

**QUANTITATIVE AND QUALITATIVE
RELIABILITY ASSESSMENT OF REPARABLE
ELECTRICAL POWER SUPPLY SYSTEMS
USING FAULT TREE ANALYSIS METHOD AND
IMPORTANCE FACTORS**

Authors:

Dallal. Kemikem , Mohamed.Boudour , Rabah. Benabid, Kambiz Tehrani

SCOPE OF PRESENTATION

“Reliability assessment of the electrical power supply system model of a Nuclear Power Plants (NPP) both quantitatively and qualitatively based on reliability modeling and using statistical and engineering methods called:

Fault Tree Analysis method and importance factors



CONTENTS

1. Introduction
2. Fault Tree Analysis method (FTA)
3. The main steps of fault tree
4. Basic Fault Tree Structure
5. Importance Factors
6. RiskSpectrum PSA software (RSW)
7. Main Screen of RSW
8. Modeling Steps
9. Results
10. Conclusion



INTRODUCTION(1/4)

The Nuclear Power Plants (NPP) is a system where the elements and sub-assemblies are themselves autonomous, interconnected and coordinated systems to meet the safety requirements of NPP that systems independently could not achieve when they are failing. The NPP is simply consisting of multiple systems which are physically separated. The exchanges between the systems are information's and not mass or energy. These systems are An engineered assemblage or combination of interrelated elements which are normally organized in a hierarchy of subsystems, components, and parts all working together as a unitary whole toward some significant common objective(s) or purpose(s).



INTRODUCTION(2/4)

Each nuclear power plant (NPP) has multiple, reliable and independent systems designed to prevent accidents, and reduce its effects should one occur. These systems are:

- Normal Power Plant Systems - Electrical (Generator and Support Systems, Substation, Normal Plant Electrical Distribution Systems and Emergency Electrical Distribution Systems).
- Normal Power Plant Systems – Mechanical.
- Emergency Safety Systems and Specialized Non-safety Nuclear Systems.
- Radioactivity monitoring system.
- Digital nuclear instrumentation system.
- Reactor emergency stop system & emergency core cooling system.
- Rod control & information system (RC & IS).
- Process computer systems.
- Nuclear power information system.
- Reactor Cooling Systems.



INTRODUCTION(3/4)

- The electrical power supply system of NPP is also composed of other systems, those systems operate independently and it must be reliable in all operation modes for safety purpose.
- There are physical separation between the systems
- It is generally composed of main power system (electrical grid), generator (house load operation), auxiliary power system and emergency power system (e.g. Diesel generator).
- The safety of the nuclear power plant depends on the availability of the continuous and reliable source of electrical energy during all modes of operation of the plant.
- Reliability assessment aimed at NPP's power supply system helps find out vulnerable spots to improve safety and reliability.



INTRODUCTION(4/4)

To fulfill the reliability assessment the following steps are carried out:

- The power system **reliability** was **assessed** and the main contributors to power system reliability have been identified, both qualitatively and quantitatively using **fault tree analysis** (FTA) method and **importance factors**.
- The **qualitative fault tree analysis** identifies the **minimal cut sets**. Cut sets are an important measure, indicating which combinations of component failures lead to system failures. (combinations of the smallest number of basic events, which, if occur simultaneously, lead to the top event).
- The **quantitative fault tree analysis** represents a calculation of the top event probability, equal to **the failure probability** of the corresponding system.
- The Importance Factors: Fussel-Vesely (FV), Birnbaum Importance, Risk Reduction Worth (RRW) and Risk Achievement Worth (RAW) are used to identify the most important components in the system.
- **Qualitative and quantitative analysis**, also **Importance Factors and Sensitivity analysis** are performed using **RiskSpectrumPSA** software, It is powerful software for reliability and safety analysis.



FAULT TREE ANALYSIS (FTA)

- ❑ FTA is a technique for reliability and safety analysis, it can be applied to complex or multi element systems.
- ❑ FTA is a systematic, deductive technique and graphical format which allow the understanding of system and relationship between subsystems (called events).
- ❑ FTA is a technique by which many events that interact to produce other events can be related using simple logical relationships.
- ❑ FTA is based on Boolean logic.
- ❑ FTA is mainly used for finding the faults and its root causes.
- ❑ FTA is supported by a wide range of software tools.



