21
Schriften aus der Fakultät Humanwissenschaften
der Otto-Friedrich-Universität Bamberg

Knowledge-Based Decision Making in Complex Environments

Methodological Aspects of Proactive Airport Security Management

Mara Gwen Cole

University
of Bamberg
Press

21 Schriften aus der Fakultät Humanwissenschaften der Otto-Friedrich-Universität Bamberg

Schriften aus der Fakultät Humanwissenschaften
der Otto-Friedrich-Universität Bamberg

Band 21

University
of Bamberg
Press
2015

Knowledge-Based Decision Making in Complex Environments

Methodological Aspects of Proactive Airport Security Management

von Mara Gwen Cole

University
of Bamberg
Press
2015

Bibliographische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Informationen sind im Internet über http://dnb.d-nb.de/ abrufbar.

Diese Arbeit hat der Fakultät Humanwissenschaften der Otto-Friedrich-Universität Bamberg als Dissertation vorgelegen.
1. Gutachter: Prof. Dr. Harald Schaub
2. Gutachter: Prof. Dr.-Ing. Mirko Hornung
Tag der mündlichen Prüfung: 13. April 2015

Herstellung und Druck: docupoint, Magdeburg
Umschlaggestaltung: University of Bamberg Press, Anna Hitthaler

ISSN:1866-8674
ISBN: 978-3-86309-332-7 (Druckausgabe)
eISBN: 978-3-86309-333-4 (Online-Ausgabe)
URN: urn:nbn:de:bvb:473-opus4-265039

Acknowledgments

This work primarily results from my occupation as scientific researcher at Bauhaus Luftfahrt e.V. from September 2008 on. The research project SiVe (Verbesserung der Sicherheit von Verkehrsinfrastrukturen), which was partially financed by the German Federal Ministry of Education and Research (BMBF), provided me with the opportunity to conduct the research that served as a basis for this thesis.

Special thanks go to my doctoral advisor apl. Prof. Dr. Harald Schaub for his openness towards the interdisciplinary approach pursued in my work. He showed confidence in my research and his thorough reviews allowed me to strengthen the results presented in this thesis.

Prof. Dr. Mirko Hornung deserves my gratitude for accepting the position as second advisor. His continuous interest in my research topic and numerous reviews not only of the papers presented in this thesis greatly contributed to my work. I am furthermore indebted to Prof. Dr. Dietrich Dörner for taking the position as third advisor.

Whereas all the SiVe project partners contributed to my research through comments and reviews, Dr. Maik Maurer deserves special mentioning as he shared his insights into the field of complexity management with me. Throughout the project duration we collaborated in extending the borders of the methodology and he thus greatly contributed to my research results.

I want to thank all my colleagues at Bauhaus Luftfahrt e.V. for creating an inspiring, challenging and fun environment to work in. I am especially grateful to Annika, Andreas, Kay, Marcia, Christoph, Michael, Milena, Holger, Arne and Arne. I am, furthermore, thankful for the continuous support from the management board of Bauhaus Luftfahrt e.V., namely Dr. Anita Linseisen and Prof. Dr. Mirko Hornung.

Finally, I am very grateful to my family for their extraordinary and permanent support and would like to thank Stefan, who always encour-

aged me in my work and showed great patience throughout the whole process of developing this thesis.

Mara Cole

Table of Contents

List of Figures

Publication Number 1: Cole and Kuhlmann (2012)

Publication Number 2: Cole (2014)

Publication Number 3: Cole and Maurer (2014)

Publication Number 4: Maurer and Cole (2012)

List of Tables

Publication Number 3: Cole and Maurer (2014)

1. Introduction

A decision on a course of action in uncertain and complex environments presents a great challenge for the decision maker. There can be contradictory or missing cues, dynamic changes of the environment, time pressure and many other factors impeding the decision task. Broad knowledge of the underlying structure of the whole system, of its elements and their interrelations, is of great importance in order to successfully master its development. Knowledge can be acquired through a continuous learning process, often based on action-outcome-feedback loops: experience of the system's reaction to goal-oriented intervention or unexpected external disturbances provides clues pertaining to the interaction of system components. Wide experience within a certain environment is necessary to be able to anticipate new developments. Envision of possible future states of the system can help to prepare for related developments. In this context, creativity can play an important role as it supports thinking beyond present constraints.

