ELSEVIER

Reliability Engineering and System Safety 75 (2002) 83–91

RELIABILITY ENGINEERING & SYSTEM SAFETY

www.elsevier.com/locate/ress

A dynamic fault tree

Marko Čepin*, Borut Mavko

Reactor Engineering Division, Jožef Stefan Institute, Jamova 39, Ljubljana, Slovenia

Received 17 March 2001; accepted 11 September 2001

Abstract

The fault tree analysis is a widely used method for evaluation of systems reliability and nuclear power plants safety. This paper presents a new method, which represents extension of the classic fault tree with the time requirements. The dynamic fault tree offers a range of risk informed applications. The results show that application of dynamic fault tree may reduce the system unavailability, e.g. by the proper arrangement of outages of safety equipment. The findings suggest that dynamic fault tree is a useful tool to expand and upgrade the existing models and knowledge obtained from probabilistic safety assessment with additional and time dependent information to further reduce the plant risk. © 2002 Elsevier Science Ltd. All rights reserved.

Keywords: Fault tree; Safety; Reliability; Probabilistic safety assessment; Risk

1. Introduction

The fault tree analysis is a widely used method for evaluation of reliability and safety [1,2]. It is applied in various sectors from chemical and railway industry for the improvement of vehicle design and software reliability. Its repute is gained primarily when integrated with the event tree analysis as a part of the probabilistic safety assessment (PSA) [1,3,4].

The classic fault tree is a static tool with its primary objective to direct the safety improvements in the context of the PSA. In this context, the fault tree has not been used to model the time requirements in the safety systems, e.g. equipment outages in real-time, e.g. change of plant states, although its idea was extended in a number of ways [5,6], e.g.:

- to perform a phased mission analysis by Burdick et al. [2] and by Dugan [7],
- to improve the software reliability by improving the late phases of the software life cycle by Leveson et al. [8] and Dugan and Lyu [9],
- to analyse the requirements specification as an early phase of the safety software life cycle by Čepin and Wardzinski [10] and Čepin and Mavko [11],
- to asses the dependability of the embedded software systems with the dynamic flowgraph methodology by Garret et al. [12] and Muthukumar et al. [13],
- to evaluate the dynamic scenarios with the event sequence diagram by Swaminathan and Smidts [14],
- to support the functional modelling of the engineering systems by Modarres and Cheon [15] and Hu and Modarres [16],
- to investigate the flow of physical signals with the GO-FLOW by Matsuoka and Kobayashi [17], which can be viewed as an upgraded success oriented complement of the fault tree.

The fault tree for its primary objective is still used as it was years ago, in spite of the fact that the risk informed methods and their applications have been widely expanded in the previous years [18,19].

The first purpose of this paper is to develop a dynamic fault tree, which extends the classic fault tree with the time requirements. The dynamic fault tree may serve as a standpoint for evaluation of the actual time dependent profile of the nuclear power plant risk. The prerequisite for the extension of the classic fault tree is the recent significant increase in capacity of modern computers, which enables fault tree evaluations to be performed in the consecutive discrete time points. The second purpose of this paper is to show an application of the dynamic fault tree, which when standalone or integrated with the event trees [20] may improve safety of the nuclear power plants [21–25].

The paper is organised as follows: Section 2 presents the mathematical model of the classic and the dynamic fault tree. Section 3 shows the application of the dynamic fault tree, which contribute to the improved nuclear power plant safety with focus on the improvement of the test and

* Corresponding author.
E-mail address: marko.cepin@ijs.si (M. Čepin).

0951-8320/02/$ - see front matter © 2002 Elsevier Science Ltd. All rights reserved.
PII: S0951-8320(01)00121-1

Nomenclature

λ_j	failure rate of the equipment modelled in the basic event j
B_j	basic event j
GD	top event
GD(t)	top event at time t
G_i	gate i
H_S	house event s
H_{st}	house event value (true or false) for the house event H_s at the time t
J	number of basic events in the fault tree
m	number of basic events in minimal cut set i
MCS_i	minimal cut set i
$\mathrm{MCS}_i\,(H_{1t}, H_{2t},\ldots,H_{st},\ldots,H_{St})$	minimal cut set i at time t
MH_{ST}	house events matrix
n	number of minimal cut sets
P	number of gates in the fault tree
$Q_{Bj}(t)$	probability of occurrence of basic event B_j at time t
$Q_{\mathrm{GD}}(t)$	top event probability at time t
$Q_{\mathrm{MCS}i}(t)$	probability of occurrence of MCS_i
q_j	probability of failure of equipment modelled in basic event j
S	number of house events
t	time
T	number of time points
T_{ij}	test interval of equipment modelled in basic event j
T_j	considered time interval
T_{pj}	outage placement time for equipment modelled in basic event j
T_{rj}	time to restore (mean time to repair) for equipment modelled in basic event j
T_{tj}	outage duration of equipment modelled in basic event j

maintenance activities. Section 4 encompasses the most important findings and suggestions.

2. Method

The notation of the classic fault tree is well known [1,2], but it is summarised in Section 2.1 as a standpoint for comparison with the notation of the dynamic fault tree, which is summarised in Section 2.2.

