Comprehensive Security Hazard Analysis for Transmission Systems

Daniel Lichte
German Aerospace Center
daniel.lichte@dlr.de

Dustin Witte
University of Wuppertal
witte@uni-wuppertal.de

Kai-Dietrich Wolf
University of Wuppertal
wolf@iss.uni-wuppertal.de

ABSTRACT

Critical energy infrastructures are more and more focused upon by politics and society. Modern society depends on these structures, since they enable the steady support of electricity and other types of energy. Deliberately precipitated hazards of certain critical parts of electrical transmission systems (ETS) can lead to catastrophic consequences. Therefore, the analysis of feasible security hazards and resulting consequences for the operation of transmission systems are a concern to transmission system operators (TSO). Alas, there is no common method available that comprehensively identifies these feasible security related scenarios and classifies them according to their overall criticality for the safe operation of the ETS. To tackle this challenge, we propose a comprehensive, yet easy-to-apply method to systematically identify and assess the criticality of security threat scenarios. It is conducted in four steps and consists of a matrix based consistency check of threat scenarios in a defined solution space and a convenient semi-quantitative assessment of a risk factor for the ETS. The approach is illustrated by the simplified generic example of an EETS.

Keywords

Physical Security, Energy Transmission Systems, Scenario Analysis, Threat Analysis, Risk Assessment.

INTRODUCTION

Critical energy infrastructures are more and more focused upon by politics and society. Modern society depends on these structures, since they enable the steady support of electricity and other types of energy. Energy infrastructures are usually broadly distributed, connecting different regions and even countries by the energy transmission system (ETS). Thus, deliberately precipitated hazards of certain critical parts of these transmission systems can lead to catastrophic consequences, e.g. the failures of energy supply in whole regions and following cascading effects.

Therefore, the analysis of feasible security hazards and resulting consequences for the operation of transmission systems are a concern for transmission system operators (TSO). Additionally, future regulations require the implementation and assessment of security measures. Since ETS offer a large number of feasible attack targets to potential attackers, prioritization of assets regarding security threat scenarios as well as asset criticality is mandatory.

Unfortunately, there is no common method available that comprehensively identifies these feasible security related scenarios and classifies them according to their overall criticality for the safe operation of the ETS. The analysis is even more complex considering the complex variety of components in an ETS and the individual level of vulnerability of these components.

To tackle this challenge, we propose a comprehensive, yet easy-to-apply method to systematically identify and assess the criticality of security threat scenarios. It is conducted in four steps and consists of a matrix-based consistency check of threat scenarios in a defined solution space and a convenient semi-quantitative assessment of a risk factor for the ETS. Hence, it enables the ranking of revealed security threats by either ETS criticality (consequences) or likelihood of occurrence. Simultaneously to its development, the approach is, due to non-

disclosure reasons, exemplarily applied to structures of an ETS. Finally, a summary over the presented procedure is given and the results are discussed, especially regarding the practical application and future work towards further enhancements.

BACKGROUND

Electric ETS (EETS) are considered critical infrastructures, since they enable the support of electrical energy. EETS, like other ETS, consist of different components needed for the distribution over long distances and transformation of high voltage electricity, e.g. 220/380 kV in Germany.

The complex structure mainly consists of overhead transmission lines and corresponding tension towers. Substations realize control and transfer to local distribution networks. Main components of substations are transformer, process control technique in control stands, big open air switching bays with bus bars along with other subcomponents (Parfomak 2014).

Although the array of the components is not very complex, the whole EETS is a very complex structure principally vulnerable to the failure of single elements of the network. The TSO undertakes a variety of functional safety measures to ensure a reliable supply of electricity, which is demanded by legislature (EnWG 2005). These measures comprise especially the (n-1)-rule of redundancy within the ETS (Schwab, 2009).

Additional to a safe and reliable operation, the legislator provides regulation to measures of cyber security to be taken against malicious attacks (EnWG 2005). Physical security of the ETS infrastructure is not yet regulated, there exists only a legal duty to implement safety precautions for trespassers so far. Since the vulnerability of EETS against i.e. terrorist attacks is increasingly focused upon, the physical security will be explicitly part of future standards, e.g. the NERC CIP-014-2 (NERC 2015). Therefore TSO are currently taking up this topic.

