ASSESSING TERRORIST THREATS FOR ENERGY INFRASTRUCTURE BY COMBINING HISTORICAL DATA AND EXPERT JUDGMENTS

Davor Šinka[1], Slavko Krajcar[2], Tomislav Bajs[3]

ABSTRACT: Energy systems are relatively attractive targets for terrorist attacks and should be adequately protected. The quantitative risk analysis (QRA), with the threat assessment as one of its standard components, is considered to be a promising methodological framework for optimizing such protection.

This paper presents the results of the research which consisted of two parts. In the first part the statistical analysis of the terrorist attacks towards energy systems was performed. The input data were derived from the Global Terrorism Database (GTD). Within the analysis relative contributions of the attacks on energy systems to the total number of attacks were determined. Also, it was examined how those contributions are influenced by various factors related to the characteristics of the target, terrorist group and the environment in which the group operates.

In the second part of the research the method for the quantitative threat assessment was developed. It is based on the results of the performed statistical analysis (i.e. on historical data) and on expert judgments. The method is applicable to the electricity, gas and oil

[1] ENCONET, Zagreb, Croatia, davor.sinka@enconet.hr

[2] University of Zagreb, Faculty of Electrical Engineering and Computing, Zagreb, Croatia, slavko.krajcar@fer.hr

[3] ENCONET, Zagreb, Croatia, tomislav.bajs@enconet.hr

sectors. The implementation of the Bayesian networks allows for taking the uncertainties into consideration, as well as for easy modifying and updating.

KEYWORDS: threat assessment, terrorism, energy infrastructure, protection, Bayesian networks

Introduction

Stable energy supply is the vital factor for the functioning of modern societies. It is well known that energy systems are primarily constructed to provide the service with the competitive costs and not to be resilient to the terrorist attacks. The importance of energy systems on one side and the vulnerability on the other side makes them attractive targets which should be adequately protected[1][2]. As always, the resources are limited and it is not possible to protect every component of energy infrastructure all the time. In other words, the protection has to be optimized.

Risk assessment and management models and methods appear to be suitable methodological framework for optimizing the protection of energy infrastructure from terrorist activities[3]. In general, such methods can be qualitative or quantitative. However, within the risk assessment and management community it is believed that only quantitative methods provide good basis for the decision making. In addition, the methods should be able to take into consideration the uncertainties of the input data and to clearly indicate how confident the analysts are about the results[4].

The terrorism risk is a function of three parameters: (1) threat, (2) vulnerability and (3) consequences[5]. It means that in order to estimate the terrorism risk one has to assess each of those parameters. This research was focused to the threat and threat assessment only. The threat can be defined as an individual or an organization having both the intent and capability to impose damage to a target. To assess the threat means to estimate the probability that a specific target is attacked in a specific way during a specific time period.

The performed research demonstrates how terrorist threats for energy infrastructure can be assessed by combining historical data (i.e. the data on terrorist attacks carried out in the past) and expert judgments. It consisted of two parts. In the first part of the research the statistical analysis of the terrorist attacks towards energy systems was performed. This part is described in Section 2. In the second part of the research, covered in Section 3, the method for the quantitative threat assessment was developed.

Historical data analysis

The historical data analysis was based on the records from the Global Terrorism Database (GTD)[6][7]. GTD, operated by the START consortium, is currently the most comprehensive unclassified database on terrorist events around the world. The data is gathered continuously since 1970 and now the database contains information on more than 140.000 terrorist attacks. For each attack 45 to 120 variables are recorded (date, location, target, weapons used, casualties, group or individual responsible …).

The analysis was focused on the 15 years period starting with 1996 and ending with 2010. All the records from that period were examined in detail and the attacks towards energy infrastructure were identified. Based on the descriptions provided in the database, for each attack the energy sector and the exact component which was targeted have been determined.

The results show that within the covered time period 36.836 attacks were recorded altogether (931 - 4.776 attacks per year). The attacks were organized in 177 states by 973 terrorist groups (Figure 1). During the same period 746 attacks were aimed towards energy infrastructure (Figure 2). Those attacks were carried out in 44 states by 56 groups.

