Fault Trees and Belief Networks in Risk Modelling: A Comparative Analysis

Oleg Uzhga-Rebrov[1], Galina Kuleshova[2]
Rezekne Academy of Technologies[1], Riga Technical University[2]

***Abstract.** Nowadays, an ever-growing complexity of technical systems can be observed worldwide, problems of rational use of nature resources and diminution in negative impact on the environment are not completely settled yet, and international competition in different areas is strengthening. All the above tendencies cause an increase of different risks: technical, ecological, political, military and financial. Due to their nature, most of the risks are caused by a set of factors with commonly unknown relationships. Therefore, the need to use risk modelling methods that enable visual representation of the sets of cause-risk relationships becomes evident. This paper briefly examines two widely used techniques of modelling risky situations: fault trees and belief networks, and provides their comparative analysis.*

***Keywords:** fault tree, logic OR gate, logic AND gate, belief network, fault tree transformation, hybrid risk assessment.*

I. INTRODUCTION

Humans have always appreciated having the possibility of representing, evaluating and analysing risky situations. Probability theory, for example, has appeared to meet the needs of evaluating players chances in risky situations. Nowadays, probability theory is a developed field of science that is widely and successfully used in diverse areas of human activity including risk assessment and analysis.

Any risk can be assessed using two components: probability of occurrence of a risky situation and the losses it might cause. When analysing this kind of situations, one has to account for many interrelated random factors (events) that might result in the occurrence of the top event related to unfavourable consequences.

To clearly represent numerous risk factors and correlations among them, visual approaches to modelling risky situations are necessary. In this paper, two widely used techniques of this kind are considered: fault trees and belief networks.

II. FAULT TREES

The idea of fault trees was first proposed by the Bell Telephone Company for the purposes of US Air Force. In [1], the following description of the technique is provided: "Fault trees are a graphic "model" of the pathways in a system that might lead to a predictable undesirable event related to losses. Numerical probabilities of occurrence can be included and propagated through the model so as to evaluate the probability of the predictable undesirable event".

Risk analysis using fault trees comprises [1]:

- graphical representation of chains of events/conditions leading to the unfavourable event;
- identification of potential fault contributors that are critical;
- better understanding of system characteristics;
- qualitative/quantitative understanding of the probability of the unfavourable event selected for analysis;
- identification of resources aimed at failure prevention;
- manual for redeploying resources to optimise control of risk;
- documentation of the results of analysis.

Let us consider some common principles of fault tree construction using an example. Fig. 1 shows a sample fault tree.

