Hindawi
Science and Technology of Nuclear Installations
Volume 2022, Article ID 4666161, 15 pages
https://doi.org/10.1155/2022/4666161

Research Article

Investigation of Loss of Feedwater (LOFW) Accident in the APR-1400 Using Fault Tree Analysis

Muhammad Zubair [1,2]

[1]*Department of Mechanical & Nuclear Engineering, University of Sharjah, P. O. BOX 27272, Sharjah, UAE*
[2]*Nuclear Energy System Simulation and Safety Research Group, Research Institute of Sciences and Engineering, University of Sharjah, P.O. BOX 27272, Sharjah, UAE*

Correspondence should be addressed to Muhammad Zubair; zubairheu@gmail.com

Received 7 March 2022; Revised 25 April 2022; Accepted 4 May 2022; Published 26 May 2022

Academic Editor: Raffaella Testoni

Nuclear power plants play a significant role in the contribution of electricity generation on a global scale. Various reactor designs have advantages over others in different aspects. APR-1400 is a pressurized water reactor that is deemed safe due to the redundancy and independence of the multiple safety systems. Probabilistic safety assessment (PSA) is well known for its effectiveness in the representation of risk and safety analysis of the systems in a nuclear power plant. It provides different scenarios of system failure and accident progression via fault tree analysis. A loss of feedwater (LOFW) accident may occur due to numerous reasons such as spurious closure of valves, component failure of heaters, pumps, tanks, or a loss of offsite power (LOOP) event. In the present research, a methodology has been developed that aims to investigate different factors contributing to the loss of feedwater. This research also aims to analyze LOFW accidents by developing fault tree models for the main feedwater system of the APR-1400 to identify the basic events, which may lead to a loss of feedwater accidents. The results of the top event probabilities, risk decrease factor (RDF), risk increase factor (RIF), minimal cut sets (MCS), basic event probabilities, and sensitivity analysis were compared with the WASH-1400 database. It has been found that the control valve (V04) and main feedwater isolation valve (V05) have more contribution to the LOFW accident. The common cause failure (CCF) analysis has been carried out, and it was found that the flow toward the check valve and steam generator are most critical for CCF.

1. Introduction

Nuclear power plants are part of a vastly developing industry, currently responsible for 10% of the worldwide electricity from an aggregate of approximately 440 power reactors. Aside from delivering electricity with minimum carbon emission, nuclear reactors are utilized in the fields of medical and various other industries [1]. While nuclear energy is making a significant contribution globally, it possesses the potential to lead to a catastrophe given appropriate safety measures are not taken. Thus, power plants have adopted extensive safety features aiming to prevent adversities leading to a safe environment for the personnel and public using a tool called probabilistic safety assessment (PSA). Probabilistic safety assessment, also known as probabilistic risk assessment (PRA), is recognized as an evaluation tool to assess the risk of the occurrence of a combination of incidents that may lead to a catastrophic accident using the fault tree or event tree analyses. This methodology has been utilized for the assessment of nuclear reactors since the late 1970s and has since become widely applied to many fields other than the nuclear industry [2].

The PSA involved a comprehensive systems analysis that required much workforce and time in the early stages, so there is a need to develop a system network to support the analysts and enable levels 1, 2, and 3 of PSA with less human resources and more consistency. In level 1 PSA, the main target is identifying initiating events that can lead to core damage. For this purpose, different tests such as hazard and operability studies and failure mode analysis can identify

initiating events [3]. In level 2 PSA, the knowledge about severe accident and containment performance, offsite emergency planning evaluation, and plant-specific accident management development is essential. A level 3 PSA is needed when public safety criteria have been defined. In level 3 PSA radiation measurement, the effect of radiation on living things around the NPP and the protection of workers' health in the NPP area is significant.

Fault tree analysis is an efficient method that contributes to the understanding of the cause of an accident. It is a visual representation of the sequence of events that took place to lead up to the failure of a component or system, consisting of a top event, intermediate events, and cut sets. Cut sets are basic events that hold the capability to turn a particular sequence of events into an accident or failure of a system while minimal cut sets are the minimum accumulation of events that will certainly lead to an accident, and excluding a single event from the minimal cut set can prevent the accident from taking place. The fault tree is constructed of building blocks, which are inclusive of primary events, intermediate events, gates, and transfer symbols. Following the construction of a fault tree, it can be analyzed qualitatively to deduce the minimal cut sets [4].

Loss of coolant accidents (LOCAs) is a type of reactor accident in which the coolant is lost from the reactor. There are two types of LOCA:

(i) Large Break LOCA (LBLOCA): in which rapture happened in one of the main primary circuit coolant pipes serving the reactor pressure vessel. LBLOCAs are usually specified for a flow aperture that is greater than~0.1 m^2.

(ii) Small Break LOCA (SBLOCA): in which the rupture and thus the rate of coolant loss is much less significant than for the LBLOCA case. The flow area associated with the break is less than~0.1 m^2.

While the loss of feedwater (LOFW) event is an accident in which the main feedwater and auxiliary feedwater of the secondary side are not supplied to steam generators. It results in a reactor trip on high RCS pressure or low SG level. RCS temperature and pressurizer level will increase due to a reduction of heat transfer until a secondary heat sink is established. This is established by the emergency feedwater (EFW) automatically starting on a low SG level.

1.1. APR-1400 Safety Features. The Advanced Power Reactor 1400 MWe (APR-1400), owned and operated by the Korea Electric Power Corporation (KEPCO), is a third-generation nuclear reactor designed to be a new and improved version of the Optimum Power Reactor 1000 MWe, OPR-1000 [5, 6]. APR-1400 is aimed to have better characteristics such as higher electricity generation capacity and longer plant design lifetime. OPR-1000 has a rated capacity of 1000 MWe and a design lifetime of 40 years whereas APR-1400 can generate electricity up to 1400 MWe and its designed lifetime is extended to 60 years. This work aims to focus on developing a fault tree for a loss of feedwater accident in an APR-1400 system.

The APR1400 is a pressurized water reactor (PWR) with two coolant loops. The RCS circulates water in a closed cycle, removing heat from the reactor core and internals and transferring it to a secondary system. The reactor vessel, steam generators, reactor coolant pumps, pressurizer, and associated piping are the major components of the RCS. Two parallel heat transfer loops, each containing one steam generator and two reactor coolant pumps, are connected to the reactor vessel as shown in Figure 1. One pressurizer is connected to one of the reactor vessel's hot legs. All RCS components are located inside the reactor containment building [7, 8].

The primary circuit meets with the second loop of the reactor in the steam generator, where steam is generated in the shell side and transported to drive the turbine, converting mechanical energy to electricity in the generator. The steam is then cooled in the condenser, and the condensate flows through the feedwater system. The feedwater system is responsible for the circulation of feedwater from the condenser to the steam generators to maintain the water level.

The APR1400 architecture includes a reactor vessel, two parallel closed loops where each loop has one steam generator (SG) and two reactor coolant pumps (RCPs), and a pressurizer (PZR) coupled to a loop. Uranium dioxide pellets wrapped in fuel rods are used to power the reactor core. The core is made up of 241 fuel assemblies with varying levels of U-235 enrichment. According to the APR1400 design, the plant is designed to last 60 years without the need for a lengthy renovation. It is built to run on a fuel cycle, from postrefueling startup to the next postrefueling startup, with an 18-month refueling interval [9].

For regular operation, the APR1400 includes a two-loop, four RCP PWR, and active safety measures. It consists of a large, substantial reactor containment building and accompanying containment systems for heat removal and fission product retention during design basis events (DBEs) and beyond DBEs (BDBEs). It has at least two distinct and independent ac power connections to the grid to reduce the chances of losing offsite electricity (LOOP). The design includes an independent, safety-related, on-site ac power production source for each division as well as a non-safety-related, alternate ac (AAC) on-site power source to reduce the danger of a station blackout (SBO). FLEX equipment (water and electrical connections) can also be connected to BDBEs.

Safety Injection System (SIS), In-containment Refueling Water Storage Tank (IRWST), a Safety Depressurization and Vent System (SDVS), a Containment Spray System (CSS), and an Auxiliary Feed Water System (AFWS) make up the APR1400 reactor's safety systems. The APR1400 reactor's major design philosophy is simplicity and redundancy, which allows it to achieve higher reliability and performance than traditional facilities. The SIS is made up of two electrical divisions and four separate mechanical trains with no tie lines between the injection pathways. One passive Safety Injection Tank (SIT) and one active Safety Injection Pump (SIP) with a Fluidic Device are installed in each train (FD). The common header established in the SIS lines of the conventional plant has been removed to ensure the SIS's

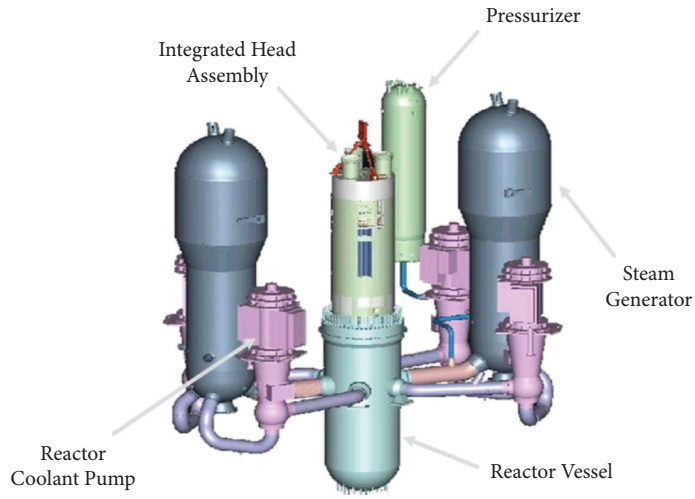

Figure 1: APR1400 reactor coolant system configuration [7].

simplicity and independence. The SIS and the Shutdown Cooling System (SCS) functions may be separated thanks to this design [10].

