Research Article GU J Sci 37(3): 1319-1339 (2024) DOI: 10.35378/gujs.1313692

Gazi University

Journal of Science

http://dergipark.gov.tr/gujs

Event Sequence Based Fault Tree Analysis to Evaluate Minimal Combination of Event Sequences Leading to the Reactor Core Damage

Damianus Toersiwi SONY TJAHYANI*, Julwan Hendry PURBA, Andi Sofrany EKARIANSYAH, Surip WIDODO, Susyadi SUSYADI, Ratih Luhuring TYAS

Research Center for Nuclear Reactor Technology, Research Organization for Nuclear Energy, National Research and Innovation Agency (BRIN), Kawasan Sains dan Teknologi BJ Habibie, Tangerang Selatan, Banten, Indonesia 15314

Highlights

- Fault tree (FT) and Event tree (ET) analysis can be used to evaluate the safety of nuclear reactor.
- This study proposed an innovative method called Event Sequence Based Fault Tree Analysis (ESFTA).
- The ESFTA integrates the qualitative FT and ET analysis to assess system failure and core damage.
- Passive core cooling system of AP1000 is evaluated to confirm the applicability of ESFTA.
- It is found that minimal combination of existing safety systems can protect the reactor core.

Article Info

Received :13 Jun 2023
Accepted:27 Nov 2023

Keywords

Fault tree analysis
Event tree analysis
Event sequence
AP1000
Core cooling system

Abstract

Probabilistic safety assessment has been widely used to evaluate nuclear power plant safety systems. It couples fault tree (FT) analysis and event tree (ET) analysis. The FT analysis is to develop failure scenarios, to quantify the failure probability, and to identify critical components. The ET analysis is to develop event sequences (ESs) leading to reactor core damage and quantify core damage frequency. Currently, there is no approach in probabilistic safety assessment that can be used to identify minimal combinations of safety system failures leading to reactor core damage. This study proposes an event sequence based fault tree analysis, which integrates the FT model with the ET model. The ET model is to identify the ESs leading to the reactor core damage. Meanwhile, the FT model is to identify minimal combinations of those ESs found in the ET model. The motivation of this study is how to identify critical safety systems in nuclear power plants to mitigate disturbances caused by a group of postulated initiating events to avoid core damage. To confirm the feasibility and the applicability of the proposed approach, the performance of the AP1000 passive core cooling system is evaluated. It is found that if an in-containment refueling water storage tank, an automatic depressurization system – full, an accumulator, a core make-up tank, and a passive residual heat removal work properly, the reactor core will remain intact. These results confirmed that the proposed approach could be applicable to identify minimal combinations of safety systems to keep the reactor core intact.

1. INTRODUCTION

Probabilistic safety assessment (PSA) is a well defined-approach for evaluating the performance of safety systems of a nuclear power plant (NPP) design [1]. The PSA results might propose new designs or recommend to change new components with higher reliability. PSA couples two different models, i.e. fault tree (FT) model and event tree (ET) model [2]. An FT model graphically shows possible system failure scenarios [3]. Using qualitative FT analysis, minimal cut sets of event combinations leading to the top event can be evaluated [4, 5]. Because of the speed and efficiency of the analysis, qualitative analysis may be used in practical engineering [6].

Meanwhile, an ET model graphically shows the sequential work of safety systems to mitigate any postulated initiating event (PIE). A PIE is an event that has been postulated to be able to create disturbances

*Corresponding author, e-mail: dami001@brin.go.id to the plant if it occurs. If safety systems, which have been designed to mitigate an initiating event (IE), do not properly work, the IE can lead to core damage depending on the success or the failure of relevant mitigating systems [7]. Using qualitative ET analysis, a number of event sequences (ESs) leading to reactor core damage can be evaluated [8]. ET can also be developed for the evaluation of hazards to get initiating events (IEs) of decommissioning activities [9].

However, there is no existing approach that can be used to find critical safety systems of an NPP that possibly cause the reactor core damage due to the occurrence of an IE. The motivation of this study is on how to identify critical safety systems in nuclear power plants (NPPs) to mitigate disturbances caused by IEs to avoid core damage. Critical safety systems are safety systems, which are needed to function to keep the reactor core intact. Therefore, we develop and propose a new FT analysis approach, which is an event sequence based fault tree analysis (ESFTA), to evaluate minimum combinations of mitigating safety systems to keep the reactor core intact. ESFTA integrates ET model with FT model. The ET model is used to identify the ESs leading to the reactor core damage. Meanwhile, the FT model is used to evaluate minimal combinations of safety systems, which could cause the reactor core damage. Hence, ESFTA is constructed based on safety systems whose functions to mitigate disturbances caused by IEs. To benchmark the applicability and the feasibility of the proposed approach, the performance of the AP1000 passive core cooling system (PXS) for a group of IEs is evaluated. The rest of the paper is organized as follows. Section 2 explains the proposed ESFTA in details. A case study to validate the proposed ESFTA is given in section 3. Furthermore, section 4 discusses and analyses the results of the case study to confirm the applicability of the proposed ESFTA to evaluate the minimal combination of ESs that can cause the reactor core damage. Finally, the study is concluded in section 5.

2. EVENT SEQUENCE BASED FAULT TREE ANALYSIS

Event sequence based fault tree analysis (ESFTA) consists of five main steps to qualitatively evaluate minimal combinations of mitigating systems leading to the reactor core damage. In the sequel, each step is elaborated in detail. Meantime, the scheme of the overall qualitative evaluation of the proposed ESFTA is shown in Figure 1.

Step 1: Select an NPP and identify its postulated initiating events (PIEs)

The purpose of this step is to select an evaluated NPP and collect all its PIEs. A PIE is an event, which is postulated to be able to create disturbances to an NPP possibly leading to the core damage if one or more safety systems do not function as expected. Relevant PIEs can be collected from various sources, such as vendor documents (safety analysis report), experts who are knowledgeable about the selected NPP, historical data, and/or previous researches (scientific publications). The output of this step is a set of PIEs of the evaluated NPP as denoted in (1).

$$\mathrm{PIE} = \left\{ pie_i \;\middle|\; i = 1, 2, \cdots n \,;\, pie_i \in \mathrm{NPP} \right\} \tag{1}$$

where pie_i is the i^{th} PIE and n is the number of IEs of the selected NPP.

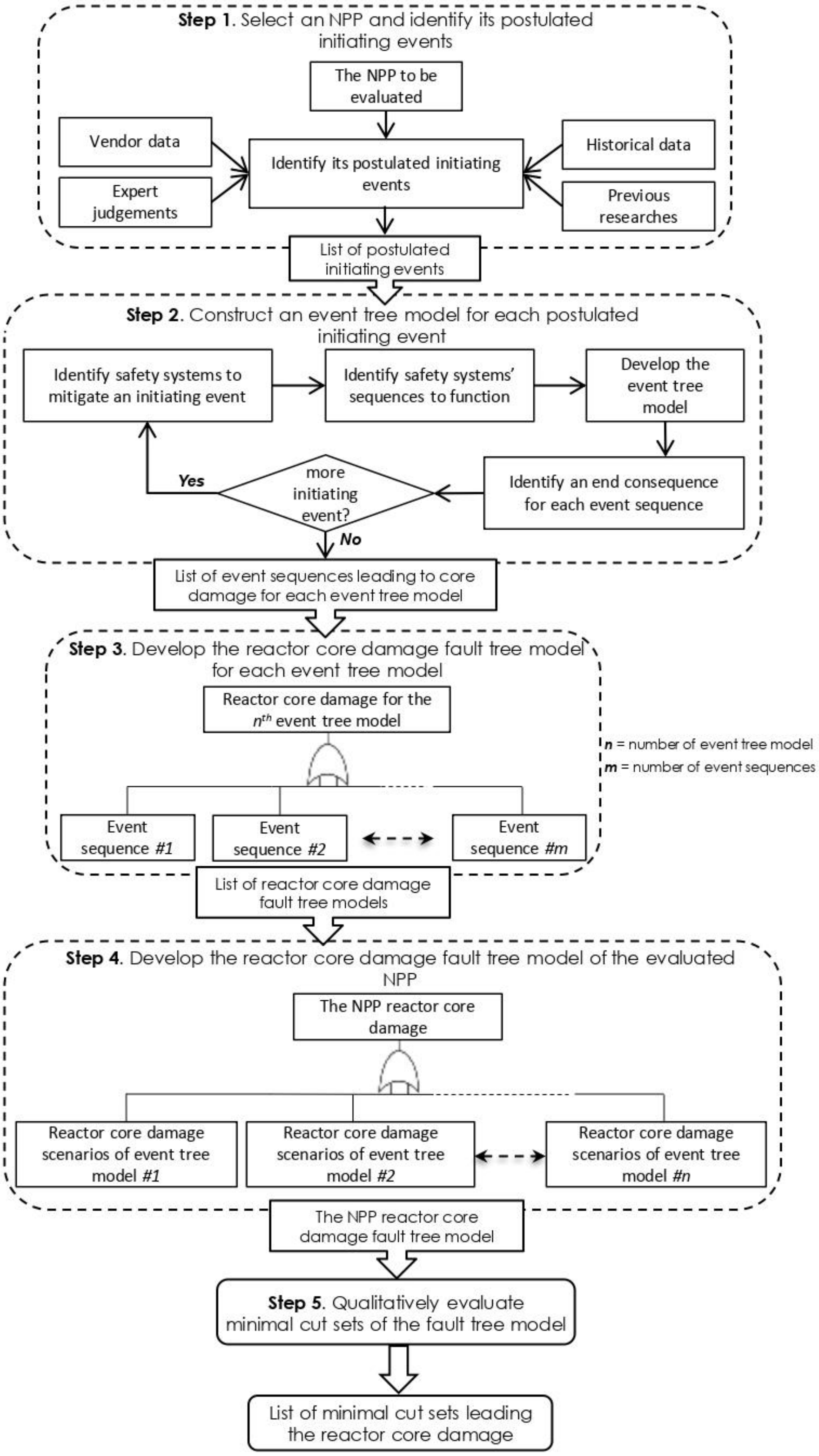

Step 1. Select an NPP and identify its postulated initiating events
The NPP to be evaluated
Vendor data
Expert judgements
Identify its postulated initiating events
Historical data
Previous researches
List of postulated initiating events
Step 2. Construct an event tree model for each postulated initiating event
Identify safety systems to mitigate an initiating event
Identify safety systems' sequences to function
Develop the event tree model
Identify an end consequence for each event sequence
more initiating event?
Yes
No
List of event sequences leading to core damage for each event tree model
Step 3. Develop the reactor core damage fault tree model for each event tree model
Reactor core damage for the nth event tree model
Event sequence #1
Event sequence #2
Event sequence #m
n = number of event tree model
m = number of event sequences
List of reactor core damage fault tree models
Step 4. Develop the reactor core damage fault tree model of the evaluated NPP
The NPP reactor core damage
Reactor core damage scenarios of event tree model #1
Reactor core damage scenarios of event tree model #2
Reactor core damage scenarios of event tree model #n
The NPP reactor core damage fault tree model
Step 5. Qualitatively evaluate minimal cut sets of the fault tree model
List of minimal cut sets leading the reactor core damage

Figure 1. *The framework of the event sequence based fault tree analysis*

Step 2: Construct an ET model for each PIE

The purpose of this step is to construct an ET model for each PIE in (1) as denoted in (2).

$$\mathrm{ET} = \left\{ et_i \,\middle|\, i = 1, 2, \cdots n \,;\; et_i \in pie_i \right\} \tag{2}$$

where et_i is the i^{th} ET model and *n* is the number of ET model corresponding to the number of IE in (1).

