Dynamic reliability and safety analyses for a passive safety system of VVER440 type reactor

Zoltan Kovacs[a], Pavol Hlavac[a], Robert Spenlinger[a]
[a]RELKO Ltd, Engineering and Consulting Services, Bratislava, Slovakia

Abstract: Dynamic Probabilistic Safety Assessment (DPSA) is a powerful tool used in risk-informed decision making in various fields, particularly in the nuclear industry. It enhances traditional PSA by considering time-dependent aspects of system behavior, including the effects of aging, maintenance, and operational changes. In addition, failure data about components is required for the purposes of reliability analysis. In practice, it is not always possible to fully obtain this data due to unavailability of primary observations and consequent scarcity of statistical data about the failure of components. To handle such situations, fuzzy set theory has been successfully used in novel PSA. The paper presents an application of dynamic fuzzy fault tree (using fuzzy operators gates) in risk-informed decision making for a passive safety system (core flooding system - hydraulic accumulator) of the VVER440 type reactor. Fuzzy fault tree construction is a specialized method used in reliability engineering and risk analysis to assess and model the potential failure modes and system vulnerabilities of a complex system. It is an extension of traditional fault tree analysis, which uses Boolean logic to represent system failures. In contrast, fuzzy fault trees incorporate fuzzy logic to handle time dependence, uncertainties and vagueness in the failure probabilities and input parameters.

Keywords: PSA, Dynamic PSA, Fuzzy Fault Tree, VVER440 Type Reactor.

1. INTRODUCTION

Fault tree analysis is widely used to assess the operational performance, reliability prediction, lifetime, and system safety of various complex systems involved in a nuclear power plant. There are several issues for comparison between fuzzy fault tree analysis and conventional fault tree analysis. Conventional fault tree analysis uses the crisp value probabilistic considerations, while linguistic variables and possibility is considered in fuzzy fault tree analysis. Conventional fault tree analysis does not give information concerning the tolerances and variation of the probability values, and the dependencies of the events, while fuzzy fault tree analysis usually uses a triangular or trapezoidal possibility, and takes into account the uncertainty in calculations. In conventional fault tree analysis, the importance of the basic event is measured based on the direct contribution to the top event, while in fuzzy fault tree analysis the contribution of uncertainties is also considered.

Further in fault tree analysis, it might be necessary to consider possible failure of components even if they have never failed before and there is no data available associated with the possible failure. The use of fuzzy fault tree analysis makes it possible to consider any possible failure events, using expert elicitation and possibility approach. This approach has been found capable to handle the linguistic variables and the imprecision of the uncertainties associated with the modeling of failures and their dependency.

In addition, fault tree analysis is not suitable where available data are insufficient for statistical inferences, or the data show a large variation. Fuzzy methodology might be the only approach when little quantitative information is available regarding fluctuations in the parameters. In fact, the experiences of experts provide an effective database supporting the estimation of required data, although they have to face the numerous conflicting evaluations. Actually, the management of the large number of tangible and intangible attributes that must be taken into account represents the main complexity of the problem. Application of fuzzy set theory makes it possible to elicit the expert judgment which is often given in natural language as linguistic variables. Building a fuzzy relation matrix through fuzzy fault tree analysis makes it possible to identify the relationship between failure modes, fuzzy symptoms and basic events, for diagnosis purposes. It takes into account the uncertainties and fuzziness of the symptoms and facilitates the effective use of information represented by fuzzy methodology. Combining fuzzy theory with fault tree analysis makes it possible to diagnose faults efficiently and can be easily designed with an aim of online prevention of the fault. The

review reveals the effectiveness of the fuzzy fault tree analysis in comparison with conventional fault tree analysis, when there is inadequate.

Fuzzy fault tree construction is a specialized method used in reliability engineering and risk analysis to assess and model the potential failure modes and vulnerabilities of a complex system. It is an extension of traditional fault tree analysis, which uses Boolean logic to represent system failures. In contrast, fuzzy fault trees incorporate fuzzy logic to handle uncertainties and vagueness in the failure probabilities and input parameters.

