https://doi.org//10.59531/ots.2023.1.1.131-142

NON-PROBABILISTIC HAZARD EVALUATION

[NEM-VALÓSZINŰSÉGI VESZÉLYELEMZÉS]

ISTVÁN BUKOVICS* – ISTVÁN KUN

John Wesley Theological College, Budapest, Hungary

* *Corresponding author*
bukovicsistvan@wjlf.hu;

Abstract. Quantitative analysis of complex risk systems often faces three major problems. The first problem is the size of the system to be examined, since the number of possible system states increases exponentially with system size. The second problem is the topology of the system which may not be tree-like. The third problem is the consideration of randomness, since risk events are in many cases single, non-repetitive, therefore probability theory is inadequate. In order to handle this deficiency we suggest to apply logical risk analysis which traces back the main risk event to elementary, controllable risk events by means of the logical structure describing the operation of the risk system. For illustrations we give some very simple structures and a soil contamination problem as a real-size example.

Keywords: logic-based risk assessment, logic-based indicators, fault tree analysis, environment pollution, soil contamination

Introduction

Reliability analysis of complex networks has been a central question of engineering for decades, and the application of methods developed for this aim has proved to be largely useful.

Publications (Szili and Pokorádi, 2014) and (Pokorádi, 2015) point out to the fact that the applicability of the familiar fault tree method for the analysis of such networks is limited.

In order to solve this problem Pokorádi suggests the truth table method. This method is well-known, operable, but it has serious drawbacks.

An important drawback is that the number of system states to be examined, as emphasized by Pokorádi, is growing at an exponential rate as a function of the number of system elements. If the number of system elements is denoted by N, then the number of system states is 2^N. In the above mentioned publications of Pokorádi very simple systems are shown as introductory illustrative examples with not more than 5 system elements – see Figure 1 later in this article – and the state probabilities of these systems can be easily computed manually. In case of 20 system elements, which is a small system, the number of system states to be handled is $2^{20} \approx 10^6$, this can be made by a computer. Nevertheless in

https://doi.org//10.59531/ots.2023.1.1.131-142

case of 50 system elements, which cannot be considered to be a very large system, the number of system states to be handled is $2^{50} \approx 10^{15}$, and this is too much even for a computer.

Other drawbacks arise from the utilization of probability.

One such point is that the truth table method, just like probabilistic fault tree analysis, supposes that elementary events (in case of reliability analysis the failures of system elements) are statistically independent. This assumption is however often not satisfied. E.g. in an electronic system the cause of the failure may be some electromagnetic shock of natural origin (thunderstroke, solar flare), which hits several system elements simultaneously. Staff members and network-bound computers of an institution can be affected by an infection –human or computer viral infection respectively – not individually, not independently of one another.

A second problematic point is that large-scale risk events are mostly unique i.e. non-repetitive. This makes application of probability theory inadequate since the notion of probability is inseparably associated with a statistical nature i.e. the event to which it belongs is repeatable arbitrarily many times under the same circumstances with a steady distribution of the experimental results.

An objection raised by (Pokorádi, 2015) to Fault Tree Analysis is that many complex risk systems have a topology which cannot be modeled with the usual serial-parallel hierarchy. A typical example is the Wheatstone bridge circuit depicted on Figure 1.c. below.

In order to handle these problems we suggest below a different approach.

Basic concepts of logical risk analysis

Logical risk analysis characterizes the risk system to be examined by means of a logical, i.e. Boolean function, hereafter referred to as the basic logical function.

The function itself describes the connections among system elements, while its variables the occurrence or non-occurrence of the events (in other words the true or active, and false or passive state respectively).

In a wide variety of cases the state of a risk system within the application area of logical risk theory can be described by a fault tree, and its behaviour can be analyzed by fault tree analysis (Bukovics, 2007). The fault tree itself is a Boolean function visualized by a logical diagram with tree-like topology, which represents the possibly multilevel interrelation between the critical event examined and its potential triggering causes. We suppose only that the events of the risk system under analysis are linked through a fixed logical structure.

https://doi.org//10.59531/ots.2023.1.1.131-142

The objective of the analysis is to originate the occurrence of the undesirable main event to simpler, so-called primitive events which are possibly under our control.

The attribute „undesirable" is used only in a stylistic sense because it is the result of a subjective judgement, so we do not define it as a notion.

The main, undesirable event as the central topic of logical risk analysis has a special name: top event. The objective of risk analysis is to give a necessary and sufficient conditions for the occurrence of the top event in the form of conjunctions and disjunctions of prime events.