An ET model is a graphical representation of subsequent events starting from the PIE to the associated consequences. In NPP ET analysis, there are two possible consequences, i.e. reactor core damage and reactor core intact. These end consequences depend on the success or the failure of relevant safety systems to mitigate the PIE. The combination of success/fail of the expected mitigating systems leading to one of those two end consequences is called as an event sequence (ES). Therefore, to develop an ET model, it is very important to understand which safety systems are expected to function to mitigate disturbances due to the occurrence of the IEs.

The goal of this step is a set of ES leading to the core damage for each ET model in (2) as denoted in (3).

$$\text{ES} = \left\{es_{ij} \,\middle|\, i = 1, 2, \cdots, n\,;\; j = 1, 2, \cdots, m\,;\;\; es_{ij} \in et_i\right\} \quad (3)$$

where es_{ij} is the j^{th} ES of the et_i, *m* is the number of ESs leading to the reactor core damage for the et_i, and *n* is the number of ET model.

Step 3: Develop the reactor core damage FT model for each ET model

The purpose of this step is to develop a FT model for each ET model leading to core damage. A FT model is a graphical representation of system failure schemes, which are might be caused by various parallel and/or sequential combinations of event. A FT model consists of a top event, basic events, and a Boolean gate to logically link the basic event to the top event.

In this step, the top event of the FT model is the reactor core damage. Meanwhile, the basic events are every single ES in (3) of the corresponding ET model, and the Boolean gate is an OR gate. The goal of this step is a set of FT models representing reactor core damage due to the occurrence of an IE as denoted in (4) and the set of basic events consists of ESs in (3) as denoted in (5).

$$\text{FT} = \{ft_i \mid i = 1, 2, \cdots, n\,;\; ft_i \in et_i\} \quad (4)$$

$$\text{B} = \left\{b_j \,\middle|\, j = 1, 2, \cdots, m\,;\;\; b_j \in ft_i\,; b_j \in \text{ES}\right\} \quad (5)$$

where ft_i is the i^{th} FT model of the corresponding ET model et_i, *n* is the number of ET model, b_i is the i^{th} basic event, which is part of set of ESs in (3), and *m* is the number of ESs leading to the reactor core damage of ET model et_i.

Step 4: Develop the reactor core damage FT model of the evaluated NPP

The intention of this step is to merge all FT model within the set in (4) into one new FT model using an OR Boolean gate. To reduce FT model, minimal cut set is applied for each the PIE using laws of Boolean algebra in Table 1. This new FT model represents various scenarios leading to the reactor core damage of the evaluated NPP. Hence, the output of this step is a FT model whose top event is the NPP reactor core damage and the basic events are all ESs generated in (5) for the set of FT models in (4).

Step 5: Qualitatively evaluate minimal cut sets of the FT model

The aim of this step is to qualitatively evaluate the generated FT model in Step 4 using laws of Boolean algebra in Table 1.

Table 1. *Laws of Boolean algebra*

Law	Expression
Idempotent	A + A = A A . A = A
Commutative	A + B = B + A

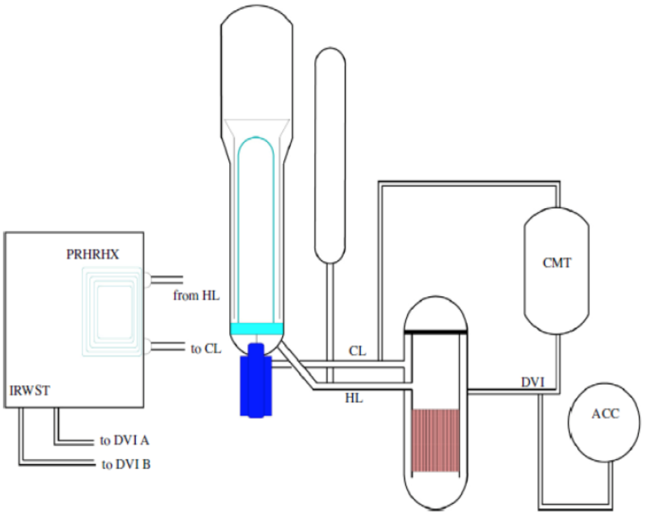
	A . B = B . A
Distributive	A . (B + C) = A . B + A . C
Absorption	A + (A . B) = A

The output of this step is a set of minimal cut sets consisting of a number of minimal combinations of ESs that could damage the reactor core if they occur. If these minimal cut sets fail to function to mitigate an IE, the reactor core will damage. On the other hand, if those minimal cut sets function properly to mitigate an IE, the reactor core will intact.

3. ESFTA VERIFICATION

This section describes how the proposed ESFTA will be verified to ensure its applicability. The performance of the passive core cooling system (PXS) to mitigate IEs in AP1000 is evaluated to examine the feasibility and effectiveness of the proposed ESFTA approach.

PXS applies the concept of passive systems. The principal of passive safety systems work based on gravity, convection, condensation, and heat circulation flow. Through the implementation of passive safety systems, system reliability can be improved, and human error is be reduced [10]. PXS consists of five mitigating safety systems, i.e. accumulator (ACC), core make-up tank (CMT), passive residual heat removal (PRHR), automatic depressurization system (ADS), and in-containment refueling water storage tank (IRWST), as graphically depicted in Figure 2 [11].



ACC = Accumulator
CMT = Core make-up tank
DVI = Direct vessel injection
HL= Hot leg
CL = Cold leg

IRWST = In-containment Refueling Water Storage Tank
PRHRHX = Passive residual heat removal Heat Exchanger

Figure 2. *Block diagram of AP1000 PXS [11]*

The function of two CMTs are to inject high flow borated water into the reactor cooling system (RCS) in a long time at any pressure. The CMT is connected to the RCS cold leg and the direct vessel injection (DVI). The balance line that is from the RCS to the upper head is open in normal condition. When it is needed, the CMTs will operate in two actions that are injection and recirculation modes. The PRHR function is to remove decay heat without operator action that is by natural circulation and has a capacity of 100%. PRHR system is connected with the hot leg side and the cold leg of the steam generator exit plenum. The system is to protect plant from events that disrupt normal steam generator (SG) operations such as loss of flow accident for feedwater, loss of offsite power, steam generator rupture, etc. The IRWST is to inject borated water in a longer time when the pressure of system was reduced near the containment pressure. This system is a large tank and is located above the RCS. Two lines connect between the IRWST and both DVI lines. Usefulness of the IRWST is to provide post LOCA flooding to settle the long-term RCS cooling, and to serve PRHR operation. ADS consists of four-valve steps that open sequentially to reduce pressure so that the PXS can do the long-term cooling process. Stages 1, 2, and 3 comprise two lines each and have two valves in series on each line. The valves are as main part of the pressurizer and are related to the top of the pressurizer.

A number of researchers have evaluated the performance of PXS to mitigate IEs in AP1000. The performance of PXS has been evaluated to mitigate Loss of Coolant Accident (LOCA) by Hung et al. [12]. They found that the natural convection model accurately represents a passive phenomenon for the heat removal process. Based on this phenomenon, the containment pressure is below the design threshold value. This condition can maintain the integrity of containment during the loss of coolant accident. Also, the highest peak of pressure is similar to the Design Control Document (DCD) result for long-term analysis. Meanwhile, Ekariansyah and Widodo [13] evaluated the PXS performance to mitigate Direct vessel injection line break (DVI-LB) using RELAP5/SCDAP/Mod 3.4. It is confirmed that the failure of DVI lines can be anticipated using injected coolant, which is operated based on a passive system so that the reactor core is always safe. The other initiating event that is considered in the AP1000 safety analysis report can use this model. The IRWST function to mitigate the IE on the long-term has also been investigated by Li Yu Quan et al [14] and Xiangbin Li et al [15]. They found that a quasi-steady-state approach using a 1-D analytical model can be applied to long-term IRWST injection core cooling processes. Furthermore, the importance levels of different parameters for the heat transfer mechanism were assessed by applying phenomena identification and ranking table.

Furthermore, ADS capability to adjust pressure has been analyzed by Hashim et al [16] They found that ADS is an important system of AP1000 to control RCS pressure, in which the dynamic reliability of the PXS increased with the reliability level of the ADS system operation. In case the ADS system fails, the probability of PXS failure reaches its high value, and the recirculation sump is impossible. PRHR capability has also been investigated by Zou et al [17]. It is confirmed that when failure of normal feedwater and main feedwater line occurs, all decay heat can be transferred from RCS to IRWST through PRHR HX. Furthermore, the RCS and steam generator pressure are under 110 percent of the design criteria, and the overfilling of pressurizer can be prevented.

In this study, the performance of PXS to prevent the core damage caused by a group of IEs in AP1000 is used to benchmark the applicability of the proposed ESFTA. An ET model is used to identify the ES scenarios leading to the reactor core damage. Meanwhile, a FT model is used to evaluate minimal combinations of safety systems, which could cause the reactor core damage for a group of PIEs belongs to AP1000.

4. RESULTS AND DISCUSSION

This section qualitatively describes how the proposed ESFTA evaluates minimal combinations of ESs of AP1000 PXS leading to core damage. To simplify the process and for verification purposes only, IEs and corresponding ET models of AP1000 PXS in this study are just taken from UKP-GW-GL-022 entitled “UK AP1000 Probabilistic Risk Assessment” provided by Westinghouse [18].