2.1. Classic fault tree

The fault tree is a tool to identify and assess all combinations of the undesired events in the context of the system operation and its environment that can lead to the undesired state of the system [1]. The undesired state of the system is represented by a top event. The logical gates integrate the primary events to the top event. The primary events are the events, which are not further developed, e.g. the basic events and the house events [1]. The basic events are the ultimate parts of the fault tree, which represent the undesired events, e.g. the component failures, the missed actuation signals, the human errors, the unavailability due to the test and maintenance activities, the common cause contributions. The house events represent the conditions set either to true or false, which support the modelling of connections between the gates and the basic events and enable that the fault tree better represents the system operation and its environment.

The classic fault tree is mathematically represented by a set of boolean equations:

$$G_i = f(G_p, B_j, H_S);\ \ i,p \in \{1\ldots P\},\ j \in \{1\ldots J\}, s \in \{1\ldots S\} \tag{1}$$

The qualitative analysis (in the process of Boolean reduction of a set of equations) identifies the minimal cut sets, which are combinations of the smallest number of basic events, which if occur simultaneously, may lead to the top event:

$$\mathrm{GD} = \bigcup_{i=1}^{n} \mathrm{MCS}_i \tag{2}$$

$$\mathrm{MCS}_i = \bigcap_{j=1}^{m} B_j \tag{3}$$

The quantitative analysis represents a calculation of the top event probability, which differs a bit from slightly inaccurate notation in Refs. [1,26]:

$$Q\mathrm{GD} = \sum_{i=1}^{n} Q_{\mathrm{MCS}i} - \sum_{i<j} Q_{\mathrm{MCS}i\cap\mathrm{MCS}j} + \sum_{i<j<k} Q_{\mathrm{MCS}i\cap\mathrm{MCS}j\cap\mathrm{MCS}k} - \cdots + (-1)^{n-1} Q \bigcap_{i=1}^{n} \mathrm{MCS}i \tag{4}$$

where

$$Q_{\mathrm{MCS}i} = Q_{B1}Q_{B2} | Q_{B1}Q_{B3} | Q_{B1} \cap Q_{B2} \ldots Q_{Bm} | Q_{B1} \cap Q_{B2} \cap \ldots \cap Q_{Bm-1} \tag{5}$$

or where under assumption that the basic events are mutually independent:

$$Q_{\mathrm{MCS}_i} = \prod_{j=1}^{m} Q_{B_j} \tag{6}$$

where

$$Q_{B_j} = Q_{B_j}(T_j, \lambda_j, q_j) \tag{7}$$

Table 1
Variations of the system configuration of AFS fault tree defined with the house events (T — house event is set to true. F — house event is set to false)

House event Id.	AF1	AF1C	AF2	AF3	AF4	AF5	AF5C	AF6	AF7	AF8	AF9	AF10	AFA	AFAC	AFC1	AFC2	AFT
AFS-CCF-AMC-V	T	T	T	F	F	F	F	T	F	F	T	F	T	T	F	T	F
AFS-SG12	T	T	T	T	T	F	F	T	F	T	T	T	T	T	T	T	T
AFS-SG1	F	F	F	F	F	F	F	F	T	F	F	F	F	F	F	F	F
AFS-SG2	F	F	F	F	F	T	T	F	F	F	F	F	F	F	F	F	F
AFS-HEP-700	T	F	T	F	T	T	F	F	F	F	T	T	T	F	F	F	F
AFS-HEP-701	F	T	F	F	F	F	T	F	F	F	F	F	F	F	F	F	F
AFS-HEP-702	F	F	F	T	F	F	F	T	F	T	F	F	F	F	F	F	F
AFS-HEP-703	F	F	F	F	F	F	F	F	T	F	F	F	F	T	F	F	F
AFS-HEP-704	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	T
AFS-SG1-P-M	F	F	F	F	T	F	F	F	F	F	F	F	F	F	F	F	F
AFS-SG1-P-T	F	F	F	T	F	F	F	F	F	T	F	F	F	F	F	F	T
AFS-SG1-P-MT	T	T	T	F	F	F	F	T	T	F	T	T	T	T	T	T	F
AFS-P1-CONTAD	T	T	T	F	T	F	F	T	T	F	T	F	F	F	F	F	F
AFS-P1-CONTD	F	F	F	F	F	F	F	F	F	F	F	F	T	T	T	T	F
AFS-CV-11048	T	T	T	T	T	T	T	T	T	T	T	T	T	T	F	F	T
AFS-TP-ESFAAB	T	T	T	T	F	F	F	F	F	T	T	F	F	F	F	F	F
AFS-TP-ESFAB	F	F	F	F	F	F	F	F	F	F	F	T	F	F	F	F	F
AFS-SEGM-VTU	T	T	T	T	T	T	T	T	T	F	T	T	T	T	F	T	F
AFS-SEGM-VU	F	F	F	F	F	F	F	F	F	F	F	F	F	F	T	F	F
AFS-SEGM-U	F	F	F	F	F	F	F	F	F	T	F	F	F	F	F	F	T
AFS-SG2-P-M	F	F	F	F	T	F	F	F	F	F	F	F	F	F	F	F	F
AFS-SG2-P-T	F	F	F	T	F	F	F	F	F	T	F	F	F	F	T	F	T
AFS-SG2-P-MT	T	T	T	F	F	T	T	T	F	F	T	T	T	T	F	T	F
AFS-P2-CONT	T	T	T	F	T	T	T	T	F	F	T	T	F	F	F	F	F