ISSN 1691-5402

http://dx.doi.org/ 10.17770/etr2017vol2.2514

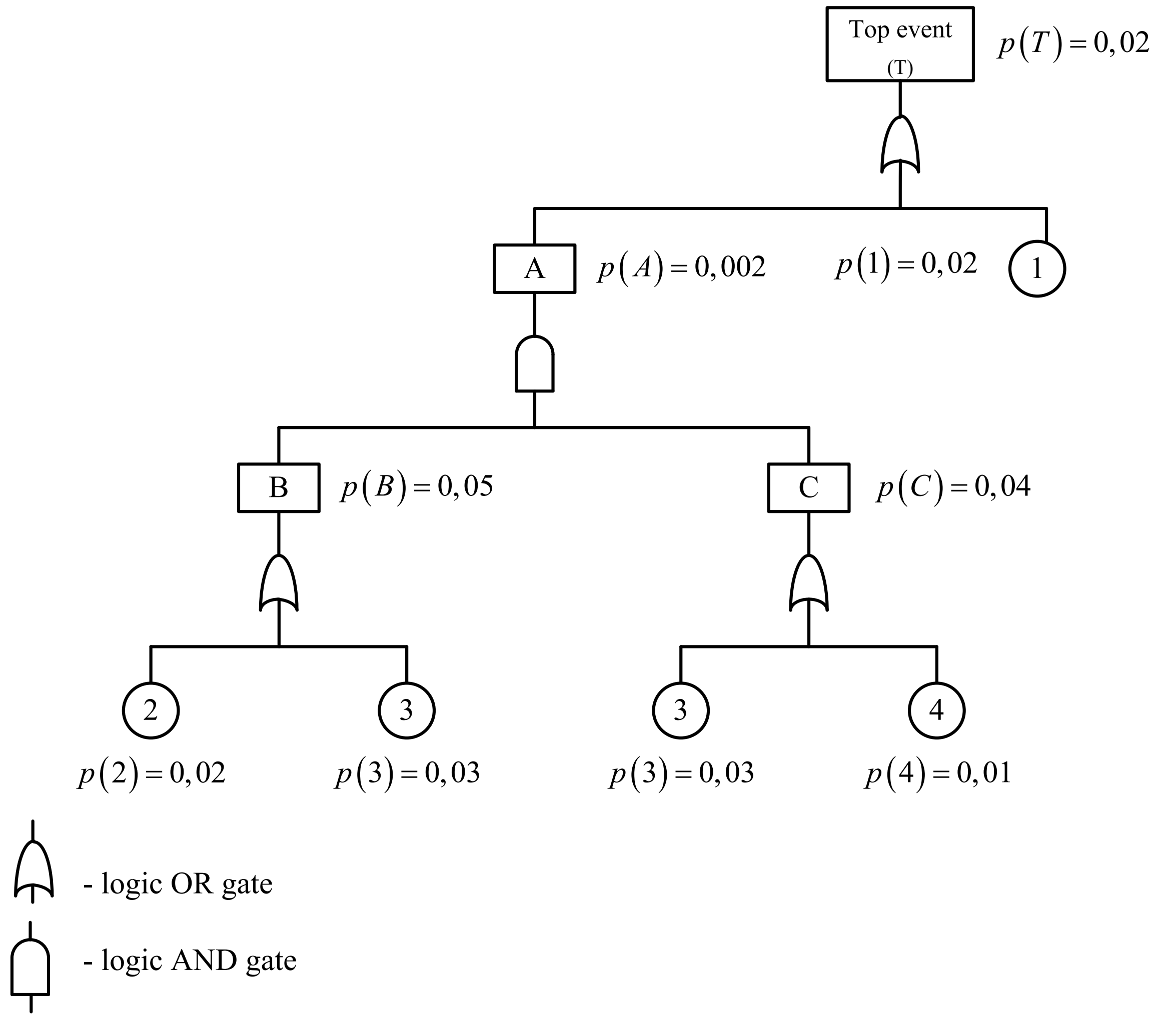


Fig. 1. Sample fault tree

In Fig. 1, nodes 1, 2, 3 and 4 represent basic events – failures of real elements of the system. Logic OR and AND gates between the nodes of events represent conditions of event occurrence in the intermediate nodes at the outputs of those logic gates. For example, an event in the intermediate node B will occur if basic event 2 *or* basic event 3 occurs; an event in the intermediate node A will occur if an event in the intermediate node B *and* in the intermediate node C occurs. To construct fault trees, other logic gates can also be used, but gates OR and AND are basic.

If an intermediate node A has got n predecessors connected with by logic gate AND, then the probability of event occurrence in that node is calculated as follows:

$$p(A)=\prod_{i=1}^{n} p(i) \tag{1}$$

where $p(i)$ - probability of event occurrence in the i-th predecessor node.

In its turn, if some intermediate node A has got n predecessors connected with it by logic gate OR, then the probability of event occurrence in that node is calculated as

$$p(A)=\prod_{i=1}^{n}\bigl(1-\bigl(1-p(i)\bigr)\bigr) \tag{2}$$

where $p(i)$ - probability of event occurrence in the i-th predecessor node

The fault tree shown in Fig. 1 depicts initial probabilities of basic events and the calculated values of the intermediate events and of the top event T.

III. BELIEF NETWORKS

Belief networks are a singly-connected graph whose each node represents the complete group of random events. Quite frequently, alternative names for the belief networks are also used, e.g. bayesian networks, bayesian belief networks, causal networks etc. A fragment of a sample belief network is given in Fig. 2.

