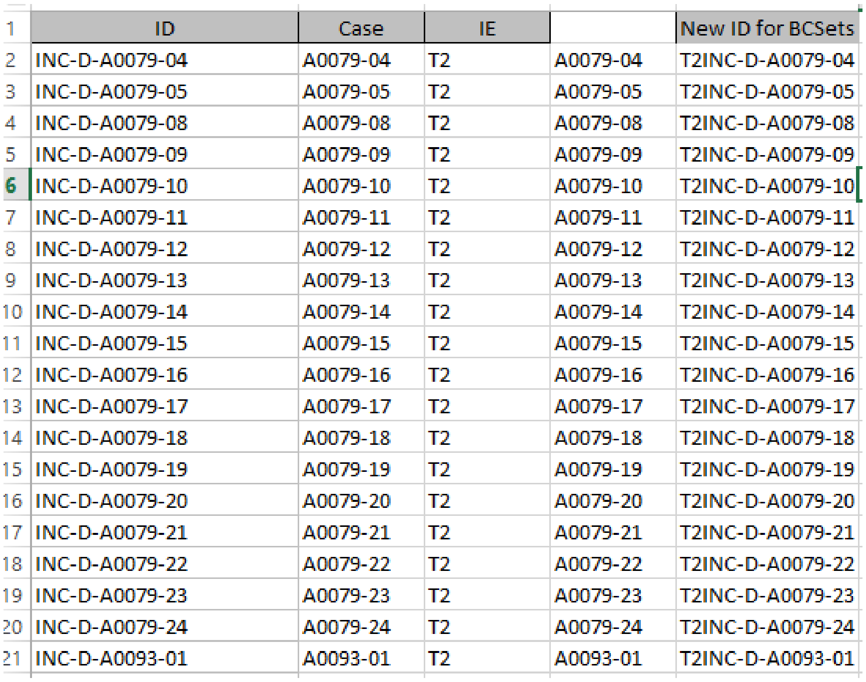
ID is unique because is different from the IDs created for Event Trees and can easily be identified with CAC associated with, as shown in the Table 7.1. Each BCSet ID is given a peculiar number referred to as queryFlag (QF). For example, an ID for CAC in the reference model such as INC-D-A0079-04, becomes T2INC-D-A0079-04, where T2 is the type of internal event associated with that fire CAC. This means that an Internal Event Tree replicated with ID T2FCA0079-04 is assigned a BCSet with ID T2INC-D-A0079-04. The identification codes for the BCSets of the initiating events of the Internal Event Trees replicated are copied into the Events table of the RiskSpectrum database in Microsoft Access.

Table 7.1: Table showing new ID developed for better selection criteria in access query.



Fire Case	IE	QF		New ID fire Event trees
FCA0079-04	T2	201		T2FCA0079-04
FCA0079-05	T2	202		T2FCA0079-05
FCA0079-08	T2	203		T2FCA0079-08
FCA0079-09	T2	204		T2FCA0079-09
FCA0079-10	T2	205		T2FCA0079-10
FCA0079-11	T2	206		T2FCA0079-11
FCA0079-12	T2	207		T2FCA0079-12
FCA0079-13	T2	208		T2FCA0079-13
FCA0079-14	T2	209		T2FCA0079-14
FCA0079-15	T2	210		T2FCA0079-15
FCA0079-16	T2	211		T2FCA0079-16
FCA0079-17	T2	212		T2FCA0079-17
FCA0079-18	T2	213		T2FCA0079-18
FCA0079-19	T2	214		T2FCA0079-19
FCA0079-20	T2	215		T2FCA0079-20
FCA0079-21	T2	216		T2FCA0079-21
FCA0079-22	T2	217		T2FCA0079-22

Table 7.2 An ID designed for easy BCSets selection



1	ID	Case	IE		New ID for BCSets
2	INC-D-A0079-04	A0079-04	T2	A0079-04	T2INC-D-A0079-04
3	INC-D-A0079-05	A0079-05	T2	A0079-05	T2INC-D-A0079-05
4	INC-D-A0079-08	A0079-08	T2	A0079-08	T2INC-D-A0079-08
5	INC-D-A0079-09	A0079-09	T2	A0079-09	T2INC-D-A0079-09
6	INC-D-A0079-10	A0079-10	T2	A0079-10	T2INC-D-A0079-10
7	INC-D-A0079-11	A0079-11	T2	A0079-11	T2INC-D-A0079-11
8	INC-D-A0079-12	A0079-12	T2	A0079-12	T2INC-D-A0079-12
9	INC-D-A0079-13	A0079-13	T2	A0079-13	T2INC-D-A0079-13
10	INC-D-A0079-14	A0079-14	T2	A0079-14	T2INC-D-A0079-14
11	INC-D-A0079-15	A0079-15	T2	A0079-15	T2INC-D-A0079-15
12	INC-D-A0079-16	A0079-16	T2	A0079-16	T2INC-D-A0079-16
13	INC-D-A0079-17	A0079-17	T2	A0079-17	T2INC-D-A0079-17
14	INC-D-A0079-18	A0079-18	T2	A0079-18	T2INC-D-A0079-18
15	INC-D-A0079-19	A0079-19	T2	A0079-19	T2INC-D-A0079-19
16	INC-D-A0079-20	A0079-20	T2	A0079-20	T2INC-D-A0079-20
17	INC-D-A0079-21	A0079-21	T2	A0079-21	T2INC-D-A0079-21
18	INC-D-A0079-22	A0079-22	T2	A0079-22	T2INC-D-A0079-22
19	INC-D-A0079-23	A0079-23	T2	A0079-23	T2INC-D-A0079-23
20	INC-D-A0079-24	A0079-24	T2	A0079-24	T2INC-D-A0079-24
21	INC-D-A0093-01	A0093-01	T2	A0093-01	T2INC-D-A0093-01

Each type of Internal Event has been assigned a peculiar number (QueryFlag) and an identification code number referred to as ETNum as indicated in Table 7.3. For example, S3 (very small LOCA) is assigned ETNum = 32 and QueryFlag =30; T2 (Turbine and Reactor Trip) is assigned ETNum=20 and QueryFlag =20, etc.

Table 7.3 Internal Events with assigned ETNum and QueryFlag

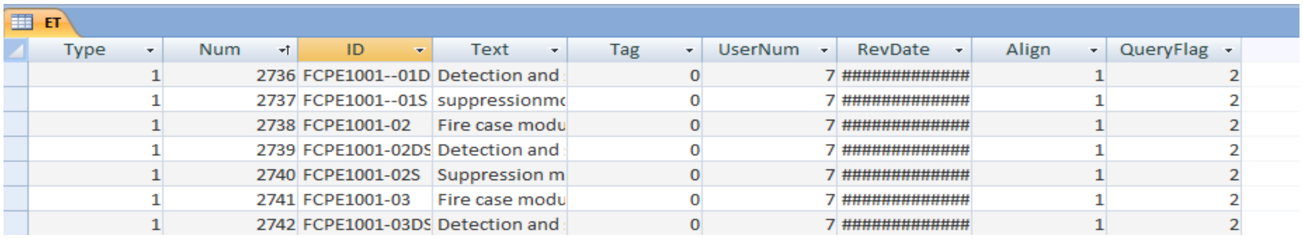
Type	ETNum	QueryFlag
T2	92	20
S3	32	30
T11	72	40
T3	97	50
T12	75	60
T8	116	70
T9B	124	80
T9A	120	90
TS	131	100
TB	139	110
HVAC		120

S2	28	130
T7	111	140
TV	132	150
T10	69	160
T1	39	170
DN	12	180

7.6.3.2 GERNERATION OF RECORDS FOR THE INTERNAL EVENT TREES

The records for the replicated Internal Event Trees are registered in other tables in the RiskSpectrum access database. These tables include, Event Tree (ET) Table, Event Tree sequence (ET_Seq) Table, Event Tree Nodes (ETNodes) Table, Event Tree Events (ETEvent) Table, and Function Event Inputs (FEInput) Table.

The Event Tree (ET) Table has the following fields: Type, Num, ID, Text, Tag, UserNum, RevDate, Align and QueryFlag as shown in the figure 7.14. The ´´type´´ is a number assigned to each type of Event Tree and Event trees of the same type have the same type number. The ´´Num´´ is a serial number assigned to each Identification ID code arrange in order, whereas the ´´text´´ describes what the ID represent. The ´´Tag´´ column can be used to tag an Event tree in the table and be used for filtering purposes. The ´´UserNum´´ is a number assign to users of the code so that changes made to any data can be traced to the user that effected those changes and the RevDate shows the date when the revision is made. The ´´Align´´ is a number indicating the kind of alignment of the Event Tree and the QueryFlag a peculiar number assign to a type of Internal Event. The QueryFlag can be used as additional selection criteria.



Type	Num	ID	Text	Tag	UserNum	RevDate	Align	QueryFlag
1	2736	FCPE1001--01D	Detection and	0	7	##############	1	2
1	2737	FCPE1001--01S	suppressionmo	0	7	##############	1	2
1	2738	FCPE1001-02	Fire case modu	0	7	##############	1	2
1	2739	FCPE1001-02DS	Detection and	0	7	##############	1	2
1	2740	FCPE1001-02S	Suppression m	0	7	##############	1	2
1	2741	FCPE1001-03	Fire case modu	0	7	##############	1	2
1	2742	FCPE1001-03DS	Detection and	0	7	##############	1	2

Figure 7.14. Typical new event Tree records generated in ET table

A registry of the new Event Trees are generated in the ET Table from the records in the Events table. Thus, the Internal Event Trees IDS copied into the Events Table together with other data are selected into the Event Tree (ET) Table using append query. The IDs and text describing the IDs of the new Internal Event Trees are selected from the Events Table by an append query criteria such as ´´Like ´T2F´, or ´S2F´ or ´T3F´ etc. sort in order. The other fields of the ET table such as type, tag, UserNum, RevDate, align and queryFlag are selected with their corresponding codes such as 1, 7, now, 1 and 20 respectively.

7.6.3.3 THE STRUCTURE OF THE EVENT TREES

The Internal Event Tree structure consist of the sequence of the events, Event Tree Nodes and Event Tree Events. These structures are represented by a table in the database and a record of the Event Trees created are registered in these tables.

The Event Tree Sequence (ET_Seq) Table has the following fields: Event Tree Number (ETNum), Sequence Number (SeqNum), Sequence Position (SeqPos), a Father Number (FatherNum), and QueryFlag as shown in upper part of figure 7.14. The fatherNum are points in the Event Tree where an input can be added and the input can be a gate, a basic event, a house event, an undeveloped event or a transfer gate. The SeqNum, SeqPos and the FatherNum are coded numbers in the database which can be selected by specifying the ETNum and the QueryFlag criteria numbers as indicated in the table 4.3 above. For example, if T2 type of Event tree is to be created, then, from Table 4.3 QueryFlag =20 and ETNum =92 are used as selection criteria.

The Event Tree Nodes (ETNodes) are the branching points in the Event Tree. The nodes have horizontal position (HPos) and Vertical positions (VPos). The ETNodes Table has the following fields: ETNum, Num, FatherNum, VPos, HPos, Alternating Number (AltNum) and QueryFlag. Since the event Trees are replicated, the fatherNum, VPos, HPos, (AltNum) which are coded for each type of internal event, do not change for a particular Internal Event Tree. Therefore, by specifying the QueryFlag and the ETNum as the selection criteria and selecting the other fields of the ETNodes table using append query of access, the records for the ETNodes of ETs are created.

The Event Tree Events (ETEvents) Table indicate the fields; ETNum, Event type (EventType), Event Number (EventNum), Position (Pos) and QueryFlag. Similarly, the fields: EventType, EventNum, Pos are coded in the database, which can be selected by specifying the QueryFlag and the ETNum as the selection criteria. The other fields of the ETEvents table are selected using append query and the records of ETEvents of the ETs are created. The ETNum field for the ETEvents table is different from that of ET_Seq Table and ETNodes Table. This should not be so and needed to be corrected through update.

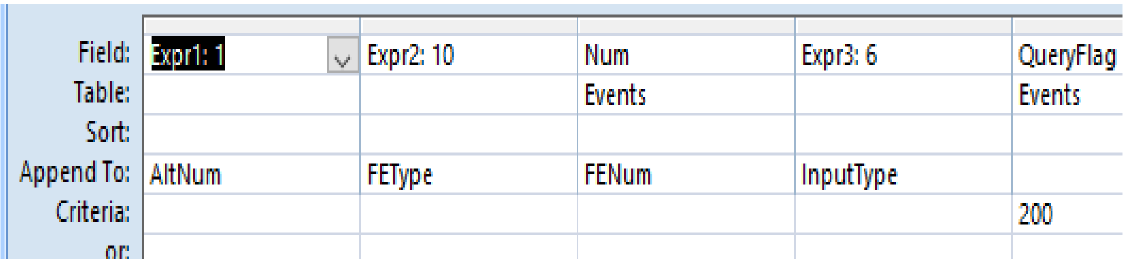
7.6.3.4 RECORDS FOR THE FUNCTION EVENT INPUT TABLE

RiskSpectrum PSA provides very powerful mechanism for changing the logic in the fault trees and event trees as well a component reliabilities for analysis. It provides a very powerful tool for changing the logic in the fault tree and event trees for analyses of special conditions. To this end, setting a number of boundary conditions to be applied when running the analysis to avoid having to change the model explicitly.

A Boundary Condition Set (BCSet) is used to explicitly specify True OR FALSE logical values for house event, basic events or gates. A BCSet can include other BCSets. BCSets can be activated in an analysis case, an initiating event or for a function event. BCSets activated in analysis cases means that the boundary conditions specified in the BCSet will be applied in the analysis you are running. BCSet can also be declared in an initiating event. This means that the boundary conditions is applied in the event trees that use the initiating event.

Function events are associated with event trees and one BCSet can be declared for each input. The conditions in the BCSet will here apply in all downstream branches from the function event in the event trees where the function is used. Through the function event input table BCSet can be set for each fire consequence analysis case internal event trees initiating events.

From the function event input (FEInput) table in the RiskSpectrum access database records are generated for the various fields of the table for the created internal events trees. The table has seven fields: Alternative Number (AltNum); Function Event Type (FEType); Function Event Number (FENum); Input Type (InputType); Input Number (InputNum); Boundary Condition Set Number (BCNum); and QueryFlag. The coded AltNum is 1, FEType is 10 representing BCSets, InputType is 6 representing Event Tree, and the assigned QueryFlag is 200. The append query is used by selecting the codes for the fields and fields of the table to be appended to as shown in the figure 7.15



Field:	Expr1: 1	Expr2: 10	Num	Expr3: 6	QueryFlag
Table:			Events		Events
Sort:					
Append To:	AltNum	FEType	FENum	InputType	
Criteria:					200
or:					

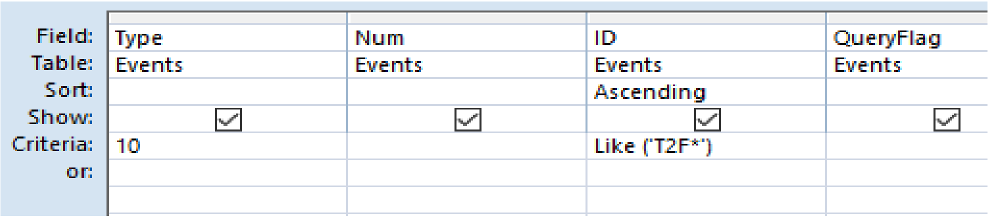
Figure 7.15 An Append query for FEInput Table

7.6.4.0 UPDATES

Updates are used to make records of the ETs up to date. A table can be updated by using another table so that fields in the tables can be linked. If the same fields exist in both tables the records of the one of them in the table can be replaced. The records of the Initiating Events (IEs) in the ETEvents' Table and the BCSets in the FEInput Table of the replicated event trees are updated to reflect their new state. The update are achieved by creating auxiliary Tables and linking the appropriate fields of the tables. The auxiliary tables are created by using data from the Events Table and two auxiliary tables are generated for the purpose of the update of the two fields of the FEInput and the ETEvents Tables.

7.6.4..1 INITIATING EVENTS FOR EVENT TREE EVENTS' TABLE UPDATE

The initiating Event (IE) of the internal event trees replicated are the top gate of the fire consequence analysis cases fault trees. The EventNum field in the ETEvent table does not represent the IEs of the internal event trees generated. Therefore, this field in the ETEvent table needed to be updated to reflect the new IEs status. The numbers representing the IEs are generated in the Event table. Updating the ETEvents to introduce the IEs is achieved by creating auxiliary table and link it with the ETEvents' table. The auxiliary table is generated from the Events table, however, the fields to be shown on the table are selected using the access query. The fields included in table are Num, ID, type, and QueryFlag. The selection criteria such as 'Like (''T2F'')', or 'Like (''S3F'')' etc. and type =10 representing BCSets are used as shown in figure 7.16



Field:	Type	Num	ID	QueryFlag
Table:	Events	Events	Events	Events
Sort:			Ascending	
Show:	☑	☑	☑	☑
Criteria:	10		Like ('T2F*')	
or:				

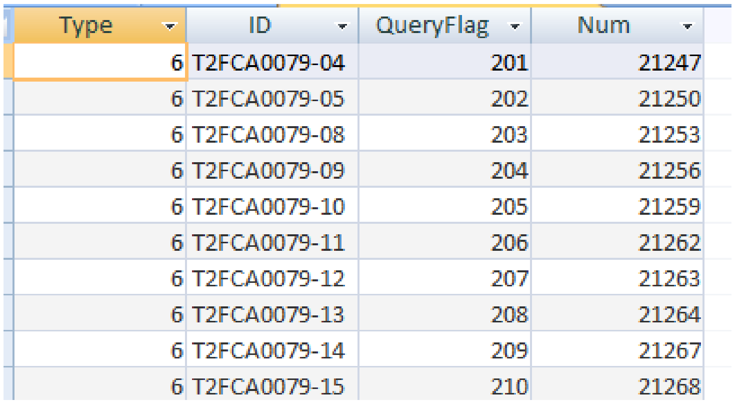
Figure 7.16 creating ancilary table to include the IES

Therefore, using access query update, the QueryFlag of the ETEvent table is linked with the queryFlag of the ancillary table to select the right CAC. The EventNum field of the ETEvents table is updated with the Num field of the ancillary Table to introduce the IEs. Thus the record will include the selection of all records from the ancillary table and only those records from ETEvents table where the joined fields are equal.

7.6.4..2 BCSets IN THE FEInput TABLE UPDATE

Two fields, InputNum and BCNum, of the Function Event Input (FEInput) table was updated to introduce BCSets for the Event Trees created. Two ancillary tables are generated for the purpose of the update. The ancillary tables from the Events table to update InputNum and BCNum fields of the FEInput table.

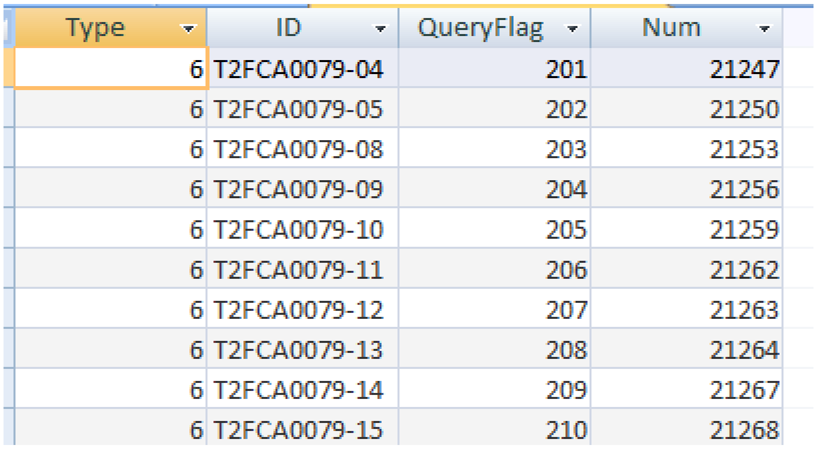
The fields of the ancillary table created to update the InputNum field in the FEInput table include the type, ID, Num and QueryFlag as shown in figure 7.17. The selection criteria include ‘type=6, representing an event tree and the ‘Like (‘’T2F’’)’ or ‘Like (‘’T8F’’)’ etc.



