Proceedings of the 12th International Conference "Reliability and Statistics in Transportation and Communication" (RelStat'12), 17–20 October 2012, Riga, Latvia, p. 234–239. ISBN 978-9984-818-49-8
Transport and Telecommunication Institute, Lomonosova 1, LV-1019, Riga, Latvia

FUZZY APPROACH TO RISK ANALYSIS AND ITS ADVANTAGES AGAINST THE QUALITATIVE APPROACH

Kamil Boc[1], Juraj Vaculík[2], Dagmar Vidriková[3]

[1]Department of Security Management, Faculty of Special Engineering, University of Zilina
Ul. 1. Maja 32, Zilina, Slovakia
Ph.: +421415136660. E-mail: kamil.boc@fsi.uniza.sk

[2]Department of Security Management, Faculty of Special Engineering, University of Zilina
Ul. 1. Maja 32, Zilina, Slovakia
Ph.: +421415136669. E-mail: juraj.vaculik@fsi.uniza.sk

[3]Department of Technical Sciences and Informatics, Faculty of Special Engineering, University of Zilina
Ul. 1. Maja 32, Zilina, Slovakia
Ph.: +421415136860. E-mail: dagmar.vidrikova@fsi.uniza.sk

Risk analysis is an important step in designing the reliable transportation and communication systems. Methods of fuzzy logic can provide a convenient way to conduct risk analyses. The article describes an application of fuzzy logic and fuzzy approach into risk analyses and into risk management process. All needed requirements for using this approach are described. The main advantage of using fuzzy approach is limitation of subjectivity in risk assessment. That can provide basis for regular repeating of risk analyses so efficient control system can be created instead of formal occasional risk analyses. Article also describes recommended modification of threat identification process to maximize mutual effect when applied together with this kind of risk analyses.

Keywords: risk analysis, fuzzy approach, risk management

Introduction

The risk analysis is considered to be a very important task of managerial process of every complex system, such as transportation, communication or information system. However, it is also considered to be one of the most difficult tasks. Bad implementation of risk analysis can lead to a subjective behaviour of a whole analysis with consecutive unclear results. We believe that the main reasons for criticism are based on qualitative essence of modern methods widely used in risk analysis. Naturally, every possible tool that can be effectively used to reduce subjectivity has to be investigated deeply.

There are a lot of approaches for conducting risk analysis. Since there are of a lot of different kinds of systems, many techniques have been developed to struggle with the most common issues of risk analysis:

- Subjectivity,
- Lack of information about threats and weaknesses,
- Formality and insubstantiality of analysis,
- Untrustworthiness of information about environment,
- Indeterminate results when analyzing alive and rapidly changing systems.

The special problem in conducting the whole analysis is the way that it is not considering the actual countermeasures, so repeating the analysis before and after implementation of additional countermeasures has completely the same results. That is the case if only information about environment is taken into account, or when meaning and significance of these data are significantly overestimated.

There is not any universal and best method for conducting risk analysis and it is unlikely that such method will be created. However, it is important to understand the strengths and weaknesses of various approaches for conducting risk analysis.

Qualitative analysis relies on the subjective judgment of the competent personnel to determine the overall risk. We believe that further development of fully qualitative approach to risk analysis is not going to reduce the common disadvantages of current methods. Perhaps, additional development of this approach can create robust methods, with extensive and useful indices of threats, weaknesses and countermeasures,

but essential problems caused by subjective matter of assessment is not going to be solved using fully qualitative methods.
Certainly there are also some advantages of conducting fully qualitative risk analysis, such as:

- Relative simplicity of risk evaluation,
- Lack of data can be substituted with experts estimations,
- Sometimes qualitative approach is ordered by law or other regulations.

Quantitative analysis is an approach that relies on specific formulae and calculations to determine the value of the risk decision variables. Certainly, there are significant advantages of quantitative approach:

- More objective,
- Based on mathematical methods,
- Meaningful statistics,
- Generally more credible than qualitative approach.

