Babczyński Tomasz
Kowalski Marcin
Łukowicz Mirosław
Magott Jan
Skrobanek Paweł
Wroclaw University of Technology, Wroclaw, Poland

Safety and reliability models of time-dependent systems

Keywords

dynamic reliability, maintenance process, fault tree with time dependencies, activity diagram

Abstract

The paper concerns models with time dependencies that can be used in modelling dynamic reliability and complex maintenance processes. Emphasis is put on models that have been elaborated with authors participation. The following models are presented: fault trees with time dependencies, probabilistic fault trees with time dependencies, reliability enhanced activity diagrams. The above models are illustrated by examples. Both types of fault trees are used in modelling the time coordination of distance protections in high voltage transmission line. Then reliability enhanced activity diagrams that express the maintenance process of computer system with redundant components. Components are submitted to failures and repairs.

1. Introduction

The most famous and widely used approaches in assessment and management of safety and reliability are event trees and fault trees. In the course of the last fifty years, various extensions have been proposed to overcome their inherent limitations.
Although event trees are scenario oriented, they are not sufficient when dynamic reliability analysis is performed. It is the case in probabilistic safety analysis of nuclear power plants or in cooperation of electric power system protections, which both involve dynamic reliability schemes. For a comprehensive overview of event trees' augmentations towards dynamic reliability assessment [23] may be referred to. In that paper, the following extensions are discussed: event sequence diagrams, extended fault trees, GO-FLOW, continuous event trees, dynamical logical analytical methodology (DYLAM), dynamic event tree analysis method (DETAM), discrete event simulation.

Fault trees [7], on the other hand, are structure oriented. Various language extensions, such as: dynamic fault trees [5], repair fault trees [4], temporal fault trees [21] or probabilistic fault trees with time dependencies [2] were explored to edge the formalism's way through a particular aspects of dependability modelling. Factors that increased applicability of fault trees were the following papers: [5], where dynamic fault trees have been introduced and [4], where repair boxes have been defined. However, descriptive power of the dynamic fault trees, repair fault trees, when such time dependencies like a sequence of time consuming activities or time redundancy have to be expressed is strictly limited. Therefore, probabilistic fault trees with time dependencies (PFTTDs) have been introduced in paper [2]. They are a probabilistic counterpart to fault trees with time dependencies (FTTDs) [8], [16], [17], which are based on a non-deterministic model without any probabilistic measures. In order to compare the temporal fault trees of paper [21] with FTTDs, let us cite the following fragment from [21]: 'We wanted to retain the essentially qualitative flavour of the fault tree notation and not add too many complex quantitative facilities to it (see Refs. [29, 30]) although many of them have obvious advantages.' Reference [29] in the above fragment corresponds to our paper [16] on FTTD from References in present paper.

In the RELEX tool [26], dynamic gates are converted into Markov models. In [4], elements of Dynamic Fault Trees (DFT) and repair boxes are translated into such a subclass of colored Petri nets that is called stochastic well formed nets. The last ones are in turn converted into Markov models. In paper [19], translation from dynamic fault trees into Bayesian networks has been presented. The aforementioned formal tools: Markov models, Petri nets, Bayesian networks are not popular among engineers. Often Monte Carlo simulation is executed in order to find reliability characteristics.

A major challenge when solving problems expressed by fault trees is computational complexity caused by exponential explosion. A possible way to tackle the problem is algebraic approach [18]. The other is an approximation as Erlang distribution approximation for PFTTD [3].

Up to now, process modeling in fault trees was confined to simple cases, e.g. repairs are represented in Repair Fault Trees [4]. Maintenance processes are much more complicated. They contain not only repairs but also such activities as: testing, preventive maintenance, corrective maintenance, which are important factors in maintenance optimization. Hence, many decisions in complex maintenance process are data-dependent.

Notably, Petri nets can be applied in dynamic reliability analysis of nuclear power plants [11] and electric power systems [10]. Petri nets are used in maintenance optimization of tramway system with time redundancy [14]. In all the above cases a time dependency is crucial factor to consider. Although once again Petri nets have proven their great expressive power, they were rejected by surveyed domain experts on the grounds that they are largely obscure.

Our goal is to build a language not only capable of expressing scenarios and structures, but also engineer friendly. The main challenge in the search for prominent extensions is to increase expressive power of a language or languages in such a skillful manner that its or their intuition to engineers is left intact.

In paper [22], original twenty control flow-patterns plus identified twenty three new patterns relevant to control-flow perspective have been presented and formally expressed in Colored Petri nets. An evaluation obtained from detailed analysis of the control-flow patterns across fourteen commercial offerings including workflow systems, business process modeling languages and business process execution languages has been given. Maintenance system is an example of workflow system. According to the evaluation UML Activity Diagrams 2.0 with BPMN and XPDL are in top three products of these fourteens. Interrestingly, UML Activity Diagrams 2.3 are partially based on Petri nets [9].

Hence an idea presented in paper [13] to combine the UML Activity Diagrams (ADs) [20], a highly expressive and practically appreciated language, with probabilistic fault trees with time dependencies [2]. Reliability-Enhanced Activity Diagrams (READs) [13] is a consequence of the effort. As a result, a wide range of behaviors such as: failures, repairs, testing, preventive and corrective maintenance, resource allocations, time-consuming activities, time redundancy, data-dependent decisions, as well as sequential and parallel activities with synchronization may be expressed in dependability models. Moreover, a profile for UML models built in IBM Rational Software Architect 8 [24] has been provided. While building our profile, we incorporate the Modeling and Analysis of Real-Time and Embedded Systems Profile [25] to specify a timing model.

In paper [12], a halfway model from PFTTD to READ, which has been called fault graphs with time dependencies, has been demonstrated.

In this paper emphasis is put on sample three models the authors collaborated on. In Section 2, distance protection schema of high voltage transmission line is outlined. In Sections 3, 4 dynamic reliability models of FTTD and PFTTD respectively for time coordination of the distance protections are presented. Then, both approaches are compared. In section 6, READ model that expresses the maintenance process of computer system with redundant components is outlined. Components are subject to failures and repairs. The above presentations are based on papers [15], [2], [13]. Finally, there are conclusions.

2. Distance protection schema

Fast and selective tripping of a faulty element is a key aim for the protection of power systems. To meet this requirement, high-speed protection systems for transmission and distribution lines are under continuous development. One of the most attractive protection schemes is distance protection [1]. It is comparatively simple to apply and can be fast in operation for faults located along most of the protected circuit. Distance protection can also provide both primary and remote back-up protection functions in a single scheme (*Figure 1*).