In the SIT, the FD, a passive flow regulator, is placed. The FD's main premise is vortex flow resistance. The standpipe, which is fitted in a rectangular direction with the exit nozzle, generates minimal resistance for the vortex and a high flow rate when water flows through it. When the water level falls below the stand pipe's top, the incoming flow is shifted to the control ports located in a tangential direction to the exit nozzle, resulting in significant vortex resistance and a low flow rate. The SIT quickly releases a considerable volume of water to fill the reactor vessel's lower plenum while the water level is above the standpipe. The SIT, on the other hand, injects a small volume of water over a lengthy period of time when the water level is below the standpipe. The FD put in the SIT replaces the low-pressure SIPs, resulting in the low-pressure SIP being eliminated.

The IRWST (In-containment Refueling Water Storage Tank) is positioned within the containment and is set up in such a manner that the injected emergency cooling water returns to it. In contrast to typical plants, this design eliminates the operator operation of switching SIP suction from the IRWST to the recirculating containment sump. IRWST's sensitivity to external threats is reduced because of its improved design. The IRWST serves as a reservoir for refueling water and a water supply for the SIS, a Shutdown Cooling System, and a Containment Spray System, which is a heat sink that condenses steam released from the pressurizer for quick depressurization if needed. This prevents high-pressure molten corium from escaping and allows for feed and bleed operations. For severe accidents, the IRWST also allows coolant to be fed to the cavity flooding system, which reduces molten corium concrete contact.

Recirculation modes of the traditional SIS, the high-pressure injection, and the low-pressure injection are integrated into one safety injection operation by using the advanced features of the FD in SIT and the IRWST. The SIS is made to enable safe water to be injected directly into the reactor vessel, preventing injected flow from being discharged through the damaged cold leg.

The Safety Depressurization and Vent System (SDVS) is a dedicated safety system designed to provide a safe means of depressurizing the reactor coolant system (RCS) during plant cooldown to cold shutdown if the pressurizer spray is unavailable and to rapidly depressurize the RCS to initiate the feed and bleed method of plant cooldown following total feedwater loss. Pilot Operated Safety Relief Valves (POSRVs) are used for feed and bleed operations. A flow line from the pressurizer steam space to the IRWST is established using this technology.

The Containment Spray System (CSS) comprises two trains and draws its pump's suction from the IRWST to lower containment temperature and pressure during containment incidents. The CSS is meant to work with the Shutdown Cooling System (SCS), which comprises two trains. These systems' pumps are all designed to be the same type and capacity. As a result of this design, the CSS has a better level of dependability than a traditional plant.

In the scenario that main feedwater is lost, the Auxiliary Feed Water System (AFWS) feeds feedwater to the steam generators (SGs) for RCS heat removal. It is divided into two divisions and four train systems. In addition, after a loss of coolant accident (LOCA), the AFWS replenishes the SGs to prevent leaking from preexisting tube leaks. The AFWS's dependability has been improved by employing two 100 percent motor-driven pumps, two 100 percent turbine-driven pumps, and two separate safety-related emergency feedwater storage tanks in the auxiliary building rather than the traditional condensate storage tank [11, 12].

1.2. Main Feedwater System. The main feedwater system is located outside the reactor building where it acts as a heat sink for the reactor core. It uses identical, redundant components or trains to ensure that system can actively function despite the failure of one of the components. This system also has the capability to isolate feedwater flow to one

or both steam generators following an accident. The main feedwater system consists of a deaerator storage tank, main feedwater isolation valves (MFIVs), feedwater check valves, feedwater control valve, a startup feedwater pump, motor-driven feedwater booster pumps, main feedwater pumps driven by a turbine, and high-pressure feedwater heaters. In this paper, it is assumed that the main feedwater system operates in full flow and at full power, with the consideration that there is no dependency on power level.

The process of condensation of steam leads to the condensate being incorporated with dissolved gases which may lead to corrosion of metallic components. Deaerators are thus employed to liberate gases from the water while also increasing the temperature of water to increase the thermal efficiency of the plant. The condensate is drained out to the deaerator storage tanks and the gases are vented out to the atmosphere [13].

The three feedwater booster pumps are motor-driven pumps responsible for pumping water from the deaerator storage tank to the suction of its corresponding main feedwater pump. The booster pumps are parallel, and each pump is followed by the main feedwater pump. A continuous flow of feedwater is ensured amidst the pumps with no isolation valve in between.

The three turbine-driven main feedwater pump delivers water from the booster pump to the two steam generators in the plant, through a series of high-pressure feedwater heaters. Each set of pumps is a combination of a booster pump and the main feedwater pump. Three identical main pumps are aligned in a parallel arrangement (A, B, and C) where each main feedwater pump supplies water from its associated booster pump, discharging to the high-pressure feedwater heaters. A check valve is located at the end of each set of feedwater pumps.

The purpose of a high-pressure (HP) feedwater heater is to preheat the feedwater before going to the steam generator to increase the thermodynamic efficiency of the plant. Two trains of HP feedwater heaters (A and B) operate in parallel where feedwater goes through three stages of heaters in each train (Heaters no. 5, 6, and 7). Feedwater drains from the higher pressure heaters into the lower pressure heaters and eventually drains into the deaerator. In addition to that, a motor-operated inlet and outlet isolation valve is equipped on either side of each HP feedwater heater train. A bypass line is also provided, which contains an isolation valve to ensure the continuous flow of feedwater in case of failure of a single component, which leads to the whole train being isolated.

A motor-driven startup pump is operated in case of a startup or shutdown to take suction of water out of the deaerator storage tanks into the two steam generators. It is generally on standby throughout normal operation.

Feedwater control valves are utilized to maintain and regulate the flow of feedwater into the steam generators. When a main steam isolation signal (MSIS) is received, the feedwater control valves are capable of closing in five seconds.

Two main feedwater isolation valves, which are hydraulically operated, are arranged in series and are situated as nearest as practicable to the containment, outside the reactor building. In case of an accident when MSIS is received, MFIVs can completely cut off the feedwater flow and isolate the feedwater system in a span of five seconds.

Feedwater check valves are designed to prevent the reverse flow of feed water from the steam generator in the event of a pump trip. A couple of feedwater check valves, placed in a series arrangement, are located directly before the steam generator to prevent the steam generators from becoming void of water in case of a pipe break in the feedwater system [14, 15]. A simplified diagram of the main feedwater system is illustrated in Figure 2.

2. Methodology

A nuclear reactor comprises a variety of mechanical systems, all of which are prone to accidents. Therefore, PSA is performed which conducts a safety analysis to assess the probability of occurrence of accidents due to each component or system and the combination of events that may lead to an accident along with the consequences. In this work, the probabilities of accidents in the main feedwater system are analyzed in an APR-1400 system which will lead to the loss of feedwater. Multiple factors in the system may contribute to causing a LOFW accident which can be brought down to a break in the feedwater line, valve malfunction, failure of pump operation, or loss of offsite power, as represented in Figure 3 [16].

A pipe break can refer to a partial or complete cleavage of the pipe which leads to the loss of feedwater from the system [17]. Following a break, the water flow to the steam generator will reduce, and eventually, the steam generator will show a signal indicating a low water level, which will cause the reactor to trip. The cause for rupture in the pipe can be attributed to features of the material used and the surrounding conditions of the pipe [18].

The valves present in the main feedwater lines allow for the flow of feedwater in a single direction, toward the steam generator. In case of failure of the control system to open a valve, the flow rate will gradually decrease or be terminated entirely [19].

A trip in any of the feedwater pumps responsible for circulating water through the system can disrupt the flow. The failure of the main feedwater pump causes the shutdown of its associated booster pump and vice versa [20].

A nuclear reactor is heavily dependent on electrical systems to run the power plant. Hence, all systems are secured to avert accidents through independent and redundant systems. The electrical system is supplied by the power transmission system that is responsible for transmitting offsite power to the nuclear power plant for the proper functioning of power-dependent systems. In case of loss of offsite power (LOOP event), the plant uses up power from emergency diesel generators. A station blackout is an accident scenario where offsite power is lost in addition to all alternate systems [21, 22].