Physical Security Risk Analysis

Physical security risk analysis in general is still an emerging field in science and practice. The definition of risk in this context is usually defined as (Contini et al. 2012, Mc Gill et al. 2007):

$$Risk = Threat \times Vulnerability \times Consequence \quad (1)$$

Various approaches to security risk assessment have been developed that may be divided into qualitative, quantitative and hybrid methods (Meritt 2008). Qualitative methods are mostly based on expert knowledge, while existing quantitative methods use discrete probabilities. The former are more widespread because of their ease of use, while at the same time the application of expert knowledge can lead to inaccurate or even wrong results (Landoll 2011). Additionally, some quantitative methods aiming at cost-benefit analysis have been developed. Typically, cost-benefit analyses of security measures would account for potential financial losses as result of an attack, the probability of occurrence of various attack scenarios and the vulnerability of the security system (Flammini et al. 2009). A comprehensive and field applicable framework that directly addresses the security of energy infrastructures was prepared by the Harnser Group for the European Commission (Harnser 2010). It is based on semi-quantitative methods and provides detailed processes and assessment metrics.

However, most approaches to security risk assessments concentrate on the assessment of vulnerability to attacks and are mostly dependent on specific attack scenarios (French & Gootzit 2011). This dependency is detrimental to a comprehensive analysis as knowledge about the behavior of a potential attacker may be insufficient (Cox Jr. 2009). Hence, a comprehensive as possible analysis of threats, e.g. attack scenarios or security hazards is important for the assessment of vulnerability and security risk as well. Garcia (2008) describes threat analysis as a process of systematic analysis to identify significant facts and implications. She proposes a method based on information gathering and organization. However, structured methods to identify threats and attack scenarios systematically are not commonly used in practice. This part of analysis mostly relies heavily on expert knowledge and is often based on creativity techniques like brainstorming, e.g. like proposed by Harnser (2010). Thus, systematically revealing feasible attack scenarios is a difficult task.

Scenario Analysis

Here, approaches to scenario analysis used in general risk analysis appear to be useful to facilitate and develop a structured comprehensive security threat or hazard analysis. A method for a systematical prediction of potential future states is the scenario technique. The technique aims at considering all influencing factors in a networked system to describe possible future scenarios (Gausemeier et al. 2014). Its usage is widespread e.g. in business administration and strategic planning. Among others, the main part of the scenario technique is the building of

scenarios. Here, a consistency check between the different estimated future states of the influencing factors of the scenario is conducted and consistent scenarios are then described in detail. The consistency check usually uses consistency matrices and due to its complexity, the implementation is computer-aided (Dönitz 2009).

Scenario analysis methods are known in defense, especially in the area of general future strategic planning. An overview is given in Nguyen and Dunn (2009). A current approach was introduced by Johansen (2018). In this approach a consistency matrix is used to determine feasible scenarios within a solution space defined by higher level categories. These categories are further detailed by characteristics determining the boundaries of the solution space. The categories and corresponding characteristics are then checked for consistency with the characteristics of all other categories.

Further, there are additional approaches that do not only check for consistency but also address the issue of varying likelihood of occurrence for each determined feasible scenario, e.g. (Jensen and Jordan 2007; de Kluyver et al. 1984). These approaches require rather detailed knowledge of the variety of characteristics used and are mathematically elaborate. Thus, the application of these methods in the field of security seems challenging.

APPROACH

The here presented work-in-progress approach aims at meeting the demands of TSO for applicable methods concerning security risk assessment. Herein, a comprehensive security hazard analysis is an important first step. Therefore the method is developed with a practical orientation. It is divided into four consecutive steps. In a first step a solution space of scenarios is defined. This allows a check of scenario consistency in a second step by application of a consistency matrix. After checking the scenario consistency, the third step consists of reasonable clustering and addition of feasible assets of an ETS to the consistency matrix. The concluding semi-quantitative risk–factor estimation is accomplished in the last step.

Since the approach is considered as work-in-progress, the application to a specific ETS is not yet finished. Due to non-disclosure agreements and ongoing application the method is only generically shown.

Defining a solution space

Defining the solution space is the first step of the presented approach, as it is preliminary for the establishment of the consistency matrix. Spanning the solution space starts with the definition of high-level categories needed for a thorough security scenario description. Usually this covers at least the categories used in the generic example of a category list shown in Table 1.

Table 1. Category List

Attacker	Mission Objective	Modus Operandi
State	Destruction	Pick-Up truck, small IED's
Terrorist	Disturbance	Drones and explosives
Criminal	Financial gain	Hobby tools, side cutter

The list in Table 1 shows a minimum configuration, further categories should be added depending on the requested level of detail. For example, distinguishing between general objectives (e.g. political) and mission objectives, separation of tools for intrusion and attack, introduction of level of knowledge (compare Harnser (2010)).

