Risk Level as Emergency Indicator: A Mathematical Framework for Nonprobabilistic Risk Systems Based on Fault Tree Methodology

BY: ISTVÁN BUKOVICS

A tanulmány célja egy olyan veszélyhelyzeti indikátor elmélet ismertetése, amely a katasztrófa kockázati rendszerek közvetlen logikai leírásának matematikai alapjaira épül, és szemlélete szorosan kapcsolódik a hibafa módszerhez.

A természeti és civilizációs katasztrófák elleni védelem egyre aktuálisabb rendészeti feladat, melynek egyik jelentős tartaléka a tudományos elméleti alapok kidolgozása.
A jelen tanulmány célja egy olyan veszélyhelyzeti indikátor elmélet ismertetése, amely a katasztrófa kockázati rendszerek közvetlen logikai leírásának matematikai alapjaira épül, és szemlélete szorosan kapcsolódik a hibafa módszerhez. Nem törekszünk feltétlenül numerikus jellegű indikátorok meghatározására, tekintve, hogy a logikai indikátorok az esetek nagy többségében mind elméleti, mind gyakorlati szempontból alkalmasabbnak látszanak. A célunk olyan (numerikus és logikai) indikátorok meghatározása, amelyek elméleti szinten, közvetlenül a szóban forgó hibafa matematikai modelljéből származtathatók, alkalmazva természetesen a klasszikus (matematikai, vagy szimbolikus) logika törvényszerűségeit és szabályait.

INTRODUCTION

The object of the present work is to outline a theory of an emergency indicator based on the mathematical foundation of immediate logic description of a risk system. This approach is closely related to fault tree methodology. It is supposed that the reader is familiar with the basics of Boolean functions as well as with fault trees[1].
In the present paper common cause problem will not be dealt with. It is postponed to a separate paper.

As for the indicators in general we don't insist to numeric features, since logic indicators seem to be frequently more adequate for both theoretical and practical purposes. What we do insist to, however, is to define indicators (numeric or logic) that can be theoretically derived from the (mathematical formulation of the) very fault tree in question using naturally the laws and rules of classical (mathematical or symbolic) logic.
An instructive example – basically due to www.sverdrup.com – can be found in Chapter 1. where some additional elements are introduced. First, the logic type of the event in question is displayed as (&) for conjunctive and (V) for disjunctive case corresponding to the traditional (but somewhat obsolete and clumsy "gate style") AND-Gate and OR-Gate respectively. Second a new outlook-style (due to Profes[2]) a fault tree is displayed in a similar fashion to the Microsoft Windows® explorer. Using outlook (or map) view in Microsoft Word® a fault tree is more conveniently viewed than with gate diagrams.
Three kinds of indicators are planned be within fault tree methodology context. First, *structural*, second *strategic*, third "*Franklin*". These are strongly related to each other. Out of them only a structural indicator the "risk level" will be dealt here.
We consider a fault tree as a *complete description* of a *risk system.* "Complete description" here is meant that all we know about the risk system in question are to be derivable from its fault tree. The notion of risk system is a basic idea. Intuitively it is the system that a fault tree is about. As for the fault tree it is considered to be as an *indirect Boolean function* with independent Boolean variables called *primitive events* (sometimes called basic events or

[1] See [Henley-Kumamoto] and [Harrison]
[2] www.profes.hu

prime events for short). Prime events are numbered separately. Thus each prime event has a “P-number” and an “E-number” (see below). It is intuitively clear from the example below. Formal definition will be given in Chapter 2.The possible values of the Boolean variables are denoted by 0, u, 1 and respectively called to be in *passive, free (uncertain)* and *active state*. The primitive state of the risk system is by definition the set of all the prime events.