The analysis revealed that energy systems are selected as target approx. ones in 50 attacks on average, which gives the contribution of 2 % (Figure 3, Figure 4). As for the subsystems, electrical energy targets are selected approx. ones in 100 attacks, while gas and oil targets are selected once in 200 attacks. The contributions for the mentioned subsystems amount to 0,94%, 0,48% and 0,61% respectively.

The contributions reflect the attractiveness of particular subsystem as a target. There are at least three possible reasons why electrical energy targets are selected more often than gas or oil. First, nowadays electrical energy infrastructure can be found almost everywhere, which is not the case with the gas and oil. Second, the attacks on electrical energy systems result with immediate effects on energy supply, which is again not the case with the gas and oil. Third, electrical power lines are easily accessible, while oil and gas pipelines are often buried and harder to access.

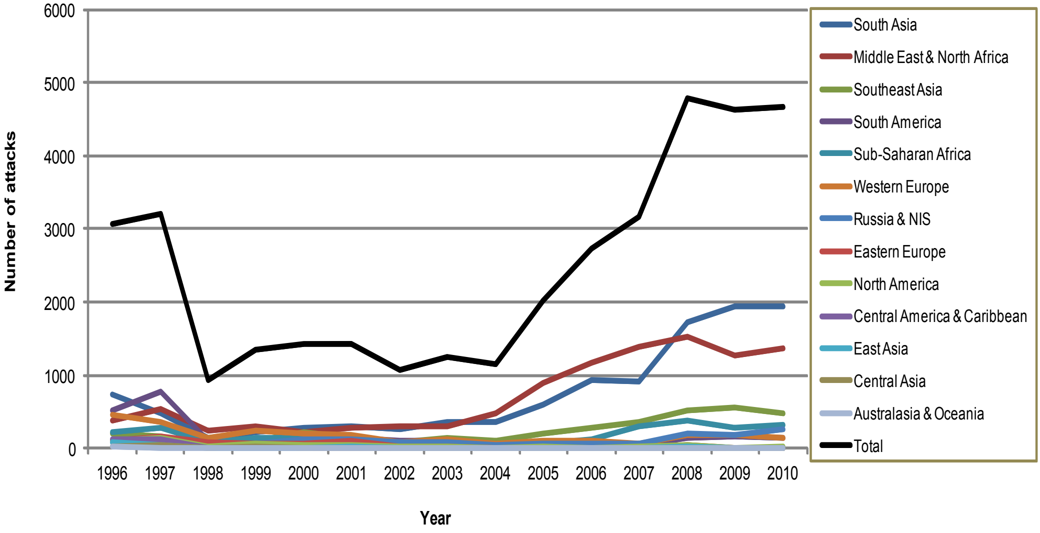

Figure 1: Terrorist attacks on all targets

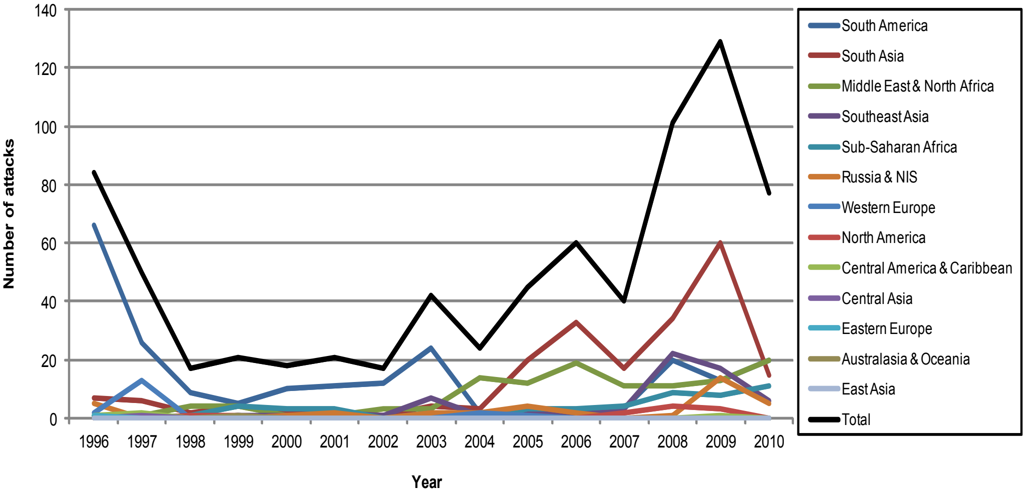

Figure 2: Terrorist attacks on energy systems

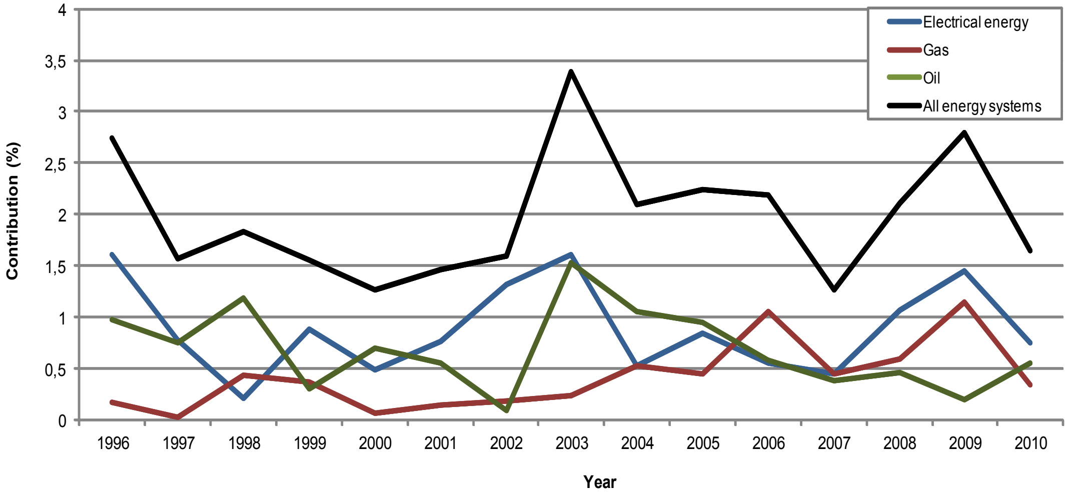

Figure 3: Relative contributions of the terrorist attacks on energy systems towards total attacks (worldwide)

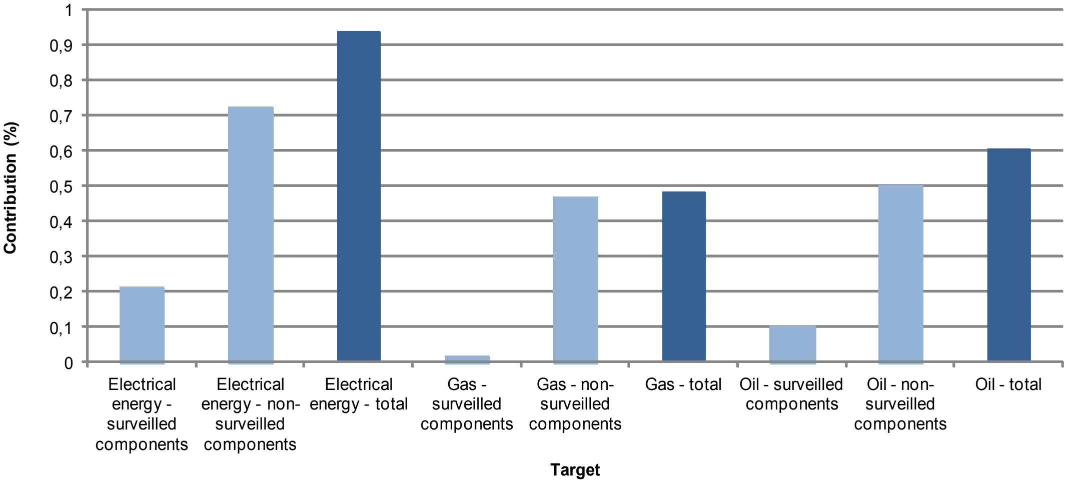

Figure 4: Relative contributions by subsectors and components

It can be noticed that the contributions of energy systems, when averaged across the world, are quite stable (black line on Figure 3). The contributions are mostly in the range between 1,5 and 2,5% and there are no major trends. However, the values for various geographical regions differ significantly (Figure 5).For instance, energy infrastructure seems to be very attractive for the terrorists in South America, while in East Asia it is not attractive at all. In order to find out what causes such differences a number of factors were analyzed.