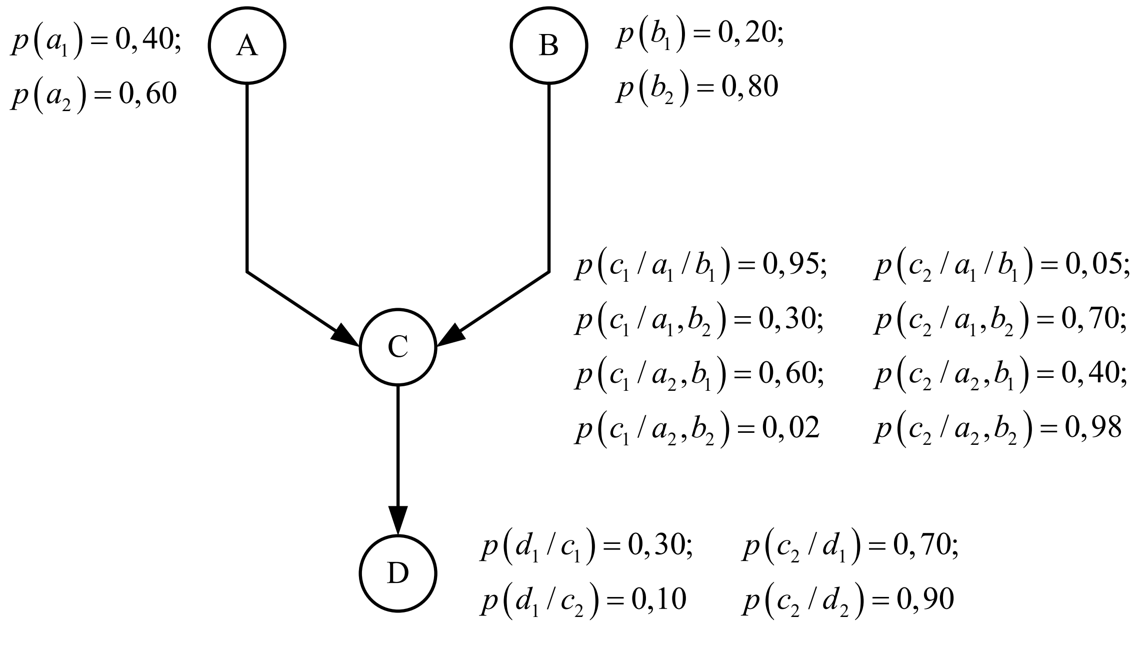

$p(a_1) = 0,40;$
$p(a_2) = 0,60$
A
B
$p(b_1) = 0,20;$
$p(b_2) = 0,80$
$p(c_1 / a_1 / b_1) = 0,95;$
$p(c_2 / a_1 / b_1) = 0,05;$
$p(c_1 / a_1, b_2) = 0,30;$
$p(c_2 / a_1, b_2) = 0,70;$
$p(c_1 / a_2, b_1) = 0,60;$
$p(c_2 / a_2, b_1) = 0,40;$
$p(c_1 / a_2, b_2) = 0,02$
$p(c_2 / a_2, b_2) = 0,98$
C
D
$p(d_1 / c_1) = 0,30;$
$p(c_2 / d_1) = 0,70;$
$p(d_1 / c_2) = 0,10$
$p(c_2 / d_2) = 0,90$

Fig. 2. A fragment of a sample belief network

Here each node represents two random events. Nodes A and B do not have any predecessors. In Fig. 2, these nodes are supplemented with matrices of unconditional probabilities of occurrence of the events connected with them.

Node C has two direct predecessors, namely, nodes A and B. In Fig. 2 that node is supplemented with matrices of unconditional probabilities of occurrence of events c_1 and c_2 for all possible combinations of events in nodes A and B.

Node D has a single direct predecessor, node C. In Fig. 2 the node is supplemented with matrices of unconditional probabilities of occurrence of events d_1 and d_2 provided that events c_1 and c_2 have occurred.

The task of probabilistic inference in belief network is formulated as determination of occurrence probabilities for the events that are of interest to us using all the information accumulated in the network. For example, for the fragment of belief network in Fig. 2, the task can be to calculate the prior probabilities of occurrence of events d_1 and d_2 based on the information about event occurrence probabilities in nodes A, B and C. Provided that an event has occurred in some node of the network, one can calculate the posterior probabilities of events in all nodes of the network.

A great deal of both accurate and approximate algorithms for probabilistic inference in belief networks have been proposed. The most common algorithm is described in [2]. More details about the algorithm can be found in [3] - [5]. The essence of the method is as follows. Special λ- and π-evaluations are propagated through the nodes of the network. After these nodes have received evaluations from other nodes, the prior values of event probabilities of the nodes are calculated in sequence. If an event has occurred in a certain node of the network, the initial evaluations are recalculated. Special λ - and π - evaluations are then forwarded in sequence to the nodes of the network and the posterior probabilities of events in all nodes of the network are calculated in sequence.

