MONTENEGRIN JOURNAL OF ECONOMICS, Vol. 9, No. 3 (July 2013), 75-94

RISK ASSESSMENT MODEL RESPECTING SEGMENTS OF THE PUBLIC

BORUT JEREB[1]

Abstract

The paper describes a broader and more detailed approach to the risk assessment model. The author's assumption is that risk is ultimately an attribute of human beings and not of things or concepts. Therefore, system processes (e.g. a model of business processes), as well as input and output and the public are divided into segments, reflecting the complexity of reality more accurately. The approach is described as sufficiently general to allow for its direct application in a large range of simulation approaches and tools.

The parameters can be used to define individual processes by using their states for representing the accumulated history of the past processes life cycles. The model includes the functions that calculate new values of parameters and output on the basis of the given input. Based on the provided tolerance levels for risks, impacts, and process parameters, the model determines whether these levels are acceptable for each defined segment of the public. The model assumes that parameters, functions and levels are non-deterministic, i.e. parameters, functions and levels may change in time.

Keywords: *Risk Management, Public, Modelling, Simulation, Business Process*

1. INTRODUCTION

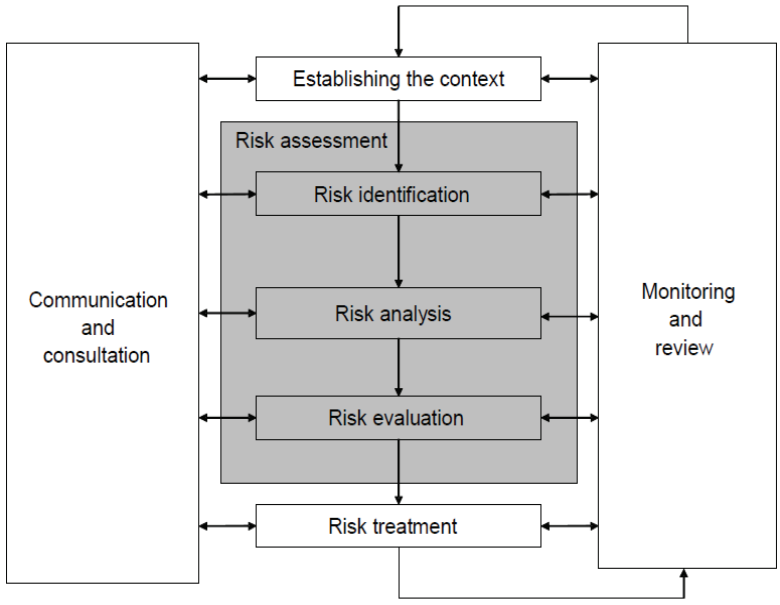
Risks are an integral part of our lives and it appears that people have never devoted as much attention to the challenges of risks as we do today. Risks are addressed by numerous articles, comments, and conversations. Perhaps expectedly, there are virtually countless conceptions and definitions of the term "risk". Even if a particular community agrees upon a single definition of risk, it is still anything but certain that such a community will reach uniform opinions or answers to questions such as [3], [19], [20], [22], [25]: How to perceive risks? How to measure them? Which risks are we most exposed to in a given moment? What are the consequences of exposure to risks – what is the impact of risks? Which risks are acceptable and to which magnitude or extent? Who are the risks acceptable to and who are they not acceptable to? How do risks change in time? What is their impact when observed individually and when taken together? What is their mutual effect and what are the consequences of these interactions? How should risks be managed? How to assess the amount of assets required to reduce, or eliminate the risks? The myriad of questions that have remained unanswered to this day points to the complexity of the problem imposed when one contemplates on a quest to address and manage the risks in a comprehensive manner.

ISO 31000:2009 establishes a number of principles that need to be implemented to make the risk management efficient [14]. A risk assessment as the key activity of the risk management is the overall process of the risk identification, the risk analysis and the risk evaluation [15] (see Figure 1). It is the topic of this paper and it requires a multidisciplinary approach since risk may cover a wide range of causes and consequences.

Despite the decade-long history of contesting views on the relations between the terms risk, uncertainty, probability, risk exposure, and risk impacts, technical science, engineering, economics, etc., employ a simplified approach where risk models predominantly, or even exclusively, use the probability distributions of risk, while failing to account for their diverse dependence on the environment.

[1] University of Maribor, Faculty of logistics Celje, Slovenia

Figure 1: Contribution of a risk assessment to the risk management process (ISO 31000)



Segments of the public are groups of people that have been identified by their current interest in, attitude to, or current behavior around, a particular issue, representing the most important part of the environment which is considered in risk management. Such an approach in which segments of the public play the central role in risk management is new in scientific technically oriented literature.

As every human being is unique, different from all others, our relations to a certain risk encountered with regards to a particular situation can also differ greatly. Hence, people have a different view on and a relation to the same risk, which may be a result of different exposure as well as of different levels of uncertainty. The problem is most commonly addressed not in relation to individuals, but in relation to groups of people, i.e. segments of the public that share a common stance with regard to a particular risk.

In scientific literature, as well as in practice, it is quite common to address risks as something intrinsic to any object, even inanimate, although only humans have the capacity of self-awareness. In his article, Glyn A. Holton [8] addresses the question of the level at which risk is actually taken: can an organization actually be at risk, or is it in fact the individuals, i.e. the employees, who are the risk takers. In this context, they can either be regarded as individuals or as a specific segment of the public, within the organization. It should be widely accepted as a fact that in case of an undesirable event, an incident, a crisis, or a disaster, every community (segment of the public) generally bears its own level of risk. If we concede that only humans have the capacity to be at risk, the ensuing question is: "Whose risk is being managed?" [8] Perhaps all that is needed is a risk model that would account for the specificity of a particular segment of the public – given that risk is exclusively in the domain of people.

Another currently relevant area dealing with the accounting for and inclusion of "uncertainty" and "exposure" in risk models seems to open up. Namely, such inclusion becomes particularly complex as soon as one accepts the fact that risks can predominantly be taken by segments of the public which are generally specific risk takers – each segment of the public (or each person) is at specific risks; hence, we are dealing with specific uncertainty and exposure in case of each individual segment of the public.

In the following step, we can ask ourselves whether the current risk models adequately account for the state of the environment in general (including a wide variety of public) which is comprised by such models, and in which past facts (as the result of past events and actions) are accumulated, which are intrinsic to the observed system and affect the state in the current mo-

ment. Do they at the very least account for the current environmental impact? The models predominantly employed in scientific literature or in practice include a considerable degree of simplification and generalization. Quite expectedly so, since without simplification and generalization, there would hardly be a single practically useful model created. In this case, we are dealing with the development which, if successful, always begins with simplification.

An approach considering the state of environment requires more complex modelling and risk management, thereby earning more trust of individuals involved in risk assessment activities than of top-ranking officials. Thus, governance is significantly improved – the model is attributed its importance, which has been confirmed by the results of surveys conducted during the implementation of risk assessment activities in organizations.

On the other hand, risks should be understood in order to be identified or perceived. We should be able to assess and measure their impacts, to monitor them, and ultimately, to manage them. In recent decades, the latter activity – i.e. risk management – has increasingly employed simulations [4], the reason being that in practice risks include the use of highly complex models [21], in which particular risks, in addition to their mutual interdependence, also depend on the environmental parameters of system processes.