After introduction, description of fuzzy fault tree approach is presented in the second part of the paper based on the references [1-4]. The third part is focused on application of fuzzy fault tree in reliability analysis of the core flooding system. Conclusions are summarized in the fourth part of the paper.

2. DESCRIPTION OF FUZZY APPROACH

Although, fault tree analysis users can easily understand and clearly find out the causes of top undesired events from systematic diagram, the approach has weak points in solving problems with uncertain failure rates of basic events. To overcome these problem researchers combined fuzzy concept to fault tree analysis and invented fuzzy fault tree analysis method to solve the problem of uncertain failure rates of basic events.

2.1. Fuzzy Logic

Reasoning in fuzzy logic is just a matter of generalizing the familiar yes-no (Boolean) logic. If true is the numerical value of 1 and false the numerical value of 0, these values indicate that fuzzy logic also permits values like 0.1 and 0.663.

Fuzzy set theory allows an element of a set to have a membership value from the interval [0,1]. Let X be a collection of object universe and its elements are represented by x. A fuzzy set A in X can be characterized by a membership function : μ_A: $X \rightarrow [0,1]$. The value of function $\mu_A(x)$ represents the degree of membership of x in A.

A membership value 1 means the element is completely in set A and 0 means the element is completely not in set A.

2.2. Fuzzy Number

Fuzzy number can be represented by a triangular or trapezoidal shape or bell shaped membership function. Generally triangular and trapezoidal membership functions are widely used to represent the failure nature of equipments. Triangular membership functions are used to represent more or less probability estimation of failure occurrence (e.g., the probability of failure occurrence is about 0.0001) and a trapezoidal membership function is better to used in describing failure probability interval of equipments (e.g., the probability of failure occurrence lies between 0.00001 and 0.000025). Due to the failure nature of the core flooding system, triangular fuzzy number is used in further calculations of this study. Details properties and calculation of triangular fuzzy number are discussed below.

A fuzzy number A is termed as triangular fuzzy number if the membership function of fuzzy number A is defined by the following equation:

$$\mu_{\mathrm{A}}(x) = \begin{cases} \dfrac{x - a_1}{a_2 - a_1}, & for\ a_1 < x < a_2, \\ \dfrac{a_3 - x}{a_3 - a_2}, & for\ a_2 \le x < a_3, \\ 0, & otherwise. \end{cases}$$

A triplet (a_1, a_2, a_3) can represent the triangular fuzzy number. The left and right expansions of triangular fuzzy number and the confidence level of probability of uncertain events can be obtained from statistical data and expert judgment of the analyzed system. In the triangular fuzzy number $A = (a_1, a_2, a_3)$, the element a_2 gives the maximal degree of membership. It means that a_2 is the value with the highest degree of membership. At the same time, a_1 and a_3 are the lower and upper bound of the evaluation data, respectively (see Figure 1).