The preceding causes are all major factors contributing to accidents related to the loss of feedwater. An area of the study of the first level of PSA was conducted using

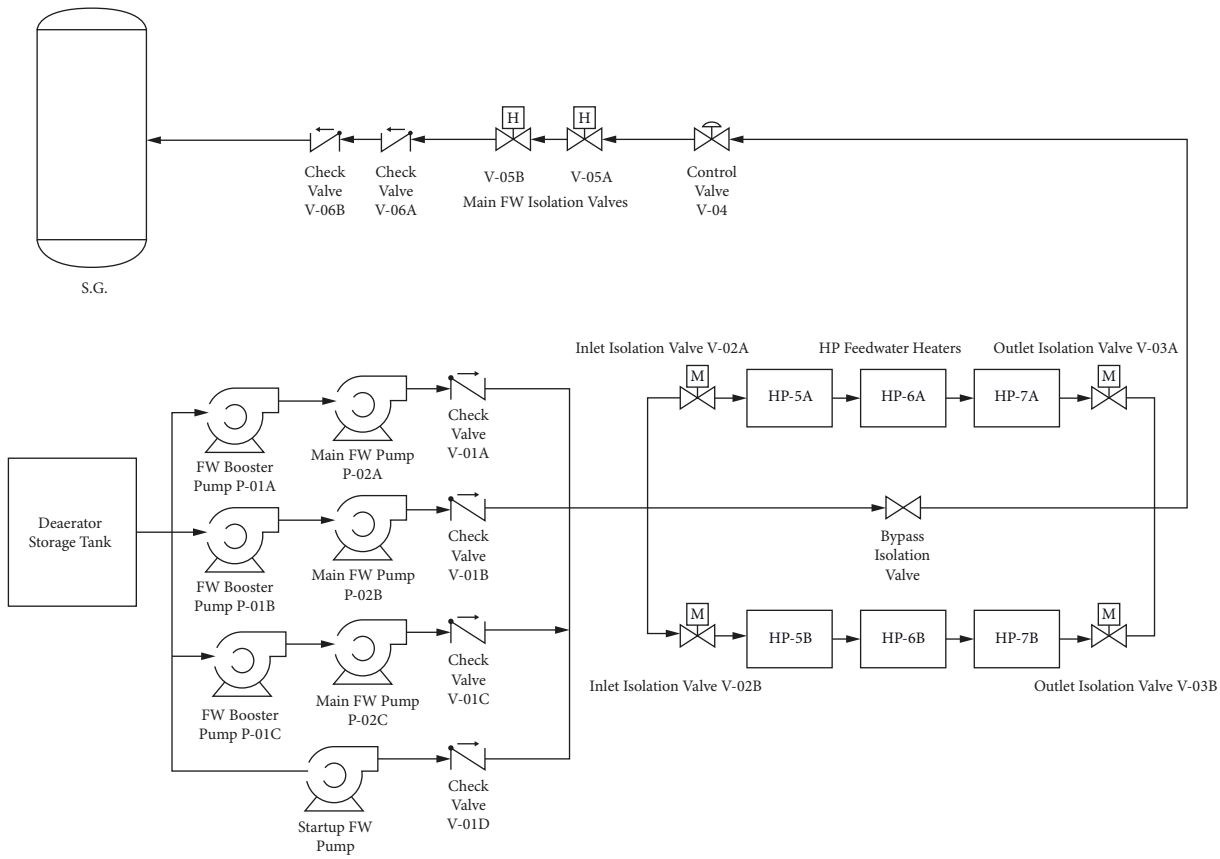

Figure 2: Simplified diagram of the main feedwater system.

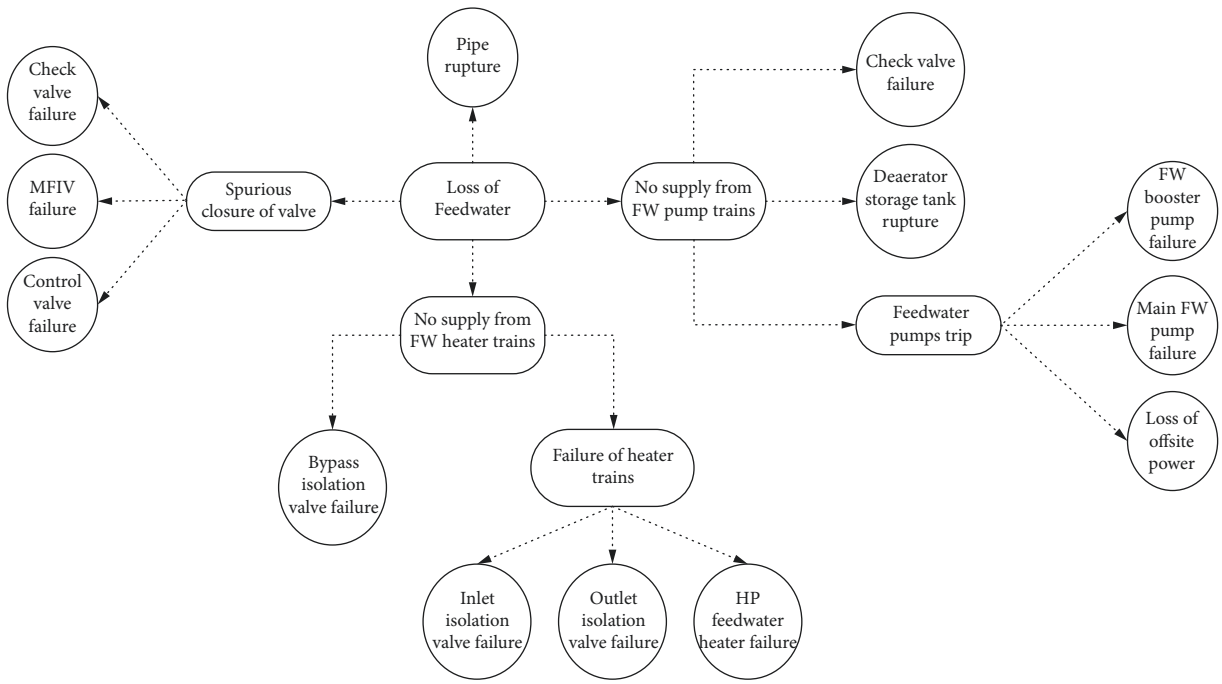

Figure 3: Factors contributing to the loss of feedwater.

RiskSpectrum Analysis Tools (RSATs) utilizing fault trees. RSAT is a software widely employed to implement reliability and safety analysis within and beyond the nuclear industry using various tools such as fault trees and event trees. [23]. Along with the calculation of the top event probability, it allows analyzing several aspects of the reliability study, in particular:

(1) Minimal cut set (MCS) analysis

(2) Uncertainty analysis

(3) Importance/Sensitivity analysis

(4) Time-dependent analysis

Calculation of the top event probability for the fault trees can be performed by assigning a failure probability to each basic event, after which the gates will be replaced with their corresponding Boolean algebraic function. The unit of failure probability of an event is generally categorized in two ways: time related or on demand.

Time-related failure is used when failure of a component or system occurs during continuous operation while failure on demand is applied in case of failure when a component or system functions on demand.

The failure rate of a component can be defined using

$$\lambda(t) = \frac{f(t)}{1 - F(t)}, \tag{1}$$

where $f(t)$ is the probability density of failure and $1 - F(t)$ is the probability that the device was successful until time t.

In the case of time-related failures, since the failure can occur at any time during the operation of the device, it is known to be independent of time where the failure rate is given in

$$\lambda = \frac{n}{T}, \tag{2}$$

where λ is the total failure rate per unit time, n is the number of failures, and T is the total operating time of the device.

Failures on demand are generally used when a device is on standby mode and is operated on demand. It is also described as unavailability which is divided into two elements, standby and demand unavailability. The standby unavailability, denoted as Q_s, is dependent on the number of demands in the time intervals between the operations of the device. It is given by

$$Q_s = \frac{\lambda_s / T_T}{2}, \tag{3}$$

where λ_s is the standby failure rate while in the dormant mode, and T_T is the time period between successive demands.

Demand unavailability is calculated using

$$Q_d = \frac{n_d}{d}, \tag{4}$$

where n_d is the sum of failures to operate the device on demand, and d is the number of failures. The sum of standby unavailability and demand unavailability gives the total unavailability of a component or system [24]. The two unavailability contributions of equations (3) and (4) together are combined to provide the total unavailability (failures per demand). $Q = Q_d + Q_s$, of a standby component.

The risk decrease factor (RDF) for a basic event with the probability Qi is calculated using

$$\text{RDF} = \frac{Q\text{Top}}{Q\text{Top}\,(Qi = 0)}, \tag{5}$$

where QTop is the top event probability and QTop ($Qi = 0$) is the top event result when the basic event Qi is perfectly reliable.