Step 1: Select an NPP and identify its PIEs

AP1000 has 26 PIEs at power operation [11]. In this study, IEs whose contribution percentage to the core damage is 1% or more and needs PXS to response to are evaluated. Those selected PIEs and their contribution percentages are displayed in Table 2.

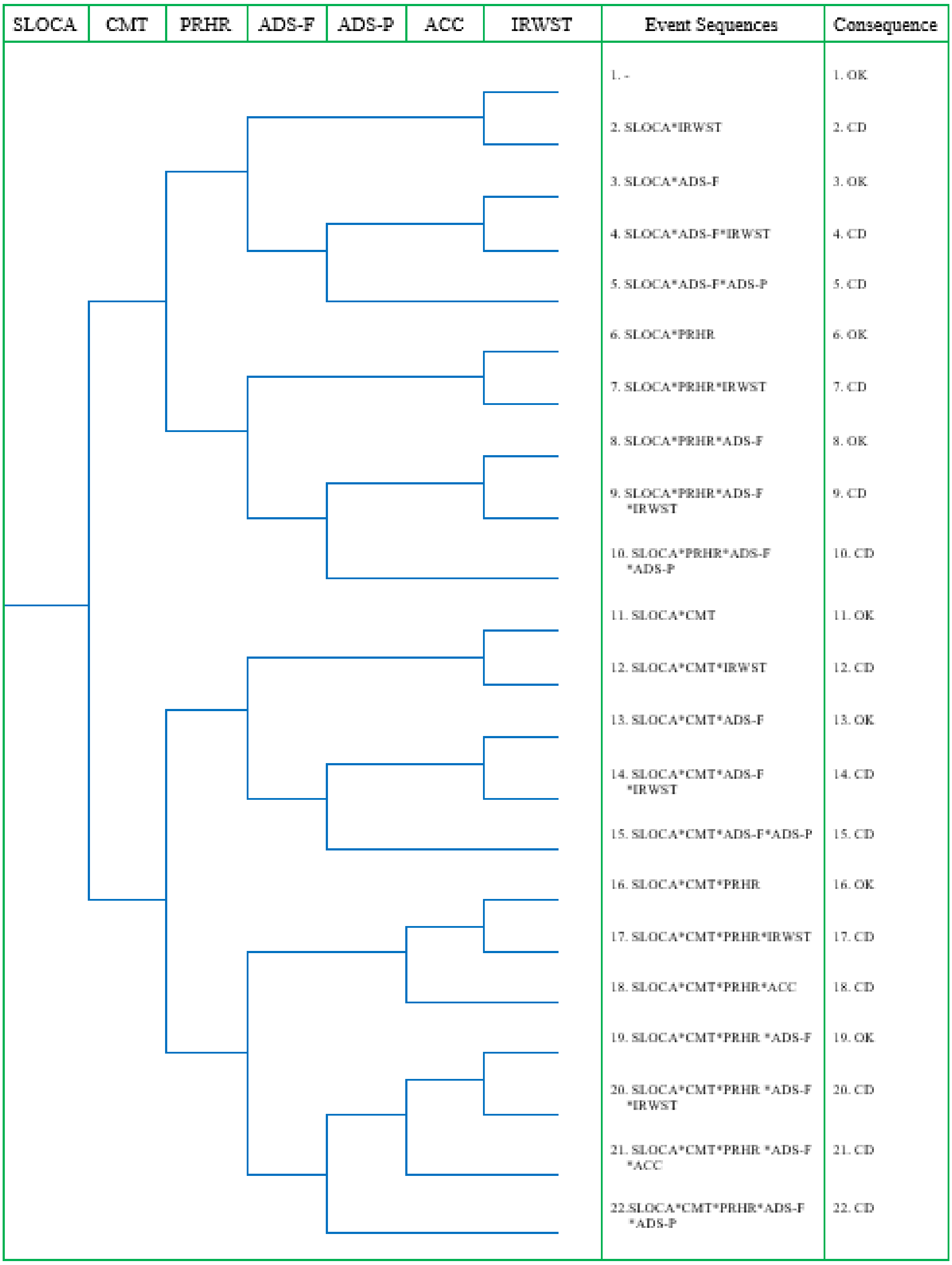
***Table 2**. PIEs to be evaluated [11]*

No.	**PIE**	**Contribution percentage to core damage**
1.	Direct vessel injection line break (DVI-LB)	39.4 %
2.	Large loss of coolant accident (LLOCA)	18.7 %
3.	Spurious automatic depressurization system actuation (SPADS)	12.3 %
4.	Small loss of coolant accident (SLOCA)	7.5 %
5.	Medium loss of coolant accident (MLOCA)	6.7 %
6.	Steam generator tube rupture (SGTR)	2.8 %
7.	Core make-up tank line break (CMT-LB)	1.5 %
8.	Anticipated transient without scram (ATWS)	1.5 %
9.	Transient	1.3 %

Those nine PIEs in Table 2 are then evaluated to find the minimal cut sets of the ES combination leading to AP1000 reactor core damage if one or more safety systems in PXS do not properly work to mitigate those PIEs.

Step 2: Construct an ET model for each PIE

Based on the 9 PIEs in Table 2, 9 ET models are constructed. One ET model is constructed for each PIE. For verification purposes only, ET models for all PIEs in Table 2 are taken from UK AP1000 Probabilistic Risk Assessment, UKP-GW-GL-022, 2007 [18]. As an example, the ET model for SLOCA is depicted in Figure 3.



Event Sequences	Consequence
1. -	1. OK
2. SLOCA*IRWST	2. CD
3. SLOCA*ADS-F	3. OK
4. SLOCA*ADS-F*IRWST	4. CD
5. SLOCA*ADS-F*ADS-P	5. CD
6. SLOCA*PRHR	6. OK
7. SLOCA*PRHR*IRWST	7. CD
8. SLOCA*PRHR*ADS-F	8. OK
9. SLOCA*PRHR*ADS-F *IRWST	9. CD
10. SLOCA*PRHR*ADS-F *ADS-P	10. CD
11. SLOCA*CMT	11. OK
12. SLOCA*CMT*IRWST	12. CD
13. SLOCA*CMT*ADS-F	13. OK
14. SLOCA*CMT*ADS-F *IRWST	14. CD
15. SLOCA*CMT*ADS-F*ADS-P	15. CD
16. SLOCA*CMT*PRHR	16. OK
17. SLOCA*CMT*PRHR*IRWST	17. CD
18. SLOCA*CMT*PRHR*ACC	18. CD
19. SLOCA*CMT*PRHR *ADS-F	19. OK
20. SLOCA*CMT*PRHR *ADS-F *IRWST	20. CD
21. SLOCA*CMT*PRHR *ADS-F *ACC	21. CD
22.SLOCA*CMT*PRHR*ADS-F *ADS-P	22. CD

Figure 3. *SLOCA ET model*

Figure 3 shows that there are 22 ESs for PIE SLOCA in which 14 ESs lead to core damage (CD). One of those ESs is number 10, which is SLOCA*PRHR*ADS-F *ADS-P. This ES means that if IE that is SLOCA occur and the three mitigating safety systems, i.e. PRHR, ADS-F, and ADS-P, fail to function as expected, the reactor core will damage. With the same procedures, the ET models for the other 8 PIEs are constructed. These ET models are depicted in Figures A1 – A8 in the appendix. Based on those ET models, ESs leading to core damage for each ET model are then identified as tabulated in Table 3.

Table 3. *ESs leading to core damage for the 9 ET models*

No.	ET model	ESs leading to core damage
1.	DVI-LB	DVI-LB*IRWST; DVI-LB*ADS-F; DVI-LB*CMT*IRWST; DVI-LB*CMT*ACC; DVI-LB*CMT*ADS-F 5 out of 7 ESs lead to core damage (CD)
2.	LLOCA	LLOCA*IRWST; LLOCA*ADS-F; LLOCA-F*ACC 3 out of 4 ESs lead to core damage (CD)
3.	SPADS	SPADS*IRWST; SPADS*ADS-F; SPADS*ACC 3 out of 4 ESs lead to core damage (CD)
4.	SLOCA	SLOCA*IRWST; SLOCA*ADS-F*IRWST; SLOCA*ADS-F*ADS-P; SLOCA*PRHR*IRWST; SLOCA*PRHR*ADS-F*IRWST; SLOCA*PRHR*ADS-F*ADS-P; SLOCA*CMT*IRWST; SLOCA*CMT*ADS-F*IRWST; SLOCA*CMT*ADS-F*ADS-P; SLOCA*CMT*PRHR*IRWST; SLOCA*CMT*PRHR*ACC; SLOCA*CMT*PRHR*ADS-F*IRWST; SLOCA*CMT*PRHR*ADS-F*ACC; SLOCA*CMT*PRHR*ADS-F*ADS-P 14 out of 22 ESs lead to core damage (CD)
5.	MLOCA	MLOCA*ADS-F*IRWST; MLOCA*CMT*ADS-F*IRWST; MLOCA*CMT*ADS-F*ADS-P 3 out of 7 ESs lead to core damage (CD)
6.	SGTR	SGTR*IRWST; SGTR*ADS-F*IRWST; SGTR*ADS-F*ADS-P; SGTR*PRHR*IRWST; SGTR*PRHR*ADS-F*IRWST; SGTR*PRHR*ADS-F*ADS-P; SGTR*CMT*IRWST; SGTR*CMT*ACC; SGTR*CMT*ADS-F*IRWST; SGTR*CMT*ADS-F*ACC; SGTR*CMT*ADS-F*ADS-P; SGTR*CMT*PRHR*IRWST; SGTR*CMT*PRHR*ACC; SGTR*CMT*PRHR*ADS-F*IRWST; SGTR*CMT*PRHR*ADS-F*ACC; SGTR*CMT*PRHR*ADS-F*ADS-P 16 out of 24 ESs lead to core damage (CD)
7.	CMT-LB	CMT-LB*IRWST ; CMT-LB*ADS-F*IRWST; CMT-LB*ADS-F*ADS-P ; CMT-LB*CMT*IRWST ; CMT-LB*CMT*ACC; CMT-LB*CMT*ADS-F*IRWST ; CMT-LB*CMT*ADS-F*ACC ; CMT-LB*CMT*ADS-F*ADS-P 8 out of 12 ESs lead to core damage (CD)
8.	ATWS	ATWS*IRWST; ATWS*ADS-F; ATWS*CMT; ATWS*PRHR 4 out of 5 ESs lead to core damage (CD)

No.	ET model	ESs leading to core damage
9.	Transient	TRANS*PRHR*IRWST; TRANS*PRHR*ADS-F *IRWST; TRANS*PRHR*ADS-F*ADS-P; TRANS*PRHR*CMT; TRANS*PRHR*CMT*ACC; TRANS*PRHR*CMT*ADS-F *IRWST; TRANS*PRHR*CMT*ADS-F *ACC; TRANS*PRHR*CMT*ADS-F*ADS-P 8 out of 13 ESs lead to core damage (CD)

Step 3: Develop the reactor core damage FT for each ET model

The FT model of all ESs of each ET model generated in Step 2 are developed. For example, the FT model for ESs leading to core damage in Table 3 of the ET in Figure 3 is shown in Figure 4.

