RESEARCH PAPERS
FACULTY OF MATERIALS SCIENCE AND TECHNOLOGY IN TRNAVA
SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA

2013 Special Number

FAULT TREE ANALYSIS OPTIMIZED BY GENETIC ALGORITHMS

Adriána LIBOŠVÁROVÁ, Peter SCHREIBER

ABSTRACT

This paper deals with possibilities of using genetic algorithms in design of costs optimization, which are needed to reach given reliability of technical system, respectively system reliability optimization by given amount of investment costs. In following chapters, there is a described design of new method, which will be later implemented in application and verified on an example.

Causal relationships between system failures and elements faults can be detected by analytic approach, when at first the undesired system fault is identified and its reasons are progressively detected. The reliability of system and its elements is analyzed using method FTA (fault tree analysis) and system is represented by fault trees. In order to optimize costs, respectively reliability, the genetic algorithms are used.

KEY WORDS

ault tree analysis, fault tree, event, gate, genetic algorithms, population, objective function, selection, crossover, mutation

INTRODUCTION

Systems have become an inseparable part of modern life; they consist of functionally bound and dependent subsystems, which serve for different purposes. It is necessary to monitor and to analyze systems even after their implementation into service. Some systems can be too expansive, what increases a complexity in the system analysis. One of the most important monitored factors is safety, i.e. reliability of the systems. Risk analysis and safety increase is applied already in the system development phase (Janíček 2009). Thanks to, the risks of possible accidents and hazards can be eliminated or reduced.

With the developing technologies and systems implementation also appears the risk of danger. In some cases, the risk of accidents can be eliminated by appropriate measures, and it allows preventing at least some types of failure. But it is not always possible in the real world. It is necessary to regard so called supporting risks already before the system implementation and to strive to mitigate them. In these cases, the compromises are made between acceptation of the system benefits and rejection because of real accident risk, which the given system

Adriana Libošvárová, Peter Schreiber - Institute of Applied Informatics, Automation and Mathematics, Faculty of Materials Science and Technology, Slovak University of Technology in Bratislava, Paulínska 16, 917 24 Trnava, Slovakia, adriana.libosvarova@stuba.sk; peter.schreiber@stuba.sk

presents. The essence of security and key to effective risk management is to properly recognize and analyze hazards. Just their correct identification helps in the design and construction of the systems to be safe for the people and the environment. And for this purpose the various techniques and tools are developed and constantly improving. (Ericson 2005, Janíček 2009)

FAULT TREE ANALYSIS

Fault tree analysis is a technique, which serves to analyze probability of technical system failure, potential risks detection and design of suitable preventive measures, which should increase system reliability. This method is regarded as deductive, because it is based on logical decomposition of certain dangerous undesired event subsequently through partial to elemental events. The undesired events can be understood as failures. They significantly influence functionality, an economics, a safety or other required properties of system. (Vincoli 2006)

The method FTA is based on principle of strict structuring. It is a graphical expression of individual fault states, which can occur in given system and cause its failure by specific combinations. The model is characterized by tree structure and its creation is based on rules of Boolean algebra, logic and probability theory. The created diagram is called fault tree (FT) and it is a basic element of this analysis technique. (Ericson 2005)

The fault tree is a diagram, which illustrates graphically and logically different ways, how a system can fail. The certain combinations of elements faults result in a creation of primary undesired event. Under the term "undesired event", it is considered each event, which is for safety inappropriate and undesired, respectively it characterizes danger, hazard or another fault state (Ericson 2005). Fault tree describes how the events follow each other and how they are mutually dependent. The events hierarchy and logical links between events are created by using so called logical gates, especially "AND" and "OR" gates. Together with fault events, they represent relationships "cause-effect". Subsequently the constructed fault tree can be qualitatively or quantitative evaluated. The choice of suitable type of evaluation depends on various factors such as established requirements. (Dunn 2002)

FTA is very extended and favorite analysis technique in practice. It can be used not only preventative to examine the system design, but also to investigate occurred problems. This method is applied on complex technical systems, whose current state is dependent on earlier time and outside influences. FTA is useful in all industry areas, which deal with safety and reliability question, for example in nuclear power, aviation, cosmonautics, etc. (Ericson 2005)

In practice, the question of finance is also solved in addition to the level of reliability security. The system reliability is set and influenced by the amount of invested money. The investments are needful to build security, to ensure service, but also for any necessary repairs due to failures. Since finance amount is limited mater, the highest possible system safety should be ensured with a certain amount of investment, alternatively the given system reliability should be achieved at minimum costs. As optimization mechanism of analysis technique FTA, genetic algorithms can be used.

PROCEDURE OF PROCESS

The first step involves constructing fault tree of a selected part of the technical system, which is analyzed through FTA. The tree has m leaf nodes u_1 - u_m, each of them represents a primary event or subsystem. Each node i has an associated reliability s_i and corresponding amount of investment n_i which is needed to achieve it. The achieved reliability is functionally dependent on maintenance costs. This dependence is generally expressed as function $s_i = g_i (n_i)$ and is shown in figure 1. These relevant data are known in advance, so the constructed fault tree can be quantitatively evaluated from primary events up to the top undesired event.