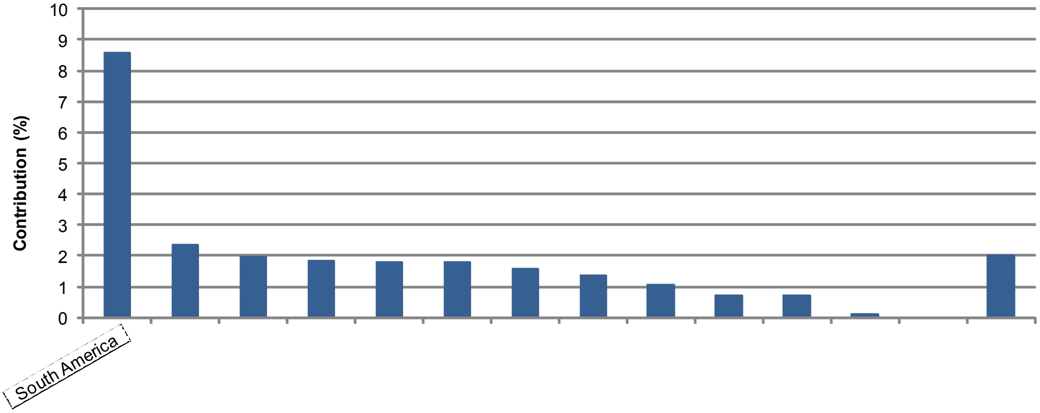

Figure 5: Relative contributions by geographical region

It's been shown that the factors having the biggest influence on the attractiveness of energy systems as terrorist attack targets are (1) the ideology of the terrorist group, (2) the presence of armed conflict in the area where the terrorists operate and (3) the activity of the terrorist group. In order to analyze the influence of the ideology, terrorist groups were divided into left wing groups, nationalists-separatists, religious groups and right-wing groups. Figure 6 shows that energy systems, as symbols of capitalism, are most attractive for the left-wing groups. Such targets are also quite attractive to nationalists-separatists, probably as the symbols of the state authority. It seems that the religious groups prefer to select targets with more direct relation with the state, while the right wing groups do not find energy systems attractive at all.

The attractiveness of energy systems is below the average in the areas where armed conflict is not present and above the average in the areas with permanent armed conflict (Figure 7). It is believed that when armed conflict is present terrorist groups tend to implement typical guerilla and military tactics, which include cutting the energy supplies of the enemy[2].