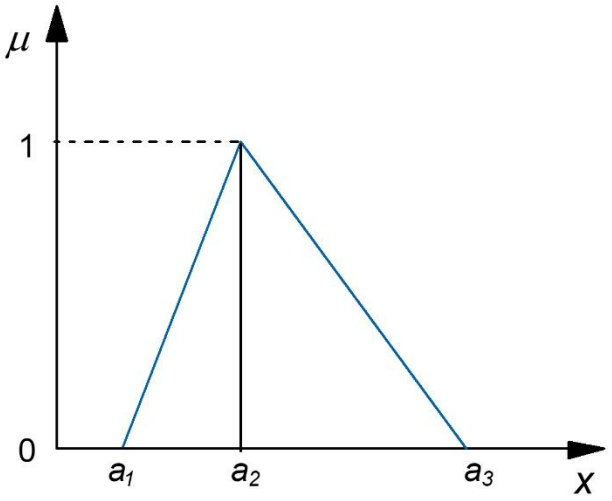

Figure 1. Triangular membership function

2.3. Fuzzy Fault Tree Analysis

A generic overview of the fuzzy fault tree analysis is shown in Figure 2. The figure shows four phases in the fuzzy fault tree analysis of a system. In the qualitative analysis phase, the fault trees are developed, fault tree gates and events are numbered and finally minimal cut sets are determined. There are many tools available to create fault trees. The outcomes of the qualitative analysis (basic events) feed into the fuzzy data approximation and quantitative analysis phases. Quantitative analysis uses minimal cut sets and fuzzy probabilities for basic events. Although mathematical formulas are available to quantify AND and OR operators that link events in the minimal cut sets, these are only suitable for crisp values. For this reason, it is necessary to define fuzzy operators for logic gates.

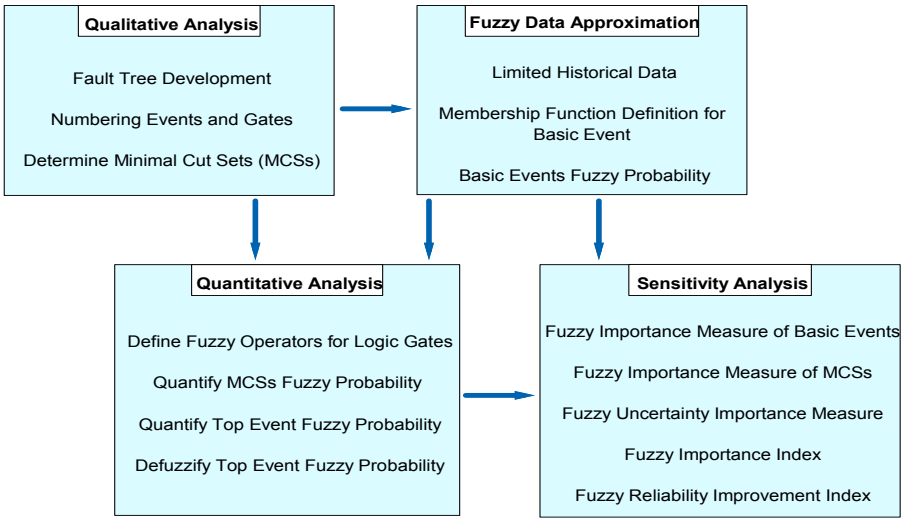

Figure 2. A generic overview of the fuzzy fault tree analysis

If the fuzzy probability of the event E_i is represented by a triangular fuzzy number as $P_i(t) = \{a_i(t), b_i(t), c_i(t)\}$, then the fuzzy operator for the AND gate with N input events can be determined as :

$$P_{FAND} = AND_F\{P_1(t), P_2(t), \ldots, P_N(t)\} = \prod_{i=1}^{N} P_i(t) = \left\{\prod_{i=1}^{N} a_i(t), \prod_{i=1}^{N} b_i(t), \prod_{i=1}^{N} c_i(t)\right\}$$

If the fuzzy probability of the event E_i is represented by a triangular fuzzy number as $P_i(t) = \{a_i(t), b_i(t), c_i(t)\}$, then the fuzzy operator for the OR gate with N input events is defined as:

$$P_{FOR} = OR_F\{P_1(t), P_2(t), \ldots, P_N(t)\} = 1 - \prod_{i=1}^{N}(1 - P_i(t))$$

$$= \left\{1 - \prod_{i=1}^{N}(1 - a_i(t)), 1 - \prod_{i=1}^{N}(1 - b_i(t)), 1 - \prod_{i=1}^{N}(1 - c_i(t))\right\}$$

For illustration, a simple fault tree is considered from Figure 3. The top event of this fault tree can be logically expressed as:

TOP EVENT = Z1+Z2 = Y1.Y2 + Y3.Y4

where '+' and '.' represent logical OR and AND, respectively. Fuzzy failure rates and fuzzy failure probabilities of the basic events in triangular form are shown in Table 1.