Since the impedance of a transmission line is proportional to its length, it is legitimate to use a protection relay capable of measuring the impedance of a line up to a fault point. Such a protection relay is designed to operate only for faults occurring between the relay location and the selected reach point, so that discrimination of faults outside the protected local section is possible. The apparent

impedance of the fault loop determined from voltage and current measured at the relay location is compared with the reach point impedance. If the calculated impedance is less than the reach point impedance, it is assumed that a fault exists in the line between the relay and the reach point.

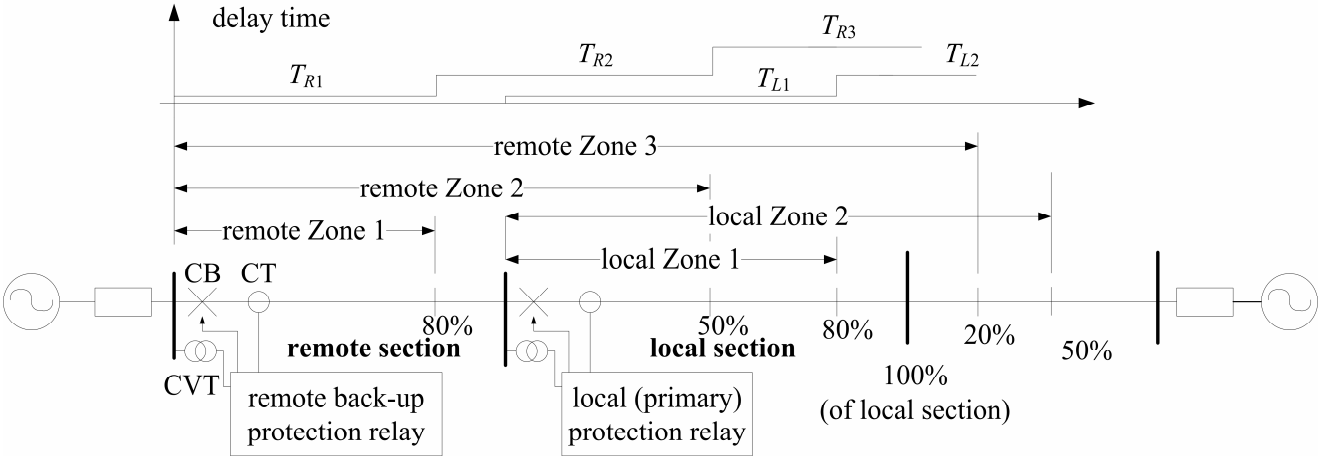

Figure 1. Protection schema of simple transmission network [15].

Distance protection relay performance is defined in terms of reach accuracy and operating time. Reach accuracy is a comparison of the actual ohmic reach of the relay under practical conditions with the relay setting value in ohms. Operating times can vary with fault current, with fault position relative to the relay setting, and with the point on the voltage wave at which the fault occurs. Measuring transient errors, e.g. produced by Capacitive Voltage Transformers (CVTs) and saturation of Current Transformers (CTs), can also adversely delay a relay operation for faults close to the reach point.

Careful selection of the reach settings and time delay settings for various zones enables correct coordination between distance relays on a power system. Basic distance protection comprises instantaneous directional Zone 1 protection and one or more time delayed zones. Typical reach and time settings for a 3-zone distance protection are shown in *Figure 1*. Distance relays usually have a reach setting covering up to 80% of the protected line for instantaneous Zone 1 protection (remote and local Zones 1 in *Figure 1*). The resulting 20% margin ensures that there is no risk of the Zone 1 protection over-reaching the protected line i.e. accidental triggering when an adjacent section is short-circuited. The overreaching can be due to errors in the current and voltage transformers, inaccuracies in line impedance data provided for setting purposes and errors of relay settings and measurements.

To ensure full cover of the line, the minimal reach setting of the Zone 2 protection should be set to 120% of protected line impedance. However, the maximal reach setting should not extend beyond 100% of the protected line plus 50% of the shortest adjacent line (50% of the local section for remote Zone 2 in *Figure 1*). Zone 2 tripping must be time-delayed to ensure grading with the primary relaying applied to adjacent circuits (local Zone 1).

Remote back-up protection for all faults on adjacent lines is provided by the second and third zone protections which are time-delayed to discriminate with Zone 2 protection plus CB tripping time for the adjacent line. Zone 3 reach should be set to at least 1.2 times the impedance presented to the local relay for a fault at the remote end of the adjacent section.

These three zones are used in order to roughly recognize fault location. Finding the zone where fault has occurred is based on measurements of impedance of transmission line from the place of protection mounting to the fault location.

Proper co-ordination of the distance relay settings with those of other relays is required. Independent timers are available for the three zones to ensure this.

In analysis performed in the paper, distance relay format is a full distance scheme, i.e., each zone is provided with independent set of impedance and time measuring elements for each impedance loop.

If the Remote Protection (RP) recognizes a fault in $\text{Zone}_\text{R}\ i$, where $i \in \{1,2,3\}$, then after time delay T_{Ri}, the RP sends signal to the remote CB in order to open it. Graded times of the tripping delays for particular zones are used ($T_{R1}<T_{R2}<T_{R3}$), i.e., the greater the zone number, the greater the time delay. For Zone 1, time delay of start of the CB tripping is usually equal to zero. Three local zones are denoted by $\text{Zone}_\text{L}\ i$, where $i \in \{1,2,3\}$. The following relation for tripping delays of these zones: $T_{L1}<T_{L2}<T_{L3}$ is also true.

For Zone 1, instantaneous tripping is normal. The Zone 2 element has to grade with the relays protecting the adjacent line (local section in *Figure 1*) since the Zone 2 element covers part of

this line. If this line has distance protection applied, the time delay required is that to cover the total clearance time of the downstream relays, i.e. time between the fault inception and the fault clearing. In addition a suitable safety margin is added. A typical time delay is 350 ms [1], and the normal range is 200-500 ms. Considerations for the Zone 3 element are the same as for the Zone 2 element, except that the downstream fault clearance time is that for the Zone 2 element of a distance relay. Assuming distance relays are used, a typical time is 800 ms [1]. Examples of impedance characteristics for Zone 1, 2, 3 are given in *Figure 2*.

