THE CASE FOR DIKE RISK

By István Bukovics

A logikai kockázatelmélet alkalmazási területén található kockázati rendszerek állapotát úgynevezett hibafával lehet leírni, viselkedésüket pedig az úgynevezett hibafa-analízissel lehet elemezni[1].

A logikai kockázatelmélet alkalmazási területén található kockázati rendszerek állapotát úgynevezett hibafával lehet leírni, viselkedésüket pedig az úgynevezett hibafa-analízissel lehet elemezni[2]. A hibafa-módszer ma már csaknem félévszázados múltra tekint vissza, ezért jelen kontextusban ismertnek tekintjük. Elméletünk szűkebb, matematikai értelmében a hibafa használata ugyanaz, mint egy Boole függvény használata, amely a rendszert érő valamely nemkívánatos eseményt (pontosabban annak bekövetkezésére vonatkozó kijelentést, állítást) logikai műveletekkel visszavezeti bizonyos egyszerűbb, hatáskörünkben lévő úgynevezett primitív eseményekre. Az, hogy egy kockázati rendszerre vonatkozóan mi minősül nemkívánatosnak teljesen szubjektív megítélés kérdése és az elmélet szempontjából érdektelen.

Introduction

Risk Systems

Intuitively by a „risk system" we mean anything that can be described by fault tree methodology[3] where all probability related notions are omitted (i.e.e. using only the Boolean part).
Formally, by (a model or, rather a description of) a „risk system" we mean an n-element set of Boolean equations of the following form:

$$E_i = C(E_{i_1}, ..., E_{i_{m_i}})$$

Here:

---

[1] Henley
[2] Henley
[3]We suppose the reader is familiar with the basics of fault tree methodology. See e.g. [Henley-Kumamoto], p. 310, Table 7.7 and [Harrison]

Letter **E** means an element – called „event" – of a fixed finite disrributive lattice[4] with *m* atoms, i = 1,…, *n*; m_i = 1,…, *n* with all $i_1,\ldots, i_{mi} > i$ (1)
C is either a conjunction or a disjunction of m_i variables.
$\mathbf{E}_i$ is said to have the logic type „A" („AND") or „V (OR, „Vel")" if it is a conjunction or disjunction respectively.
The system of this equations is usually called *structural equations.*
Events occuring on the right hand sides are called *explicants* of the event of the left hand side.
Events occuring *only* on the right hand sides are called *primitive* events (primevents, prime explicants or just primes for short) and denoted by p.
Events that are not primes are sometimes called *complex* (events).
The *state indicator* of an event can be 0, x , 1 called respectively *passive*, *free* and *active.*

A FORMAL FRAMEWORK

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

$p \wedge (q \wedge r) = (p \wedge q) \wedge r$ and $p \vee (q \vee r) = (p \vee q) \vee r$ (associatiive laws)
$p \wedge q = q \wedge p$ and $p \vee q = q \vee p$ (commutative laws)
$p \wedge (q \vee p) = p$ and $p \vee (q \wedge p) = p$ (absorption laws)
$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$ and $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$ (distributive laws)

It can be proved (see any textbook on lattices) that:
for arbitrary elements p, q, r of **P** U **E**,
$p \wedge p = p$ and $p \vee p = q$ (idempotency)
$p \wedge q = p$ if and only if $p \vee q = q$

The elements E_j of **E** (j = 1 … m, m ≤ 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:

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

[4] Loosely speaking a Boolean algebra without negation
[5] In lattice theory their frequently used names are "infimum – supremum" "meet-unio", while in logic "conjunction - disjunction"

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…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 "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 $p_1... p_n$ be denoted by **p** called a "*state vector*".
If all $p_1... p_n$ is primary we speak of "*primary state*". If all the "E-numbers (value) are given we speak of "*system state* If for a **p**, FT (**p**) = 1 then we say that the risk system, described by the ternary indirect function FT is *active* in the state **p**.
If for a **p**, FT (**p**) = 0 then we say that the risk system, described by the ternary indirect function FT is *passive* in the state **p**.
If for a **p**, FT (**p**) = u then we say that the risk system, described by the ternary indirect function FT is undetermined or *free* in the state **p**.