Table 1. Fuzzy failure data for basic events (t=1000 hours)

Basic Event	Fuzzy Failure Rates			Fuzzy Failure Probabilities		
	λ_{i1}	λ_{i2}	λ_{i3}	$a_{i1}(t)$	$b_{i2}(t)$	$c_{i3}(t)$
Y1	1.00E-5	2.00E-5	3.00E-5	0.01	0.02	0.03
Y2	2.00E-5	4.00E-5	5.00E-5	0.02	0.04	0.05
Y3	3.00E-5	5.00E-5	6.00E-5	0.03	0.05	0.06
Y4	3.00E-5	4.00E-5	5.00E-5	0.03	0.04	0.05

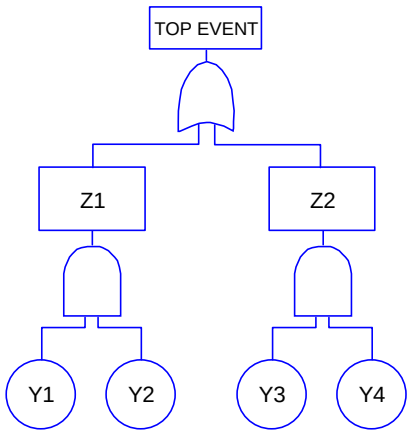

Figure 3. Fuzzy fault tree for illustration

Using the fuzzy operators of AND gate and the data from Table 1, the fuzzy probabilities of the minimal cut sets can be estimated as: *Pr {Z1} (t) = {0.0002, 0.0008, 0.0015}* and *Pr{Z2} (t) = {0.0009, 0.0020, 0.0030}.*

Now using the fuzzy operators of the OR gate and the fuzzy probabilities of the minimal cut sets, the fuzzy top event probability is: *Pr {TOP EVENT} = {0.0011, 0.0028, 0.0045}*. This result implies that the probability of the top event is between 0.0011 and 0.0045, and the most probable value is 0.0028.

2.4 Defuzzification

As fuzzy numbers are used for uncertainty quantification process in system safety and reliability engineering, the results obtained are also fuzzy numbers. Defuzzification is a process of converting fuzzy numbers into crisp values. A number of approaches, such as: the weighted average approach, the mean max membership approach, the centre of area approach, the mean of maxima approach, the centre of maxima approach, and the centroid approach are available for defuzzification process. No single defuzzification technique is suitable for all applications. The "centre of area" method is one of the widely used methods for the defuzzification of fuzzy numbers in reliability engineering applications. According to this method, a triangular fuzzy number $A = [a_1,b_1,c_1]$ can be defuzzified as:

$$X = \frac{\int x\mu_{\tilde{A}}(x)dx}{\int \mu_{\tilde{A}}(x)dx} = \frac{\int_{a_1}^{b_1} \frac{x-a_1}{b_1-a_1}xdx + \int_{b_1}^{c_1} \frac{c_1-x}{c_1-b_1}xdx}{\int_{a_1}^{b_1} \frac{x-a_1}{b_1-a_1}dx + \int_{b_1}^{c_1} \frac{c_1-x}{c_1-b_1}dx} = \frac{1}{3}(a_1 + b_1 + c_1)$$

The defuzzified value of the above fuzzy number is: (0.0011 + 0.0028 + 0.0045)/3 = 0.0028.

2.5 Fuzzy Importance Measure

In conventional fault trees, there are several kinds of importance measures: Birnbaum importance measure, Fractional contribution, Fussell-Vesely importance measure, risk increase factor and risk decrease factor. These importance measures are calculated to know the importance of a basic events in minimal cut sets of a system. In fuzzy fault tree analysis, fuzzy importance measure of a basic event is calculated by measuring the difference between two fuzzy probabilities of the top event of a fault tree with and without existence of that basic event.