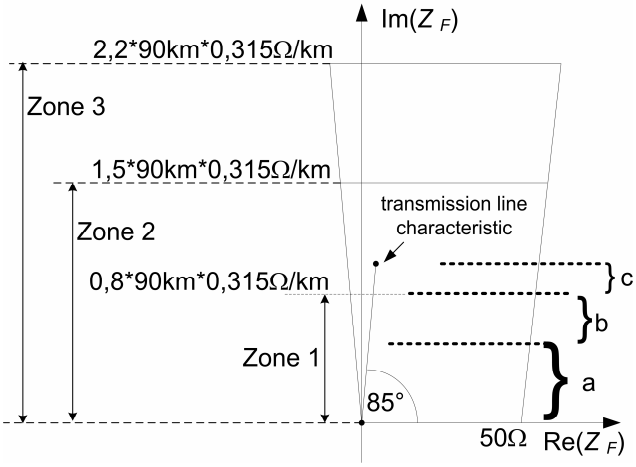

Figure 2. Impedance characteristic of the relays [15].

In the analysis performed in the paper, the following parameters were taken into account: entrance time to and exit time from impedance characteristics of appropriate zones for local protection (LP) and remote protection (RP) under assumption: the fault is located by relays in subsection depicted in *Figure 1* as *a*. These times are denoted as $T_{Xen(ex)Y|a}$, where $X \in \{L, R\}$, L for the LP, R for the RP, *en* is for entrance times to, *ex* for exit time from impedance characteristics of the Zone Y, where $Y \in \{1,2,3\}$ under assumption: the fault is located by relay in subsection *a*. CB tripping lasts the time T_{off}. Each of these times is characterized by minimal and maximal, respectively, values T_{min} and T_{max}, e.g. $T_{off\ min}$, $T_{off\ max.}$
Problem to be solved is as follows.

Problem 1
Input data:
Power transmission line with distance protection schema is analyzed. The transmission line is represented by its characteristic impedance and the power system by equivalent source impedances and loads. Fault cases are represented by their locations, types and resistances. For each protection there are its protection zones that cover different parts of the line. For each zone, its impedance characteristics are given. Circuit breakers are described by their interrupting times.
Output data:
Time delay settings for each zone of each distance protection.

3. Time coordination of distance protections using fault trees with time dependencies

This section is based on paper [15].
Fault Tree with Time Dependencies (FTTD) analysis starts with identifying hazards (dangerous situations). For each hazard, a FTTD is created.
Let us make the following assumption regarding the fault occurrence.

Assumption 1: Should the fault occur in the analysis interval, it is permanent and no other fault may happen.

According to requirements specification, if there is a fault in the local section (LS), and additionally the local protection (LP) and the local circuit breaker (CB) are efficient, then only the LS should be disconnected. The analyzed *hazard* is event E1: *remote CB tripping provided the local CB can be opened*. Hence, the hazard occurs when a greater than required part of power network is isolated. The FTTD for this hazard and fault located by relays in subsection *a* is illustrated in *Figure 3.*
Duration time of an event is length of time interval between the start and the end of the event. Minimal and maximal duration times of an event are expressed by the pair <min, max> which is close to right upper corner of the rectangle that represents this event. If the duration of an event is not known then it can be assumed that the minimal duration time is equal to 0, while the maximal one is infinity. In this case the notation <0, ∞> is used. An example of the event with such duration time is E15 in *Figure 3.* If duration time of the event is given by <0,0>, it means that the event is immediate one with zero duration time. Minimal and maximal, respectively, duration times of event E9 are minimal and maximal values of CB tripping time.

Gates used in FTTD are of two classes: causal and are causal XOR. In order to illustrate delay time, let

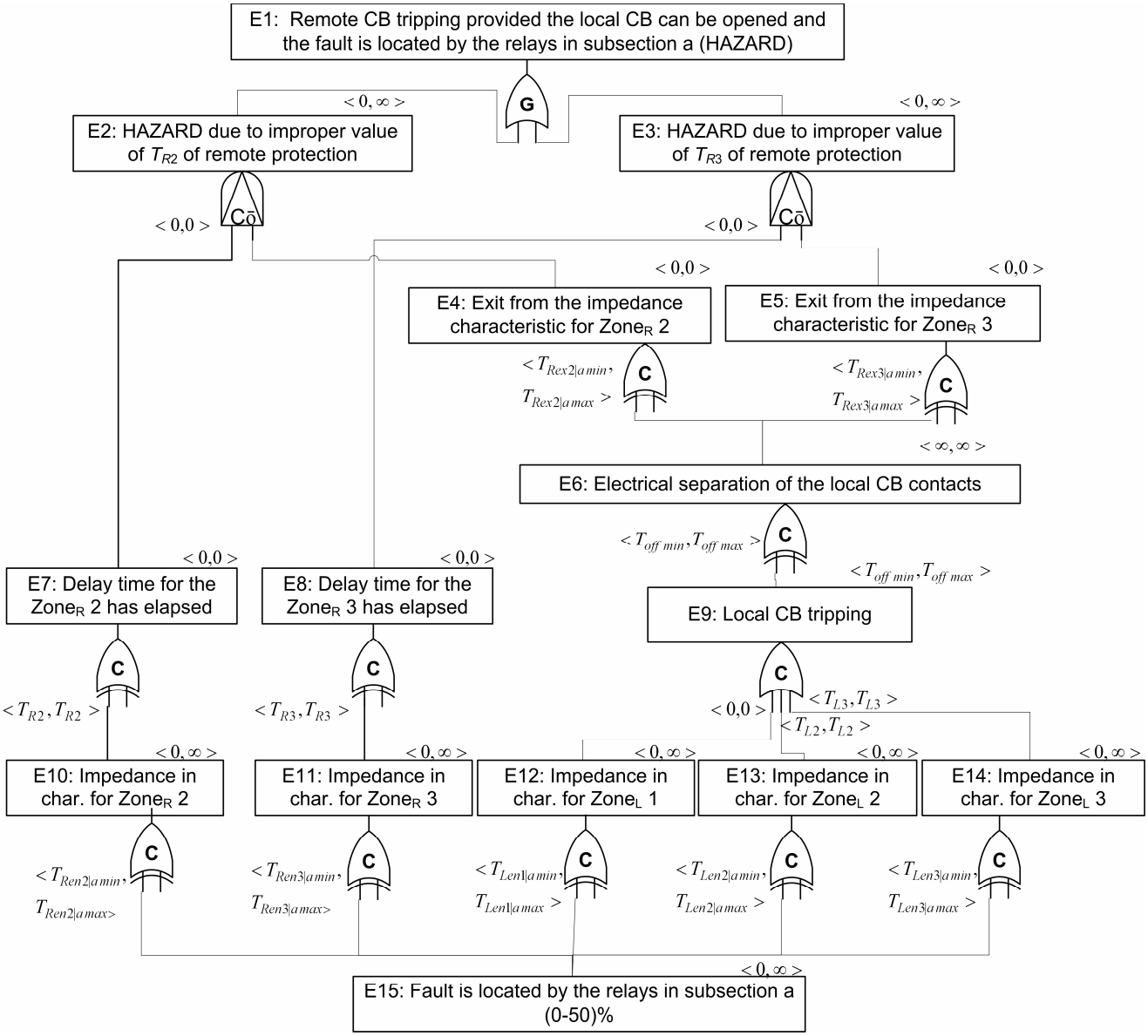

Figure 3. FTTD for hazard: remote CB tripping provided the local CB can be opened and the fault is located by relays in subsection *a* [15].