THE MAIN STEPS OF FAULT TREE ANALYSIS (1/2)

1. Identification of the FTA objectives

The objectives of the FTA can be as follows:

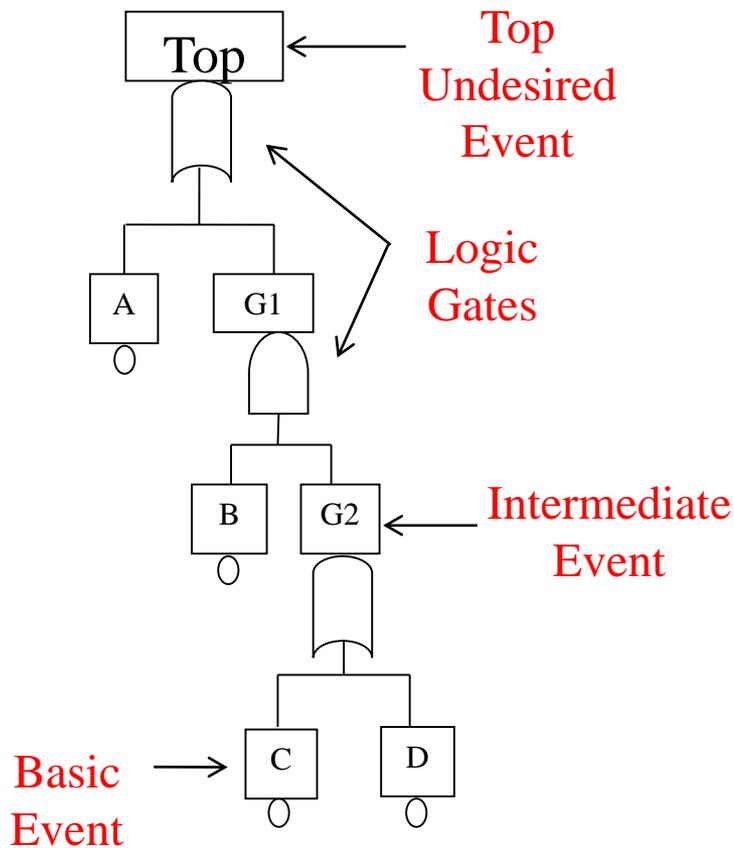
- ❑ Comparison of various design of the system in terms of reliability.
 - ❑ Reliability evaluation of the system under study.
 - ❑ Identification of the most important components to the safety and therefore decrease their maintenance period.
- ## 2. Definition of the undesired event (top event).
- ## 3. Construction of the fault tree respecting the following points:
- ❑ Usually several different, but equivalent, fault trees can be constructed for the given system. also, different top events load to different fault trees.
 - ❑ For any specified Top event, each possible event is examined to see whether it can, either alone or in conjunction with some other event(s), cause the Top event.
- 

THE MAIN STEPS OF FAULT TREE ANALYSIS (2/2)

- ❑ The primary events (Intermediate Event) that lead to the Top event and the secondary events (Basic Event) that cause each of the primary events are determined. the procedure is continued until all the basic failures are identified (basic events).
 - ❑ The set of events that are all required to produce an event of interest are connected to AND gates.
 - ❑ The set of events that can individually produce an event of interest are connected to OR gates.
4. Qualitative assessment of the fault tree.
 5. Quantitative assessment of the fault tree.
 6. Interpretation of the obtained results.



BASIC FAULT TREE STRUCTURE



Logic equations:

$$Top = A + G_1$$

$$G_1 = B \times G_2$$

$$G_2 = C + D$$

Minimal cut sets (MCS):

$$Top = A + BC + BD$$

Qualitative assessment of FT

MCS is composed of first and second order cuts.

Basic event failure probabilities:

$$P_A, P_B, P_C, P_D$$

Top event probability:

Quantitative assessment of FT

$$P_{Top} = P_A + (P_B \times P_C) + P_B \times P_D$$

IMPORTANCE FACTORS (1/3)

It is obvious that some components in a system are more important for the system reliability than other components. For this, the importance factors used RiskSpectrum PSA software and Matlab are calculated.