Two fuzzy importance measure methods are presented and compared the results with each other to verify the results: 1) Fuzzy distance method and 2) Fuzzy ranking method.

Fuzzy distance method

In fuzzy fault tree analysis, fuzzy importance measure of a basic event or component is calculated by measuring the difference between two fuzzy probabilities of the top event of a fault tree with and without existence of that basic event. The fuzzy important measure of basic events can be evaluated by using fuzzy distance method. First calculate the fuzzy number $(G_T - G_{Ti})$ where i = 1, 2, 3,... for all basic events and find the maximum fuzzy number of $(G_T - G_{Ti})$. Then the fuzzy distance between each fuzzy number $(G_T - G_{Ti})$ and the maximum fuzzy number of $(G_T - G_{Ti})$ are calculated by Graded Mean Integration Representation (GMIR) distance method. GMIR of a triangular fuzzy number $G = (a,b,c)$ can be found as follow:

$P(G) = (a + 4b + c)/6.$

The distance between two fuzzy numbers can be defined as follow: $P(G_1) - P(G_2)$. Then the fuzzy important measure can be found:

FIM = 1/ (1 + distance of fuzzy number)

The larger the distance, the higher the importance level of the component for the system is. Detail of this method is explained in the reference [1]. Tyagi, S.K., D. Pandey and R. Tyagi, 2010. Fuzzy set theoretic approach to fault tree analysis. Int. J. Eng. Sci. Technol., 2: 276-283.

Fuzzy ranking method

Detail of this method is explained in the reference [2].

3. RELIABILITY ANALYSIS OF THE CORE FLOODING SYSTEM

3.1. Description of the System

The system is used for the emergency core cooling in case of loss of coolant accident (LOCA). It is gravity-driven cooling. The system uses gravity to drive the coolant through the reactor in the event of a LOCA. This can be achieved by having the coolant storage tanks located above the reactor pressure vessel (RPV) and connected to the reactor by gravity [5].

This is a passive system, which is automatically activated at a pressure drop in the reactor coolant system (RCS) below 3.5 MPa. The system is actuated without initiation signal and electrical power supply. After depletion of own energy the system must be replaced by the low pressure safety injection system (LPSI). The core flooding system is in standby state during normal operation of the nuclear power plant.

The system consists of two independent subsystems, each with two hydraulic accumulators (HA). One subsystem supplies the boric acid solution below the core and second subsystem above the core. The boric acid solution is under the pressure of nitrogen in HA (see Figure 4).