For any state vectors **p**, **q** we define

$$\mathbf{p} \le \mathbf{q} \text{ if and only if for all } i = 1,\dots,n \; p_i \le q_i,$$

$$\mathbf{p} \ge \mathbf{q} \text{ if and only if } \mathbf{q} \le \mathbf{p}$$

and

$$\mathbf{p} < \mathbf{q} \text{ if and only if } \mathbf{p} \le \mathbf{q} \text{ and } \mathbf{p} \ne \mathbf{q}$$

It follows form the above:

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

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

---

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

Motivations

Although fault tree methodology is the most favourable in risk assesment there are some situations where its usage is problematic or obsolete.
First, there are nonprobabilistic cases where the very notion of probabity is meaningless. (Events, such as terrorist attacs, climatic extremities, unique disasters etc.)
Second, the systematic application of the notion if *state* is missing in fault tree context so the question of „what is the risk of a system *in a given state* ***s*** " makes no sense.
Third, Cutsets and Path sets are clumsy to handle if the number of primes (basic events) is above a hundred. In nonprobabilistic cases smal probability approximation are not applicable, thus one cannot negligate cutsets with small probability.
Fourth, the consequent introduction of the notion of *level* leads to paradoxical results such as that the topevent is not always on the top level. Thus one is deprived from the possibility to defend a risk system using *level defence* see later in the paper.
We attempt to outline an approach to tackle these problems.

The Concept of Level

Let we are given an arbitrary Risk System **RS** according to the definition given in the introduction and let it be fixed henceforward. Let *n*, *m* denote its number of events, and prime events respectively.
Definition:
The 0-level of **RS**, denoted by Level(**RS**) = 0, is the set of all the primevents of **RS**
The 1-level of **RS,** denoted by Level(**RS**) = 1, is the set of all the events with explicants on the 0 level.
The *L*-level of **RS** (*L* = 1,...), denoted by Level(**RS**) = *L,* is the set of all the events with explicants on the L - 1 level but not below.
The maximal level of a RS is denoted by Lmax.
The level of an event e is generally denoted by Level(e).
Definition:
An event of level L is *transient* if it has at least an explicant of level L.
Remark:
It may happen that an event of level L has an explicant of level L + 1 and that event E_1 (usually called “top event”) is at level L < Lmax.

Definition:
An event of level L < Lmax is *hypertransient* if it has an explicant of level > L.
Definition:
A RS is *Dominant* if the level its top event = Lmax, otherwise it is *Recessive*
Defending Level L means that (the disjunction of) all the events on Level L must be passive (in the sense of Boolean algebra).
From now on we speak of level defense only in the case of Level = 1
A minimal set of primes ensuring level 1 defense is called a *Defense set* (of the RS in question)
Remark:
If a set of primes defenses Level 1 then it autoamtivcall akk the highest levels.

Example:

Let the events of level 1 be:
E1 = E2 x E3,
E2 = E4 + E5,
E5 = E6 x E7.
We show, that
E1+E2+E5 = (E4+E6)x(E4+E7).

Drop the event symbol `E`, replace all events by its explicants in:
1+2+5
This is a disjunctive normal form (DNF)
In List form:
(1) 1
(2) 2
(3) 5
Reduce every complex event to primes and use the absorption law:
In (1) E1 is complex: E1 = E2 x E3.
Put (2x3) to (1) and omit parenthesis.
The DNF in the following new list form follows:
(1) 2x3
(2) 2
(3) 5

Here:
2 in (2) absorbs 2x3 in (1) .
After clearing, the new Minterm-list becomes:
(1) 2
(2) 5
In (1) E2 is complex: E2 = E4 + E5.
Put (4+5) to (1) and expand:
(1) (4+5) = 4+5

