Application of logic-probability approach for survivability analysis of security system

Sergey Rodin

Information Security Department,
Lviv Polytechnic National University, UKRAINE, Lviv,
S. Bandery street 12, E-mail: serg0768@gmail.com

Abstract – The article is dedicated to analysys of the survivability of security systems using logical-probability approach. In this paper is described the analysis application and its purpose. The methods and their analogues are noted. The analysis procedure and problems of method were described. The advantages and disadvantages were analyzed.

Key words – logic-probability, approach, survivability, analysis, security system.

I. Introduction

The survivability analysis of modern structurally complicated technical systems and objects is carried out at all stages of the system's life cycle. At the same time the following goals were set:

- justification of the quantitative requirements for survivability system or its components ;
- comparative analysis of survivability options of scheme-structural constructing of the system and justification of choice of the most rational option, including the value criteria;
- definition of achieved (expected) level of survivability system and / or its components, including the calculation indicators of survivability and parameters of the distribution characteristics of survivability system components as input data for the calculation survivability of the whole system;
- justification and checking the effectiveness of the proposed (implemented) steps to rework flaws or vulnerabilities, which are aimed at improvement of survivability;
- solving various optimization tasks;
- check of conformity expected (achieved) level of survivability of the system with the established requirements (control survivability), when direct experimental confirmation their level of survivability impossible or technically and economically inexpedient. At the design stage calculation survivability is conducted to predicting survivability of the designed system. At the stage of testing and exploitation the calculation is carried out for assess the quantitative indicators survivability of designed system survivability.

II. The method i analogues

The level of security should meet the importance of the object, which is expressed through his category - this is the basic principle of designing effective security system. The proposed approach allows us to quantify assess of the security level of object by analyzing the survivability of security system.

It is based on two concepts: degree of risk and the level of security. Under analyzing survivability of security system we will mean the risk assessment process and the security level. The analysis is carried out using the logical-probability models. The structure of the system is described by using of the boolean algebra, and quantitative risk assessment is carried out using probability theory.

Among analogs can be noted [1]:

- fault tree analysis (FTA);
- event tree analysis (ETA);
- hazards and operability analysis (HAZOR);
- checklist analysis and others.

These methods (mostly of foreign origin) are used to analyze the causes of failures of technical systems and forecasting of accidents. Lack of adequate mathematical apparatus do not allow the transformation of these models to a form suitable for analysis, so the results are usually interpreted at the qualitative level. In the writings of scientists, especially Dr.Tech.Sci I.A. Rjabinin [2], the founder of scientific school of logical-probability methods of analysis, was laid methodological base that allows to obtain quantitative risk assessment as degree of risk.

III. The mathematical apparatus

The theoretical basis of logic-probability methods are operations over the functions of Boolean algebra. Here the required minimum.

Boolean function puts logical arguments in accordance of logical value. It is a set of logical operations. The basic logical operations are: disjunction ($\vee$), conjunction ($\wedge$) and negation ('). De Morgan's law (law of inversions) allows us to represent the conjunction through disjunction of inverse values and vice versa: $A \wedge B = (A' \vee B')'$, $A \vee B = (A' \wedge B')'$.

Disjunction of elementary conjunction is called a disjunctive normal form (DNF).

There are several forms of DNF. If the ranks of elementary conjunctions is the same, such DNF is called perfect DNF (PDNF). Elementary conjunction are orthogonal if their multipli is zero. If all members of DNF pairwise orthogonal, then it is a orthogonal DNF (ODNF). Nonrepeated DNF has no argument with the same index.

Probability function is the probability that a boolean function is true. To move from boolean functions to probabilistic should be present:

- PDNF;
- ODNF;
- Nonrepeated in basis functions conjunction-negation.

IV. The analysis procedure

1. Firstly scenatio of danger development is made, which represents a logic-probability model of the security system. The scenario is represented as a graph (such as "tree") and contains three types of events: initiating (IE), intermediate and destination. Initiating event (IE) describe external influences on the system. Intermediate events are obtained by logical combination of two or more events. The most common:

- conjunction of events (output event occurs only in the presence of events on both inputs);

- disjunction events (output event occurs in the presence of at least one event on one of the inputs).