If the minimal cut sets are not assumed as mutually independent, the second and the next items in Eq. (4) are written as follows:

$$Q_{\mathrm{MCS}_i \cap \mathrm{MCS}_j} = Q_{\mathrm{MCS}_i} Q_{\mathrm{MCS}_j|\mathrm{MCS}_i} \tag{8}$$

$$Q_{\mathrm{MCS}_i \cap \mathrm{MCS}_j \cap \ldots \cap \mathrm{MCS}_n} = Q_{\mathrm{MCS}_i} Q_{\mathrm{MCS}_j|\mathrm{MCS}_i} \cdots Q_{\mathrm{MCS}_n|\mathrm{MCS}_i \cap \mathrm{MCS}_j \cap \ldots \cap \mathrm{MCS}_{n-1}} \tag{9}$$

If the minimal cut sets are assumed as mutually independent, the second and the next items in Eq. (4) are written as:

$$Q_{\mathrm{MCS}_i \cap \mathrm{MCS}_j} = Q_{\mathrm{MCS}_i} Q_{\mathrm{MCS}_j} \tag{10}$$

$$Q_{\mathrm{MCS}_i \cap \mathrm{MCS}_j \cap \ldots \cap \mathrm{MCS}_n} = Q_{\mathrm{MCS}_i} Q_{\mathrm{MCS}_j} \cdots Q_{\mathrm{MCS}_n} \tag{11}$$

In either case, Eq. (4) can be simplified and approximated with its first item:

$$Q_{\mathrm{GD}} = \sum_{i=1}^{n} Q_{\mathrm{MCS}_i} \tag{12}$$

For Q_{MCS_i} less than 0.1, the approximate results stay in 10% of accuracy in the conservative side. The approximate results show slightly higher failure probabilities than the exact value [1].

Such classic fault tree is a standardised tool for evaluation and improvement of systems reliability and nuclear power plants safety [1,3].

2.1.1. House events table

In the classic PSA it is possible that for a single safety system several fault trees are needed. They may differ because of different success criteria or/and different boundary conditions, as they are linked to different scenarios with different requirements (i.e. several different functional events for the same safety system may appear in the event trees) [27]. This may result in a situation that a single system or subsystem is modelled with more than one or even with many fault trees. Each of them is used in its appropriate scenario branch (i.e. event tree portion). It is possible to integrate all such fault trees including their respective success criteria under one integrated fault tree, or an umbrella fault tree [28]. In this case, the house events are used to switch on and off respective parts of the integrated fault tree. Each defined combination of the house events values (value of the respective house events is set either to true or to false) suits both: its respective function event and the success criteria of its respective fault tree.

The house events table is introduced to document, which house events are switched on and which off for certain fault tree top event to suit its respective function event in its appropriate scenario branch. The house events table represents the model of all combinations of the success criteria for a certain system in a single fault tree by definition of the house events values for each function event and the success criteria for its respective fault tree.

The house events table identifies all house events in the model of the system in its left column of the table. For each house event in this table it is determined if its value is set to