The DNF in the following new list form follows:
(1) 4
(2) 5
(3) 5

Here:
5 in (3) is repeated in (2) .
After clearing, the new Minterm-list becomes:
(1) 4
(2) 5

In (1) E5 is complex: E5 = E6 x E7.
Put (6x7) to (2) and omit parenthesis.
The DNF in the following new list form follows:
(1) 4
(2) 6x7
By standard Boolean manipulation we get the following CNF with factors (Defense Sets):
(1) 4,6
(2) 4,7

CASE STUDY

The Defense Sets

The Top Event of the Risk System: FLOODING THROUGH DIKE SECTION
LEGEND:
Reference: //www.citg.tudelft.nl/live/binaries/57bf3919-13fb-4577-9b9d-f541a1b0c022/doc/voortman_thesis.pdf
Number of Prime Events = 24
Number of Complex Events = 42
The `Franklin parameters`: Prevention Cost/Prevention Time are measured by an arbitrary (but fixed in advance) unit, say 100% = 100$ where 100% corresponds to the prime event with the highest value of the Franklin parameter.
(The actual data are randomly chosen for the sake of the example.)
`DEFENCE SET` contains the minimal set of prime events (indices) necessary to passivate in order to prevent all the events on level 1.
The fully detailed mathematical derivation of the defense sets and further details are avaible from the author: istvan.bukovics@katved.hu

	Prevention Cost [%] Index = 100	Prevention Time [%] Index = 100	Number of events	DEFENCE SET
1	808,51%	754,26%	16	5,11,12,15,19-21,24,26,27,34,35,37-40
2	864,89%	788,30%	16	6,11,12,15,19-21,24,26,27,34,35,37-40

The Fault Tree

(V): FLOODING THROUGH DIKE SECTION
1(&): INTERNAL EROSION
1.1: piping
1.2: burst of cover layer
2(V): BREACHING THROUGH INNER SLOPE
2.1(&): INNER EROSION
2.1.1: micro instability of inner revetment
2.1.2: uplifting of inner revetment
2.1.3: phreatic line intersects inner slope
2.2(&): SLOPE COATING DAMAGE
2.2.1: erosion of uncovered inner slope
2.2.2(V): COLLAPSE OF INNER REVETMENT
2.2.2.1: erosion of inner revetment
2.2.2.2(V): OVERTOPPING
2.2.2.2.1(V): OVERFLOWING
2.2.2.2.1.1: settlement
2.2.2.2.1.2: foreshore erosion
2.2.2.2.2(V): WAVE OVERTOPPING
2.2.2.2.2.1: settlement
2.2.2.2.2.2: foreshore erosion
2.2.2.3(V): LEAKING
2.2.2.3.1: phreatic line intersects inner slope
2.2.2.3.2: uplifting of inner revetment
2.3(V): INNER EROSION INSTABILITY
2.3.1: erosion of collapsed inner slope
2.3.2(V): MACRO INSTABILITY INNER SLOPE
2.3.2.1: curved slide plane
2.3.2.2: linear slide plane
3(V): BREACHING THROUGH OUTHER SLOPE
3.1(&): OUTER EROSION MACRO INSTABILITY
3.1.1: erosion of collapsed outer slope
3.1.2(V): MACRO INSTABILITY OUTER SLOPE
3.1.2.1: curved slide plane -foreshore erosion
3.1.2.2: linear slide plane- foreshore erosion
3.2(&): DAMAGE OF OUTER SLOPE REVETMENT
3.2.1: erosion of uncovered outer slope
3.2.2(V): COLLAPSE OF OUTER REVETMENT
3.2.2.1(V): REVETMENT DAMAGE
3.2.2.1.1: sliding of revetment
3.2.2.1.2: collapse of toe structure - foreshore erosion
3.2.2.2: uplifting of revetment
3.2.2.3: erosion of revetment

References

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

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

Nievergelt, J. E., ea:
Computer Approaches to Mathematical Problems.
Prentice-Hall, Inc. New Jesey, USA, 1974