Type	ID	QueryFlag	Num
6	T2FCA0079-04	201	21247
6	T2FCA0079-05	202	21250
6	T2FCA0079-08	203	21253
6	T2FCA0079-09	204	21256
6	T2FCA0079-10	205	21259
6	T2FCA0079-11	206	21262
6	T2FCA0079-12	207	21263
6	T2FCA0079-13	208	21264
6	T2FCA0079-14	209	21267
6	T2FCA0079-15	210	21268

Figure 7.17: The record for an auxiliary table that is created to update the InputNum in the FEinputs

Similarly, the fields of the ancillary table generated to update the BCNum field of the FEInput table include ID, Num, and QueryFlag. The selection criteria is based on the ‘Like (‘’T2IN’’)’ or ‘Like (‘’S3IN’’)’ etc. and the ancillary table created is shown in figure 7.18



Type	ID	QueryFlag	Num
6	T2FCA0079-04	201	21247
6	T2FCA0079-05	202	21250
6	T2FCA0079-08	203	21253
6	T2FCA0079-09	204	21256
6	T2FCA0079-10	205	21259
6	T2FCA0079-11	206	21262
6	T2FCA0079-12	207	21263
6	T2FCA0079-13	208	21264
6	T2FCA0079-14	209	21267
6	T2FCA0079-15	210	21268

Figure 7.18 the record for an auxiliary table that is created to update the InputNum in the FEinputs

The QueryFlag of the ancillary and the FEInput tables are linked for the update. As a results the selection will include all records from the ancillary table and only those records from FEInput table where the joined fields are equal. The Num field of the ancillary table is used to update the InputNum field of FEInput table.

Lastly, the BCNum field in the FEInput table is updated by the Num field of the ancillary table by linking the QueryFlag of the ancillary table for update of BCNum and the FEInput table. The assumption is that the CAC BCSet in the initiating event will have the same effect on the Boolean equation.

Some of the consequence analysis cases share BCSets. Those special cases which share BCSet are recorded in RiskSpectrum since their selection in the query update is complicated. These special cases are listed in the Table 7.5

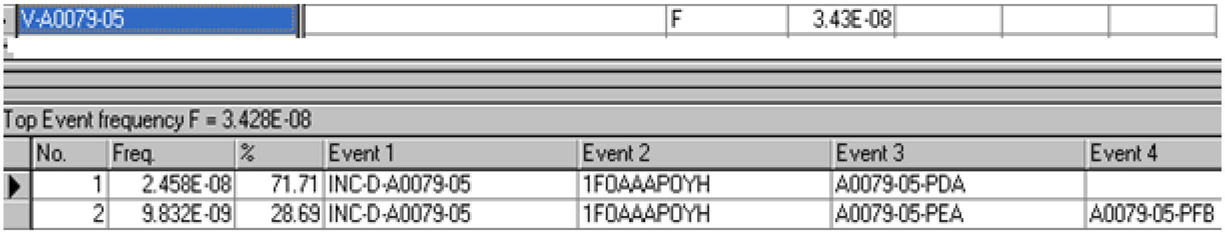
Table 7.5: Consequence Analysis Cases (CAC) with peculiar BCSets

CAC	TYPE	CAC	TYPE
FCC0007-02-04	T2	FCC0008-10-03	T8
FCC0007-05-02	T2	FCC0008-11-03	T8
FCC0007-10-02	T2	FCC0008-12-03	T8
FCC0007-11-02	T2	FCPE0140-07-02	T8
FCC0007-12-02	T2	FCC0007-02-03	T9B
FCC0008-02-02	T2	FCC0007-10-01	T9B
FCC0008-05-02	T2	FCC0007-11-01	T9B
FCC0008-10-02	T2	FCC0007-12-01	T9B
FCC0008-11 02	T2	FCC0008-02-01	T9A
FCC0008-12-02	T2	FCC0008-05-01	T9A
FCPE0138-08-01	S3	FCC0008-10-01	T9A
FCPE0138-09-01	S3	FCC0008-11-01	T9A
FCPE0138-11-01	S3	FCC0008-12-01	T9A
FCPE01389-12-01	S3	FCPE0143-09-04	TS
FCPE0138-13-01	S3	FCPE0143-13-03	TS

FCPE0140-02-02	S3	FCPE0143-14-03	TS
FCPE0140-12-02	S3	FCPE0143-15-03	TS
FCPE0143-09-01	S3	FCC0018-07-1	TB
FCC0018-07-2	T11	FCC0018-11-1	TB
FCC0018-11-2	T11	FCPE0138-08-02	S2
FCC0007-02-01	T3	FCPE0138-09-02	S2
FCC0007-05-01	T3	FCPE0138-11-02	S2
FCPE0140-07-01	T3	FCPE0138-12-02	S2
FCPE0143-09-03	T12	FCPE0138-13-02	S2
FCPE0143-13-02	T12	FCPE0140-02-01	S2
FCPE0143-14-02	T12	FCPE0140-12-01	S2
FCPE0143-15-02	T12	FCPE0143-09-02	T7
FCC0007-02-02	T8	FCPE0143-13-01	T7
FCC0007-05-03	T8	FCPE0143-14-01	T7
FCC0007-10-03	T8	FCPE0143-15-01	T7
FCC0007-11-03	T8	FCPE0143-09-05	TV
FCC0007-12-03	T8	FCPE0143-13-04	TV
FCC0008-02-03	T8	FCPE0143-14-04	TV
FCC0008-05-03	T8	FCPE0143-15-04	TV

7.7.0 VALIDATION

The conversion model in RiskSpectrum was validated to verify the appropriateness of the new model. The frequency of each Fire Consequence Analysis case (CAC) of the conversion model and the reference model are quantified and the frequencies compared. Different top event frequencies were obtained for most of the cases. For example as shown in figure 7.19 & 7.20, the top event frequency for the conversion model V-A0079-05 is 3.458E-08 with two MCSs, whereas the reference model INC-D-A0079-05 has top Event frequency of 3.597E-10 with same number of MCSs. The Event 2 of the two MCSs of the reference model and the conversion model are different. The reference model has 1FOAACONTH: operator failure to control feedwater system (AA) and the conversion model has 1FOAAAPOYH: operator failure to backup automatic signals of feedwater system (AA). The events 1, 3 and 4 are the same as shown in figure 7.19

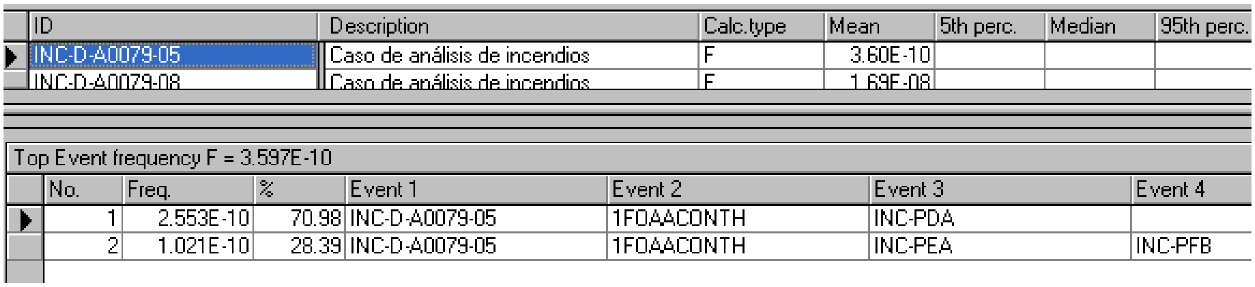


V-A0079-05		F	3.43E-08

Top Event frequency F = 3.428E-08

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4
1	2.458E-08	71.71	INC-D-A0079-05	1FOAAAPOYH	A0079-05-PDA	
2	9.832E-09	28.69	INC-D-A0079-05	1FOAAAPOYH	A0079-05-PEA	A0079-05-PFB

Figure 7.19 Example of results of validation of Conversion model

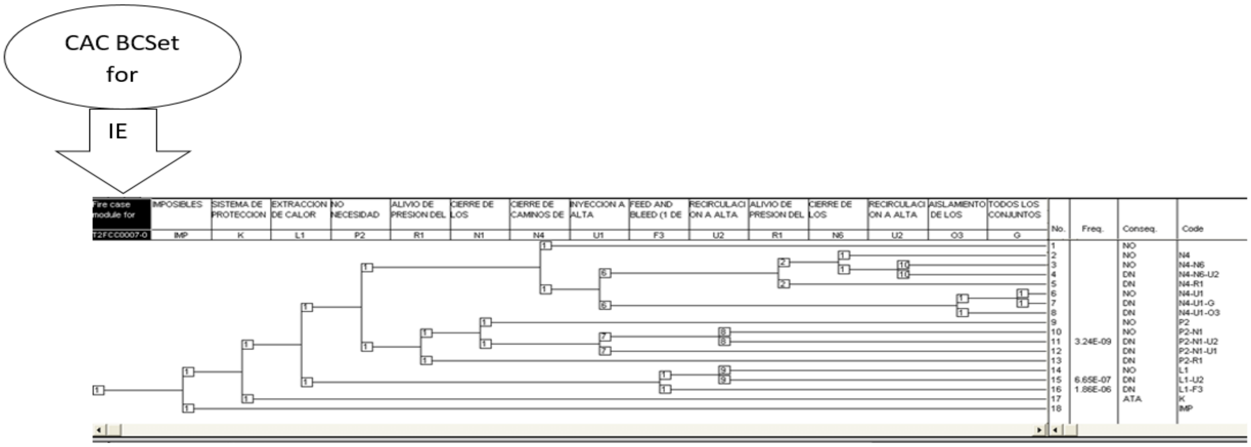


ID	Description	Calc.type	Mean	5th perc.	Median	95th perc.
INC-D-A0079-05	Caso de análisis de incendios	F	3.60E-10			
INC-D-A0079-08	Caso de análisis de incendios	F	1.69E-08			

Top Event frequency F = 3.597E-10

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4
1	2.553E-10	70.98	INC-D-A0079-05	1FOAACONTH	INC-PDA	
2	1.021E-10	28.39	INC-D-A0079-05	1FOAACONTH	INC-PEA	INC-PFB

Figure 7.20: Typical results of validation of the reference model.

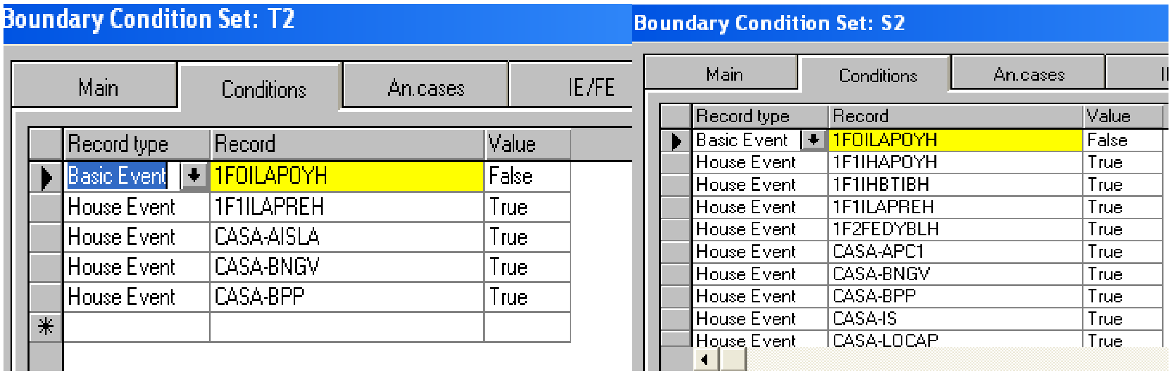


No.	Freq.	Conseq.	Code
1		NO	
2		NO	N4
3		NO	N4-N6
4		DN	N4-N6-U2
5		DN	N4-R1
6		NO	N4-U1
7		DN	N4-U1-G
8		DN	N4-U1-O3
9		NO	P2
10		NO	P2-N1
11	3.24E-09	DN	P2-N1-U2
12		DN	P2-N1-U1
13		DN	P2-R1
14		NO	L1
15	6.65E-07	DN	L1-U2
16	1.86E-06	DN	L1-F3
17		ATA	K
18			IMP

Figure 7.21 showing the CAC BCSet set as the IE BCset for the Event trees created

In the reference model each of 384 fire consequence analysis case has a BCSet assigned to quantify its CDF. However, in the conversion model each fire case is linked to an internal Event tree, therefore, the BCSet per case becomes the Initiating event BCSet of the internal Event trees as indicated in figure 7.21 above. This accounts for the differences in the quantification of top frequency values for the reference and the conversion model. This demonstrate clearly that if the right BCSets are not assigned properly the right results will not be obtained.

After careful observation, the initiating events BCSets of the internal events Trees of the reference model are absent in the conversion model. For example the boundary condition set for T2 and S2 as shown in figure 7.22 are absent in the conversion model. It can be seen that operator failure to control feedwater system, shown in yellow, is set FALSE instead of TRUE. This means that the Basic Event should not appear in the Boolean equation.



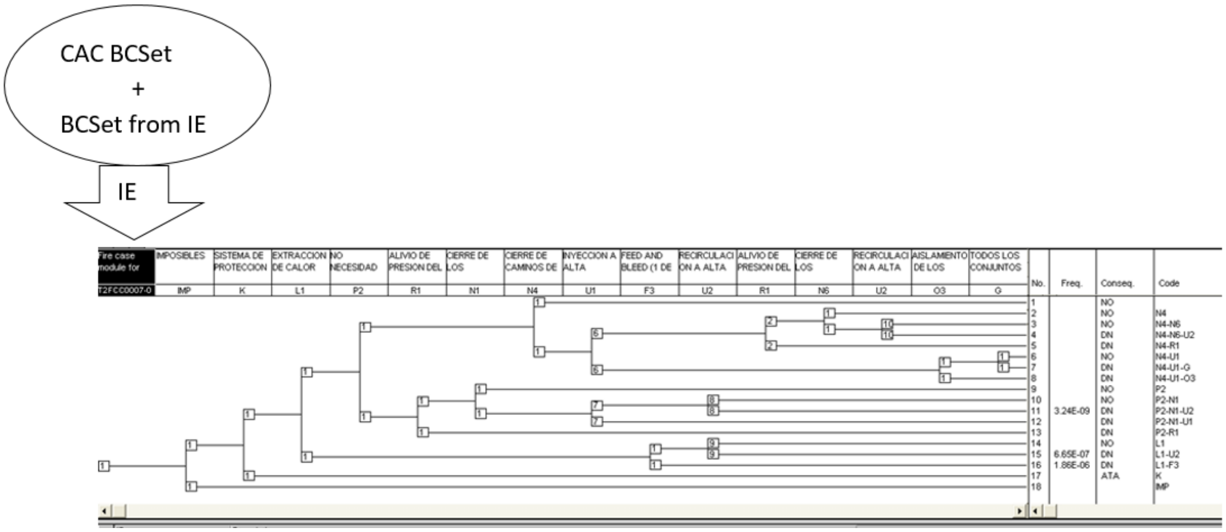
Boundary Condition Set: T2

Record type	Record	Value
Basic Event	1FOILAPOYH	False
House Event	1F1ILAPREH	True
House Event	CASA-AISLA	True
House Event	CASA-BNGV	True
House Event	CASA-BPP	True

Boundary Condition Set: S2

Record type	Record	Value
Basic Event	1FOILAPOYH	False
House Event	1F1IHAPOYH	True
House Event	1F1IHBTIBH	True
House Event	1F1ILAPREH	True
House Event	1F2FEDYBLH	True
House Event	CASA-APC1	True
House Event	CASA-BNGV	True
House Event	CASA-BPP	True
House Event	CASA-IS	True
House Event	CASA-LOCAP	True

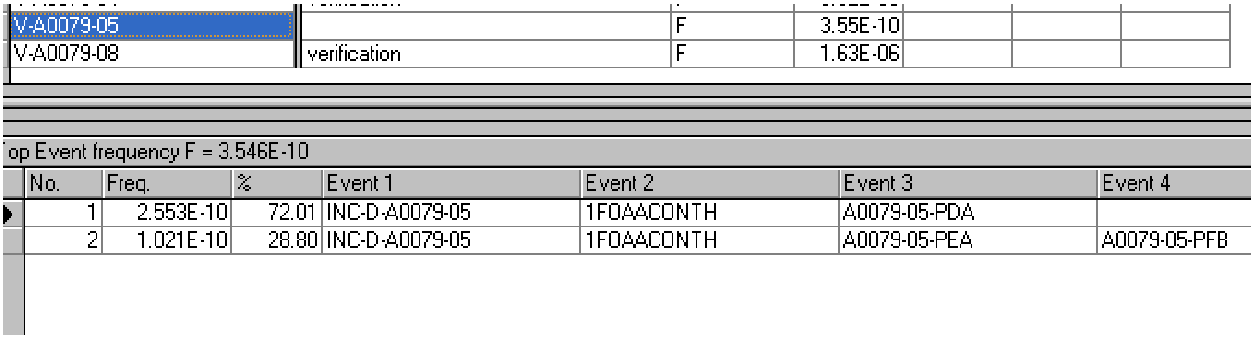
Figure 7.22 Boundary conditions set for T2 and S2



No.	Freq.	Conseq.	Code
1		NO	
2		NO	N4
3		NO	N4-N6
4		DN	N4-N6-U2
5		DN	N4-R1
6		NO	N4-U1
7		DN	N4-U1-G
8		DN	N4-U1-O3
9		NO	P2
10		NO	P2-N1
11	3.24E-09	DN	P2-N1-U2
12		DN	P2-N1-U1
13		DN	P2-R1
14		NO	L1
15	6.65E-07	DN	L1-U2
16	1.86E-06	DN	L1-F3
17		ATA	K
18			IMP

Figure 7.23 showing the combination of CAC BCSet and the BCSet of the internal Events Initiating event (IE)

When the BCSets of the CAC and the initiating Events (IE) are combined in the conversion model, as indicated in figure 7.22, same results are obtained for most of the Fire CACs for both the reference and the conversion models. For example V-A0079-05 and INC-D-A0079-05 top event frequency are equal with same MCSs as shown in figure 7.24 &7.20. However, few needed to adapt to modifications in order to achieve the needed verification.



V-A0079-05		F	3.55E-10		
V-A0079-08	verification	F	1.63E-06		

'op Event frequency F = 3.546E-10

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4
1	2.553E-10	72.01	INC-D-A0079-05	1FOAACONTH	A0079-05-PDA	
2	1.021E-10	28.80	INC-D-A0079-05	1FOAACONTH	A0079-05-PEA	A0079-05-PFB

Figure 7.24: Results of validation of the conversion model after BCSet correction

The observation show that almost 90% of the consequence analysis cases were valid after the validation. The total CDF of the reference model $CDF_{reference} = 9.83 \times 10^{-6}$ [93, 100] whereas the total CDF of the conversion model is 7.65x10^{-7}, provided the BCSets of the invalidated fire consequence analysis cases are not modified.

About 46 consequence Analysis Cases had different validation results for the mean frequency and the number of Minimal Cut sets (MCS) as shown in Table 7.7. Few have equal number of MCS but different mean frequency. The combination of BCSets for the fire consequence analysis cases and the BCsets for the Initiating Events for the Internal Event Trees is not appropriate for all fire consequence analysis cases. Therefore, there is the need to modify those few cases in order to obtain same results as the reference model. The original intention is that we maintained the originality of the reference model, but as far as boundary condition cut sets are concerned few modification are necessary in order to obtain the desire results.