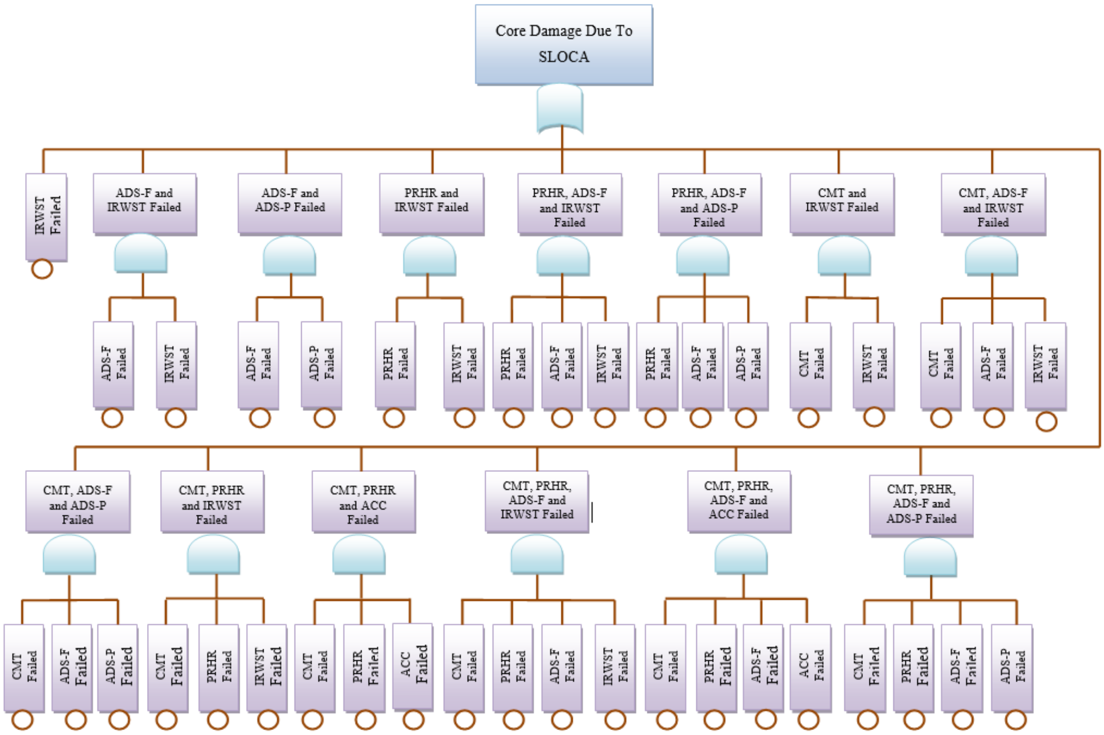


Figure 4. *FT model for SLOCA ET model*

Using the same procedures, the FT models for the other 8 ET models are constructed as depicted in Figures B1 – B8 in the Appendix.

Step 4: Develop the reactor core damage FT model of the evaluated NPP

Based minimal cut set on the FT models generated in Step 3, a new FT model whose top event is the NPP reactor core and the basic events are all ESs leading to the reactor core damage is developed as shown in Figures 5, 6, and 7.

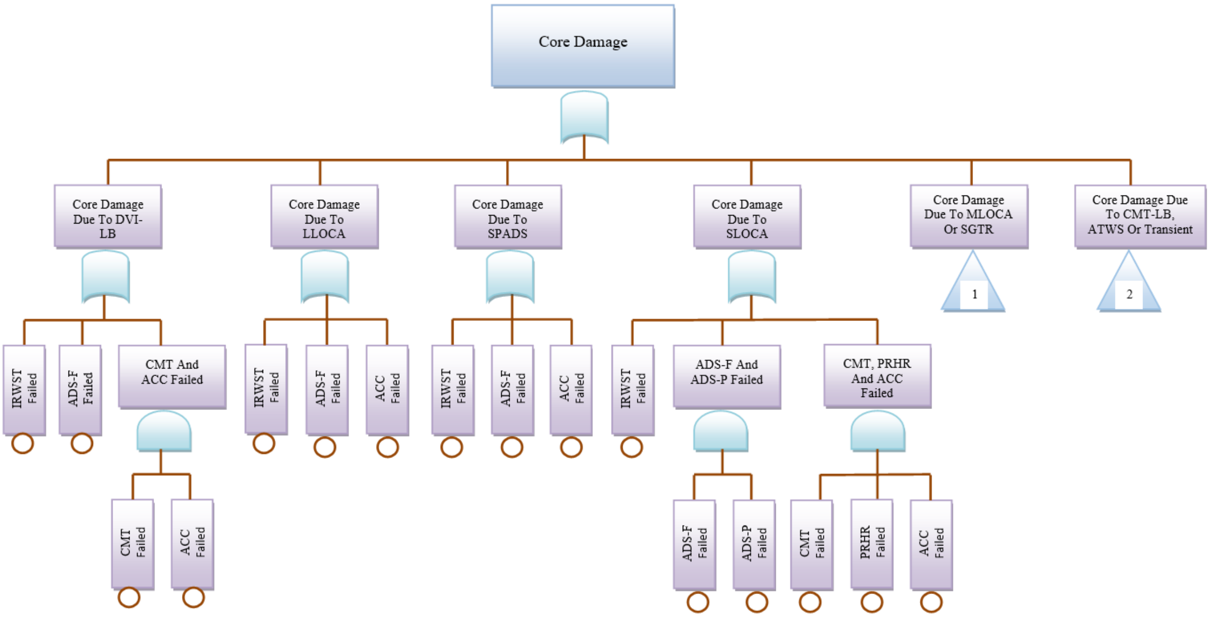


Figure 5. *Reactor core damage FT model with transfer in 1 to Figure 6 and transfer in 2 to Figure 7*

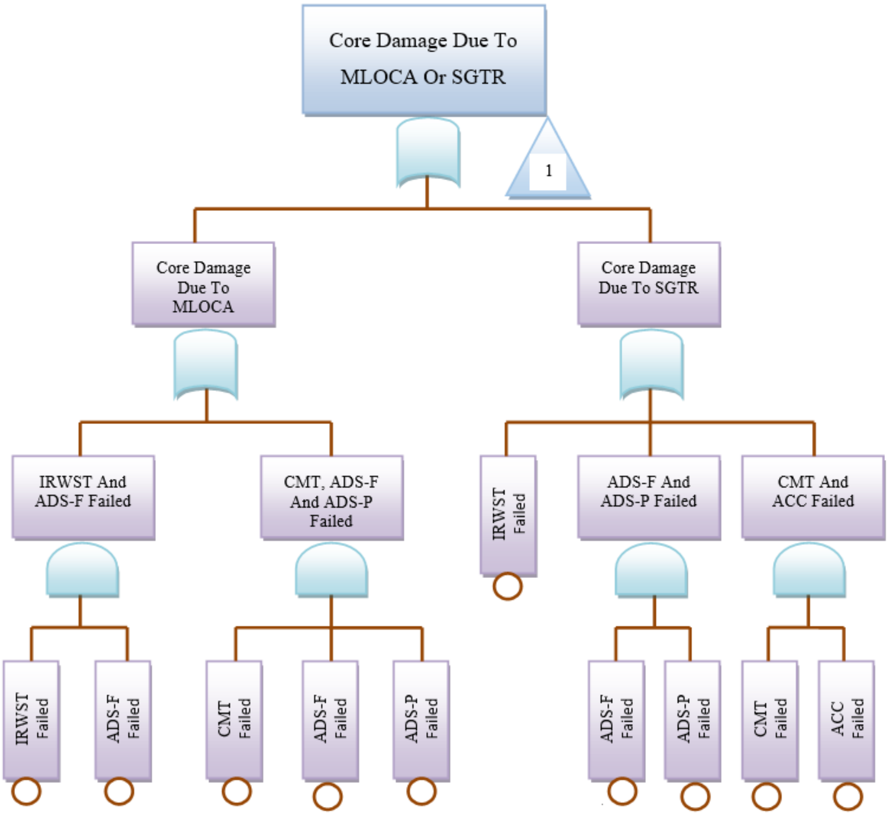


Figure 6. *FT model of core damage due to MLOCA or SGTR (transfer out 1) from Figure 5*

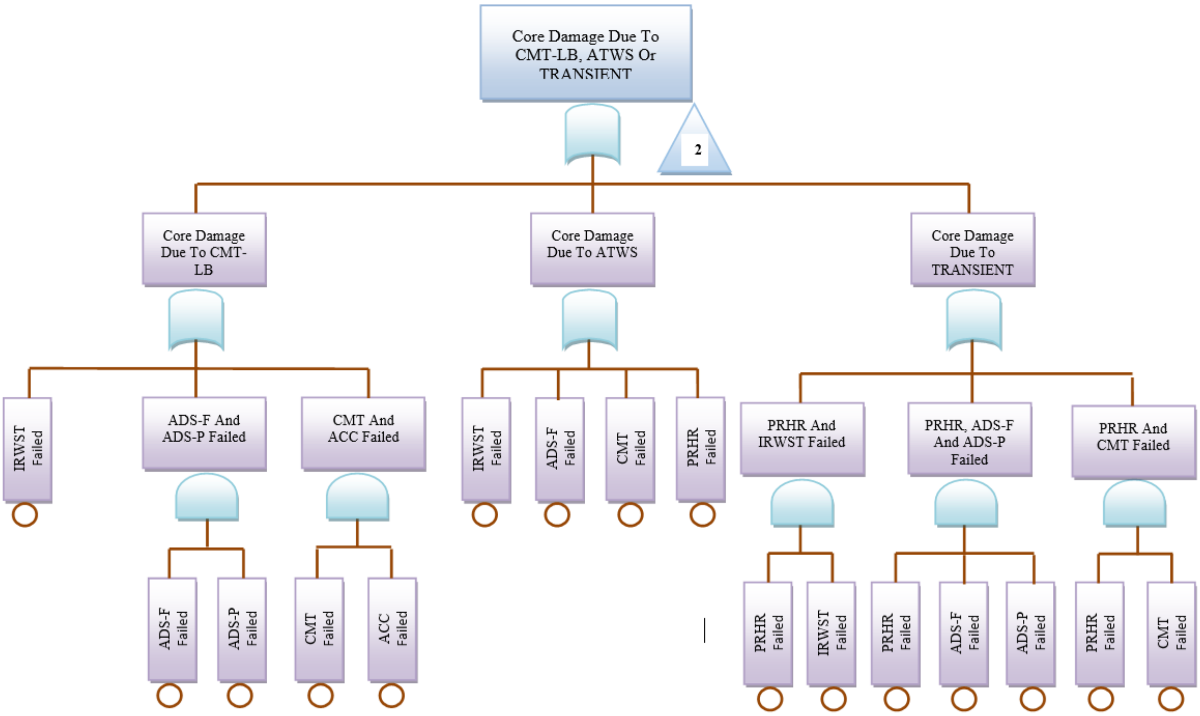


Figure 7. *FT model of core damage due to CMT-LB, ATWS or TRANSIENT (transfer out 2) from Figure 5*

Step 5: Qualitatively evaluate minimal cut sets of the FT model

Using laws of Boolean algebra in Table 1, the FT model in Figure 5 is qualitatively evaluated to find minimal cut sets describing minimal combinations of ESs that could damage the reactor core if they occur. The minimal cut sets for each FT model generated by the proposed ESFTA are shown in Table 4.