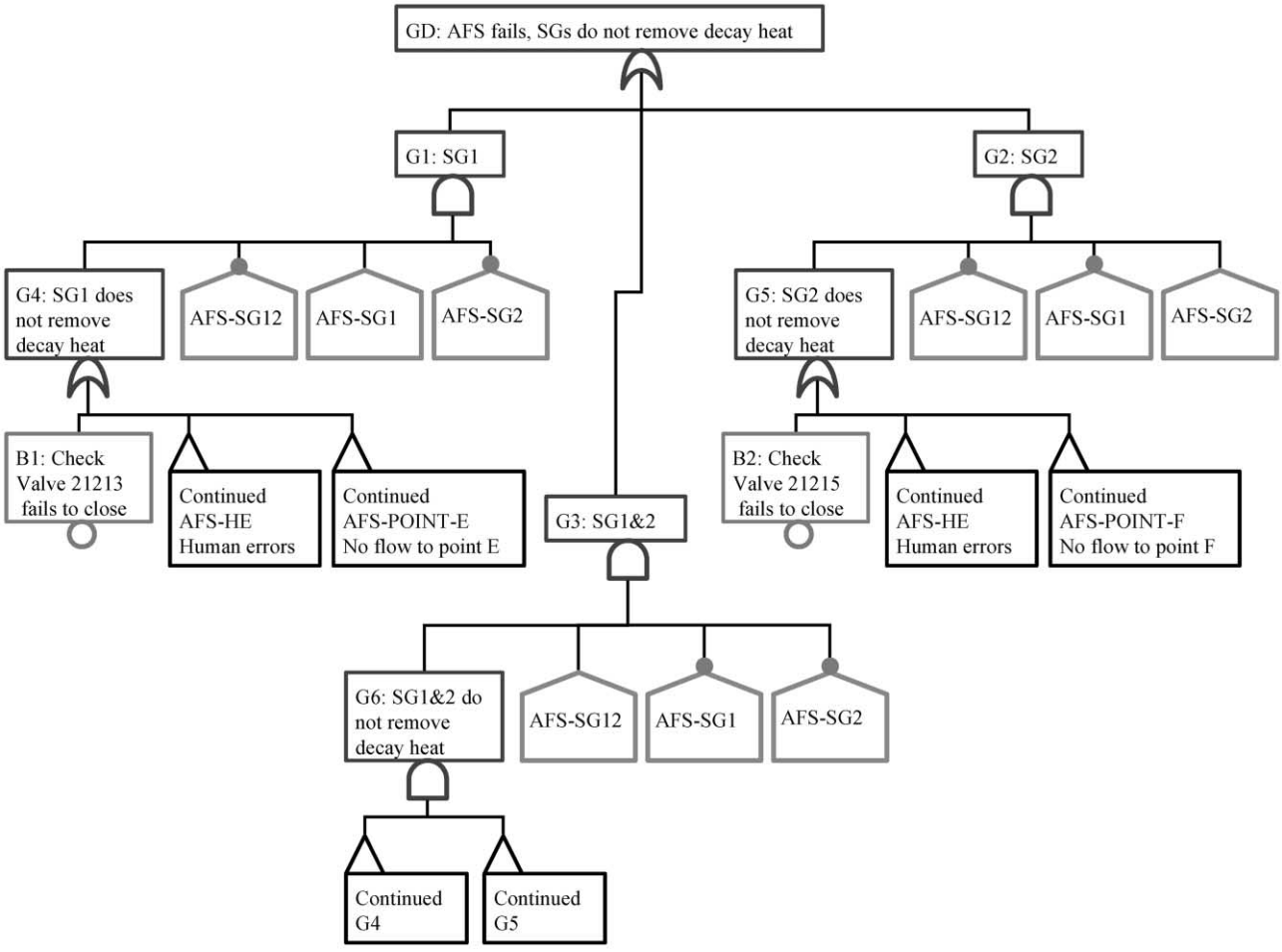

Fig. 1. An example of the integrated fault tree for the auxiliary feedwater system.

true (marked with T) or to false (marked with F) for each of the system configurations. The names of configurations, which suit the respective fault trees, are identified in the upper row of the table. The identified system configurations appear as functional events in the event trees for evaluation of the core damage frequency (level 1 of the PSA).

Table 1 shows an example of the house events table for the auxiliary feedwater system (AFS). Twenty-four house events are identified in 24 rows in the first column. The next 17 columns represent 17 configurations of AFS, which differ by the success criteria or the boundary conditions. For each of AFS configurations (e.g. AF1), the appropriate house events are set to false (marked with F) and others are set to true (marked with T), that the fault tree suits its configuration.

For example, for the configuration AFC1, the following five house events have to be set to true: AFS-SG12, AFS-SG1-P-MT, AFS-P1-CONTD, AFS-SEGM-VU, AFS-SG2-P-T.

Fig. 1 shows the example of the upper part of the integrated fault tree for the AFS. The configuration AF1 is considering both steam generator (SG) lines (success criteria: AFS fails if one of three AFS pumps fails to feed one out of two SG lines). House events in the figure are set to the following values: AFS-SG12 = T, AFS-SG1 = F, AFS-SG2 = F, as it is defined in Table 1. The configuration AF5 is considering only second SG line (success criteria: AFS fails if motor or turbine driven pump fails to feed the intact SG — second one is assumed as the intact SG). The house events in the figure are set to the following values in this case: AFS-SG12 = F, AFS-SG1 = F, AFS-SG2 = T, as it is defined in Table 1.

The combinations of house events modelled under certain gates intentionally include negations of certain house events (negations are represented by small circle above the house event). Such modelling reduces the possibility of determination the faulty combination of house events values for certain fault tree configuration, because only couple of right combinations of house events values give reasonable results in the list of minimal cut sets. The wrong combination of house events values would result in unreasonable results, e.g. an empty set of minimal cut sets.

The list of minimal cut sets for the example of the AFS fault tree shown in Fig. 1 would be an empty set for five out of eight combinations of values of three house events included in Fig. 1 (AFS-SG12, AFS-SG1, AFS-SG2).

Only in three right combinations of the respective house events values (T,F,F; F,T,F; F,F,T) the resulted qualitative analysis would give the reasonable set of minimal cut sets.

Such house events table documents all configurations of the certain system fault tree. The documented configurations are later used in the linking of the event and fault trees.

2.2. Dynamic fault tree

The dynamic fault tree is a fault tree, which is extended with the time requirements using the house events matrix and the time dependent probabilistic models for the basic events. It represents an extension of the classic fault tree with time. It is written by a set of equations of type:

$$G_i(t) = f(G_p, B_j, H_{st}); \quad i,p \in \{1...P\},\ j \in \{1...J\},\ s \in \{1...S\}\ t \in \{1...T\} \tag{13}$$

The input of status of house events is achieved through the house events matrix:

$$\|\mathrm{MH}_{ST}\| = \begin{Vmatrix} H11 & H_{12} & \cdots & & H_{1T} \\ H_{21} & \cdots & & & \cdots \\ \cdots & & H_{st} & \cdots & \cdots \\ H_{S1} & \cdots & & & H_{ST} \end{Vmatrix} \tag{14}$$

The house events matrix is a representation of house events switched on and off through the discrete points of time. It includes the house events, which timely switch on and off parts of the fault tree in accordance with the status of the modelled system.