Psychological research in the area of knowledge-based decision making as well as creativity serves as the basis for this dissertation, which applies them to the context of airport security. A major challenge within this field is to overcome the reactive approach currently predominant: New security measures are implemented mostly in the aftermath of attacks, strengthening the system to counteract these past threats. Against this background it is important to develop a proactive approach to airport security management, forestalling possible future threats. Such an approach has to be based on in-depth knowledge of elements and interrelations of the security system and should allow inclusion of creative, out of the box ideas for novel attacks. The development of a software tool fulfilling these challenges, the so-called Scenario Builder, has been pursued in the course of this dissertation. The methodological foundations, its functionality and use as well as possible ways to analyse the resulting data will be presented.

One obstacle to a proactive approach to airport security is the fact that incidents occur only very rarely. As described above, knowledge can be acquired through feedback loops, indicating whether or not one's actions caused the desired effects. Because of the very low frequency of incidents in the context of airport security it is not possible, for example, to change the arrangement of the security measures and evaluate the success on the basis of the next ten or twenty incidents. It is argued that the Scenario Builder offers a (partial) tool-based substitution for these real-world feedback-loops, allowing the user to generate plausible future threat scenarios, rearrange or delete security measures from the analysis and trace the effects on the measures involved.

The thesis is structured as follows: Based on a description of basic characteristics of the airport security system, Section 2 describes fundamental requirements for decision making in the context of airport security. Section 3 lays the foundation by describing fundamentals of decision making. A short outline of the theoretical background is followed by a discussion of approaches taking the real-world setting of decisions into account. The field of Naturalistic Decision Making is identified as most relevant in the context of this thesis and consequently is presented in more detail. The level of knowledge of the decision maker is of fundamental importance. In the following Section 4, psychological dimensions of the concept of creativity are presented. The focus of this section lies on confluence approaches to creativity and, furthermore, on the relation between creativity and knowledge.

In Section 5 the psychological approaches are transferred to the field of airport security and linked to the proactive approach to the management thereof put forward throughout the dissertation. Airport security is introduced as a complex system. It is argued that proficiency and the ability to anticipate possible future threats are highly relevant characteristics for decision making within the context of airport security. This observation necessitates the high relevance of creativity to airport security. Currently, creativity is mostly attributed to malevolent organisations. If a proactive approach is to be successful, this has to change fundamentally. Finally, a short introduction to the methodologies underlying the developed proactive approach is outlined.

The main part of the thesis is comprised of four publications dealing with different aspects of the developed approach to airport security. The publications are briefly introduced in Section 6 and their particular contributions to the central topic are highlighted. Emphasis is placed on the strongly interdisciplinary character of the work, reflected by the different disciplinary backgrounds of the journals and the book that published the papers. In the final Section 7 a summary of the thesis is provided. Contributions to the different fields of research underlying the publications are discussed and possible connecting points for future work in the field of psychology as well as aviation management are identified.

2. Requirements for Decision Making in Airport Security

Mobility is a basic human need and fundamental to the economic and social welfare of a society, particularly in the face of globalisation. Reliable and efficient transportation, on long as well as short distances, is a major enabler for this development. As far as air transportation is concerned, airports offer the node through which the connection between ground and air transport is provided. They act as gateways through which access to the air transportation system is granted. During recent decades the air transport system has been susceptible to a broad range of (terrorist) attacks, motivated by a variety of intentions. This has led to the development of many layers of security mechanisms installed within airports, intended to mitigate possible attacks. The challenge for airport operators is to provide a hassle-free travel experience for the customer while, at the same time, assuring a high level of security and dealing with the pressure to operate cost-effectively.

The airport security system is in itself highly complex, tying together security measures and personnel, national and international rules and regulations, diverging interests of different stakeholders and many other aspects. To simultaneously manage this broad range of demands, experts need to draw on in-depth knowledge of the interrelations of system components and the resulting behaviour of the overall system. Handling the system successfully is, furthermore, complicated by the ever evolving, innovative character of possible threats. The high level of creativity, feeding into the planning and realisation of attacks, poses a great challenge to the management of airport security. These unknown future threats can be met by a proactive advancement of airport security based on creative conception of possible threats and the identification of related weaknesses in the security system.

