Risk Differentiation for Critical Infrastructure Protection

Sascha Meng[1], Marcus Wiens[2], Frank Schultmann[3]

[1]*Karlsruhe Institute of Technology, Karlsruhe, Germany. E-mail: sascha.meng@kit.edu*

[2]*Karlsruhe Institute of Technology, Karlsruhe, Germany. E-mail: marcus.wiens@kit.edu*

[3]*Karlsruhe Institute of Technology, Karlsruhe, Germany. E-mail: frank.schultmann@kit.edu*

ABSTRACT: Critical infrastructures, e.g. electricity transmission / distribution, public transport and health care systems, need to be protected against various internal and external risks which can be safety- and / or security-relevant. Predominately probability-based methods are hitherto used for analysing the whole spectrum of risks. We think this is an insufficient approach, presumably leading to inefficient resource allocation and biased risk perception, as it does not consider the different natures of risk. This paper looks at the key difference between safety- and security-relevant risks, highlights resulting implications for critical infrastructure protection and describes a possible approach for handling these different types of risk.

Keywords: critical infrastructure protection, safety-relevant risks, security-relevant risks.

1 INTRODUCTION

Systems and their related assets and facilities are referred to as critical infrastructure if they are essential for social and economic welfare (e.g., Cohen 2010, Schätter *et al.* 2014). They are the backbone of a nation's health and security (DHS 2012). Critical infrastructures are increasingly connected, interdependent and complex, usually spatially far off and, thus, hard to protect. They are continuously exposed to myriad internal and external risks of different nature. This implies that it is important to use appropriate risk analysis methods to achieve sufficient levels of safety and security.

Risks can be categorised manifoldly. One important distinguishing feature of risks is their nature respectively source of origin. A distinction can be made between two types of risk (Bieta *et al.* 2009). On the one hand risks can be unintentionally caused by random or natural events (hereafter referred to as 'type 1 risks'). Type 1 risks can be adequately analysed using statistical distributions and simulations. Risks may, however, also be deliberately caused by malicious human behaviour (hereafter referred to as 'type 2 risks'). Unlike type 1 risks which are caused by randomness, type 2 risks cannot be analysed solely relying on statistical measures. They additionally require the consideration of interactive, rational decision-making processes between the involved persons or groups, as well as their "intentions, motivations, preferences and capabilities" (Ayyub *et al.* 2007). However, very often exclusively probability-based risk analysis methods are applied to both types of risk. In consequence, this inevitably misleads risk perception, causes misjudgement and wastes scarce resources when dealing with type 2 risks (Hall 2009, Brown and Cox 2011).

For improving critical infrastructure protection, we propose to apply different risk analysis approaches to meet the challenges associated with the different natures of risk. Furthermore, we recommend combining these different approaches where necessary and suitable, considering the individual characteristics of the types of risk at hand. The remainder of our paper is structured as follows. In section 2 we point out important differences between safety- and security-relevant risks. Subsequent to highlighting implications for critical infrastructure protection in section 3, we describe in section 4 how to approach the risk analysis process when confronted with different types of risk. The paper ends with a brief discussion of the issues raised.

2 SAFETY- AND SECURITY-RELEVANT RISKS

Critical infrastructures are exposed to miscellaneous natural and man-made threats (hazards). Like all man-made systems, critical infrastructures are, to some extent, shielded from the surrounding environment. This shielding aims both at protecting the system against negative impacts from the surrounding environment and vice versa. These threats cause, with a (un-)known probability, damage or other adverse effects to the system or the surrounding environment, constituting safety- and security relevant risks for critical infrastructures (Aven and Renn 2010). The main difference between safety- and security relevant risks is their source of origin (Piètre-Cambacédès and Bouissou 2010).

Within the context of critical infrastructure protection, the concept of safety aims at preventing, detecting, and reacting to events which accidently harm people, property or the environment, endangered through the critical infrastructure (Firesmith 2003). In other words, the concept of safety primarily deals with randomness, whether it is caused by nature (e.g., natural occurring events such as fires, floods, storms, earthquakes), human behaviour (e.g., unintentional mistakes, ignorance) and / or other errors (e.g., excessive burden, material defects). Safety, realized through appropriate system design and safety barriers (e.g., physical barriers, digital barriers), aims at protecting the environment from hazards resulting from the existence and / or operation of man-made systems (Burns *et al.* 1992, Firesmith 2003). Thus, safety-relevant risks are predominately type 1 risks (cf. section 1) which are

unintentionally caused by random (or natural) events. In comparison, the concept of security deals with preventing, detecting, and reacting to events which maliciously harm people, property (assets and facilities, but also data) or the environment, endangered through the critical infrastructure (Firesmith 2003). Unlike the concept of safety, the concept of security deals with events which are caused by intentional malicious human behaviour or, in other words, with attacks rather than accidental events (e.g., arson, fraud, crime, terrorism). Security, realized as well through appropriate system design and security barriers (e.g., physical barriers, digital barriers), aims at protecting man-made systems against internal and external attacks (Burns *et al.* 1992, Firesmith 2003). Thus, security-relevant risks are mainly type 2 risks (cf. section 2) which are caused by deliberate malicious human behaviour (e.g., Piètre-Cambacédès and Bouissou 2010, Raspotnig and Opdahl 2013, Meng *et al.* 2014).