The number of rows in the house events matrix represents a number of those house events in the model, which are modelling the behaviour of the certain system configuration as a function of time. The house events, which are constant with time for certain system configuration, may be excluded from the house events matrix.

The number of columns represents the number of time periods in which mutually different system configurations exist.

The qualitative analysis finds the minimal cut sets, which are not necessary the same in each time point t:

$$\mathrm{GD}(t) = \bigcup_{i=1}^{n} \mathrm{MCS}_i\,(H_{1t}, H_{2t}, \ldots, H_{st}, \ldots, H_{St}) \tag{15}$$

where

$$\mathrm{MCS}_i(H_{1t}, H_{2t}, \ldots, H_{St}, \ldots, H_{St}) = \bigcap_{j=1}^{m} B_j \tag{16}$$

The quantitative analysis includes calculation of the top event probability:

$$Q_{\mathrm{GD}}(t) = \sum_{i=1}^{n} Q_{\mathrm{MCS}_i(H_{1t},\ldots H_{st},\ldots H_{St})} - \sum_{i<j} Q_{\mathrm{MCS}_i(H_{1t},\ldots H_{st},\ldots H_{St})\cap\mathrm{MCS}_j(H_{1t},\ldots H_{st},\ldots,H_{St})} + \sum_{i<j<k} Q_{\mathrm{MCS}_i(H_{1t},\ldots,H_{st},\ldots H_{St})\cap\mathrm{MCS}_j(H_{1t},\ldots H_{st},\ldots H_{St})\cap\mathrm{MCS}_k(H_{1t},\ldots H_{st},\ldots H_{St})} - \ldots + (-1)^{n-1} Q \bigcap_{i=1}^{n} \mathrm{MCS}_i(H_{1t}, \ldots H_{st}, \ldots H_{St}) \tag{17}$$

which may be approximated (see Section 2.1):

$$Q_{\mathrm{GD}}(t) = \sum_{i=1}^{n} Q_{\mathrm{MCS}_i}(H_{1t}, H_{2t}, \ldots H_{st}, \ldots, H_{St}) \tag{18}$$

where

$$Q_{\mathrm{MCS}i}(H_{1t}, H_{2t}, \ldots, H_{st}, \ldots, H_{St}) = Q_{B1}(t)Q_{B2}(t)|Q_{B1}(t)Q_{B3}(t)|Q_{B1}(t) \cap Q_{B2}(t)\ldots Q_{Bm}(t)|Q_{B1}(t) \cap Q_{B2}(t) \cap \ldots \cap Q_{Bm-1}(t) \tag{19}$$

or where under assumption that the basic events are mutually independent:

$$Q_{\mathrm{MCS}_i}(H_{1t}, H_{2t}, \ldots, H_{st}, \ldots, H_{St}) = \prod_{j=1}^{m} Q_{B_j}(t) \tag{20}$$

where the time dependent failure probabilities of basic events are calculated as a function of several parameters:

$$Q_{B_j}(t) = Q_{B_j}(\lambda_j, q_j, T_{ij}, T_{tj}, T_{rj}, T_{pj,\ldots t}) \tag{21}$$

An example equation for calculation of the time dependent failure probabilities of basic events was developed in Ref. [3].

Fig. 2 shows, that two separate uses of house events matrix are distinguished: case A on the left side of the figure serves for modelling of outage of equipment and case B on the right side of the figure serves for modelling of more operational modes of the equipment.

Case A: the house event under OR gate serves for modelling of an outage of equipment modelled in gate or basic event under mentioned OR gate. With the house event 1 (H1) set to 0 (false) the gate 1 (G1) depends on the basic event 1 (B1). With the house event 1 (H1) set to 1 (true) the gate 1 (G1) is 1 (true) independently of basic event 1 (B1). With the house event 1 (H1) set to 1 (true) the outage of equipment modelled in the basic event 1 (B1) is simulated. The time diagram explains the house events matrix, which for time points T2 and T3 simulate the outage of equipment modelled in basic event 1 (B1).

Case B: the house event under AND gate serves for modelling of more operational modes of the equipment modelled in the gate or basic event under mentioned AND