As a decision environment, the complex airport security system can be characterised by certain requirements. There are two central aspects affecting the decision making process: knowledge of the system itself and creativity with regard to possible future states. Figure 1 schematises components relevant for the decision making process in the context of airport security. Knowledge and creativity are reflected in the four boxes in the requirements area on the left hand side of the figure, with knowledge relating to the two boxes at the top and creativity to the two lower ones. To gain a thorough understanding of these two concepts it is necessary to investigate related research in the field of psychology since knowledge-based decision making in complex environments as well as human creativity are two established areas of research within this field.

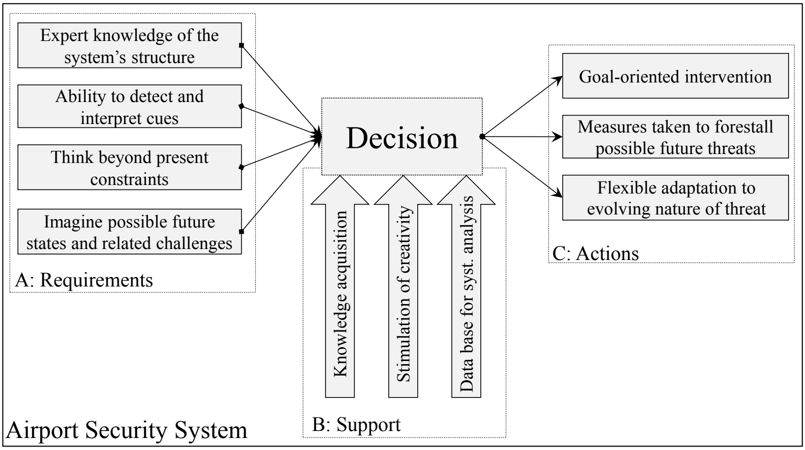

Expert knowledge of the system's structure
Ability to detect and interpret cues
Think beyond present constraints
Imagine possible future states and related challenges
A: Requirements
Decision
Knowledge acquisition
Stimulation of creativity
Data base for syst. analysis
B: Support
Goal-oriented intervention
Measures taken to forestall possible future threats
Flexible adaptation to evolving nature of threat
C: Actions
Airport Security System

Figure 1: Basic components of approach to airport security system

The complexity of the airport security systems calls for an approach to support the decision making process based on the insights gained from psychological research. As mentioned above, fostering the acquisition of expert knowledge and inspiring creative thought are two fundamental means of supporting the decision maker, acting in the airport environment. These are represented by two of the three arrows in the middle section of Figure 1 labelled "Support". The third arrow highlights another important pathway by which the decision maker can be assisted in his task: the generation of a data base reflecting the decision space and allowing the user to systematically analyse relations between components as well as effects of actions can provide support during the decision making process.

The ultimate goal, however, is addressed by the area on the right hand side of Figure 1 labelled “Actions”. Supporting decision making aims at improving the quality of the decision. The three boxes reflect different actions that can result from decisions and support the effectiveness of these in the context of airport security. The publications forming the main part of this dissertation present different steps towards reaching this goal. For example, how the identified decision requirements stimulated the development of the Scenario Builder as a decision support tool is described. The different aspects supporting the decision as highlighted in Figure 1 are discussed and how a data base can provide a basis for future-oriented decision making is demonstrated. Examples for possible actions are, furthermore, provided.

The next two sections will address psychological aspects and provide a theoretical background for the understanding of the decision situation before these insights into airport security are applied in Section 5 and 6.

3. Decision Making in Complex Environments

The field of decision making has evolved substantially over the past few centuries and even over recent decades. In this introductory section, historical developments leading to the current research landscape are traced. Based on their relevance for decision making in the complex setting of airport security, a number of approaches and models are presented in more detail. Two aspects will be highlighted throughout this section: the environment in which a decision task is placed and the domain-specific knowledge of the decision maker. Requirements of anticipatory thinking will be discussed from a decision making perspective. This section provides the fundamentals for the development of a future-oriented approach to airport security.

3.1 Theoretical Background of Decision Making Research

Research conducted in the area of decision making encompasses a wide range of topics and methods. There is "no single, universally endorsed, overarching theoretical framework that researchers use to organize and guide their efforts" (Goldstein and Hogarth 1997:3). A number of avenues of interest have been followed during the last sixty years and directly shape the current research landscape. This section will pursue a focussed approach and will cover theoretical developments leading to today's knowledge-based decision making theories. Goldstein and Hogarth (1997) as well as Newell et al. (2007) provide a broader account.