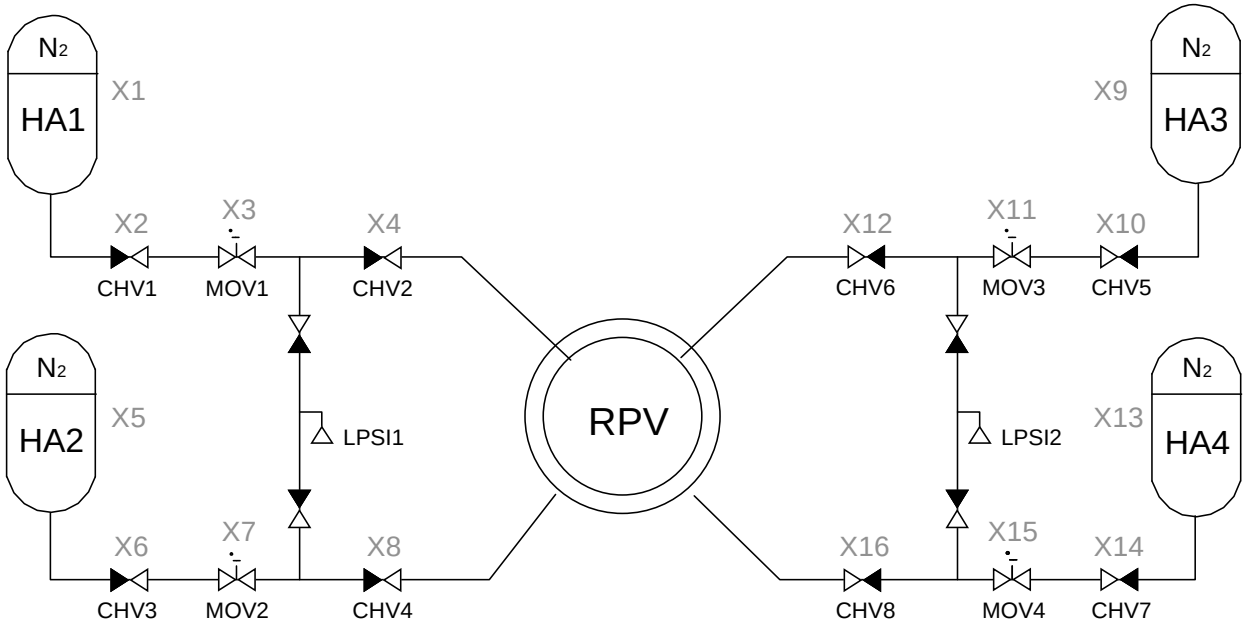

Figure 4. Core flooding system

HAs are connected with reactor pressure vessel by pipings. The pressure difference between RCS and HA is maintained by two check valves. One check valve is located at the reactor vessel to prevent leakage of coolant from RCS in case of piping break between the vessel and HA. The second check valve, is located near to HA. Each check valve has its bypass line with two valves and throttle orifice. The bypass lines are used to check the tightness of the check valves.

The motor operated valve is located between the check valves which prevents the draining of HA during a planned plant outage connected with decreased RCS pressure under initiating pressure of HA (3.5 MPa).

Two safety valves are used to protect HA against excessive pressure increase of nitrogen. The exhaust of the safety valves is led to the containment.

The removal of nitrogen from HAs can be performed through the manual valves and the series of throttle orifices to the air conditioning system. This train is used to drain the HA during maintenance or repairs.

Given pressure drop in RCS below 3.5 MPa in case of accident, boric acid solution is injected into the core by nitrogen expansion. The float valve is closing after depletion of HA, to avoid potential nitrogen infiltration into RCS and at the same time the isolating valve is manually closed.

The availability of each HA is checked once per eight years in operating mode 7 when the reactor is empty. The fuel is located in the spent fuel pool. Based on the water flow from HA to the reactor, the hydraulic resistance of the train is checked.

Into the piping of HA the LPSI subsystems are connected. Function of these subsystems is checked once per three years. So, the test interval of some components of core flooding system is 3 years *(X4, S8, X12 and X16)*.

The pressure of nitrogen and the level of boric acid solution in the HAs are continuously monitored. Concentration of boric acid solution is checked at least once per month and after restoring the availability in case of HA maintenance or its associated systems.

Due to the test interval of 8 years, there is lack of reliability data of some components *(X1, X2, X3, X5, X6, X7, X9, X10, X11, X13, X14 and X15*).

3.3. Method of evaluating the fuzzy probability of basic events

The available limited historical data is used for this purpose. Error factor is the percentage level of error allowed in the failure probability of the component. The system analyst decides the error factor and the value can vary widely depending on the application area and the criticality of the system under study. The value of x_1, x_2 and x_3 are defined as:

$x_1 = q_p/EF$, $x_2 = q_p$ and $x_3 = q_p.EF$

where q_p is the median value of the failure probability and EF is the error factor. The fuzzy probabilities of basic events are presented in Table 2.