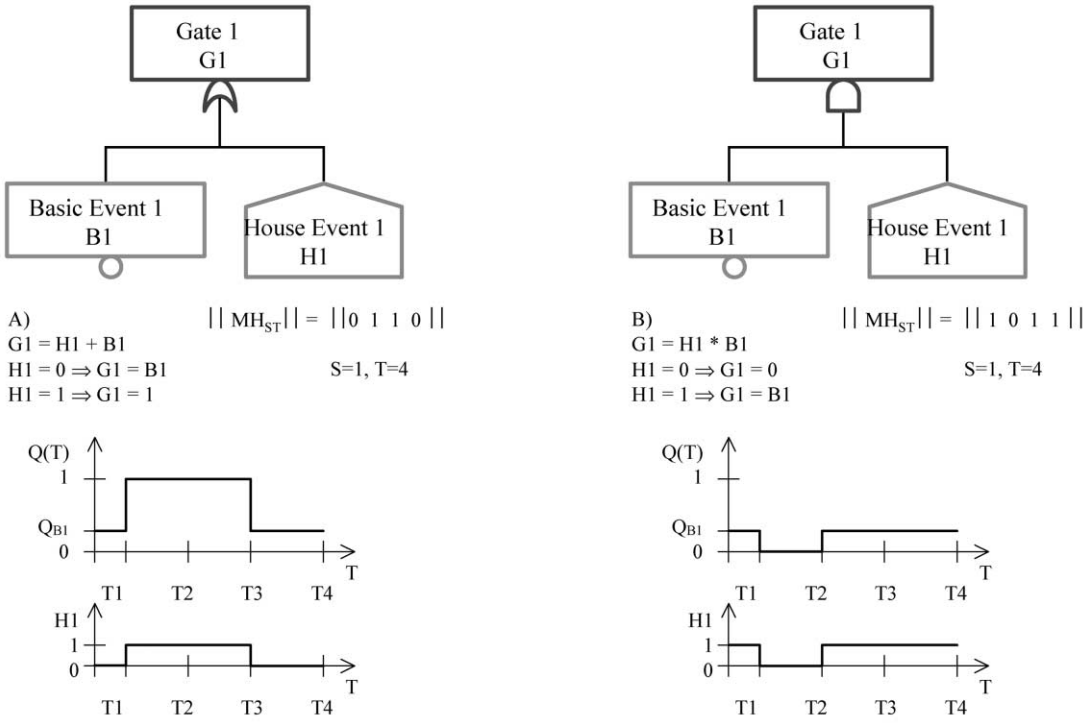

Fig. 2. Examples of the house events matrix.

gate or for modelling of more success criteria of the equipment modelled in the gate or basic event under mentioned AND gate. With the house event 1 (H1) set to 0 (false) the gate 1 (G1) is 0 (false). With the house event 1 (H1) set to 1 (true) the gate 1 (G1) depends on the basic event 1 (B1). With the house event 1 (H1) set to 0 (false) the second operational mode of system modelled in gate 1 (G1) is modelled, where the equipment modelled in the basic event 1 (B1) is not considered in the model. The time diagram explains the house events matrix, which for time point T2 simulate second operational mode of the system modelled in gate 1 (G1). In time point T2 the equipment modelled in the basic event 1 (B1) is not considered in the model. The first operational mode of the system modelled in gate 1 (G1) at the time points: T1, T3 and T4, requires that the equipment modelled in the basic event 1 (B1) is considered in the model and can contribute to the gate 1 (G1).

The dynamic fault tree enables modelling of time requirements in two ways:

by introduction of the time dependent models for probabilities of component failures (representing basic events unavailability),
by introduction of the house events matrix, which defines timely switching on and off the portions of the fault tree (representing the portions of the system).

Consideration of only one out of two mentioned ways for modelling of certain phenomena is important to avoid double counting. For example if the test and maintenance contributions are considered in the probabilistic models for components it is not correct to model their contributions once again within the house events matrix.

As the classic fault tree represents an integral part of PSA, where linking of fault trees with event trees lead to the overall results, also dynamic fault trees are at the plant level linked with the event trees.

The main advantage of the dynamic fault tree compared to e.g. Petri nets [29,30] or Markov Chains [6,31] is in that it is more understandable to the current users of the PSA. No additional knowledge of other methods is needed, only the use of the fault tree is extended. In theory, each of the time points in the time scale of the dynamic fault tree analysis can be also obtained by a classic fault tree analysis with appropriate conditions.

The dynamic fault tree can handle small or large models as the classic fault tree analysis does. Furthermore, no new models are needed for the application of the dynamic fault tree. The existing fault tree models can be used and be updated with the additional house events, which enable to distinguish configurations in their respective time points.

3. Application of the dynamic fault tree

The application of the dynamic fault tree includes: the configuration control and integration of several modes of equipment operation. In this sense the application of the dynamic fault tree contributes to the improvement of test

Table 2
Probabilistic data (example of 10 components)

	Each column suits its respective component data									
T_t	5	10	5	10	5	20	5	10	10	5
T_r	20	20	20	20	20	20	20	20	20	20
T_i	600	200	300	250	500	600	600	600	600	600
λ	0.0001	0.0002	0.0003	0.0004	0.0001	0.0001	0.0001	0.0001	0.0001	0.0001
Q	0.001	0.001	0.001	0.001	0.002	0.003	0.004	0.001	0.001	0.001

and maintenance activities of the safety equipment in a nuclear power plant.

The configuration control is a management of the component arrangements (component status: available versus unavailable) to control the risk of an entity under investigation.

The idea of the configuration control is to calculate the mean value of the selected risk measure over the considered time interval and among the variable parameters find their optimal values (which in turn result in minimal mean value of the selected risk measure). The variable parameters are primarily those parameters, which may vary to result in minimisation of risk, e.g. the outage placement times.

The dynamic fault tree is used for modelling and evaluation of an entity under investigation, because the classic fault tree is not able to monitor its top event probability as a function of time to follow the changes of the system configuration. For each of the selected discrete time points in the selected time interval an appropriate equipment configuration is determined and it is noted in appropriate column in the house events matrix (Section 2.2). The system unavailability, which serves as a risk measure at the system level, is calculated for all selected time points. The mean system unavailability over selected time interval is calculated from the time dependent unavailabilities. The optimal arrangement of components outages is determined on base of minimisation of the mean system unavailability (obtained from minimal cut sets, which contain basic events, which model equipment outages) as a function of arrangement of equipment configuration:

$$\frac{1}{N}\sum_{T=0}^{T=N-1} Q_{\mathrm{GD}}(t, T_{\mathrm{p}_j}) = \min \Rightarrow \text{optimum } T_{\mathrm{p}_j};\ j \in \{1 \ldots J\} \quad (22)$$

Timing of outages is identified with the outage placement times ($T_{\mathrm{p}j}$). $T_{\mathrm{p}j}$ is the time passed from starting time of evaluation (time 0) to the point in time in which the equipment outage has ended. It is assumed that for periodically tested components the test is performed in each period at time $T_{\mathrm{p}j}$ after start of the period.