This paper describes an integrated risk model that takes into account the aspects of risk at which segments of the public are considered and consequently, new areas of risk management are identified. The aim is not quantification, but to break ground for future quantitative models. Our study is based on the risk management models described in the most important "risk" ISO standards [14], [15] and [17].

The rest of the paper is organized, as follows: Chapter two describes the problem of the risk definition, which is crucial for understanding the design principle of the proposed models. The third chapter describes the proposed principles to build a model considering segments of the public. Contribution completes the final section and appendix contains mathematical formulas, which are the basis for the construction of a model of risk assessment.

2. WHAT IS RISK? – THE PROBLEM OF RISK DEFINITIONS

The term *risk* is used in many spheres of our lives. We all believe to understand its meaning, yet there are numerous different interpretations. Some are listed in the following Internet references [4], [10], [11], [12]. Each field tends to interpret it in its own way: even within a single field, opinions often clash on various interpretations and even in an individual case, views on the risk arise that are often different and even opposing. The only conclusion that appears beyond debate is that *risk* and *probability* are two inseparable terms. When addressing the former, the latter is always included in the discussion; the reverse, needless to say, is not true.

In principle at least, there also appears to be some level of consent as to what one can do about risks. They can be avoided, reduced, accepted as they are, or even transferred to others (e.g. to an insurance company). Each field forms its own definition of risks, or assumes the existing one. These definitions are not perfect, since one deals with a complex term – and the very number of different definitions is evidence underpinning this assertion. The use of respective definitions that tend to reduce the complexity of risks is inevitable for exact scientific disciplines, as they are the only way to enable the use of the concept, i.e. to operationalize it. On the other hand, risks attract interest and the issues around them are currently very relevant. A number of people deal with risk management methods for analyzing and managing risks, such as VaR [31], SARA [24], which are increasingly more complex and which include increasingly more risk properties or parameters. Standards have been defined and risk management frameworks have been established. Some of them are: AS/NZ 4360 [1], ISO 31000:2009 [14] and ISO/IEC 31010:2009 [15], ISO/IEC 27005:2011 [17], The Risk IT Framework [13].

Recently, the quest for a definition of risk has lead to a point when experts at the international institution ISO could not reach an agreement on some of the key terms that define risk – and thus to define risk itself. Hence, the standard ISO/IEC 27005:2008 Information technology – Security techniques – Information security risk management [16]lacks the precise definition of terms such as threat, vulnerability, probability of an occurrence, and, last but not least, risk. Soon

after the publication of this standard, Steven J. Ross [27] published an article paying attention to this problem. Terje Aven points on the similar problem of risk management terminology in ISO 31000 standard [30], where he says: “The frameworks are, for instance, unclear about the meaning and understanding of fundamental concepts, including risk and probabilities.”

Thus, the main question that remains to be answered is "what is risk". What is the definition of risk? How does one go about discussing risk, measuring it, and managing it in the absence of an agreement on its definition? According to Mun [23], the terms uncertainty and risk are different, yet related. Risks are the results of uncertainty, something that is undertaken by (or intrinsic to) somebody (or something), as a result of uncertainty. The same author submits that at the beginning, there is always uncertainty and the risks related to it, and that through time in which certain actions and events take place, these risks turn to facts. Furthermore, this author asserts that one can also encounter uncertainty that does not involve risk at all. This is described in the case of an airplane coming down to a certain crash, with only two passengers and one old parachute the functioning of which is doubtful at best. Both passengers are faced with the same uncertainty as to whether the parachute will open or not. If the object of uncertainty is the old parachute and the two passengers agree upon who will use it, then the person to use the parachute will assume the entire risk related to opening of the parachute from the moment he/she jumps out of the airplane until the very moment when he/she pulls the string and the parachute either opens or not. Meanwhile, the second person, having agreed not to use the parachute, does not assume any risk with regard to the functioning of the parachute; at the same time, the second person is also quite certain to die.

According to Holton [8], risk includes only two essential components:

a) *uncertainty* and
b) *exposure*.

Uncertainty and exposure are, however, the most difficult concepts to define and account for. This paper shall henceforth employ Holton's definition. As such, this definition may fundamentally challenge the currently prevailing view on risks and the way they are addressed. The following example may clarify the issue. A bridge as a building does not undertake any risk, regardless of how poorly it may be built. Risks are only taken by stakeholders (people) related to this bridge in one way or the other. This is important, particularly because the bridge itself does not include a dimension of exposure as it will be defined shortly. Furthermore, the interpretation of uncertainty is assumed by (intrinsic to) the bridge.

To simplify, "a person" can be understood in particular cases either as a natural person (an individual) or a juristic person (a legal entity), although the latter is readily translatable into the specific community, or a group, of natural persons. Furthermore, such simplification soon leads to a dead end. There are very few examples in which only stakeholders in companies and organizations are the exclusive risk takers; rather, the risk also includes employees, stockholders, investors, the local community, etc. Any one of these stakeholders (or any group of them) indulges in their own uncertainty and exposure [8].

Since probability is a constituent part of risk, I shall now briefly address this issue, as well. Knight [7] distinguished between two types of risk:

a) "real or objective risk" which includes logic, probability and statistical methods; and
b) "uncertainty or subjective risk" where the idea of quantifying probability is hardly helpful – when probabilities are defined by individuals based on their beliefs, or when the system of values is established, based on opinions in order to describe their uncertainty.

Hence, it can be said with regard to risk that probability may be used as risk metrics; however, its use may be bounded and deficient. What is missing is the measure of "uncertainty", at least [7]. The problem of uncertainty and subjectivity always arises when we are faced with risk management. This is presented also in the paper of Terje Aven [29], where he argues the presence of subjectivity even in “objective” risks.

2.1 Uncertainty

Uncertainty is a condition when one does not know whether a proposition or an assertion is true or false. Probability is the metrics that is most commonly used to express uncertainty; however, its applicability is bounded. At best, it can assess the uncertainty we are able to perceive.

However, what Knight designates as *risk* (*objective risk* and *subjective risk*) will in this paper be referred to as *uncertainty* (*objective uncertainty* and *subjective uncertainty*) as defined by Holton.

In designing the model this paper proposes the use of the term *uncertainty* as used by Holton. Uncertainty will be further divided according to the Knight's approach. In the following text the following two terms shall be used:

a) objective uncertainty and
b) *subjective uncertainty*.

2.2 Exposure

The litmus test for exposure is "*Would we care?"* [8] In other words, a person is exposed when an event has some material or non-material consequences for that person. People are thus exposed when we care about whether a certain proposition is true or false [8].

We can be exposed to risk and be fully aware of it (balancing on the fence of a high bridge) or not be aware of it at all (balancing on the same fence while sleepwalking). Risk can be taken very seriously (speed limits in a village where a police patrol is always on duty), or act quite indifferently to it (speeding through the village in the middle of the night, knowing that the police patrol is not there and assuming that everyone is asleep). Thus, exposure introduces additional indistinctness, or undefinability, which depends primarily on the individual or a certain segment of the public and its perception of exposure and, consequently, of risk. Hence, we are not only dealing with the problem of metrics of uncertainty (see [6]), but rather with a problem of the metrics of exposure.