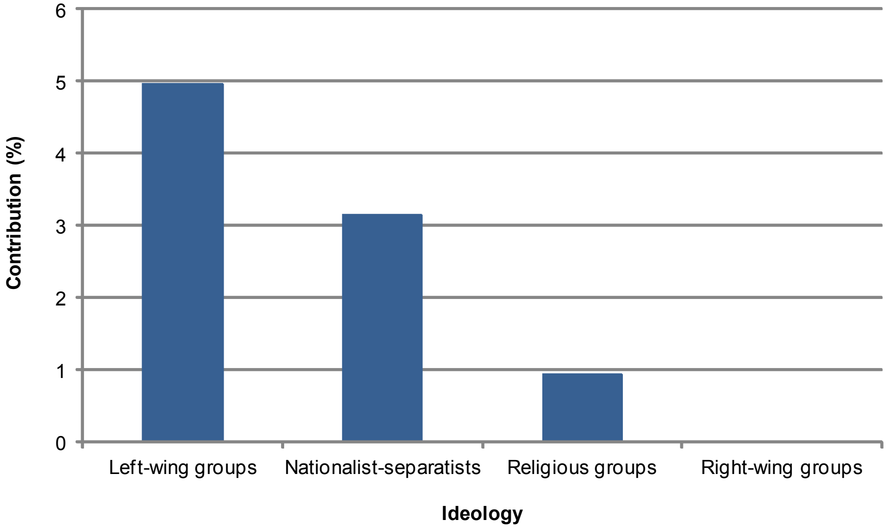

Figure 6: Relative contributions by ideology

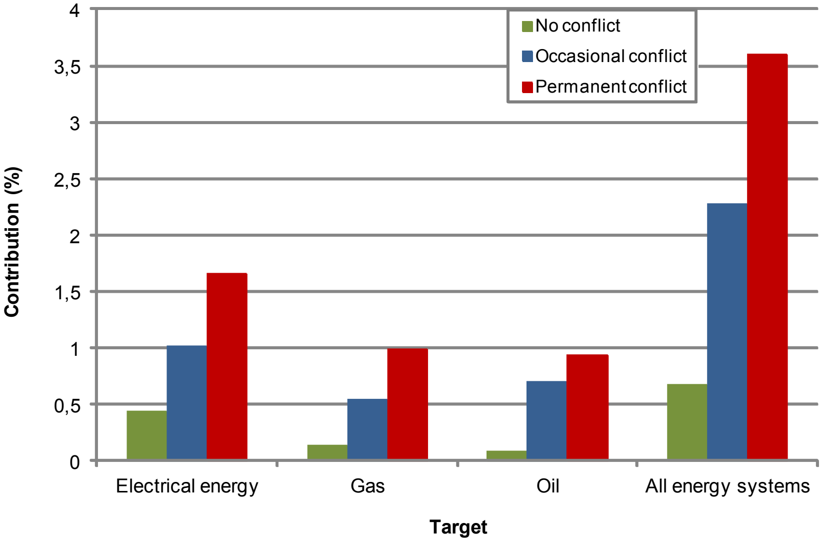

Figure 7: Relative contributions by presence of armed conflict

As for the influence of the terrorist group activity, the results of the analysis indicate that energy systems are more attractive for the groups which organize attacks more frequently (Figure 8). However, this phenomena hasn't been explained yet.

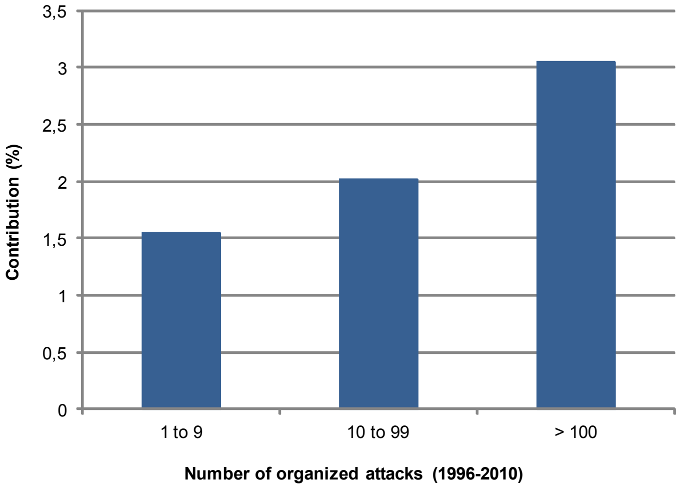

Figure 8: Relative contributions by terrorist group activity

Method description

The proposed threat assessment method is based on the results of the historical data analysis. It allows for combining the data on terrorist attacks carried out in the past with expert judgments. The method is quantitative, capable of taking into consideration the uncertainties of the input data and expressing the confidence level of the results. It is designed to be used by energy systems' operators within the electrical, gas and oil sectors.

The threat (i.e. the probability of attacking specific target in a specific way by the specific terrorist group) is calculated as a product of 5 factors in a way that the number of attacks the terrorist group organizes in the area of interest is multiplied by 4 conditional probabilities:

$$T_{i,j} = N_{A_j} \cdot P(A_{EN}|A) \cdot P(A_{SE}|A_{EN}) \cdot P\left(A_{TA_j}\middle|A_{SE}\right) \cdot P\left(A_{S_{i,j}}\middle|A_{TA_j}\right) \quad (1)$$

T	threat (/yr)	A	attack on any target
i	index of terrorist attack scenario	A_{EN}	attack on energy sector
j	index of terrorist group	A_{SE}	attack on energy subsector of interest (electrical energy, gas, oil)
k	index of consequence type	A_{TA}	attack on target (energy system) of interest
N_A	number of terrorist attacks in the area of interest (/yr)	A_S	attack according to particular scenario

The equation implies that specific energy system can be attacked in specific way by specific terrorist group only if this group (1) decides to organize an attack, (2) selects energy sector (i.e. energy infrastructure) among all potential targets, (3) selects energy subsector of interest, (4) selects energy system of interest and (5) selects particular attack scenario. The first 3 factors in the equation are determined by utilizing historical data, while the other 2 factors are determined by expert judgment.