The degree of risk is determined through the degree of uncertainty associated with the risk. Uncertainty, in the sense of being uncertain about the outcome of or having incomplete knowledge in a decision-situation, can be classified into two categories – aleatoric (inherent, stochastic) and epistemic (subjective, systemic) uncertainty (e.g., Kiureghian and Ditlevsen 2009, Senge *et al.* 2014). Aleatoric uncertainty is caused by inherent randomness (parameter variability), whereas epistemic uncertainty is caused by a lack of knowledge or ignorance of the decision-maker (e.g., Hora 1996, Paté-Cornell 1996, Helton *et al.* 2010, Ayyub 2014). Aleatoric uncertainty is not necessarily based on a lack of knowledge and, thus, cannot be fully eliminated. In contrast, epistemic uncertainty can be eliminated over time if the decision-maker gets more information (Ayyub 2014). With regard to safety- and security-relevant risks, safety-relevant risks are dominated by aleatoric uncertainties (with randomness as the decisive feature), whereas security-relevant risks are dominated by epistemic uncertainties and uncertainties caused through strategic interactions (with deliberate choice as the decisive feature) (Bieta *et al.* 2009).

Both the concept of safety and security have many commonalities and are frequently difficult to distinguish (e.g., fraudster who want to enrich themselves or arsonists are by definition a security risk (as they intentionally harm the system), but also pose a safety risk when their actions affect others too), and they sometimes cause each other. To protect a threatened critical infrastructure against safety- and security-relevant risks, it is necessary to take into consideration the different natures of these risks and their initiating hazardous events. It is also important for decision-makers to use appropriate, effective and versatile risk analysis approaches which take into consideration the crucial differences between these different concepts.

3 IMPLICATIONS FOR CRITICAL INFRASTRUCTURE PROTECTION

Risk management for critical infrastructure protection is affected by and depends on organisational achievable, technical feasible, economic reasonable and legally allowed safety and security measures. Also, the wishes and demands of different stakeholders (e.g., infrastructure owners and operators, government, customers, the public) need to be taken into consideration.

Different stakeholders are affected by different types of risk and have a different risk perception. Thus, it is necessary to consider all stakeholders who can possibly influence infrastructure protection and operation. That means many heterogeneous risks need to be considered and analysed. As already mentioned in section 2, safety- and security-relevant risks should be seen as different concepts with unequal properties. This implies that different risk analysis approaches are required to sufficiently analyse all identified risks. However, in practice, critical infrastructure operators usually apply just ‘standard’ risk analysis approaches to the whole spectrum of risks.

By ‘‘standard’ risk analysis approaches’ we mean generally known, well-established empirical and / or statistical risk analysis approaches, such as variance analysis, probability risk analysis, scenario analysis or Bayesian analysis (e.g., Schoemaker 1995, Wright and Goodwin 1999, Min *et al.* 2007, Dillon *et al.* 2009). These approaches, when used as stand-alone risk analysis approach, are suitable for analysing naturally or randomly occurring events or, in other words, when dealing with safety-relevant risks of type 1. By comparison, when analysing safety- or security-relevant risks of type 2, decision-makers additionally need to consider the strategic interactions between themselves and the intelligent adverse human counterpart. Thus, as information about the preferences and capabilities of the adversary are usually barely known, it is often not possible to reliably conclude from past events to future events, solely relying on ‘standard’ risk analysis approaches.

For analysing security-relevant threats and hazards, we suggest applying other, more appropriate risk analysis approaches than the widely used ‘standard’ risk analysis approaches. In particular, we propose using game theoretic approaches as they explicitly consider the strategic interactions between two or more humans. Game theoretic reasoning improves safety- and security-relevant decision-making (when confronted with type 2 risks) in several ways, forcing decision-makers to get a realistic idea of risk reduction limitations, to think about the attackers preferences, capabilities and their possible attack-strategies and, thus, to develop ‘customised’ defence strategies (considering the strategies which they cannot choose) (Wiens *et al.* 2014). However, experiences and knowledge gained in the past (e.g., related empirical and statistical data) are important sources of information for game theoretic reasoning.