The details of the missing MCS from each of the identified consequence analysis cases can be seen in Appendix A, where all the MCS present in both the reference model and the conversion model are red colored at the edge. The uncolored ones are the missing MCS.

Table 7.7: consequence Analysis Cases with different top Event mean frequency and Minimal Cut sets (MCS)

	CAC	Con.	Refer.	con.	refer.		CAC	Con.	Refer.	con	refer.
		freq	freq	MCS	MCS			freq	Freq	MCS	MCS
No.						**No**					
1	C0003-03	1.10E-07	1.40E-07	17	22	21	PE0140-02-01	2.18E-09	1.58E-09	1	1
2	C0003-28	7.65E-09	2.57E-08	5	14	22	PE0142-02	2.26E-09	1.40E-09	1	1
3	C0003-30	7.80E-09	2.65E-08	5	14	23	PE0143-14-03				1
4	C0007-02-04		6.28E-08		17	24	PE2001-03	3.08E-08	3.48E-08	2	8
5	C0007-03	2.26E-09	1.40E-09	1	1	25	PE2001-04	3.64E-08	4.12E-08	3	5
6	C0007-05-02		5.75E-09		1	26	R0133-01	4.49E-07	5.74E-07	28	42
7	C0008-02-01		1.33E-09		1	27	R0134-01	6.48E-07	7.99E-07	36	58
8	C0008-02-02		1.33E-09		1	28	R0139-3B-01	4.23E-08	5.22E-08	6	8
9	C0008-02-03		2.66E-07		74	29	R0139-3B-02	2.62E-08	3.21E-08	2	4
10	C0008-05-03	7.26E-10	1.65E-08	33	6	30	R0139-3C-01	1.98E-08	2.45E-08	1	3
11	C0018-05	2.24E-09	1.38E-09	1	1	31	R0139-3C-02	3.68E-07	4.49E-07	19	27
12	C0018-06	2.24E-09	1.38E-09	1	1	32	S0187-03	9.66E-08	9.15E-08	21	21
13	C0018-07-1	1.65E-08	1.36E-08	6	6	33	S0187-04	9.66E-08	9.15E-08	21	21
14	C0018-07-2	1.65E-08	1.36E-08	6	6	34	S0187-07	2.86E-07	2.80E-07	40	40
15	C0020-05	2.54E-09	1.84E-09	1	1	35	S0187-08	2.33E-07	2.29E-07	32	32
16	C0043-10	1.42E-09		2		36	S0190-05	5.65E-08	7.69E-09	7	20
17	C0045-08	1.31E-08	2.66E-08	6	12	37	T0167-01		2.44E-09		4
18	PE0138-07	2.23E-07		2		38	T0167-02-1	1.82E-09	1.82E-09	1	2
19	PE0138-08-01		3.08E-09		1	39	T0167-02-4	1.70E-09	2.15E-09	1	
20	PE0138-08-02	9.96E-09	1.04E-09	2	2	40	T0167-03	5.46E-09		2	

6.8.0 Conversion of model to CAFTA and Risk Monitor

The conversion Fire PSA model could not be converted to CAFTA due to software incompatibility. Some bugs may have accounted for the crashing of the CAFTA software. The apparent lockup slow down the display of certain large fault trees leading to crashing after many screen refreshes. The drawing of fault tree CAFTA would skip some horizontal lines when more than 7 levels are displayed. The CAFTA would not accept a comma in an equation or direct value in embedded in the code which are not apparent to the user of RiskSpectrum. The challenge is beyond the scope of this research work for which the conversion of the Fire PSA model to appropriate Risk Monitor model can be achieved.

A model suitable for Risk Monitor should facilitate a simultaneous single quantification of all the fire scenarios. The challenges associated with the less than 10% consequence analysis cases in the validation process is the BCSets based and not the approach of quantification. Alternative single quantification model has been developed that is suitable for Fire Risk monitor purposes. The proposed fire PSA model is a simple and explicit method to build a single-top external event PSA model for Risk monitoring system.

7.9.0 CONCLUSION

The challenges associated with the conversion of the Fire PSA (the reference model) model to Risk Monitor suitable model has been identified. The proposal solution has been provided and solved to some extent possible. However, the Fire PSA model suffered conversion challenges in CAFTA and could not be validated in CAFTA.

The reference model could not be converted properly by CAFTA, the new quantification software. Some of the Consequence Analysis Cases are randomly selected leaving out some others. Some of the accident sequences carrying core damage are not integrated in the model. That is, information is lost in the conversion. The initiating event of the internal Events Tree is not well integrated. There was the challenge of obtaining one single Core Damage frequency from the 384 CDF`s from the reference model within the RiskSpectrum ® quantification software.

The proposal of solution was changing the orientation of the consequences as a unique result of CDF associated with Events trees of internal events. This is achieved by creating fault trees for all the 384 CAC and the top header of the fault trees becomes the initiators of the fire internal event trees.

IDs for fire basic Events are developed and entered in RiskSpectrum® and fire fault trees created. The creation of internal Events` trees using Microsoft Access utilizing the RiskSpectrum® Access database and outcome observed in graphics in RiskSpectrum®. Fire PSA conversion model has been developed and the challenge of 384 CDF has been overcome with single unique CDF.

The results of the validation show that 90% of the fire Consequence Analysis Cases (CAC) are valid when the boundary Cut Set (BCSet) for the fire CAC and the BCSets for Initiating Events of the internal Event trees are combined. When the initiating event BCSets for the reference model and the conversion model are combined and the BCSet, operator failure to control feedwater system is set FALSE instead of TRUE, most of the results were confirmed. The remaining CAC BCSets needed to be modified to get the desired result.

The anticipated resolution of incompatibility issues with the CAFTA code and RiskSpectrum code can resolve the conversion of the developed model in CAFTA. However, a model suitable for Risk Monitor purposes should facilitate a simultaneous single quantification of all the fire scenarios. The results has shown that the proposed Fire PSA model is a simple and explicit method to build a single-top external Event PSA model for Risk Monitor system.

CONCLUSION AND RECOMMENDATION

CONCLUSION

One original contribution of this PhD is the historical risk-informed grounds for embarking countries to acknowledge the radiological risk posed by fire. The study have shown that risk and cost component of the plant can be reduced when appropriately planned and engineered. This will prevent the use of expensive bacfits and prescriptive regulations as USA implemented after Brown Ferry Nuclear Power station fire accident in 1975. The experiences of the countries reviewed have shown that residual risk remains even after expensive retrofit.

The study has shown that the domestic and industrial fire safety regulations are inadequate and ineffective means of NPP fire safety. The three countries (USA, Germany and Japan) studied, have developed distinctive regulations, standards and guidelines to prevent, control and mitigate fires at NPP.

This PhD study recommends that for NPP fire safety considerations Ghana’s nuclear power programme should be well planned and engineered before construction using the state-of-the-art methods and technology. This will save the country from expensive retrofit to ensure fire safety.

This PhD study will form the basis for development of regulations for fire safety of NPP future deployment in Ghana. The USNRC prescriptive, risk-informed, and performance-based regulations provide useful lessons for Ghana to consider, but does not represent adequate design bases regulation for new nuclear power plant.

One original contribution of this PhD is the affirmation that the fire protection programme for the new power reactor should be based on the defense-in-depth approach couple with highly developed safety culture backed by regulation. This is shown in Japanese fire safety culture but the lack of backing of the appropriate regulation became a challenge during the accident at Fukushima. The lessons learned initiated the change in the Japanese NPP fire regulations.

One of the original contribution of this PhD is that the methods of fire risk assessment should be based on integration of deterministic and probabilistic methodologies using the appropriate state-of-the-art technology. The integration will complement the two methods of fire safety assessment. The risk insight from PSA will supplement the deterministic methods to ensure adequate fire risk assessment based on which risk-informed decisions will be taken.

One of the original contribution of this PhD is the development of an innovative way of communicating Risk to decision-makers and management so that prompt risk-informed decision could be taken. The fire-related risk unavailability matrix, Fire-related system and key safety functions unavailability matrix has been developed and used as an innovative tool for risk-informed decision-making at Spanish PWR NPP. The unavailability of fire protection systems does not significantly affect the risk. The fire risk matrix identifies the fire zones that contribute the most to the fire-related risk. These zones belong to the control building and electric penetrations building

Another unique contribution of the PhD is the evaluation of the contribution of fire to the overall Core Damage frequency. The aggregation of Internal Events PSA model and Fire PSA model have shown that the Fire PSA contributes 38.4% to the Risk Increase (RI).

One original contribution of this PhD is that the current fire PSA model of the Spanish Westinghouse PWR in RiskSpectrum® is not suitable for risk monitor purposes. The model computes CDF for each of the 384 fire case scenarios and after screening the final CDF is determined outside the RiskSpectrum code. However, Risk Monitor requires a unique single CDF to determine the instantaneous risk at the plant at any time.

The findings of this PhD is that CAFTA® (quantification software for Risk Monitor) is not capable of converting completely and sequentially RiskSpectrum® files into its own files.

One original contribution of this PhD is that the Westinghouse PWR fire PSA model has been developed to estimate a single unique CDF for all the 384 fire case scenarios. This is achieved by modifying the Boundary cut set (BCSets) for a few of the fire consequence analysis cases.

One original contribution of this PhD is that more incompatibility issues have been identified with RiskSpectrum® code and the CAFTA© code. This work is contributing to the development and upgrade of the PSA software to include cross platform conversion of models. Most importantly contributing to the international PSA software standardization efforts.

RECOMMENDATION

It is recommended to the operator of the Westinghouse PWR NPP to further work to check the Fire PSA model for possible inconsistent in the less than 10 % of the fire consequence analysis cases that were not validated in the conversion model.

The project of converting Fire PSA model in RiskSpectrum to CAFTA model and consequently create Fire risk monitor is recommended to continue. When the upgrade and standardization of the CAFTA software is complete the second and third milestone of the project is continued. For example some of the challenges encountered like Fault tree display failing (crash) after many screen refreshes. Display was also very slow (apparent lockup) on certain large fault trees has been bug fixed in version 5.4. The project is recommended to:

- Convert the model in CAFTA®.
- Validate the model in CAFTA®
- Create a new thermometer for the Fire PSA.

This will cumulate in the Creation of a risk Monitor model from quantification model and create a fire thermometer and mitigation events. Introduction of fire related equipment into Risk Monitor.

REFERENCCES

[1] https://www.nei.org/Knowledge-Center/Nuclear-Statistics/World-Statistics, 20 July 2017.

[2] IAEA SAFETY STANDARDS SERIES No. SF-1, FUNDAMENTAL SAFETY PRINCIPLES, INTERNATIONAL ATOMIC ENERGY AGENCY VIENNA, 2006

[3] IAEA Safety Glossary, Terminology used in Nuclear Safety and Radiation Protection 2016 Revision page 8

[4] Deterministic safety analysis for nuclear power plants: safety guide, International Atomic Energy Agency, 2009. — (IAEA safety standards series, ISSN 1020–525X

[5] Ralph R Fullwood, Probabilistic Risk Assessment in the Nuclear Power Industry: Fundamentals and Applications

[6] NUREG-75/014, "Reactor Safety Study—An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400, U.S. Nuclear Regulatory Commission, October 1975. (Agency wide Documents Access and Management System (ADAMS) Accession No. ML083570090)

[7] NUREG/KM-0009, Historical Review and Observations of Defense-in-Depth, April 2016

[8] U.S. Atomic Energy Commission, "Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants,“ WASH-740, pages vii, 5, and 21, March 1957.

[9] U.S. Nuclear Regulatory Commission, "USNRC Strategic Plan Fiscal Years 2014-2018," NUREG-1614, Volume 6, August 2014. (ADAMS Accession No. ML14246A439)

[10] U.S. Nuclear Regulatory Commission, Public Website, Glossary, http://www.nrc.gov/reading-rm/basic-ref/glossary/defense-in-depth, 2016

[11] IAEA INSAG-10, Defense in Depth in Nuclear Safety, A report by the International Nuclear Safety Advisory Group, 1996.

[12] SAFETY SERIES No. 75-INSAG-4, SAFETY CULTURE, IAEA, VIENNA, 1991 STI/PUB/882 ISBN 92-0-123091-51991

[13] Basic safety principles for nuclear power plants: 75-INSAG-3 rev. 1 / a report by the International Nuclear Safety Advisory Group. — Vienna: International Atomic Energy Agency, 1999.

[14] HSE Research Report 367, 2005, 'A Review of Safety Culture and Safety Climate Literature for the Development of the Safety Culture Inspection Toolkit' page 3

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, SAFETY ASSESSMENT FOR FACILITIES AND ACTIVITIES, IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), IAEA, Vienna (2016).

[16] NUREG-1150, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants—Final Summary Report," U.S. Nuclear Regulatory Commission, December 1990.

[17] NRC, 60FR42622, Use of Probabilistic Risk Analysis methods in nuclear Regulatory Activities, 1995.

[18] NUREG/CR-2300, A Guide to the Performance of Probabilistic Risk Assessments for Nuclear, Power Plants, Final Report, January 1983

[19] http://www.nfpa.org/about-nfpa/nfpa-overview/history-of-nfpa, 12 July 2016

[20] Editorial". J. Radiol. Prot. 27: 211–215. 2007. doi:10.1088/0952-4746/27/3/e02

[21] https://en.wikipedia.org/wiki/Windscale_fire, 18/09/2017

[22] Walter W. Maybee, A brief history of Fire protection in the United States Atomic Energy Commission 1947-1975, National Fire Protection Association, Conference fall 1978

[23] NRC, Appendix A to Part 50—General Design Criteria for Nuclear Power Plants,

[24] NUREG/BR-0361, “The Browns Ferry Nuclear Plant Fire of 1975 and the History of NRC Fire Regulations,” February 2009. (ADAMS Accession No. ML091250195)

[25] BTP APCSB 9.5-1, “Guidelines for Fire Protection for Nuclear Power Plants” www.nrc.gov/docs/ML0706/ML070660458.pdf, 18/09/2017

[26] GL 77-02, “Nuclear Plant Fire Protection Functional Responsibilities, Administrative Controls and Quality Assurance, August 4, 1977, ADAMS Accession No. ML031280293

[27] NRC, SECY92.263. "Elimination of Requirements Marginal to Safety," July 24, 1992

[28] SECY-98-058, “Development of a Risk-Informed, Performance-Based Regulation for Fire Protection at Nuclear Power Plants,” March 26, 1998

[29] NUREG-1742, “Perspectives Gained from the IPEEE Program,” Volumes 1 and 2, April 2002

[30] NFPA 805, “Performance-Based Standard for Fire Protection for Light-Water Reactor Electric Generating Plants” (2001 Edition)

[31] NEI, “Spurious Actuation of Electrical Circuits Due to Cable Fires: Results of an Expert Elicitation” (Report No. 1006961) in May 2002

[32] NEI 00-01, “Guidance for Post-Fire Safe-Shutdown Circuit Analysis” (Revision 2 issued May 2009)

[33] NRC, RIS 2005-30, “Clarification of Post-Fire Safe-Shutdown Circuit Regulatory Requirements” January 2005.

[34] NRC, EGM 09-002, “Enforcement Guidance Memorandum—Enforcement Discretion for Fire Induced Circuit Faults,” May 14, 2009

[35] NUREG/BR-0522, Fire Protection Program for Operating Reactors, ML1420/ML14209A040, August, 2014.

[36] SAND90-1827, “Fire Safety Lessons Learned from the Design and Operation of Commercial Nuclear Reactor Facilities,” Sandia National Laboratories, February 1993. (ADAMS Accession No. ML090420618)

[37] NUREG/CR- 4681, “Enclosure Environment Characterization Testing for the Base Line Validation of Computer Fire Simulation Codes,” March 1987

[38] NUREG/CR-4527, “An Experimental Investigation of Internally Ignited Fires in Nuclear Power Plant Control Cabinets,” Part I: “Cabinet Effects Tests,” Volume 1, issued April 1987 [38]

[39] NUREG/CR-4527, “An Experimental Investigation of Internally Ignited Fires in Nuclear Power Plant Control Cabinets,” Part II: “Room Effects Tests,” Volume 2, issued November 1988

[40] NUREG/CR-4832, “Analysis of the LaSalle Unit 2 Nuclear Power Plant: Risk Methods Integration and Evaluation Program (RMIEP),” Volume 9: “Internal Fire Analysis,” January 1990

[41] NUREG/CR-6850 and EPRI 1011989, “EPRI/NRC RES Fire PRA Methodology for Nuclear Power Facilities,” Sandia National Laboratories/U.S. Nuclear Regulatory Commission/Electric Power Research Institute, September 2005.

[42] Gallucci, R.H.V, 1980, ‘’A methodology for evaluating the probability for fire loss of nuclear power safety function’’ PhD thesis at Rensselaer Poly. Institute Troy NY GAO 1983

[43] M. Kazarians, N. Siu, and G. Apostolakis, “Fire Risk Analysis for Nuclear Power Plants: Methodological Developments and Applications,” Risk Analysis, Volume 5, pp. 33–51, 1985.

[44] N. Siu, “Physical Models for Compartment Fires,” Reliability Engineering, Volume 3, pp. 229–252, 1982.

[45] NUREG/CR-6834, “Circuit Analysis—Failure Mode and Likelihood Analysis,” Sandia National Laboratories, September 2003.

[46] NUREG/CR-6738, “Risk Methods Insights Gained From Fire Incidents,” Sandia National Laboratories, September 2001.

[47] NUREG-1824 and EPRI 1011999, Volumes 1–7, “Verification and Validation of Selected Fire Models for Nuclear Power Plant Applications,” produced under an interagency memorandum of understanding with the U.S. Department of Commerce, National Institute of Standards and Technology, May 2007.

[48] NUREG-1852, “Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire,” U.S. Nuclear Regulatory Commission/Science Applications International Corporation/Sandia National Laboratories, October 2007.