Table 2. Fuzzy probabilities of basic events

Notation of basic event	Name of basic event	Fuzzy failure probability		
		$a_i(t)$	$b_i(t)$	$c_i(t)$
X1	HA1	9.57E-07	2.87E-06	8.61E-06
X2	CHV1	8.80E-04	2.64E-03	7.92E-03
X3	MOV1	2.27E-03	6.81E-03	2.04E-02
X4	CHV2	3.31E-04	9.92E-04	2.98E-03
X5	HA2	9.57E-07	2.87E-06	8.61E-06
X6	CHV3	8.80E-04	2.64E-03	7.92E-03
X7	MOV2	2.27E-03	6.81E-03	2.04E-02
X8	CHV4	3.31E-04	9.92E-04	2.98E-03
X9	HA3	9.57E-07	2.87E-06	8.61E-06
X10	CHV5	8.80E-04	2.64E-03	7.92E-03
X11	MOV3	2.27E-03	6.81E-03	2.04E-02
X12	CHV6	3.31E-04	9.92E-04	2.98E-03
X13	HA4	9.57E-07	2.87E-06	8.61E-06
X14	CHV7	8.80E-04	2.64E-03	7.92E-03
X15	MOV4	2.27E-03	6.81E-03	2.04E-02
X16	CHV8	3.31E-04	9.92E-04	2.98E-03
X17	CCF-CHV1357	4.40E-06	1.32E-05	3.96E-05
X18	CCF-CHV2468	1.65E-06	4.95E-06	1.49E-05
X19	CCF-MOV1234	1.14E-05	3.42E-05	1.03E-04

3.4 Fuzzy failure probability of the top event

Fuzzy fault tree is constructed for the system (Figure 5) with the top event of success criterion: at least 1 out of 4 trains is required. The result can be shown as a triangular fuzzy number (0.000017450, 0.000052361, 0.00015798) and the fuzzy probability of the final event in failure probability per year can be shown as follow:

$$\mu_A(x) = \begin{cases} 0 & (x < 0.000017450) \\ (x-a)/(b-a) & (0.000017450 < x < 0.000052361) \\ (c-x)/(c-b) & (0.000052361 < x < 0.00015798) \\ 0 & (x > 0.00015798) \end{cases}$$