Various approaches to structuring the research area's history are documented in the literature. For example, Goldstein and Hogarth (1997) and Newell et al. (2007) differentiate between the history of judgement research and decision research, tracing developments in these two fields separately. Cohen (1993), in contrast, analyses paradigm shifts according to the attitude of the research community towards decision biases. He identifies three different approaches: the formal-empiricist, the rationalist, and the naturalistic paradigm. A researcher's theoretical beliefs can be revealed by answering the question of which rules the mind applies when making decisions, as Gigerenzer and Gaissmaier point out. They identify "logic, statistics, or heuristics" (2011:452) as possible answers. In the following, a short overview of influential concepts for the development of the field of decision making is provided.

Foundations of current approaches to decision making reach back some centuries. The concept of rational choice can be traced to a written exchange in the seventeenth century between the mathematicians Fermat and Pascal. They discussed a range of gambling problems, leading to the notion that, in order to make a rational choice, one needs to choose the option with the mathematically highest expected value (Newell et al. 2007). In 1738 Bernoulli (English translation: Bernoulli 1954) suggested exchanging the objective measure of expected *value* with expected *utility*, a subjective measure (Cohen 1993), to better fit human decision behaviour.

Drawing on the concept of expected utility, von Neumann and Morgenstern published their *Theory of Games and Economic Behavior* in the mid-twentieth century. The second edition of this book (1947) included axioms to test the rationality of a person's decisions thus specifying "conditions under which utility could be measured objectively" (Goldstein and Hogarth 1997:5). Based on this work, Savage (1954) merged the subjective concept of utility with the notion that probabilities of decision alternatives are also subjective, implying that choice is based on a person's subjectively expected utility (Cohen 1993). He, furthermore, introduced the differentiation between small worlds and large worlds as decision settings. Small worlds can be described as a decision situation under conditions of extensive information and large worlds as situations in which important knowledge is not known by the decision maker (Gigerenzer and Gaissmaier 2011). In such an uncertain decision environment requirements for a purely rational choice cannot be met. Simon (1955) also stressed the relevance of imperfect knowledge in decision making and added that the limited "computational capacities that are actually possessed by [...] man" (1955:99) additionally prevent decisions from satisfying rational standards. From this perspective, people are forced to abandon optimal decision strategies (Marewski et al. 2010) as prescribed by the classical decision theory described above.

Emphasizing the resulting irrationality of decision makers, Kahneman and Tversky developed their heuristics and biases approach in the early 1970s (Kahneman et al. 1982). They hypothesise that

> "people rely on a limited number of heuristic principles which reduce the complex tasks of assessing probabilities and predicting values to simpler judgmental operations. In general, these heuristics are quite useful, but sometimes they lead to severe and systematic errors." (Tversky and Kahneman 1974:1124)

The study of intuitive judgement based on heuristics and biases has initiated substantial interest (Kahneman 2003) and has had strong influences on decision making research (Gigerenzer 1996). Nevertheless, this rather negative view of the human decision maker as being prone to systematic cognitive biases has been countered by the notion that an approach focussing only on the decision process itself is too narrow and the quality of a decision cannot be evaluated on this basis. Simon coined a metaphor illustrating his view of the relation between actor and environment: "Human rational behavior [...] is shaped by a scissors whose two blades are the structure of task environments and the computational capabilities of the actor" (Simon 1990:7).

The notion of the dependence of the quality of a decision on the conditions under which it is made has inspired different researchers to investigate decision making under realistic conditions. Two approaches to decision making in the real world will be described in more detail in the following section.

3.2 Decision Making and Knowledge in the Real World

Historic approaches and classic decision theory pursue a rather narrow approach to decision making and are not capable of coping with challenges outside the context of the laboratory. Two approaches that deliberately go beyond the constraints of controlled experiments are focussed on in the following: Naturalistic Decision Making and Fast and Frugal Heuristics. Both approaches include the environment as a constituent feature in the decision making process. Whereas the latter pursues a quite narrow approach, mainly focussing on the distinct decision event, Naturalistic Decision Making aims at a detailed understanding of the conditions that allow experienced decision makers to act reasonably in complex environments. It is thus argued, that Naturalistic Decision Making can offer very valuable insights in the decision making process relevant for the scope of this work. A special emphasis will be put on the role of expertise and knowledge-acquisition processes within the two approaches.