Primitive events, in short prime events are events which, within the given event system, cannot be originated from other events, they are not consequences of other events, but they are causes of other events, and all events can be originated from these events.

The top event is composed from the prime events through „substituting" the prime events into the basic logical function.

A partial or intermediate event is composed from the prime events through substituting the prime events into a truncated version of the basic logical function.

(Bukovics, 2007) introduces the notion of a covered prime event. Prime event PE will be called covered, if either PE belongs to a disjunctively connected prime event group where the joint state of the whole group can be active while PE is passive or PE belongs to a conjunctively connected prime event group where the joint state of the whole group can be passive while PE is active. Hence prime event PE is covered if the other prime events in the same disjunctive or conjunctive event group can neutralize the effect of PE on the joint state of the group. This notion becomes important if we cannot control directly the state of PE (typically when PE is some natural phenomenon) but we can counterbalance the effect of PE through other prime events.

We speak about triggering if the active state of a partial event brings about the occurrence of the top event.

We speak about parrying if if the passive state of a partial event turns away the occurrence of the top event.

Normal forms and critical points

The conjunctive normal form is a representation of the basic logical function where the state of the top event is traced back to the states of a set of non-reducible groups of prime events in such a way that if in each group at least one prime event is active then the top event is also active. These groups will be called strong points. Nevertheless, a strong point is actually a parrying scenario, because if each prime event in the group is passivated then the top event will thereby be passivated as well. The conjunctive normal form is the

https://doi.org//10.59531/ots.2023.1.1.131-142

conjunction of prime event groups where the prime events within the groups are connected disjunctively.

Analogously, the disjunctive normal form is a representation of the linkage system between the occurrences of the prime events and that of the top event where the state of the top event is traced back to the states of a set of non-reducible groups of prime events in such a way that if at least in one group each prime event is activated then the top event is also activated. These groups will be called weak points. Nevertheless, a weak point is actually a triggering scenario, because if each prime event in the group is activated then the top event will thereby be activated as well. The disjunctive normal form is the disjunction of prime event groups where the prime events within the groups are connected conjunctively.

Two different conjunctive normal forms of the same Boolean function (in our case the same fault tree) contain always the same prime event groups, only the order of the groups within the normal form and the order of prime events within the groups may be different. The same is true for the disjunctive normal form.

Strong and weak points are together called critical points.

The exact discussion of normal forms can be found in standard textbooks of mathematical logic, see e.g. (Birkhoff and Bartee, 1970), (Demetrovics et al, 1985), (Jaglom, 1983).

It is fundamentally important to state that conjunctive and disjunctive normal forms exist not only for fault trees but for a much wider class: for all positive formulae of propositional logic. A logical forula is called positive if it does not contain any of the negations of the prime events. In this case the normal forms will not contain the negations of prime events either, therefore normal forms look exactly like in the tree-like case. In what follows we will suppose positivity.Top events, prime events, normal forms have sense in this wider class of cases, only the hierarchical form of logical dependence of the top event from prime events as a basic assumption is not required in the more general case. This means that the analysis technique to be discussed in the sequel remains valid for Boolean systems which cannot be described by a fault tree. As an example we will see this in the case of the Wheatstone bridge circuit.

Based on the above mentioned theory, it is clear that the top event is in passive state if and only if at least one of its strong points is in passive state. A strong point is in passive state if and only if each of its prime events is in passive state. Hence the passivation of all prime events of a strong point is actually a parrying scenario, the conjunctive normal form is a collection of parrying scenarios.

Similarly, based on the above mentioned theory, it is clear that the top event is in active state if and only if at least one of its weak points is in active state. A weak point is in active state if and only if each of its prime events is in active state. Hence the activation of all

https://doi.org//10.59531/ots.2023.1.1.131-142

prime events of a weak point is actually a triggering scenario, the disjunctive normal form is a collection of triggering scenarios.

Logical indicators

In this section we will be engaged in defining indicators based on the logical structure of the risk system by means of logical risk analysis. A suggestion to create a logical indicator concept usable in public administration is given in (Bukovics, 2015).

Active crisis potential of a prime event is the number of strong points containing the given prime event.

Hence, according to the definition of strong points if at least one prime event of its strong point is active then the parrying scenario does not work.

Analogously, passive crisis potential of a prime event is the number of weak points containing the given prime event.

Hence, according to the definition of the weak point, if at least one of its prime events is passive, then the triggering scenario does not work.

We introduce some notations.