[49] Stetkar, J.W., W.J. Shack, and H.P. Nourbakhsh, “The Current State of Transition to Risk-Informed Performance-Based Fire Protection Programs,” U.S. Nuclear Regulatory Commission Advisory Committee on Reactor Safeguards, February 2011. (ADAMS ML110430035)

[50] N. Siu, K. Coyne, and N. Melly, Fire PRA Maturity and Realism: A Technical Evaluation, A Technical Opinion Paper, U.S. Nuclear Regulatory Commission January 2016, p 76

[51] Pietrangelo, A.R., Nuclear Energy Institute, “Industry support and use of PRA and risk-informed regulation,” letter to A.M. Macfarlane, Chairman, U.S. Nuclear Regulatory Commission, December 19, 2013. (ADAMS ML13354B997)

[52] Kuritzky, A., N. Siu, K. Coyne, D. Hudson, and M. Stutzke, “L3PRA: Updating NRC’s Level 3 PRA insights and capabilities,” Proceedings of IAEA Technical Meeting on Level 3 Probabilistic Safety Assessment, Vienna, Austria, July 2-6, 2012, International Atomic Energy Agency, Vienna, Austria (2013). (ADAMS ML12173A092)

[53] R. Wittmann, Fire Safety Regulations for Nuclear Power Plants in Germany and the Various Dimensions of German KTA Standardization Activities. Is there a Benefit Today? Siemens AG Power Generation, Erlangen, Germany, IAEA-SM-345/11

[54] Björn Elsche, Marina Röwekamp, Wilfried Neugebauer, Rainer Gersinska, Ongoing Enhancements in the German Nuclear Regulatory Framework with Respect to Fire Safety, 23rd International Conference on Structural Mechanics in Reactor Technology (SMiRT 23) - 14th International Post-Conference Seminar on “FIRE SAFETY IN NUCLEAR POWER PLANTS AND INSTALLATIONS“ Salford, United Kingdom, August 17-18, 2015

[55] The Federal Office for Radiation Protection (Bundesamt für Strahlenschutz – BfS), ´´The safety Requirements for Nuclear Power plants´´ Federal Gazette (BAnz AT 30.03.2015 B2.) on 24 January 2013

[56] Björn Elsche, Günter Fischer, Stefan Kirchner, the Multi-Stage Fire Safety Concept in German Nuclear Power Plants, 21th International Conference on Structural Mechanics in Reactor Technology (SMiRT 21) -12th International Post Conference Seminar on “Fire Safety in Nuclear Power Plants and Installations“München, Germany September 13-15, 2011

[57] Heinz Peter Berg and Jan Hauschild, Probabilistic Assessment of Nuclear Power Plant Protection against External Explosions, 2012 Bergand Hauschild, licensee InTech. Chapter 5

[58] BfS SAFETY CODES AND GUIDES –TRANSLATIONS, Nuclear Power Plant Safety Criteria, Promulgation of 21 October 1977

[59] Heinz-Peter Berg and Marina Röwekamp (2010). Current Status of Fire Risk Assessment for Nuclear Power Plants, Nuclear Power, Pavel Tsvetkov (Ed.), ISBN: 978-953-307-110-7, InTech, Available from: http://www.intechopen.com/books/nuclear-power/current-status-of-fire-risk-assessment-for-nuclear-powerplants

[60] Martina Kloos and Joerg Peschke, Improved Modelling and Assessment of the Performance of Firefighting Means in the Frame of a Fire PSA, Science and Technology of Nuclear Installations, Volume 2015, Article ID 238723, 10 pages, 15 January 2015.

[61] www.iaea.org/inis/collection/NCLCollectionStore/_Public/31/051/31051385.pdf, H. P. Berg, FIRE RISK ASSESSMENT IN GERMANY, 26-09-2016

[62http://www.world-nuclear.org/information-library/country-profiles/countries-g-n/japan-nuclear-power.aspx, cited 26-09-2016

[63] IAEA International Fact Finding Expert Mission of Fukushima Daiichi NPP Accident Following Great East Japan Earthquake and Tsunami (24 May-2 June 2011), Mission Report, 16 June 2011

[64] Report, A comparison of U.S. and Japanese regulatory requirements in effect at the time of the Fukushima accident, November 2013, https://www.nrc.gov/docs/ML1332/ML13326A991

[65] Japan Nuclear Authority Website: http://www.nsr.go.jp/archive/nsc/NSCenglish/

[66] Kuramoto Takahiro, Recent advancements of probabilistic risk assessment methodologies and risk monitoring usages in Japan, Nuclear Safety and Simulation, Vol. 6, Number 1, March 2015

[67] INTERNATIONAL ATOMIC ENERGY AGENCY, Fire Protection in Nuclear Power Plants: A Safety Guide, Safety Series No. 50-SG-D2 (Rev.1), IAEA, Vienna (1992).

[68] INTERNATIONAL ATOMIC ENERGY AGENCY, ASSET Guidelines: Revised 1991 Edition, IAEA-TECDOC-632, Vienna (1991).

[69] INTERNATIONAL ATOMIC ENERGY AGENCY, Inspection of Fire Protection Measures and Fire Fighting Capability at Nuclear Power Plants, Safety Series No. 50-P-6, IAEA, Vienna (1994).

[70] INTERNATIONAL ATOMIC ENERGY AGENCY, Evaluation of Fire Hazard Analyses for Nuclear Power Plants, Safety Series No. 50-P-9, IAEA, Vienna (1995).

[71] INTERNATIONAL ATOMIC ENERGY AGENCY, Organization and Conduct of IAEA Fire Safety Reviews at Nuclear Power Plants, IAEA Services Series No. 2, IAEA, Vienna (1998).

[72] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparation of Fire Hazard Analyses for Nuclear Power Plants, Safety Reports Series No. 8, IAEA, Vienna (1998).

[73] INTERNATIONAL ATOMIC ENERGY AGENCY, Treatment of Internal Fires in Probabilistic Safety Assessment for Nuclear Power Plants, Safety Reports Series No. 10, IAEA, Vienna (1998).

[74] NRC, SECY-90-016, “Evolutionary Light Water Reactor (LWR) Certification Issues and Their Relationship to Current Regulatory Requirements,” January 12, 1990, and associated SRM, June 26, 1990

[75] NRC, Regulatory Guide 1.120, “Fire Protection Guidelines for Nuclear Power Plants”, June 1976

[76] NRC, Branch Technical Position CMEB 9.5-1, "Guidelines for Fire Protection for Nuclear Power Plants" 1 May 1976.

[77] Regulatory Guide 1.174, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” U.S. Nuclear Regulatory Commission, Washington

[78] USNRC Generic Letter 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities—10CFR 50.54(f)," November 23, 1988

[79] IAEA-TECDOC-1421, Experience gained from fires in nuclear power plants: Lessons learned, 2004

[80] Nathan Siu, Kevin Coyne, Selim Sancaktar, and Nicholas Melly, Fire PRA Maturity and Realism: A Discussion and Suggestions for Improvement, U.S. Nuclear Regulatory Commission: MS CSB 4A07M, Washington, DC

[81] NUREG- 1150, Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, Vol. 1, December 1990

[82] Fire PRA Implementation Guide, EPRI, December 1995. EPRI TR-105928 (Including

[83] Fire-Induced Vulnerability Evaluation (FIVE), EPRI, April 1992. EPRI TR-100370. Supplement: EPRI SU-105928).

[84] Fire PRA Implementation Guide, EPRI, December 1995. TR-105928 (including Supplement: EPRI SU-105928).

[85] Procedures for the External Event Core Damage Frequency Analyses for NUREG-1150, NUREG/CR-4840, U.S. NRC, Washington, DC, 1990.

[86] U.S. Nuclear Regulatory Commission, “An Approach for Using Probabilistic Risk Assessment in Risk Informed Decisions on Plant-Specific Changes to the Licensing Basis,” Regulatory Guide 1.174, Revision 1, November 2002.

[87] U.S. General Accounting Office, “Nuclear Regulation—NRC Needs to More Aggressively and Comprehensively Resolve Issues Related to the Davis-Besse Nuclear Power Plant’s Shutdown,” GAO-04-415, May 2004.

[88] U.S. Nuclear Regulatory Commission, “NRC Incident Investigation Program,” MD 8.3, March 27, 2001.

[89] U.S. Nuclear Regulatory Commission, “NRR Reactor Operating Experience Program,” LIC-401, May 17, 2005.

[90] U.S. Nuclear Regulatory Commission, “Effective Risk Communication—Guideline for Internal Risk Communication,” NUREG/BR-0318, December 2004.

[91] U.S. Nuclear Regulatory Commission, “Effective Risk Communication—The Nuclear Regulatory Commission’s Guideline for External Risk Communication,” NUREG/BR-0308, January 2004

[92] Gareth W. Parry Michele Laur Michael D. Tschiltz, A process for risk-informed decision-making, U. S. Nuclear Regulatory Commission, ML053540044,

[93] Pedro Diaz, Enric Estruch, Javier Dies, Carlos Tapia, Alfredo De Blas & Matthew Asamoah (2016): Development and assessment of fire-related risk unavailability matrices to support the application of the maintenance rule in a PWR nuclear power plant, Journal of Nuclear Science and Technology, DOI: 10.1080/00223131.2016.1193066

[94] Pedro Díaz Bayona, Proyecto de investigación para el desarrollo y aplicación de herramientas de valoración de riesgos tecnológicos en centrales nucleares españolas a partir de la técnica de Análisis Probabilista de Seguridad, Doctoral Thesis, November 2017.

[95] Spanish Nuclear Power Plant. Análisis de Incendios: Selección de Componentes [Fire analysis: components selection]. Barcelona: Spanish Nuclear Power Plant; 2010.

[96] Spanish Nuclear Power Plant. Análisis Probabilista de Seguridad de Incendios: Informe resumen [Fire probabilistic safety assessment: summary report]. Barcelona: Spanish Nuclear Power Plant; 2010

[97] N. Siu, K. Coyne, and N. Melly, Fire PRA Maturity and Realism: A Technical Evaluation, A Technical Opinion Paper, Office of Nuclear Regulatory Research U.S. Nuclear Regulatory Commission, January 2016

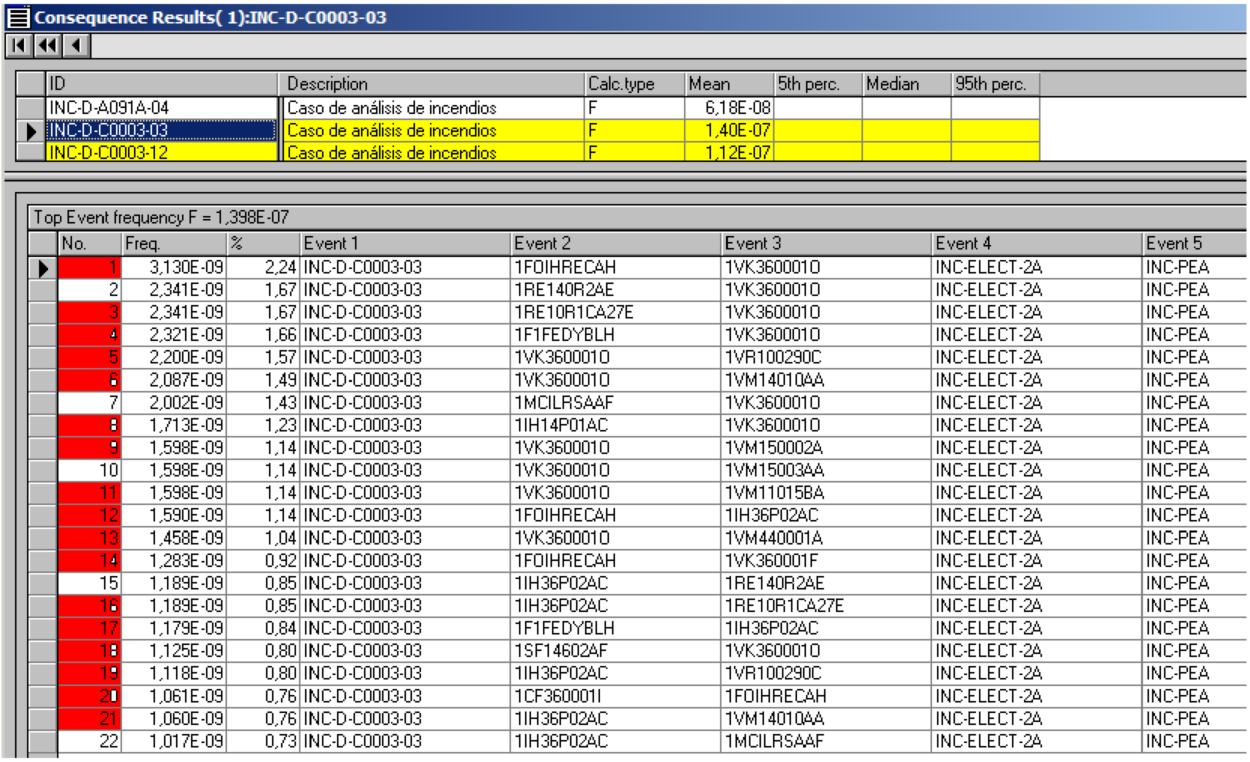
[98] NEA/CSNI/R, Risk Monitors the State-of-the- arts in their development and use at Nuclear Power Plants, 2004

[99] Enrique Melendez Asensio and Roberto Herrero Santos, Use of PSA model XML Standard Formats for V&V, Consejo de Seguridad Nuclear

[100] P. Díaz, E. Estruch, J. Dies, C. Tapia, A. De Blas, M. Asamoah, FIRE-RELATED SYSTEMS AND KEY SAFETY FUNCTIONS UNAVAILABILITY MATRIX DEVELOPMENT AND ASSESSMENT, American Nuclear Society Topical Meeting on Probabilistic Safety Assessment and Analysis(PSA2015), Sun Valley, ID, USA, April 25-30 2015

APPENDIX: invalidated Consequence Analysis Cases

Consequence Analysis cases with different number of Minimal Cut Sets (MCS) for the reference model and the conversion model. The common MCS are coloured red and the missing MCS uncoloured. The cases are in blue.



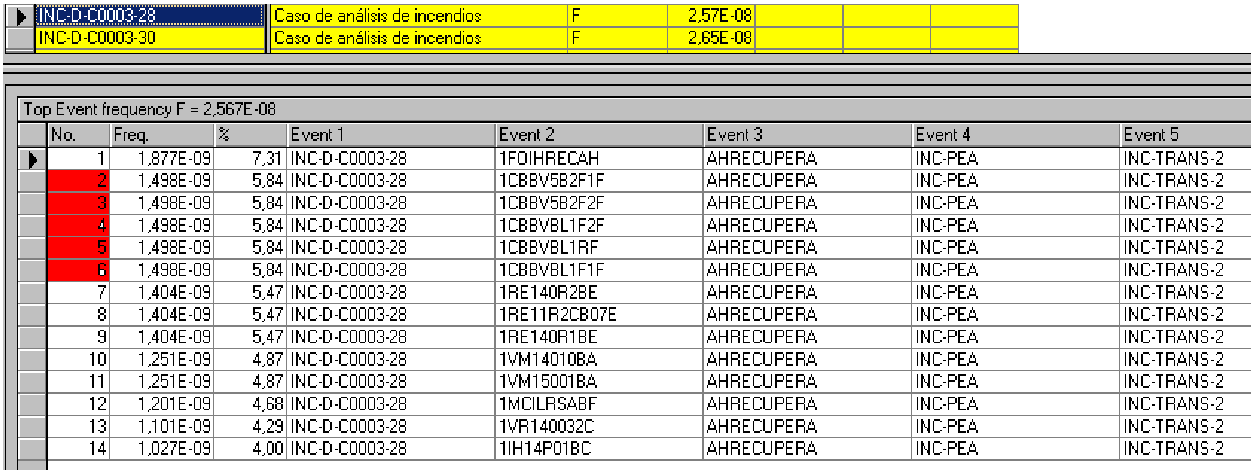
Consequence Results(1):INC-D-C0003-03

ID	Description	Calc.type	Mean	5th perc.	Median	95th perc.
INC-D-A091A-04	Caso de análisis de incendios	F	6,18E-08			
INC-D-C0003-03	Caso de análisis de incendios	F	1,40E-07			
INC-D-C0003-12	Caso de análisis de incendios	F	1,12E-07			

Top Event frequency F = 1,398E-07

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4	Event 5
🟥 1	3,130E-09	2,24	INC-D-C0003-03	1FOIHRECAH	1VK3600010	INC-ELECT-2A	INC-PEA
2	2,341E-09	1,67	INC-D-C0003-03	1RE140R2AE	1VK3600010	INC-ELECT-2A	INC-PEA
🟥 3	2,341E-09	1,67	INC-D-C0003-03	1RE10R1CA27E	1VK3600010	INC-ELECT-2A	INC-PEA
🟥 4	2,321E-09	1,66	INC-D-C0003-03	1F1FEDYBLH	1VK3600010	INC-ELECT-2A	INC-PEA
🟥 5	2,200E-09	1,57	INC-D-C0003-03	1VK3600010	1VR100290C	INC-ELECT-2A	INC-PEA
🟥 6	2,087E-09	1,49	INC-D-C0003-03	1VK3600010	1VM14010AA	INC-ELECT-2A	INC-PEA
7	2,002E-09	1,43	INC-D-C0003-03	1MCILRSAAF	1VK3600010	INC-ELECT-2A	INC-PEA
🟥 8	1,713E-09	1,23	INC-D-C0003-03	1IH14P01AC	1VK3600010	INC-ELECT-2A	INC-PEA
🟥 9	1,598E-09	1,14	INC-D-C0003-03	1VK3600010	1VM150002A	INC-ELECT-2A	INC-PEA
10	1,598E-09	1,14	INC-D-C0003-03	1VK3600010	1VM15003AA	INC-ELECT-2A	INC-PEA
🟥 11	1,598E-09	1,14	INC-D-C0003-03	1VK3600010	1VM11015BA	INC-ELECT-2A	INC-PEA
🟥 12	1,590E-09	1,14	INC-D-C0003-03	1FOIHRECAH	1IH36P02AC	INC-ELECT-2A	INC-PEA
🟥 13	1,458E-09	1,04	INC-D-C0003-03	1VK3600010	1VM440001A	INC-ELECT-2A	INC-PEA
🟥 14	1,283E-09	0,92	INC-D-C0003-03	1FOIHRECAH	1VK360001F	INC-ELECT-2A	INC-PEA
15	1,189E-09	0,85	INC-D-C0003-03	1IH36P02AC	1RE140R2AE	INC-ELECT-2A	INC-PEA
🟥 16	1,189E-09	0,85	INC-D-C0003-03	1IH36P02AC	1RE10R1CA27E	INC-ELECT-2A	INC-PEA
🟥 17	1,179E-09	0,84	INC-D-C0003-03	1F1FEDYBLH	1IH36P02AC	INC-ELECT-2A	INC-PEA
🟥 18	1,125E-09	0,80	INC-D-C0003-03	1SF14602AF	1VK3600010	INC-ELECT-2A	INC-PEA
🟥 19	1,118E-09	0,80	INC-D-C0003-03	1IH36P02AC	1VR100290C	INC-ELECT-2A	INC-PEA
🟥 20	1,061E-09	0,76	INC-D-C0003-03	1CF360001I	1FOIHRECAH	INC-ELECT-2A	INC-PEA
🟥 21	1,060E-09	0,76	INC-D-C0003-03	1IH36P02AC	1VM14010AA	INC-ELECT-2A	INC-PEA
22	1,017E-09	0,73	INC-D-C0003-03	1IH36P02AC	1MCILRSAAF	INC-ELECT-2A	INC-PEA

MCS for the reference model case INC-D-C0003-03. The coloured are the MCS for the conversion model

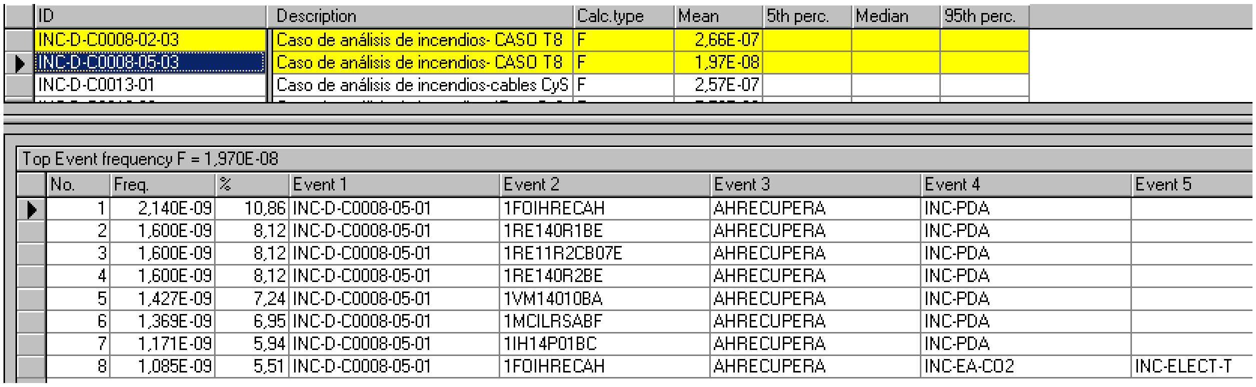


INC-D-C0003-28	Caso de análisis de incendios	F	2,57E-08			
INC-D-C0003-30	Caso de análisis de incendios	F	2,65E-08			