The risk increase factor (RIF) for a basic event with the probability Qi is calculated using

$$\text{RDF} = \frac{Q\text{Top}\,(Qi = 1)}{Q\text{Top}}, \tag{6}$$

where QTop is the top event probability and QTop ($Qi = 1$) is the top event result when the basic event Qi is certainly failed.

Data collected from the different sources were modeled in the RiskSpectrum software to obtain a top event probability from each source. The basic event probabilities used, given in Table 1, are plotted in Figure 4 to show the difference in the magnitudes. The figure illustrates that the data collected in the present research from U.S. NRC/IAEA and WASH-1400 databases are mostly similar except for a few components. The difference can be explained due to assumptions about the system boundaries made in the databases regarding each component.

When taking the failure probability of a component/system into consideration, the system boundary determines to what extent the component/system would be considered. For example, according to the IAEA document, the component boundary for the motor-operated control valve included the valve, motor, controls, relays, protection, logic, and automation. However, in the case of the WASH-1400 report, the probability for only a motor-operated valve was reported, due to which the failure probability is much smaller in magnitude for the latter report.

Quantification of a fault tree can be performed using several methods, one of which is using the failure probability of the basic events to obtain the top event failure probability. Failure probability indicates the unreliability of the specified component or event. The failure probabilities of individual components related to the main feedwater system were taken from NUREG-6928 and IAEA-478, which are documentations of data regarding pressurized water reactors, collected from the U.S. Nuclear Regulatory Commission (U.S. NRC) and International Atomic Energy Agency (IAEA), respectively. The probabilities collected are documented in Table 1 [25–27]. The top event probability calculated by the software was validated by modeling an identical fault tree and utilizing the data collected from WASH-1400, a reactor safety study report, for comparison of results from the two databases [28, 29]. The units for the mean component failure rates are given in per hour (h-1) and the demand probabilities are given in per demand (d-1).

Table 1: Component unreliability of the main feedwater system.

Basic event	Component code	NUREG-6928 /IAEA-478 Mean	WASH-1400 Mean
Check valve fails to open	A, AI, AH, F, K, P	$1.30E-05$/d	$1.00E-04$/d
Control valve fails to open	AE	$2.50E-02$/d	$1.00E-03$/d
HP feedwater heater failure	AA, AB, T, V, W, Y	$1.30E-05$/h	$7.10E-04$/h
Hydraulically operated MFIV fails to open	AF, AG	$1.51E-03$/d	$3.00E-04$/d
Large leak from the deaerator storage tank	B	$2.75E-09$/h	$1.00E-10$/h
Motor-driven booster pump fails to run	D, I, N	$4.54E-06$/h	$3.00E-05$/h
Motor-driven bypass line isolation valve fails to open	AD	$1.07E-03$/d	$1.00E-03$/d
Motor-driven inlet isolation valve fails to open	U, Z	$1.07E-03$/d	$1.00E-03$/d
Motor-driven outlet isolation valve fails to open	AC, X	$1.07E-03$/d	$1.00E-03$/d
Motor-driven startup pump fails to start	S	$2.23E-03$/d	$1.00E-03$/d
Pipe rupture >3″ in diameter	AJ	$1.00E-10$/h	$1.00E-10$/h
Total loss of offsite power	C	$4.10E-06$/h	$1.00E-05$/d
Turbine-driven main feedwater pump fails to run	E, J, O	$5.77E-06$/h	$3.00E-05$/h

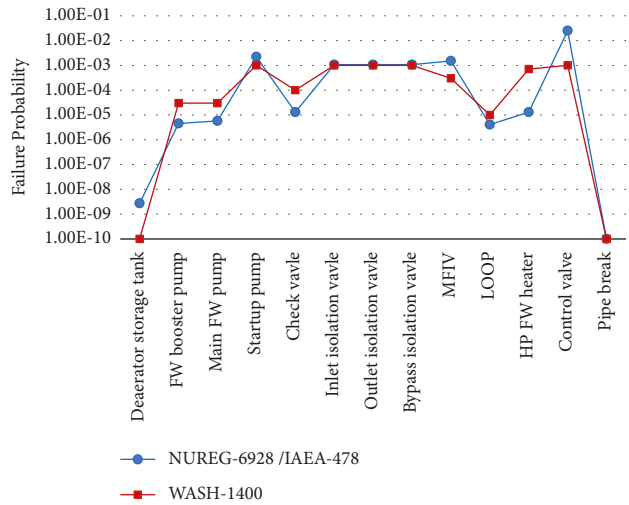

Figure 4: Comparison of basic event probabilities.

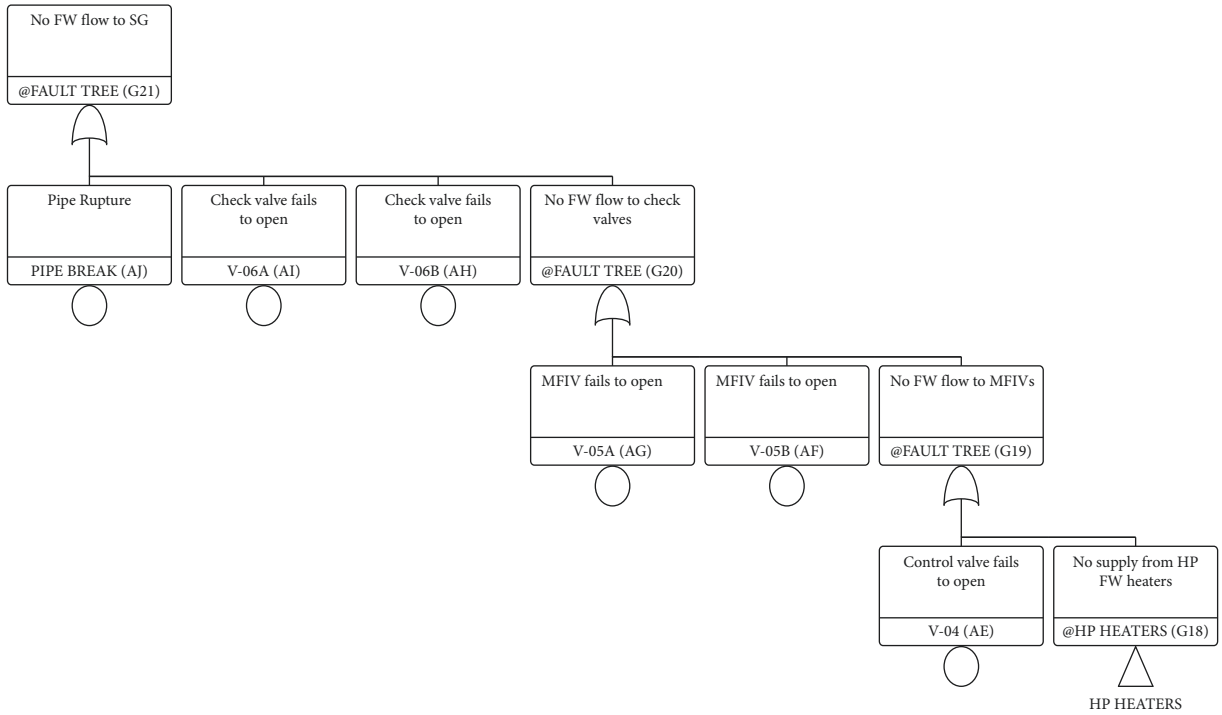

Figure 5: Fault tree for main feedwater system.