Following, characteristics are defined to specify the set-up categories as shown in the example in Table 1. Here, the elicitation of expert knowledge from both sides, TSO as well as security experts seem to make sense to compile characterizations of the chosen categories as thorough as possible.

However, the size of the solution space should be cautiously considered (Johansen 2018). On the one hand, it should include all feasible scenarios. On the other hand, the number of included scenarios is a result of a combinatorial computation. Thus, for example a scenario space with c=3 categories with n=3 characteristics each leads to a high number of included scenarios:

$$n^c = 3^3 = 27$$

Checking consistency of scenarios

As the solution space is defined, the consistency matrix is then used to check the consistency of these characteristics in the different categories. Figure 1 shows the resulting consistency matrix M for the simple solution space in Table 1.

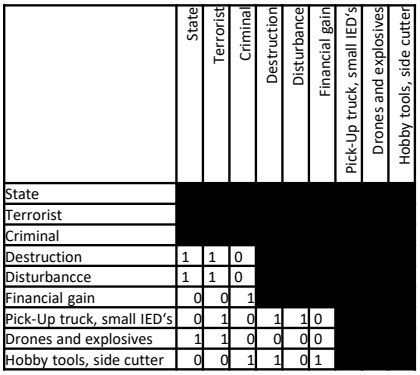

Figure 1. Consistency Matrix M for Solution Space

The depicted matrix in Figure 1 is only diagonally used for checking consistency by comparing the characteristics of each category with those of all other categories. Hence, a thorough cross checking is possible, where only basic consistency is considered. An estimation of a likelihood of such combinations is not conducted. Since manual evaluation is not manageable for a higher number of categories and characteristics, a computer-based analysis is helpful. The result of cross-checking the elements of the consistency matrix is a list of all basically consistent scenarios regardless of their likelihood of occurrence. Hence, also scenarios which are very unlikely to occur (black swan events) are part of the further conducted hazard analysis. Table 2 shows a list of the scenarios resulting from the example.

Table 2. List of Consistent Scenarios

Attacker	Mission Objective	Modus Operandi
State	Destruction	Drones and Explosives
	Disturbance	Drones and Explosives
Terrorist	Destruction	Pick-Up truck, small IED's
		Drones and Explosives
	Disturbance	Pick-Up truck, small IED's
		Drones and Explosives
Criminal	Financial Gain	Hobby Tools, Side Cutter

The list in Table 2 shows that very unlikely scenarios are now further considered, as they are basically consistent. These scenarios potentially remain unconsidered when the feasible solution is not systematically analyzed.

Clustering and addition of assets to consistency matrix

The third step consists of clustering assets followed by the addition of the clustered assets to the consistency matrix. Asset clustering is reasonable due to the relatively great number of components in EETS and their conclusive allocation to the functional structures of the EETS. Thus, the functional structure specifies the asset clusters. Examples of distinct functional structures in an EETS used for the example are listed in Table 3.

Table 3. Examples of Functional Structures in an EETS

Asset Cluster	Sub-Assets
Transformer	Active Part
	Buchholz Relais

	Grommet
	Cooling Devices
Control Stands	Central Process Cell Unit
	Process Control Technique
	Distributing Cabinet
	Optical Fiber Connection
Switching Bays	Circuit Breaker
	Cutoff Switch
	Isolator
	Conductors

The defined functional structures fulfill specific sub processes, which supply the key processes of energy transmission and transforming. The clustering in functional structures is reasonable, since the malfunction of single components in these clusters leads at least to a loss of the sub function or process. Hence, a differentiation between these components regarding their criticality to the key processes is not possible. Additionally, the topographical location of the components is strictly based on the functional structure.

Following, the defined asset clusters are then added to the consistency matrix. Here, the consistency is only checked for the attack means and their potential effect on the asset cluster. Figure 2 shows the updated consistency matrix.

	State	Terrorist	Criminal	Destruction	Disturbance	Financial gain	Pick-Up truck, small IED's	Drones and explosives	Hobby tools, side cutter	Transformator	Control Stand	Switching Bays
State												
Terrorist												
Criminal												
Destruction	1	1	0									
Disturbancce	1	1	0									
Financial gain	0	0	1									
Pick-Up truck, small IED's	0	1	0	1	1	0						
Drones and explosives	1	1	1	1	0	0						
Hobby tools, side cutter	0	0	1	1	0	1						
Transformator							1	1	0			
Control Stand							1	0	0			
Switching Bays							1	1	1			

Figure 2. Updated Consistency Matrix with Clustered Assets

The resulting consistent scenarios including the attacked asset for the used example are listed in Table 4.