1. EXAMPLE OF A FAULT TREE[3]

Below the original fault tree gate diagram can be seen. For legend, see the reference. Traditionally, fault trees are applied to risk systems having events with probability. Although nonprobabilistic events (such as for instance a terrorist attack or climatic extremities) evidently have their risk (but not probability), they cannot be treated by probabilistic risk assessment or described by fault tree methodology. It is possible, however to keep the successive explication[4] technique characteristic to fault tree construction and dispensing with the probabilistic side. For now on we term this approach as “logic risk assessment” or “non probabilistic” risk assessment / analysis”. As a result a *direct* (or *immediate*) *logical description* of events is provided in the form of an *indirect Boolean function* or, in other equivalent form, of a system of Boolean equations.

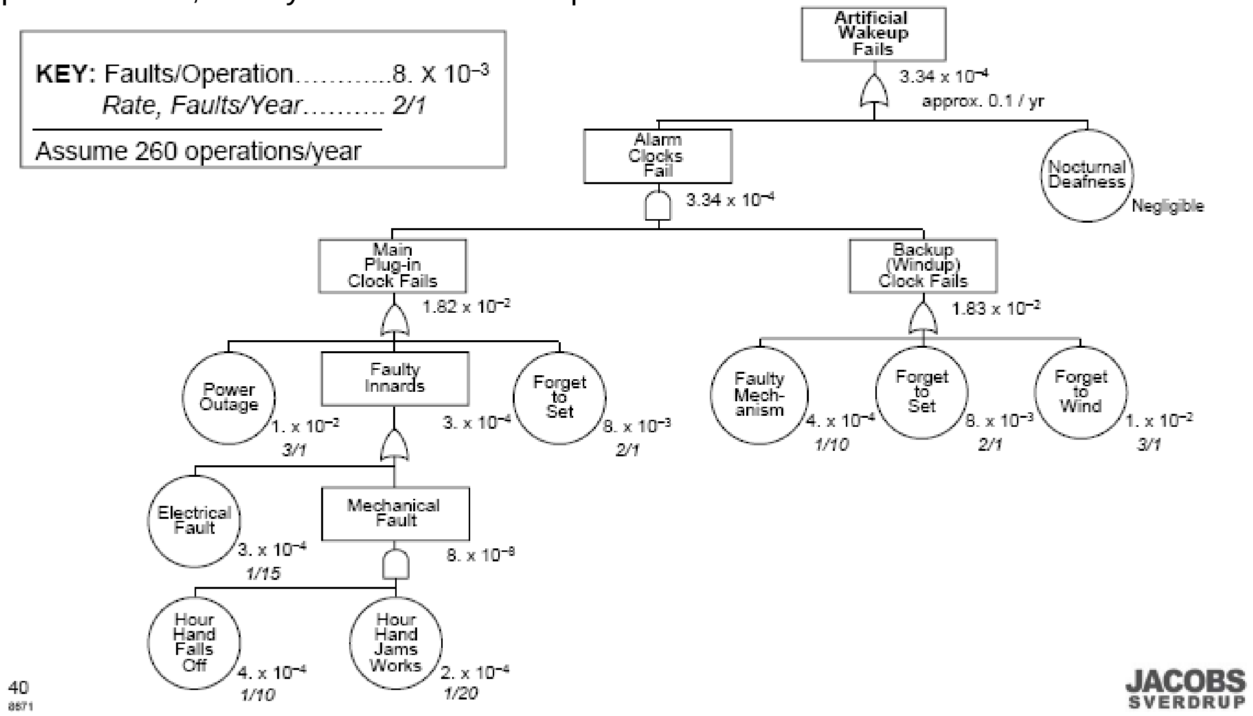


Figure 1.
The original traditional form of the fault tree example.
(By Jacobs Engineering Group Inc. www.sverdrup.com)

(V): FAULT TREE EXAMPLE

[3] See: P.L. Clemens**:** Fault Tree Analysis: Jacobs Engineering Group Inc. February 20024th Edition http://www.sverdrup.com/safety/fta.pdf

[4] See [Carnap] for the most thorough discussion of the concept of explication.

