Tool for analysis of the fault tree with time dependencies

Streszczenie. Analiza drzew niezadostności jest często stosowana techniką wspomagającą analizę bezpieczeństwa systemów. Jednym z obszarów zastosowań są systemy czasu rzeczywistego, dla których istotne są nie tylko informacje o tym, czy hazard może wystąpić, ale również informacje związane z aspektami czasowymi. W niniejszej pracy zostało zaproponowana oprogramowanie w formie pliku XML oraz przedstawiono analizę drzew niezadostności z zależnościami czasowymi, w tym podejmowano numerycznie jak i parametrycznie.

Abstract. The fault tree analysis is one of the most frequent used methods of supporting the safety systems analysis. Real time systems are one of the fields of applications. Information of hazard occurrence in these systems is as important as information related to timing aspects. In this chapter the models of gates has been collected, the notation of events for XML file generation has been given and application for analyzing of fault trees with time dependencies, given both numerically and parametrically, has been shown.

Słowa kluczowe: drzewa niezadostności z zależnościami czasowymi, oprogramowanie do analizy drzew niezadostności

Keywords: fault trees with time dependencies, tool for fault tree analysis.

1. Introduction

The safety is one of the most important aspects of systems. Safety system is a system which, directly or by initiation of a given scheme of events, does not lead to hazard. Hazard is defined as a risky situation, for example: a loss of aircraft controlling, a dangerous concentration of gas, a lack of cooling of the reactor in a nuclear power plant, targeting two trains on one track, but also a lack of materials for the production (material loss), a lack of goods in shops, or even late delivery of drugs.

Hazard is then the situation that can lead to an accident, for example: injury or death of people or considerable material loss.

Application of certain techniques of analysis is required in order to avoid the above mentioned situations [1], [2]. The analysis of fault trees is one of the most frequent used techniques – without taking into account the time aspects (norm [3], [4]) or extended with time aspect [5-9]. Detailed description of issues related to analysis of fault trees with time dependencies ("top-down" approach – from hazard to causes) can be found in [10], [8].

Analysis of the fault trees with time dependencies is a technique of building the cause-leading-to-hazard tree for each identifiable risky situation (for each hazard). This type of tree is defined as the fault tree – the example of this tree is given in subchapter 3. Classic analysis of fault trees [4] lets to identify minimal cut sets which can lead to occurrence of hazard. "Minimal" means that all events in this cut set are necessary and sufficient for occurrence of hazard.

Usage of the classic analysis of fault trees makes the analysis of time dependencies between events impossible to perform, though this kind of dependencies can be very important. They carry information such as, time of hazard occurrence (if hazard can be tolerated), time from occurrence of given events to hazard (for example between failure of the cooling pump in nuclear reactor and over temperature of the core), dependencies between events and others.

The knowledge of time aspects gives the opportunity of preventing of hazard occurrence as well as of decreasing the risk of hazard occurrence by, among others, usage of better devices (if closing of safety valve lasts to long, another, faster one, can be used), introducing of protection/redundancy, or even for changing of the project of system.

The tools (software) for the analysis of classic fault trees and for the analysis of fault trees with time dependencies is not ready jet for commercial usage. The possibility of carrying out the analysis using the time given as parameters and possibility of introduction of FTTD from XML file is an important novelty.

It is necessary, and often essential for a running system, to describe the time conditions as a parameters, like: tmax – maximal time of delivery, tmin – minimal time of reaction, tzmin, tmax – respectively, minimal, maximal time of security response time and then to perform the analysis that will provide the information about what conditions must be satisfied by those parameters.

Examples of using of FTTD analysis can be found in [11], [12], [13].

2. Models of gates and events

The analysis of fault trees with time dependencies can be performed with different kinds of gates [8], [14].

The types of gates that are supported by software named INES v.2 will be show in this subsection. Notation of events is show on Fig 1.

\[ \langle \alpha^S, \beta^S \rangle \]

Fig.1. Event notation

Time parameters \( \langle \alpha^S, \beta^S \rangle \) describe, respectively, minimal and maximal time of event duration, and are necessary for output events of causal gates and leaves.

This parameters are described by superscript \( S \).