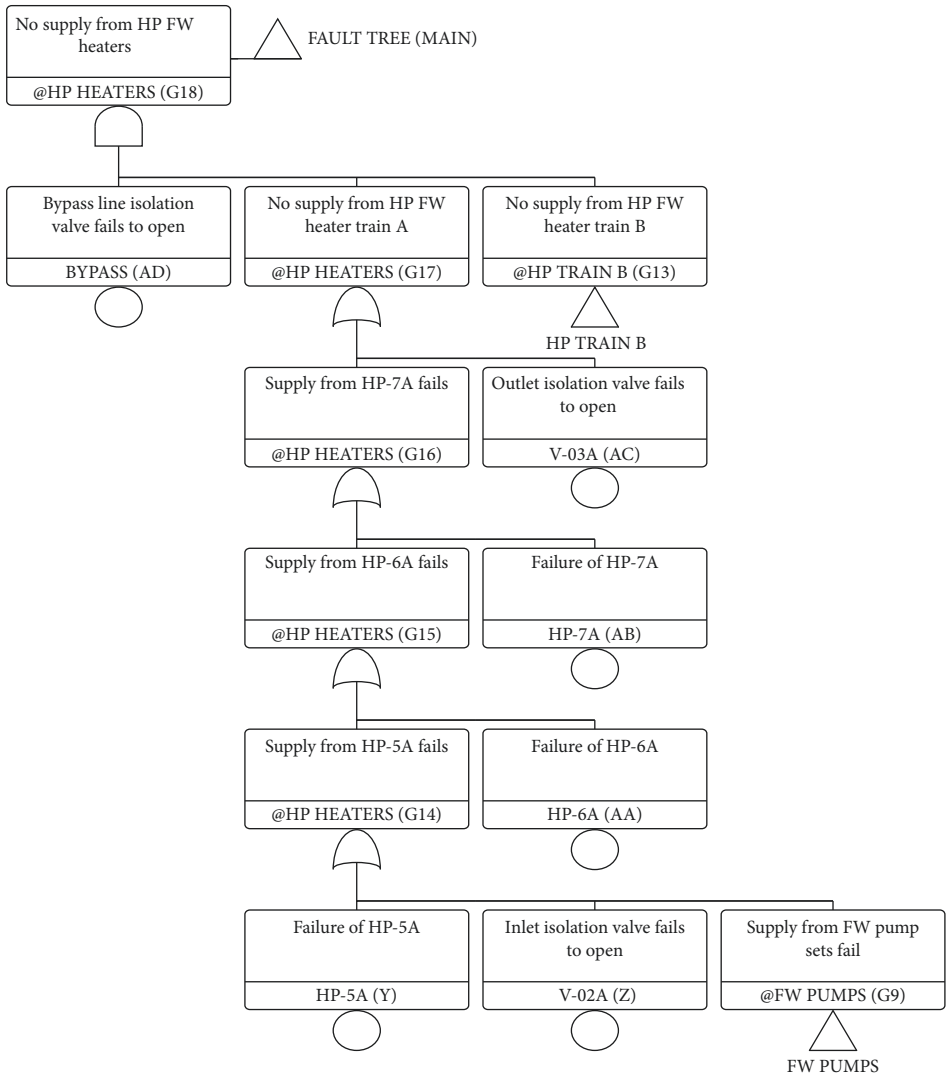

Figure 6: Fault tree for HPFW heaters.

3. Results and Discussion

The following figures show show the constructed fault tree representing the different causes of a loss of feedwater accident. Figure 5 shows the top event and addresses the malfunction of valves located before the steam generator, and it continues in Figure 6 through the transfer symbol. It considers a pipe break downstream of the check valves, spurious closure of the two check valves, and a couple of main feedwater isolation valves or the control valve. Figures 6 and 7 focus on feedwater supply from the two trains of HP feedwater heaters which may include the closure of the bypass isolation valve, the outlet or inlet isolation valves, or the failure of one of the three functioning heaters. Figure 8 directs the fault tree toward the feedwater pump trains. Figures 9–12 are continuations of the fault tree that discusses the various reasons for the failure of supply from the trains of feedwater pumps. Figures 9–11 consider the feedwater pump trains A, B, and, C, respectively, while Figure 12 reviews the startup pump train which remains on standby throughout normal operation. The above-mentioned fault trees address the failure of the check valve to open, a large leak in the deaerator storage tank, pump trip, or loss of offsite power. The fault trees were constructed assuming only the main feedwater system is considered, and a single-component failure takes place while the plant is under normal operation. In the case of single-component failure, it is assumed that the system will function despite the failure of a single component. Considering support systems or other system interconnections in the modeled fault tree would result in an increase in the top event probability. The single failure criterion is applied to determine the availability of systems and components. This criterion stipulates that the safety systems should be able to perform their specified functions when any single failure occurs. A failure should be assumed in the system or component that would have the largest negative effect on the calculated safety parameter.

In the model of the main feedwater system in RiskSpectrum, the top event considered was the loss of feedwater which returned a failure probability for a LOFW accident. The results of running the MCS analysis showed a simulated

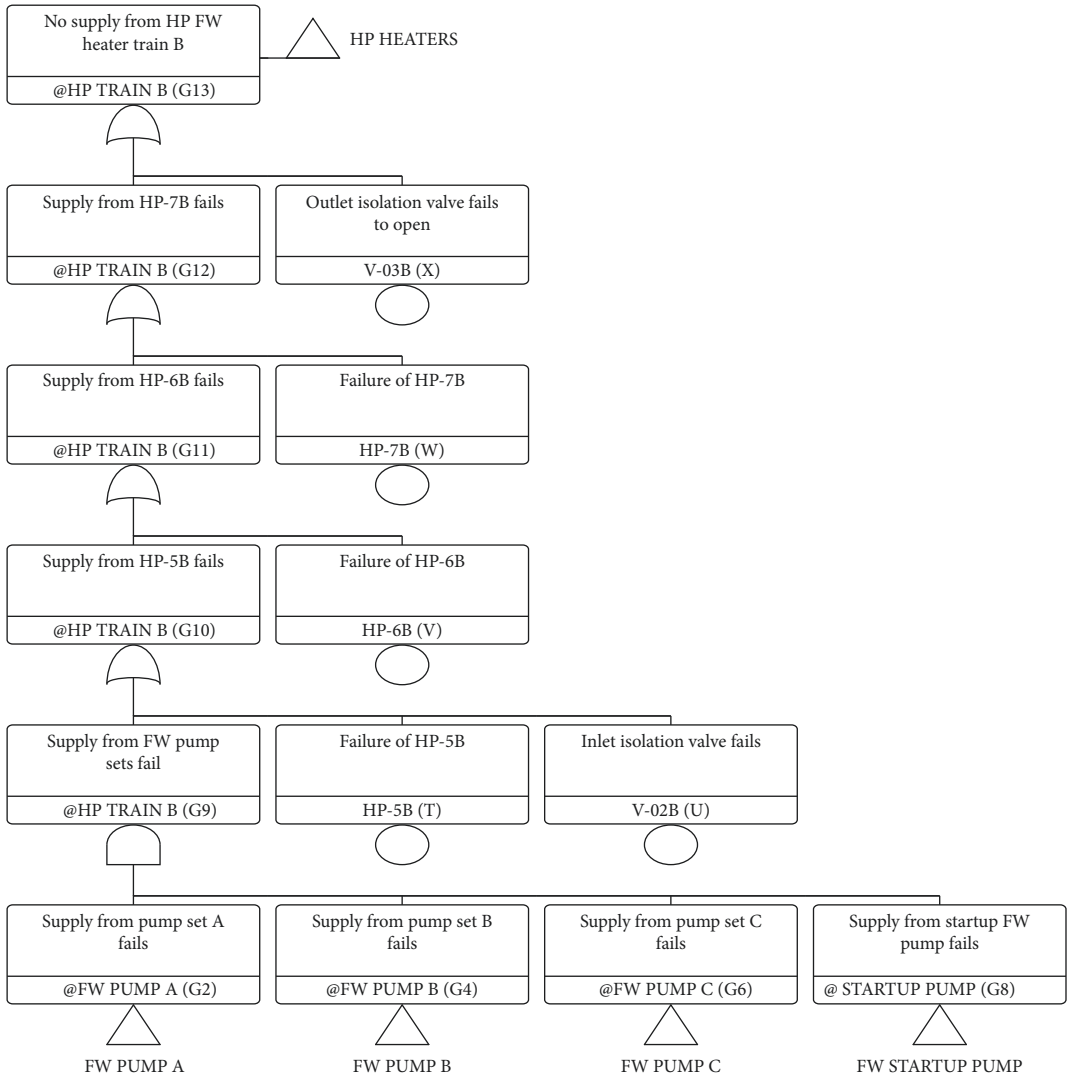

Figure 7: HPFW train B.

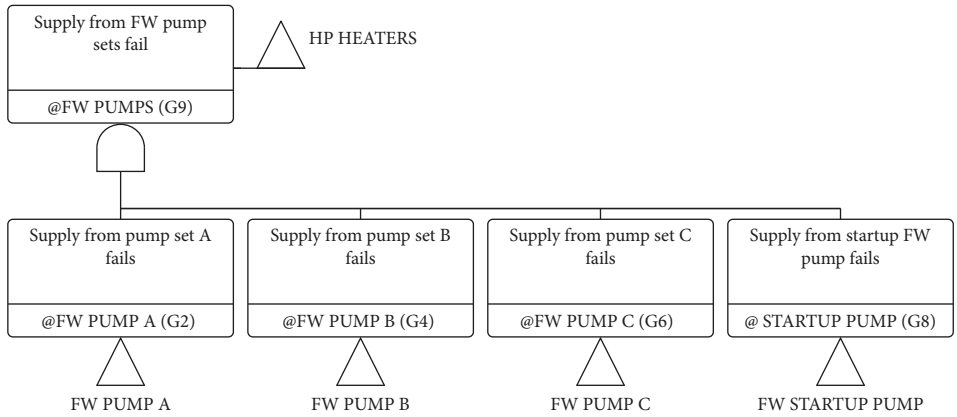

Figure 8: Fault tree for FW pump.

failure probability from the U.S. NRC and IAEA databases to be $2.797E-02$ with 87 minimal cut sets while the probability from WASH-1400 was calculated as $2.199E-02$ with 138 minimal cut sets. The number of minimal cut sets represents different accident scenarios where the occurrence of a specific set of faults leads up to the top event, and the exclusion of any event can avoid the top event from taking place.