Also, quantitative approach is provided for cost-benefit analysis. Many corporate decisions requiring the expenditure of limited resources are made only after a careful cost-benefit analysis. This means that the perceived benefit of the project must outweigh the cost involved in such a project. Quantitative analysis can provide the information necessary to analyze the costs and benefits of proposed controls [1].

However, quantitative analysis is very complex, sometimes even not understood correctly by management and important concerns about risks can be overridden with information, that can be easily measured and they are proven by statistics. That is the main reason why implementing fuzzy logic is meaningful – because fuzzy logic can calculate also with non-accurate inputs [2] so the whole analysis does not rely only on data that can be exactly measured.

Implementing the Fuzzy Logic

Fuzzy logic is a convenient way to map an input space to an output space [3]. Method with implementing fuzzy logic that we describe in this article is suitable for risk analyses of highly dynamic systems where other approaches are often impractical. Comprehensive understanding of some processes in the system is required and is critical for conducting risk analysis based on fuzzy logic:

- Correct and consistent identification of sources of risk,
- Understanding the process of risk activation,
- Correct identification of input data that determines significance of risk.

The most important feature of risk analysis based on fuzzy logic is that the whole process leads to creating the control system that can effectively reduce risk. Because of exact output of analysis and consideration of countermeasures we can repeat risk analysis on a regular basis with valuable output.

Moreover, using fuzzy logic and methods based on fuzzy logic we can reduce subjectivity to acceptable level, because we are using quantitative input data so subjectivity is moved to process of creating relations and dependencies between input data and risk assessment, so it can be better controlled. Certainly, subjectivity is not eliminated completely. However, it is unlikely that method with no subjectivity will ever exist for risk analysis.

Basic element of risk analysis is a risk assessment. It is the activity that measures the strength of the overall system and provides the information necessary to make planned improvements based on information risks. There are also other stages of the risk analysis that make up risk management process (such as testing and gathering information, risk mitigation or risk reporting) that can be even more time-consuming, but we will focus our attention on the process of risk assessment, because it is a part that can use a fuzzy approach effectively.

The basic equation for risk calculation is risk = assets * probability [4]. Fuzzy approach uses methods of fuzzy logic to quantify both needed parts using quantitative input data. The main idea is to determine a few fuzzy variables for every part (assets, probability) of every risk that can be defined with fuzzy sets so in the following phase we use fuzzy rules and base of rules to build a fuzzy system. The fuzzy system is based on some "common sense" statements. [3]

One of the biggest advantages of fuzzy logic is that the whole system is very flexible [5]. This is especially important in dynamic systems. We can say that every situation that we can solve with fuzzy logic we can also solve with other methods. However, the fuzzy logic can be the most efficient one. Modifying the fuzzy system is simple because the changes require only adding some other variables or rules [6]. There is no need to change majority of what was done before.

Determining Value of Assets with Fuzzy Logic

The value of asset can be determined in two ways:

- Financial value of asset,
- Severity of the impact to company when asset is stolen, destroyed or temporary unavailable.

We believe that these two parts are completely equal. Sometimes even financial value of asset can be considered as less important especially when they are insured and easily accessible on the market. However, impact of destroyed assembly line can be fatal no mater of insurance of line itself or goods made by line, but because of layoff time that can produce significant loss.

Because of this, we prefer to use both factors in calculating value of each asset. Overall value will be determined by fuzzy system that will treat both factors equally, so lay-off time that can cause significant financial loss is equal to stealing or destroying of asset with the same value.

There are some methods for financial value estimations that are widely used:

- Cost valuation – this approach to determining the value of an asset uses the economic principle of substitution.
- Market valuation – this approach is based on the economic principles of competition and equilibrium, better known as the law of supply and demand.
- Income valuation – this approach is based on the economic principle of expectation. This principle states that the value of an asset is equal to the expected incomes from that asset [1].

Using these methods, financial value of assets can be determined. With the next step we estimate the layoff time of crucial activities if various assets are stolen, destroyed or unavailable for normal operation. Then we can build a fuzzy system that will determine the value of each asset as logical conjunction of these two values – financial value and severity of impact of assets loss. Fuzzy logic is a convenient way to solve this task because there is no need to convert a lay-off time of various business processes directly to financial value and vice versa.