We are convinced that it is important for critical infrastructure protection to clearly differentiate between different types of risk and to apply a more differentiated risk analysis approach for both natures of risk.

4 APPROACH TO HANDLE DIFFERENT TYPES OF RISK

As previously mentioned, safety- and security-relevant risks are often analysed using the same analysis methods (see Table 1). In practice, decision-makers rarely differentiate between the different natures of risk, although this distinction is necessary to apply appropriate analysis methods to different risks.

Table 1: Risk analysis process without differentiation between different natures of risk (own table)

risk analysis process	
risk identification	e.g., fires, floods, storms, earthquakes, unintentional mistakes, ignorance, material defects, fraud, terrorism
risk categorization	safety- and security-relevant risks
	type 1 risks and type 2 risks (fires, floods, storms, earthquakes, unintentional mistakes, ignorance, material defects, fraud, terrorism)
analysis methods selection	empirical / statistical methods (e.g., variance analysis, probability risk analysis, scenario analysis, Bayesian analysis)

We propose a clear distinction between risks of different nature before analysing them (see Table 2). In the first step, all relevant risks need to be identified (risk identification) and available information / knowledge on it from all accessible sources need to be gathered. In the second step, the identified risks need to be categorised as safety- or security relevant (risk categorization), and whether they are type 1 or 2 risks. Next, the applicability of the risk analysis approaches, known and available to the decision-maker, has to be determined (approach applicability determination) and possible weak points of them, which otherwise would bias risk perception, need to be identified (approach weak point identification). Then, if necessary, supplementary methods and approaches need to be found to extend the respective risk analysis models (approach improvement). These last three steps can be summed up as analysis method(s) selection process.

Table 2: Risk analysis process with differentiation between different natures of risk (own table)

risk analysis process			
risk identification	e.g., fire, floods, storms, earthquakes, unintentional mistakes, ignorance, material defects, fraud, terrorism		
risk categorization	safety-relevant risks		security-relevant risks
	type 1 risks (fire, floods, storms, earthquakes, unintentional mistakes, ignorance, material defects)	type 2 risks (under certain circumstances fire (arson), fraud, terrorism)	type 2 risks (fire (arson), fraud, terrorism)
analysis method(s) selection	empirical / statistical methods (e.g., variance analysis, probability risk analysis, scenario analysis, Bayesian analysis)	game theory and / or other strategic decision-analysis methods (supplemented by empirical / statistical methods)	game theory and / or other strategic decision-analysis methods (supplemented by empirical / statistical methods)

Last but not least, the results of the analysis with and without risk differentiation should be compared (approach review). This step is important to gain further insights into the decision-problem to be solved because decision-makers are often confronted with an information overflow and, thus, have problems to identify the key information relevant for solving the decision-problem.

No single risk analysis approach will ever provide an optimal solution for critical infrastructure protection. The determination of risk is always subjective and, thus, the whole process of risk analysis (as part of a risk management process) only supports the decision-making process, but does not substitute it.

5 ADDED VALUE FOR THE POST 2015 FRAMEWORK FOR DISASTER RISK REDUCTION

Our work deals with critical infrastructure protection against natural and man-made hazards and, thus, supports disaster risk reduction. In future, disasters, whether of natural origin (e.g., fire, floods, storms, earthquakes) or man-made (e.g., fire, oil spills, terrorism, transport accidents), will have severe consequences because of the increasing connectivity, interdependency and complexity of critical infrastructures world-wide. Our work points out a crucial aspect of risk analysis which always needs to be considered – the different natures of risk. Therefore, research in future should focus more on the development of tailored risk analysis and risk management approaches to meet the challenges associated with the different natures of risk. In this context, research also should pay more attention to the increasing complexity of the decision-making processes themselves.

6 CONCLUSIONS

There is a need for rethinking the way how safety- and security-relevant risks are analysed. Risk managers and risk management systems often do not explicitly distinguish between them. This supports and amplifies misallocation of resources and sometimes even increases the risks. It is important to pay more attention to choosing the right risk analysis approach(es) for a certain risk, considering the fact that critical infrastructures become more and more interdependent, complex and, thus, harder to protect. It is

necessary that critical infrastructure owners and operators apply other, more suitable risk analysis approaches to protect their systems against emerging threats. Both safety- and security-relevant risks have common features and are sometimes inseparable, implicating that risk analysis research should focus more on integrating different risk analysis approaches to achieve holistic analysis approaches for systems threatened by safety- and security-relevant hazards.

7 ACKNOWLEDGEMENTS

This research was partly supported by the research project RIKOV, financed by the German Federal Ministry of Education and Research (BMBF).