Importance measures are often used as:

- ❑ Tools for evaluating and classifying the impact of components on the system behavior with respect to reliability
- ❑ Tools to identify components that should be modified or replaced with higher quality components

The most frequently used importance factors are:

- **Fussell-Vesely (FV):**

$$I^{FV}(i/t) = \frac{\sum_{C_j: x_i \in C_j} P(C_j)}{1 - h(p(t))} \quad \text{for } i: 1, \dots, n$$

where x_i represents the failure of component i , C_j denotes the minimal cut set, and $h(p(t))$ represents the system reliability with respect to a specified system function.



IMPORTANCE FACTORS (2/3)

- ***Risk Reduction Worth (RRW):***

$$I^{RRW}(i/t) = \frac{1 - h(p(t))}{1 - h(1_i, p(t))} \quad \text{for } i = 1, \dots, n$$

$h(1_i, p(t))$ denotes the (conditional) probability that the system is functioning when it is known that component i is functioning at time t .

- ***Risk Achievement Worth (RAW):***

$$I^{RAW}(i/t) = \frac{1 - h(0_i, p(t))}{1 - h(p(t))} \quad \text{for } i = 1, \dots, n$$

$h(0_i, p(t))$ denotes the (conditional) probability that the system is functioning when component i is in a failed state at time t .



IMPORTANCE FACTORS (3/3)

○ Birnbaum Importance:

Birnbaum's importance measure of component i at time t is computed as follows:

$$I^B(i/t) = h(1_i, p(t)) - h(0_i, p(t)) \quad \text{for } i = 1, \dots, n$$

Where,

- $h(1_i, p(t))$ denotes the (conditional) probability that the system is functioning when it is known that component i is functioning at time t ,
- $h(0_i, p(t))$ denotes the (conditional) probability that the system is functioning when component i is in a failed state at time t .



RISKSPECTRUM PSA SOFTWARE (RSW)

- The complete linked Fault Tree and Event Tree tool and powerful calculation engine
- Includes:
 - Data editor
 - Fault Tree editor.
 - Event Tree editor.
 - Analysis Tool (MCS generator).
 - Importance Analysis
 - Sensitivity Analysis
- All data stored in a relational database:
- Easy to browse, find relations and ,update .
- data is never repeated but stored in one place.
- Capability to handle very large FT models
- Solve Boolean equations => MCSs

Before the construction of FT, a reliability model must be associated with each basic event in the tree. A reliability model is a set of mathematical formulas that specify how to calculate the reliability characteristics of a basic event.

Each reliability model has one or more parameters that appear in the formulas.



MAIN SCREEN OF RSW

1 Data Editing that enables to quickly introduce all input information about basic event to build fault trees, run analysis and study results

2

3

All input information are converted in Boolean equation which need to be combined into one by applying the rules of Boolean algebra to obtain the equation for top event, consisting of basic events products sum. The calculation of the top event probability is presented as follows:

Each basic event is described by a reliability model and associated with a probability measure. Monitored, repairable components model is applied for components in our case. This reliability model represents the repairable components. The failure and repair process are represented using exponential distributions. The required reliability data for this model are the failure rate (λ) and the repair rate (μ). In this model, the unavailability $Q(t)$ is computed as follows

$$Q_{Top\ event} = \sum_{i=1}^n Q_{MCS_i}$$

$$Q_{MCS_i} = \prod_{i=1}^m Q_{B_i}$$

$$Q = \frac{\lambda}{\lambda + \mu}$$

Data Reports

MODELING STEPS

The proposed method is tested on the practical example of the NPP's power supply system. Its operating modes are 

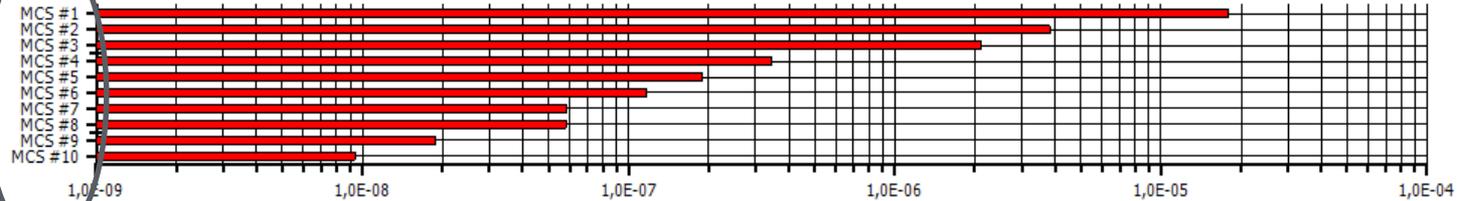
The components in the system are all repairable with constant failure rate λ and constant repair rate μ , some of them had two failure modes.