The dynamic fault trees with links to the event trees are used for modelling and evaluation of entity under investigation at the plant level. The core damage frequency serves as a risk measure [27].

The most important prerequisite for successful application of the dynamic fault tree is the use of appropriate probabilistic models for basic events, which should suit as much as possible the nature of entities modelled in those basic events (e.g. note at the end of Section 2.2) and the specific data [32].

A small example of a system consisting of 10 components in series was evaluated. Table 2 shows the probabilistic data for the components according to the probabilistic model from Ref. [3]. It is assumed that test and maintenance of a component result in as-good-as-new state.

The time dependent system unavailability $Q(t)$ was calculated as a function of components unavailability, which are functions of outage placement time. The calculations were done for a large number of sets of respective outage placement times. The resulted unavailability were compared and the minimal mean unavailability $Q = 0.378$ and associated set of outage placement times $T_{\mathrm{p}j}$ ($j \in \{1 \ldots 10\}$; 573, 189, 244, 234, 367, 460, 555, 478, 517, 522) was identified. Fig. 3 shows the time dependent system unavailability versus time in identified arrangement.

Results show that it is possible to reduce system unavailabilities with appropriate time placement of test and maintenance activities.

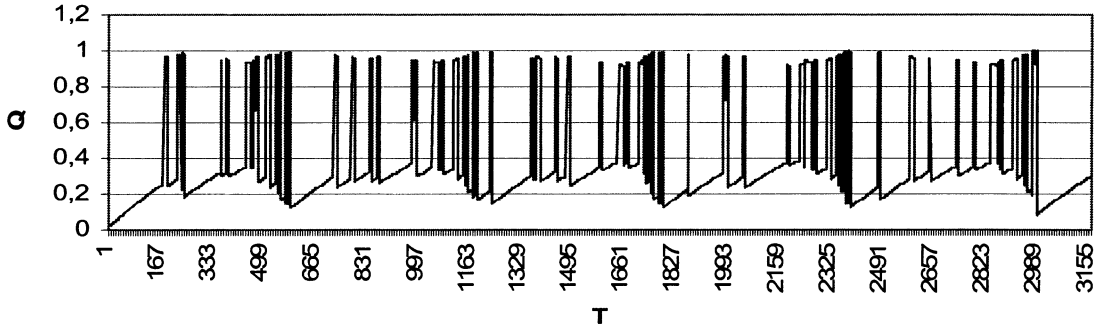

Fig. 3. System unavailability versus time in the optimal arrangement of component outages (example of 10 components).

For larger cases and real examples it is necessary to develop a suitable optimisation method, which is capable to deal with non-linear problems and with extreme large number of combinations. An optimisation method based on the simulated annealing algorithm was developed, which determines the optimal schedule of safety equipment outages. It is documented in Ref. [33] and it shows promising results.

4. Conclusions

The fault tree as it is currently used in the PSA mostly does not model the time requirements in safety systems. It is not able to monitor its top event probability as a function of time to follow the changes of the system configuration. A dynamic fault tree was developed in sense to increase the applicability of the classic fault tree and to enable evaluation of the actual time dependent risk profile.

The dynamic fault tree is a fault tree, which is extended with the time requirements using the house events matrix and the time dependent probabilistic models for basic events. The house events matrix is a matrix, which represents the house events switched on and off through the discrete points of time. It includes house events values (true or false) for all house events in their respective fault tree and for all considered discrete time points. House events values for certain house event in certain time point correspond to the status of the modelled system, in which parts of the fault tree may be switched on and off in accordance with its status. The most important prerequisite for successful application of the dynamic fault tree is the use of appropriate probabilistic models for basic events, which should suit as much as possible the nature of entities modelled in those basic events.

Applications of the dynamic fault tree include evaluation of the time dependent risk profile and optimisation of parameters in probabilistic models to minimise the overall risk, such as configuration control.

The results show that there may exist more or even many equipment arrangements with same or similarly low system unavailability. The most important result of the method is not a selection of the most suitable equipment arrangement among those which results in similarly low unavailability, but it is to prevent such equipment arrangements which result in high unavailabilities.

The results confirm that the dynamic fault tree is a useful tool to expand and upgrade the existing models and knowledge obtained from PSA, with additional, time dependent information to further reduce the nuclear power plant risk.

Acknowledgements

This research was supported by Ministry of Education, Science and Sport, Republic of Slovenia.

