Threat Analysis: Scenarios and Their Likelihoods

Dustin Witte

Institute for Security Systems, University of Wuppertal, Germany. E-mail: dustin.witte@uni-wuppertal.de

Daniel Lichte

Institute for the Protection of Terrestrial Infrastructures, German Aerospace Center, Germany. E-mail: daniel.lichte@dlr.de

Kai-Dietrich Wolf

Institute for Security Systems, University of Wuppertal, Germany. E-mail: wolf@iss.uni-wuppertal.de

To carry out a complete security risk assessment, three fields must be taken into consideration, namely threat, vulnerability and consequence. This paper is dedicated to threat analysis as a process to think ahead scenarios of possible future attacks. An approach for the description of potential threats and the quantification of their likelihoods is presented. The method is based on a common scenario developing process and extended by specifics of security risk assessment considering uncertainties regarding the occurring scenario. The approach is presented in the course of a generic assessment of physical security of a high voltage transmission substation. It is split into three steps. First, an asset is defined for which a space of possible scenarios is construed by structuring feasible threats according to morphological analysis. Therefore, threat descriptors and characteristics are determined for the example of the transmission substation. Second, the likelihoods of scenarios are assessed by judging the cross-impact between characteristics using a Bayesian network. Dependencies between descriptors are assumed. Marginal and conditional probabilities of the characteristics are estimated, respectively. In a final step, a comprehensive list of scenarios is generated by forming the Cartesian product of characteristics grouped by the descriptors. Scenario likelihoods are computed by the chain rule for Bayesian networks. The scenario list can then serve as a starting point for vulnerability and consequence analysis.

Keywords: Threat Analysis, Scenario Development, Morphological Analysis, Cross-Impact Analysis, Bayesian Network, Quantitative Method, Physical Security, Critical Infrastructure Protection.

1. Introduction

To carry out a complete security risk assessment, three fields must be taken into consideration, namely threat, vulnerability and consequence. This paper is dedicated to threat analysis as a process to think ahead scenarios of possible future attacks. Even though in general the attack procedure is unknown in detail, the characteristics of possible attack types should be elaborated, since a valid security risk assessment should at best comprise all feasible attack scenarios.

An attribute of security risk assessment is the high degree of uncertainty regarding the effectiveness of security measures (Garcia, 2017). Concerning threats, multiple sources of uncertainty can be identified. On the one hand there is a lack of knowledge about which type of attack occurs as multiple qualitatively different attacks are feasible. On the other hand there often is a lack of evidence about the likelihoods of occurring scenarios. However, knowledge about potential attacks is crucial in order to design effective security measures. Therefore, methods for threat analysis should consider uncertainties.

Garcia (2008) defines threat analysis as a 'process in which information about a threat or potential threat is subjected to systematic and thorough examination in order to identify significant facts and derive conclusions therefrom.' In this paper, threat analysis is considered as a process to determine plausible threat scenarios and assess corresponding likelihoods.

In this paper we present an approach for the description of potential threats and the assessment of their likelihoods. Uncertainties regarding the effectively occurring scenario are considered, but uncertainties in the likelihood assessment itself are not included. The method is based on a common scenario developing process and extended by specifics of security risk assessment. Descriptors are defined (see Table 1), which structure potential threat characteristics. The development of scenarios is combined with the setup of a Bayesian network to assess the likelihoods quantitatively.

Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
Published by Research Publishing, Singapore.
ISBN: 978-981-14-8593-0; doi:10.3850/978-981-14-8593-0

2. Background

2.1. *Threat Analysis*

Garcia (2008) describes a three-part methodology for threat definition. First, the information needed to describe the threat is determined. This information is then collected in the subsequent process. Garcia names motivation, potential goals based upon targets, tactics, numbers and capabilities as necessary information.

Then, information is collected. Depending on the asset to be protected, regional, national and international threats should be considered. Information can be gained by examining the social conditions, the interest groups and the attractivity of the asset itself. Sources of information are e.g. intelligence, crime analysis and studies, professional organizations and services, published literature and government directives.