Belief networks are widely used to model risks in complex multi-aspect situations. Some examples of their use are provided in [6]- [11].

IV. POSSIBILITIES OF TRANSFORMING FAULT TREES INTO BELIEF NETWORKS

Fault tree technique has several important points:

(a) Events in all nodes of the tree are binary events;

(b) The events are statistically independent of each other;

(c) The trees represent logic relationships between the events.

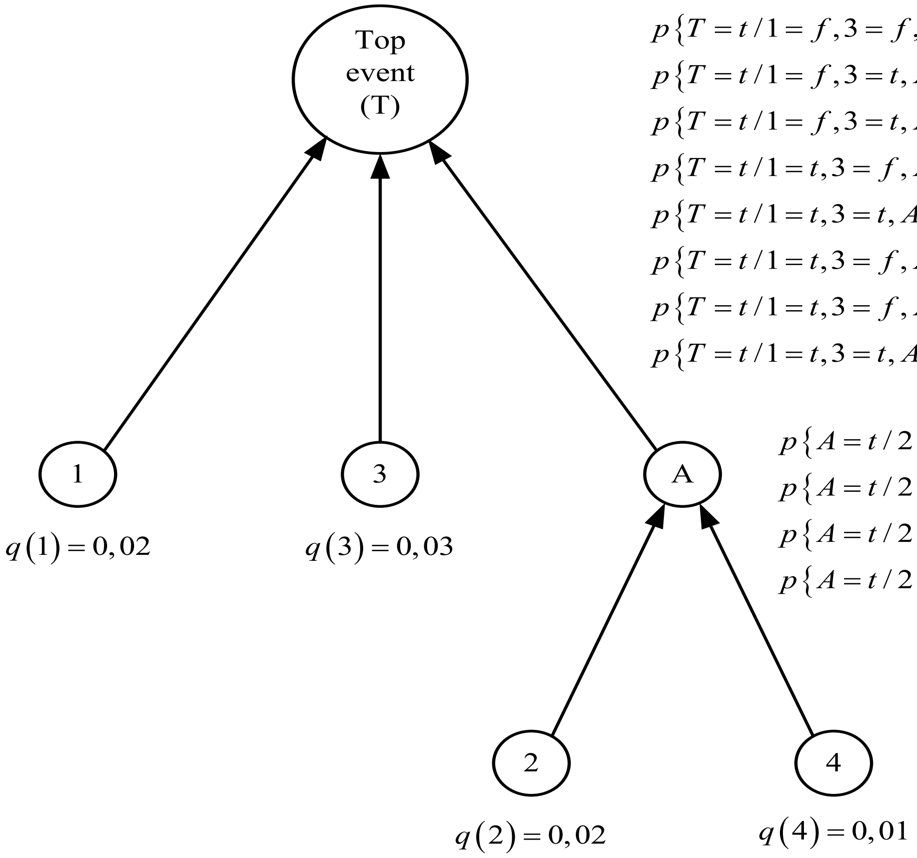
A characteristic feature of belief network is that the probabilities of event occurrence in network nodes are either unconditional or stipulated by the events in the predecessor nodes of relevant nodes.

From that simple analysis it directly follows that different aspects of the knowledge necessary for successful risk modelling and analysis are encoded by means of fault trees and belief networks. So it seems attractive to combine the advantages of both techniques. One possible way to realise that idea is to transform fault trees into equivalent belief networks and then, using the obtained network representation, to apply the procedures that are in principle impossible for fault trees.

This paper employs the algorithm for fault trees transformation into belief networks presented in [12]. Simplistically, the algorithm consists in the execution of these procedures:

1. For each terminate node in the fault tree, a root node is created in the belief network.
2. For the output of every logic gate in the fault tree, a corresponding node in the belief network is created.
3. For each node in the belief network corresponding to the logic gate in the fault tree, a table of conditional probabilities is made where the probabilities characterize the states in successor node depending on the states in predecessor nodes.