2.3 Risk

Risk can be described as exposure to uncertainty, therefore it follows from the above definition of exposure that risk depends on the attitude of persons (segment of the public). Since both uncertainty and exposure are difficult to define, risk is not easily definable, either. As a result, risk is difficult to model. It then follows that it is impossible to operationally define risk in a way that would allow its effective management [8]. At best, individuals and/or communities (the segments of the public) can define their perception of risk, which is mostly highly simplified. For example, a well-known simplified approach is multiplying probability by potential loss. Problems arising from using such a simplified approach are described in Taleb's Black Swan [28] or in Hubbard's The Failure of Risk Management [6].

The rest of this paper is based on the assumption that risk includes the public as a necessarily defined parameter and is composed of:

a) Uncertainty, which should be divided into:
   - Objective uncertainty and
   - Subjective uncertainty;
b) Exposure.

3. PRINCIPLES TO BUILD A MODEL CONSIDERING THE SEGMENTS OF THE PUBLIC

The described model pursues the ambition to be sufficiently general in order to be able to use in various situations and in various fields where risk is encountered – perhaps as suggested by Holton [8], who, in his examples, refers to trading natural gas, launching a new business, military adventures...., as well as romance. Although the model described in this article can be used in a wide array of fields, the example of a business process model is provided in the following subsection.

Depending on the particular field at hand that we wish to model, the importance of a particular part of the model (various public, internal vs. external, dynamic behaviour in time, etc.) may

differ; however, it can seldom happen that an individual part of the model is completely negligible in a particularly used case.

The terms and definitions described in the model in this paper are based on the ISO 31000 [14] and ISO 31010 [15], denoting a high-level model of risk management. In this paper the model is expanded in a way that nothing from the ISO standard is ignored. In the mentioned standard there are many hints indicating the awareness of different public with their own properties, but the idea of the segments of the public (according to their interests) is not used.

The following text in this chapter is focused on those ideas of ours which are different compared to the ISO 31000. More consistent relations between risk, the consequence, the process state, risk, the consequence and the process state criteria (borders of accepting) are described in a mathematical form in the appendix. This theoretical consideration is underpinned by a simple example of a business process using documents. The described model is easy to use in simulations which are mostly employed to optimize processes when a mathematical model is not available (when a mathematical formula is too complex) and we ask ourselves "What if...?"

3.1 Process, its state and time dimension

Business processes are represented by process graphs, i.e. mathematical structures in which the nodes represent a particular process and the link between two nodes represents their relation.

> *Example* Clerk A regularly receives documents of two types: document X and document Y. Upon receipt, clerk A performing the business process A establishes whether documents are adequate for further processing. If any document is not, Clerk A rejects it, producing the explanation Z, including a request for the amendment of the document. If the document is adequate for further processing, it is recorded in Incoming Mail and forwarded to other clerks: type X documents are forwarded to the clerk B, performing the business process B; and type Y documents are forwarded to the clerk C, performing the business process C. Figure 2 illustrates this simplified example of business processes.

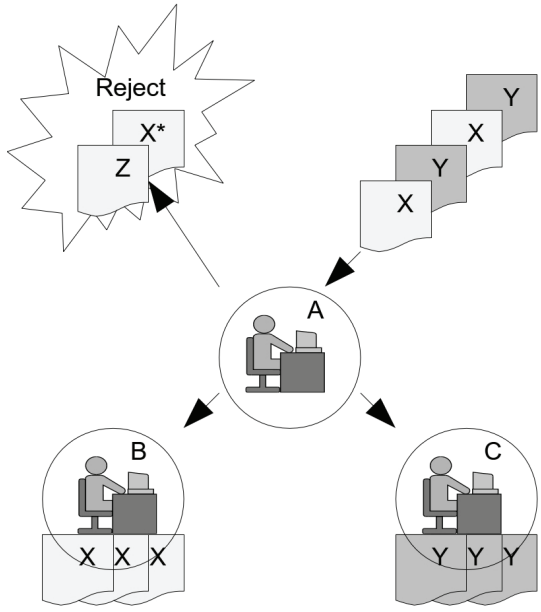
The state of each process is described by parameters – the process state depends on its specific properties which are represented by its parameters. Some examples of such parameters are: process time parameters, the maturity level, sensibility to some types of risks, the period of the year in which its importance may be low or high, the risk acceptance, the impact acceptance, etc. The model does not define what each parameter actually represents, nor does it define the number of parameters.

> *Example* In our business processes example, the process A parameter could be the number of delays involved in forwarding or rejecting any document by the clerk A (the clerk acts later than required by the respective regulations). If the clerk A never makes a mistake, the type X documents are sent to the clerk B. However, the clerk could make a mistake and send a wrong document to the clerk B. A document may also be ambiguous and it may only later become evident that it is of a different type than initially believed by the clerk A. In the first or second case, the document sent to the clerk B is of the wrong type. Within the process B, the number of wrong type documents received can be measured and recorded in a particular parameter of the process B.

The most important aspect of process parameters is that they allow for the past life cycle of each business process to be "accumulated" within them; this accumulated information is then used to accumulate the impacts and new business process parameter values. In this way, modelling also comprises the "history" of the modelled system. These parameters include the accumulated history of past moments and accordingly, the past combinations of risks and other impacts relevant to the business process.

> *Example* In the above example, each individual delay could be insignificant while a number of delays could have adverse consequences. It is, therefore, not only necessary to record individual delays, but also the total sum of all delays. This is an example of an additional process parameter.

Figure 2: A simplified business process in which the clerk A reviews and sorts / classifies the received documents and forwards them to the business processes B (clerk B) and C (clerk C).



The model should include the dimension of time, which introduces non-determinism. In many real situations, some or all processes include the time dimension in their input, output, or in the manner in which the following state of a process is calculated (see the Appendix).

3.2 Internal and external context

In general the external context represents the external environment while the internal context represents the internal environment, in which the organization strives to achieve its objective. See [14] for detailed explanation.

For the sake of simulation possibilities of the model in this paper the "world" of system processes is represented by the combination of all known inputs and outputs. The "world" is the environment in which system processes "live". Processes in the "world" depend on the stream of inputs – resources of any kind (goods, services, information, etc) and their mixture – through them. In their life cycle, they change their own "world" by their output, which, at the same time, is a part of the information stream.

All inputs, outputs, risks, and consequences of a process, and consequently, the entire “known world”, should be segmented into "internal" and into "external". The observed system, composed of processes with all their parameters and mutual "output-input" relationships between processes, defines the internal world, while the external world is defined by everything else. In the model, only risks as part of the external input, and consequences as part of the external output of the observed system processes, are of our interest. See figure 3.