Finally, the information is organized. Garcia suggests a table in which the information is specified and judged for each threat that is found. The likelihood of different actions is qualitatively assessed as low, medium or high. The capabilities of the attacker are listed as features.

2.2. *Scenario Development*

Scenario analysis is a common tool to prepare for multiple plausible futures. A variety of techniques for developing scenarios exist (Bishop et al., 2007). A scenario describes a feasible future situation. This paper focuses on predictive scenarios for the purpose of forecasting. Morphological analysis and cross-impact analysis are two techniques valuable for developing predictive scenarios. Both techniques are introduced in the following.

2.2.1. *Morphological Analysis*

Morphological analysis can be used to scan the field of possible futures. More specifically, it is a technique to systematically generate scenarios by structuring the examined problem. The problem is structured by dividing it into multiple dimensions of uncertainties, each describing one part of the problem. For each dimension, a range of possible values have to be defined. A scenario space is construed by combining the values, one for each dimension. (Ritchey, 2006)

The scenario space may contain combinations of values which are inconsistent, either because of logical contradictions or empirical constraints. These scenarios are excluded from the scenario space by a cross-consistency assessment in which the values of different dimensions are compared pair-wise and their consistency is assessed. (Ritchey, 2006)

Johansen (2018) outlines a morphological method for long-term defense planning. Mutually exclusive sets of future states are worked out. By combining the states, a list of all scenarios is derived. The scenarios are filtered by assessing the cross-consistency of the states.

Morphological analysis is a powerful tool to determine scenarios, but a likelihood assessment of scenarios is not part of the technique.

2.2.2. *Cross-Impact Analysis*

Cross-impact analysis according to Gordon (1994) can be used to examine the likelihood of events. It is assumed that scenarios can be characterized by the occurrence or non-occurrence of events. Dependencies between the events can exist and are expressed by conditional probabilities.

Cross-impact analysis comprises two steps. First, the events to be examined are defined. The corresponding scenarios are obtained by combining the events. Second, the probabilities of the events are judged by consulting experts. Both, the marginal probabilities of the events and the conditional probabilities between the event pairs are judged and collected in a cross-impact matrix.

It should be noted that a probabilistic relationship between the probabilities in the cross-impact matrix exists. Inconsistencies can emerge when the probabilities are judged independently. (Moskowitz and Sarin, 1983)

Sarin (1978) describes a method to consider the dependencies between more than two events. The conditional probabilities are judged sequentially for higher order dependencies starting with the marginal probabilities. The axioms of probability theory are obeyed by calculating the minimal and maximal probability and considering their values when judging.

De Kluyver and Moskowitz (1984) describe a method considering only dependencies between two events. A theoretically correct probability is introduced which satisfies the axioms of probability theory. The deviation between judged and theoretically correct probability is measured by deviation terms. The deviation terms are used to minimize the deviation by optimization.

The combination of both techniques, morphological analysis and cross-impact analysis, is demonstrated by Nguyen and Dunn (2009) in the context of defense planning.

2.3. *Bayesian Network*

A Bayesian network is a common way to represent knowledge considering uncertainties (Jensen and Jordan, 2007) and has already been applied to security risk assessment problems, e.g. by Drago et al. (2016) to evaluate the vulnerability of physical protection systems or to assess the vulnerability of gas pipelines (Fakhravar et al., 2017).

A Bayesian network is a probabilistic graphical model. It can be described by a directed acyclic graph consisting of nodes and edges representing random variables and probabilistic dependencies between the variables, respectively. Conditional

Table 1. Descriptors

Descriptor	Description
Actor	Actor describes the affiliation of the potential attacker to distinct groups, e.g. state, extremist network, criminal group, individual.
Goal	The definition of the goal comprises the underlying aims or claims of the actor, ranging from change of political systems to monetary gains.
Target	The target describes the functional unit of the asset which is attacked, e.g. transformer, the transmission lines or the control systems.
Attack Method	Here, the general modus operandi of the attacker to disrupt or destroy the target is outlined.
Attack Means	Attack means characterizes weapons or other tools available to the attacker to disrupt or destroy the attacked target.
Access Means	Access means depicts hardware and tools available to the attacker to break through installed security measures.
Knowledge	Knowledge details the level of knowledge the attacker has regarding the general and specific engineering of target and site, the organization and the characteristics of the security system installed at the site.