Table 4. *Minimal cut sets of FT*

No.	FT model	Minimal cut sets
1.	DVI-LB	IRWST ; ADS-F ; CMT*ACC
2.	LLOCA	IRWST ; ADS-F ; ACC
3.	SPADS	IRWST ; ADS-F ; ACC
4.	SLOCA	IRWST; ADS-F*ADS-P ; CMT*PRHR*ACC
5.	MLOCA	IRWST*ADS-F ; CMT*ADS-F*ADS-P
6.	SGTR	IRWST ; ADS-F*ADS-P ; CMT*ACC
7.	CMT-LB	IRWST ; ADS-F*ADS-P ; CMT*ACC
8.	ATWS	IRWST ; ADS-F ; CMT ; PRHR
9.	Transient	PRHR*IRWST ; PRHR*ADS-F*ADS-P ; PRHR*CMT

No.	FT model	Minimal cut sets
10.	Evaluated NPP	IRWST ; ADS-F ; ACC ; CMT; PRHR

It can be seen from Table 4 that the reactor core will damage if one of the three combination of sequential safety systems fail to mitigate IE SLOCA, for example in row #4 of Table 4. Those three combinations are an individual in-containment refueling water storage tank (IRWST), a combination of automatic depressurization system - Full and Partial (ADS-F*ADS-P), or a combination of core make-up tank, passive residual heat removal, and accumulator (CMT*PRHR*ACC).

Table 4 also shows that the reactor core of AP1000 will damage if one of five combination of sequential safety systems fail to mitigate the group of PIEs belongs to AP1000. Those five combinations are an individual of in-containment refueling water storage tank (IRWST), automatic depressurization system - Full (ADS-F), accumulator (ACC), core make-up tank (CMT), and passive residual heat removal (PRHR) (row #10 of Table 4). This means that if one of those five combinations fail to mitigate any PIE belongs to AP1000, its reactor core will damage. However, core damage state will depend on the type of safety system that failed. On the other hand, if those minimal cut sets function properly to mitigate any PIE, the reactor core will intact.

These results have ensured that the proposed ESFTA can be feasibly used to evaluate minimal combinations of mitigating safety systems, which need to properly function to avoid reactor core damage. In future studies, this proposed ESFTA still needs to be assessed more deeply to see how it will perform for different NPPs. More results obtained will confirm its applicability in evaluating the safety operations of NPPs.

5. CONCLUSION

The most concern of the safety assessment is the understanding of the capabilities of safety systems to properly mitigate any PIE. If all safety system properly work as expected, the reactor core will intact. This study proposes an event sequence based fault tree analysis to evaluate the minimal combinations of fail safety systems leading to reactor core damage. By knowing these minimal combinations, anticipative measurements can be performed to keep the reactor core intact. The proposed new approach has been applied to evaluate the performance of the passive core cooling system (PXS) to mitigate PIEs in AP1000. It is found that if in-containment refueling water storage tank (IRWST), automatic depressurization system - full (ADS-F), accumulator (ACC), core make-up tank (CMT), and passive residual heat removal (PRHR) work properly, the reactor core will intact for the occurrence of any PIE. These results ensured that the proposed approach can be applicable to evaluate the safety design of NPPs.

ACKNOWLEDGEMENT

The work presented in this paper was funded by the Research Organization for Nuclear Energy (ORTN) of National Research and Innovation Agency (BRIN).

CONFLICTS OF INTEREST

No conflict of interest was declared by the authors.

REFERENCES

[1] Contini, S., Fabbri, L., Matuzas, V., “A novel method to apply importance and sensitivity analysis to multiple fault-trees”, Journal of Loss Prevention in the Process Industries, 23: 574-584, (2010).

[2] Khakzad, N., Khan, F., Amyotte, P., “Risk-based design of process systems using discrete-time Bayesian networks”, Reliability Engineering & System Safety, 109: 5-17, (2013).

[3] Purba J. H., Tjahyani, D. T. S., Susila, I. P., Widodo, S., Ekariansyah, A. S., “Fuzzy probability and α-cut based-fault tree analysis approach to evaluate the reliability and safety of complex engineering systems”, Quality and Reliability Engineering International, 38: 2356-2371, (2022).

[4] Kabir, S., “An overview of fault tree analysis and its application in model based dependability analysis”, Expert Systems with Applications, 77: 114-135, (2017).

[5] Walker, M., Papadopoulos, Y., “Qualitative temporal analysis: Towards a full implementation of the Fault Tree Handbook”, Control Engineering Practice, 17: 1115-1125, (2009).

[6] Li, S., Lou, J., Zong, X., Ma, S.,“Application of Fault Tree Analysis to the DCS Reliability of Nuclear Power Plants”, IMCEC 2022 - IEEE 5th Advanced Information Management, Communicates, Electronic and Automation Control Conference, 1863-1868, (2022).

[7] Purba J. H., Tjahyani D. T. S., Widodo S, Ekariansyah A.S., “Fuzzy probability based event tree analysis for calculating core damage frequency in nuclear power plant probabilistic safety assessment”, Progress in Nuclear Energy, 125: 103376, (2020).

[8] Li, J., “Fault-Event Trees Based Probabilistic Safety Analysis of a Boiling Water Nuclear Reactor’s Core Meltdown and Minor Damage Frequencies”, Safety, 6, (2020).

[9] Jeong, K. S., Lee, K. W., Jeong, S. Y., Lim, H. K., “Estimation on probability of radiological hazards for nuclear facilities decommissioning based on fuzzy and event tree method”, Annals of Nuclear Energy, 38: 2606-2611, (2011).

[10] Purba, J. H., “A fuzzy probability algorithm for evaluating the AP1000 long term cooling system to mitigate large break LOCA”, Atom Indonesia, 41: 113-121, (2015).

[11] Queral, C., Montero-Mayorga, J.,“Risk reduction due to modification of normal residual heat removal system of AP1000 reactor to meet European Utility Requirements”, Annals of Nuclear Energy, 91: 65-78, (2016).

[12] Hung, Z. Y., Ferng, Y. M., Hsu, W. S., Pei, B. S., Chen, Y. S.,“Analysis of AP1000 containment passive cooling system during a loss-of-coolant accident”, Annals of Nuclear Energy, 85: 717-724, (2014).

[13] Ekariansyah, A. S., Widodo, S., “Performance analysis of AP1000 passive systems during direct vessel injection (DVI) line break”, Atom Indonesia, 42: 79-88, (2016).

[14] Quan, L.Y., Jian, C. H., Li, D. L., Yann, S., Shen, Y. Z., Kai, Y., Fang, F. F., “Analytical studies of long-term IRWST injection core cooling under small break LOCA in passive safety PWR”, Annals of Nuclear Energy, 88: 218-236, (2016).

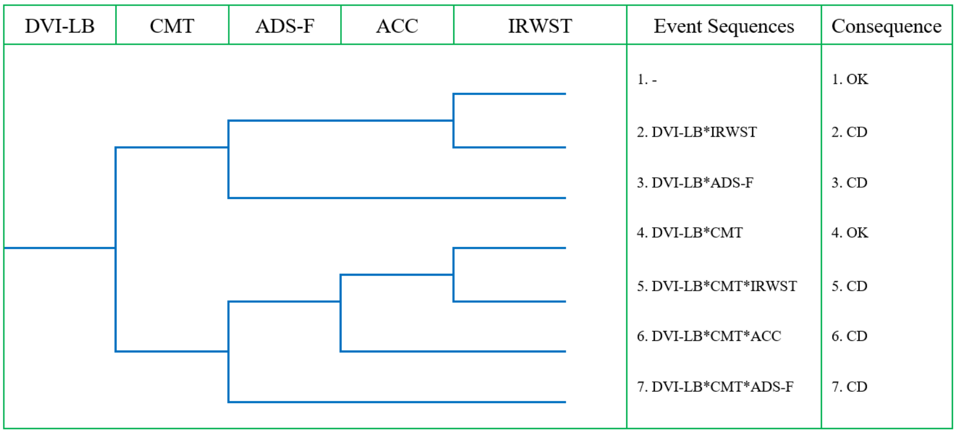
[15] Li, X., Li, N., Wang, Z. Y., Fu, X., Lu, D., Yang, Y., “Phenomena identification and ranking table for passive residual heat removal system in IRWST”, Annals of Nuclear Energy, 94: 80-86, (2016).

[16] Hashim, M., Hidekazu, Y., Takeshi, M., Ming, Y.,“Application case study of AP1000 automatic depressurization system (ADS) for reliability evaluation by GO-FLOW methodology”, Nuclear Engineering and Design, 278: 209-221, (2014).

[17] Zou, J., Li, Q., Tong, L. L., Cao, X. W., “Assessment of passive residual heat removal system cooling capacity”, Progress in Nuclear Energy, 70: 159-166, (2014).