Some authors distinguish the fact that fuzzy logic is based on natural language as one of the most important. But since fuzzy logic is built atop the structures of everyday language, it not only makes it easy for us to use it (since fuzzy logic more closely "speaks our language") but it also takes advantage of the long history of natural language [3].

Determining the Probability that a Vulnerability will be Exploited

Determining the probability is not more complicated than estimating a value of assets. Simple and universal technique is to choose and specify for each risk fuzzy variables that can be objectively (but not necessary precisely) enumerated and that are in definite relation with a particular risk.

A reliable method for this is to analyze the past events and determine the critical variables from the past events. Variables can be described as enumeration of threat and enumeration of countermeasures. We need to specify dependencies using fuzzy logic and use fuzzy sets to define particular values.

There are some occasions when there is more efficient another more specific technique for estimating a probability of risk. All the variables can describe only efficiency of various countermeasures with defined mutual relations. To specify a relation we use attributes. There are three kinds of possible attributes:

- Sufficient condition – means that this countermeasure is theoretically sufficient for complete elimination of risk (for example regular backup of information system can eliminate risk of data loss),
- Necessary condition – means that elimination of risks is not possible to achieve without this countermeasure (for example security awareness is necessary for elimination of risk connected to social engineering),
- Sufficient and necessary condition – means that both attributes are present and other countermeasures have limited impact.

In Fig. 1 we illustrate this concept graphically. In the upper left image there are two countermeasures marked as CM1 and CM2 and both have no attributes assigned. In this case the output that represents the probability that vulnerability will be exploited is symmetrical. In the upper right image countermeasure CM1 is marked with a sufficient condition attribute, while CM2 is marked with no attribute. Analogically, in the bottom images: CM1 is marked as a necessary condition (left) and a sufficient and necessary condition (right).

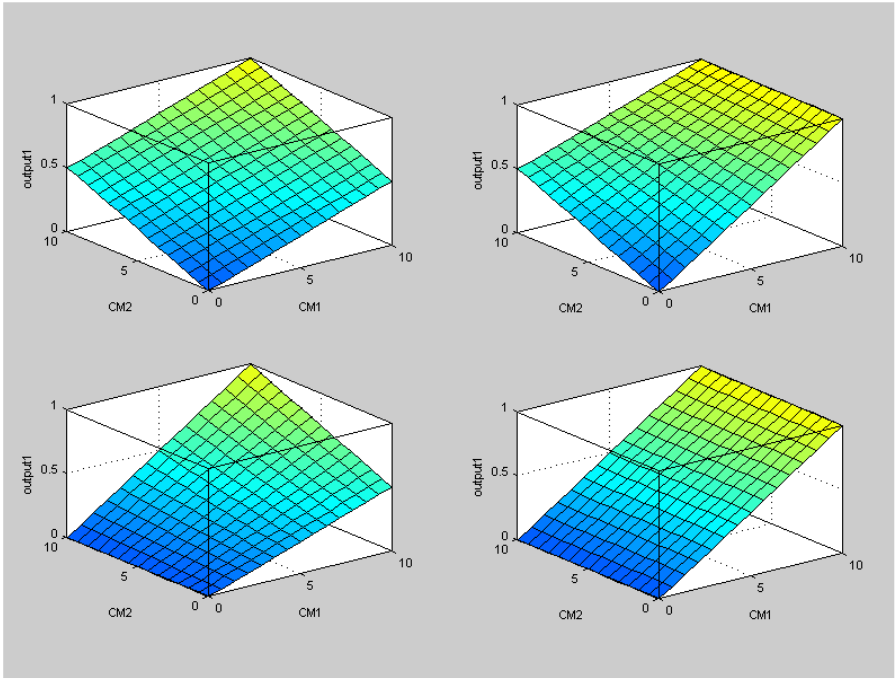

Figure 1. Various relations of attributes in determining the probability that vulnerability will be exploited, source: authors

There is a simple example. We are considering risk that intangible assets in the information system will be corrupted because of accidental fault from personnel. We define countermeasures for elimination of this risk:

- Data Backup,
- Training,
- System monitoring and extra pay for no violation of internal rules.