probability tables quantify the probabilistic dependencies. (Ben-Gal, 2008)

A Bayesian network represents the joint probability distribution over its random variables. Thus, joint probabilities are consistent with the axioms of probability theory. (Jensen and Jordan, 2007)

De Waal and Ritchey (2007) combine morphological analysis and Bayesian networks for strategic decision support. The method is shown on the basis of a case study for fire-fighting. The impact of situational variables on fire-fighting methods and environmental consequences are analyzed by applying both methods in sequence. First, the most important variables are identified and defined by structuring the problem via morphological analysis. The existence of dependencies between the variables are judged pair-wise analogous to the procedure of a cross-consistency assessment. In a second step, a Bayesian network is set up to quantify the dependencies between the variables. The method seems promising for the development of a comprehensive scenario space together with a well-founded probabilistic model for likelihood assessment.

3. Approach

In the following an approach to analyze threats in the context of physical security is presented. The approach is split into three steps. First, an asset is defined for which a space of possible threat scenarios is developed by determining threat descriptors and characteristics according to morphological analysis. Secondly, likelihoods of scenarios are assessed by judging the cross-impact between the characteristics. For this purpose a Bayesian network, a well-founded model to represent uncertain knowledge, is set up. In a final step, the scenario likelihoods are computed by means of the Bayesian network.

3.1. *Threat Definition*

3.1.1. *Defining the Asset*

The first step is to define the asset, since threat scenarios depend on the asset to be secured. The approach is demonstrated in the course of physical security of a high voltage transmission substation. The function of such a substation is the adjustment of the electric voltage within the power grid. Due to the integrated system of generation, transmission and distribution of electric energy, it is an important element of the power supply. The transmission substation comprises the transformer as well as the transmission lines and control systems connected to the transformer. Depending on the transformed voltage, a transformer may weigh multiple hundred tons, e.g. 435 t for a 345 kV transformer. Most transformers are custom-made and are subject to extensive delivery times. (Parfomak, 2014)

The power supply itself is a critical infrastructure. A disruption potentially has a high impact on modern societies. (Alcaraz and Zeadally, 2015)

3.1.2. *Determining Descriptors and Characteristics*

A threat is here understood as a scenario which comprises information about different key factors. Each factor covers a part of the threat description. Hence, in this paper it is called a threat descriptor. The set of descriptors is defined to cover all threats. A higher number of descriptors increases the differentiation of threats, but also increases the analysis' complexity.

With given descriptors, assumptions about possible characteristics are made. The characteristics here are chosen in a way to describe each threat covered by the analysis sufficiently accurate. Descriptors and sample characteristics shown in Table 1 are suggested.

The transformer substation is further analyzed

Table 2. Selected Descriptors and Characteristics

Actor	Target	Attack Means	Knowledge
State	Transformer	Explosive Weapons	Complete
Extremist Network	Transmission Lines	Handguns	Public
Criminal Group	System Controls	Hand Tools	
Individual			

using a subset of the suggested descriptors to reduce the analysis' complexity without loss of generality. The selected descriptors and characteristics are shown in Table 2. Here, the targets are restricted to the main target types, namely transformer, transmission lines and system controls, but in principle a distinction between multiple targets of the same type, e.g. multiple transformers, is possible by choosing appropriate characteristics. However, their potentially redundant behavior is not part of the threat analysis but may be part of a subsequent consequence analysis.

3.2. *Likelihood Assessment*

After the threat has been defined, the likelihood of scenarios is modeled by a Bayesian network. The Bayesian network is built up based on threat descriptors and their characteristics. The descriptors are used as random variables, while the characteristics form the possible states of the random variables.

