NEW HIERARCHY TREE MODEL FOR HANDLING RISK SOURCES

Stoycho STOEV

Abstract

The article offers a version of a model for handling basic sources of potential risk and defines basic components of the structure. From functional point of view are discussed the feasibility for implementation of the model as well as the specifics of setting and conversion of hierarchy tree structure for correct relationship between individual components.

Introduction

The development of modern business processes seeks to optimize economic efficiency. As a part of business ambience risk sources influence to a great degree the process of making business decisions. The risk in general is uncertainty (Chapman, 2003, p.35), and the economy seeks to isolate or avoid unstable environment. In this sense, traditional business processes are increasingly integrated elements of risk management.

The definition of risk management is presented as “coordinated activities to direct and control the Organization of risk” (ISO/IEC Guide'73, 2009, p.2). Successful management of risk implemented in the organization may affect the likelihood and consequences of emerging risks (ISO 31000, 2010, p.10). Therefore, these include benefits associated with better information in decision making, increased operational efficiency, financial reporting, competitive advantage and thus, better market presence.

The goal that we set in this article is to present a new hierarchy tree model for processing the overall risk within the corporeal management in quantification of existing sources of risk in the midst of implementing a software product.

I. The risk as an essential component of contemporary reality

The ISO / IEC 31000 standard discusses the risk (ISO 31000, 2010 as an important factor influencing organizations. It determines the consequences in terms of

---

1 Department of Informatics, University of economics – Varna, Bulgaria. e-mail: s.stoev@ue-varna.bg
economic efficiency and professional reputation, as well as environmental, safety and social performance. Therefore, risk management helps organizations effectively cope with threats in an environment filled with uncertainty. Risk management is a process (Hillson, 2015, p.60), carried out continuously and integrated into the organizational structure of the company. This necessitates the inclusion of separate risk processing activities in the provision of overall corporate information.

Risk management activities are carried out in three main stages (ISACA, 2009, c.9):
- Identification and description of common risk sources into a register;
- Integration in a common model;
- Taking risk-justified business decisions;

In this sense, the role of different models for quantification of individual risks, as well as a logical link between the different elements within the overall risk increases.

Availability and/or the possibility of accidents-events seen in terms of the dynamics of a particular environment (fig.1). We can divide Business environment in two main fields: static and dynamic. In the static section is defined the concept of vulnerability (Astahov, 2010, p.153) which depends on the current state of the system. vulnerabilities in general have been identified as sources of risk and have some quantifiable dimension. In the perspective of the system changes, the sources of risk are defined as hazards. Due to the alleged nature of the amendment, they can hardly be listed in respect of their variance and value.

From an analytical point of view risk vulnerabilities are valuable due to their characteristics (Kerzner, 2009):
- These are recognizable. As part of internal company environment, risk vulnerabilities are components of business processes occurring in the company. Therefore they have the potential to be recognized and assessed.
- Predictable. Unlike the risk hazards that are outside the corporate environment, risk-vulnerability as part of it and hence predictable. Business knows and manages to a greater extent the environment in which it develops.

Fig. 1. Types of sources of risk depending on the environment

From an analytical point of view risk vulnerabilities are valuable due to their characteristics (Kerzner, 2009):
- These are recognizable. As part of internal company environment, risk vulnerabilities are components of business processes occurring in the company. Therefore they have the potential to be recognized and assessed.
- Predictable. Unlike the risk hazards that are outside the corporate environment, risk-vulnerability as part of it and hence predictable. Business knows and manages to a greater extent the environment in which it develops.
Company controlled. The company is able to take preventive measures to reduce risk or respond to the threat of risk occurrence, i.e. business has greater control over the environment.

The organization of the sources of risk in a common system is necessary in terms of its automated processing. The diversity of sources of IT risk involves the use of a complicated system to calculate the overall risk. The main structures used in models of risk management are network and hierarchical ones.

Network structure (Wallace, Keil, Rai, A. 2004) allows building of complex interrelationships between individual risk sources. The major problem is related to the scale of composition. In the realization of networks with large numbers of elements presentation and management of the system are complicated, making it unsuitable for use.

The tree like structure is widely used in risk management. It is implemented in two main trees for analysis: Fault tree analysis, (ISO 31010, 2009, c.61) and Event tree analysis (Hohlov, 2001, p.64).


Complicated pattern of risk sources is proposed by Garvey (Garvey, 2009, p.7), in the system-of-systems hierarchy, which describes the relationship between abstract sets. A system with real components of hierarchy is represented by Mohammad (Mohammad, 1991), where individual subsystems are fixed and it allows flexible inclusion of new components.