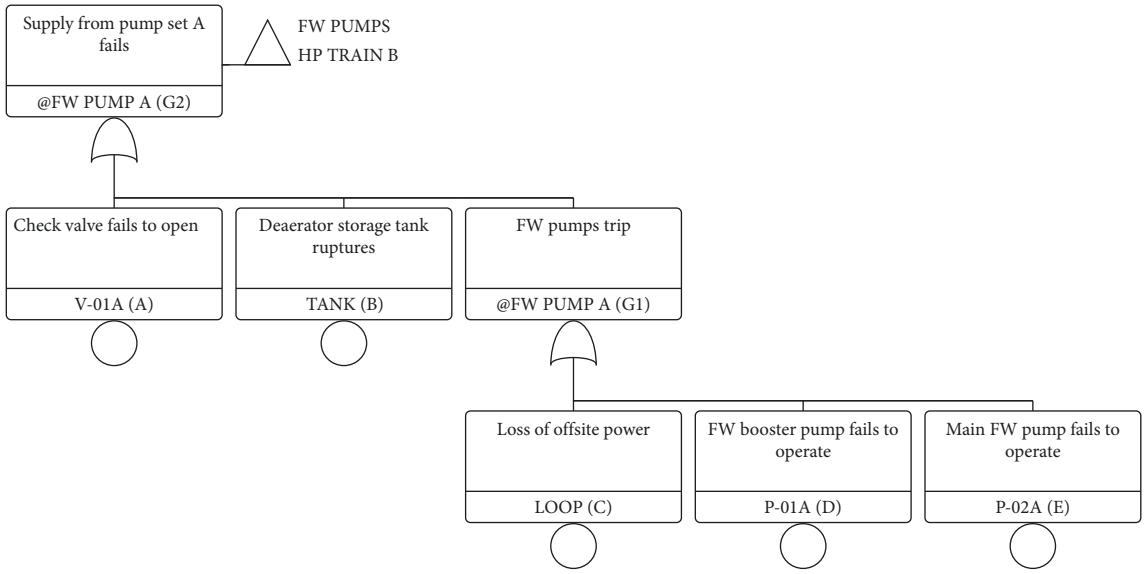

Figure 9: FW pump set A fails.

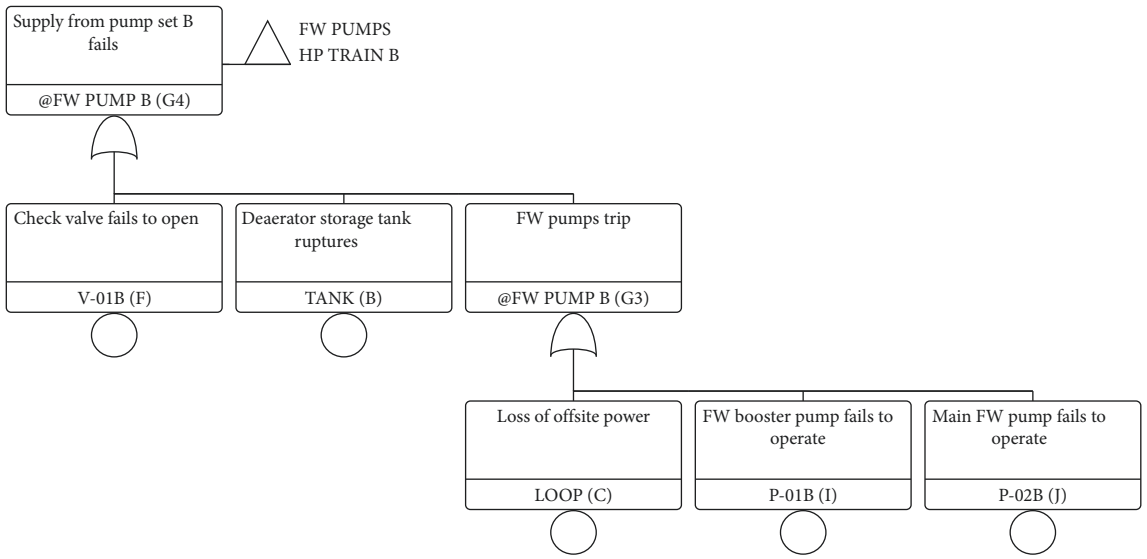

Figure 10: FW pump set B fails.

A qualitative analysis of the fault tree is based on an identification of the minimal cut sets. Since system failure occurs, all the events in at least one minimal cut set occur. The number of events in a cut set is called the order of the cut set. The minimal cut sets are ranked according to their order. It may be argued that single-event cut sets are highly undesirable as only one failure can lead to the top event, two-event cut sets are better, and so on. Further, ranking based on human errors and active/passive equipment failure is also common. The qualitative approach is however potentially misleading. It may be that larger cut sets have a higher failure probability than smaller ones; this requires a quantitative analysis. Common cause failures are due to a single event affecting multiple events in the fault tree. This might be a power failure miscalibrating all sensors. Less obviously, elements such as common manufacturer and common location may also lead to common cause failures.

The top event probabilities, as seen in Figure 13, show that the probability of failure in the present research based on U.S NRC/IAEA databases is slightly greater than that of WASH-1400. The small difference could be attributed to the probability of the startup pump which has the highest contribution toward the G9 gate. Since the U.S NRC/IAEA databases have a higher probability for startup pump failure than in WASH-1400, it arises these differences in the proceeding calculations as the probabilities are further cumulated. Another underlying source of variation in the results is the difference in the probabilities of each component due to the varying component boundaries used in each document, as highlighted before.

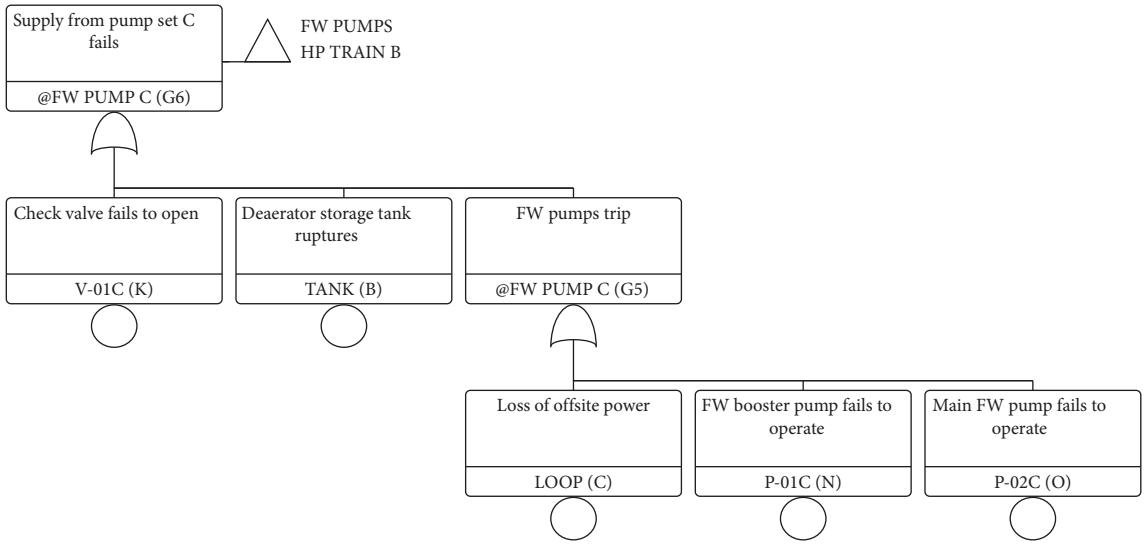

Figure 11: FW pump set C fails.

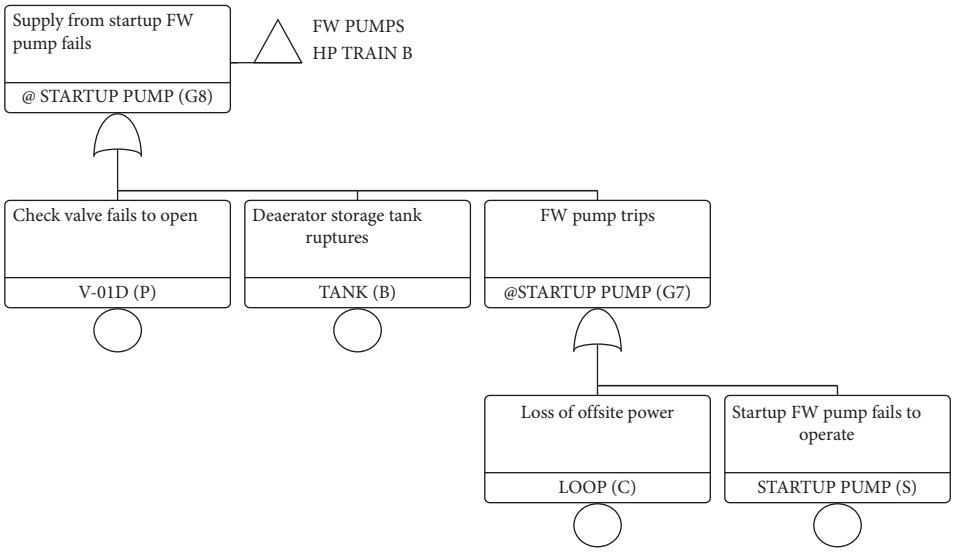

Figure 12: FW pump startup to fail.