generalization. Causal gates are denoted by symbol 'C', while generalization gates by symbol 'G'. The generalization gate behaves as ideal logical circuit gate with zero propagation times. For output events of generalization gates there are no duration time parameters. Duration times of these events depend on duration times of input events. For causal gates, output event (effect) is delayed with respect to input event or input events (causes). The delays are expressed by their minimal and maximal values represented by the pair <min, max>, which is close to symbol of the gate. For output events of causal gates the duration times are assigned.

Gates are numbered in the following way: number of gate is equal to the number of its output event. Gate 1 is generalization OR. Gates 2 and 3 are causal priority AND. Gate 9 is a causal OR. The other gates us consider events E15, E12 and causal XOR gate 12. Delay between start of the fault (E15) and start of event (E12 - "the fault loop impedance measured by the LP is located inside the characteristic set for Zone 1") is expressed by minimal and maximal values of $T_{Len1|a}$, which are time parameters of the gate.

Among causal gates, there are ones with and without cause-effect overlapping. Gates without cause-effect overlapping are denoted by symbol ō. Gates 2 and 3 are without cause-effect overlapping, while the others are with cause-effect overlapping.

Let us consider events E15, E12, and gate 12 which is causal XOR with cause-effect overlapping.

The graphical representation of the causal XOR gate with cause-effect overlapping with two input and one output events is given in *Figure 4.*

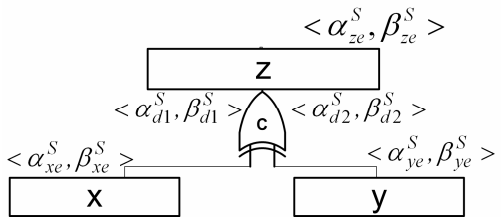

Figure 4. The causal XOR gate with cause-effect overlapping and its events [15].

Meaning of time parameters given in *Figure 4* is as follows:

- α^S_{d1}, β^S_{d1} – represent, respectively, minimal and maximal delay time between start of event x (cause) and start of the event z (effect); effect must started not earlier than α^S_{d1} and not later than β^S_{d1} counted from start of the event x,
- α^S_{d2}, β^S_{d2} – represent, respectively, minimal and maximal delay time between start of event y (cause) and start of the event z (effect),
- α^S_{xe}, β^S_{xe} - minimal and maximal duration time of the event *x*,
- α^S_{ye}, β^S_{ye} - minimal and maximal duration time of the event *y*.

Formal definition of causal XOR gate with cause-effect overlapping is given by formula (1).

$$
\begin{aligned}
&occur(z) \Rightarrow \\
&(occur(x) \wedge duration(x) \geq \alpha^S_{d1} \\
&\wedge \tau(xs) + \alpha^S_{d1} \leq \tau(zs) \leq \tau(xs) + \beta^S_{d1} \\
&\wedge \tau(zs) \leq \tau(xe)) \qquad (1) \\
&\oplus (occur(y) \wedge duration(y) \geq \alpha^S_{d2} \\
&\wedge \tau(ys) + \alpha^S_{d2} \leq \tau(zs) \leq \tau(ys) + \beta^S_{d2} \\
&\wedge \tau(zs) \leq \tau(ye))
\end{aligned}
$$

where:
$\tau(is)$ – time instant in which event *i* was started, $i \in \{x,y,z\}$,
$\tau(ie)$ - time instant in which event *i* was ended, $i \in \{x,y,z\}$,
occur(*i*) is the logical formula with meaning: event *i* has occurred, $i \in \{x,y,z\}$,
duration(*x*) is length of time interval when event *x* has occurred, analogically: duration(*y*),
$\oplus$ - logical symbol "exclusive disjunction" (events *x* and *y* cannot both occur).
The time relations between the event *x* (one of causes) and the event *z* (effect) are shown in *Figure 5*. The symbol $\tau(zs)$ with the edge $\leftrightarrow$ illustrates the time interval in which the event *z* can be started.

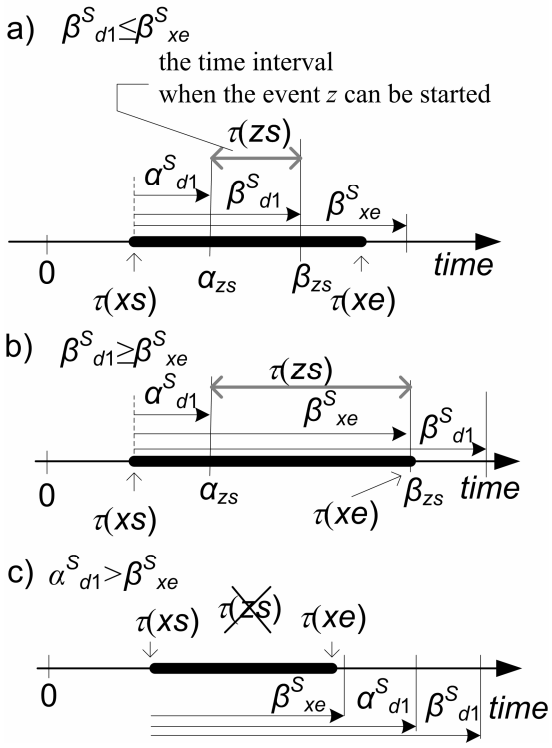

Figure 5. The time relations between the event *x* and the start of the event *z* for causal XOR gate with cause-effect overlapping [15].