Top Event frequency F = 2,567E-08

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4	Event 5
1	1,877E-09	7,31	INC-D-C0003-28	1FOIHRECAH	AHRECUPERA	INC-PEA	INC-TRANS-2
🟥 2	1,498E-09	5,84	INC-D-C0003-28	1CBBV5B2F1F	AHRECUPERA	INC-PEA	INC-TRANS-2
🟥 3	1,498E-09	5,84	INC-D-C0003-28	1CBBV5B2F2F	AHRECUPERA	INC-PEA	INC-TRANS-2
🟥 4	1,498E-09	5,84	INC-D-C0003-28	1CBBVBL1F2F	AHRECUPERA	INC-PEA	INC-TRANS-2
🟥 5	1,498E-09	5,84	INC-D-C0003-28	1CBBVBL1RF	AHRECUPERA	INC-PEA	INC-TRANS-2
🟥 6	1,498E-09	5,84	INC-D-C0003-28	1CBBVBL1F1F	AHRECUPERA	INC-PEA	INC-TRANS-2
7	1,404E-09	5,47	INC-D-C0003-28	1RE140R2BE	AHRECUPERA	INC-PEA	INC-TRANS-2
8	1,404E-09	5,47	INC-D-C0003-28	1RE11R2CB07E	AHRECUPERA	INC-PEA	INC-TRANS-2
9	1,404E-09	5,47	INC-D-C0003-28	1RE140R1BE	AHRECUPERA	INC-PEA	INC-TRANS-2
10	1,251E-09	4,87	INC-D-C0003-28	1VM14010BA	AHRECUPERA	INC-PEA	INC-TRANS-2
11	1,251E-09	4,87	INC-D-C0003-28	1VM15001BA	AHRECUPERA	INC-PEA	INC-TRANS-2
12	1,201E-09	4,68	INC-D-C0003-28	1MCILRSABF	AHRECUPERA	INC-PEA	INC-TRANS-2
13	1,101E-09	4,29	INC-D-C0003-28	1VR140032C	AHRECUPERA	INC-PEA	INC-TRANS-2
14	1,027E-09	4,00	INC-D-C0003-28	1IH14P01BC	AHRECUPERA	INC-PEA	INC-TRANS-2

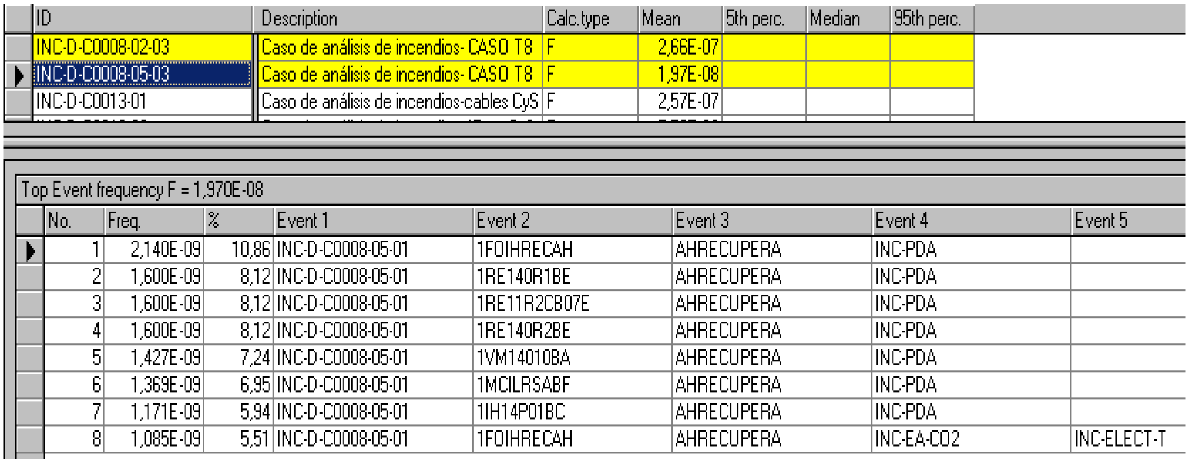
MCS for the reference model case INC-D-C0003-28. The coloured are the MCS for the conversion model.



ID	Description	Calc.type	Mean	5th perc.	Median	95th perc.
INC-D-C0008-02-03	Caso de análisis de incendios- CASO T8	F	2,66E-07			
INC-D-C0008-05-03	Caso de análisis de incendios- CASO T8	F	1,97E-08			
INC-D-C0013-01	Caso de análisis de incendios-cables CyS	F	2,57E-07			

Top Event frequency F = 1,970E-08

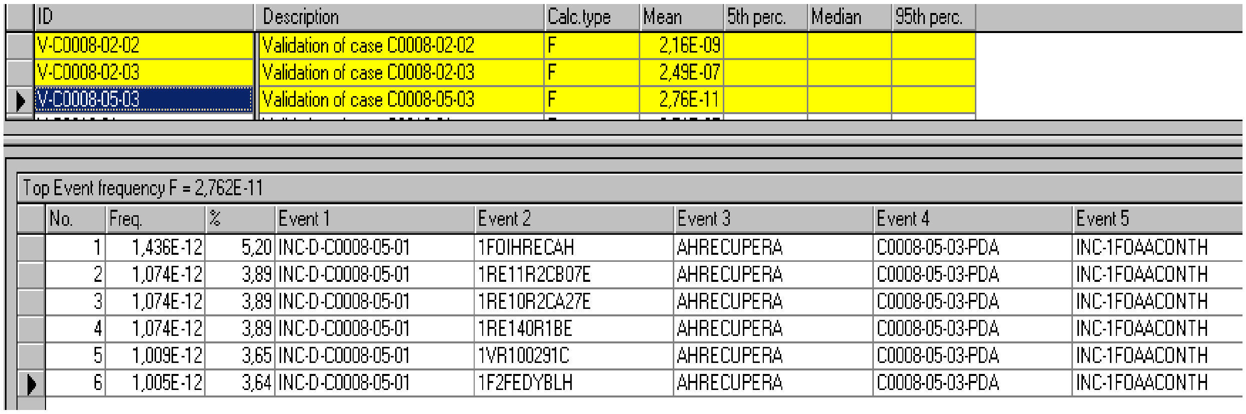
No.	Freq.	%	Event 1	Event 2	Event 3	Event 4	Event 5
1	2,140E-09	10,86	INC-D-C0008-05-01	1FOIHRECAH	AHRECUPERA	INC-PDA	
2	1,600E-09	8,12	INC-D-C0008-05-01	1RE140R1BE	AHRECUPERA	INC-PDA	
3	1,600E-09	8,12	INC-D-C0008-05-01	1RE11R2CB07E	AHRECUPERA	INC-PDA	
4	1,600E-09	8,12	INC-D-C0008-05-01	1RE140R2BE	AHRECUPERA	INC-PDA	
5	1,427E-09	7,24	INC-D-C0008-05-01	1VM14010BA	AHRECUPERA	INC-PDA	
6	1,369E-09	6,95	INC-D-C0008-05-01	1MCILRSABF	AHRECUPERA	INC-PDA	
7	1,171E-09	5,94	INC-D-C0008-05-01	1IH14P01BC	AHRECUPERA	INC-PDA	
8	1,085E-09	5,51	INC-D-C0008-05-01	1FOIHRECAH	AHRECUPERA	INC-EA-CO2	INC-ELECT-T



ID	Description	Calc.type	Mean	5th perc.	Median	95th perc.
INC-D-C0008-02-03	Caso de análisis de incendios- CASO T8	F	2,66E-07			
INC-D-C0008-05-03	Caso de análisis de incendios- CASO T8	F	1,97E-08			
INC-D-C0013-01	Caso de análisis de incendios-cables CyS	F	2,57E-07			

Top Event frequency F = 1,970E-08

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4	Event 5
1	2,140E-09	10,86	INC-D-C0008-05-01	1FOIHRECAH	AHRECUPERA	INC-PDA	
2	1,600E-09	8,12	INC-D-C0008-05-01	1RE140R1BE	AHRECUPERA	INC-PDA	
3	1,600E-09	8,12	INC-D-C0008-05-01	1RE11R2CB07E	AHRECUPERA	INC-PDA	
4	1,600E-09	8,12	INC-D-C0008-05-01	1RE140R2BE	AHRECUPERA	INC-PDA	
5	1,427E-09	7,24	INC-D-C0008-05-01	1VM14010BA	AHRECUPERA	INC-PDA	
6	1,369E-09	6,95	INC-D-C0008-05-01	1MCILRSABF	AHRECUPERA	INC-PDA	
7	1,171E-09	5,94	INC-D-C0008-05-01	1IH14P01BC	AHRECUPERA	INC-PDA	
8	1,085E-09	5,51	INC-D-C0008-05-01	1FOIHRECAH	AHRECUPERA	INC-EA-CO2	INC-ELECT-T

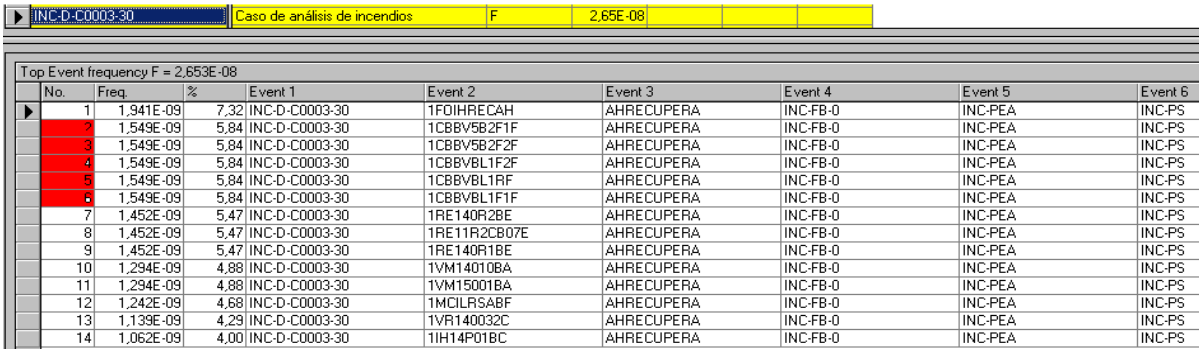


ID	Description	Calc.type	Mean	5th perc.	Median	95th perc.
V-C0008-02-02	Validation of case C0008-02-02	F	2,16E-09			
V-C0008-02-03	Validation of case C0008-02-03	F	2,49E-07			
V-C0008-05-03	Validation of case C0008-05-03	F	2,76E-11			

Top Event frequency F = 2,762E-11

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4	Event 5
1	1,436E-12	5,20	INC-D-C0008-05-01	1FOIHRECAH	AHRECUPERA	C0008-05-03-PDA	INC-1FOAACONTH
2	1,074E-12	3,89	INC-D-C0008-05-01	1RE11R2CB07E	AHRECUPERA	C0008-05-03-PDA	INC-1FOAACONTH
3	1,074E-12	3,89	INC-D-C0008-05-01	1RE10R2CA27E	AHRECUPERA	C0008-05-03-PDA	INC-1FOAACONTH
4	1,074E-12	3,89	INC-D-C0008-05-01	1RE140R1BE	AHRECUPERA	C0008-05-03-PDA	INC-1FOAACONTH
5	1,009E-12	3,65	INC-D-C0008-05-01	1VR100291C	AHRECUPERA	C0008-05-03-PDA	INC-1FOAACONTH
6	1,005E-12	3,64	INC-D-C0008-05-01	1F2FEDYBLH	AHRECUPERA	C0008-05-03-PDA	INC-1FOAACONTH

MCS for CAC case INC-D-C0008-02-03 are different for both the reference and conversion model.

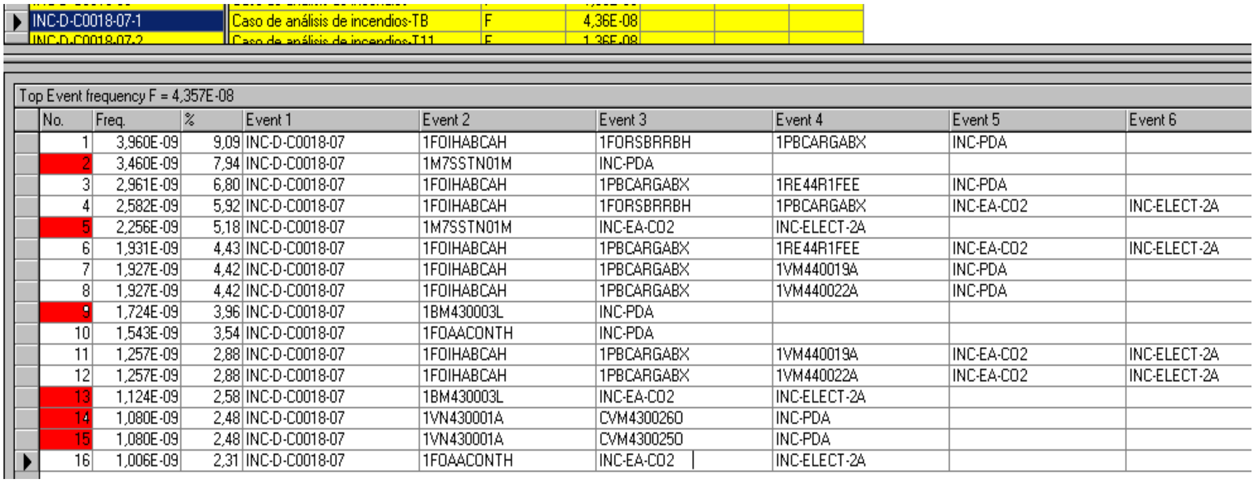


INC-D-C0003-30	Caso de análisis de incendios	F	2,65E-08			

Top Event frequency F = 2,653E-08

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4	Event 5	Event 6
1	1,941E-09	7,32	INC-D-C0003-30	1FOIHRECAH	AHRECUPERA	INC-FB-0	INC-PEA	INC-PS
2	1,549E-09	5,84	INC-D-C0003-30	1CBBV5B2F1F	AHRECUPERA	INC-FB-0	INC-PEA	INC-PS
3	1,549E-09	5,84	INC-D-C0003-30	1CBBV5B2F2F	AHRECUPERA	INC-FB-0	INC-PEA	INC-PS
4	1,549E-09	5,84	INC-D-C0003-30	1CBBVBL1F2F	AHRECUPERA	INC-FB-0	INC-PEA	INC-PS
5	1,549E-09	5,84	INC-D-C0003-30	1CBBVBL1RF	AHRECUPERA	INC-FB-0	INC-PEA	INC-PS
6	1,549E-09	5,84	INC-D-C0003-30	1CBBVBL1F1F	AHRECUPERA	INC-FB-0	INC-PEA	INC-PS
7	1,452E-09	5,47	INC-D-C0003-30	1RE140R2BE	AHRECUPERA	INC-FB-0	INC-PEA	INC-PS
8	1,452E-09	5,47	INC-D-C0003-30	1RE11R2CB07E	AHRECUPERA	INC-FB-0	INC-PEA	INC-PS
9	1,452E-09	5,47	INC-D-C0003-30	1RE140R1BE	AHRECUPERA	INC-FB-0	INC-PEA	INC-PS
10	1,294E-09	4,88	INC-D-C0003-30	1VM14010BA	AHRECUPERA	INC-FB-0	INC-PEA	INC-PS
11	1,294E-09	4,88	INC-D-C0003-30	1VM15001BA	AHRECUPERA	INC-FB-0	INC-PEA	INC-PS
12	1,242E-09	4,68	INC-D-C0003-30	1MCILRSABF	AHRECUPERA	INC-FB-0	INC-PEA	INC-PS
13	1,139E-09	4,29	INC-D-C0003-30	1VR140032C	AHRECUPERA	INC-FB-0	INC-PEA	INC-PS
14	1,062E-09	4,00	INC-D-C0003-30	1IH14P01BC	AHRECUPERA	INC-FB-0	INC-PEA	INC-PS

MCS for the reference model case INC-D-C0003-30. The coloured are the MCS for the conversion model.

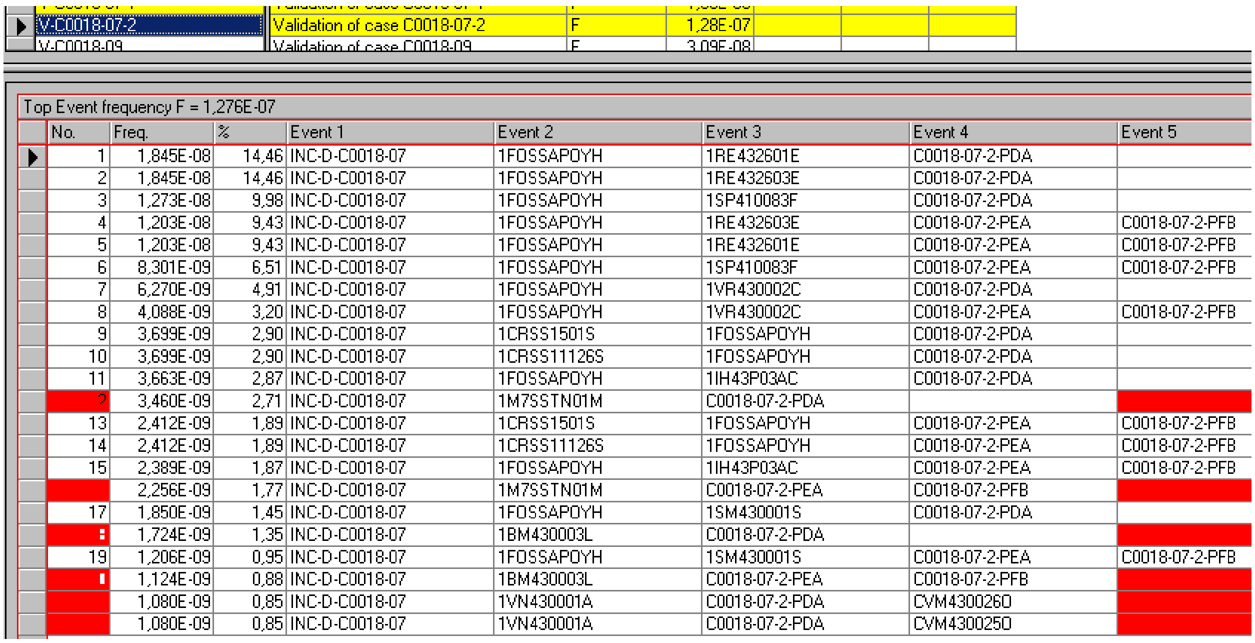


▶	INC-D-C0018-07-1	Caso de análisis de incendios-TB	F	4,36E-08		
	INC-D-C0018-07-2	Caso de análisis de incendios-T11	F	1,36E-08		