1(&): E2

1.1(V): E4

1.1.1(V): E6

1.1.1.1(V): E9

1.1.1.1.1: p5, e11

1.1.1.1.2: p6, e12

1.1.1.2: p4, e10

1.1.2: p2, e7

1.1.3: p3, e8

1.2(V): E5

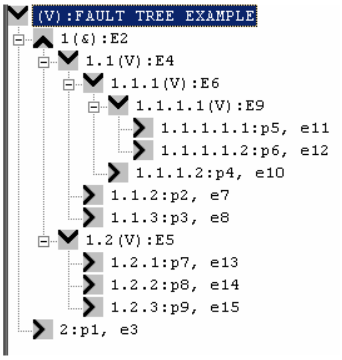
1.2.1: p7, e13

1.2.2: p8, e14

1.2.3: p9, e15

2: P1, E3

Figure 2.
The fault tree in the outlook view in Microsoft Word form



```
(V):FAULT TREE EXAMPLE
 1(&):E2
   1.1(V):E4
     1.1.1(V):E6
       1.1.1.1(V):E9
         1.1.1.1.1:p5, e11
         1.1.1.1.2:p6, e12
       1.1.1.2:p4, e10
     1.1.2:p2, e7
     1.1.3:p3, e8
   1.2(V):E5
     1.2.1:p7, e13
     1.2.2:p8, e14
     1.2.3:p9, e15
 2:p1, e3
```

Figure 3.
The fault tree as displayed by Profes (www.profes.hu)

According to the example above the Boolean equations are as follows:
(“+”, “x” are for disjunction and conjunction i.e. “OR” and “AND” respectively. Prime events (denoted by the “P-numbers”) are those not occurring in the left hand side of an equation between “E-numbers”. “E-numbers” and “P-numbers” correspond to the fault tree nodes.

E1 = E2 + E3
E2 = E4 x E5
E4 = E6 + E7 + E8
E5 = E13 + E14 + E15
E6 = E9 + E10

$E9 = E11 + E12$

$p1 = E3$
$p2 = E7$
$p3 = E8$
$p4 = E10$
$p5 = E11$
$p6 = E12$
$p7 = E13$
$p8 = E14$
$p9 = E15$

2. A FORMAL FARAMEWORK

Formally, a Risk System is a pair $< \underline{\mathbf{P}}, \underline{\mathbf{E}}, \wedge, \vee >$, where
$\underline{\mathbf{P}}$ is a finite set $\underline{\mathbf{P}} = \{p_1,..., p_n\}$, $n > 0$, integer,
$\underline{\mathbf{E}}$ is a finite set $\underline{\mathbf{E}} = \{E_1,..., E_m\}$, $m > 0, \leq n$ integer,
$\wedge, \vee$ **(**alternatively sometimes denoted by +, x respectively) are algebraic operations[5] defined on $\underline{\mathbf{P}}$ U $\underline{\mathbf{E}}$ satisfying that for arbitrary elements p, q, r of $\underline{\mathbf{P}}$ U $\underline{\mathbf{E}}$, the following axioms for the *distributive lattices* hold:

$$p \wedge (q \wedge r) = (p \wedge q) \wedge r \text{ and } p \vee (q \vee r) = (p \vee q) \vee r$$
$$p \wedge q = q \wedge p \text{ and } p \vee q = q \vee p$$
$$p \wedge (q \vee p) = p \text{ and } p \vee (q \wedge p) = p$$
$$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r) \text{ and } p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$$

It can be proved (see any textbook on lattices) that for arbitrary elements p, q, r of $\underline{\mathbf{P}}$ U $\underline{\mathbf{E}}$,

$$p \wedge p = p \text{ and } p \vee p = q$$
$$p \wedge q = p \text{ if and only if } p \vee q = q$$

The elements E_j of $\underline{\mathbf{E}}$ ($j = 1 \ldots m$, $m \leq n$) are Boolean "*clauses"* meaning either pure conjunction or disjunction. Their members are called the *explicants* of E_j being the *explicandum* of the explicants. The prime events are alternatively called "*prime explicants*" Event E_1 is called the "*main explicandum*" or "*Main Event*". The latter is not to be confused with the traditional fault tree term "Top Event". This will be defined separately later in the paper.