The first factor in Equation (1) (the number of the attacks organized per year) is estimated by analyzing how many attacks per year were organized in the past and by taking trends into consideration. The input to the equation is not single value but the probabilistic distribution of values, which allows to take the uncertainties into consideration.

The second factor (the probability of selecting energy sector of interest) is approximated by the relative contribution of the attacks on energy sector towards all terrorist attacks (Figure 3) and by applying the correction factors related to the ideology, presence of armed conflict and the activity of the terrorist group (Figures 6, 7 and 8). This factor, also expressed in the form of the probability distribution, is calculated as follows:

$$P(A_{EN}|A) = P(A_{EN}|A)_0 \cdot f_{ID} \cdot f_{AC} \cdot f_{CO} \tag{2}$$

$P(A_{EN}|A)_0$ uncorrected probability of attack against energy sector

f_{ID} correction factor for terrorist group ideology

f_{AC} correction factor for terrorist group activity

f_{CO} correction factor for security environment

The third factor (the probability of selecting particular energy subsector) is approximated by the relative contribution of the attacks in the subsector of interest (electrical, oil or gas) towards total attacks in energy sector (Figure 4).

The remaining 2 factors in the Equation (1) are much more target specific than the first 3 factors. Because of that, it is more appropriate to estimate them by expert judgment than by utilizing historical data. In order to determine the fourth factor in the formula (the probability of selecting energy system of interest) experts have to assess relative attractiveness of the analyzed energy system by comparing its characteristics with the characteristics of other systems in the subsector. Two "special cases" should be mentioned. First, if the energy system of interest is the only one in the subsector the probability of the selection equals 1. Second, if there are n identical energy systems within the sub sector, this factor amounts to1/n. Those "special cases", however, usually do not apply.

In order to determine the last factor in the Equation (1) (the probability of selecting particular attack scenario), the experts have to compare the attractiveness of various scenarios. This is performed by constructing the so-called utility function for the terrorist group and by estimating the expected utility for each attack scenario:

$$P\left(A_{S_{i,j}} \middle| A_{TA_j}\right) = \frac{EU_{p_{i,j}}}{\sum_i EU_{p_{i,j}}} \tag{3}$$

$$EU_{p_{i,j}} = P_{SU_{p_{i,j}}} \cdot U_{p_{i,j}} \tag{4}$$

$$U_{p_{i,j}} = \sum_k C_{p_{i,j,k}} \cdot w_{Cp_{j,k}} \tag{5}$$

EU_p perceived expected utility

U_p utility function

P_{SU_p} perceived probability of success

C_p perceived magnitude of consequences

w_{Cp} scaling constant

Although the equations for assessing threats are not too complicated, adequate tools have to be used for carrying out the calculations, since the majority of the inputs are probability distributions and not single values. The tools implemented in this case are the Bayesian nets. In addition to the capability for handling the uncertainties, Bayesian nets provide intuitive overview of the variables and their relationships and allow for easy data updating and model transformations. Figure 9 shows how Equation (1) transforms into the Bayesian net. The example refers to the threat assessment where 3 attack scenarios are analyzed and for each scenario 3 types of consequences are taken into consideration.