- nSP: number of strong points
- nWP: number of weak points
- nESP(k): number of enclosing strong points (active crisis potential) of prime event k
- nEWP(k): number of enclosing weak points (passive crisis potential) of prime event k

Now we define the indicators:

- Act(k) = nESP(k)/nSP: triggering power of prime event k
- Pas(k) = nEWP(k)/nWP: parrying power of prime event k

Triggering power of prime event k characterizes the property of this event to what proportion its active state can activate strong points, i.e. to what extent it can disable the parrying scenarios. The higher this proportion is, the larger role this prime event has in the occurrence of the top event, and the less other prime events are necessary for the occurrence of the top event. If this proportion is 100 % then prime event k alone is able to trigger the top event.

Parrying power of prime event k characterizes the property of this event to what proportion its passive state can passivate weak points, i.e. to what extent it can disable the triggering scenarios. A practical manifestation of this indicator is identified in (Nagy, 2011) as the robustness against effects endangering critical infrastructures. The higher this proportion is, the larger role this prime event has in the prevention of the top event, and

https://doi.org//10.59531/ots.2023.1.1.131-142

the less other prime events are necessary for the prevention of the top event. If this proportion is 100 % then prime event k alone is able to parry the top event.

On the basis of the above mentioned concepts both triggerng and parrying power satifies the earlier cited general requirements stated in the related literature about the function of the indicator (Olsson et al, 2004), (KIM, 2013), (FAO, 1999). Particularly, both of these powers suggestively characterize the distance from the passive state of the risk system as a desirable objective and the movement in this direction respectively.

Sensitivity coefficient and triggering power

The study (Pokorádi, 2011) suggests a sensitivity analysis method to examine probabilistic fault trees. Sensitivity analysis itself leads back proportional change of the probability of the top event as dependent variable to the proportional changes of the probability of the prime events as independent variables. A major practical limitation of the method is the earlier mentioned exponential growth of the number of system states.

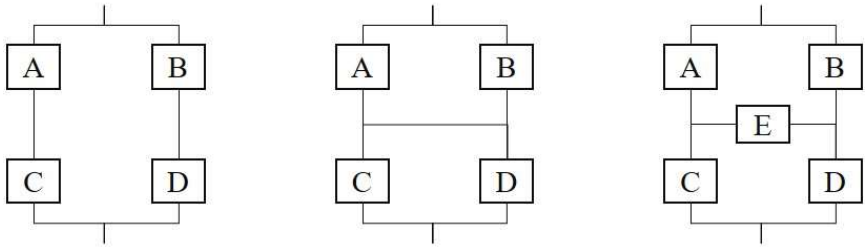
A theoretical limitation appears when non-probabilistic events are encountered in the system.

The above mentioned logical risk analysis may help in handling the problem caused by both size limitations and non-probabilistic events. Logical risk analysis does not use probabilities, therefore the infinitesimal sensitivity analysis used in (Pokorádi, 2011) cannot be performed in the present paper.

Nevertheless, at the same time sensitivity coeffcients belonging to prime events computed in the framework of the sensitivity analysis express particularly to what extent activation of the given prime event contributes to the activation of the top event. A similar content can be attributed to triggering power calculable in logical risk analysis. Although the ways of computation for the two different kinds of indicators are essentially different, they express similar contents.

https://doi.org//10.59531/ots.2023.1.1.131-142

Examples for the application of logical indicators



1.a. 1.b. 1.c.

Figure 1. a: *parallel-serial switching; b: serial-parallel switching; c: bridge switching*

Figures 1.a. and 1.b. are analyzed in (Szili and Pokorádi, 2014) while Figure 1.c. in (Pokorádi, 2015). A letter code refers to a prime event meaning failure of a system component. Activation of certain combinations of such failures lead to the activation of the top event, i.e. the inoperability of the system. I the original form prime events had occurrence probabilites and the analysis was made using truth table. Here we carry out a logical analysis therefore we eliminate the application of probabilities.

In the cases 1.a. and 1.b. system failure follows a fault tree structure while in case 1.c. does not. The reason is that element E has an effect on the system failure through both perpendicular branches (AC and BD respectively).

In what follows we demonstrate the application of the above detailed theory. We present the conjunctive normal form (CNF), the disjunctive normal form (DNF) and then we compute the logical indicators.

Case a.

Conjunctive normal form: (A+B)(A+D)(B+C)(C+D)
Disjunctíve norma form AC+BD
Strong points: {A, B}, {A, D}, {B, C}, {C, D}
Weak points: {A, C}, {B, D}

https://doi.org//10.59531/ots.2023.1.1.131-142

Indicators:

***Table 1**. Logical indicators for Case a*

Code	nESP(k)	Act(k)	nEWP(k)	Pas(k)
A	2	50,0%	1	50,0%
B	2	50,0%	1	50,0%
C	2	50,0%	1	50,0%
D	2	50,0%	1	50,0%

Case b.