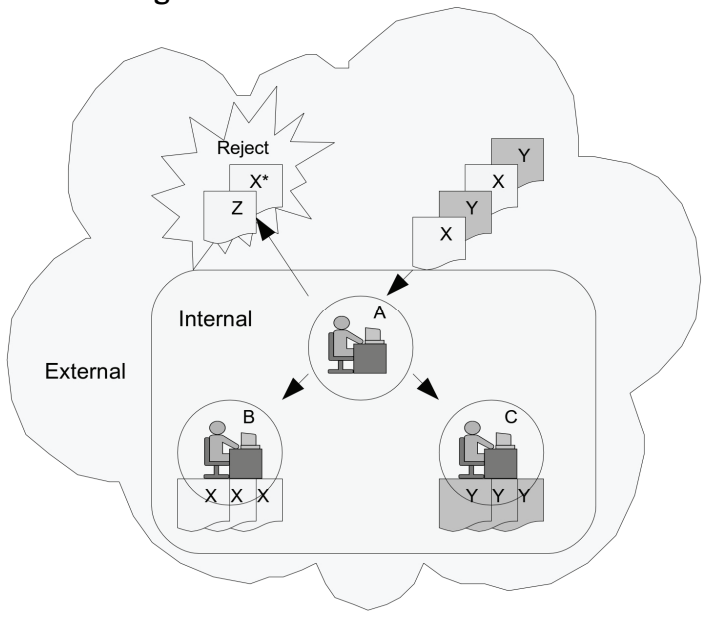
Usually, we do not have the exact knowledge of processes of the external world with all their parameters; however, we do know the input (and risks) from the external world to the observed system, as well as the output (and consequences) sent to the external world from the observed system.

In a real situation, it is difficult or even impossible to have any influence on the external risks entering the observed system; on the other hand, we have the power to minimize or even to avoid the internal risks (which are consequences from yet another process of the system). Consequently, the ability to influence the internal risks (or consequences) is the reason why the internal world should be distinguished from the external one.

Example Let us illustrate this with our business processes example with clerks: the Company has the power to reduce the clerk A's risks related to incorrectly forwarded

documents to the clerks B and C by adopting appropriate internal rules and procedures, thus affecting the internal output (including internal consequences) to some extent. However, the Company has no power over the print quality of the incoming documents; hence, the print quality is an external risk.

Figure 3: Segmentation of inputs and outputs of a system of processes according to whether the origins and terms are internal or external



3.3 Risk

Risks as part of the process input described in (2) are of special interest in risk modelling. Risks cause some kind of (business) loss. The loss is represented by consequences, which, in turn, are parts of the process output described in (3). Risks inevitably cause consequences; however, in addition to risks, consequences also depend on the process state and input in general.

Example One example of two risks in the process described above is arrival of a poorly legible document – perhaps a poor photocopy of the original document. Poor legibility of a document can pose a threat to the correctness of its further processing. The clerk A may confirm such a document as being correct and forward it for further processing; however, it may turn out later in the process that an essential part of this document is illegible or not legible enough to allow for the certainty of its particular contents. This, in turn, can lead to even bigger material or non-material damage with legal consequences. Thus, processing a copy of a document (this can include bad print due to a worn out printer cartridge or toner) always includes an increased risk of damage incurred later in the process. Similarly, damage with legal consequences may result from an unjustified rejection of a document.

In addition, a detailed analysis of the example of risk may lead to a conclusion that misprocessing of the type X documents may cause considerable damage while the damage due to misprocessing of the type Y documents is quite negligible. Hence, in practice, the extent of potential damage would have been determined according to the share of the type X documents and the expected (given the known data from the past) occurrence of misprocessing. The damage thus established represents a consequence of the type X document misprocessing. Meanwhile, the consequence of the type Y document misprocessing is negligible.

As every person is uniquely different from every other person, so can our relations to a certain risk posed with regard to a particular situation also differ greatly. Hence, people have differential views of and relations to the same risk. This may be a result of different exposure, as well

as of different uncertainty. However, this problem is most commonly addressed not in relation to individuals, but in relation to groups of people, i.e. segments of the public who share a common stance with regard to a particular risk.

Risk is defined, according to our approach, by objective and subjective uncertainty and by exposure. All three values are indicators that can not be comprised in one indicator (by multiplication, for example). They should remain the subject of investigation as separate values throughout the whole risk assessment.

Some time ago we tried to combine all three indicators into a single unit and thus created a mess of subjectivity, objectivity and exposure. In addition to this, we tried to unify these indicators among various risk takers. In doing so, we proposed compromises among various stakeholders, which led to the problem of confidence in the used risk model. The problem of the model credibility is one of the chief problems in risk management.

In practice, we have more confidence in calculations of objective than subjective uncertainty, irrespective of the fact that we are faced by relatively small statistical samples. Such a point of view is explained in Hubbard's book [6]. Subjective evaluation poses the problem described by the Prospect Theory [5]. In our practice we were mostly confronted with subjectivity in risk assessment (which consists of the phase of risk identification, risk analysis and evaluation).

Finally, we should compare our approach to the standard, in which it is written, as follows [14]: “Organizations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on organization's objectives is risk.” This definition still does not provide for explicit differentiation between objective and subjective, and there is no word about exposure. But later in the text there are many hints about divergence among various people, between objectiveness and subjectiveness. Further, there are explicit hints [15], for example, expressed in “perceptions and values of external stakeholders” or “the way in which probabilities are to be expressed”, etc. Also [15] explicit awareness of different objective (“reviews of historical data”) and subjective methods (“identify risks by means of a structured set of prompts of questions”) for risk identification is mentioned. The standard identifies qualitative, semi-quantitative or quantitative methods used in risk analyses, it refers to the estimation of risks and consequences – however, there is just a slight awareness of the objective and subjective nature of uncertainty and about exposure, but not an explicit recognition of the risk indicators structure. The standard assumes only likelihood as the one, all-inclusive indicator of uncertainty, but without exposure.

3.4 Consequences

In our model, consequences are calculated with a function with properties similar to the function employed to calculate parameter values (see the Appendix). Function parameters, too, are the same, but the calculation differs. Consequences are the result of combined effects of inputs and internal states of processes, while internal states of a process can also be changed. As we already mentioned above: when a consequence terminates in the system, such a consequence becomes a risk originating in the system in the next period of time and it is of special importance for risk management, because it is within the scope of our influence and target actions.

3.5 Risk Criteria

Furthermore, risk criteria representing acceptance borders should also be defined for risks, impacts, and process states.

Each time the consequence and parameter values are calculated, the calculated values must be compared against the tolerance values for the following:

a) risks that present specific inputs in a particular process,
b) calculated values of particular business process parameters, and
c) values of calculated effects

for each segment of the public, respectively.

If any of the tolerance values is exceeded, the analysis of the causes leading to such a condition should be commenced.

Example For the business process A (see Figure 2) and for all segments of the public it is true that risks and acceptance borders do not change over time. The risks that accompany business processes should be:

a) R_1 – poorly legible received document.
b) R_2 – delays resulting from untimely forwarding or rejection of a document by the clerk A.
c) R_3 – wrong type of the document sent from the clerk A to the clerk B.

The following individual segments of the public have been observed:

a) SJ1 – employees who carry out the business process A.
b) SJ2 – owners of the business process A.
c) SJ3 – users of the business process A.

Objective and subjective uncertainty, exposure and risks have the following set of four values: {Ø – zero value, S – relatively small values, M – middle values, H – relatively high values}. Although we use the same designation of values, they have different implications for uncertainty, exposure and risks. Tables 1 to 3 show values that change in simulations.

Table 4 shows the calculated risks by using a function (see the equation (19) in Appendix for example). In this case the function is simplified in order to calculate risk as the worst option in the Cartesian product between objective and subjective uncertainty, and the exposure.