This notation is used for selection of static parameters, derived from specification of system and used devices (for example: time of valve closure, time of train travel from the semaphore to the junction with the road), laws of physics (ex.: time of transmission of audio signal in the air), operator settings (ex.: the value of the time lag between the signal from the sensor and emergency switch), etc. The notation of the gates that are supported by INES software is show on fig. 2.

In the generalization gates output event is the same as one of the input events (for XOR gate) or occur when the input events coexist (for AND gate) – start corresponds to the start of event which has occurred later, and the end corresponds to end of the event which has ended earlier.

In causal gates the output event is the result of event (XOR gate) or coexistent events (AND gate) and can occur

PRZEGŁĄD ELEKTROTECHNICZNY (Electrical Review), ISSN 0033-2097, R. 86 NR 9/2010
with delay to start of the cause (XOR gate) or the causes (AND gate). Duration time of the event does not depend on the cause.

In causal gates the result (output event) can occur with delay hence in this type of gates the time parameters describing minimal and maximal delay time for each cause (XOR gate) or the delay time — from the moment of coexistence of causes is given.

In causal gates the result (output event) can occur with delay hence in this type of gates the time parameters describing minimal and maximal delay time for each cause (XOR gate) or the delay time — from the moment of coexistence of causes is given.

In causal gates the result (output event) can occur with delay hence in this type of gates the time parameters describing minimal and maximal delay time for each cause (XOR gate) or the delay time — from the moment of coexistence of causes is given.

The knowledge about time relation allows us to, e.g.:
- introduce the protection to the system (satisfying the time restriction given from analysis),
- induce the time delay between events (e.g. using catalyst or inhibitory),
- modify the system components, e.g. if safety components works to slow.

In order to carry out an analysis, we need to choose a time instant as a zero time. In order to make interpretation of the results simpler, we can choose hazard start as the zero time. In this situation we can make calculation for hazard from formula (1). More information about this request is given in [8] i[15].

\[
< \alpha_{hs} = 0; \beta_{hs} = 0 > \\
< \alpha_{he} = \alpha_{he}^S; \beta_{he} = \beta_{he}^S >
\]

Parameters \(\alpha_{he}, \beta_{he} \) specify, respectively, the minimum and maximum time instant of the hazard's start and minimum and maximum time instant of the hazard's end. Therefore, in accordance with the formula (1), the hazard starts in "0" time and its duration is not less than \( \alpha_{he} \) and not greater than \( \beta_{he} \) (in particular, \( \beta_{he} \) may be equal to \( \infty \)). Unlike static parameters (with superscript \( S \)), e.g. \(\alpha_{he}, \beta_{he} \) parameters without superscript \( e \) (e.g. \(\alpha_{he}, \beta_{he} \)) are dynamic parameters. This parameters are counting in FTTD analysis reflection zero time instant and organize events in time. This dynamic parameters are evaluated during the FTTD analysis in relation to zero. Knowing these parameters it is possible to organize events in time.

2.2. The model of gates

The models of gates are given in Fig. 2. In this subsection, in order to demonstrate the idea of gates, we will show in details only two models. For other gates given in Fig. 2 we will show only formulas.

Causal AND

The causal AND gate is given in Fig.4.

\[
< \alpha_{xc}, \beta_{xc} > \\
< \alpha_{yc}, \beta_{yc} >
\]

Fig.4. Causal priority AND gate with two input events x, y and output event z

Formal definition of this gate is given by formula (2).

\[
\text{occur}(z) \Rightarrow \text{occur}(x) \land \text{occur}(y) \land \text{duration}(x \land y) \geq a_x^S \\
\land \max(\tau(x), \tau(y)) + a_x^S \leq \tau(z) \leq \max(\tau(x), \tau(y)) + \beta_x^S \\
\land \tau(z) \leq \min(\tau(xc), \tau(ye))
\]

According to the formula (2), if \( z \) had occurred and then \( x \) and \( y \) occurred together in minimally \( a_x^S \) time units. The event \( z \) had occurred not earlier that \( a_x^S \) time units and not later that \( \beta_x^S \) time units counting from start of the event which had started later.