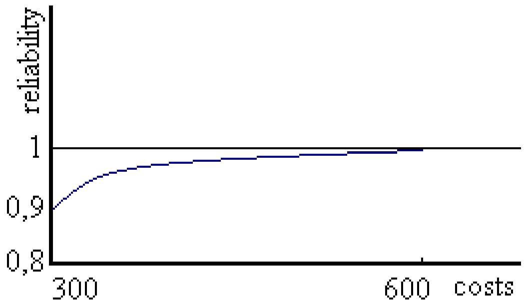

Fig. 1 *Reliability dependence on costs*

Using Boolean algebra relations allows calculating reliability of given tree – system part, generally $S = f_1(s_1, s_2, ..., s_m)$. In given reliability, system maintenance costs are calculated as sum of all costs of subsystems maintenance $N = f_2(n_1, n_2, ..., n_m) = \Sigma n_i$.

After correct construction and evaluation of the complete fault tree, genetic algorithms are appropriately applied to optimize. Optimization can be done in terms of:

- achieving certain system reliability with minimal financial investment,
- achieving the maximum possible system reliability with given amount of investment.

FAULT TREE REPRESENTATION IN ACCORDANCE WITH GA

Data on system elements reliability and the associated costs are known through calculation, historical experience or are available from the supplier (Janíček 2009). The important information consists in their representation. These data tend to be written to real numbers format.

In terms of genetic algorithms methodology, it is possible to work with real numbers. The following figure illustrates the example of fault tree with registered reliabilities of primary fault events.

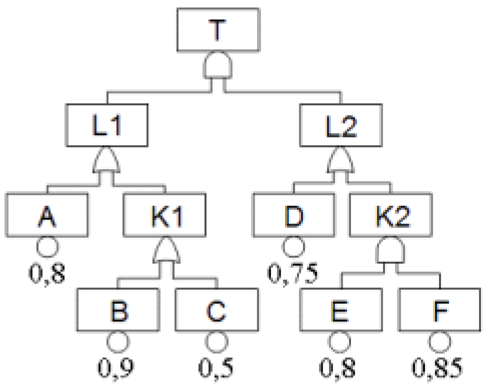

Figure 2 *Example of FT representation and reliability evaluation*

The value that belongs to one node of the tree corresponds to one gene and all values together represent one individual (figure 3).

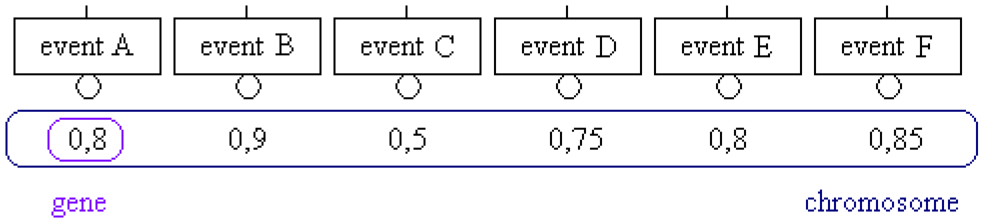

Fig. 3 *Example of chromosome and its genes in fault tree*

DESIGN OF GENETIC ALGORITHM

On the basis of fault tree analysis and its quantitative evaluation, the chromosome is available. Then the whole population is created by modifying alleles of given chromosome to the other values of the appropriate domain. Each population will consist of 100 individuals.

In the next step objective function is chosen. Its form depends on the established purpose of the genetic algorithm, i.e.:

1. with limited financial sources to achieve maximum reliability of the technical system, i.e.:
   - to maximize reliability, i.e. OF_1: reliability → maximum,
   - the genes are represented by values of financial investments of individual nodes N_i.
2. to achieve the given system reliability with minimum costs, i.e.:
   - to minimize costs, i.e. OF_2: costs → minimum,
   - the genes are represented by reliabilities of individual nodes S_i.

Then by using the fitness function, all individuals are rated for suitability and success (Hynek 2008). By each created solution, of the top undesired event occurrence probability (or system reliability) and also invested costs in the concrete measures are simultaneously calculated. By calculating costs, it is necessary to control, if maximum possible amount of investment is not exceeded. For example, if significantly increased system reliability is achieved at specific combination of costs of individual nodes, but investment amount needed in order preventive measures is also exceeded. In this case, the solution is unsuitable and its fitness is automatically equal to zero.