Top Event frequency F = 4,357E-08

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4	Event 5	Event 6
1	3,960E-09	9,09	INC-D-C0018-07	1FOIHABCAH	1FORSBRRBH	1PBCARGABX	INC-PDA	
🟥 2	3,460E-09	7,94	INC-D-C0018-07	1M7SSTN01M	INC-PDA			
3	2,961E-09	6,80	INC-D-C0018-07	1FOIHABCAH	1PBCARGABX	1RE44R1FEE	INC-PDA	
4	2,582E-09	5,92	INC-D-C0018-07	1FOIHABCAH	1FORSBRRBH	1PBCARGABX	INC-EA-CO2	INC-ELECT-2A
🟥 5	2,256E-09	5,18	INC-D-C0018-07	1M7SSTN01M	INC-EA-CO2	INC-ELECT-2A		
6	1,931E-09	4,43	INC-D-C0018-07	1FOIHABCAH	1PBCARGABX	1RE44R1FEE	INC-EA-CO2	INC-ELECT-2A
7	1,927E-09	4,42	INC-D-C0018-07	1FOIHABCAH	1PBCARGABX	1VM440019A	INC-PDA	
8	1,927E-09	4,42	INC-D-C0018-07	1FOIHABCAH	1PBCARGABX	1VM440022A	INC-PDA	
🟥 9	1,724E-09	3,96	INC-D-C0018-07	1BM430003L	INC-PDA			
10	1,543E-09	3,54	INC-D-C0018-07	1FOAACONTH	INC-PDA			
11	1,257E-09	2,88	INC-D-C0018-07	1FOIHABCAH	1PBCARGABX	1VM440019A	INC-EA-CO2	INC-ELECT-2A
12	1,257E-09	2,88	INC-D-C0018-07	1FOIHABCAH	1PBCARGABX	1VM440022A	INC-EA-CO2	INC-ELECT-2A
🟥 13	1,124E-09	2,58	INC-D-C0018-07	1BM430003L	INC-EA-CO2	INC-ELECT-2A		
🟥 14	1,080E-09	2,48	INC-D-C0018-07	1VN430001A	CVM4300260	INC-PDA		
🟥 15	1,080E-09	2,48	INC-D-C0018-07	1VN430001A	CVM4300250	INC-PDA		
16	1,006E-09	2,31	INC-D-C0018-07	1FOAACONTH	INC-EA-CO2	INC-ELECT-2A		

MCS for the reference model case INC-D-C0008-07-1. The coloured are the MCS for the conversion model

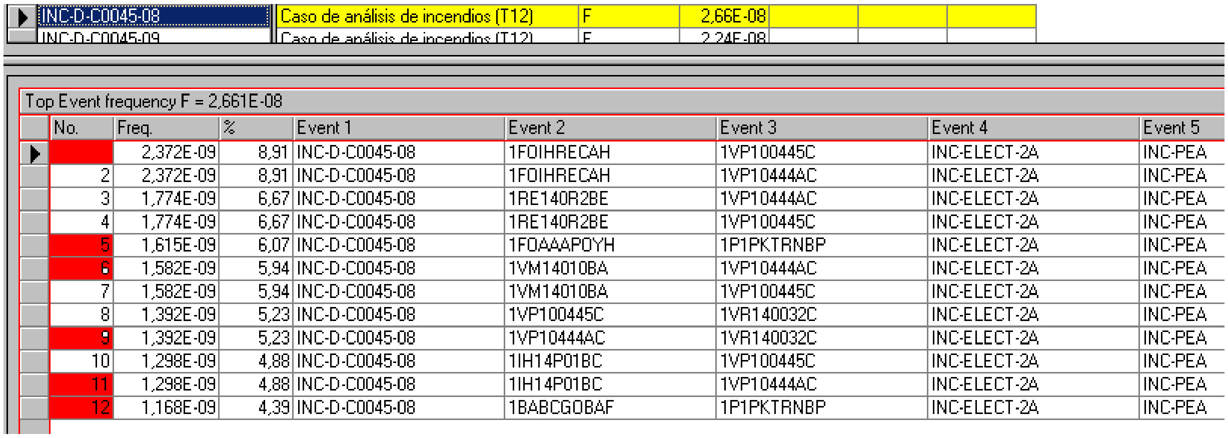


▶	V-C0018-07-2	Validation of case C0018-07-2	F	1,28E-07		
	V-C0018-09	Validation of case C0018-09	F	3,09E-08		

Top Event frequency F = 1,276E-07

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4	Event 5
1	1,845E-08	14,46	INC-D-C0018-07	1FOSSAPOYH	1RE432601E	C0018-07-2-PDA	
2	1,845E-08	14,46	INC-D-C0018-07	1FOSSAPOYH	1RE432603E	C0018-07-2-PDA	
3	1,273E-08	9,98	INC-D-C0018-07	1FOSSAPOYH	1SP410083F	C0018-07-2-PDA	
4	1,203E-08	9,43	INC-D-C0018-07	1FOSSAPOYH	1RE432603E	C0018-07-2-PEA	C0018-07-2-PFB
5	1,203E-08	9,43	INC-D-C0018-07	1FOSSAPOYH	1RE432601E	C0018-07-2-PEA	C0018-07-2-PFB
6	8,301E-09	6,51	INC-D-C0018-07	1FOSSAPOYH	1SP410083F	C0018-07-2-PEA	C0018-07-2-PFB
7	6,270E-09	4,91	INC-D-C0018-07	1FOSSAPOYH	1VR430002C	C0018-07-2-PDA	
8	4,088E-09	3,20	INC-D-C0018-07	1FOSSAPOYH	1VR430002C	C0018-07-2-PEA	C0018-07-2-PFB
9	3,699E-09	2,90	INC-D-C0018-07	1CRSS1501S	1FOSSAPOYH	C0018-07-2-PDA	
10	3,699E-09	2,90	INC-D-C0018-07	1CRSS11126S	1FOSSAPOYH	C0018-07-2-PDA	
11	3,663E-09	2,87	INC-D-C0018-07	1FOSSAPOYH	1IH43P03AC	C0018-07-2-PDA	
🟥 2	3,460E-09	2,71	INC-D-C0018-07	1M7SSTN01M	C0018-07-2-PDA		🟥
13	2,412E-09	1,89	INC-D-C0018-07	1CRSS1501S	1FOSSAPOYH	C0018-07-2-PEA	C0018-07-2-PFB
14	2,412E-09	1,89	INC-D-C0018-07	1CRSS11126S	1FOSSAPOYH	C0018-07-2-PEA	C0018-07-2-PFB
15	2,389E-09	1,87	INC-D-C0018-07	1FOSSAPOYH	1IH43P03AC	C0018-07-2-PEA	C0018-07-2-PFB
🟥	2,256E-09	1,77	INC-D-C0018-07	1M7SSTN01M	C0018-07-2-PEA	C0018-07-2-PFB	🟥
17	1,850E-09	1,45	INC-D-C0018-07	1FOSSAPOYH	1SM430001S	C0018-07-2-PDA	
🟥	1,724E-09	1,35	INC-D-C0018-07	1BM430003L	C0018-07-2-PDA		🟥
19	1,206E-09	0,95	INC-D-C0018-07	1FOSSAPOYH	1SM430001S	C0018-07-2-PEA	C0018-07-2-PFB
🟥	1,124E-09	0,88	INC-D-C0018-07	1BM430003L	C0018-07-2-PEA	C0018-07-2-PFB	🟥
🟥	1,080E-09	0,85	INC-D-C0018-07	1VN430001A	C0018-07-2-PDA	CVM4300260	🟥
🟥	1,080E-09	0,85	INC-D-C0018-07	1VN430001A	C0018-07-2-PDA	CVM4300250	🟥

MCS for the conversion model case V-c0018-07-2. The coloured are the MCS for the reference model with Event 5 missing.

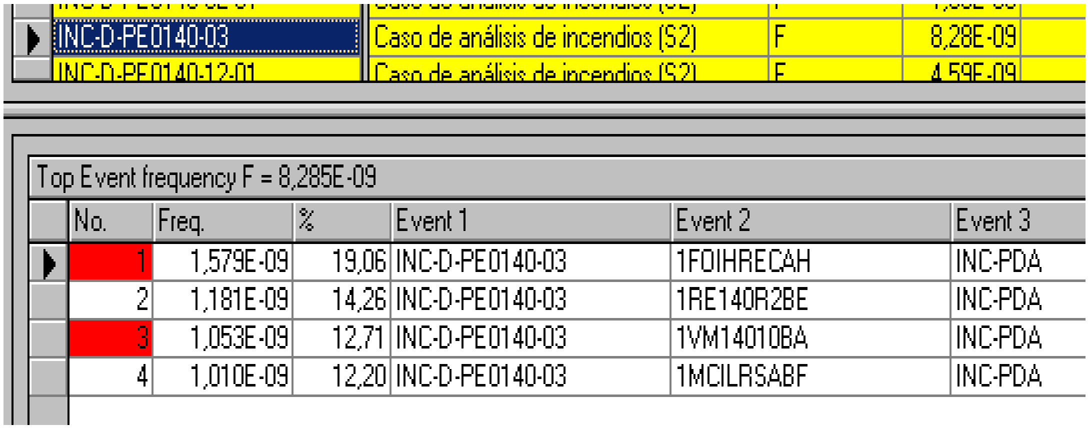


INC-D-C0045-08	Caso de análisis de incendios (T12)	F	2,66E-08		
INC-D-C0045-09	Caso de análisis de incendios (T12)	F	2,24E-08		

Top Event frequency F = 2,661E-08

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4	Event 5
🟥	2,372E-09	8,91	INC-D-C0045-08	1FOIHRECAH	1VP100445C	INC-ELECT-2A	INC-PEA
2	2,372E-09	8,91	INC-D-C0045-08	1FOIHRECAH	1VP10444AC	INC-ELECT-2A	INC-PEA
3	1,774E-09	6,67	INC-D-C0045-08	1RE140R2BE	1VP10444AC	INC-ELECT-2A	INC-PEA
4	1,774E-09	6,67	INC-D-C0045-08	1RE140R2BE	1VP100445C	INC-ELECT-2A	INC-PEA
🟥 5	1,615E-09	6,07	INC-D-C0045-08	1FOAAAPOYH	1P1PKTRNBP	INC-ELECT-2A	INC-PEA
🟥 6	1,582E-09	5,94	INC-D-C0045-08	1VM14010BA	1VP10444AC	INC-ELECT-2A	INC-PEA
7	1,582E-09	5,94	INC-D-C0045-08	1VM14010BA	1VP100445C	INC-ELECT-2A	INC-PEA
8	1,392E-09	5,23	INC-D-C0045-08	1VP100445C	1VR140032C	INC-ELECT-2A	INC-PEA
🟥 9	1,392E-09	5,23	INC-D-C0045-08	1VP10444AC	1VR140032C	INC-ELECT-2A	INC-PEA
10	1,298E-09	4,88	INC-D-C0045-08	1IH14P01BC	1VP100445C	INC-ELECT-2A	INC-PEA
🟥 11	1,298E-09	4,88	INC-D-C0045-08	1IH14P01BC	1VP10444AC	INC-ELECT-2A	INC-PEA
🟥 12	1,168E-09	4,39	INC-D-C0045-08	1BABCGOBAF	1P1PKTRNBP	INC-ELECT-2A	INC-PEA

MCS for the reference model case INC-D-C0045-08. The coloured are the MCS for the conversion model

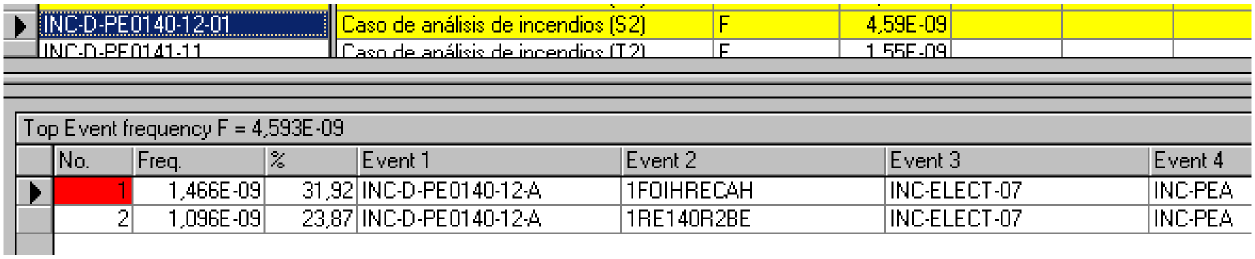


INC-D-PE0140-03	Caso de análisis de incendios (S2)	F	8,28E-09
INC-D-PE0140-12-01	Caso de análisis de incendios (S2)	F	4,59E-09

Top Event frequency F = 8,285E-09

No.	Freq.	%	Event 1	Event 2	Event 3
🟥 1	1,579E-09	19,06	INC-D-PE0140-03	1FOIHRECAH	INC-PDA
2	1,181E-09	14,26	INC-D-PE0140-03	1RE140R2BE	INC-PDA
🟥 3	1,053E-09	12,71	INC-D-PE0140-03	1VM14010BA	INC-PDA
4	1,010E-09	12,20	INC-D-PE0140-03	1MCILRSABF	INC-PDA

MCS for the reference model case INC-D-PE0140-03. The coloured are the MCS for the conversion model

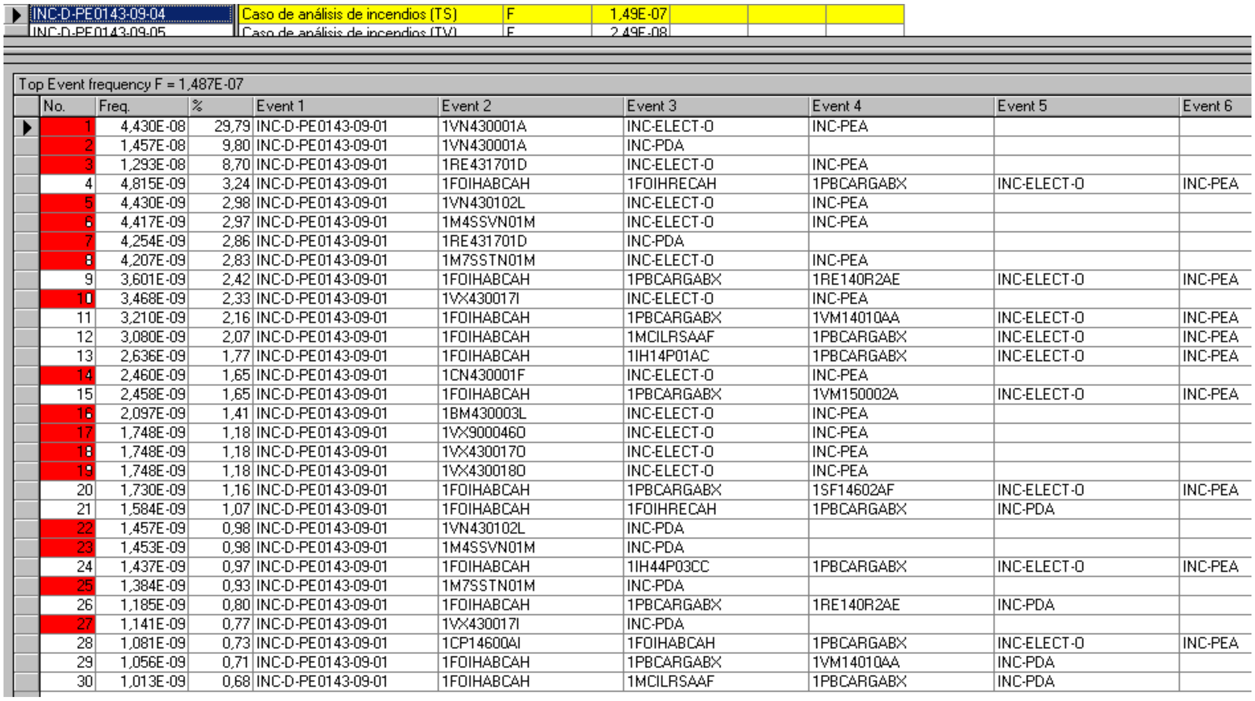


INC-D-PE0140-12-01	Caso de análisis de incendios (S2)	F	4,59E-09		
INC-D-PE0141-11	Caso de análisis de incendios (T2)	F	1,55E-09		

Top Event frequency F = 4,593E-09

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4
🟥 1	1,466E-09	31,92	INC-D-PE0140-12-A	1FOIHRECAH	INC-ELECT-07	INC-PEA
2	1,096E-09	23,87	INC-D-PE0140-12-A	1RE140R2BE	INC-ELECT-07	INC-PEA

MCS for the reference model case INC-D-PE0140-12-01. The coloured are the MCS for the conversion model

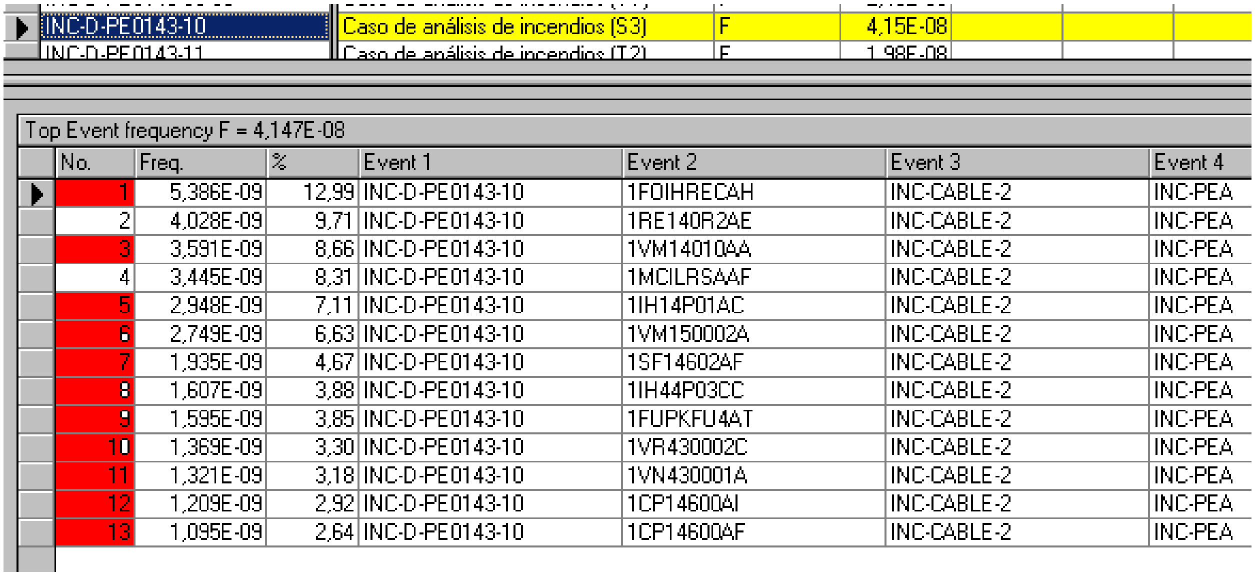


INC-D-PE0143-09-04	Caso de análisis de incendios (TS)	F	1,49E-07
INC-D-PE0143-09-05	Caso de análisis de incendios (TV)	F	2,49E-08