The transfer to a Bayesian network is done in two steps. First, the descriptors are related to each other by assuming directed dependencies. A dependency indicates that by knowing the state of one descriptor, the belief of the depending descriptors changes. Figure 1 shows a possible relation of the selected descriptors. Here, the knowledge of the actor influences the judgement regarding the knowledge of the attacker and the attack means. Both, knowledge and attack means influence the judgement of the likelihood of a target to be the aim of an attack.

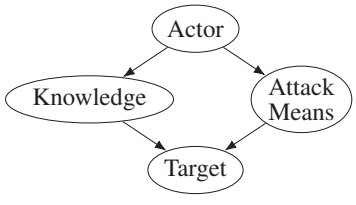

Fig. 1. Descriptor Dependencies

The second step is the quantification of the dependencies by specifying probability tables. The tables contain marginal probabilities for independent descriptors and conditional probabilities for dependent descriptors.

Table 3 shows marginal probabilities for the chosen example. Here, the occurrence of a specific actor is assessed regardless of other descriptors. The likelihood of a state being the actor of a scenario is judged to be very low. Extremist networks are judged to be more likely, even more likely are individuals, while criminal groups are judged to be most likely. The sum of all probabilities has to be equal to one. The judgement may be based on evidence, but when evidence is missing, the likelihoods have to be estimated by experts.

Table 4 and 5 show first order conditional probability tables. The knowledge is assumed to be highly dependent on the actor. A state is judged to always have complete knowledge about the asset, while the likelihood of complete knowledge decreases from extremist network over criminal group to individual. Similarly the access to and use of attack means is judged.

Table 6 shows a second order conditional probability table. The target of an attack depends on two descriptors. In addition to specific attack means, the degree of knowledge about the asset is assumed to be significant for choosing targets. For instance given that the attacker uses hand tools and has only public knowledge about the asset, it is judged that both, the transformer and the control systems, will be target of an attack. However, when the attacker uses the same means but has complete knowledge an attack of control systems seems more likely.

Table 3. Marginal Probability Table of Actor

State	Extremist Network	Criminal Group	Individual
0.01	0.09	0.60	0.30

3.3. *Threat Evaluation*

After defining the threats and assessing their likelihoods, the scenarios are generated by calculating the Cartesian product of the characteristics grouped by descriptors. Thereby all characteristics, which are part of different descriptors, are combined. The result is a list of all scenarios construable on the basis of the threat definition.

Table 4. Conditional Probability Table of Knowledge

Actor	Knowledge	
	Complete	Public
State	1.00	0.00
Extremist Network	0.40	0.60
Criminal Group	0.30	0.70
Individual	0.05	0.95

Table 5. Conditional Probability Table of Attack Means

Actor	Attack Means		
	Explosive Weapons	Handguns	Hand Tools
State	1.00	0.00	0.00
Extremist Network	0.50	0.50	0.00
Criminal Group	0.00	0.40	0.60
Individual	0.00	0.10	0.90

Table 6. Conditional Probability Table of Target

Attack Means	Knowledge	Target		
		Transformer	Transmission Lines	System Controls
Explosive Weapons	Complete	0.80	0.10	0.10
Explosive Weapons	Public	0.80	0.10	0.10
Handguns	Complete	0.20	0.00	0.80
Handguns	Public	0.40	0.00	0.60
Hand Tools	Complete	0.10	0.00	0.90
Hand Tools	Public	0.40	0.00	0.60

The probability of each scenario is computed by the chain rule for Bayesian networks (Jensen and Jordan, 2007):

$$P(S_i) = \prod_{k=1}^{K} P(A_{k,i} \mid \mathrm{pa}(A_{k,i})) \qquad (1)$$

where S_i is the i-th scenario, K the number of descriptors and $A_{k,i}$ the characteristic of the k-th descriptor which is part of the i-th scenario. $\mathrm{pa}(A_{k,i})$ refers to all characteristics which are parents of $A_{k,i}$ in the dependency graph and also part of the i-th scenario.