Now we define:

$$p \leq q \text{ if and only if } p \wedge q = p$$

For now on, a Risk System (RS) will be described (modeled) by a *ternary* indirect monotonic function FT ($p_1... p_n$), n integer, fixed, where each p_i ($i = 1 \ldots n$) is a ternary variable with values 0, u,1. This FT ("Fault tree") function results if all E_j are eliminated using the Boolean expressions defining the E_j -s. Variables p_i are interpreted respectively as
$p_i = 0$ whenever the prime event (belonging to p_i) does not occur (i.e. is not the case),
$p_i = 1$ whenever the prime event (belonging to p_i) does occur (i.e. is the case).
$p_i = u$ whenever the prime event (belonging to p_i) is "undefended". This – as the "third logical value" – is interpreted within traditional ternary logic as "uncertain" or

[5] In lattice theory their frequently used names are "infimum – supremum" "meet-unio", while in logic "conjunction - disjunction"

“undetermined” or “unknown” or “free”. We prefer the latter[6]. Thus if $p_i = u$ then p_i is said to be in a free state or just a free prime (event) for short.
As usual in Boolean logic (or algebra) we define an *ordering relation* on the set of the possible values of the events postulating $0 < u < 1$. By this, we define conjunction and disjunction as

$$p \wedge q = \min(p, q) \text{ and } p \vee q = \max(p, q)$$

respectively for arbitrary ternary variables p, q.

Now let any series $p_1 \ldots p_n$ be denoted by $\underline{\mathbf{p}}$ called a “*state vector*”.
If all $p_1 \ldots p_n$ is primary we speak of “*primary state*”. If all the “E-numbers (value) are given we speak of “*system state* If for a $\underline{\mathbf{p}}$, FT ($\underline{\mathbf{p}}$) = 1 then we say that the risk system, described by the ternary indirect function FT is *active* in the state $\underline{\mathbf{p}}$.
If for a $\underline{\mathbf{p}}$, FT ($\underline{\mathbf{p}}$) = 0 then we say that the risk system, described by the ternary indirect function FT is *passive* in the state $\underline{\mathbf{p}}$.
If for a $\underline{\mathbf{p}}$, FT ($\underline{\mathbf{p}}$) = u then we say that the risk system, described by the ternary indirect function FT is undetermined or *free* in the state $\underline{\mathbf{p}}$.

For any state vectors $\underline{\mathbf{p}}$, $\underline{\mathbf{q}}$ we define

$$\underline{\mathbf{p}} \leq \underline{\mathbf{q}} \text{ if and only if for all } i = 1,\ldots,n \ p_i \leq q_i,$$

$$\underline{\mathbf{p}} \geq \underline{\mathbf{q}} \text{ if and only if } \underline{\mathbf{q}} \leq \underline{\mathbf{p}}$$

and

$$\underline{\mathbf{p}} < \underline{\mathbf{q}} \text{ if and only if } \underline{\mathbf{p}} \leq \underline{\mathbf{q}} \text{ and } \underline{\mathbf{p}} \neq \underline{\mathbf{q}}$$

It follows form the above:

$$\underline{\mathbf{p}} \leq \underline{\mathbf{q}} \text{ and } \underline{\mathbf{q}} \leq \underline{\mathbf{r}} \text{ implies } \underline{\mathbf{p}} \leq \underline{\mathbf{r}}$$
$$\underline{\mathbf{p}} \leq \underline{\mathbf{q}} \text{ and } \underline{\mathbf{q}} \leq \underline{\mathbf{p}} \text{ implies } \underline{\mathbf{p}} = \underline{\mathbf{q}}$$
$$\underline{\mathbf{p}} \leq \underline{\mathbf{q}} \text{ and } \underline{\mathbf{p}} = \underline{\mathbf{q}} \text{ implies } \underline{\mathbf{p}} = \underline{\mathbf{q}} \text{ or } \underline{\mathbf{p}} < \underline{\mathbf{q}}$$

The primary state of an RS can conveniently be represented by the “*state page*[7]”