- 1) FT is constructed using Riskspectrum PSA software. 
- 2) The reliability of electric power supply system model is performed using **quantitative and qualitative** FTA
- 3) Finally results are interpreted



RESULTS

The MCSs are a synthetic result which identifies the critical components. The most important MCS identified from the FT built for the 1LHA Bus are:



Qualitative assessment

#	Probability	MCSs
<i>Top event</i>	2.474E-05	
1	1.80E-05	1LGP-FAIL, BR4-FAIL
2	3.82E-06	1LHA-FAIL2
3	2.10E-06	1LHA-FAIL1
4	3.45E-07	1LGB-FAIL2, 1LGP-FAIL
5	1.90E-07	1LGB-FAIL1, 1LGPFail
6	1.17E-07	1LGP-FAIL, OFFSITEPOWER220kV, TRANSFORMER-FAIL2
7	5.81E-08	1LGP-FAIL, BR3-FAIL, OFFSITEPOWER220kV
8	5.81E-08	1LGP-FAIL, BR2-FAIL, OFFSITEPOWER220kV

The top event failure probability is 2.474E05 and the number of Minimal cuts is 89. MCS contains first, second and third order cuts.

The simultaneous failures of diesel generator (1LGP) and breaker 4 (BR4) have the greatest contribution to the top event with a percentage of 72.73% while the failure of the 1LHA Bus contribute with 15.43% and 8.49% according to failure mode(1,2). **This result is logic because** the disconnecter is ideal and the failure frequency of the bus 1LHA according to failure mode(1,2). (3,679E-03; 4,643E-04) is less than those of 1LGP (1,743E+02) and BR4 (3,030E-02).

RESULTS

- According to the importance factors, the major components contributors to the unavailability of power from the 1LHA bus are:

□ FV means that at least the component i is at least in a MCS which lead to “no power on the 1LHA bus” (Top event) and it is the most critical. This is correct according to MCSs . Notice from table that the Fussell-Vesely values are the highest for diesel generator 1LGP and Breker 4, they are also the most unreliable components.

ID basic event	Description of Basic Events	FV	RRW	RAW
1LGP-FAIL	Failure of diesel generator	7.61E-01	4.18E+00	8.65E+00
BR4-FAIL	Failure of breaker 4	7.27E-01	3.67E+00	3.66E+03
1LHA-FAIL2	Failure of bus 1LHA according to failure mode 2	1.54E-01	1.18E+00	4.04E+04
1LHA-FAIL1	Failure of bus 1LHA according to failure mode 1	8.49E-02	1.09E+00	4.04E+04
1LGB-FAIL1	Failure of bus 1LGB	1.40E-02	1.01E+00	3.66E+03
BR3-FAIL	failure of breaker 3	9.72E-03	1.01E+00	4.00E+00

RESULTS

ID basic event	I^B
1LGP-FAIL	2.0803E-004
BR4-FAIL	0.0905
1LHA-FAIL2	1
1LHA-FAIL1	1
1LGB-FAIL1	0.0905
BR3-FAIL	7.440Ee-005

Birnbaum importance are calculated using Matlab.

- ❑ A small change in the reliability of diesel generator 1LGP and Breaker 3 will result in a comparatively large change in the reliability of Bus 1LHA at time t.
- ❑ The rate at which the availability of Bus 1LHA increases as the availability of component 1 LHA(1,2) and Breaker 4 increases.

RESULTS

- ❑ Components with the highest value of RAW are the Bus 1LHA (1,2), the Breaker 4 and Bus1LGB (1), . These components should be maintained well, so the reliability of the system is not reduced significantly. In consequence, the maintenance priority for those components should be set high.
- ❑ The important components with the highest values of RRW are the diesel generator (1LGP) . It should also be noted that the values for Breaker 4 and the Bus1LHA (1,2) are notably large. It is worth increasing the reliability of these respective components, so the system reliability can be increased significantly.