3.2.1 Fast and Frugal Heuristics

The classical justification for the use of heuristics by humans is – analogue with the heuristics and biases program of Kahneman and Tversky – that they allow the decision maker to attain a positive trade-off between time and effort invested and the accuracy achieved (Payne et al. 1993). From this perspective, the use of heuristics has a negative influence on the quality of decisions because the limited effort invested can lead to erroneous outcomes. In contrast, Todd and Gigerenzer pursue an approach to heuristics in decision making that is based on the "major discovery, [...] that saving effort does not necessarily lead to a loss in accuracy" (Todd and Gigerenzer 2012:26). From this perspective, a trade-off in line with the effort-accuracy framework is no longer necessary, as heuristics can simultaneously be faster and more accurate. For a range of decision problems in the real world Todd and Gigerenzer found "an inverse U-shaped relation between amount of information computation, and time on the one hand and predictive accuracy on the other" (Todd and Gigerenzer 2012:27). The U-shaped relation implies that, at a certain point, more information does not improve the decision quality but harms it (for example, detailed models can overfit new data (Marewski et al. 2010)).

The reason why this less-is-more effect (Gigerenzer and Gaissmaier 2011) can produce positive outcomes is that heuristics are not applied randomly. They are adapted to suit the particular decision environment in which they are employed. Following Simon's scissors metaphor, just as the two blades of a scissors need to fit perfectly together for the scissors to cut, heuristics and environments need to be adjusted for decision strategies to be successfully employed. Decision makers have individual sets of heuristics at their disposal to cope with the uncertain world around them (Goldstein and Gigerenzer 2011). These heuristics exploit the evolved cognitive abilities of the decision maker (Gigerenzer 2001) as well as the patterns of information in the environment (Todd and Gigerenzer 2007). A heuristic can be defined as follows: It "is a strategy that ignores part of the information, with the goal of making decisions more quickly, frugally, and/or accurately than more complex methods" (Gigerenzer and Gaissmaier 2011:454). They are composed of a number of building blocks that determine the process of decision making (Gigerenzer 2001):

- search rules: give the search for alternatives and cues a direction
- stopping rules: specify criteria for stopping the search
- decision rules: indicate inferences that should be made based on the acquired information.

The repertoire of heuristics a decision maker can draw on has been labelled "Adaptive Toolbox" (Gigerenzer and Selten 2011).

As an example, one tool in this toolbox is the so-called recognition heuristic. It draws on the information one can derive from the lack of recognition and aims at making "inferences about unknown quantities in the world" (Gigerenzer and Goldstein 2011). The recognition heuristic tells the decision maker which alternative to choose, given that one is recognized and the other is not. In this case the heuristics state that the decision maker should infer that the recognized alternative has the higher criterion value. Gigerenzer and Goldstein (2011) provide an overview of 25 experimental studies that have recently dealt with the recognition heuristic.

The research program pursued by Gigerenzer and colleagues aims at an explication of the interactions of mind and world that underlie decision making. Advances have been described in a number of books (Gigerenzer et al. 1999, Todd et al. 2012, Hertwig et al. 2013). To emphasize the necessary fit between the environment and the heuristics described above the term "Ecological Rationality" (Todd and Gigerenzer 2007, Todd et al. 2012) has been chosen for this approach. The environment affects the decision maker in a number of ways. It provides, for example, information about the decision situation and influences the individual's goals (Todd and Gigerenzer 2012). Differences in reacting to certain information patterns in the environment have been attributed to experience as well as personality traits and attitudes. The set of heuristics an individual draws on is not fixed and the contents of the adaptive toolbox can evolve and grow based on experience and learning (Todd and Gigerenzer 2012). It is, therefore, apparent that with "sufficient appropriate experience, performance differences can appear [...] [as] experts know where to look and tend to rely on limited search" (Todd and Gigerenzer 2012:23).

The ecological rationality approach broadened the narrow focus of earlier approaches to decision making. The research presented in this section acknowledges the fact that decisions cannot be detached from their specific environment, as their quality can only be evaluated in consideration of the conditions under which they were made. Knowledge acquisition through experience and learning can help the expert to develop a domain-specific toolbox, precisely adapted to address the relevant task in a fast and frugal way. The approach focusses on decision situations in which heuristics can be employed and concentrates on specific decision mechanisms. Specific decision situations are emphasised in the next section where a theory will be introduced that places emphasis on expert decision making in complex, real-world environments.