8 REFERENCES

Aven, T. and Renn, O., 2010. *Risk Management and Governance*. Berlin, Heidelberg: Springer.

Ayyub, B.M., 2014. *Risk Analysis in Engineering and Economics*. 2nd ed. Boca Raton, FL: CRC Press.

Ayyub, B.M., McGill, W.L., and Kaminskiy, M., 2007. Critical Asset and Portfolio Risk Analysis: An All-Hazards Framework. *Risk Analysis*, 27 (4), 789–801.

Bieta, V., *et al.*, 2009. Zustandsrisiken und Verhaltensrisiken sind nicht dasselbe: Die Sicht der Spieltheorie zum Risikomanagement. *Risiko Manager*, 2009, pp. 16–19.

Brown, G.G. and Cox, L.A., 2011. How Probabilistic Risk Assessment Can Mislead Terrorism Risk Analysts. *Risk Analysis*, 31 (2), 196–204.

Burns, A., McDermid, J., and Dobson, J., 1992. On the Meaning of Safety and Security. *The Computer Journal*, 35 (1), 3–15.

Cohen, F., 2010. What makes critical infrastructures Critical? *International Journal of Critical Infrastructure Protection*, 3 (2), 53–54.

DHS, 2012. *National Protection and Programs Directorate: Office of Infrastructure Protection Strategic Plan: 2012–2016*. Washington, DC: U.S. Department of Homeland Security.

Dillon, R.L., Liebe, R.M., and Bestafka, T., 2009. Risk-Based Decision Making for Terrorism Applications. *Risk Analysis*, 29 (3), 321–335.

Firesmith, D.G., 2003. *Common Concepts Underlying Safety, Security, and Survivability Engineering*. Technical Note (SCM/SEI-2003-TN-033). Pittsburgh, PA: Carneige Mellon University.

Hall, J., 2009. The Elephant in the Room Is Called Game Theory. *Risk Analysis*, 29 (8), 1061.

Helton, J.C., *et al.*, 2010. Representation of analysis results involving aleatory and epistemic uncertainty. *International Journal of General Systems*, 39 (6), 605–646.

Hora, S.C., 1996. Aleatory and epistemic uncertainty in probability elicitation with an example from hazardous waste management. *Reliability Engineering & System Safety*, 54 (2-3), 217–223.

Kiureghian, A.D. and Ditlevsen, O., 2009. Aleatory or epistemic? Does it matter? *Structural Safety*, 31 (2), 105–112.

Meng, S., Wiens, M., and Schultmann, F., 2014. A game theoretic approach to assess adversarial risks. *In:* C. Brebbia, ed. *Risk Analysis IX*. Southampton: WIT Press, 141–152.

Min, H.-S., *et al.*, 2007. Toward modeling and simulation of critical national infrastructure interdependencies. *IIE Transactions*, 39 (1), 57–71.

Paté-Cornell, M.E., 1996. Uncertainties in risk analysis: Six levels of treatment. *Reliability Engineering & System Safety*, 54 (2-3).

Piètre-Cambacédès, L. and Bouissou, M., 2010. Modeling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes). *In:* IEEE, ed. *Proceeding of the 2010 IEEE International Conference on Systems, Man and Cybernetics (SMC)*. Piscataway, USA: IEEE, 2852.

Raspotnig, C. and Opdahl, A., 2013. Comparing risk identification techniques for safety and security requirements. *Journal of Systems and Software*, 86 (4), 1124–1151.

Schätter, F., *et al.*, 2014. A multi-stage scenario construction approach for critical infrastructure protection. *In:* S. Hiltz, *et al.*, eds. *ISCRAM 2014 Conference Proceedings: Book of Papers*. 11th International Conference on Information Systems for Crisis Response and Management. University Park (Pennsylvania): The Pennsylvania State University, 397–406.

Schoemaker, P., 1995. Scenario planning: a tool for strategic thinking. *Sloan Management Review*, 36 (2), 25–40.

Senge, R., *et al.*, 2014. Reliable classification: Learning classifiers that distinguish aleatoric and epistemic uncertainty. *Information Sciences*, 255, 16–29.

Wiens, M., *et al.*, 2014. Optimizing Security vis-à-vis Terrorist Attacks: An Application for Public Rail Transport Systems. *In: Conference Proceedings: 9th Security Research Conference 'Future Security'*. September 16 – 18, 2014, Berlin (in press). Berlin.

Wright, G. and Goodwin, P., 1999. Future-focussed thinking: combining scenario planning with decision analysis. *Journal of Multi-Criteria Decision Analysis*, 8 (6), 311–321.