3. THE RISK LEVEL AS A STRUCUTURAL INDICATOR

Within the present context *structural indicators* are considered to be those not depending on the *state* of the risk system in question but rather characterize the logic *structure* of the risk system (described by the fault tree function FT) as a *whole*.
Let a Risk System RS be given and fixed and $L \geq 0$ integer.
By definition, for L = 0 the L-level of RS is the set of all the prime explicants.
For L = 1 the L-level of RS is the set of all the explicandi having only prime explicants.
For $L \geq 2$ the L-level of RS is the set of all the explicandi having only explicants on L – 1 level (but not on lower level).
The level of an explicandum (or event) E_i is denoted by *Level* (E_i)
The number of all the levels of RS will be denoted by nLevels.
Events E_i (i.e. explicandi) on level L = nLevels i.e. when *Level* (E_i) = nLevels are called “Top Events”

[6] Due to some resemblance to the Shannon’s Switching Game. See e.g.: [Nievergelt ea.]
[7] Introduced by Profes (www.profes.hu)

The RS of the example above has three levels: L = 0, 1, 2. In this case the number of the top events happens to be 1 and it does **not** coincide with the main event E_1 Being on Level = 1. This is quite typical in risk systems.
The *level diagram* for this RS is on Figure 4.

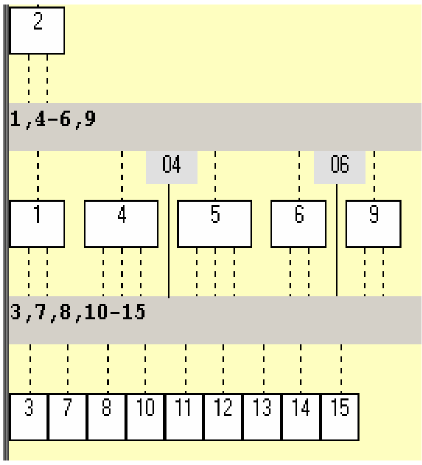


Figure 4.
Level diagram for the example RS

White box color and dotted lines mean that each event is in Free State. It can be seen that there are peculiar events (namely E_4 and E_6) possessing the same level as their explicandi:

E4 = E6 + E7 + E8
Level (E4) = 1 and also, Level (E6) = 1

Similarly,

E6 = E9 + E10
Level (E6) = 1 while Level (E9) = 1, too.

By definition, an event having the same level as one of its explicants is called "*weak transient*". An event having the lower level as one of its explicants is called "strong *transient*". In other word a strong transient event has at least one explicant having the same a higher level than itself.
An example for strong transient can be seen on Figure 5