Conjunctive normal form: (A+B)(C+D)
Disjunctíve norma form AC+AD+BC+BD
Strong points: {A, B}, {C, D}
Weak points: {A, C}, {A, D}, {B, C}, {B, D},{A, B}, {C, D}
Indicators:

***Table 2.** Logical indicators of Case b*

Code	nESP(k)	Act(k)	nEWP(k)	Pas(k)
A	1	50,0%	2	50,0%
B	1	50,0%	2	50,0%
C	1	50,0%	2	50,0%
D	1	50,0%	2	50,0%

Case c.

Conjunctive normal form: (A+C)(A+E+D)(B+E+C)(B+D)
Disjunctive norma form AB+CD+AED+BEC
Strong points: {A, C}, {A, E, D}, {B, E, C}, {B, D}
Weak points: {A, B}, {C, D}, {A, E, D}, {B, E, C}

Indicators:

***Table 3**. Logical indicators of Case c*

Code	nESP(k)	Act(k)	nEWP(k)	Pas(k)
A	2	50,0%	2	50,0%
B	2	50,0%	2	50,0%
C	2	50,0%	2	50,0%
D	2	50,0%	2	50,0%
E	2	50,0%	2	50,0%

https://doi.org//10.59531/ots.2023.1.1.131-142

The above mentioned examples are only illustrative, their small size and structural simplicity does not allow to exhibit their practicability. Realistic, genuine expamples are discussed in the paper (Bukovics et al, 2015). One of them is the "Soil Contamination" problem, to be presented below.

The total number of events is 55, from which 26 are prime events. For the sake of brevity we do not present the original fault tree, only the indicators based on prime events. According to the computer analysis of the fault tree the number of strong points is 9, the number of weak points is 1560.

Values of the above mentioned indicators:

***Table 4**. Potencial based indicators for "Soil contamination"*

Code	Event name	nESP(k)	Act(k)	nEWP(k)	Pas(k)
1	direct harmful human intervention	1	11,1%	390	25,0%
2	significant soil displacement	1	11,1%	390	25,0%
3	extrusive magmatic activity	1	11,1%	390	25,0%
4	elevation level of contaminated groundwater	1	11,1%	390	25,0%
5	direct wash-out of soil	1	11,1%	520	33,3%
6	direct glacial erosion	1	11,1%	520	33,3%
7	direct ablation by wind	1	11,1%	520	33,3%
8	part of contamination remains in soil	1	11,1%	1560	100,0%
9	part of contamination reaching groundwater causes groundwater level elevation	1	11,1%	1560	100,0%
10	wastewater injected into soil	1	11,1%	780	50,0%
11	wastewater migration occurs	1	11,1%	780	50,0%
12	indirect wash-out of soil	1	11,1%	312	20,0%
13	indirect glacial erosion	1	11,1%	312	20,0%
14	közvetett széllehordás indirect ablation by wind	1	11,1%	312	20,0%
15	van talajvíz a felső akviferben groundwater presence in upper aquifer	3	33,3%	120	7,7%
16	diapirizmus diapirism	3	33,3%	120	7,7%
17	meteor activity	3	33,3%	120	7,7%
18	groundwater in upper layer	1	11,1%	600	38,5%
19	lower layer	1	11,1%	600	38,5%
20	soil freezing	2	22,2%	240	15,4%
21	soil boring	2	22,2%	240	15,4%
22	medium soil displacement	3	33,3%	504	32,3%
23	indirect human activity	1	11,1%	312	20,0%
24	minor soil displacement	1	11,1%	480	30,8%
25	glacial overstress	1	11,1%	240	15,4%
26	soil sinkage	1	11,1%	240	15,4%

https://doi.org//10.59531/ots.2023.1.1.131-142

We can see from Table 4 that the prime events of soil contamination having the largest triggering role ("groundwater, diapirism", "meteor activity") are natural phenomena outside of our sphere of action.

Nevertheless, in this case we can use the earlier defined notion of coveredness. Among the weak points delivered by computer analysis we can find e.g. the following ones:

{2, 7, 8, 9, 10, 15, 22}
{3, 5, 8, 9, 10, 16, 22}
{1, 5, 8, 9, 10, 17, 22}

In these weak points (and in many other weak points not listed here) we can find the above mentioned three prime events which are connected to natural phenomena therefore they are not controllable, namely the ones coded as 15, 16 and 17 respectively. At the same time prime event 10 („wastewater injected into soil") belongs to each of the three enumerated weak points. This prime event is not a natural phenomenon, and it can be controlled under appropriate checking. Therefore if we keep this last mentioned prime event continuously in passive state then we can prevent the activation of the three above mentioned triggering scenarios. This means that prime event 10 which is controllable can cover prime events 15, 16 and 17 which are not conrollable.