Fig. 3 shows a belief network obtained through the transformation of the fault tree depicted in Fig. 1. The nodes of that network corresponding to the outputs of logic gates in the fault tree, are supplemented with matrices of conditional probabilities. However, these matrices are not equivalent to the matrices of conditional probabilities in the standard belief network. In those new matrices there are presented probabilities of states t (failures of the respective elements) depending on the states of elements mapped by predecessor nodes. These probabilities can only have two values: 0 and 1. To explicitly show the difference of these conditional probabilities from common conditional probabilities, we denote the first probabilities by symbol q.



$$
\begin{aligned}
&p\{T=t/1=f,3=f,A=f\}=0;\\
&p\{T=t/1=f,3=f,A=t\}=1;\\
&p\{T=t/1=f,3=t,A=f\}=1;\\
&p\{T=t/1=f,3=t,A=t\}=1;\\
&p\{T=t/1=t,3=f,A=f\}=1;\\
&p\{T=t/1=t,3=t,A=f\}=1;\\
&p\{T=t/1=t,3=f,A=t\}=1;\\
&p\{T=t/1=t,3=f,A=t\}=1;\\
&p\{T=t/1=t,3=t,A=t\}=1.
\end{aligned}
$$

$$
\begin{aligned}
&p\{A=t/2=f,4=f\}=0;\\
&p\{A=t/2=t,4=f\}=0;\\
&p\{A=t/2=f,4=t\}=0;\\
&p\{A=t/2=t,4=t\}=1.
\end{aligned}
$$

Fig.3. Belief network obtained through the transformation of the fault tree shown in Fig.1

Unfortunately, standard algorithms of probability distribution cannot be applied in the belief networks obtained through the transformation of the corresponding fault trees. For that purpose, algorithms for probability distribution in fault trees can be used taking into account the specifics of the transformed logic relations.

At a glance, it seems that fault tree transformation into equivalent belief network does not ensure any advantages. That statement can only be true for the transformation of standard fault trees. Some situations of that kind are discussed in [12]. Belief networks enable modelling the situations that cannot in principle be modelled by fault trees. Suppose that an intermediate node A in the belief network is connected with its predecessors by a logic AND gate (Fig. 4). Let us also assume that the element corresponding to that node can be damaged due to some exterior reason (not known a priori) when other elements represented by nodes 1 and 2 are functioning properly. A situation like that cannot in principle be modelled with the help of the fault tree; though it can be fairly simply modelled by means of the belief network. In Fig. 4, specifically, in the matrix of conditional probabilities of node A, instead of zero values of probabilities corresponding to the proper functioning of elements in nodes 1 and 2, there is written the value of probability q of element A damage due to some implicit external reason.

Another example is the so-called noisy-OR gate. Let us have a look at Fig. 5. Let us assume that elements 1 and 2 can be damaged as a result of improper actions of the service staff. Here, the nature of the damage is such that the corresponding element continues keeping some extent of work capacity while element in node A continues to work properly.

Such chances of maintaining work capacity of element A at the time when work capacity of element 1 or element 2 is partly damaged, can sufficiently easily be modelled with the help of a belief network: in the matrix of conditional probabilities of node A there are written corresponding values of probabilities q_1 and q_2 instead of 1.

Different points of fault trees transformation into belief networks are also considered in [13]-[16].