From these countermeasures there is one countermeasure that has attribute – it is data backup, because complete online data backup can theoretically completely eliminate this risk. In real scenario keeping data on different location also would be required for complete elimination [7]. Other countermeasures can only partially eliminate this risk therefore no attribute is assigned to them.

In Fig. 2 there is a graphical representation of relations between various countermeasures and probability of risk.

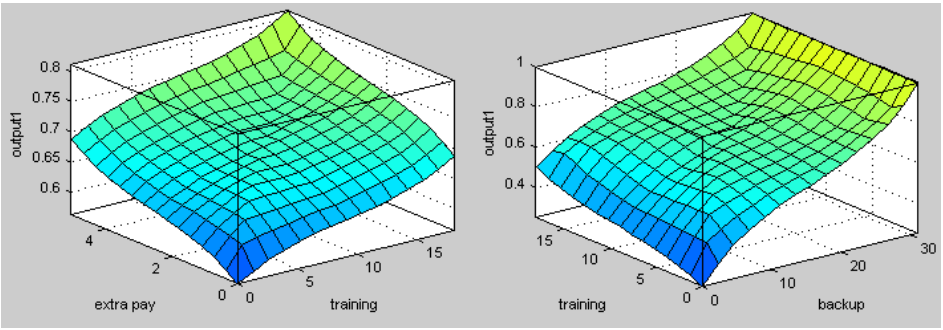

Figure 2. Concrete application of attributes in real scenario, source: authors

Using this approach we have to modify other techniques during risk management process, especially risk identification that has to take into account all other possible information, such as:

- Existence of risk itself, especially existence of source of risk,
- Sufficient motivation for harmful actions (if applicable),
- Similar past events,
- Other indicators of existence of risk.

Benefits of Fuzzy Approach for Risk Management

There are some important benefits of fuzzy approach for risk management process that are not possible to achieve with fully qualitative methods. The fuzzy risk assessment, no matter of used methods and input data, leads to a specific numerical output. Any further changes of input data also change this output, so regular repeating of analysis is meaningful.

Certainly, suitable and comprehensive input data for constructing the fuzzy system is required. There are a lot of risks that normally do not seem to be important and it looks that there is no need to take some countermeasures against them. Using only fully qualitative approach can lead to underestimation of these risks, because occasional analysis conducted under normal circumstances will not uncover their negative potential. However, under some specific and rare circumstances the same risk can be significant and dangerous. If we can define and track indicators that are associated with these rare circumstances then we can struggle effectively also with these kinds of risk.

Regular repeating of fuzzy risk analysis is important for achieving the optimal results. That is a reason why there are good results of using fuzzy approach for assessing the highly dynamic systems where there are regular changes in values of input data. Some risks can be evaluated only after long and time-consuming tracking and analysis of statistical data. This is not going to change no matter of method we are going to use, however some fully qualitative methods do not really require this tracking and they can use subjectivity instead. This seems to be a dangerous practice in the management of complex systems.

Relation with other Techniques in Risk Management Process

Since the comprehensive risk analyses conducted with fuzzy approach can be very time-consuming it is important to focus on meaningful and dangerous risks. It is important to combine risk analysis with correct threat identification.

Threat identification is a substantial part of risk management process. It is important to define relation between threat identification and risk assessments.

As we have mentioned before, we prefer fuzzy approach for analyzing systems that are dynamic and are difficult to analyze with other methods. In this kind of systems, there are sometimes situations that we have very limited available information about dangerous risks:

- We know how to deal with risk so we know which countermeasures theoretically to take to prevent risk to occur,
- We have information about current countermeasures, especially how efficient they are compared to ideal countermeasures that could theoretically eliminate the risk completely.

With this information we can build fuzzy system for risk assessment. If we do not have this information we cannot conduct a comprehensive risk analysis, so these data can be understood as minimal requirements for conducting a risk analysis.