For example, the probability of the scenario of an extremist network having public knowledge about the asset attacks the transformer by using explosive weapons is computed as follows:

$$\begin{aligned} &P(\text{Extremist Network}, \text{Public Knowledge}, \\ &\quad \text{Explosive Weapons}, \text{Transformer}) \\ &= P(\text{Extremist Network}) \\ &\quad \cdot P(\text{Public Knowledge} \mid \text{Extremist Network}) \\ &\quad \cdot P(\text{Explosive Weapons} \mid \text{Extremist Network}) \\ &\quad \cdot P(\text{Transformer} \mid \text{Public Knowledge}, \\ &\qquad\qquad \text{Explosive Weapons}) \\ &= 0.09 \cdot 0.6 \cdot 0.5 \cdot 0.8 \\ &= 0.0216 \end{aligned} \qquad (2)$$

The evaluation for the transmission substation produces a total of 72 scenarios. Table 7 lists a selection of these scenarios and corresponding likelihoods. They are ranked according to their likelihood to point out the most likely scenarios. Scenarios with a resulting likelihood of zero are not listed, as they are inconsistent within this assessment. It can be seen that attacks with hand tools and public knowledge, either committed by an individual or a criminal group, are most likely. It should be noted that the list only represents the likelihood of threat scenarios. Vulnerability and the consequences of such scenarios are not assessed here.

As the number of scenarios is large, the likelihood for single scenarios is small, especially when using all suggested descriptors. Thus, a cluster analysis may be useful to work out groups of similar scenarios systematically.

4. Conclusion

An approach for threat analysis considering uncertainties regarding the occurring scenario was shown using the example of a high voltage transmission substation. After defining the asset, a scenario space for threats was construed by determining the descriptors actor, target, attack means and knowledge together with possible characteristics for each descriptor. The belief in combinations of characteristics was assessed via a Bayesian network. The assessment resulted in a joint probability distribution from which the likelihood of whole scenarios were computed by applying the chain rule for Bayesian networks.

The approach enables the creation of a comprehensive scenario space due to morphological analysis, thus enabling a potentially comprehensive and consistent threat analysis. As the likelihood assessment is based on a Bayesian network, it is probabilistically well-founded and can be solved using common tools for analysis of Bayesian networks. The analysis process is not restricted to threat analysis of physical security. It is conceivable that the descriptors can be extended to include all type of situations, e.g. natural hazards,

Table 7. Ranked Scenarios

Likelyhood	Characteristics			
	Actor	Knowledge	Target	Attack Means
0.1539	Individual	Public	System Controls	Hand Tools
0.1512	Criminal Group	Public	System Controls	Hand Tools
0.1026	Individual	Public	Transformer	Hand Tools
0.1008	Criminal Group	Public	Transformer	Hand Tools
0.1008	Criminal Group	Public	System Controls	Handguns
0.0972	Criminal Group	Complete	System Controls	Hand Tools
0.0672	Criminal Group	Public	Transformer	Handguns
0.0576	Criminal Group	Complete	System Controls	Handguns
0.0216	Extremist Network	Public	Transformer	Explosive Weapons
0.0171	Individual	Public	System Controls	Handguns
0.0162	Extremist Network	Public	System Controls	Handguns
0.0144	Extremist Network	Complete	Transformer	Explosive Weapons
0.0144	Extremist Network	Complete	System Controls	Handguns
0.0144	Criminal Group	Complete	Transformer	Handguns
0.0121	Individual	Complete	System Controls	Hand Tools
0.0114	Individual	Public	Transformer	Handguns
0.0108	Extremist Network	Public	Transformer	Handguns
0.0108	Criminal Group	Complete	Transformer	Hand Tools
0.0080	State	Complete	Transformer	Explosive Weapons
0.0036	Extremist Network	Complete	Transformer	Handguns
0.0027	Extremist Network	Public	Transmission Lines	Explosive Weapons
0.0027	Extremist Network	Public	System Controls	Explosive Weapons
0.0018	Extremist Network	Complete	Transmission Lines	Explosive Weapons
0.0018	Extremist Network	Complete	System Controls	Explosive Weapons
0.0014	Individual	Complete	Transformer	Hand Tools
0.0012	Individual	Complete	System Controls	Handguns
0.0010	State	Complete	Transmission Lines	Explosive Weapons
0.0010	State	Complete	System Controls	Explosive Weapons
0.0003	Individual	Complete	Transformer	Handguns
0.0000	State	Complete	Transformer	Handguns
⋮	⋮	⋮	⋮	⋮

accidents and operational failures.