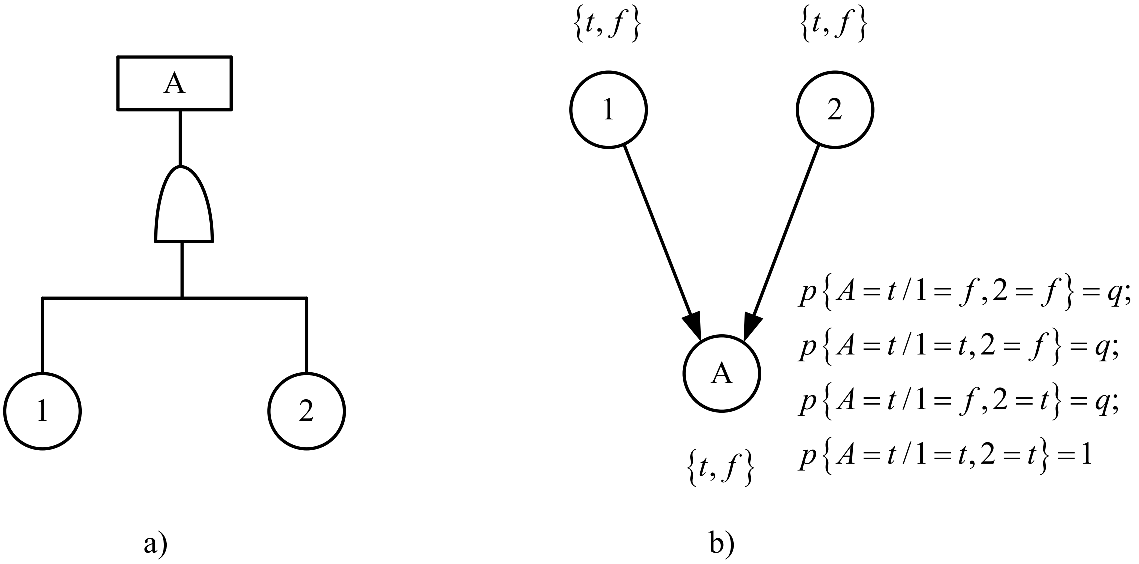


Fig. 4. Graphical representation of the phenomenon of common reason of failure with the help of a fragment of belief network

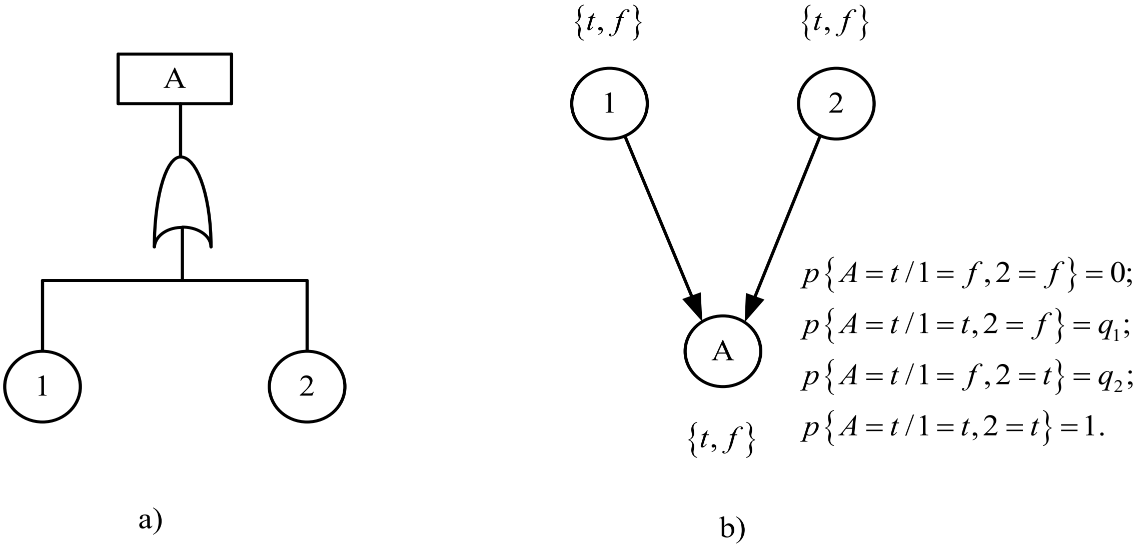


Fig. 5. Graphical representation of the noisy-OR gate by means of a fragment of belief network

Good results have been shown by joint modelling of risks with the help of belief networks and fault trees. In [8], [9] a hybrid approach to modelling risks in socio-technical systems is proposed. Socio-technical system is a system that comprises a technical part (say, manufacturing) and management and organisational parts. Besides that, the system has to take into account both the impact of the surrounding environment on the system and the impact of the system on the environment. The authors propose to model all possible factors of risk and their correlations at the management and organisational levels using belief networks and to model risk factors and their correlations in the technical part of the system by means of fault trees. This kind of modelling enables successful incorporation of the advantages of both approaches.

V.CONCLUSIONS

Fault trees and belief networks are widely used to model and analyse different kind of risks. Fault trees enable a visual representation of all events leading to the occurrence of an unfavourable basic event and of logic connections between them. They however fail in modelling non-standard risky situations.