Values $T_{Len1|a\,min}$, $T_{Len1|a\,max}$ represent minimal and maximal delay times between time instant E15 starts and time instant E12 starts. Maximal duration time of event E15 is equal to ∞. Therefore, in order to cause E12, according to expression (1), the following conditions have to be satisfied: $T_{Len1|a\,min} < duration(E15)$ and $\tau(\mathrm{E12}s) \leq \tau(\mathrm{E15}e)$.
Hence, the fault (E15) has to last at least $T_{Len1|a\,min}$, and it has to end not earlier than instant when the impedance seen by the LP is in the characteristic set for Zone 1 (E12), i.e. events E12 and E15 are overlapped.
According to expression (1), the following relation holds:
$\tau(\mathrm{E15}s) + T_{Len1|a\,min} \leq \tau(\mathrm{E12}s) \leq \tau(\mathrm{E15}s) + T_{Len1|a\,max}$
Let us analyze events E9, E12, and gate 9. In this case, the overlapping condition: $\tau(\mathrm{E9}s) \leq \tau(\mathrm{E12}e)$ is satisfied because $\tau(\mathrm{E9}s) = \tau(\mathrm{E12}s)$ (delay time for gate 9 is 0) and $\tau(\mathrm{E12}s) \leq \tau(\mathrm{E12}e)$.
The gate 2 is a causal priority AND without the overlapping.
Formal definition of causal priority AND gate without cause-effect overlapping is given by formula (2).

$$
\begin{aligned}
&occur(z) \Rightarrow \\
&occur(x) \wedge occur(y) \wedge \boldsymbol{\tau}(xs) \leq \boldsymbol{\tau}(ys) \qquad (2) \\
&\wedge \boldsymbol{\tau}(ys) + \boldsymbol{\alpha}^S_d \leq \boldsymbol{\tau}(zs) \leq \boldsymbol{\tau}(ys) + \boldsymbol{\beta}^S_d
\end{aligned}
$$

where:

- α_d^S, β_d^S represent the minimal and maximal time delays between the start time instant of the later cause y and the effect *z*.

In this gate, event *x* is at the priority input, i.e. must start prior to the event at the second input. The examples, when event *z* can occur are given in *Figure 6. a, b, d* and the example when event *z* cannot occur is given in *Figure. 6. c.*

For this gate there is no cause-effect overlapping, i.e. neither $\tau(zs) \le \tau(ye)$ nor $\tau(zs) \le \tau(xe)$ is required.

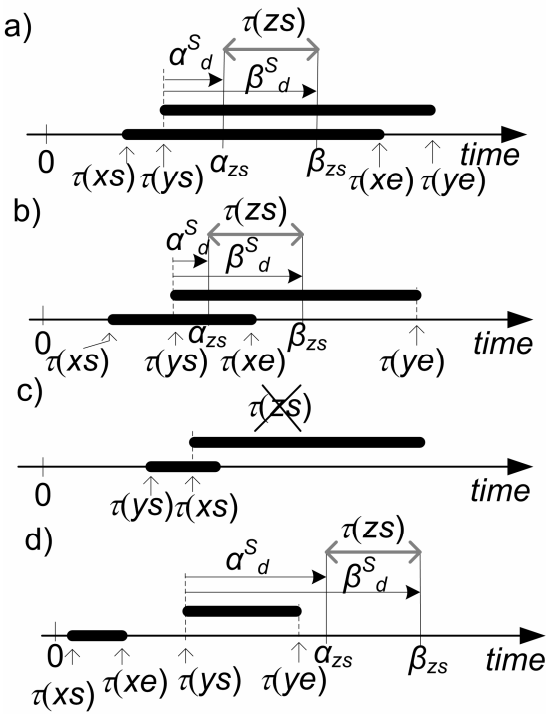

Figure 6. Time relations between the events for causal priority AND gate without cause-effect overlapping: a), b) events occurred together, c) events occurred in incorrect order, d) events occurred in disjoint time intervals [15].

For gate 2, if event E2 has occurred then event E7 had occurred not later than event E4. According to the definition of the causal priority AND gate without cause-effect overlapping (see expression (2)), if the event E2 has occurred, then the start of event E7 had occurred not later than the start of event E4, i.e. τ(E7*s*)≤τ(E4*s*). In this case, the RP trips remote CB and this is prior to fault clearance symptoms impacted by LP. Hence, the RP relay has reacted too early and caused occurrence of the hazard event E2. Delay time of gate 2 is equal to 0, since in this case the hazard starts immediately after E4 has started. In order to avoid the hazard, the following condition: τ(E4s)<τ(E7s) has to be satisfied.

If the local CB is not opened by the LP (e.g. local CB failed), then event E4 does not occur, and the hazard does not occur (in this case the remote CB should be opened).

Let us suppose that the RP had observed that the local CB is opened (event E4) before time delay T_{R2} has passed, i.e. τ(E4*s*)≤τ(E7*s*), so the RP will not trip the remote CB. Hence, event E2 does not occur (the hazard does not occur).

The E1 event occurs if at least one of events E2 or E3 has occurred. Hence, the hazard occurs, if at least one remote protection time delay for Zone 2 or Zone 3 has been set incorrectly.

Let us consider the sub-tree with event E2 as a root. In this sub-tree, left sub-tree with event E7 as a root concerns the RP, while right sub-tree with event E4 as a root concerns the LP. In sub-tree with event E3 as a root, left sub-tree with event E8 as a root concerns the RP, while right sub-tree with event E5 as a root concerns the LP.

If a fault is located by the LP and the RP in subsection *a* of the LS, then impedance seen by the RP can be inside operating characteristics of Zone_R 2 or Zone_R 3. Therefore, tripping of the remote CB can be started after time delays T_{R2}, T_{R3}, respectively, relative to entry instant of impedance into characteristics of Zone_R 2, Zone_R 3. These times are given by real numbers, and are represented by delay times of causal XOR gates with numbers 7 and 8 (see expression (1)). Equality of minimal and maximal time delays for each input is a specific case of general definition of causal XOR gate. Time T_{R2} is the time from start instant of event E10 till start instant of event E7. The event E7 lasts 0 ms, E10 can last longer.

If the fault located by relay in subsection *a* of the LS occurred at time instant τ and it still lasts then impedance seen by the RP enters into characteristics of Zone_R 2 at instant $\tau + T_{Ren2|a}$. Time $T_{Ren2|a}$ is the delay time of causal XOR gate 10. Time $T_{Ren3|a}$ is the delay time of causal XOR gate 11.

A trajectory of the impedance seen by the RP exits from characteristics of Zone_R 2 after time $T_{Rex2|a}$ in relation to the instant of electrical separation of contacts in the local CB. This is time delay between start instant of event E6 and start instant of event E4. Event E4 lasts zero time while E6 lasts infinite time.

CB tripping lasts the time T_{off} (*Figure 3*). Hence, delay time of gate 6, i.e. time between start instant of event E9 and start instant of event E6, is equal to T_{off}. Event E9 lasts time T_{off}.