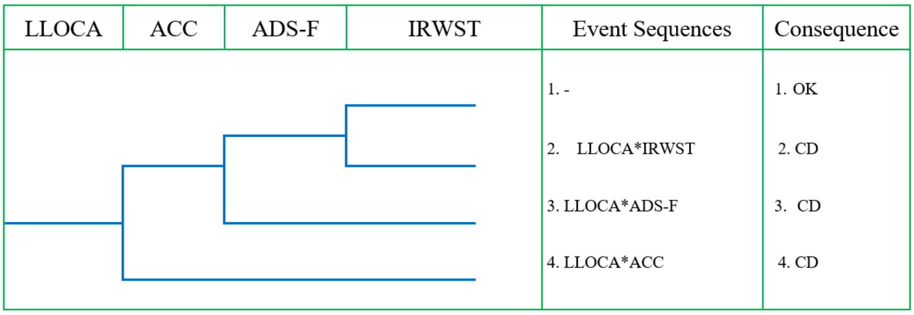
[18] Westinghouse, “UK AP1000 Probabilistic Risk Assessment UKP-GW-GL-022”, (2007).

APPENDIX



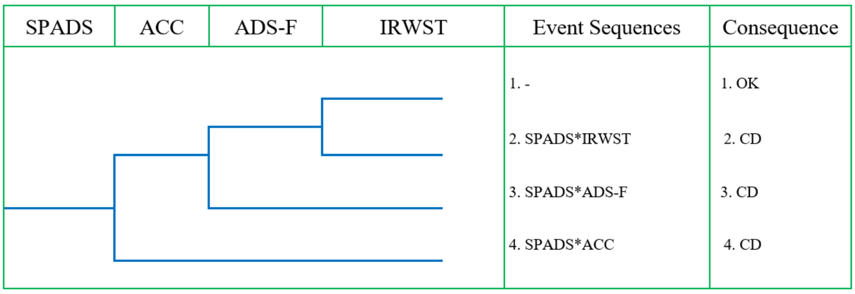
Event Sequences	Consequence
1. -	1. OK
2. DVI-LB*IRWST	2. CD
3. DVI-LB*ADS-F	3. CD
4. DVI-LB*CMT	4. OK
5. DVI-LB*CMT*IRWST	5. CD
6. DVI-LB*CMT*ACC	6. CD
7. DVI-LB*CMT*ADS-F	7. CD

Figure A1. *DVI-LB ET model*



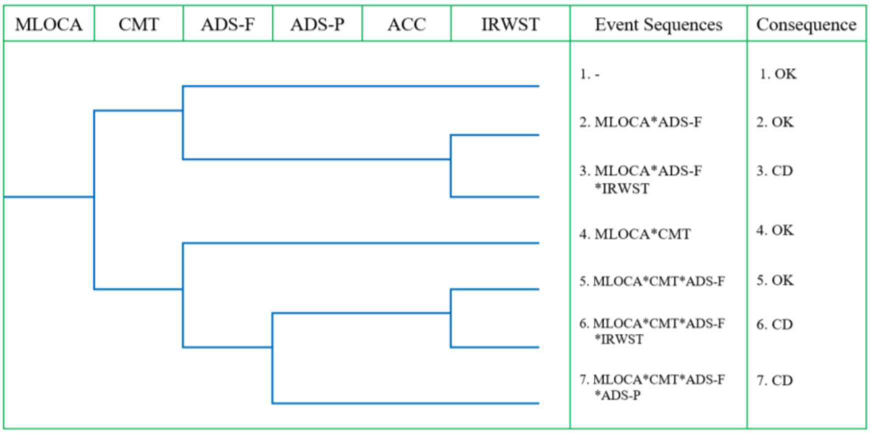
Event Sequences	Consequence
1. -	1. OK
2. LLOCA*IRWST	2. CD
3. LLOCA*ADS-F	3. CD
4. LLOCA*ACC	4. CD

Figure A2. *LLOCA ET model*



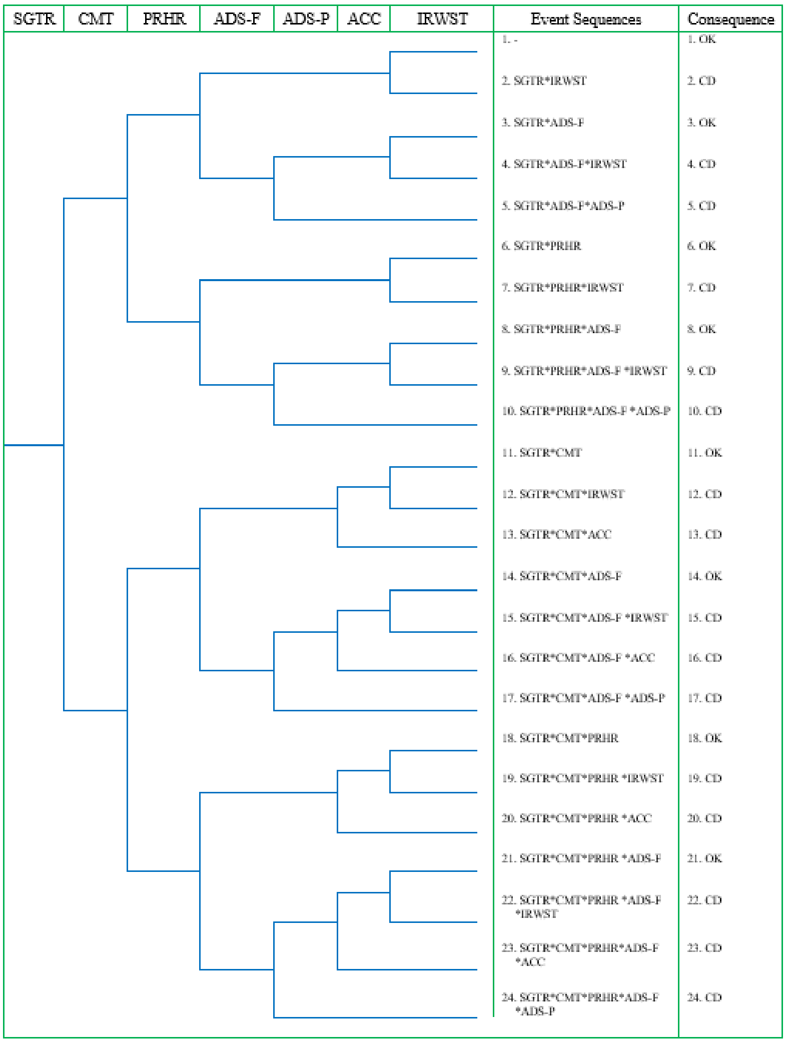
Event Sequences	Consequence
1. -	1. OK
2. SPADS*IRWST	2. CD
3. SPADS*ADS-F	3. CD
4. SPADS*ACC	4. CD

Figure A3. *SPADS ET model*



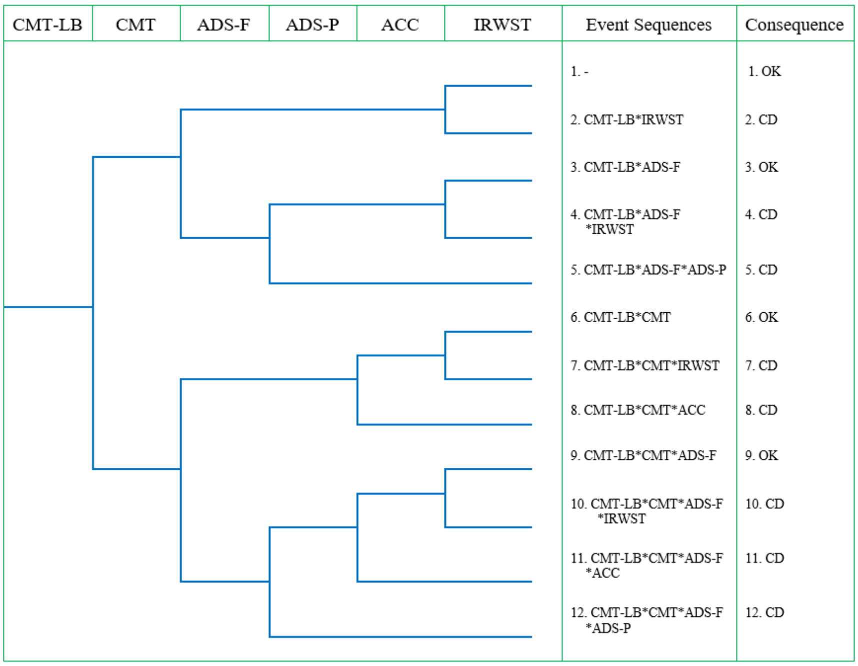
Event Sequences	Consequence
1. -	1. OK
2. MLOCA*ADS-F	2. OK
3. MLOCA*ADS-F *IRWST	3. CD
4. MLOCA*CMT	4. OK
5. MLOCA*CMT*ADS-F	5. OK
6. MLOCA*CMT*ADS-F *IRWST	6. CD
7. MLOCA*CMT*ADS-F *ADS-P	7. CD

Figure A4. *MLOCA ET model*



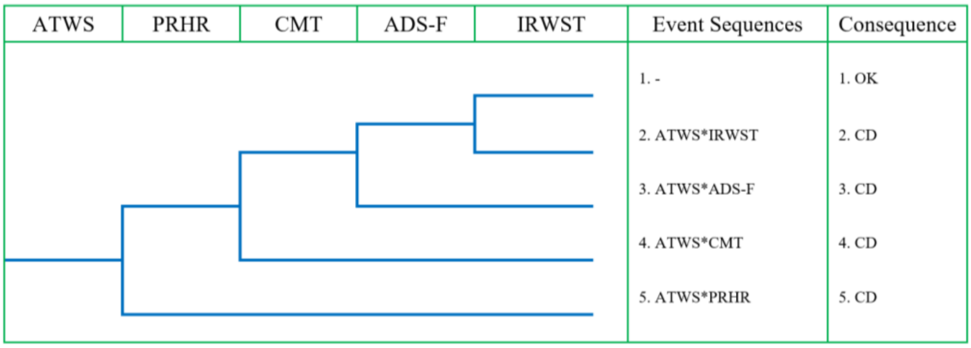
Event Sequences	Consequence
1. -	1. OK
2. SGTR*IRWST	2. CD
3. SGTR*ADS-F	3. OK
4. SGTR*ADS-F*IRWST	4. CD
5. SGTR*ADS-F*ADS-P	5. CD
6. SGTR*PRHR	6. OK
7. SGTR*PRHR*IRWST	7. CD
8. SGTR*PRHR*ADS-F	8. OK
9. SGTR*PRHR*ADS-F *IRWST	9. CD
10. SGTR*PRHR*ADS-F *ADS-P	10. CD
11. SGTR*CMT	11. OK
12. SGTR*CMT*IRWST	12. CD
13. SGTR*CMT*ACC	13. CD
14. SGTR*CMT*ADS-F	14. OK
15. SGTR*CMT*ADS-F *IRWST	15. CD
16. SGTR*CMT*ADS-F *ACC	16. CD
17. SGTR*CMT*ADS-F *ADS-P	17. CD
18. SGTR*CMT*PRHR	18. OK
19. SGTR*CMT*PRHR *IRWST	19. CD
20. SGTR*CMT*PRHR *ACC	20. CD
21. SGTR*CMT*PRHR *ADS-F	21. OK
22. SGTR*CMT*PRHR *ADS-F *IRWST	22. CD
23. SGTR*CMT*PRHR*ADS-F *ACC	23. CD
24. SGTR*CMT*PRHR*ADS-F *ADS-P	24. CD