In this context, we offer hierarchy tree model distinguished with versatility of the sources of risk and the possibility of practical implementation.

II. Hierarchy tree model for estimation of risk

Construction of a structural diagram of connections between sources of risk to define the requirements that it must meet for the purpose of study:

- We adopt that structural scheme must have a hierarchy nature. This will allow prioritization of risk sources, a clearer link between the components, the relationship between the sources of risk, more easily analyze of different sets of risk, etc..

- The structure reflects a snapshot of risk. That interrupts processes in time to examine the current state of the environment.

- The relationship between two or more components of risk to allow the inclusion of complex logic structures such as averaging, minimization, maximization or exclusion. This would allow not only the aggregation of individual values to obtain a total risk, but degeneration of complex logic model, too.
- Implementation of connection methods to quantify risk factors. Ability to use existing methods for quantifying risk structure for common risk analysis in the project.

We are offering the implementation structural diagram of the connections between the elements of risk to utilize tree like structure, and in particular binary tree. First, it must reflect the interaction of the components two by two, which may be linked to a simplified logical connections and secondly, the hierarchy tree structure data clearly visualize it easily and clearly built as a structure.

Used as basis for the realization of the hierarchy tree structure is one of the options of the binary tree to calculate the mathematical expression (Cormen, Leiserson, Rivest and Clifford, 2002). E.g. the following formula:

\[ f = (a+b) \times c \]

may be represented as binary tree (figure 2). The content of the tree is determined by two main types of nodes: leaves (end nodes without subordinate components) and nodes connected to one or two subordinate components. To calculate the expression in the establishment of the tree, all mathematical operations are expressed as nodes, while variables are end nodes (leaves).

![Figure 2. Schematic presentation of an expression through a binary tree](image)

Therefore, to realize the structure for handling sources of risk, the binary tree must be converted as follows. The leaves are defined as quantifying the various sources of risk, and the remaining units appear connection between them. The risk handling tree versions shown on figure 3.
Fig. 3. Tree structure of the relation between sources of risk

Where $R_{all}$ is the overall risk as a result of the links between all nodes in the tree.

To scan binary tree is used a recursive algorithm (Davis and Olson, 1988). For calculation under PostOrder method (left-right-root). In the logic of the code it is assumed that the left and right unit are valuable, but the root is a logical function to connect the two values (figure 4).

Fig. 4. PostOrder sequence of getting about the tree
In cases where the two subordinate nodes are also logical, i.e. a function, the result of which is also a numerical value and can be interpreted as a sheet node (i.e. a source of risk). The difference in calculating the part of the tree or the entire structure depends on what unit is passed as a parameter to the algorithm.

III. Key elements of the tree

Innovation in the proposed structure is hierarchical differentiation of all elements into two basic types (i.e. the elements of the tree are not homogeneous and are divided functionally):

1. **Information elements.** Nodes containing a specific value for a particular source of risk. As a medium (information carrier) they contain information on the nature of the source of risk, its quantification and other features.

2. **Multiplexer.** The general definition of a multiplexer is “Combinational logic with two types of inputs and one output, which provides connectivity to multiple sources of signal to a receiver”. In its function there are connecting nodes, hierarchically at least one level above the leaves and their role is to afford to build more complex logic between subordinate units.

   We divide multiplexers in two main groups (figure 5):

   1. Realized simpler logic or processing such as addition, subtraction, averaging, getting larger or smaller of the two input values, etc..

   2. Realizing specific logic. That makes it possible to implement complex algorithms to calculate the incoming data, including indirect contact with other nodes of the hierarchy tree.

![Fig. 5. Connection between information nodes and multiplexers](image)
Figure 5 illustrates an example of a risk tree with four information nodes R11, R12, R21 and R22, connected through the multiplexers M1 and M2.

More specific is the Rall node, which is the root of the tree and through it will be derived total value of the risk model.

IV. Potential for using the model

The versatility of the model is presented through the implementation of several key features:

- **Multiplication of nodes.**
  In some of the options for structuring the sources of risk it is possible for a single source to influence the overall risk in different branches of the hierarchy tree (Figure 6). The model defines the possibility of replication in different branches of the tree associated with various elements of risk and varying weight of quantification.