Among the prime events with parrying power higher than minimal only "soil boring" can be considered to be a controllable human activity. Parrying power of "wastewater injected into soil" is however 50 %, and this prime event is a controllable human activity, therefore its passivation is possible, thereby decreasing the chance of soil contamination by 50 %.

Summary and prospect

The feasibility of reliability analysis of logical networks is strongly limited by the combinatorical burst due to size increase. In this case we can measure the effect of individual prime event on the occurrence of the top event by means of the indicators of the logical risk analysis.

It is reasonable to develop the conceptual system and analytic apparatus of the sensitivity analysis of the method, as it is usual in the case of probabilistic analyses.

https://doi.org//10.59531/ots.2023.1.1.131-142

REFERENCES

[1] Birkhoff, G., Bartee, T.C.(1970): Modern Applied Algebra. – McGraw-Hill, New York.

[2] Bukovics I., Fáy Gy. Kun I. (2015): A jó állam és a védelmi szféra (The good state and the defence sphere). Hadmérnök 10(2): 208-222. http://hadmernok.hu/152_19_bukovicsi_fgy_ki.pdf

[3] Demetrovics J., Denev, J., Pavlov, R. (1985): A számítástudomány matematikai alapjai (Mathematical foundations of computer science). – Tankönyvkiadó, Budapest.

[4] (FAO, 1999): Pressure-State-Response Framework and Environmental Indicators. – In: Livestock, Environment and Development Initiative (LEAD), Food and Agriculture Organisation of the UN (FAO), Indicators.

[5] Jaglom, I. M. (1983): Boole struktúrák és modelljeik (Boole structures and their models). – Műszaki Könyvkiadó, Budapest.

[6] Nagy R. (2011): A kritikus infrastruktúra védelme elméleti és gyakorlati kérdéseinek kutatása (Research in theoritcal and practical problems of the defence of critical infrastructure). Doctoral dissertation. – National University of Public Service, Budapest.

[7] Olsson, J. A., Hilding-Rydevik, T., Aalbu, H., Bradley, K. (2004): Indicators for Sustainable Development. Paper for discussion, European Regional Network on Sustainable Development, Nordregio, Nordic Centre for Spatial Development, Cardiff, 23-24.

[8] Pokorádi L. (2011): Sensitivity Investigation of Fault Tree Analysis with Matrix-Algebraic Method. – Theory and Applications of Mathematics & Computer Science 1(1): 34-44.

[9] Pokorádi L. (2015): Failure Probability Analysis of Bridge Structure Systems. – In: Proc. 10th Jubilee IEEE International Symposium on Applied Computational Intelligence and Informatics, May 21-23. Timişoara, Romania, 319-322. https://doi.org/10.1109/SACI.2015.7208220

[10] Szili T., Pokorádi L. (2014): Igazságtábla alkalmazása rendszer megbízhatóság elemzésére (Application of the truth table method for the analysis of system reliability). In: Fiatal műszakiak tudományos ülésszaka XIX (Scientific session of young engineers XIX). Kolozsvár, 2014. március 20-21. 377-380.

[11] Teljesítménymenedzsment 1. Fejlesztési módszertan a szervezeti célok meghatározására, valamint a szervezeti teljesítmény indikátorok kidolgozásának támogatására. (Efficiency management 1. Development methodology for for the designation of organizational objectives and for the support of the elaboration of

https://doi.org//10.59531/ots.2023.1.1.131-142

organizational efficiency indicators). Közigazgatási és Igazságügyi Minisztérium, Budapest.

Absztrakt. A komplex kockázati rendszerek mennyiségi elemzése során három különböző probléma merül fel. Először: a lehetséges rendszerállapotok száma a rendszer méretével expononciálisan nő. Másodszor: a rendszer topológiája sokszor nem fa-struktúrájú. Harmadszor: a véletlenség figyelembe vétele, mivel a kockázati események gyakran egyediek, nem ismétlődőek, ezért a valószínűségszamításban általában feltételezett tömegjelenségek itt nem jellemzőek. Ezeknek a prolémáknak a kezelésére a logikai kockázatelemzést javasoljuk, amely a kockázati főeseményt logikai eszközökkel, minél nagyobb arányban kézben tartható elemi eseményekre vezeti vissza. A módszert néhány nagyon egyszerű példán illlusztáljuk, majd egy valóságos talajszennyezési példán mutatjuk be.