Figure A5. *SGTR ET model*



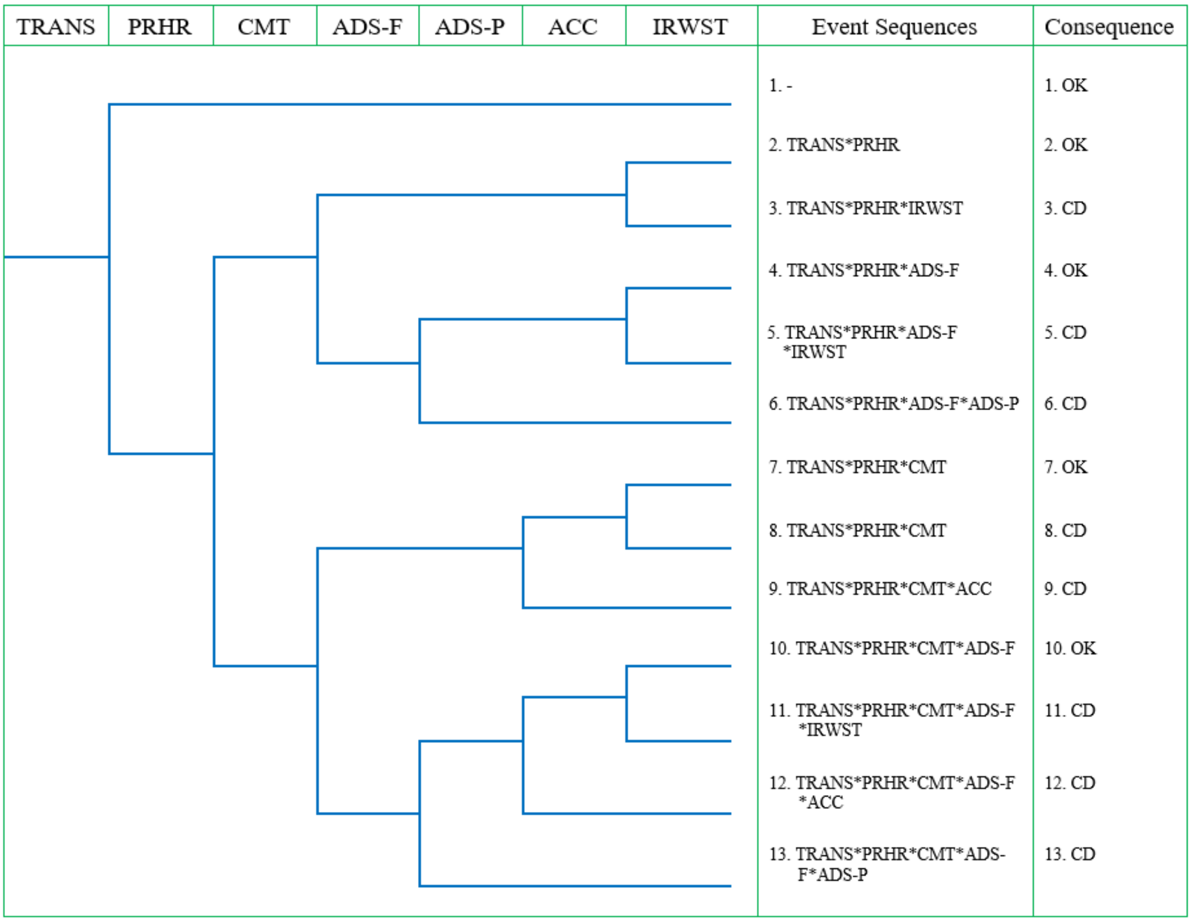
Event Sequences	Consequence
1. -	1. OK
2. CMT-LB*IRWST	2. CD
3. CMT-LB*ADS-F	3. OK
4. CMT-LB*ADS-F *IRWST	4. CD
5. CMT-LB*ADS-F*ADS-P	5. CD
6. CMT-LB*CMT	6. OK
7. CMT-LB*CMT*IRWST	7. CD
8. CMT-LB*CMT*ACC	8. CD
9. CMT-LB*CMT*ADS-F	9. OK
10. CMT-LB*CMT*ADS-F *IRWST	10. CD
11. CMT-LB*CMT*ADS-F *ACC	11. CD
12. CMT-LB*CMT*ADS-F *ADS-P	12. CD

Figure A6. *CMT-LB ET model*



Event Sequences	Consequence
1. -	1. OK
2. ATWS*IRWST	2. CD
3. ATWS*ADS-F	3. CD
4. ATWS*CMT	4. CD
5. ATWS*PRHR	5. CD

Figure A7. *ATWS ET model*



Event Sequences	Consequence
1. -	1. OK
2. TRANS*PRHR	2. OK
3. TRANS*PRHR*IRWST	3. CD
4. TRANS*PRHR*ADS-F	4. OK
5. TRANS*PRHR*ADS-F *IRWST	5. CD
6. TRANS*PRHR*ADS-F*ADS-P	6. CD
7. TRANS*PRHR*CMT	7. OK
8. TRANS*PRHR*CMT	8. CD
9. TRANS*PRHR*CMT*ACC	9. CD
10. TRANS*PRHR*CMT*ADS-F	10. OK
11. TRANS*PRHR*CMT*ADS-F *IRWST	11. CD
12. TRANS*PRHR*CMT*ADS-F *ACC	12. CD
13. TRANS*PRHR*CMT*ADS-F*ADS-P	13. CD