RESULTS

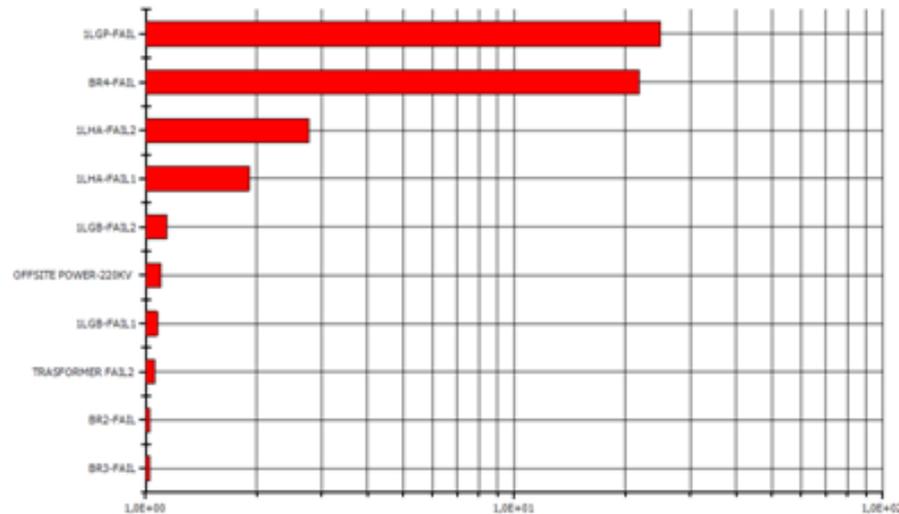
- RRW represents the maximum decrease in Top event (no-power supply of the 1LHA Bus) that can be expected to improve the reliability of the component i. Improving the reliability of those components (1LGP, BR4,1LHA, ...) in decreasing order most likely increased the reliability of Top event.
- RAW represents the immunity of the power supply system with respect to the failure of components (1LGP, BR4,1LHA, ...) in increasing order

in addition to all analysis, the determination of how rapidly the output of an analysis changes with respect to variation in the input, an analysis of sensitivity is carried out.



RESULTS

Sensitivity analysis is used to assess how the system behaves when the input parameters of each component varies.



- Using Risk spectrum software we conclude that the failure probability of the top event is most sensitive to the reliability data of the following components sorted in decreasing order: (1LGP, BR4, 1LHA (two failure modes), OFFSITEPOWER220kV, LGB-FAIL1, TRASFORMER-FAIL2, BR2 and BR3) and their values are: 2.49E+01, 2.18E+01, 2.77, 1.91, 1.14, 1.10, 1.08, 1.06, 1.03, 1.03.



- ❑ The objectives of the sensitivity analysis is to understand the sensitivity of the overall failure results of the Bus 1LHA towards the reliability parameters of the particular basic event. The idea is to find that the occurrence of top event “no power on the 1LHA bus” are sensitive to some of the BE mentioned above (1LGP, BR4, 1LHA (1,2),..).
- ❑ Then we need to spend efforts to verify whether the parameters used for this particular component are realistic. If not we need to try to provide as realistic as possible analysis for the reliability parameters of this component, not to bias the final results.
- ❑ The sensitivity analysis could be done also for assumptions and simplifications (more important area) used during the modeling of system. In this case the idea is to check how sensitive the results are towards the assumptions made, and then make more detailed analysis for the assumptions that appears to be the most sensitive ones .



CONCLUSION

The qualitative and quantitative analysis of the FT allowed us to:

- Model the possible combinations of components failures, that can lead to the undesired event "no power on 1 LHA bus",
- Calculate the probability of top event based on the probability of the MCSs,
- Show the most important MCSs identified from the FT,
- Rank the components based on the calculation of importance factors and give the most sensitivity of the failure probability of the top event to the reliability data.
- the method used in this article can be used for other types of production system among others (solar or wind park)