References

[1] Roberts NH, Vesely WE, Haasl DF, Goldberg FF. Fault tree handbook, NUREG-0492. Washington: US NRC, 198.
[2] Burdick GR, Fussel JB, Rasmuson DM, Wilson JR. Phased mission analysis: a review of new developments and an application. IEEE Trans Reliab 1977;R-26(1):43–9.
[3] Čepin M, Mavko B. Probabilistic safety assessment improves surveillance requirements in technical specifications. Reliab Engng Syst Saf 1997;56:69–77.
[4] Kumamoto H, Henley EJ. Probabilistic risk assessment and management for engineers and scientists, vol. 208. New York: IEEE Press, 1996.
[5] Ren Y, Dugan JB. Optimal design of reliable systems using static and dynamic fault trees. IEEE Trans Reliab 1998:234–44.
[6] Siu N. Risk assessment for dynamic systems: an overview. Reliab Engng Syst Saf 1994;43:43–73.
[7] Dugan JB. Automated analysis of phased-mission reliability. IEEE Trans Reliab 1991;40(1):45–52.
[8] Leveson NG, Cha SC, Shimeall TJ. Safety verification of ADA programs using software fault trees. IEEE Trans Soft Engng 1991:48–59.
[9] Dugan JB, Lyu MR. System reliability analysis of an N-version programming application. IEEE Trans Reliab 1994;43(4):513–9.
[10] Wardzinski A, Čepin M. Fault tree analysis. Informatyka 1997;6:28–32 (in Polish).
[11] Čepin M, Mavko B. Fault tree developed by an object-based method improves requirements specification for safety-related systems. Reliab Engng Syst Saf 1999;63:111–25.
[12] Garrett J, Guarro SB, Apostolakis GE. The dynamic flowgraph methodology for assessing the dependability of embedded software systems. IEEE Trans Syst, Man Cybernetics 1995;25(5):824–40.
[13] Muthukumar CT, Guarro SB, Apostolakis G. In: Aldemir T, Siu NS, Mosleh A, Cacciabue PC, Goktepe BG, editors. Dependability of embedded software systems, Reliability and safety assessment of dynamic process systems, vol. 120. Heidelberg: Springer, 1994. p. 59–77, NATO ASI Series F.
[14] Swaminathan S, Smidts C. The mathematical formulation for the event sequence diagram framework. Reliab Engng Syst Saf 1999;65:103–18.
[15] Modarres M, Cheon SW. Function-centered modeling of engineering systems using the goal-success tree technique and functional primitives. Reliab Engng Syst Saf 1999;64:181–200.
[16] Hu YS, Modarres M. Evaluating system behavior through dynamic master logic diagram modeling. Reliab Engng Syst Saf 1999;64:241–69.
[17] Matsuoka T, Kobayashi M. GO-FLOW: a new reliability analysis methodology. Nucl Sci Engng 1988;98:64–78.
[18] Samanta P, Kim IS, Mankamo T, Vesely WE. Handbook of methods for risk-based analyses of technical specifications, NUREG/CR-6141. Washington DC: US NRC, 1995.
[19] Caruso MA, Cheok MC, Cunningham MA, Holahan GM, King TL, Parry GW, Ramey-Smith AM, Rubin MP, Thadani AC. An approach for using risk assessment in risk-informed decisions on plant-specific changes to the licensing basis. Reliab Engng Syst Saf 1999;63:231–42.
[20] Papazoglou IA. Mathematical foundations of event trees. Reliab Engng Syst Saf 1998;61:169–83.
[21] Harunuzzaman M, Aldemir T. Optimization of standby safety system maintenance schedules in nuclear power plants. Nucl Technol 1996;113:354–67.
[22] Vaurio JK. Optimization of test and maintenance intervals based on risk and cost. Reliab Engng Syst Saf 1995;49:23–36.
[23] Martorell S, Carlos S, Sanchez A, Serradell V. Constrained optimization of test intervals using a steady-state genetic algorithm. Reliab Engng Syst Saf 2000;67:215–32.

[24] Yang JE, Sung TY, Yin Y. Optimization of the surveillance test interval of the safety systems at the plant level. Nucl Technol 2000;132:352–65.
25. Čepin M, Gomez Cobo A, Martorell S, Samanta P. Methods for testing and maintenance of safety related equipment: examples from an IAEA research project. Proc ESREL99: Saf Reliab 1999;1:247–51.
[26] Villemeur A. Availability, maintainability and safety assessment, Methods and techniques, vols. 1,2. West Sussex: Wiley, 1992.
[27] Čepin M. Estimation of event frequencies on the various system and plant levels. EUROCOURSE, PSARID, Garching 2001.
[28] Vrbanić I, Kaštelan M. Optimization of NPP Krško PSA model structure by the employment of house events. Proc Nucl Energy Central Europe 1997:414–21.
[29] Leveson NG, Stolzy JL. Safety analysis using petri nets. IEEE Trans Soft Engng 1987;13(3):386–97.
[30] Gorski J, Magott J, Wardzinski A. Modeling fault trees using petri nets. Proc SAFECOMP95, Villa Charlotta, Italy 1995.
[31] IAEA-TECDOC-669, Case study on the use of PSA methods: assessment of technical specifications for the reactor protection system instrumentation. IAEA: Vienna, 1992.
[32] Jordan Cizelj R, Mavko B, Kljenak I. Component reliability assessment using quantitative and qualitative data. Reliab Engng Syst Saf 2001;71:81–95.
[33] Čepin M. Optimization of safety equipment outages improves safety. Reliab Engng Syst Saf 2002, submitted for publication.