Selection, respectively choice of individuals into reproductive process is done through the roulette. In this selection mechanism, the individuals with a higher valuation have higher probability of selecting, but also for weak individuals, there is a little chance of becoming parents and providing their genetic material. (Hynek 2008)

The next step is the applying genetic operators on the appropriate solutions - crossover and mutation. By multiple crossover, two chromosomes are divided at random, but the same position and behind each odd division point will exchange parts of their chains (figure 4). (Kvasnička 2000)

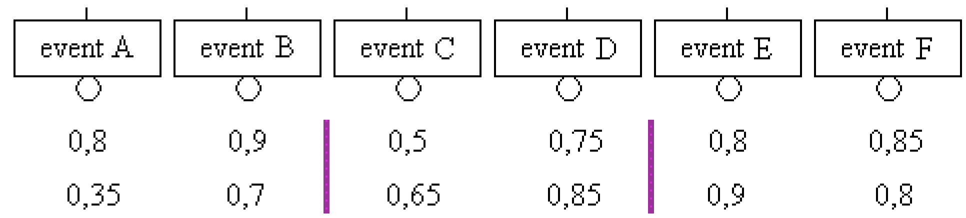

Fig. 4 *Crossover of parent chromosomes*

After crossover, a mutation is applied on new offspring. Through this operator, the gene value is changed to another random, but allowed value of the domain, which belongs to the specific primary event. (Kvasnička 2000)

The last step is to form a new population, to which the genetic algorithm process will be repeated again. In this case, it is appropriate to use elitism, through which 6 of the best valued individuals from the previous generation enter in the new population, along with 94 new individuals generated by the described crossing and mutation process.

If for the last *k* algorithm iterations only slight or no change occurs in the potential solutions in comparison with previously the most successful solution, the cycle would not be repeated (Hynek 2008). Fulfillment of this designed terminating condition terminates the whole process of the genetic algorithm.

CONCLUSION

This paper provides an interesting aspect of using genetic algorithms in conjunction with FTA in practice in commercial areas (e.g. reduction of serious accidents occurrence, compliance with safety standards, etc.). There is a described design of methodology how to optimize maintenance of system represented by fault tree.

The genetic algorithm design by itself consists of the compilation of objective function, the choice of selection mechanism, the use of genetic operators and not least of the determination of terminating condition. In the course of individual cycles of iteration genetic algorithm process, there is an attempt for every solution to achieve its optimum depending on the chosen objective function. The best and satisfactory solutions are subjected to reproductive process - crossover and mutation. By the correct design it is possible to reach that every additional population of solutions contains better or at least as good solutions as the previous generation. The proposed approach will be processed in the usable application, through which its functionality will be tested on a practical example.

ACKNOWLEDGMENT

Európska únia
Európsky fond regionálneho rozvoja

This publication is the result of implementation of the project: "Increase of Power Safety of the Slovak Republic"(ITMS: 26220220077) supported by the Research & Development Operational Programme funded by the ERDF.

Operačný program VÝSKUM a VÝVOJ

REFERENCES

1. AVEN, Terje. 2008. *Risk Analysis*. Chichester: John Wiley & Sons Ltd. ISBN 978-0-470-51736-9
2. DUNN, William R. 2002. Fault Tree Analysis. In: *Practical Design of Safety-Critical Computer Systems*. Solvang: Reliability Press, s. 166 – 174. ISBN 0-9717527-0-2
3. ERICSON II., Clifton A. 2005. *Hazard Analysis Techniques for System Safety*. Hoboken: John Wiley & Sons, Inc. ISBN 978-0-471-72019-5
4. HAUPT, R. L., HAUPT, S. E. 1998. *Practical Genetic Algorithms*. New York: John Wiley & Sons, Inc. ISBN 0-471-18873-5
5. HYNEK, Josef. 2008. *Genetické algoritmy a genetické programování*. Praha: Grada Publishing, s.r.o. ISBN 978-80-247-2695-3

6. JANÍČEK, F., KOVÁCS, Z. 2009. *Spoľahlivosť v elektroenergetike*. Bratislava: Renesans, s.r.o. ISBN 978-80-89402-12-0
7. JANKOVIĆ, Mladen. Genetic Algorithm Library. 2012 [cit. 2013-01-21]. Dostupné na internete: http://www.codeproject.com/Articles/26203/Genetic-Algorithm-Library
8. KVASNIČKA, V., POSPÍCHAL, J., TIŇO, P. 2000. Genetický algoritmus (GA). In: *Evolučné algoritmy*. Bratislava: STU, s. 31 – 57. ISBN 80-227-1377-5
9. SEKAJ, Ivan. 2004. Riešenie problémov pomocou genetických algoritmov. *Automatizace*, **47**(9), 552 – 555.
10. SCHREIBER, P., VAŽAN, P., TANUŠKA, P. Production optimization by using genetic algorithms and simulation model of production system. In: *Annals of DAAAM and Proceedings of DAAAM Symposium*. - 22-25th October 2008, Trnava, Slovakia, ISSN 1726-9679, ISBN 978-3-901509-68-1, pp. 1229-1230
11. ŠTRBO, M., TANUŠKA, P., GESE, A. The proposal of preliminary hazard analysis for safety-critical control systems. In: *INFOKOM-5*. - ISSN 2219-293X. - Infokommunikacionnyje technologii v nauke, proizvodstve i obrazovanii : 5. meždunarodnaja naučno-techničeskaja konferencija, Kislovodsk, Stavropoľ, 2 - 6 maja 2012. - Stavropoľ : Severo-Kavkazskij gumanitarno-techničeskij insitut, 2012, s. 162-167, časť 1
12. VINCOLI, Jeffrey W. 2006. Fault Tree Analysis. In: *Basic Guide to System Safety*. Hoboken: John Wiley & Sons, Inc., s. 139 – 151. ISBN 978-0-471-72241-0