Table 4. Updated Feasible Attack Scenarios Including Assets

#	Attacker	Mission Objective	Modus Operandi	Asset
1	State	Destruction	Drones and Explosives	Transformer
2				Switching Bays
3	State	Disturbance	Drones and Explosives	Transformer
4				Switching Bays
5	Terrorist	Destruction	Pick-Up truck, small IED's	Transformer
6				Control Stand
7				Switching Bays
8			Drones and Explosives	Transformer
9				Switching Bays

10		Disturbance	Pick-Up truck, small IED's	Transformer
11				Control Stand
12				Switching Bays
13			Drones and Explosives	Transformer
14				Switching Bays
15	Criminal	Financial Gain	Hobby Tools, Side Cutter	Switching Bays

Table 4 shows that the attack modes applicable to the assets vary. Hence, not all assets are potential aims for the varying attack scenarios. The criticality of the asset cluster is estimated in the next section.

Risk-Factor estimation

In this last step, the risk factor is estimated by applying a straight-forward semi-quantitative scheme. The scheme consists of four different unweighted assessment categories. Figure 3 shows the assessment scheme.

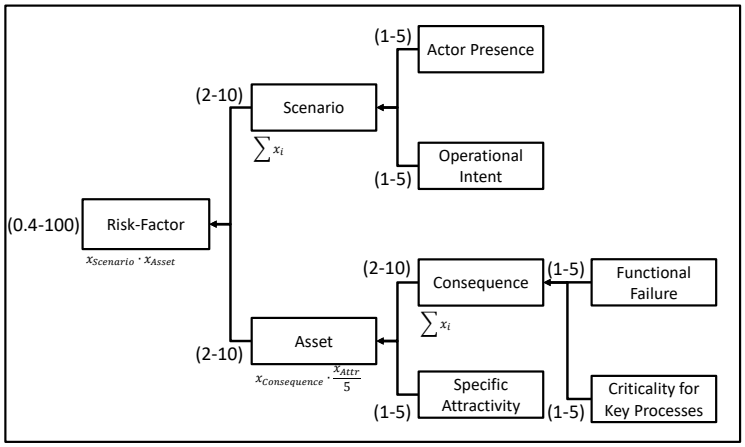

Figure 3. Scheme for Risk-Factor Estimation

The two main comprised assessment levels are scenario and asset factors. The presence of the actor in the surrounding of the considered infrastructure, as well as the estimation of the intent to conduct attacks is assessed within the scenario factor. Figure 4 shows the rating scheme for scenario factors and the functional failure likelihood as part of the asset factors.

Functional Failure

Score		Description
1	Very low	Damage unlikely, No limitation of function
2	Low	Light damage, Limitation of function unlikely
3	Medium	Visible damage, Light limitation of function
4	High	Major damage, Limitation of function likely
5	Very high	Destruction, Functional failure

Actor Presence / Operational Intent

Score		regional	national	Inter-national	
1	Very low			X	Potential
					Documented
2	Low		X	X	Potential
				X	Documented
3	Medium		X	X	Potential
			X	X	Documented
4	High	X	X	X	Potential
			X	X	Documented
5	Very high	X	X	X	Potential
		X	X	X	Documented

Figure 4. Rating Scheme for Assessment Factors

For the scenario factors, we use available evidence of expert sources to rate the presence of the actor and similar attacks. Additionally, Figure 4 outlines how to rate the functional failure factor. Similar to the other factors, expert knowledge is used for judgement. In this case, it is rational to involve technical knowledge from the TSO. The knowledge of the TSO is also needed when estimating the criticality of the sub processes and corresponding assets within the ETS for the key processes. Its estimation is a separate procedure itself, which is not discussed further in this paper. Analogously to the other factors of the scheme, the resulting ratings can range from "very low" (1) to "very high" (5). Possible results for the considered asset clusters are given in Table 5. The consecutive consequence estimation of severity is computed by summarizing the ratings of likelihood of functional failure and

asset criticality (see Figure 4).