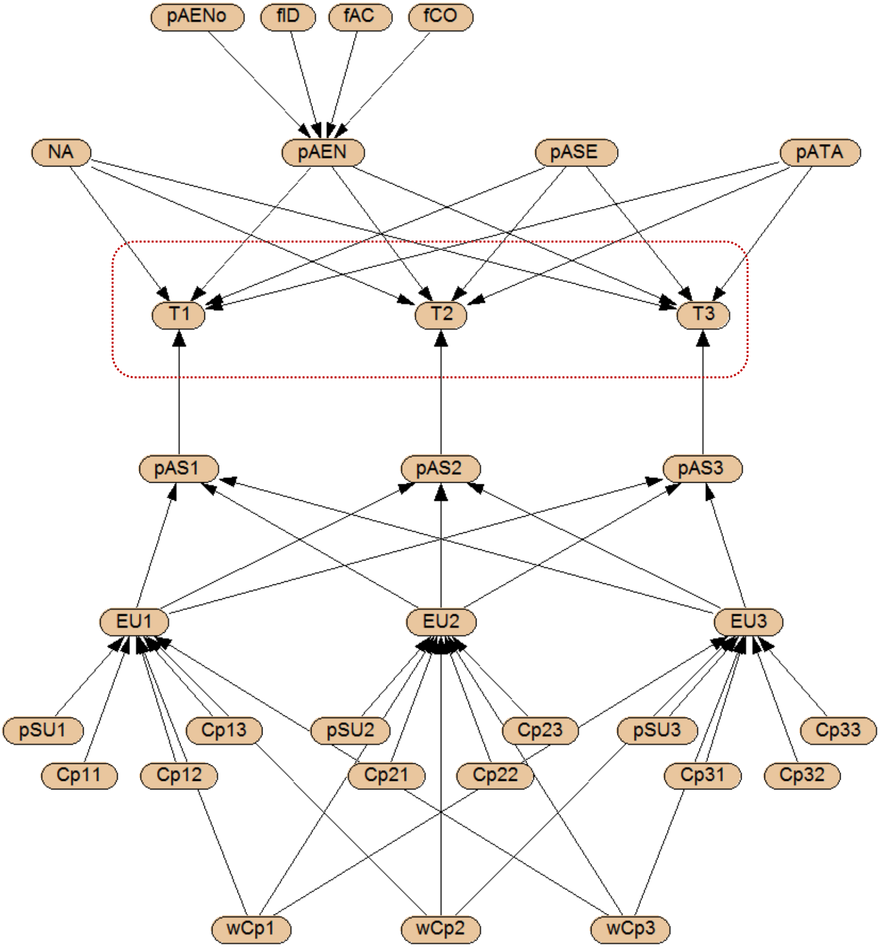

Figure 9: Bayesian net for assessing terrorist threats (example)

On Figure 10 the expanded view of the net shown on Figure 9 is given. In this case not only the variables and their relationships are represented but also input values and the results. The final results (within the area marked with the red line) are provided as expected values and also as probability distributions. The distributions indicate the level of the uncertainty of the results. The input parameters determined by the historical data analysis are grouped in the upper area (i.e. above the final results), while the inputs determined by expert judgment are positioned in the lower area.