If the fault is located by relays in subsection *a* of the LS then impedance seen by the LP can be inside operating characteristics of Zone_L 1, Zone_L 2 or Zone_L 3. Hence, local CB tripping can be started immediately, after time T_{L2}, or T_{L3}, respectively, with respect to entry instant of impedance seen by the LP

into characteristic for Zone_L 1, Zone_L 2 or Zone_L 3. Three times, namely, 0, T_{L2}, or T_{L3} are time delays of causal OR gate no. 9. They are equal to lengths of time intervals between start instants of input events E12, E13, E14 of this gate and start instant of output event E9.

A formal definition of a causal OR similar to the definition of causal XOR with cause-effect overlapping is given by formula (1), except that symbol $\oplus$ is replaced by $\vee$.

On a causal OR gate additional requirements can be imposed. For example, for gate 9 it is required that output event E9 starts at instant when the earliest time delays: 0, T_{L2}, or T_{L3}, respectively, for Zone_L 1, Zone_L 2 or Zone_L 3 elapsed:

$$\tau(\text{E9}s) = \min\{\tau(\text{E12}s), \tau(\text{E13}s) + T_{L2}, \tau(\text{E14}s) + T_{L3}\}$$

where $\tau(\text{E}i s)$ for $i \in \{9, 12, 13, 14\}$ is start instant of event Ei.

Entry times of impedance into characteristics for zones Zone_L 1, Zone_L 2 and Zone_L 3 are times $T_{Len1|a}$, $T_{Len2|a}$, and $T_{Len3|a}$. These times are time delays of gates 12, 13, and 14.

In [15], formal analysis of the FTTD has been given. Now we give only an intuitive derivation of a formula.

In order to avoid the hazard E2, event E4 has to start before event E7, i.e., $\tau(\text{E4}s) < \tau(\text{E7}s)$. Moreover, minimal value of $\tau(\text{E7}s)$ has to be greater than maximal value of $\tau(\text{E4}s)$. Minimal delay between the start of event E15 and the start of event E7 is equal to $T_{R2} + T_{Ren2|a\,min}$, see path between events E15 and E7 in *Figure 3*. Maximal delay between the start of event E15 and the start of event E4, provided $\tau(E9s) = \tau(E12s)$ is equal to $T_{Rex2|a\,max} + T_{off\ max} + T_{Len1|a\,max}$. Hence, requirement for time delay T_{R2} of Zone 2 of the remote protection is as follows:

$$T_{Rex2|a\,max} + T_{off\ max} + T_{Len1|a\,max} - T_{Ren2|a\,min} < T_{R2}.$$

In order to solve the Problem 1 using FTTD, we propose the following method:

1. Having power transmission line with distance protection zones, identify subsections. Subsection is such a part of a section that is covered by a set of zones of local and back-up protections.
2. For each subsection, create FTTD for the hazard and for faults that are located by protections in this subsection.
3. Having the FTTDs, find formulae for time delays of each zone of each protection.
4. Find minimal and maximal values of variables that occur in the formulae from point 3.
5. Calculate time delay for each zone of each protection.

Minimal and maximal values of variables that occur in the formulae obtained in point 3. can be found by experiments with real power system or from computer simulation of the system using e.g. EMTP [6].

In paper [15], maximal values of variables that occur in the formulae from point 3. have been evaluated in two ways using EMTP. First, the greatest 0.5% values of entry and exit times of trajectories into or from impedance characteristics have been omitted. Then the greatest 0.1% values of the times have been neglected.

4. Time coordination of distance protections using probabilistic fault trees with time dependencies

Assumption 2: Hazard probability due to improper value of time delay TRj of j-th zone of remote protection, where $j \in \{2,3\}$, should be below 0.005 (0.5%) level.

Probabilistic fault tree with time dependencies (PFTTD) for the time coordination is of similar shape as this from *Figure 3*. Delay times for gates are expressed by random variables.

Let R(X) be a realization of random variable X, i.e., a value generated according to the distribution of the X.

Causal XOR gate is described as follows:

$$\begin{aligned} &occur(z) \Rightarrow \\ &(occur(x) \wedge \tau(zs) = \tau(xs) + R(d1)) \\ &\oplus (occur(y) \wedge \tau(zs) = \tau(ys) + R(d2)) \end{aligned} \tag{3}$$

where *d1* (*d2*) - random variable (RV) that represents time delay between the occurrence (start) of the cause *x* (*y*) and the effect *z*.

Causal priority AND gate is described as follows:

$$\begin{aligned} &\text{occur}(z) \Rightarrow \\ &(\text{occur}(x) \wedge \text{occur}(y) \\ &\wedge \tau(xs) \le \tau(ys) \wedge \tau(zs) = \tau(ys) + R(d)) \end{aligned} \tag{4}$$

where: *d* - RV that represents the time delay between the occurrence of the latter cause y and the effect *z*.

Causal OR gate is described as follows:

$$\begin{aligned} &\text{occur}(z) \Rightarrow \\ &(\text{occur}(x) \wedge \tau(zs) = \tau(xs) + R(d1)) \\ &\vee (\text{occur}(y) \wedge \tau(zs) = \tau(ys) + R(d2)). \end{aligned} \tag{5}$$

In order to solve the Problem 1 using PFTTD, we propose the following method:

1. Having power transmission line with distance protection zones, identify subsections. Subsection is such a part of a section that is covered by a set of zones of local and back-up protections.
2. For each subsection, create PFTTD for the hazard and for faults that are located by protections in this subsection.
3. Find probability distribution of RVs that appear in the PFTTD.
4. Using PFTTD simulator, find time delay for each zone of each protection.

In paper [2], the probability distributions in point 3. have been determined using EMTP.

5. Comparison of time coordination of distance protections using FTTD and PFTTD

First of all, FTTD model is a non-deterministic one, in which only minimal and maximal values of time parameters are known. Although the parameters of the FTTD for the protection schema have been determined in such way that predefined parts of greatest values of some random variables have been omitted, in FTTD there are no probabilistic measures at all. Calculation of time delays for zones of protections is analytic. Having knowledge about size of the omitted parts of random variable values and shape of formulae for the time delays, a hazard probability estimates can be found [15].

In PFTTD approach, probability distributions of entry (exit) times to (from) impedance characteristics of protection zones are determined. Hence, more probabilistic information is involved. Such time delays that the hazard is not greater than a bound are calculated by PFTTD based simulation.

The time delay values obtained by both approaches are close.