Table 5. Possible results of asset criticality estimations

Asset Cluster	Criticality
Transformer	5
Control Stands	4
Switching Bays	3

The last considered factor on asset level is the attractiveness of the asset clusters to the specific generated scenarios. Here, the rating should be done separately for every consistent scenario set up by the analysis. Thus, the results for an asset cluster may differ depending on the categories chosen for the consistency analysis. The scenario-specific attractiveness is added to the consequence assessment as an additional factor solely able to lower the asset factor (see Figure 4).

Finally asset and scenario level ratings are combined to estimate a risk factor. It considers both factors equally by multiplying the result of both, scenario and asset factor (see Figure 4). The resulting risk factors vary between 0.8 (low risk) and 100 (high risk). The computed results for the generated scenarios of the generic example are listed in Table 6.

Table 6. Results for Risk Factor Assessment

#	Actor Presence	Operational Intent	Functional Failure	Criticality	Specific Attractivity	Scenario Factor	Asset Factor	Risk Factor
1	1	1	5	5	5	3	10	30
2	1	1	4	3	3	3	3	9
3	1	1	5	5	5	3	7	21
4	1	1	4	3	5	3	5	15
5	3	3	5	5	5	6	8	48
6	3	3	5	4	4	6	5.6	33.6
7	3	3	4	3	3	6	3.6	21.6
8	3	3	5	5	5	6	8	48
9	3	3	4	3	3	6	3.6	21.6
10	3	3	5	5	5	6	8	48
11	3	3	3	4	4	6	5.6	33.6
12	3	3	4	3	3	6	3.6	21.6
13	3	3	5	5	5	6	8	48
14	3	3	4	3	3	6	3.6	21.6
15	5	5	1	3	4	10	6.4	64

The results arranged in descending order regarding the estimated risk factor show differing, wide varying risk results. It gets visible that the set-up scenario list also includes attack scenarios with very low-level risk estimation. To make the results more accessible, the usage of a security hazard risk matrix as shown in Figure 5 is helpful to visualize them.

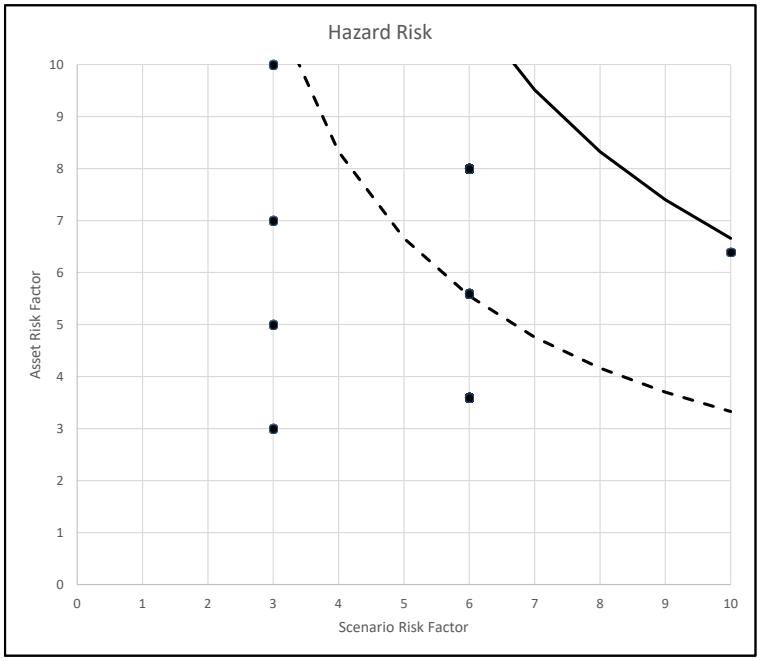

Figure 5. Security Hazard Risk Matrix

In Figure 5, the grey lines denote thresholds indicating the intensity of consideration in further analysis of security measures. In our example, the dashed line marks an overall hazard risk rating of 33.3, thus one third of the possible range of rankings. Scenarios below this first threshold are of low priority for further analysis, while scenarios exceeding a rating of 33.3 are considered important but not critical for security analysis and investment decisions. Accordingly, the drawn-through line marks the threshold for the hazard scenarios that should be prioritized in further analysis. Lowering the vulnerability of these scenarios exceeding a rating of 66.6 with appropriate security measures is the benchmark criterion for the further security analysis process.

CONCLUSION

This paper introduces a straight-forward practical approach to security hazard analysis that enables a comprehensive view on feasible security threat scenarios. It is developed as a part of a broader physical security analysis for EETS, but is suitable for the application of security analysis to other domains.