If the acceptance borders were such that acceptable risks are as described in the table 5, the risk R_3 would be unacceptable to all segments of the public and the risk R_2 would be unacceptable to SJ_2, while the remaining risks are acceptable.

In practice, we need to decide what to do with these risks. If we want to reduce them, it is necessary to take steps towards reducing uncertainty and/or exposure. In a similar way we should calculate and assess the business processes states and the corresponding impacts.

3.6 Other data considered in risk assessment

The other collected data are important, but they are not the topic of this paper. For the sake of completeness they shall be listed, as follows:

a) Resources needed to operate the business process. If this process is the IT process, then we choose among information, application, IT infrastructure and the people responsible to execute the IT process (they are the IT sources); in the case of a logistics process we choose among the flow of goods or services, information, logistics infrastructure and suprastructure and people (they are logistic sources), etc. Any risk, occurring in an observed process, can have an effect on one or more of these sources.
b) The nature or type of goods or materials (flammable or frozen materials, for example) needed in the life cycle of a business process in order to produce the process output, which is a product or service.
c) Segments of the public. These public are risk takers (for example: owners, employees, management, union representatives, residents in the 20km-circle around the nuclear plant, etc).
d) The level at which risk arises. Usually we distinguish between business and technological levels, but sometimes we introduce intermediate levels. These levels are usually in connection with one or more specific segments of the public. There are four levels proposed as example [26].

4. CONCLUSION

Risk management is a process aimed at enhancement and development of the security level in an organization. It gives the organization a broad view on the risks that can affect its productivity and performance, thus enabling it to make appropriate risk management decisions. The knowledge of risks to which an organization is exposed, of the reasons that caused their occur-

rence, and of the effects that are caused by them, is of vital importance for any organization aiming at protecting itself from the risks, or avoiding them altogether.

Organizations need tools to handle risks; these tools should be easy to use and inexpensive. Most commonly, organizations use simulations of models of their own business. This approach is relatively easy to employ and it is also rather inexpensive provided the organization has already established a framework for making ongoing assessment and simulations. Establishing such a framework demands relatively high investments, also into building a model, as the outcome of the simulations. A fair model is a prerequisite for the success of the entire story of risk management following successful simulations.

The proposed model of risk assumes several dimensions that should be accounted for in a simulation. There are probably some instances of models in which one or another dimension was taken into account, or perhaps even some that account for all the dimensions proposed in the article; however, the review of the scientific literature did not prove the examples of this kind providing for such a model in an intelligible way.

The model is complex, yet still constructed in such a way that it allows for omitting a particular dimension defined by the segmentation. Thus, it can be simplified to the level of commonly used models.

In reality, the process of building a model of complex tasks with all the relations is usually too complex a problem to create the final model in just a few steps or even in one single step. Building the model means to adapt the model many times through time, making it more precise and useful by adding more knowledge about its input and rules defined by the functions, calculating impacts and process states.

The approach at which first knowledge is collected about input, output, risks and consequences, internal and external ones, followed by the calculation of the consequences, from the level of processes to the level of the whole system of processes, by means of parameters (which define the states) and functions, is a bottom-up approach. In many situations in real process modelling we strive to gather as much possible as knowledge about the system of the observed processes, even if only approximate at the first step. Later, step by step, we build more precise and hopefully better models in cycles of collecting additional knowledge of inputs, outputs, risks, impacts, parameters, and the knowledge about the function that calculates the impacts of processes. All new knowledge should be segmented as in the first step. Such an approach is a top-down approach.

However, segmentation is obviously required to set up a model that can be used for simulations, and it does not matter which approach (top-down or bottom-up) is chosen. Working on both approaches together gives us the best results in the shortest time span. According to our experience, the top-down approach is more effective for programming, expanding, or changing the database of knowledge (or rules) about the model.

Without any influence to generalization, the model should be resized from the level of processes to the level of activities or even to the level of particular tasks. However, this paper remains focused on the level of processes.

The model is fairly easy to use with simulation languages, such as GPSS [9]; the main problem, however, remains the definition of risks, particularly when the model is intended to be used in its entirety, i.e. including all the dimensions provided. Hence, the model once again brings about the situation in which we have the tools, but we lack the real knowledge and capacity to make full use of them. The field of risk management may well have developed to a level at which it requires a special kind of experts to solve the most intricate problems. Risk management, on the other hand, requires another type of experts. At today's level of development, risk managers can probably manage the risk models as well, if they are provided with the relevant information on risks and their properties.

Appendix

Process Outline

In this paper, business processes are represented by process graphs, i.e. mathematical structures in which the nodes represent a particular process and the link between two nodes represents their relation.

The Process graph *PG* is defined as a directed graph [2]:

$$PG = \{P, E\} = \{P, (P_k, P_l), (P_m, P_n) \ldots (P_q, P_r)\}; \quad k,l,m,n,q,r = \{1,2,3,\ldots,|PG|\} \tag{1}$$

where *P* represents a set of resources of any kind (goods, services, information, etc) and their mixture; *E* represents a set of edges representing the flow of any kind of resources, in which particular processes from *P* are the sources and destinations, respectively, of such flows. *E* is a set of ordered pairs, in which the pair (P_x, P_y) is considered to be directed from the process P_x to the process P_y. It represents the output resources flow for the process P_x and the input resources flow for the process P_y. Each pair (P_x, P_y) represents the information on the mutual relationship between the process P_x and P_y. P_x is a direct predecessor of P_y and vice versa, P_y is a direct successor of P_x. In our model, both *P* and *E* are finite sets.

The behavior of the process P_k is influenced by its input denoted by *Input*(P_k). The output of the process P_k is denoted by *Output*(P_k) and it is generated according to the following items:

a) its current status (or state in which the process is),
b) its current input, and
c) the rules for generating the output according to the status and input.

Calculation of the process states described by parameters is further explained in the paper.

The definitions of the process P_k input and output are, as follows:

$$Input(P_k) = \{(P_x, P_k)\} = \{Inp_{k,1}, Inp_{k,2}, \ldots, Inp_{k,n}\} \tag{2}$$

$$Output(P_k) = \{(P_k, P_y)\} = \{Out_{k,1}, Out_{k,2}, \ldots, Out_{k,n}\} \tag{3}$$

Introducing time and the process state

The state of the process P_k is described by the following equation [2]:

$$State(P_k, t) = \{Par_{k,1}(t), Par_{k,2}(t), \ldots, Par_{k,m}(t)\} \tag{4}$$

In which $Par_{k,x}(t)$ denotes the value of the parameter *x* of the process P_k in time *t*.

In addition, there is the function Φ_{SC} that calculates new values of the process parameters (i.e. the new state) in each discrete (temporal) moment, based on:

a) Business process input *Input*(P_k,*t*);
b) Current values of business process parameters *State*(P_k,*t*).

$$State(P_k, t + \Delta) = \Phi_{SC}\begin{pmatrix} Input(P_k, t), \\ State(P_k, t) \end{pmatrix} \tag{5}$$

Equation (4) represents the state of the process P_k, which is changing through time. In the case of discrete simulation, the new state of the P_k is evaluated for every single time slice Δ by the function Φ_{SC}, which calculates new states as represented by the equation (5). The *State*(P_k, *t*)

comprises all accumulated influences spread from P_k in the future. These influences are based on the past combinations of inputs and states of the P_k. In other words: it represents a kind of accumulated history of the P_k, that could be reflected in the future by generated impacts.

