Tool for analysis of the fault tree with time dependencies

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 tolerance (if hazard can be tolerated), time from occurrence of given events to hazard (for example between failure of the cooling pomp 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, trmin – minimal time of reaction, tzmin, tzmaz – 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.

<αS, βS> Event name

Fig.1. Event notation

Time parameters <αS, βS> 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...