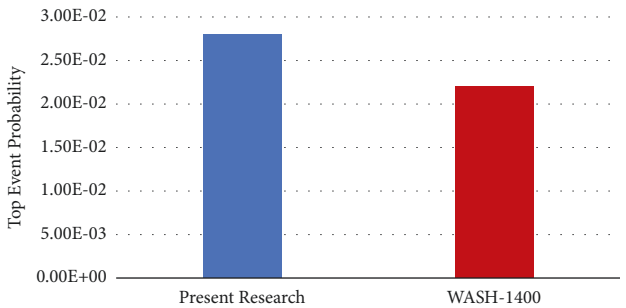

Figure 13: Comparison of top event probability.

Figure 14 illustrates the probabilities of the top minimal cut sets according to the U.S. NRC/IAEA database and the WASH-1400 report, respectively. It can be observed that, in both cases, the minimal cut set with the highest probability is the failure of the control valve, followed mostly by other types of valves or a combination of valves. While the order of

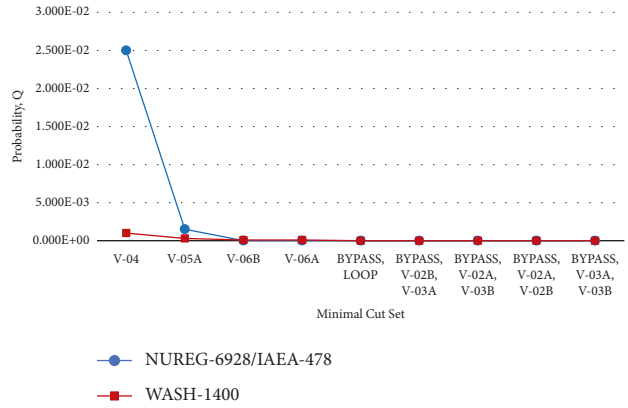

Figure 14: Comparison of top minimal cut set probabilities.

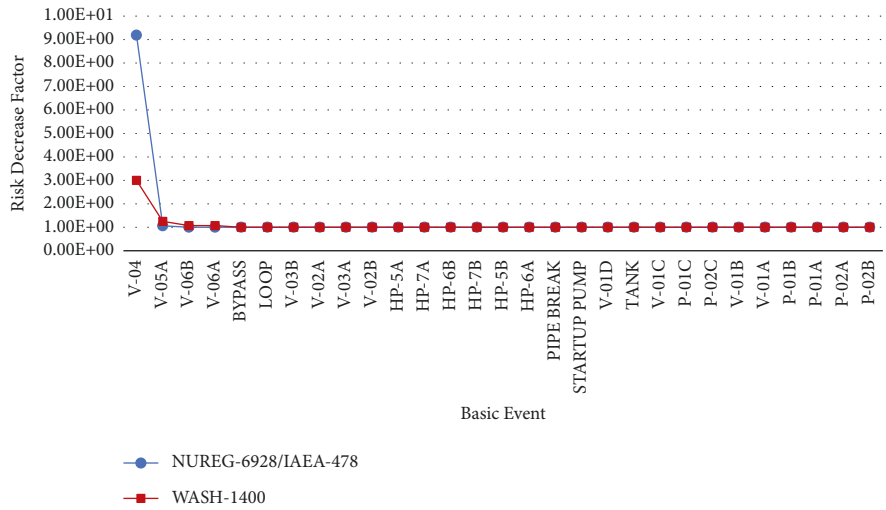

Figure 15: Comparison of risk decrease factors for each basic event.

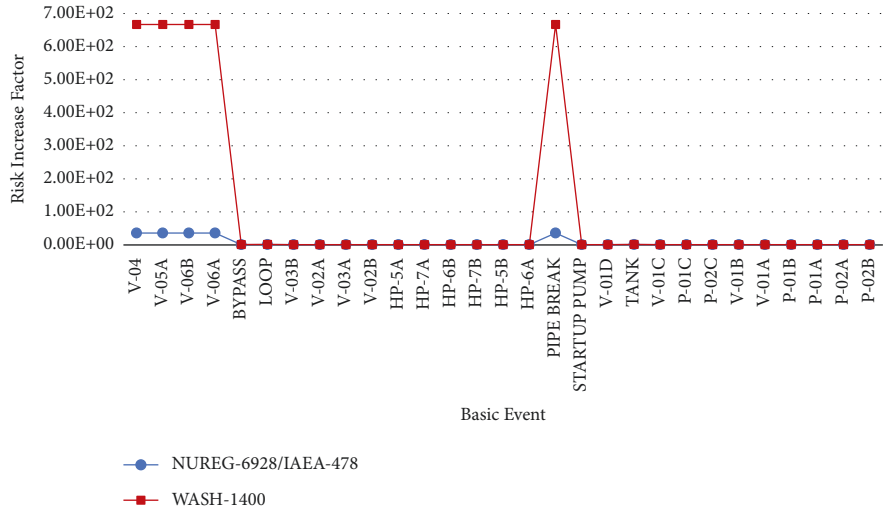

Figure 16: Comparison of risk increase factors for each basic event.

minimal cut sets from both sources is similar, there are slight differences such as the magnitude of probabilities. According to Figure 14, the failure probability of the control valve is $2.50E-02$ while the same event has a probability of $1.00E-03$. The minimal cut sets help in the identification of the weakest points in the feedwater system, namely, the

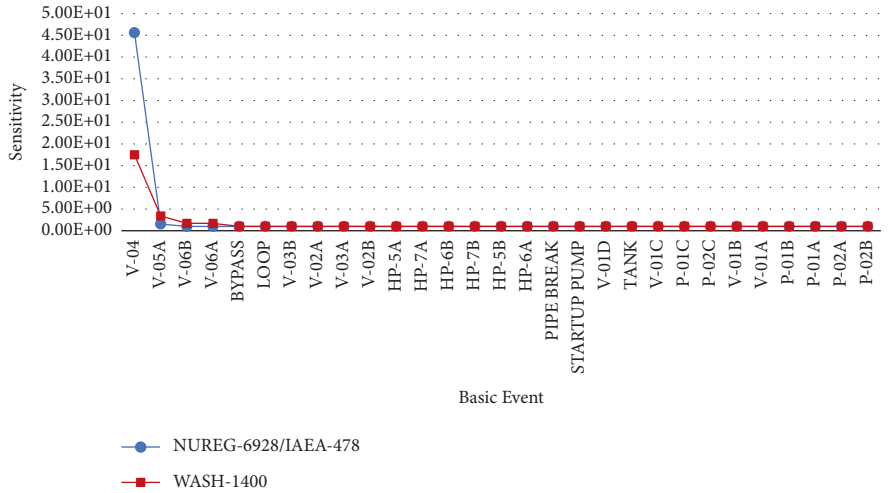

Figure 17: Comparison of the sensitivity calculations of the system toward each basic event.

Table 2: Importance analysis for CCF groups.

No.	ID	FC	RDF	RIF	Sens.	Sens. high	Sens. low
1	No flow to check valve	$1.05E-01$	$1.12E+00$	$3.58E+01$	$2.1E+00$	$5.42E-02$	$2.53E-02$
2	No flow to SG	$1.04E-08$	$1.00E+00$	$3.58E+01$	$1.00E+00$	$2.79E-02$	$2.79E-02$

valves which can be resolved by the addition of valves in parallel or usage of valves with a lower failure probability.

Figure 15 shows a comparison of the risk decrease factor for each basic event while Figure 16 illustrates the same for the risk increase factor. It can be observed that the risk decrease factor for the control valve from the NUREG-6928 and IAEA-478 reports is a lot higher than from WASH-1400. In the case of the risk increase factor while most events have a similar value, a few basic events such as the closure of the control valve, check valve or MFIVs, and pipe break have a higher value when the data was collected from WASH-1400. The importance/sensitivity analysis was also performed on the fault trees as shown in Figure 17. Data collected from the databases showed that control valve failure was most sensitive to a LOFW accident but data from the U.S. NRC and IAEA sources have a higher value than the WASH-1400 report.

All of the sensitivity calculations are carried out by setting the value(s) under consideration (unavailability, frequency, or individual parameter value) equal to the nominal value divided by the sensitivity factor. The sensitivity factor can be any value higher than 1. The default value is 10. For groups of basic events, the nominal unavailabilities for all basic events in the group are divided by the sensitivity factor.