Finite event describes the dangerous condition of the system (for example, the penetration of the intruder to the secure area).

Developing of a scenario is a creative task. Quality of analisys depends on the completeness of description of the security system and also depends on causal relationships between events. Therefore, it is desirable to involve real expert practitioners in object security for developing scenario.

2. Function of hazards $y(z_1...z_n)$ is compiled. Its arguments are the IE, and value are finite (dangerous) event. Each shortest path of dangerous functioning (SPDF) is a minimal set of IE, conjunction which leads to a dangerous condition (SPDF = $\wedge z_i$). Hazard function of the system is a disjunction SPDF:

$$y(z_1...z_n) = \vee[\wedge z_i] \quad (1)$$

3. Function of hazard is reduced to one of three forms and replaced to probability function $P\{y(z_1...z_m)\}$ as follows:

- z_i is replaced on $P\{z_i = 1\} = R_i$
- z_i' is replaced on $P\{z_i' = 1\} = Q_i = 1 - R_i$

where R_i - the probability of the i-th IE.

4. Searching value of probability functions:

$$\psi(y) = P\{y(z_1...z_m) = 1\} \quad (2)$$

Equation (2) determines the degree of risk in the system.

V. The problem of initial data

The problem of initial data is crucial for any analytical method. Impossibility of obtaining of reliable data can reduce and even negate the practical utility of the best method.

For the survivability analysis of security system several types of initial data can be used:

- technical specifications of technical security means (results of tests), such as probability of intruder detecting by detection means Pdetect, the probability of false alarms Pfa, error probability of access control Peac;
- the time of the guard movement and the intruder movement, time to overcome physical barriers, and others. (including the results of tests or analytical assessments)
- the results of threats analysis may be assessed, based on the statistics of attacks or reflect intuitive understanding of the features and character of one or another threat, which can be formalized in various "models intruder" and others.

From the foregoing follows that initial data of the third type should be used carefully. When reliable assess are impossible, better way is to simplify the model than using unreliable data. The quality of the method is largely determined by the reliability of initial data.

VI. Advantages and disadvantages of the method

The advantages of the method:

1. Ability to obtain justified quantitative criterion of quality of security system (as opposed to "artificial" methods ("weighted summation" objective function, etc.). The analysis of survivability can be considered as a method of multi-criteria optimization.

2. Ability to build a safe operation model of the security system, to determine the "vulnerabilities" of the system and assess the "contribution" of each, ranked their by degree of danger.

3. Ability to detect structure of the security system. In terms of logical-probability methods, system of any nature can be attributed to:

- structurally simple (reduced to the parallel, serial, tree models);
- structurally complicate (not reducible to such)
- associative (united disordered elements, based on the attribute of destination).

Security system is associative (structureless) system. Elements in it are united by objective function - the provision security of object. Analysis of survivability allows structuring a security system - it can become structurally simple and even (with a creative approach to the compiling scenario development of danger) find features of a structural complicated system.

Disadvantages:

1. The complexity of the logical transformations in the analysis of complicated scenarios (transfer from functions of dangerous condition (1) to the functions of probability (2)). To facilitate the calculations developed a range of methods.

2. Diversity of initial data (objective, are reliable assessments and subjective , reflecting "expectations threat ").

Conclusion

Thus, the logical-probability method is a powerful mechanism for analysis of structurally complicated systems. Their use for the analysis security of security systems allows to quantify the security level of the object and are the basis for the design of effective security systems.

References

[1] M. I. Faleeva, Ed., Nadezhnost' tehnicheskih sistem i tehnogennyj risk [The reliability of technical systems and technogenic risk]. Moscow: Delovoj jekspress Publ., 2002.

[2] I.A. Rjabinin, Nadezhnost' i bezopasnost' strukturno-slozhnyh sistem [Reliability and security of structurally complicated systems]. St. Peterburg: Politehnika Publ., 2000.