In the above explained equations we still do not consider the following described segmentations including the risks and segments of the public.

Risk

In this subsection we still do not consider the segments of the public. They are topic of the next subsection, in which the most important equations are repeated.

According to the definition of risks it follows:

$$Risk(P_k,t) \subseteq Input(P_k,t) \tag{6}$$

General input in time t of the process P_k is denoted by $GeneralInput(P_k,t)$ and is defined as:

$$GeneralInput(P_k,t) = Input(P_k,t) - Risk(P_k,t) \tag{7}$$

If risk is exposure to uncertainty and if uncertainty is divided into the objective and subjective uncertainty as described above, the set of risks of the process P_k in the proposed model is the set of threesome vectors and it is denoted by $Risk(P_k,t)$:

$$\begin{aligned} Risk(P_k,t) &= \{R_{k,1}(t), R_{k,2}(t),\ldots, R_{k,m}(t)\} = \\ &\left\{\begin{array}{l} (Uncertainty_{k,1}(t), Exposure_{k,1}(t)), \\ (Uncertainty_{k,2}(t), Exposure_{k,2}(t)), \\ \ldots, \\ (Uncertainty_{k,m}(t), Exposure_{k,m}(t)) \end{array}\right\} = \\ &\left\{\begin{array}{l} (ObjUncertainty_{k,1}(t), SubUncertainty_{k,1}(t), Exposure_{k,1}(t)), \\ (ObjUncertainty_{k,2}(t), SubUncertainty_{k,2}(t), Exposure_{k,2}(t)), \\ \ldots, \\ (ObjUncertainty_{k,m}(t), SubUncertainty_{k,m}(t), Exposure_{k,m}(t)) \end{array}\right\} \end{aligned} \tag{8}$$

If the sets of objective uncertainty, subjective uncertainty and exposure are expressed as:

$$\begin{aligned} &ObjUncertainty(P_k,t) = \\ &\{ObjUncertainty_{k,1}(t), ObjUncertainty_{k,2}(t),\ldots, ObjUncertainty_{k,m}(t)\} \end{aligned} \tag{9}$$

$$\begin{aligned} &SubUncertainty(P_k,t) = \\ &\{SubUncertainty_{k,1}(t), SubUncertainty_{k,2}(t),\ldots, OubUncertainty_{k,m}(t)\} \end{aligned} \tag{10}$$

$$\begin{aligned} &Exposure(P_k,t) = \\ &\{Exposure_{k,1}(t), Exposure_{k,2}(t),\ldots, Exposure_{k,m}(t)\} \end{aligned} \tag{11}$$

then the function Φ_{RC} of risk calculating should be written as:

$$Risk(P_k,t) = \Phi_{RC}\begin{pmatrix} ObjUncertainty(P_k,t), \\ SubUncertainty(P_k,t), \\ Exposure(P_k,t) \end{pmatrix} \quad (12)$$

Whereby in (8) and (12):

a) P_k is process *k*.
b) *ObjUncertainty* (P_k, *t*) is objective uncertainty in the process P_k at time *t*.
c) Sub*Uncertainty* (P_k, *t*) is subjective uncertainty in the process P_k at time *t*.
d) *Exposure* (P_k , *t*) is exposure in the process P_k at time *t*.
e) Particular risks for the process P_k are represented by a set of m risks {$R_{k,1}$ (*t*), $R_{k,2}$ (*t*), ..., $R_{k,m}$ (*t*)} at time *t*.
f) Function Φ_{RC} calculates risks.

Consequences

According to the definition of consequences (impacts), regardless of segment of the public parameter it follows:

$$Consequence(P_k,t) \subseteq Output(P_k,t) \quad (13)$$

General output of a process P_k at time *t* is denoted by *GeneralOutput*(P_k,*t*) and it is defined as:

$$GeneralOutput(P_k,t) = Output(P_k,t) - Consequence(P_k,t) \quad (14)$$

Consequences are represented as a set:

$$Consequence(P_k,t) = \{C_{k,1}(t), C_{k,2}(t), \ldots, C_{k,m}(t)\} \quad (15)$$

Consequence is again calculated with a function with properties similar to the function employed to calculate parameter values. Function parameters, too, are the same; only the calculation differs.

The function Φ_{CC} calculates the consequences by applying the output generation rules, for a given combination of *Input* (P_k, *t*) and *State* (P_k, *t*). The set of consequences of the process P_k is denoted by *Consequence* (P_k, *t*) and it is calculated for every time slice Δ, as follows:

$$Consequence(P_k,t+\Delta) = \Phi_{CC}\begin{pmatrix} Input(P_k,t), \\ State(P_k,t) \end{pmatrix} = \Phi_{CC}\begin{pmatrix} Risk(P_k,t), \\ GeneralInput(P_k,t), \\ State(P_k,t) \end{pmatrix} \quad (16)$$

Considering (5) and (16), consequences should also be calculated as:

$$Consequence(P_k, t+\Delta) = \Phi_{CC}\begin{pmatrix} Risk(P_k, t), \\ GeneralInput(P_k, t), \\ \Phi_{SC}\begin{pmatrix} Input(P_k, t-\Delta), \\ State(P_k, t-\Delta) \end{pmatrix} \end{pmatrix} \quad (17)$$

	SJ_1	SJ_2	SJ_3
R_1	S	S	Ø
R_2	M	M	Ø
R_3	S	S	Ø

Table 1: Objective uncertainty as to the individual risk and segment of the public.

	SJ_1	SJ_2	SJ_3
R_1	Ø	S	S
R_2	Ø	H	H
R_3	Ø	M	H

Table 2: Subjective uncertainty as to the individual risk and segment of the public.

	SJ_1	SJ_2	SJ_3
R_1	S	M	S
R_2	S	M	H
R_3	M	H	H

Table 3: Exposure to the individual risk and segment of the public.

	SJ_1	SJ_2	SJ_3
R_1	S	M	S
R_2	M	H	H
R_3	M	H	H

Table 4: Calculated risks for an individual segment of the public.

	SJ_1	SJ_2	SJ_3
R_1	S,M	S,M	S,M
R_2	S,M	S,M	S,M,H
R_3	S	S	S,M

Table 5: Accepted risks for an individual segment of the public.

As presented in the equation (17), the consequence following this moment (the time of observing the *PG*), denoted by *Consequence(P_k, t+Δ),* depends on the following:

a) *Input(P_k, t)* which is composed of:
   - *Risk(P_k, t)* and
   - *GeneralInput(P_k, t)*;

b) *State(P_k, t)* composed of:
   - *Input(P_k, t-Δ)* and
   - *State(P_k, t-Δ)*

c) Functions Φ_{CC} and Φ_{SC}.

Segmenting by taking into account public segmentation

Simulations should be conducted for each segment of the public separately. The given view adopted throughout this article, however, justifies the calculation of risk, impact and process states for each particular segment of the public.