Thank you for your attention



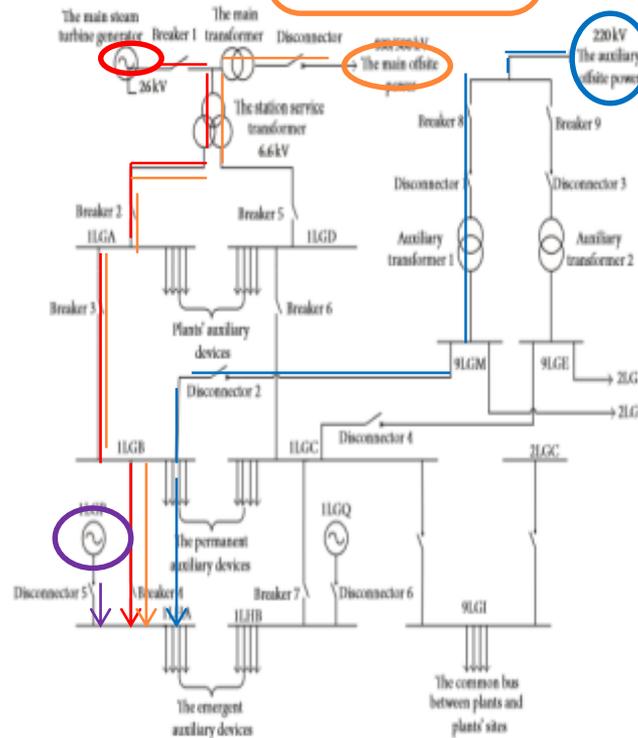
OPERATING MODE OF NPP'S POWER SUPPLY SYSTEM

Normal operation of NPP

Shutdown state of NPP

Loss power from 26kV bus (generator + main offsite Grid)

Loss of generator, main and auxiliary offsite power supplies



FT CONSTRUCTION IN RSW

Fault Tree editor

MCS generator

Data editor

The screenshot displays the RiskSpectrum software interface. The main window shows a table of analysis results for a fault tree case named '1LHA'. The table includes columns for ID, Char #, Description, Calculation type, MCS Result, UNC Mean, TD Mean, 5th perc., and Median. The event '1LHA' is highlighted, with a description of 'no power on 1LHA bus' and an MCS result of 2.47E-05.

ID	Char #1	Description	Calculation type	MCS Result	UNC Mean	TD Mean	5th perc.	Median
1LGA-NOT SUP		1LGA bus not supplied	Q	6,18E-04				
1LHA		no power on 1LHA bus	Q	2,47E-05	2,47E-05	2,33E-05	2,47E-05	2,47E-05
1LHA-BUS NOT SU		1LHA bus not supplied	Q	1,82E-05				
1LHA-FAIL		1LHA bus fail according to failure mode(1,2)	Q	5,91E-06				

Below the main table, a 'Results' tab is active, showing a table of minimal cut sets. The top event probability is Q = 2.474E-05. The table lists 14 minimal cut sets, each with a probability and a percentage. A dashed box highlights the first four cut sets, which are labeled as 'minimal cut sets'.

No	Probability	%	Event 1	Event 2	Event 3	Event 4	Event 5	Event 6	Event 7	Event 8	Event 9	Event 10
1	1,80E-05	72,73	1LGP-FAIL	BR4-FAIL								
2	3,82E-06	15,43	1LHA-FAIL									
3	2,10E-06	08,49	1LHA-FAIL									
4	3,45E-07	01,40	1LGP-FAIL	1LGP-FAIL								
5	1,90E-07	00,77	1LGP-FAIL	1LGP-FAIL								
6	1,17E-07	00,47	1LGP-FAIL	OFFSITE POWER-2	TRASFORMER FAIL2							
7	5,81E-08	00,23	1LGP-FAIL	BR2-FAIL	OFFSITE POWER-220KV							
8	5,81E-08	00,23	1LGP-FAIL	BR3-FAIL	OFFSITE POWER-220KV							
9	1,88E-08	00,08	1LGP-FAIL	TRANSFORMER1-F	TRASFORMER FAIL2							
10	9,36E-09	00,04	1LGP-FAIL	BR2-FAIL	TRANSFORMER1-FAIL2							
11	9,36E-09	00,04	1LGP-FAIL	BR3-FAIL	TRANSFORMER1-FAIL2							
12	7,19E-09	00,03	1LGP-FAIL	BR8-FAIL	TRASFORMER FAIL2							
13	3,58E-09	00,01	1LGP-FAIL	BR2-FAIL	BR8-FAIL							
14	3,58E-09	00,01	1LGP-FAIL	BR3-FAIL	BR8-FAIL							