Top Event frequency F = 1,487E-07

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4	Event 5	Event 6
🟥 1	4,430E-08	29,79	INC-D-PE0143-09-01	1VN430001A	INC-ELECT-0	INC-PEA		
🟥 2	1,457E-08	9,80	INC-D-PE0143-09-01	1VN430001A	INC-PDA			
🟥 3	1,293E-08	8,70	INC-D-PE0143-09-01	1RE431701D	INC-ELECT-0	INC-PEA		
4	4,815E-09	3,24	INC-D-PE0143-09-01	1FOIHABCAH	1FOIHRECAH	1PBCARGABX	INC-ELECT-0	INC-PEA
🟥 5	4,430E-09	2,98	INC-D-PE0143-09-01	1VN430102L	INC-ELECT-0	INC-PEA		
🟥 6	4,417E-09	2,97	INC-D-PE0143-09-01	1M4SSVN01M	INC-ELECT-0	INC-PEA		
🟥 7	4,254E-09	2,86	INC-D-PE0143-09-01	1RE431701D	INC-PDA			
🟥 8	4,207E-09	2,83	INC-D-PE0143-09-01	1M7SSTN01M	INC-ELECT-0	INC-PEA		
9	3,601E-09	2,42	INC-D-PE0143-09-01	1FOIHABCAH	1PBCARGABX	1RE140R2AE	INC-ELECT-0	INC-PEA
🟥 10	3,468E-09	2,33	INC-D-PE0143-09-01	1VX430017I	INC-ELECT-0	INC-PEA		
11	3,210E-09	2,16	INC-D-PE0143-09-01	1FOIHABCAH	1PBCARGABX	1VM14010AA	INC-ELECT-0	INC-PEA
12	3,080E-09	2,07	INC-D-PE0143-09-01	1FOIHABCAH	1MCILRSAAF	1PBCARGABX	INC-ELECT-0	INC-PEA
13	2,636E-09	1,77	INC-D-PE0143-09-01	1FOIHABCAH	1IH14P01AC	1PBCARGABX	INC-ELECT-0	INC-PEA
🟥 14	2,460E-09	1,65	INC-D-PE0143-09-01	1CN430001F	INC-ELECT-0	INC-PEA		
15	2,458E-09	1,65	INC-D-PE0143-09-01	1FOIHABCAH	1PBCARGABX	1VM150002A	INC-ELECT-0	INC-PEA
🟥 16	2,097E-09	1,41	INC-D-PE0143-09-01	1BM430003L	INC-ELECT-0	INC-PEA		
🟥 17	1,748E-09	1,18	INC-D-PE0143-09-01	1VX9000460	INC-ELECT-0	INC-PEA		
🟥 18	1,748E-09	1,18	INC-D-PE0143-09-01	1VX4300170	INC-ELECT-0	INC-PEA		
🟥 19	1,748E-09	1,18	INC-D-PE0143-09-01	1VX4300180	INC-ELECT-0	INC-PEA		
20	1,730E-09	1,16	INC-D-PE0143-09-01	1FOIHABCAH	1PBCARGABX	1SF14602AF	INC-ELECT-0	INC-PEA
21	1,584E-09	1,07	INC-D-PE0143-09-01	1FOIHABCAH	1FOIHRECAH	1PBCARGABX	INC-PDA	
🟥 22	1,457E-09	0,98	INC-D-PE0143-09-01	1VN430102L	INC-PDA			
🟥 23	1,453E-09	0,98	INC-D-PE0143-09-01	1M4SSVN01M	INC-PDA			
24	1,437E-09	0,97	INC-D-PE0143-09-01	1FOIHABCAH	1IH44P03CC	1PBCARGABX	INC-ELECT-0	INC-PEA
🟥 25	1,384E-09	0,93	INC-D-PE0143-09-01	1M7SSTN01M	INC-PDA			
26	1,185E-09	0,80	INC-D-PE0143-09-01	1FOIHABCAH	1PBCARGABX	1RE140R2AE	INC-PDA	
🟥 27	1,141E-09	0,77	INC-D-PE0143-09-01	1VX430017I	INC-PDA			
28	1,081E-09	0,73	INC-D-PE0143-09-01	1CP14600AI	1FOIHABCAH	1PBCARGABX	INC-ELECT-0	INC-PEA
29	1,056E-09	0,71	INC-D-PE0143-09-01	1FOIHABCAH	1PBCARGABX	1VM14010AA	INC-PDA	
30	1,013E-09	0,68	INC-D-PE0143-09-01	1FOIHABCAH	1MCILRSAAF	1PBCARGABX	INC-PDA	

MCS for the reference model case INC-D-PE0143-09 04. The coloured are the MCS for the conversion model

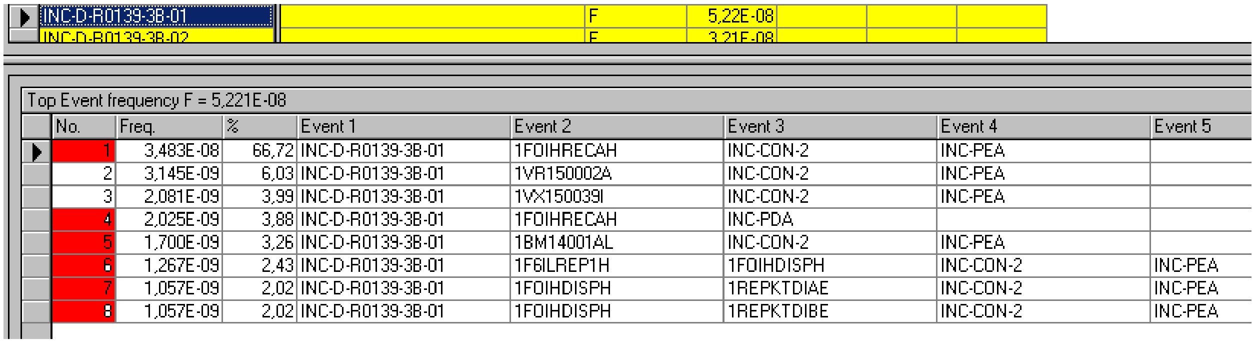


INC-D-PE0143-10	Caso de análisis de incendios (S3)	F	4,15E-08
INC-D-PE0143-11	Caso de análisis de incendios (T2)	F	1,98E-08

Top Event frequency F = 4,147E-08

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4
🟥 1	5,386E-09	12,99	INC-D-PE0143-10	1FOIHRECAH	INC-CABLE-2	INC-PEA
2	4,028E-09	9,71	INC-D-PE0143-10	1RE140R2AE	INC-CABLE-2	INC-PEA
🟥 3	3,591E-09	8,66	INC-D-PE0143-10	1VM14010AA	INC-CABLE-2	INC-PEA
4	3,445E-09	8,31	INC-D-PE0143-10	1MCILRSAAF	INC-CABLE-2	INC-PEA
🟥 5	2,948E-09	7,11	INC-D-PE0143-10	1IH14P01AC	INC-CABLE-2	INC-PEA
🟥 6	2,749E-09	6,63	INC-D-PE0143-10	1VM150002A	INC-CABLE-2	INC-PEA
🟥 7	1,935E-09	4,67	INC-D-PE0143-10	1SF14602AF	INC-CABLE-2	INC-PEA
🟥 8	1,607E-09	3,88	INC-D-PE0143-10	1IH44P03CC	INC-CABLE-2	INC-PEA
🟥 9	1,595E-09	3,85	INC-D-PE0143-10	1FUPKFU4AT	INC-CABLE-2	INC-PEA
🟥 10	1,369E-09	3,30	INC-D-PE0143-10	1VR430002C	INC-CABLE-2	INC-PEA
🟥 11	1,321E-09	3,18	INC-D-PE0143-10	1VN430001A	INC-CABLE-2	INC-PEA
🟥 12	1,209E-09	2,92	INC-D-PE0143-10	1CP14600AI	INC-CABLE-2	INC-PEA
🟥 13	1,095E-09	2,64	INC-D-PE0143-10	1CP14600AF	INC-CABLE-2	INC-PEA

MCS for the reference model case INC-D-PE0143-10. The coloured are the MCS for the conversion model

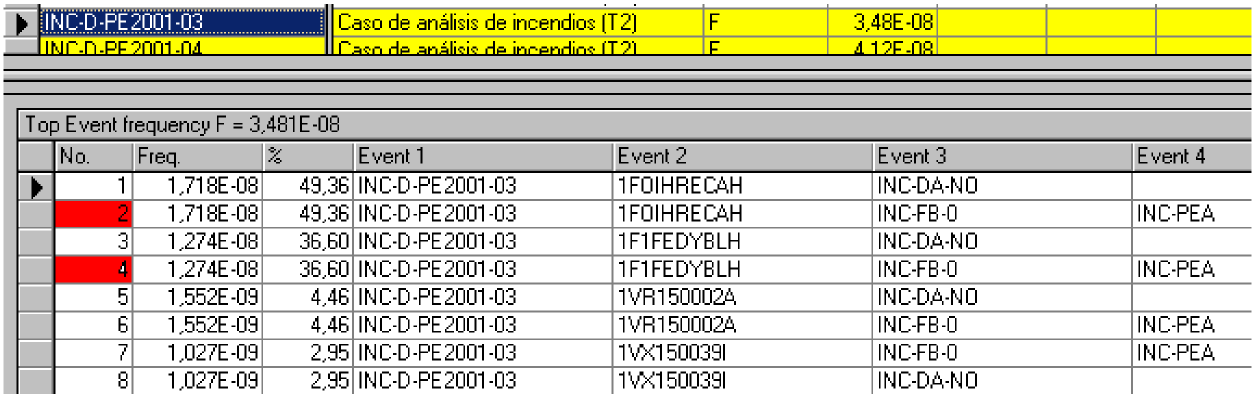


INC-D-R0139-3B-01		F	5,22E-08			
INC-D-R0139-3B-02		F	3,21E-08			

Top Event frequency F = 5,221E-08

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4	Event 5
🟥 1	3,483E-08	66,72	INC-D-R0139-3B-01	1FOIHRECAH	INC-CON-2	INC-PEA	
2	3,145E-09	6,03	INC-D-R0139-3B-01	1VR150002A	INC-CON-2	INC-PEA	
3	2,081E-09	3,99	INC-D-R0139-3B-01	1VX150039I	INC-CON-2	INC-PEA	
🟥 4	2,025E-09	3,88	INC-D-R0139-3B-01	1FOIHRECAH	INC-PDA		
🟥 5	1,700E-09	3,26	INC-D-R0139-3B-01	1BM14001AL	INC-CON-2	INC-PEA	
🟥 6	1,267E-09	2,43	INC-D-R0139-3B-01	1F6ILREP1H	1FOIHDISPH	INC-CON-2	INC-PEA
🟥 7	1,057E-09	2,02	INC-D-R0139-3B-01	1FOIHDISPH	1REPKTDIAE	INC-CON-2	INC-PEA
🟥 8	1,057E-09	2,02	INC-D-R0139-3B-01	1FOIHDISPH	1REPKTDIBE	INC-CON-2	INC-PEA

MCS for the reference model case INC-D-R0139-38-01. The coloured are the MCS for the conversion model

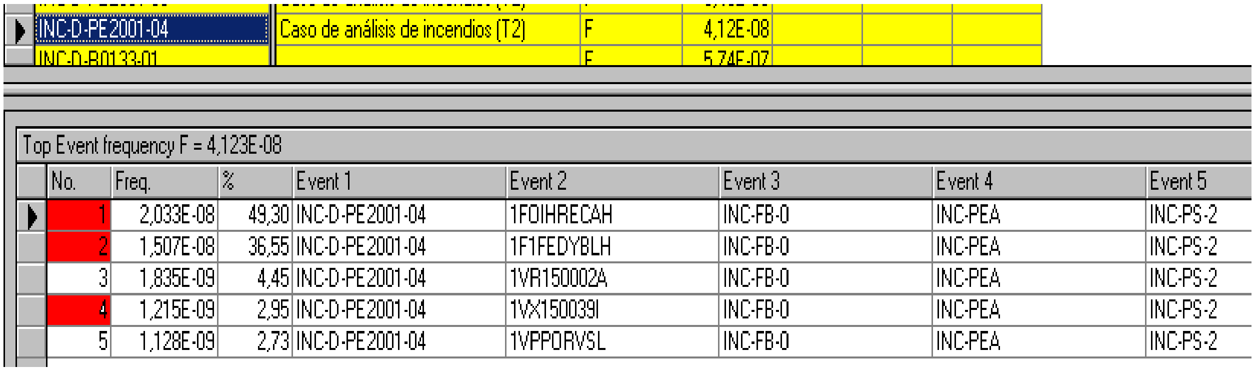


INC-D-PE2001-03	Caso de análisis de incendios (T2)	F	3,48E-08			
INC-D-PE2001-04	Caso de análisis de incendios (T2)	F	4,12E-08			

Top Event frequency F = 3,481E-08

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4
1	1,718E-08	49,36	INC-D-PE2001-03	1FOIHRECAH	INC-DA-NO	
🟥 2	1,718E-08	49,36	INC-D-PE2001-03	1FOIHRECAH	INC-FB-0	INC-PEA
3	1,274E-08	36,60	INC-D-PE2001-03	1F1FEDYBLH	INC-DA-NO	
🟥 4	1,274E-08	36,60	INC-D-PE2001-03	1F1FEDYBLH	INC-FB-0	INC-PEA
5	1,552E-09	4,46	INC-D-PE2001-03	1VR150002A	INC-DA-NO	
6	1,552E-09	4,46	INC-D-PE2001-03	1VR150002A	INC-FB-0	INC-PEA
7	1,027E-09	2,95	INC-D-PE2001-03	1VX150039I	INC-FB-0	INC-PEA
8	1,027E-09	2,95	INC-D-PE2001-03	1VX150039I	INC-DA-NO	

MCS for the reference model case INC-D-PE2001-03. The coloured are the MCS for the conversion model

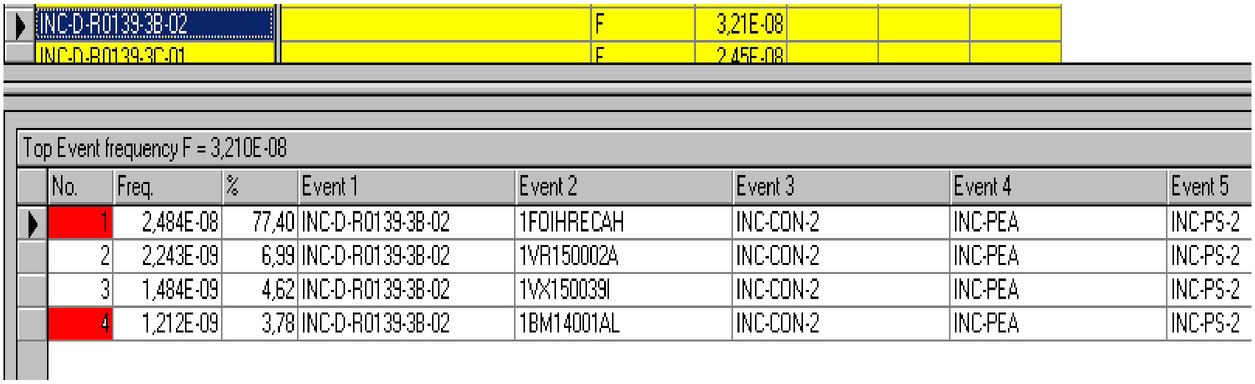


INC-D-PE2001-04	Caso de análisis de incendios (T2)	F	4,12E-08			
INC-D-R0133-01		F	5,74E-07			

Top Event frequency F = 4,123E-08

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4	Event 5
🟥 1	2,033E-08	49,30	INC-D-PE2001-04	1FOIHRECAH	INC-FB-0	INC-PEA	INC-PS-2
🟥 2	1,507E-08	36,55	INC-D-PE2001-04	1F1FEDYBLH	INC-FB-0	INC-PEA	INC-PS-2
3	1,835E-09	4,45	INC-D-PE2001-04	1VR150002A	INC-FB-0	INC-PEA	INC-PS-2
🟥 4	1,215E-09	2,95	INC-D-PE2001-04	1VX150039I	INC-FB-0	INC-PEA	INC-PS-2
5	1,128E-09	2,73	INC-D-PE2001-04	1VPPORVSL	INC-FB-0	INC-PEA	INC-PS-2

MCS for the reference model case INC-D-PE2001-04. The coloured are the MCS for the conversion model

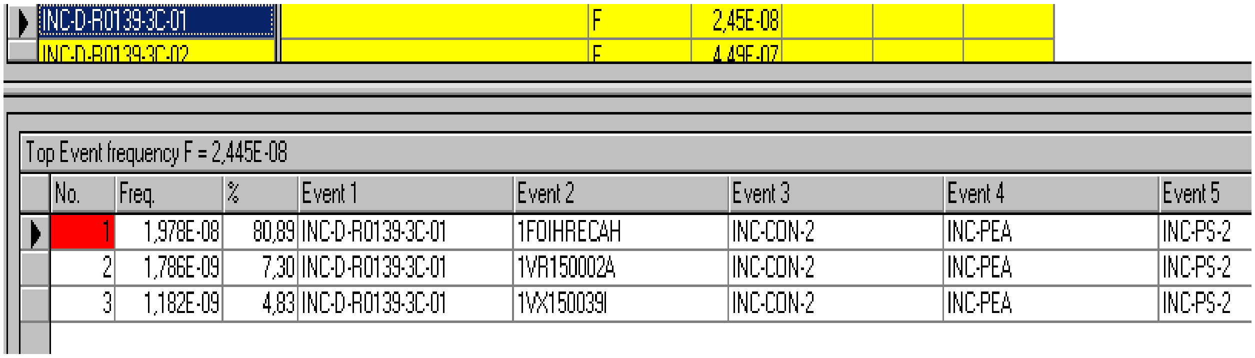


INC-D-R0139-3B-02		F	3,21E-08		
INC-D-R0139-3C-01		F	2,45E-08		

Top Event frequency F = 3,210E-08

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4	Event 5
1	2,484E-08	77,40	INC-D-R0139-3B-02	1FOIHRECAH	INC-CON-2	INC-PEA	INC-PS-2
2	2,243E-09	6,99	INC-D-R0139-3B-02	1VR150002A	INC-CON-2	INC-PEA	INC-PS-2
3	1,484E-09	4,62	INC-D-R0139-3B-02	1VX150039I	INC-CON-2	INC-PEA	INC-PS-2
4	1,212E-09	3,78	INC-D-R0139-3B-02	1BM14001AL	INC-CON-2	INC-PEA	INC-PS-2

MCS for the reference model case INC-D-R0139-38-02. The coloured are the MCS for the conversion model

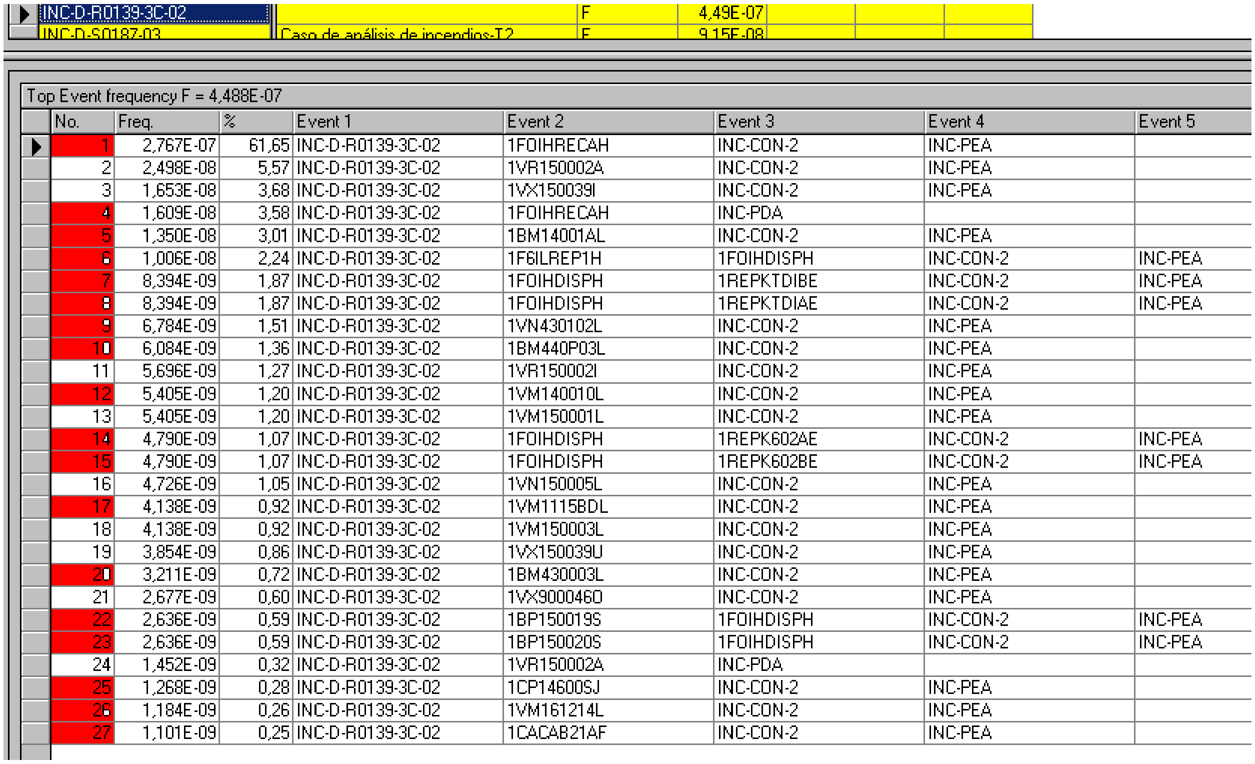


INC-D-R0139-3C-01		F	2,45E-08		
INC-D-R0139-3C-02		F	4,49E-07		

Top Event frequency F = 2,445E-08

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4	Event 5
1	1,978E-08	80,89	INC-D-R0139-3C-01	1FOIHRECAH	INC-CON-2	INC-PEA	INC-PS-2
2	1,786E-09	7,30	INC-D-R0139-3C-01	1VR150002A	INC-CON-2	INC-PEA	INC-PS-2
3	1,182E-09	4,83	INC-D-R0139-3C-01	1VX150039I	INC-CON-2	INC-PEA	INC-PS-2