In (7) *GeneralInput* of the process P_k does not depend on a segment of the public. General input does not include exposure or uncertainty – it is just data. However, for the sake of generality, it should depend on a segment of the public regardless that it is the same for all public. According to this approach the equation (7) should be expressed as:

$$\begin{aligned} &GeneralInput(P_k, Public_l, t) = \\ &Input(P_k, Public_l, t) - Risk(P_k, Public_l, t) \end{aligned} \tag{18}$$

The equation (12) for calculating risks conducting the segment of the public is expressed as:

$$\begin{aligned} &Risk(P_k, Public_l, t) = \\ &\Phi_{RC}\begin{pmatrix} Uncertainty(P_k, Public_l, t), \\ Exposure(P_k, Public_l, t) \end{pmatrix} = \\ &\Phi_{RC}\begin{pmatrix} ObjUncertainty(P_k, Public_l, t), \\ SubUncertainty(P_k, Public_l, t), \\ Exposure(P_k, Public_l, t) \end{pmatrix} \end{aligned} \tag{19}$$

The equation (5) for calculating processes considering (18) the state conducting the segment of the public and segmenting input to risks, uncertainty and exposure (see (19)) is:

$$\begin{aligned} &State(P_k, Public_l, t+\Delta) = \\ &\Phi_{SC}\begin{pmatrix} Input(P_k, Public_l, t), \\ State(P_k, Public_l, t) \end{pmatrix} = \\ &\Phi_{SC}\begin{pmatrix} Risk(P_k, Public_l, t), \\ GeneralInput(P_k, Public_l, t), \\ State(P_k, Public_l, t) \end{pmatrix} = \\ &\Phi_{SC}\begin{pmatrix} \Phi_{RC}\begin{pmatrix} ObjUncertainty(P_k, Public_l, t), \\ SubUncertainty(P_k, Public_l, t), \\ Exposure(P_k, Public_l, t) \end{pmatrix}, \\ GeneralInput(P_k, Public_l, t), \\ State(P_k, Public_l, t) \end{pmatrix} \end{aligned} \tag{20}$$

The equation (16) for calculating consequences, considering (19), (20) and conducting segments of the public, is:

$$\begin{aligned} &Consequence\left(P_k, Public_l, t+\Delta\right) = \\ &\Phi_{IC}\begin{pmatrix} Input\left(P_k, Public_l, t\right), \\ State\left(P_k, Public_l, t\right) \end{pmatrix} = \\ &\Phi_{CC}\begin{pmatrix} Risk\left(P_k, Public_l, t\right), \\ GeneralInput\left(P_k, Public_l, t\right), \\ State\left(P_k, Public_l, t\right) \end{pmatrix} = \\ &\Phi_{CC}\begin{pmatrix} \Phi_{RC}\begin{pmatrix} ObjUncertainty\left(P_k, Public_l, t\right), \\ SubUncertainty\left(P_k, Public_l, t\right), \\ Exposure\left(P_k, Public_l, t\right) \end{pmatrix}, \\ GeneralInput\left(P_k, Public_l, t\right), \\ State\left(P_k, Public_l, t\right) \end{pmatrix} \end{aligned} \tag{21}$$

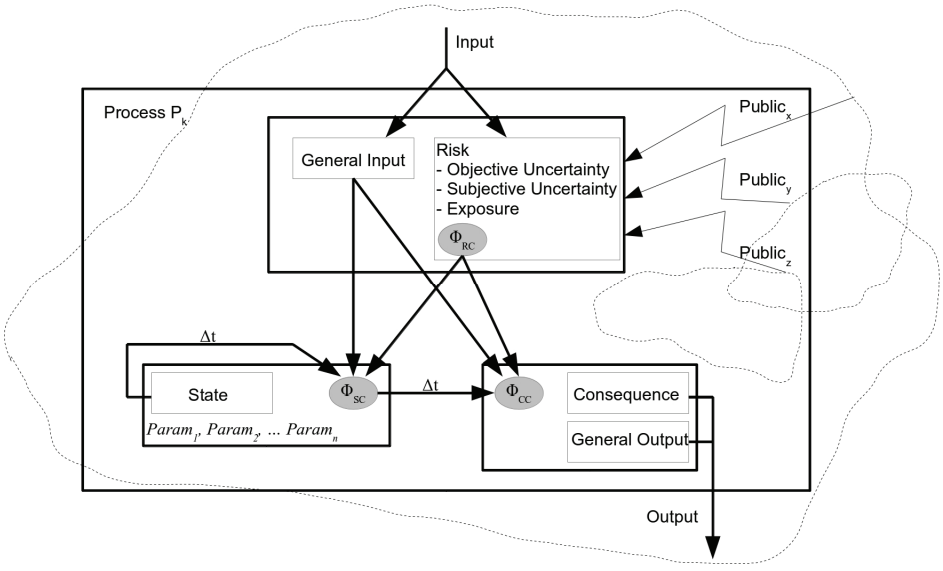
Considering the equations (17), (18), (19), (20) and conducting segments of the public risks should be expressed with the equation (22):

$$\begin{aligned} &Consequence\left(P_k, Public_l, t+\Delta\right) = \\ &\Phi_{CC}\begin{pmatrix} \Phi_{RC}\begin{pmatrix} ObjUncertainty\left(P_k, Public_l, t\right), \\ SubUncertainty\left(P_k, Public_l, t\right), \\ Exposure\left(P_k, Public_l, t\right) \end{pmatrix}, \\ GeneralInput\left(P_k, Public_l, t\right), \\ State\left(P_k, Public_l, t\right) \end{pmatrix}, \\ &\Phi_{CC}\begin{pmatrix} \Phi_{RC}\begin{pmatrix} ObjUncertainty\left(P_k, Public_l, t\right), \\ SubUncertainty\left(P_k, Public_l, t\right), \\ Exposure\left(P_k, Public_l, t\right) \end{pmatrix}, \\ GeneralInput\left(P_k, Public_l, t\right), \\ \Phi_{SC}\begin{pmatrix} \Phi_{RC}\begin{pmatrix} ObjUncertainty\left(P_k, Public_l, t-\Delta\right), \\ SubUncertainty\left(P_k, Public_l, t-\Delta\right), \\ Exposure\left(P_k, Public_l, t-\Delta\right) \end{pmatrix}, \\ GeneralInput\left(P_k, Public_l, t-\Delta\right), \\ State\left(P_k, Public_l, t-\Delta\right) \end{pmatrix} \end{pmatrix} \end{aligned} \tag{22}$$

The equation (19) shows how to calculate risk, being the input to a business process based on objective and subjective uncertainty and exposure at a point in time. The equation (20) shows how to calculate process states based on known risks, general input and process states recorded for a prior time slice at a certain point in time. The equation (21) explains the calculation of the impact based on the same inputs as for internal process states. The equation (22) gives the calculation of consequences using a transitive relation for the calculation of internal process states in a prior time slice by taking into consideration risks, general input and internal process states in the time slice prior to the last time slice. All equations include business processes and segments of the public.

These equations constitute the foundation of the algorithm for the calculation of the consequences in a model. The impact calculation is central to risk management modeling, and it is illustrated by Figure 4.