Figure A8. *Transient ET model*

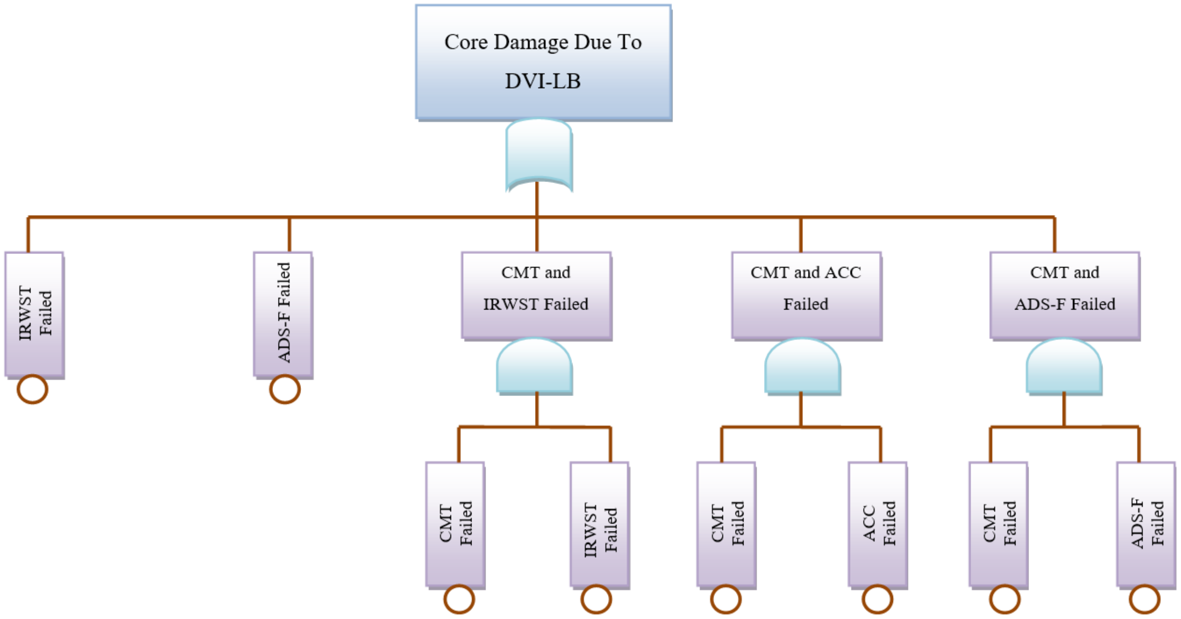


Figure B1. *FT model for DVI-LB ET model*

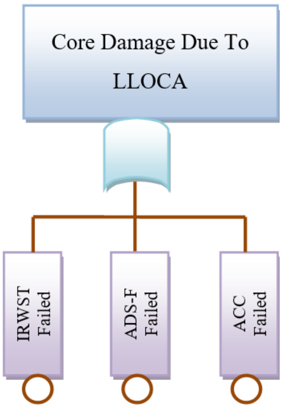


Figure B2. *FT model for LLOCA ET model*

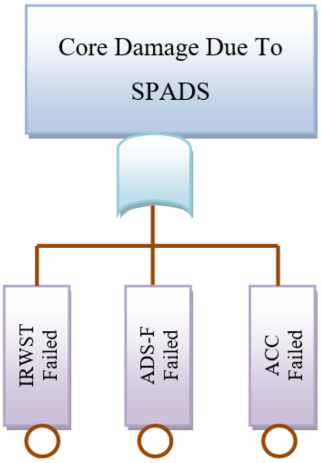


Figure B3. *FT model for SPADS ET model*

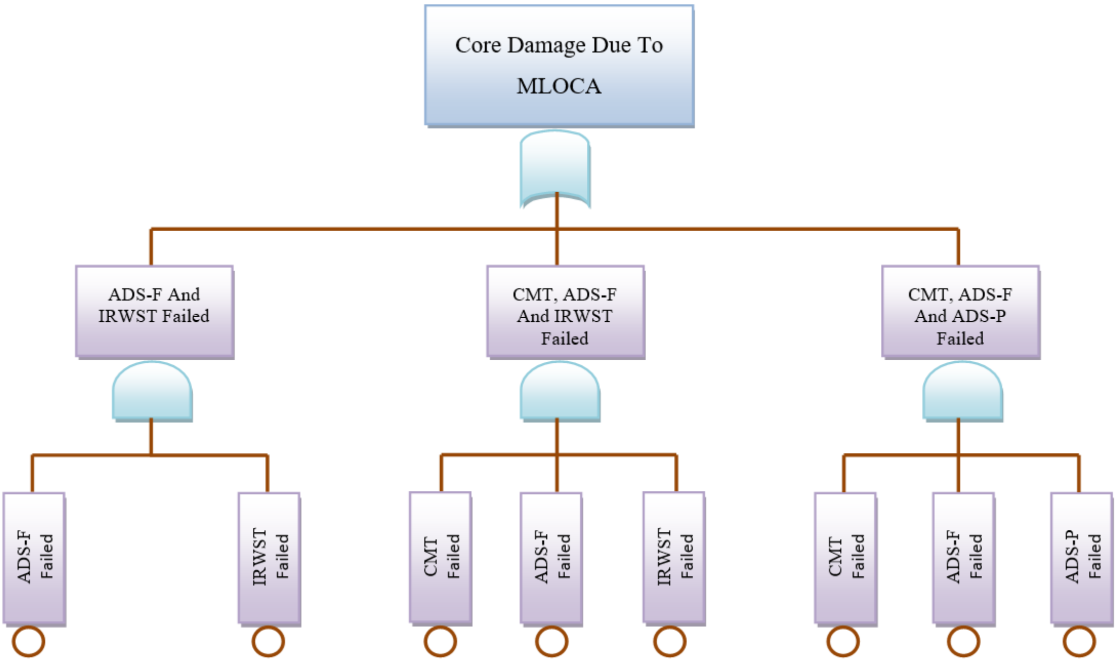


Figure B4. *FT model for MLOCA ET model*

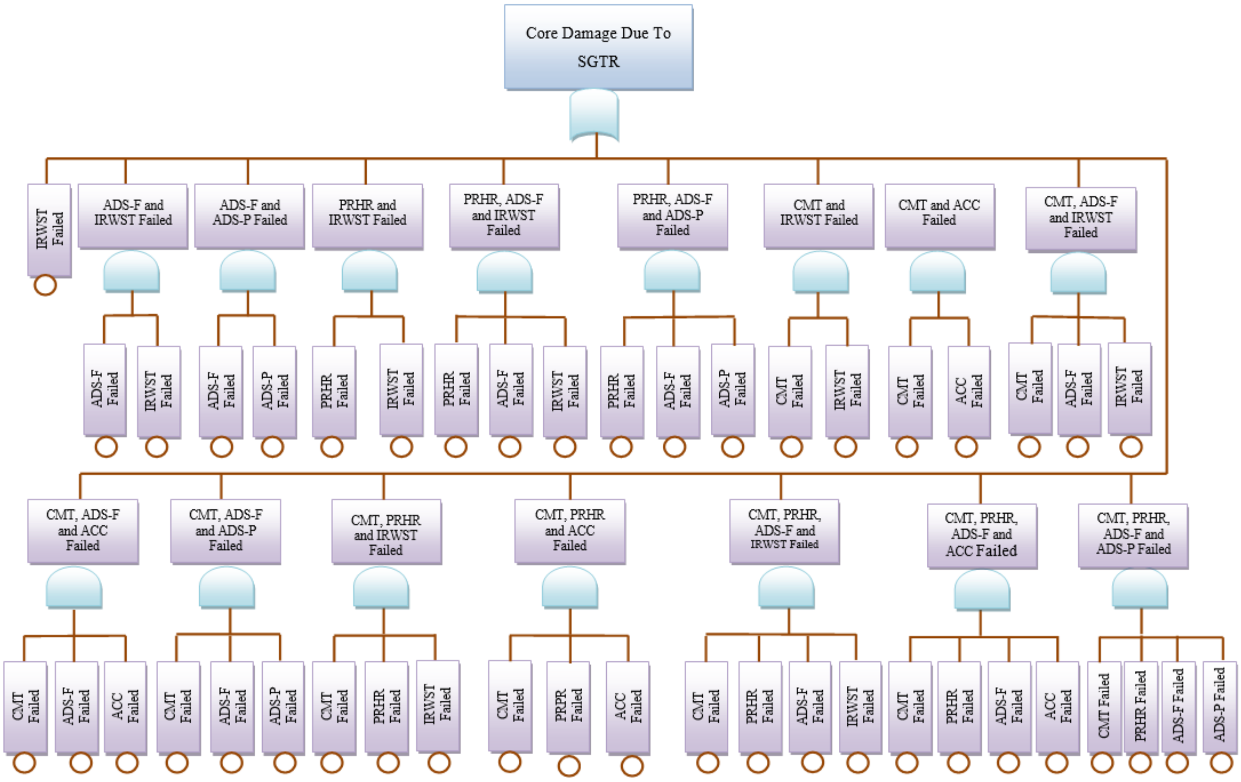


Figure B5. *FT model for SGTR ET model*

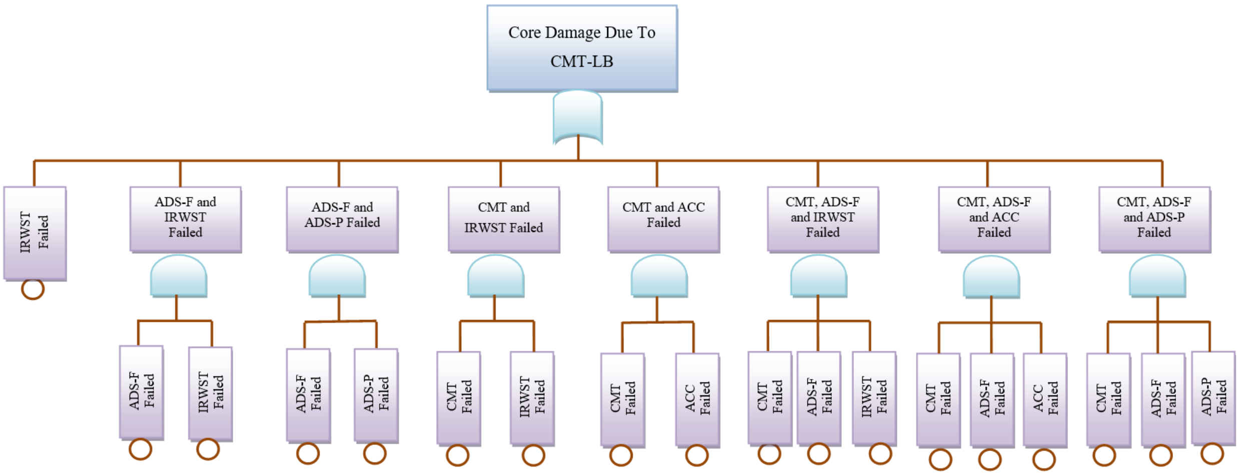


Figure B6. *FT model for CMT-LB ET model*

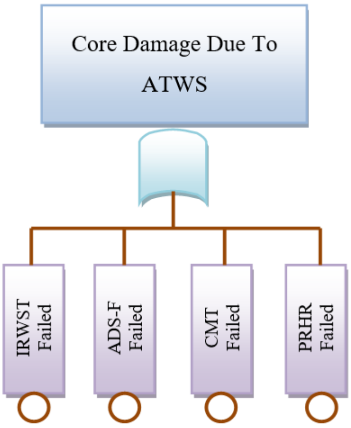


Figure B7. *FT model for ATWS ET model*

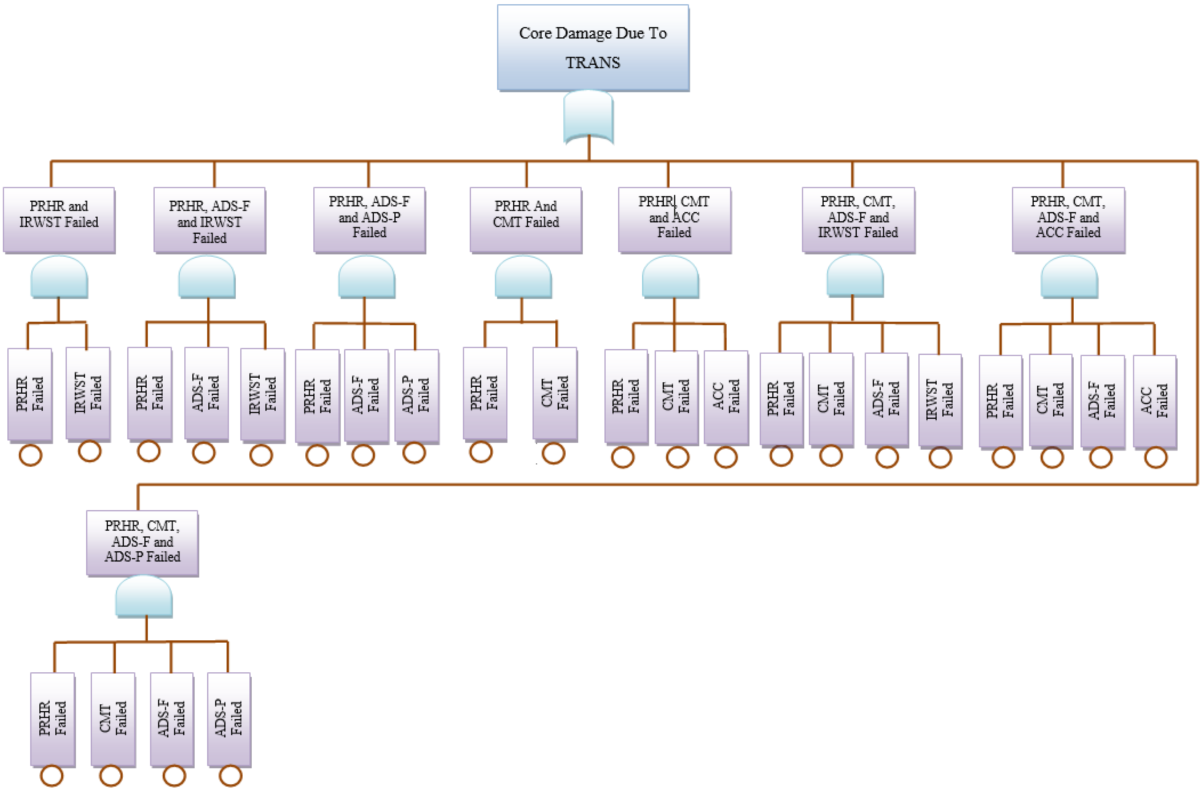


Figure B8. *FT model for Transient ET model*