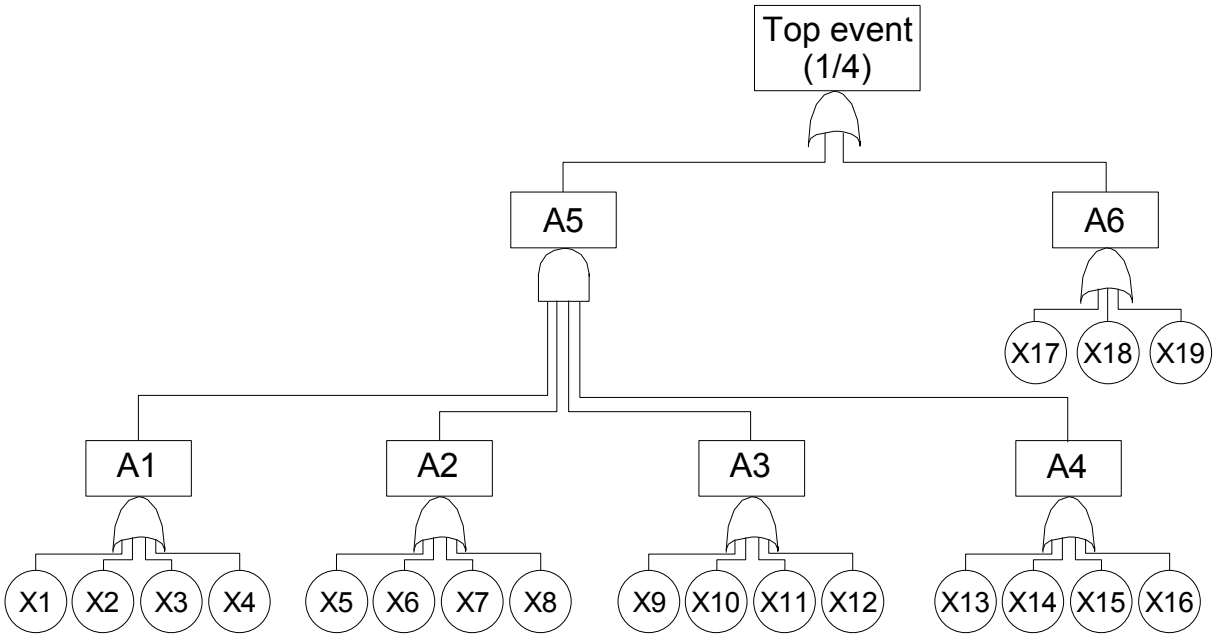

Figure 5. Fuzzy fault tree of the system

3.5. Defuzzification

The result is a triangular fuzzy number $A = \{a_1, b_1, c_1\}$ which is defuzzified as:

X=(0.000017450 + 0.000052361 + 0.00015798)/3 = 0.000075930 = 7.59E-5

The results of conventional PSA for HA system

Name	Mean	5%	Median	95%
@HA(14)-00	5.24E-05	2.03E-05	4.60E-05	1.04E-04

3.6. Fuzzy Importance Measure of Basic Events

Fuzzy distance method and fuzzy ranking method are used to determine the level of importance of each basic event**.** Both methods give the same ranks of fuzzy importance measure for basic events (see Table 3).

Table 3. Fuzzy importance analysis results

Notation of basic event	Fuzzy distance metod	Ranking fuzzy method
X1	0.999958203	2.13812E-05
X5	0.999958203	2.13812E-05
X9	0.999958203	2.13812E-05
X13	0.999958203	2.13812E-05
X4	0.999958218	2.13762E-05
X8	0.999958218	2.13762E-05
X12	0.999958218	2.13762E-05
X16	0.999958218	2.13762E-05
X2	0.999958244	2.13677E-05
X6	0.999958244	2.13677E-05
X10	0.999958244	2.13677E-05
X14	0.999958244	2.13677E-05
X3	0.999958309	2.13458E-05
X7	0.999958309	2.13458E-05
X11	0.999958309	2.13458E-05
X15	0.999958309	2.13458E-05
X18	0.999964252	1.93648E-05
X17	0.999974334	1.60041E-05
X19	1	7.44885E-06

4. CONCLUSION

It can be concluded that the core flooding system has high reliability despite the fact that it is tested only once every 8 years. The fuzzy fault tree analysis gives higher failure probability of the system (7.59E-5) than the conventional fault tree analyses (5.24E-5). However, after implementation of the new failure probability into the PSA model of the plant, there is only negligible changes in the core damage frequency and large early release frequency.

Fuzzy importance measure methods are applied to determine the critically importance of basic events.

By using the fuzzy importance measures the system reliability, availability and planning of future maintenance and inspection works can be improved.

Ranking of the components:

1. CCFs of components have the most importance contribution to the failure probability of the core flooding system,
2. components with test interval of 8 years.
3. components with test interval of 3 years.

References

[1] Tyagi, S.K., D. Pandey and R. Tyagi, Fuzzy set theoretic approach to fault tree analysis. Int. J. Eng. Sci. Technol., 2: 276-283, 2010.

[2] Thorani, Y.L.P., P.P.B. Rao and N.R. Shankar, Ordering generalized trapezoidal fuzzy numbers. Int. J. Contemp. Math. Sci., 7: 555-573, 2012.

[3] Nyan Win Aung et al., Fuzzy fault tree analysis of the marine diesel engine jacket water cooling system, Information Technology Journal 13 (3): 425-433, 2014.

[4] Sohag Kabir et al., A review of applications of fuzzy sets to safety and reliability engineering, School of Engineering and Computer Science, University of Hull, UK, DEIS H2020 project (Grant Agreement 732242), 2018.

[5] Update of level 1 PSA for full power operation of Unit 1 of Mochovce NPP – PSA of internal events, RELKO report, No.1R0218, Bratislava, October 2018.