Common Cause Failure (CCF) analysis has been carried out for all groups expected to contribute to causing top events. The results presented in Table 2 reveal that no flow to the check valve and no flow to the steam generator are the most critical contributors to CCF. The fractional contribution (FC), risk decrease factor (RDF), risk increase factor (RIF), and sensitivity were analyzed in Table 2.

For the present study, the parametric alpha-factor model is chosen because the alpha-factor model can handle common cause component group sizes of different levels, can be adopted even when no statistical data on common cause failure rates are available, and is more accurate compared to other parametric models. The alpha-factor model estimates the CCF frequencies from a set of ratios of failures and the total component failure rate.

4. Conclusion

APR-1400 is a nuclear power plant designed to generate and supply electricity. The coolant in the primary system gets cooled in the steam generator where water in the secondary circuit is heated and transported to run the turbine. The main feedwater system ensures the circulation of the feedwater approaching from the turbines, back to the steam generator. The system consists of independent, redundant systems to ascertain the flow of feedwater, increasing the reliability of the system. However, every system is prone to failure, and a combination of faults may lead to a severe accident. Some of the basic events identified, which may lead to failure of the system, are pipe break, closure of valves, pump trip, heater failure, deaerator storage tank rupture, or loss of offsite power.

Probabilistic safety analysis (PSA) was utilized to analyze the loss of feedwater accidents in an APR-1400 plant. A fault tree was constructed in the RSAT software which simulated different accident scenarios due to faults in the main feedwater system which may lead to a LOFW accident. The present research showed the top event probability of $2.797E-02$, which is very close to $2.199E-02$, obtained from WASH 1400. A comparison of top event probabilities, risk decrease factor, risk increase factor, and sensitivity analysis was also analyzed. The results of the importance analysis showed that the control valves and main feedwater

isolation valves have a significant contribution to LOFW accidents. Hence, more attention and preventive maintenance are required for these components to achieve a high level of safety. The comparison of failure probabilities showed well agreement with the WASH-1400 database. The difference in results may have been caused due to the difference in the component boundaries assumed in each database.

Abbreviations

PSA: Probabilistic safety analysis
LOFW: Loss of feedwater
U.S. NRC: United States Nuclear Regulatory Commission
IAEA: International atomic energy agency
PRA: Probabilistic risk assessment
APR-1400: Advanced power reactor 1400 MWe
KEPCO: Korea Electric Power Corporation
OPR-1000: Optimum power reactor 1000 MWe
MFIV: Main feedwater isolation valves
HP: High pressure
FW: Feedwater
MSIS: Main steam isolation signal
LOOP: Loss of offsite power
RSAT: RiskSpectrum analysis tools
MCS: Minimal cut set
RDF: Risk decrease factor
RIF: Risk increase factor.

Data Availability

The data used to support the finding of the study can be obtained from the author upon request.

Conflicts of Interest

The author declares no conflicts of interest.

Acknowledgments

This research was supported by the Office of Vice-Chancellor for Research & Graduate Studies, University of Sharjah, under Grant no. V.C.R.G./R. 1325/2021.

References

[1] "Nuclear power in the world today," 2020, https://www.world-nuclear.org/information-library/current-and-future-generation/nuclear-power-in-the-world-today.aspx#:~:text=Nuclear%20energy%20now%20provides%20about,in%20about%20220%20research%20reactors.

[2] G. Petrangeli, *Nuclear Safety*, Butterworth-Heinemann, Amsterdam, Netherlands, 1st edition, 2006.

[3] International Atomic Energy Agency, *Regulatory Review of Probabilistic Safety Assessment (PSA) Level-1 IAEA-TECDOC-1135*, IAEA, Vienna, Austria, 2000.

[4] W. E. Vesely, F. F. Goldberg, N. H. Roberts, and D. F. Hassl, *Fault Tree Handbook NUREG_0492"*, U.S. Nuclear Regulatory Commission, Washington, D.C., USA, 1981.

[5] S. M. Goldberg and R. Rosner, "Nuclear reactors: generation to generation," 2011, https://www.a4macad.org/sites/default/files/academy/pdfs/nuclearReactors.pdf.

[6] M. Zubair and A. Ishag, "Sensitivity analysis of APR-1400's reactor protection system by using riskspectrum PSA," *Nuclear Engineering and Design*, vol. 339, pp. 225–234, 2018.

[7] U.S. Nuclear Regulatory Commission, "Pressurized water reactor (PWR) systems," 2014, https://www.nrc.gov/docs/ML1427/ML14274A090.pdf.

[8] ARIS—Technical Data, "Status report 83—advanced power reactor 1400 MWe (APR1400)," 2011, https://aris.iaea.org/sites/overview.html.

[9] Korea Electric Power Corporation (KEPCO) and Korea Hydro & Nuclear Power Co., Ltd. (KHNP), *Chapter 1—Introduction and General Discussion. APR1400 Final Safety Evaluations*, KHNP, Gyeongju-si, Republic of Korea, 2018.

[10] Korea Electric Power Corporation (KEPCO) and Korea Hydro & Nuclear Power Co., Ltd. (KHNP), *Chapter 6—Engineered Safety Features. APR1400 Final Safety Evaluations*, KHNP, Gyeongju-si, Republic of Korea, 2018.

[11] KEPCO, "Safety systems & features," 2022, https://home.kepco.co.kr/kepco/EN/G/htmlView/ENGEHP00102.do?menuCd=EN07060102#:~:text=The%20APR1400%20reactor's%20safety%20systems,Feed%20Water%20System%20.

[12] APR1400, *Design Control Document Tier 2. Chapter 19, Probabilistic Risk Assessment and Severe Accident evaluation*, Korea Electric Power Corporation and Korea Hydro and Nuclear Power Co., Ltd., Naju-si, South Korea, 2014.

[13] "Chapter 10 boiler feedwater deaeration," 2020, https://www.suezwatertechnologies.com/handbook/chapter-10-boiler-feedwater-deaeration.

[14] U.S. Nuclear Regulatory Commission, *Auxiliary/Emergency Feedwater System Reliability (NUREG/CR-5500), 1987–1995*, INEEL, Mexico City, Mexico, 1998.

[15] "Design control document," 2018, https://www.nrc.gov/docs/ML1822/ML18228A657.pdf.

[16] M. Zubair and Q. Amjad, "Calculation and updating of common cause failure unavailability by using alpha factor model," *Annals of Nuclear Energy*, vol. 90, pp. 106–114, 2016.

[17] International Atomic Energy Agency, "Accident analysis for nuclear power plants with pressurized water reactors," 2003, https://www-pub.iaea.org/MTCD/publications/PDF/Pub1162_web.pdf.

[18] H. Rezaei, B. Ryan, and I. Stoianov, "Pipe failure analysis and impact of dynamic hydraulic conditions in water supply networks," *Procedia Engineering*, vol. 119, pp. 253–262, 2015.

[19] P. Groudev and M. Pavlova, "Total loss of feed water for VVER 1000," 2000, https://www.researchgate.net/publication/234006015_Total_Loss_of_Feed_Water_for_VVER_1000/link/02bfe50e290bf3ae96000000/download.

[20] E. Lewis, *Nuclear Power Reactor Safety*, Wiley, Hoboken, NJ, USA, 1977.

[21] M. Zubair, A. Ababneh, and A. Ishag, "Station black out concurrent with PORV failure using a generic pressurized water reactor simulator," *Annals of Nuclear Energy*, vol. 110, pp. 1081–1090, 2017.

[22] A. Volkanovski, A. Ballesteros Avila, M. Peinador Veira, D. Kančev, M. Maqua, and J. Stephan, "Analysis of loss of offsite power events reported in nuclear power plants," *Nuclear Engineering and Design*, vol. 307, pp. 234–248, 2016.

[23] Relcon AB, "Risk spectrum professional user manual," 1998, https://www.riskspectrum.com.

[24] International Atomic Energy Agency, *Manual on Reliability Data Collection for Research Reactors PSAs IAEA-TECDOC-636*, IAEA, Vienna, Austria, 1992.

[25] S. Eide, T. Wierman, C. Gentillon, D. Rasmuson, and C. Atwood, "Industry-average performance for components and initiating events at U.S. commercial nuclear power plants (NUREG/CR-6928)," 2007, https://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6928/.

[26] International Atomic Energy Agency, *Component Reliability Data for Use in Probabilistic Safety Assessment*, IAEA, Vienna, Austria, 1988.

[27] S. Eide, C. Gentillon, T. Wierman, and D. Rasmuson, "Reevaluation of station blackout risk at nuclear power plants," *Analysis of Station Blackout Risk*, vol. 2, 2005.

[28] U.S. Nuclear Regulatory Commission, *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. Appendix II*, U.S. Nuclear Regulatory Commission, Rockville, MD, USA, 1975.

[29] U.S. Nuclear Regulatory Commission, *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants (NUREG-75/014), Appendices III & IV*, U.S. Nuclear Regulatory Commission, Rockville, MD, USA, 1975.