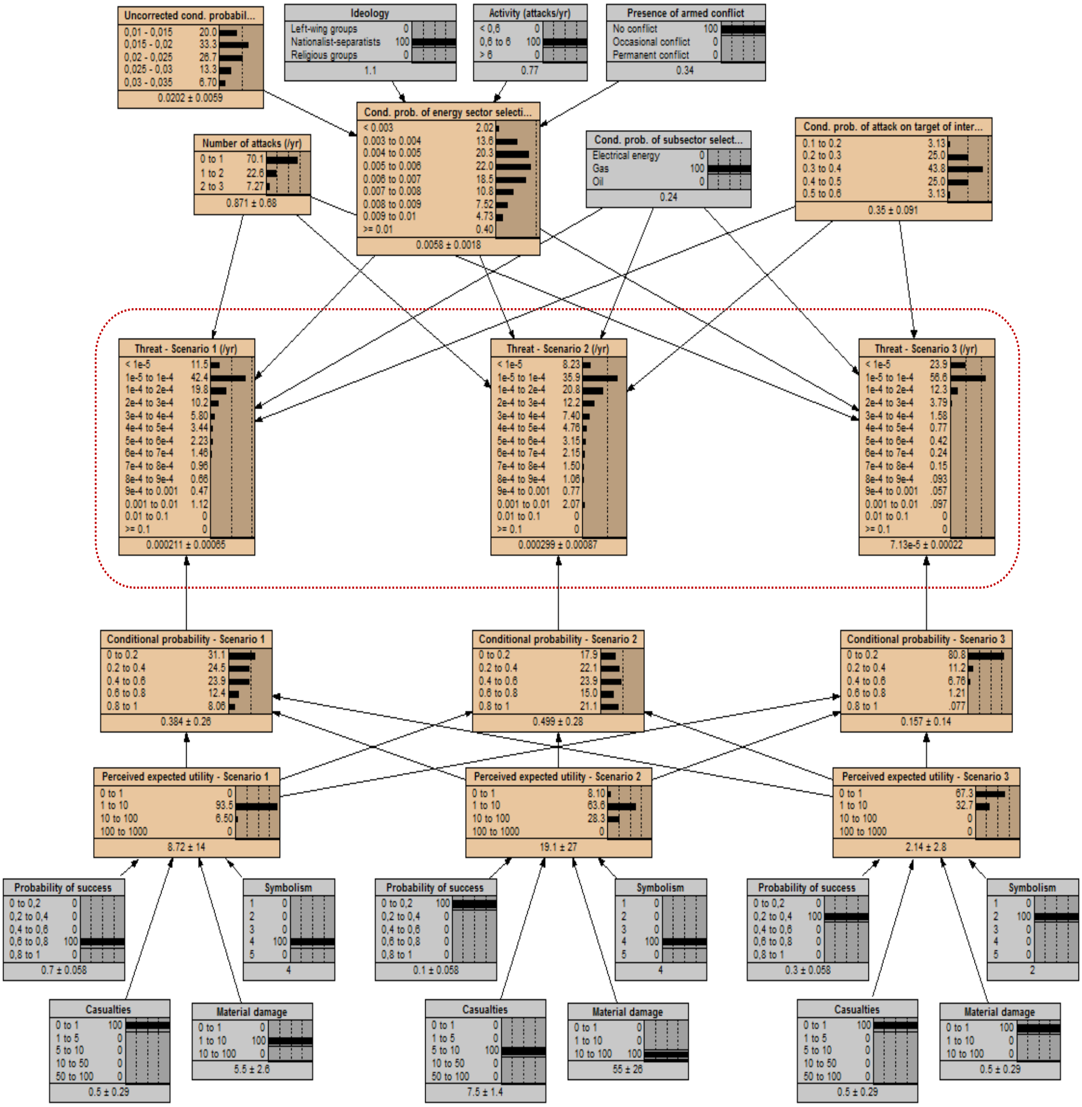

Figure 10: Bayesian net for assessing terrorist threats - expanded view (example)

Conclusion

Within the scope of the research the method for the quantitative assessment of terrorist threats was developed. It allows for combining the historical data and expert judgments and it's designed to be used by energy systems' operators in the electrical, gas and oil sectors.

The proposed method was applied in the pilot project aimed to improve protection strategies and plans for the oil storage and transport system. The system, which is a part of Croatian critical infrastructure, consists of terminals with a total storage capacity of approx. 1,7 x 106 m3and of approx. 620 km long pipelines. The pilot project provided an opportunity to identify strengths and weaknesses of the method. Gathered experience should provide the basis for further improvements.

References

1. Ackermann, G., Abhayarante, P., Bale, J., Bhattacharjee, A., Blair, C., Hansell, L., Jayne, A., Kosal, M., Lucas, S., Moran, K., Seroki, L., Vadlamudi, S., *Asssessing Terrorist Motivations for Attacking Critical Infrastructure, Lawrence Livermore National Laboratory, Livermore, 2007.*
2. P. Toft, A. Duero, A. Bieliauskas, *Terrorist targeting and energy security, Energy Policy, 38, 2010, pp. 4411-4421.*
3. Garrick, B., J., *Perspectives on the Use of Risk Assessment to Address Terrorism, Risk Analysis, Vol. 22, No. 3, 2002., pp. 421-423.*
4. Cox, L., A.*, What's Wrong with Risk Matrices?, Risk Analysis, Vol. 28, No. 2, 2008., pp. 497-512.*
5. Willis, H., H., Morral, A., R., Kelly, T., K., Medby., J., J., *Estimating Terrorism Risk, RAND Center for Terrorism Risk Management Policy, Santa Monica, 2005.*
6. *About the Global Terrorism Database (GTD), available at http://www.start.umd.edu/gtd/about*
7. G. LaFree, L. Dugan, H.V. Fogg, J. Scott, *Building a global terrorism database, University of Maryland, 2006.*