3.2.2 Naturalistic Decision Making

Naturalistic Decision Making (NDM) can be traced back to a workshop in 1989, where scientists from different backgrounds gathered, all with a common interest in the question of how research in decision making can be better adapted to real-world tasks (Klein et al. 1993). This workshop was the first in a series of conferences to follow (the 11th conference took place in 2013), each reflecting the continuous evolvement of this sub-discipline of decision making. This section will outline the fundamentals of NDM, touch on related decision making models and present recent developments in the understanding of the decision situation.

3.2.2.1 Background

In the first anthology on NDM, which was based on the 1989s workshop, NDM is defined as the "attempt to understand how human decision makers actually make decisions in complex real-world settings and to learn how to support these processes" (Klein et al. 1993:vii). The context in which decisions relevant to NDM are made can be sketched out by the following aspects: ill-structured problems, uncertain and dynamic environments, shifting and ill-defined or competing goals, action/feedback loops, time stress, high stakes, multiple players and organizational settings (Orasanu and Connolly 1993). Orasanu and Connolly (1993) mention expertise and knowledge of the decision maker as further aspects central to the decision task.

The next conference took place five years later. In this period of time the relative emphasis placed on the two main aspects of decision making – field setting and expertise – had changed. In the publication based on the second conference, NDM is defined as "the way people use their experience to make decisions in field settings" (Zsambok 1997:4). This declaration clearly is not compatible with models and research methods based on the classic decision theory described above. Thus, NDM researchers had to pursue a different approach:

> "Instead of beginning with formal models of decision making, we began by conducting field research to try to discover the strategies people used. Instead of looking for ways that people were suboptimal, we wanted to find out how people were able to make tough decisions under difficult conditions." (Klein 2008:456)

In a review article Lipshitz et al. (2001) specify four essential characteristics of NDM. Apart from the focus on experienced decision makers, which he and his colleagues take for granted, NDM can be described by its

- process orientation (cognitive process of decision maker),
- situation-action matching decision rules (decision making as matching rather than choice),
- context-bound informal modelling (domain- and context specific knowledge, sensitivity to semantic and syntactic content), and
- empirical-based prescription (derivation of prescriptions from descriptive models) (Lipshitz et al. 2001).

One important aspect of the NDM framework is the focus of interest beyond the isolated decision event (Orasanu and Connolly 1993). As demonstrated above, this notion connects the ecological rationality approach with NDM. Concepts drawn from cognitive psychology, such as schemas or mental models, are integrated into the decision process, making it possible to include aspects such as perception, recognition of situations and the development of appropriate responses in the scope of research. Within the framework of NDM, the understanding of decision making shifted from a event-oriented and "domain-independent general approach to a knowledge-based approach exemplified by decision makers who had substantial experience" (Klein 2008:457).

3.2.2.2 Models

This understanding of the decision making process is reflected in a number of models. They challenge the prevailing decision theories as they are generated by researchers who "embarked on the construction of descriptive models of proficient decision makers in natural contexts without relying on normative choice models as starting points" (Lipshitz et al. 2001:333). Lipshitz (1993) presents nine different decision making models that were developed independently of each other and that describe aspects of decision making in various settings.

Among those models referred to by Lipshitz (1993) is, for example, a model by Rasmussen (1993) who differentiates between skill-based, rule-based and knowledge-based control of behaviour to gain a better understanding of human errors in complex systems. In his model of cognitive control, these different levels of behaviour can interact to produce situation-specific decision making procedures. The so-called image theory, introduced by Beach (1993), draws attention to the decision maker's values and ideals. They are captured in what he calls images, defined as "schematic knowledge structures [used] to organize [...] thinking about decision" (Beach 1993:151). A subset of principles, goals and plans relevant for a specific decision situation are represented in the so-called frame (Lipshitz 1993). A third model that should gain some attention in the years to come – called the recognition-primed decision (RPD) model – was developed by Klein (1993) in the course of his research on decision processes of fire-fighters in emergency situations. This model will be described in more detail in the next paragraph as it can be viewed as a prototypical NDM model (Lipshitz et al. 2001).