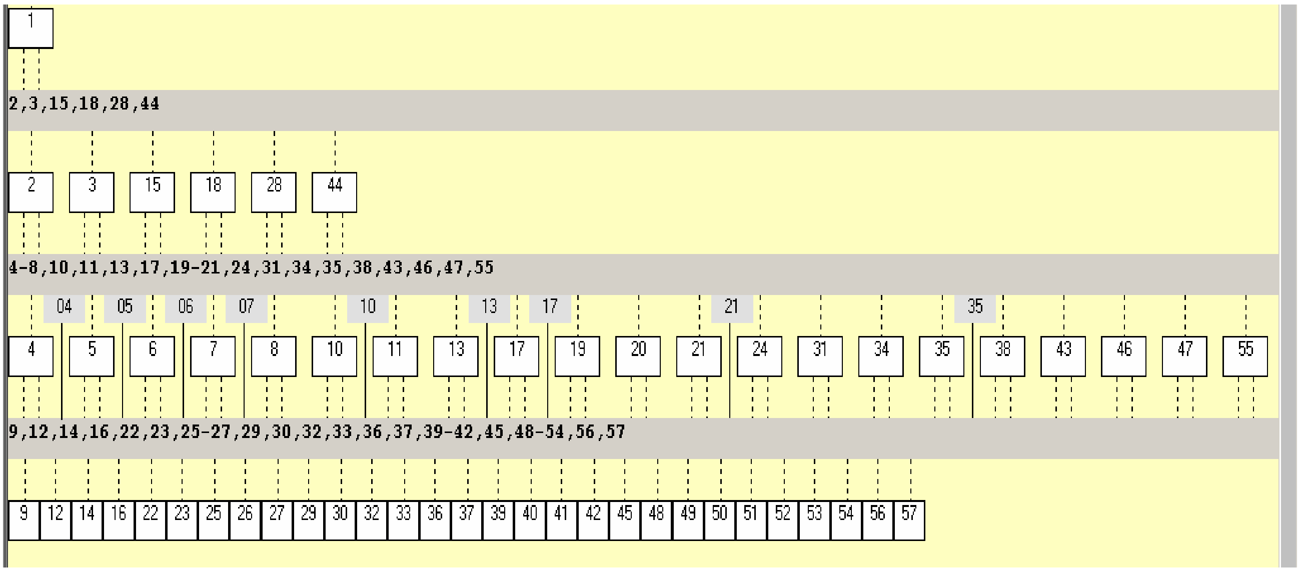


Figure 5

Dominant risk system with strong transient. Event #8 (at level = 1) has an explicant #18 with higher level (L = 2) than itself. Grey box refers to transients, grey stripe to" bus"

The pertaining fault tree example is basically due to Arthur D. Little Inc. (www.adlittle.com) the Boolean expressions are:

E1 = E2 x E3
E2 = E4 x E5
E3 = E6 x E7
E4 = E8 + E9
E5 = E10 + E53
E6 = E11 + E12
E7 = E13 + E14
E8 = E18 + E54
E10 = E19 + E52
E11 = E15 + E16
E13 = E17 + E30
E15 = E34 x E35
E17 = E38 + E39
E47 = E50 + E51

E18 = E20 x E21
E19 = E26 + E27
E20 = E22 + E23
E21 = E24 + E25
E24 = E28 + E29
E28 = E31 + E55
E31 = E32 + E33
E34 = E36 + E37
E35 = E42 + E43
E38 = E40 + E41
E43 = E44 + E45
E44 = E46 + E47
E46 = E48 + E49
E55 = E56 + E57

The theoretical significance of the level-concept is that a level never can be avoided ("jumping over" or omitted): Once a level is defended (meaning that all the events belonging to the level are defended) then all the higher levels are automatically also defended. Such a device is unknown in traditional fault tree methodology.
In conventional fault tree methodology the main event and the top event are not conceptually distinguished. It is tacitly accepted to be the same.
It is suggested that a risk system (described with a fault tree) with the usual behavior where the top and the main event coincide is to be called "*dominant*" otherwise "*recessive*". It interestingly turns out that recessive risk systems seem to be quite frequent.

4. SOME EXAMPLES OF RECESSIVE RISK SYSTEMS

Reference	**Number of levels**	**Number of events**	**Number of transients**
[Hayes]	3	167	26
[SRS]	3	38	4
NASA	4	315	54

In the cases above common causes has not been taken into consideration.
Common cause problem will be dealt with in a separate paper.

REFERENCES

[Carnap]: Carnap, R.: Logical foundations of probability.
University of Chicago Press, Chicago, 1950

[Harrison]: Harrison, M. A.: Introduction to Switching and Automata Theory.
McGraw-Hill, New York etc. 1965.

[Hayes:] Hayes, K. R.: Final report: Inductive hazard analysis for GMOs
CSIRO Division of Marine Research 2004
http://www.deh.gov.au/settlements/publications/biotechnology/hazard/fault.html

[Henley - Kumamoto]: Henley, E. J., - Kumamoto, H.: Reliability Engineering and Risk Assessment
Prentice Hall, 1981.

[NASA]: Fault Tree Analysis – Apollo 13 incident.
http://drushel.cwru.edu/apollo13/appF-pt4.pdf

[SRS]: The Safety and Reliability Society Symposium. 1989: “Reliability on the Move: Safety and Reliability in Transportation” www.sars.org.uk