MCS for the reference model case INC-D-R0139-3C-01. The coloured are the MCS for the conversion model

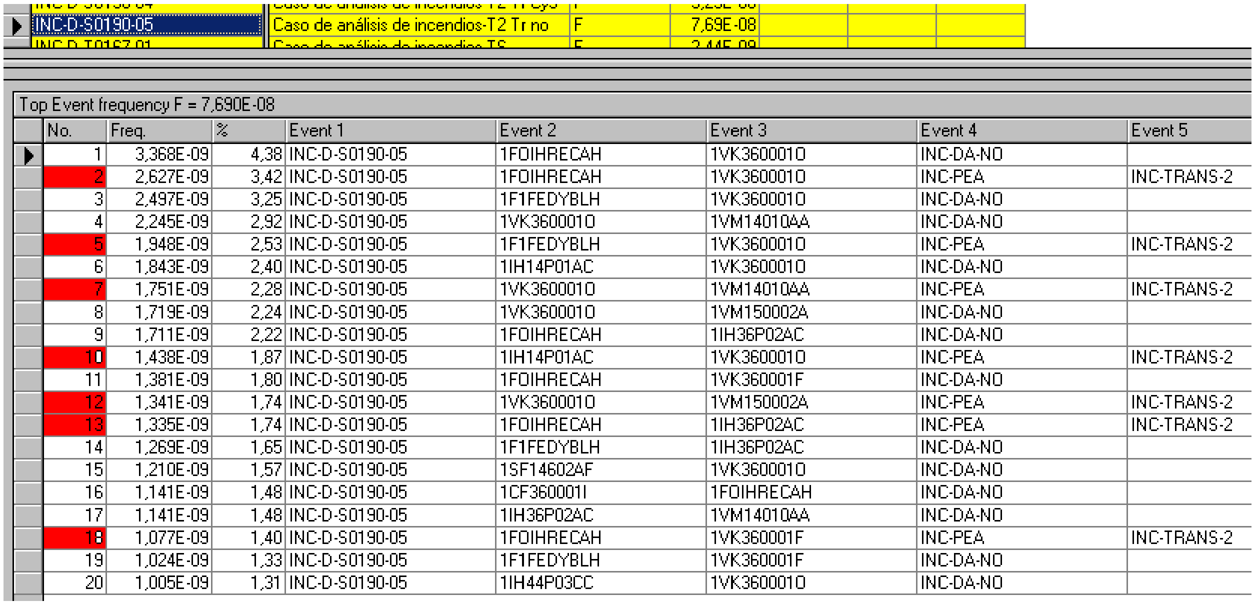


INC-D-R0139-3C-02		F	4,49E-07
INC-D-S0187-03	Caso de análisis de incendios-T2	F	9,15E-08

Top Event frequency F = 4,488E-07

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4	Event 5
🟥 1	2,767E-07	61,65	INC-D-R0139-3C-02	1FOIHRECAH	INC-CON-2	INC-PEA	
2	2,498E-08	5,57	INC-D-R0139-3C-02	1VR150002A	INC-CON-2	INC-PEA	
3	1,653E-08	3,68	INC-D-R0139-3C-02	1VX150039I	INC-CON-2	INC-PEA	
🟥 4	1,609E-08	3,58	INC-D-R0139-3C-02	1FOIHRECAH	INC-PDA		
🟥 5	1,350E-08	3,01	INC-D-R0139-3C-02	1BM14001AL	INC-CON-2	INC-PEA	
🟥 6	1,006E-08	2,24	INC-D-R0139-3C-02	1F6ILREP1H	1FOIHDISPH	INC-CON-2	INC-PEA
🟥 7	8,394E-09	1,87	INC-D-R0139-3C-02	1FOIHDISPH	1REPKTDIBE	INC-CON-2	INC-PEA
🟥 8	8,394E-09	1,87	INC-D-R0139-3C-02	1FOIHDISPH	1REPKTDIAE	INC-CON-2	INC-PEA
🟥 9	6,784E-09	1,51	INC-D-R0139-3C-02	1VN430102L	INC-CON-2	INC-PEA	
🟥 10	6,084E-09	1,36	INC-D-R0139-3C-02	1BM440P03L	INC-CON-2	INC-PEA	
11	5,696E-09	1,27	INC-D-R0139-3C-02	1VR150002I	INC-CON-2	INC-PEA	
🟥 12	5,405E-09	1,20	INC-D-R0139-3C-02	1VM140010L	INC-CON-2	INC-PEA	
13	5,405E-09	1,20	INC-D-R0139-3C-02	1VM150001L	INC-CON-2	INC-PEA	
🟥 14	4,790E-09	1,07	INC-D-R0139-3C-02	1FOIHDISPH	1REPK602AE	INC-CON-2	INC-PEA
🟥 15	4,790E-09	1,07	INC-D-R0139-3C-02	1FOIHDISPH	1REPK602BE	INC-CON-2	INC-PEA
16	4,726E-09	1,05	INC-D-R0139-3C-02	1VN150005L	INC-CON-2	INC-PEA	
🟥 17	4,138E-09	0,92	INC-D-R0139-3C-02	1VM1115BDL	INC-CON-2	INC-PEA	
18	4,138E-09	0,92	INC-D-R0139-3C-02	1VM150003L	INC-CON-2	INC-PEA	
19	3,854E-09	0,86	INC-D-R0139-3C-02	1VX150039U	INC-CON-2	INC-PEA	
🟥 20	3,211E-09	0,72	INC-D-R0139-3C-02	1BM430003L	INC-CON-2	INC-PEA	
21	2,677E-09	0,60	INC-D-R0139-3C-02	1VX900046O	INC-CON-2	INC-PEA	
🟥 22	2,636E-09	0,59	INC-D-R0139-3C-02	1BP150019S	1FOIHDISPH	INC-CON-2	INC-PEA
🟥 23	2,636E-09	0,59	INC-D-R0139-3C-02	1BP150020S	1FOIHDISPH	INC-CON-2	INC-PEA
24	1,452E-09	0,32	INC-D-R0139-3C-02	1VR150002A	INC-PDA		
🟥 25	1,268E-09	0,28	INC-D-R0139-3C-02	1CP14600SJ	INC-CON-2	INC-PEA	
🟥 26	1,184E-09	0,26	INC-D-R0139-3C-02	1VM161214L	INC-CON-2	INC-PEA	
🟥 27	1,101E-09	0,25	INC-D-R0139-3C-02	1CACAB21AF	INC-CON-2	INC-PEA	

MCS for the reference model case INC-D-R0139-3C-02. The coloured are the MCS for the conversion model

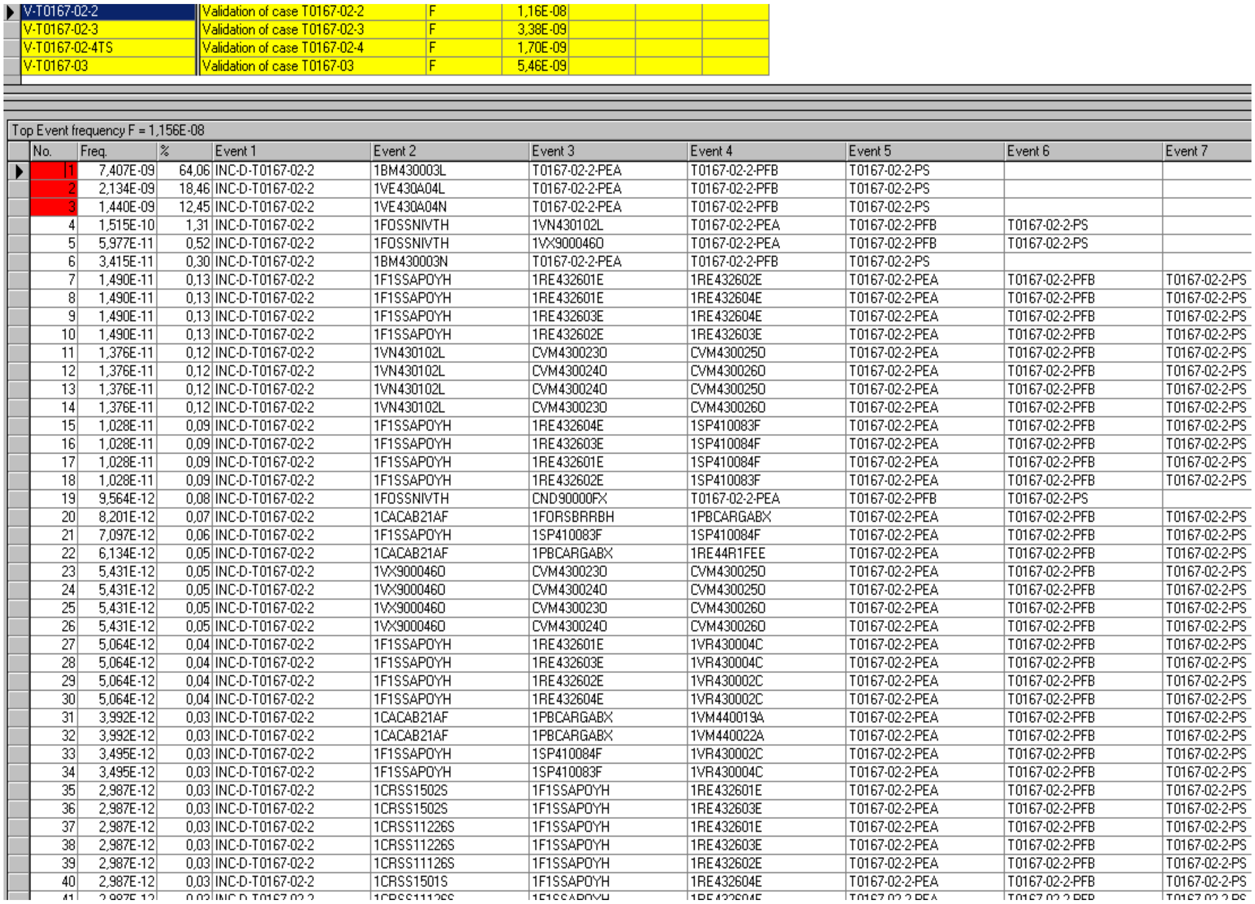


INC-D-S0190-05	Caso de análisis de incendios-T2 Tr no	F	7,69E-08

Top Event frequency F = 7,690E-08

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4	Event 5
1	3,368E-09	4,38	INC-D-S0190-05	1FOIHRECAH	1VK3600010	INC-DA-NO	
🟥 2	2,627E-09	3,42	INC-D-S0190-05	1FOIHRECAH	1VK3600010	INC-PEA	INC-TRANS-2
3	2,497E-09	3,25	INC-D-S0190-05	1F1FEDYBLH	1VK3600010	INC-DA-NO	
4	2,245E-09	2,92	INC-D-S0190-05	1VK3600010	1VM14010AA	INC-DA-NO	
🟥 5	1,948E-09	2,53	INC-D-S0190-05	1F1FEDYBLH	1VK3600010	INC-PEA	INC-TRANS-2
6	1,843E-09	2,40	INC-D-S0190-05	1IH14P01AC	1VK3600010	INC-DA-NO	
🟥 7	1,751E-09	2,28	INC-D-S0190-05	1VK3600010	1VM14010AA	INC-PEA	INC-TRANS-2
8	1,719E-09	2,24	INC-D-S0190-05	1VK3600010	1VM150002A	INC-DA-NO	
9	1,711E-09	2,22	INC-D-S0190-05	1FOIHRECAH	1IH36P02AC	INC-DA-NO	
🟥 10	1,438E-09	1,87	INC-D-S0190-05	1IH14P01AC	1VK3600010	INC-PEA	INC-TRANS-2
11	1,381E-09	1,80	INC-D-S0190-05	1FOIHRECAH	1VK360001F	INC-DA-NO	
🟥 12	1,341E-09	1,74	INC-D-S0190-05	1VK3600010	1VM150002A	INC-PEA	INC-TRANS-2
🟥 13	1,335E-09	1,74	INC-D-S0190-05	1FOIHRECAH	1IH36P02AC	INC-PEA	INC-TRANS-2
14	1,269E-09	1,65	INC-D-S0190-05	1F1FEDYBLH	1IH36P02AC	INC-DA-NO	
15	1,210E-09	1,57	INC-D-S0190-05	1SF14602AF	1VK3600010	INC-DA-NO	
16	1,141E-09	1,48	INC-D-S0190-05	1CF360001I	1FOIHRECAH	INC-DA-NO	
17	1,141E-09	1,48	INC-D-S0190-05	1IH36P02AC	1VM14010AA	INC-DA-NO	
🟥 18	1,077E-09	1,40	INC-D-S0190-05	1FOIHRECAH	1VK360001F	INC-PEA	INC-TRANS-2
19	1,024E-09	1,33	INC-D-S0190-05	1F1FEDYBLH	1VK360001F	INC-DA-NO	
20	1,005E-09	1,31	INC-D-S0190-05	1IH44P03CC	1VK3600010	INC-DA-NO	

MCS for the reference model case INC-D-S0190-05. The coloured are the MCS for the conversion model



V-T0167-02-2	Validation of case T0167-02-2	F	1,16E-08		
V-T0167-02-3	Validation of case T0167-02-3	F	3,38E-09		
V-T0167-02-4TS	Validation of case T0167-02-4	F	1,70E-09		
V-T0167-03	Validation of case T0167-03	F	5,46E-09		

Top Event frequency F = 1,156E-08

No.	Freq.	%	Event 1	Event 2	Event 3	Event 4	Event 5	Event 6	Event 7
1	7,407E-09	64,06	INC-D-T0167-02-2	1BM430003L	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS		
2	2,134E-09	18,46	INC-D-T0167-02-2	1VE430A04L	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS		
3	1,440E-09	12,45	INC-D-T0167-02-2	1VE430A04N	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS		
4	1,515E-10	1,31	INC-D-T0167-02-2	1FOSSNIVTH	1VN430102L	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS	
5	5,977E-11	0,52	INC-D-T0167-02-2	1FOSSNIVTH	1VX9000460	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS	
6	3,415E-11	0,30	INC-D-T0167-02-2	1BM430003N	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS		
7	1,490E-11	0,13	INC-D-T0167-02-2	1F1SSAPOYH	1RE432601E	1RE432602E	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
8	1,490E-11	0,13	INC-D-T0167-02-2	1F1SSAPOYH	1RE432601E	1RE432604E	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
9	1,490E-11	0,13	INC-D-T0167-02-2	1F1SSAPOYH	1RE432603E	1RE432604E	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
10	1,490E-11	0,13	INC-D-T0167-02-2	1F1SSAPOYH	1RE432602E	1RE432603E	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
11	1,376E-11	0,12	INC-D-T0167-02-2	1VN430102L	CVM4300230	CVM4300250	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
12	1,376E-11	0,12	INC-D-T0167-02-2	1VN430102L	CVM4300240	CVM4300260	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
13	1,376E-11	0,12	INC-D-T0167-02-2	1VN430102L	CVM4300240	CVM4300250	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
14	1,376E-11	0,12	INC-D-T0167-02-2	1VN430102L	CVM4300230	CVM4300260	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
15	1,028E-11	0,09	INC-D-T0167-02-2	1F1SSAPOYH	1RE432604E	1SP410083F	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
16	1,028E-11	0,09	INC-D-T0167-02-2	1F1SSAPOYH	1RE432603E	1SP410084F	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
17	1,028E-11	0,09	INC-D-T0167-02-2	1F1SSAPOYH	1RE432601E	1SP410084F	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
18	1,028E-11	0,09	INC-D-T0167-02-2	1F1SSAPOYH	1RE432602E	1SP410083F	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
19	9,564E-12	0,08	INC-D-T0167-02-2	1FOSSNIVTH	CND90000FX	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS	
20	8,201E-12	0,07	INC-D-T0167-02-2	1CACAB21AF	1FORSBRRBH	1PBCARGABX	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
21	7,097E-12	0,06	INC-D-T0167-02-2	1F1SSAPOYH	1SP410083F	1SP410084F	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
22	6,134E-12	0,05	INC-D-T0167-02-2	1CACAB21AF	1PBCARGABX	1RE44R1FEE	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
23	5,431E-12	0,05	INC-D-T0167-02-2	1VX9000460	CVM4300230	CVM4300250	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
24	5,431E-12	0,05	INC-D-T0167-02-2	1VX9000460	CVM4300240	CVM4300250	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
25	5,431E-12	0,05	INC-D-T0167-02-2	1VX9000460	CVM4300230	CVM4300260	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
26	5,431E-12	0,05	INC-D-T0167-02-2	1VX9000460	CVM4300240	CVM4300260	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
27	5,064E-12	0,04	INC-D-T0167-02-2	1F1SSAPOYH	1RE432601E	1VR430004C	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
28	5,064E-12	0,04	INC-D-T0167-02-2	1F1SSAPOYH	1RE432603E	1VR430004C	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
29	5,064E-12	0,04	INC-D-T0167-02-2	1F1SSAPOYH	1RE432602E	1VR430002C	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
30	5,064E-12	0,04	INC-D-T0167-02-2	1F1SSAPOYH	1RE432604E	1VR430002C	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
31	3,992E-12	0,03	INC-D-T0167-02-2	1CACAB21AF	1PBCARGABX	1VM440019A	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
32	3,992E-12	0,03	INC-D-T0167-02-2	1CACAB21AF	1PBCARGABX	1VM440022A	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
33	3,495E-12	0,03	INC-D-T0167-02-2	1F1SSAPOYH	1SP410084F	1VR430002C	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
34	3,495E-12	0,03	INC-D-T0167-02-2	1F1SSAPOYH	1SP410083F	1VR430004C	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
35	2,987E-12	0,03	INC-D-T0167-02-2	1CRSS1502S	1F1SSAPOYH	1RE432601E	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
36	2,987E-12	0,03	INC-D-T0167-02-2	1CRSS1502S	1F1SSAPOYH	1RE432603E	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
37	2,987E-12	0,03	INC-D-T0167-02-2	1CRSS11226S	1F1SSAPOYH	1RE432601E	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
38	2,987E-12	0,03	INC-D-T0167-02-2	1CRSS11226S	1F1SSAPOYH	1RE432603E	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
39	2,987E-12	0,03	INC-D-T0167-02-2	1CRSS11126S	1F1SSAPOYH	1RE432602E	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
40	2,987E-12	0,03	INC-D-T0167-02-2	1CRSS1501S	1F1SSAPOYH	1RE432604E	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS
41	2,987E-12	0,03	INC-D-T0167-02-2	1CRSS11126S	1F1SSAPOYH	1RE432604E	T0167-02-2-PEA	T0167-02-2-PFB	T0167-02-2-PS

MCS for the conversion model case V-T0167-02-2. The coloured are the MCS for the reference model