To reach this goal, the approach uses a matrix-based method to create consistent scenarios of varying characterizations of different categories. The characterizations describe the differing scenarios, while the number of categories can be increased to reach a more detailed scenario description. In a second step, assets are clustered topographically as well as functionally and cross-checked for consistency with the set-up scenarios. Following, we introduce the straight-forward rating scheme for risk factor estimation. Thus, it is possible to estimate the likelihood of every consistent feasible scenario. Therefore, asset as well as scenario factors are considered in the assessment. In a last step, the usage of a threat risk matrix is proposed to support the visualization of the overall risk. Therein, rating thresholds of 33.3 and 66.6 on the rating scale ranging from 0.25 to 100 are proposed to set possible levels of prioritization.

As a result, the presented approach expands common security threat analysis by a systematic procedure that enables a comprehensive consideration of scenarios including those with very low probability occurrence but severe consequences. Additionally, it combines the probability of functional failure of the asset with its process criticality. However, this rating requires the definition of key processes as well as component criticality.

Practice shows that the approach allows adapting the level of detail for most applications. At the same time, this remains a challenge besides the overall easy implementation in TSO environment. Balancing between the desired level of detail needed for analysis and the rapid growth of the solution space tends to be time-consuming. Furthermore, highly detailed scenario spaces show great overlaps in resulting scenario characterizations. Combined with the easily implementable but rather rough estimation of scenario likelihood this leads to higher numbers of very similar scenarios. Clustering of these scenarios represents a possible solution.

Further work is needed in order to embed the threat analysis process into the higher level security risk assessment. Additionally, further evaluation, for example on other ETS or similar infrastructures, should be done. A huge

overall task is the ongoing development of more sophisticated methods to create a comprehensive set of scenarios considering the estimated likelihood of their realization.

REFERENCES

Contini, S. & Fabbri, L. & Matuzas, V. and Cojazzi, G. (2012) Protection of Multiple Assets to Intentional Attacks. A Methodological Framework, 11th Probalistic Safety Assessment 2012, Proc. intern. conf., Helsinki.

Cox Jr., L. A. (2009) Risk Analysis of Complex and Uncertain Systems, Springer, New York.

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

Dönitz, E. (2009) Effizientere Szenariotechnik durch teilautomatische Generierung von Konsistenzmatrizen, Gabler Verlag, Wiesbaden.

Flammini, F., Gaglione, A., Mazzocca, N. and Pragliola, C. (2009) Quantitative security risk assessment and management for railway transportation infrastructures, Critical Information Infrastructure Security, Springer, Berlin.

French, G. S. and Gootzit, D. (2011) Defining and Assessing Vulnerability of Infrastructure to Terrorist Attack, Vulnerability, Unvertainty and Risk: Analysis, Modeling and Management, Proc. conf., Hyattsville.

Gausemeier, J., Plass, C. and Wenzelmann, C. (2014) Zukunftsorientierte Unternehmensgestaltung. Strate-gien, Geschäftsprozesse und IT-Systeme für die Produktion von morgen, Carl Hanser Verlag, München.

Garcia, M. L. (2008) The Design and Evaluation of Physical Protection Systems, 2nd ed, Butterworth-Heinemann, Burlington.

German Energy Industry Act (EnWG) (2005), §11(1) §12(1).

German Federal Industry of the Interior (2008), Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), Berlin.

Harnser Group (Ed.) 2010. A Reference Security Management Plan for Energy Infrastructure, European Commission, Brussels.

Jensen, F. V. and Jordan (2007) Bayesian Networks and Decision Graphs, Information Science and Statistics, Springer, Berlin.

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

Landoll, D. J. (2011) The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments, 2nd ed., CRC Press, Boca Raton.

McGill, W. L., Ayyub, B. M. and Kaminskiy, M. (2007) Risk Analysis for Critical Asset Protection, Risk Analysis, 27 (5), 1265–1281.

Meritt, J. W. (2008) A Method for Quantitative Risk Analysis, 22nd National Information Systems Security Conference, Proc. nat. conf., Arlington.

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

North American Electric Reliability Corporation (NERC) (2015) – CIP-014-2 – Physical Security, URL: https://www.nerc.com/pa/Stand/Pages/Project-2014-04-Physical-Security.aspx, 28.01.2020

Schwab, A. J. (2009) Elektroenergiesysteme – Erzeugung, Transport, Übertragung und Verteilung elektrischer Energie, Springer, Berlin.

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