  ![Fig. 6. Multiplied impact of the source of risk](image)

- **Decomposition of tree like structure for analysis.**
  The model allows to calculate the total risk, with the exclusion of certain areas of the hierarchy tree structure (Figure 7). This allows a detailed investigation of the influence of the sources of risk and changing the weight of various elements.
If the tree is built of separate branches of homogeneous sources of risk affecting the environment, the exclusion of individual branches will allow:

- On the one hand, the aim is for the specific medium to determine the influence of only one part of the tree.
- On the other hand, a separate source of risk can be included dependless of risk management level – a common structure.

Figure 8 shows the three main phases in the model for calculating and managing risk sources. At the first phase “information analysis” is carried out selection of significant sources of risk and building the tree. At the second stage are calibrated tree components. At the third phase is carried out assessment of the sources of risk in specific environments through expert analysis. Information obtained is transformed in reverse direction into a tree and at phase 1 are carried out the necessary analyzes.
V. Model specifics

In the implementation of the model attention should be paid to several key issues related to its normal functioning. We emphasize on the following specifics:

- **Range of values for a single source of risk.** Operation of model requests for appropriate definition of limits of change of each source of risk. On the one hand it allows controlling the correctness of submitted data and on the other helped to determine the quantitative intervals nodes-multiplexers or overall risk. All values set in the tree are virtually non-negative in the range \([0..1]\).

- **We define the requirements to the structure of tree.** The logical functionality of the tree is subject to the following rules:
  
  A. Each multiplexer must be connected with two sources of risk, that is to have filled his links. This allows the multiplexer to fulfill its tasks. Otherwise it leads to expression without specific result (\(x=y+\ldots\)).
  
  B. The concept model suggests the possibility of an end node (source of risk) connected to the subordinate units. That is, there are two nodes without multiplexer to connect them. The point is to avoid expression without a mathematical operation between them (\(x=yz\)).

- **Methods for estimation of the overall risk.** For the possible values for the risk, as has been mentioned, is considered the plurality of 0 to 1 (or 0 to 100%). In the implementation of more complex tree structures it leads to unnecessary complication of the process of their construction. In fact, the problem consists not in determining the lower limit of risk, it should always be 0, but rather to set the maximum possible value for risk. We come to the conclusion for two versions of defining the range of possible values for total risk.
  
  A. **Standard method.** In this method, the overall risk ranges from 0 to 1. To achieve this target, the range of each source of risk is set in a manner in which the calculation of the overall risk does not exceed 1. Although this method is generally accepted to represent the values of the risk, in a developed hierarchical structure with the increase of the number of leaves in the tree, the method is complicated.
  
  B. **Equated method.** Another possible method is the one of equivalent limits of the value of the overall risk. The basis of the method lies in the preparation to identify possible ranges. In two steps, based on the minimum and maximum values for each source of risk, are calculated both limits for the overall risk of the entire tree. The upper limit is assumed to be 100 percent risk and in future processing of the total risk it is equated to it. For example, if for the calculated interval \((0.23..1.34)\) for certain values of the leaves we get 1.139, this percentage of the overall risk can be presented
as $1,139 / 1.34 = 0.85$ or 85%. This method, although the need for preparation, facilitates the construction of more complex hierarchical structures.

- **Import of structures.** Tree like structure allows easy importing partial or entirely external structure to the current one in order to realize a more complex model of the environment. In Figure 9 are demonstrated the steps of connecting the two structures. At the first stage – the root of the second structure (total risk) is reorganized with desired multiplexer, then at the second step the selected source of risk for the first tree is replaced with all second structure.

- **Tracking of risk values in time.** Tree like structure accepts values and allows for calculation of overall risk at different time points (Figure 10). Each filling of the structure represents the instantaneous impact of risk factors in the middle of the given time.

![Fig. 9. Importing an external structure](image)

Time sections of the sources of risk are specific risk vulnerabilities of the environment. Modifications to the common or individual risks are tested in an environment of defined time points or in different specific media in the process of realization of the product. Changed values vary between the minimum and maximum possible limit for individual tested model parameters.

**VI. Conclusion**

The proposed hierarchy tree structure for handling sources of risk is a real alternative to existing models. Tree like structure offers a flexible approach to implement logic suitable for a particular business entity and is also suitable for applying different techniques for analysis of results.
The purpose of the model is to offer a logical foundation for the realization of software for automating processes for risk management.

**End Notes**

1. The importance of risk management is also emphasized in NIST (2002), p. 4.
2. Astakhov accepts that vulnerabilities do not cause direct loss of assets, yet under certain conditions that may represent prerequisites for damages originating from the risk.

**References**