The comprehensive scenario list can serve as a starting point for vulnerability and consequence analysis by extracting relevant scenarios. For this purpose further methods to find relevant scenario groups may be useful, e.g. cluster analysis.

The assumption of dependencies between descriptors may be a difficult task. The process may be simplified by combining the set up of the Bayesian network with a cross-impact method. First, all marginal and conditional probabilities could be assessed independent of previously defined dependencies as part of the cross-impact analysis. Then the likelihood judgement could be transferred to a Bayesian network. To consider uncertainties regarding expert knowledge, appropriate distributions may be used in the Bayesian network.

References

Alcaraz, C. and S. Zeadally (2015, January). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection 8*, 53–66.

Ben-Gal, I. (2008). Bayesian networks. In F. Ruggeri, R. S. Kenett, and F. W. Faltin (Eds.), *Encyclopedia of Statistics in Quality and Reliability*. Wiley.

Bishop, P., A. Hines, and T. Collins (2007, February). The current state of scenario development: an overview of techniques. *Foresight 9*(1), 5–25.

de Kluyver, C. A. and H. Moskowitz (1984, March). Assessing scenario probabilities via interactive goal programming. *Management Science 30*(3), 273–278.

de Waal, A. and T. Ritchey (2007, December). Combining morphological analysis and bayesian networks for strategic decision support.

ORiON 23(2).

Drago, A., S. Marrone, N. Mazzocca, R. Nardone, A. Tedesco, and V. Vittorini (2016, December). A model-driven approach for vulnerability evaluation of modern physical protection systems. *Software & Systems Modeling*.

Fakhravar, D., N. Khakzad, G. Reniers, and V. Cozzani (2017). Security vulnerability assessment of gas pipelines using bayesian network. In M. Čepin and R. Briš (Eds.), *Safety and Reliability*, Leiden, the Netherlands. CRC Press.

Garcia, M. L. (2008). *The Design and Evaluation of Physical Protection Systems* (Second ed.). Amsterdam: Elsevier, Imprint: Butterworth-Heinemann.

Garcia, M. L. (2017). Introduction to vulnerability assessment. In L. J. Fennelly (Ed.), *Effective Physical Security* (Fifth ed.)., pp. 23–53. Amsterdam: Elsevier, Imprint: Butterworth-Heinemann.

Gordon, T. J. (1994). Cross-impact method. *Millennium Project*.

Jensen, F. V. and Jordan (2007, February). *Bayesian Networks and Decision Graphs* (Second ed.). Information Science and Statistics. Berlin: Springer.

Johansen, I. (2018). Scenario modelling with morphological analysis. *Technological Forecasting & Social Change 126*, 116–125.

Moskowitz, H. and R. K. Sarin (1983, June). Improving the consistency of conditional probability assessments for forecasting and decision making. *Management Science 29*(6), 735–749.

Nguyen, M.-T. and M. Dunn (2009). Some methods for scenario analysis in defence strategic planning. Technical Report DSTO-TR-2242, Defence Science and Technology Organisation, Canberra, Australia.

Parfomak, P. W. (2014, June). Physical security of the u.s. power grid: High-voltage transformer substations. Technical Report R43604, Library of Congress, Congressional Research Service, Washington D.C., United States.

Ritchey, T. (2006, July). Problem structuring using computer-aided morphological analysis. *Journal of the Operational Research Society 57*(7), 792–801.

Sarin, R. K. (1978, February). A sequential approach to cross-impact analysis. *Futures 10*(1), 53–62.