Conclusion is that in the PFTTD approach hazard probability estimate is more exact, while in the FTTD approach computation costs are smaller.

6. Reliability enhanced activity diagram of computer system maintenance process

This section is based on paper [13].

In this section a computer system consisting of several components and repair facilities (*Figure 7*) will be investigated by means of READ. For the system to run properly, one CPU, one disc and one memory unit must be working properly, i.e. be in the "Running" state. However, to advocate for reliability, hot spares of disc and memory units were introduced.

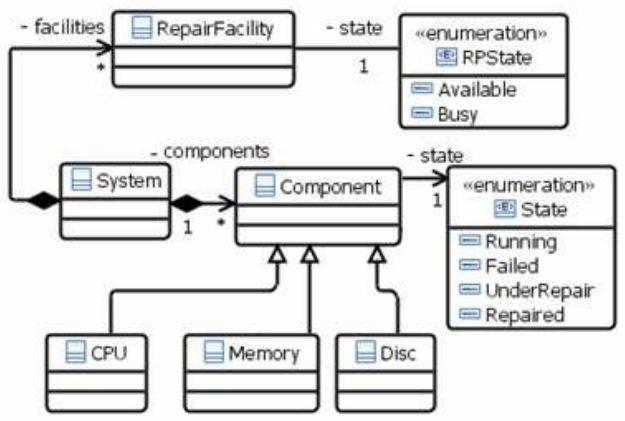

Figure 7. Classes and enumerations modeling the case study system [13].

When a component fails, it waits for an 'Available' repair facility and subsequently undergoes repair. Contrary, a repair facility is 'Busy' when servicing another component being in the 'UnderRepair' state.

All in all, in the case study maintenance process five components and two repair facilities comprise the system (*Figure 8*). In the READ method, we consider UML Object Diagram to be defining the Initial Object Set.

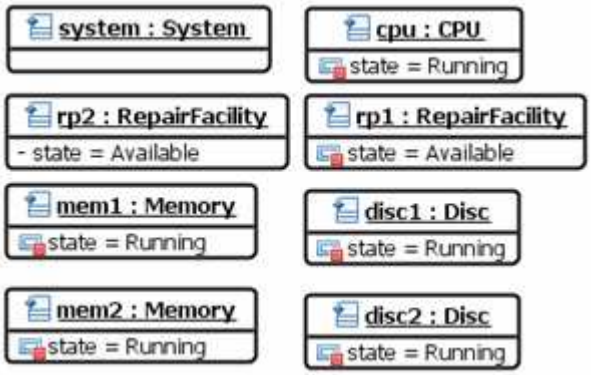

Figure 8. Initial Object Set [13].

To group actions, gates and objects the model (*Figure 9*) is divided into three vertical partitions, those being Regular service, Repair and Maintenance process state. Objects flow horizontally between them as system components fail and repair. Let us analyze the top-most model section: CB1, A1, CB2, T1, CB4, CB3, G5, CB5, G6, CB6, A6 and T4 which apply to memories. The middle and bottom section work alike.

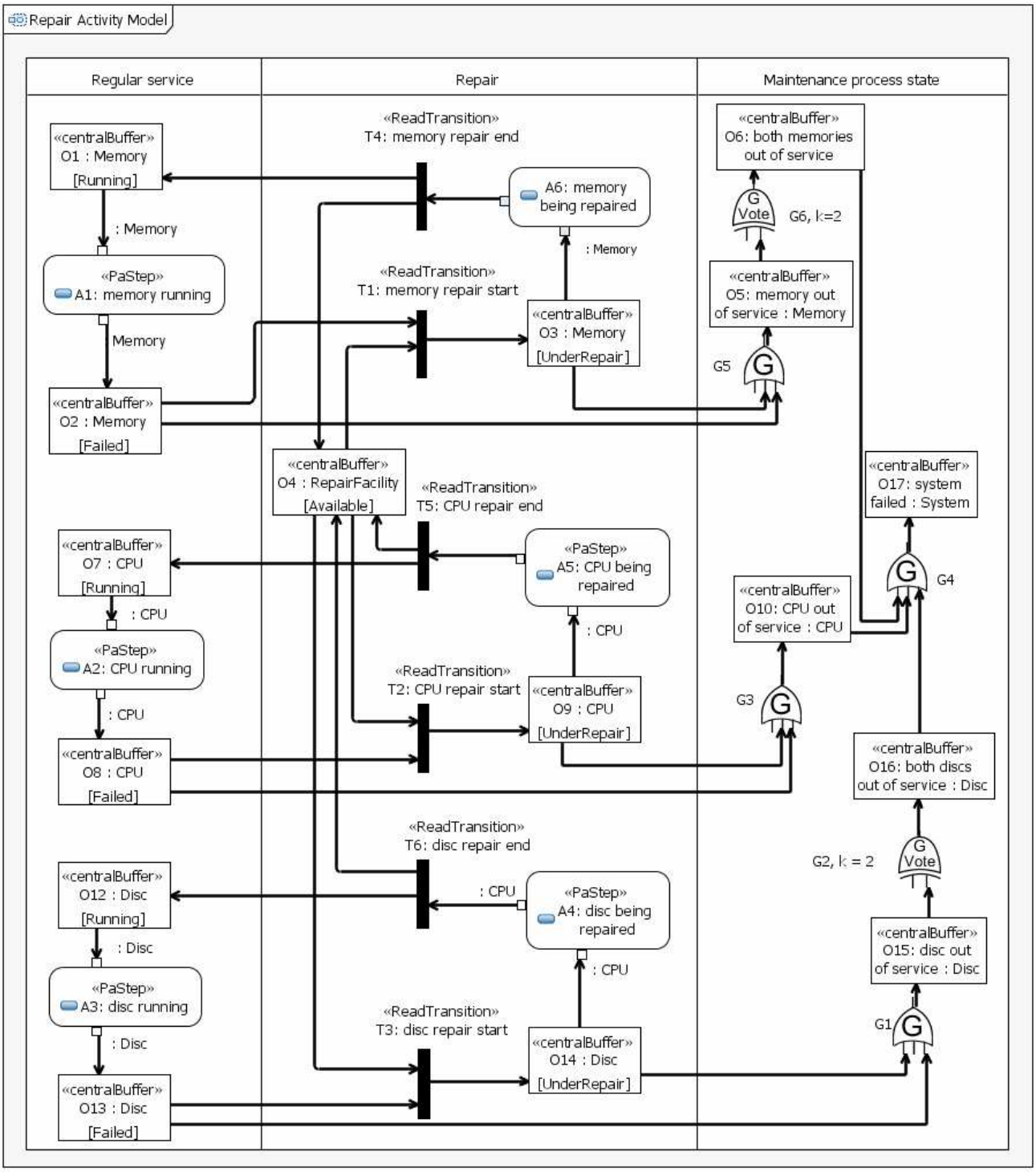

Figure 9. The case study model [13].