Figure 4: The main elements of the risk management model



Risk criteria

For risks the acceptance border is calculated in the equation (23), using the function Φ_{RAB}; the acceptance border for the consequences is defined with the equation (24) by the function Φ_{CAB}; and the acceptance border for the process states is defined with the equation (25) by the function Φ_{SAB}.

$$RiskAcceptanceBorder(P_k, Public_l, t) = \{RAB_{k,l,1}(t), RAB_{k,l,2}(t), ..., RAB_{k,l,m}(t)\} = \Phi_{RAB}(Risk(P_k, Public_l, t)) \quad (23)$$

$$ConsequenceAcceptanceBorder(P_k, Public_l, t) = \{CAB_{k,l,1}(t), CAB_{k,l,2}(t), ..., CAB_{k,l,m}(t)\} = \Phi_{CAB}(Consequence(P_k, Public_l, t)) \quad (24)$$

$$StateAcceptanceBorder(P_k, Public_l, t) = \{SAB_{k,l,1}(t), SAB_{k,l,2}(t), ..., SAB_{k,l,m}(t)\} = \Phi_{SAB}(State(P_k, Public_l, t)) \quad (25)$$

In the equations (26), (27) and (28), tolerable, or acceptable values for risk, consequences, and values of the process states are defined according to the given acceptance borders.

$$AcceptedRisks(P_k, Public_l, t) = \{R_{k,l,x}(t); x = 1,2,...,m \wedge R_{k,l,x}(t) < RAB_{k,l,x}(t)\} \quad (26)$$

$$AcceptedConsequences(P_k, Public_l, t) = \{C_{k,l,x}(t); x = 1,2,...,m \wedge C_{k,l,x}(t) < CAB_{k,l,x}(t)\} \quad (27)$$

$$AcceptedStates(P_k, Public_l, t) = \{Param_{k,l,x}(t); x = 1,2,...,m \wedge Param_{k,l,x}(t) < SAB_{k,l,x}(t)\} \quad (28)$$

The equations (29), (30) and (31) define the unacceptable (intolerable) values which represent a set of values that is equal to the set of all possible values minus the set of acceptable values.

$$NotAcceptedRisks(P_k, Public_l, t) = Risk(P_k, Public_l, t) - AcceptedRisks(P_k, Public_l, t) \quad (29)$$

$$NotAcceptedConsequences(P_k, Public_l, t) = Consequence(P_k, Public_l, t) - AcceptedConsequences(P_k, Public_l, t) \quad (30)$$

$$NotAcceptedStates(P_k, Public_l, t) = State(P_k, Public_l, t) - AcceptedStates(P_k, Public_l, t) \quad (31)$$

References

[1] AS/NSZ 4360:2004; Risk management; Standards Australia. (2004). ISBN 0-7337-5904-1

[2] Borut Jereb (2009); Segmenting Risks in Risk Management; Logistic & Sustainable Transport; Vol 1, Issue 3

[3] Christian Bluhm (2002), Ludger Overbeck, Christoph Wagner; An Introduction to Credit Risk Modeling; ISBN:158488326X

[4] Dan X. Houston, Gerald T. Mackulak, James S. Collofello (2001) Stochastic simulation of risk factor potential. Journal of Systems and Software, Vol 59, Issue 3. doi:10.1016/S0164-1212(01)00066-8

[5] Daniel Kahneman and Amos Tversky; Prospect Theory: An Analysis of Decision under Risk; Econometrica, 47(2), pp. 263-291, March 1979

[6] Douglas W. Hubbard; The Failure of Risk Management: Why It's Broken and How to Fix It. John Wiley & Sons, Inc. ISBN 978-0-470-38795-5

[7] Frank Knight (1921) Risk, Uncertainty, and Profit. New York: Hart, Schafner, and Marx.

[8] Glyn A. Holton (2004) Defining Risk. Financial Analyst Journal; Vol 60, No 6. CFA Institute.

[9] GPSS (2009). http://en.wikipedia.org/wiki/GPSS. Acessed june 2009

[10] http://en.wikipedia.org/wiki/Risk; june. 2010

[11] http://www.businessdictionary.com/definition/risk.html; june. 2010

[12] http://www.investorwords.com/4292/risk.html; june. 2010

[13] ISACA: The Risk IT Framework. (2009). ISBN 978-1-60420-111-6

[14] ISO 31000: Risk management - Principles and guidelines; First edition; International Organization for Standardization; 2009

[15] IEC/ISO 31010: Risk management – Risk assessment techniques; Edition 1.0; International Organization for Standardization; International organization for Standardization; 2009
[16] ISO/IEC 27005:2008; Information technology - Security techniques - Information security risk management; International Organization for Standardization; 2008.
[17] ISO/IEC 27005:2011; Information technology - Security techniques - Information security risk management, Second edition; International Organization for Standardization; 2011.
[18] IT Governance Institute: Enterprise value, Governance of IT Investments, Getting Started With value Management. (2008). ISBN 978-1-60420-067-6, 2008
[19] Jukka Hallikas, Iris Karvonenb, Urho Pulkkinenb, Veli-Matti Virolainenc, Markku Tuominena (2004) Risk management processes in supplier networks. International Journal of Production Economics; Vol 90, Issue 1. doi:10.1016/j.ijpe.2004.02.007
[20] Lorenzo Benedetti, Davide Bixio, Filip Claeys, peter A. Vanrolleghem (2008) Tools to support a model-based methodology for emission/immission and benefit/cost/risk analysis of wastewater systems that considers uncertainty. Environmental Modelling & Software; Vol 23, Issue 8. doi: 10.1016/j.envsoft.2008.01.001
[21] Matthew Pritsker (2006) The hidden dangers of historical simulation. Journal of Banking & Finance; Vol 30, Issue 2. doi:10.1016/j.jbankfin.2005.04.013
[22] Michael B. Gordy (2003) A risk-factor model foundation for ratings-based bank capital rules. Journal of Financial Intermediation; Vol 12, Issue 3. doi: 10.1016/S1042-9573(03)00040-8
[23] Mun, J. (2006). ModelingRisk. Wiley finance series. ISBN-13 978-0-471-78900-0
[24] SARA (Security Auditor's Research Assistant). (2009, december). http://www.enisa.europa.eu/act/cert/support/chiht/tools/sara-security-auditors-research-assistant
[25] Scott, Hal S. (2005) Capital Adequacy beyond Basel, Banking, Securities, and Insurance; ISBN-13: 978-0-19-516971-3; doi: 10.1093/acprof:oso/9780195169713.003.0006. Oxford Scholarship Online: January 2007
[26] Steve Schlarman (2009) IT Risk Exploration: The IT Risk Management Taxonomy and Evolution. ISACA Journal; Vol 3
[27] Steven J. Ross (2006) Four Little Words. ISACA Journal; Vol 1
[28] Taleb, Nassim. (2007) The black swan: the impact of the highly improbable. Random House. ISBN 978-1-4000-6351-2
[29] Terje Aven (2010) On how to define, understand and describe risk. Reliability Engineering and System Safety. Elsevier. doi: 10.1006/j.ress2010.12.020
[30] Terje Aven (2011) On the new ISO guide on risk management terminology. Reliability Engineering and System Safety. Elsevier. doi: 10.1006/j.ress2010.01.011
[31] Value at risk. (2009, junij). http://en.wikipedia.org/wiki/VaR