However, a lot of other information has to be analyzed prior to process of risk assessment that will use only this kind of information. Some information cannot be objectively obtained and verified. In this case, information should be isolated from risk assessment (because we expect a quantitative output from risk assessment) and it should be moved completely to phase of threat identification. During risk assessment phase, the technical aspects of each risk are assessed and defined [8].

In the phase of threat identification we can use approved methods to analyze threats using a pre-defined factors, such as generalized method derived from the method specified in FM 3-19.30 [9] that define several factors:

- Factor 1: Proven or theoretical existence of source of risk.
- Factor 2: Capability. It is apparent that current countermeasures do not eliminate risk.
- Factor 3: Intentions. For human caused risks only.
- Factor 4: History. Demonstrated activity over time or past events (like disasters).
- Factor 5: Targeting. Current credible information on activity indicative of preparations for specific type of attack or event.

After that a threat can be classified on scale and then deep risk analysis can be conducted for significant risks:

1. Critical: factors 1, 2, and 5 are present. Factors 3 or 4 maybe present.
2. High: factors 1, 2, 3, and 4 are present.
3. Medium: factors 1, 2, and 4 are present.
4. Low: factors 1 and 2 are present. Factor 4 may be present.
5. Negligible: factors 1 and/or 2 may be present [9].

Risk assessment should be based on information that is essential for estimation of risk exposure and on the effectiveness of defence mechanism that should protect us from actual threats. These data are based on effectiveness of countermeasures so they are available for us. Critical task is then to define fuzzy system correctly so it will match real relations and dependencies in real system.

Conclusion

We can conclude that there are several reasons why to use fuzzy logic in the process of risk analysis:

- Fuzzy approach creates flexible framework that can built on top of the experience of experts, [3]
- Fuzzy logic is tolerant to imprecise data, [10]
- Regular risk analysis based on fuzzy logic can create an effective control system.

Various risks that endanger complex systems have very difficult mechanisms of activation so precise mathematical modelling the system is usually too complex for practical application. Fuzzy logic with built-in toleration to imprecise data is an ideal tool for enhancing the effectiveness of risk analysis. Certainly, fuzzy approach requires real experiences of experts and competent personnel to identify and collect needed data and to build a fuzzy system. However, subjective evaluation is limited especially compared to other methods.

Acknowledgements

This paper is supported by VEGA 1/0981/11 project: Model of integrated security system optimization framework for protection of specific objects realized by means of expert system.

References

1. Landoll, D. *The Security Risk Assesment Handbook.* New York: Auerbach Publication. ISBN 0-8493-2998-1. 2006. 473 p.
2. Wang P, Da Ruan, Kerre E. *Fuzzy Logic A Spectrum of Theoretical & Practical Issues.* Berlin: Springer. ISBN 978-3-540-71257-2. 2007. 464 p.
3. Jang, R., Gulley, N. 1997. Fuzzy Logic Toolbox User's Guide. Natick, Massachusetts: The MathWorks, Inc.
4. Jean-Paul Chavas. *Risk analysis in theory and practice.* London: Elsevier Academic Press. ISBN 0-12-170621-4. 2004. 256 p.
5. Da Ruan. *Fuzzy Sets and Fuzzy Information. Key Selected Papers by Lofti A. Zadeh.* Bejing: Bejing Normal Univeristy Press. ISBN 7-303-05324-7. 2000.
6. Mcneill, M., Ellen, T. *Fuzzy Logic, a Practiacal Approach.* London: Academic Press. ISBN 0-12-485965-8. 1994. 309 p.
7. Peltier, Thomas R. *Information security risk analysis.* Boca Raton: CRC Press. ISBN 0-8493-3346-6. 2005. 341 p.
8. Carr, V., Tah, J. H. M. A *fuzzy approach to construction project risk assessment and analysis: construction project risk management system.* London: Advances in engineering software. 2001.
9. FM 3-19.30: *Physical Security*, Headquatres, Department of the Army, USA, 2001
10. Bojadziev, G., Bojadziev, M. *Fuzzy Logic for Business, Finance and Management.* Singapore: World Scientific Publishing. ISBN-13 978-981-270-649-2, ISBN-10 981-270-649-6. 2007. 232 p.