Time analysis for FTTD in the tool are the "effect to reason", thus assuming that the dynamic parameters are known for events \( z \) we can designate dynamic parameters for \( x \) and \( y \) of (3).
Generalization AND

\[
\begin{align*}
\text{occur}(z) & \Rightarrow \text{occur}(x) \land \text{occur}(y) \land \text{overlap}(x, y) \land \\
& \max(\tau(x), \tau(y)) = \tau(z) \land \min(\tau(xe), \tau(ye)) = \tau(ze) \\
\{a_{x} = a_{x}, \beta_{y} = \beta_{y}, a_{y} = a_{y}, \beta_{x} = \beta_{x} & \} \\
a_{xy} & = a_{xy} - \beta_{y} \land \beta_{y} = \beta_{xy}, a_{yx} = a_{yx} - \beta_{x} \land \beta_{x} = \beta_{xy} \\
a_{x}^{y} & \leq \beta_{x} \\
a_{y}^{x} & \leq \beta_{y} \\
\end{align*}
\]

Generalization priority AND

\[
\begin{align*}
\text{occur}(z) & \Rightarrow \text{occur}(x) \land \text{occur}(y) \land \tau(xs) \leq \tau(ys) \\
\land \text{overlap}(x, y) \land \tau(ys) \leq \tau(ze) \land \min(\tau(xe), \tau(ye)) = \tau(ze) \\
\{a_{y} = a_{y}, \beta_{y} = \beta_{y}, a_{x} = a_{x}, \beta_{x} = \beta_{x} & \} \\
a_{xy} & = a_{xy} - \beta_{y} \land \beta_{y} = \beta_{xy}, a_{yx} = a_{yx} - \beta_{x} \land \beta_{x} = \beta_{xy} \\
a_{x}^{y} & = \beta_{x} \\
a_{y}^{x} & = \beta_{y} \\
\end{align*}
\]

Causal XOR

\[
\begin{align*}
\text{occur}(z) & \Rightarrow \text{occur}(x) \land x = z \oplus \text{occur}(y) \land y = z \\
\{a_{x} = a_{x}, \beta_{x} = \beta_{x}, a_{y} = a_{y}, \beta_{y} = \beta_{y} & \} \\
a_{xy} & = a_{xy} - \beta_{x} \land \beta_{x} = \beta_{xy}, a_{yx} = a_{yx} - \beta_{y} \land \beta_{y} = \beta_{xy} \\
\end{align*}
\]

Fig. 5. Formal definition and models for other types of FTTD gates

Causal AND

\[
\begin{align*}
\text{occur}(z) & \Rightarrow \text{occur}(x) \land \text{occur}(y) \land \tau(xs) \leq \tau(ys) \\
\land \text{duration}(x \land y) & \geq \alpha_{x}^{y} + \tau(ys) + \alpha_{y}^{x} \leq \tau(zs) \leq \tau(ys) + \beta_{y}^{x} \\
& \land \tau(ze) \leq \min(\tau(xe), \tau(ye)) \\
\{a_{y} = a_{y}, \beta_{y} = \beta_{y}, a_{x} = a_{x}, \beta_{x} = \beta_{x} & \} \\
a_{xy} & = a_{xy} - \beta_{y} \land \beta_{y} = \beta_{xy}, a_{yx} = a_{yx} - \beta_{x} \land \beta_{x} = \beta_{xy} \\
\end{align*}
\]

Inequalities \(a_{x}^{y} \leq \beta_{x}^{y}\) and \(a_{y}^{x} \leq \beta_{y}^{x}\) specify static conditions which must be satisfied for the hazard could occur. In this case, check whether the maximum duration of each of the reasons is sufficient to call effect.

Causal priority AND

The main difference between priority AND gate and gate without priority is that in a priority gate events must occur in determined order, e.g.: first event x, then event y. Therefore this gate is a special case of gate without priority. The formal definition of causal priority AND gate is given in formula (4), while the system of equations and inequalities needed for timing analysis is given in formula (5).

Confirming the analysis formulas (3) and (5), causal priority AND gate constitutes a special case (one of two) of gate without priority. Therefore, when estimating the complexity of computational algorithm taking priority gate, we can accept that its computational complexity is not greater than the algorithm without priority gate. Analysis of the complexity of computing was carried out at work [8] and in worst case complexity is class \(O(2^{2n})\).

Next gates in FTTD

Formal definitions and formulas for analysis FTTD were shown on Fig. 5. Detailed information, see [8], [15].