Belief networks are the most appropriate tool for modelling qualitative relations among the factors (events). The edges in the graph of belief network explicitly represent probabilistic relationships among the events. Provided that a certain event (events) has occurred in the network, probabilities of other events can be recalculated using a formal algorithm.

Belief networks perfectly suit modelling risks in complicated situations [6], [7] and in complex socio-technical systems [8], [9]. Good results have also been produced by the joint use of fault trees and belief networks.

Both fault trees and belief networks require a large amount of initial information. That does not cause any problem if sufficient statistical data are available. However, when expert evaluation of relevant probabilities is performed, it is more preferable to employ fuzzy probabilistic evaluations and use fuzzy versions of the algorithms for probability propagation through fault trees and belief networks.

REFERENCES

[1] P.L. Clemen, *Fault tree analysis*, 1993. [Online]. Available:http://rischioatmosfereesplosive.studiomarigo.it/profiles/marugo2/images/file 1736612536. pdf Clemens. [Accessed: Oct.27, 2016].

[2] J. Pearl, *Probabilistic reasoning in intelligent systems*. New York: Wiley, 1989.

[3] A.N. Borisov, O.I. Uzhga-Rebrov and K.I.Savchenko, *Verojatnostnij vivod v intellektualnih sistemah*, Riga, 2002. (In Russian)

[4] R.E. Neapolitan, *Probabilistic reasoning in expert systems*. Los Altos, CA: Morgan Kaufman, 1999.

[5] O.I. Uzhga-Rebrov, *Upravlenije neopredelennostjami, Chastj 1. Sovremennije koncepcii i prilozhenija teorii verojatnostej*, Rezekne: RA Publishers, 2004. (In Russian)

[6] Y.Y. Bayrakarli, (2006). Application of Bayesian probabilistic networks for liquefaction of soil, *6th Int. Phd Symposium in civil Engineering,* Zurich, August 23 – 26, 2006.

[7] Y.Y. Bayrakarly, J.W. Baner and M.H. Faber. "Uncertainty treatment in earthquake modeling using Bayesian probabilistic networks", Georisk, Vol. 5, No. 1, pp. 45 – 48, 2011.

[8] A. Léger, C. Duval, Ph. Weber, E. Levrat, and R. Farret. "Bayesian network modelling the risk analysis of complex socio technical systems", *Workshop on advanced Control and Diagnosis, ACD'2006*, Nancy, France, 2006.

[9] A. Léger, R. Farret, C. Duval, E. Levrat, P. Weber and B. Iung, A safety barriers-based approach for the risk analysis of socio-technical systems. *Proceedings of the 17th World Congress*, The International Federation of Automatic Control, Seoul, Korea, pp.6938 – 6943, 2008.

[10] G. Medina-Oliva, Ph. Weber, Ch. Simon and B. Iung, Bayesian networks applications on dependability, risk analysis and maintenance. *The 2nd IFN Workshop on Dependable Control of Discrete Systems, DCDS'09*, Bari, Italy, 2009.

[11] L. Portinale and A. Bobbio, "Bayesian networks for dependability analysis: an application to the digital control reliability", *Proceedings of the 15th Conference on Uncertainty in Artificial Intelligence, UAT-99*, pp. 551 – 558, 1999.

[12] A. Bobbio, L. Portinale, M. Minishino and E. Ciancamerla, "Improving the analysis of dependable systems by mapping fault trees into Bayesian networks", Reliability Engineering and System Safety, 71, pp. 249 – 260, 2001.

[13] Ch. Cornalla and P. Giudici, "Statistical models for operational risk management", Physica A 338, pp. 166 – 172, 2004.

[14] M. Hamada, H. F. Martz, C.S. Reese, T. Graves, V. Johnson and A.G. Wilson, "A fully Bayesian approach for combining multilevel failure information in fault tree quantification and optimal follow-on recourse allocation", Reliability Engineering and System Safety, 86, pp. 297 – 305, 2004.

[15] Ch.-G. Jong and S.-S. Leu, "Bayesian-network-based hydro-power fault diagnosis system-development by fault tree transformation", Journal of Marine Science and Technology, Vol. 21, No. 4, pp. 367 – 379, 2013.

[16] N. Khakzad, F. Khan and P. Amyotte, "Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches", Reliability Engineering and System Safety, 96, pp. 925 – 932, 2011.