Objects from *Figure 8* fill in CB1 and CB4 central buffers of the top section at the initial analysis moment causing the A1 action to start two times in parallel (one for the 'mem1' and the other for the 'mem2' object). This action models correct memory operation, therefore its timing model defines a proper random variable. After A1 has finished for some memory unit (the first failed memory), the action removes the respective object from CB1 and puts it into CB2 changing its state to 'Failed'. Next, if a repair facility is available, the T1 transition realizes the allocation of the facility. As a result, the memory object is moved to the CB3 buffer and its repair is initialized.

If the component is failed, or it is under repair, the G5 GOR gate puts an object into CB5 buffer denoting that the component is out of service. If the second memory fails, CB6 occurs through G6, and the system is failed (CB17) on the virtue of the G4 GOR gate.

The A6 action lasts as long as the component is

repaired. Next, the repair facility is released (T4) and the repaired memory is restored into the 'Running' state (CB1). This causes a change in the CB5 buffer effectively restoring the whole system by removing objects from CB6 and CB17.

7. Conclusion

It has been shown how fault trees with time dependencies that are non-deterministic models and probabilistic fault trees with time dependencies can be used in dynamic reliability analysis of electric power system. Both approaches have been compared. Reliability enhanced activity diagram (READ) model of relatively simple maintenance process of the computer system with redundancies has been presented.

Now we are developing READs in order to model and optimize much more complex process as low-cost airlines maintenance.

References

[1] ALSTOM T&D (2002). Network Protection & Automation Guide, First edition, ALSTOM.

[2] Babczyński, T., Łukowicz, M. & Magott, J. (2010). Time coordination of distance protections using probabilistic fault trees with time dependencies. *IEEE Transaction on Power Delivery*, July, Vol. 25, No. 3, 1402-1409.

[3] Babczyńsk,I, T., Łukowicz, M. & Magott, J. (2010). Selection of Zone 3 time delay for backup distance protection using probabilistic fault trees with time dependencies. *Przegląd Elektrotechniczny, Electrical Review*, Vol. 86, No 9, 208-215.

[4] Bobbio, A. & Codetta, D. (2004). Parametric fault trees with dynamic gates and repair boxes. *Proc. Annual Symposium on Reliability and Maintainability*, 459-465.

[5] Dugan, J.B., Bavuso, S.J. & Boyd, M.A. (1992). Dynamic fault-tree models for fault-tolerant computer systems. *IEEE Trans. Reliab*., Vol. 41, No 3, 363-367.

[6] *EMTP* (*Electromagnetic Transient Program*) "Reference manual", Leuven center, 1987.

[7] *Fault Tree Analysis (FTA)* (1990). International Technical Commission, IEC Standard, Publication 1025.

[8] Górski, J., Magott, J. & Wardzinski, A. (1995). Modelling fault trees using Petri nets. *Proc. SAFECOMP*'95, Belgirate, Italy, *LNCS*, Springer-Verlag.

[9] ISO/IEC 15909-1, *High-level Petri nets: Concepts, definitions and graphical notation*, 2004.

[10] Jenkins, L. & Khincha, H.P. (1992). Deterministic and stochastic Petri net models of protection schemes. *IEEE Transaction on Power Delivery* , Vol. 7, No 1.

[11] Lee, S.J. & Seong, P.H. (2004). Development of automated operating procedure system using fuzzy colored Petri nets for nuclear power plants. *Annals of Nuclear Energy*, Vol. 31, 849-869.

[12] Kowalski, M. & Magott, J. (2011). Conjoining fault trees with Petri nets to model repair policies. *Artificial Intelligence and Soft Computing*, Springer (to appear).

[13] Kowalski, M. & Magott, J. (2011). Towards an UML profile for maintenance process and reliability analysis. *Artificial Intelligence and Soft Computing*, Springer (to appear).

[14] Kowalski, M., Magott, J., Nowakowski, T. & Werbińska-Wojciechowska, S. (2011). Analysis of transportation system with the use of Petri nets. *Maintenance and Reliability*, 2011, No 1, 117-128.

[15] Łukowicz, M., Magott, J. & Skrobanek, P. (2011). Selection of minimal tripping times for distance protection using fault trees with time dependencies. *Electric Power Systems Research*, doi:10.1016/j.epsr.2011.03.003 (to appear).

[16] Magott, J. & Skrobanek, P. (2000). A method of analysis of fault tree with time dependencies. *Proc. SAFECOMP* 2000, Rotterdam, The Netherlands, LNCS,Vol. 1943, Springer-Verlag, 2000, 176-186.

[17] Magott, J. & Skrobanek, P. (2002). Method of time Petri net analysis for analysis of fault trees with time dependencies. *IEE Proceedings - Computers and Digital Techniques*, Vol. 149, No 6, 2002, 257-271.

[18] Merle, G., Roussel, J.-M., Lesage, J.-J. & Bobbio, A. (2010). Probabilistic algebraic analysis of fault trees with priority dynamic gates and repeated events. *IEEE Transactions on Reliability*, Vol. 59, No 1, 250-261.

[19] Montani, S., Portinale, L., Bobbio, A. & Codetta-Raiteri, D. (2008). RADYBAN: a tool for reliability analysis of dynamic fault trees through conversion into dynamic Bayesian networks. *Reliability Engineering and System Safety*, Vol. 93, Issue 7, July, 922-932.

[20] OMG *Unified Modeling Language (OMG UML), Superstructure Version 2.3* (2010). May.

[21] Palshikar G.K. (2002). Temporal fault trees. Information and Software Technology, Vol. 44, 137-150.

[22] Russel, N., ter Hofstede, A.H.M., van der Aalst, W.M.P. & Mulyar, N. (2006). *Workflow control-flow patterns, A revised view.*

[23] Siu, N. (1994). Risk assessment for dynamic systems: An overview. *Reliability Engineering and System Safety*, Vol. 43, 43-73.
[24] Developer Works on IBM Rational Software Architect https://www.ibm.com/developerworks/rational/
[25] *The UML Profile for MARTE: Modeling and Analysis of Real-Time and Embedded Systems*. http://www.omg.org/omgmarte/Specification.htm
[26] http://www.relex.com/resources/art Resources on Fault Trees