3. Software for analysis FTTD - INES v.3

3.1. Introduction

The steps of the FTTD analysis using the tool is given in Fig. 6.

The current version of the software permits for using the gate outlined in section 2 while constructing analysis of
FTTD. The time parameters can be specified both - numerically or as parameters (text).

1. FTTD construction (for each hazard) using Visio stencil given in [16] (result: FTTD in xml file).

2. Analysis FTTD using INES v.3 tool (results are saved in xml file).

3. Analysis results of the analysis.

Fig.6. The steps of the FTTD analysis

The analysis of fault trees with time dependencies can be performed with different kinds of gates [8],[14].

3.2. FTTD construction

The process of the FTTD construction is described e.g. in [7],[8],[15], but if we want to use INES v.3 tool then the output xml file format is. The notation of gates and events is given in Fig.7. The parser in INES v.2 tool recognizes keywords for gate or event numbers and loads parameters (parameters must be separate using ";") in order for the items on the Fig. 7b.

In this time moment we make ours FTTDs using Visio 2005 stencil (the stencil can be download from WWW site [16] or install using plug-in [17]). The part of stencil is given in Fig. 7a.

Fig.7. FTTD elements a) Visio stencil [16] b) notation of FTTD gates and events

3.3. FTTD analysis

The engine for analysis of FTTD has been made available through a web page (given in Fig. 8).

It is sufficient to select the file that contains the description of FTTD (see section 3.2). Analysis results are given as minimal cut sets (see Fig. 8) in the XML format. An MS Visio plug-in were developed too [17]. The plug-in may be used to execute the analysis as well as to draw a fault tree with time dependencies in the required XML format.

Time analysis for FTTD with many gates is shown in table 1. The current version does not yet implement mechanisms for reducing the calculations presented in [16].

Table 1. Time analysis for FTTD with many gates

<table>
<thead>
<tr>
<th>Number of gates</th>
<th>INES v.2 run time [ms]</th>
<th>FTTD source file</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>184.69</td>
<td>FT_przykl_12.vsd [16]</td>
</tr>
<tr>
<td>24</td>
<td>265.62</td>
<td>FT_przykl_24.vsd [16]</td>
</tr>
<tr>
<td>36</td>
<td>400.63</td>
<td>FT_przykl_36.vsd [16]</td>
</tr>
<tr>
<td>48</td>
<td>589.37</td>
<td>FT_przykl_48.vsd [16]</td>
</tr>
<tr>
<td>60</td>
<td>836.72</td>
<td>FT_przykl_60.vsd [16]</td>
</tr>
</tbody>
</table>

The results constitute an average time of 100 measurements and also cover disk usages (starting from load DNZC to save the results). Testing was conducted on an IBM ThinkPad T43 with Intel Pentium 1.86GHz with 2 GB RAM running under Windows XP.

3.4. Case study

In this section the analysis of FTTD given in [7] and [15] will be considered.

In first step FTTD consistent with the notation given in subsection 3.2. must be prepared (see Fig. 9). The tree must be saved as xml file.

Afterwards the analysis trough WWW site can be done (see Fig. 10).

The result of the analysis are minimal cut sets (MCS) given in the xml notation (see Fig. 8). The MS Visio plug-in offers a visualization of these XML files as well. The plug-in is still under construction, but the first version has been already given at WWW site [17].

The xml notation and graphical representation of the one MCS is given respectively in Fig. 11a and 11b.

Fig.9. FTTD for gas burner system (given in [7]) – Visio 2005 sheet

After the analysis trough WWW site can be done.
4. Conclusions

Although the fault trees analysis is one of the often used methods of safety analysis it does not allow us to perform the analysis of time dependencies. FTTD are used for this type of analysis. Time dependencies can be given numerically or parametrically. With the parametrically given time dependencies the analysis of FTTD let us to fix the limitations for parameters, what is important during designing, implementing and configuring of systems.

The tool for FTTD analysis has been presented in this paper. The notation has been proposed. The library, as a pattern for Visio application, that allows us to draw the FTTD and to save it in accordance to proposed notation has been formulated as well.

The tests of the efficiency of software for FTTD up to 60 gates has been performed. The results are given in chapter 3.