The development of the RPD model is based on studies conducted by Klein and his colleagues, who found that fire-fighters were not making active choices, but rather "saw themselves as acting and reacting on the basis of prior experience" (Klein 1993:139). Furthermore, they were not aiming at finding the most optimal solution but at identifying actions that would be both efficient and applicable. These observations led Klein to believe that two aspects, namely situation assessment and mental simulation, are core processes for generating plausible actions. The model assumes that people organise experience in a repertoire of patterns they can relate to when they have to make quick decisions. In the simplest variation, the decision maker immediately recognizes the situation and follows the obvious course of action (Klein 2008). This notion builds on the hypothesis that skilled decision makers have a certain set of learned prototypes at their disposal, allowing them to immediately relate a perceived situation to an appropriate reaction and consequently act according to the first option identified (Lipshitz et al. 2001). A more complex case involves the conscious evaluation of the possible course of action, employing mental simulation to detect possible problems that could arise from typical actions in the specific situation context. If problems are anticipated, further options are considered in order of their relevance until a feasible action is identified (Klein 1993).

The RPD model has been subject to a number of modifications, for example, the adaptation to different decision environments or to new findings (e.g. insertion of the new function “diagnose the situation” (Klein 1997) or integration of schemata and mental models (Liphsitz and Ben Shaul 1997)).

One central requirement in the RDP model is the existence of expertise on the part of the decision maker. According to Klein (2008), expertise is stored in patterns and includes causal dependences of situations. In specific situations, these patterns “highlight the most relevant cues, provide expectancies, identify plausible goals, and suggest typical types of reactions” (Klein 2008:457). Thus, expert knowledge enables the identification of typical attributes of a situation, the development of mental models, the mental simulation of a course of action and the following anticipation of possible consequences of the co-evolution of situation and action (Lipshitz et al. 2001). The “RPD model underscores the crucial role of domain-specific knowledge or experience in proficient decision making. No step in the model can be executed effectively without such knowledge” (Lipshitz 1993:109). Of course, RPD decision strategies are not applicable in every decision making process. They are appropriate in situations that include time pressure, unstable conditions and an experienced decision maker. They are, for example, not suited for situations where the decision maker encounters highly combinatorial problems or alphanumerical data (Klein 1993). Klein (2008) has demonstrated in his studies that RPD strategies are employed in 80% to 90% of the decisions, on condition that the situation environment corresponds to the criteria described above.

Decision making in accordance with the RPD model builds on the assertion that it “is primed by the way the situation is recognized [...] [but] not completely determined by that recognition” (Klein 1993:140). An approach to situation awareness in naturalistic decision making environments is outlined in the following section. Furthermore, the possibility of future oriented decision making is discussed.

3.2.2.3 Situation Awareness and Anticipatory Thinking

Researchers interested in situation awareness (SA) regard the decision maker’s perception of a current decision making situation as the driving factor: “In most settings effective decision making largely depends on having a good understanding of the situation at hand” (Endsley 1997:269). According to Endsley, SA is defined as “the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future” (Endsley 1988:97, cited in: Endsley 1997:270). He distinguishes between three different phases of SA: in the first level relevant environmental factors are perceived, the second level aims at an understanding of those factors in relation to the decision makers’ goals and the third level relates to the achievement of an understanding of possible future developments of the factors.

Limited cognitive capacities restrict the formation of SA. To circumvent these deficiencies the experienced decision maker can rely on schemas and mental models that provide means to classify specific situations. They can support the decision maker by guiding the attention towards critical cues, by evoking specific expectations concerning the future development of relevant factors and by providing direct links between characteristics of the situation and typical actions (Endsley 1997). The orientation towards possible future developments of the system, particularly in the third level of the SA approach, is also relevant in Klein’s RPD model, where the experienced decision maker employs mental simulation to detect possible future complications. This aspect will be considered further in the following.

Anticipatory thinking is defined as “the process of imagining how unexpected events may affect plans and practices” (Klein et al. 2010:235). It supports the decision maker in detecting nonobvious demands of possible future states and consequently helps him to prepare and position himself for their occurrence. The ability to consolidate experiences and concepts is a precondition to act and react goal-oriented upon the environment and allows the decision maker to “guard against and forestall potential threats” (Klein et al. 2010:235). Anticipatory decision making is not only oriented towards the most likely futures but explicitly includes events that exhibit a low probability and a high level of threat simultaneously. Klein et al. (2010) describe a number of aspects which, in addition, are relevant for the concept of anticipatory thinking, including its importance for planning and replanning, the generation of expectancies and its role in steering the attention of the decision maker. Expertise is guiding the attention towards relevant cues and events while ignoring or downplaying others since “[e]xperience and training have created the right patterns” (Klein et al. 2010:236).

Knowledge acquisition thus lies at the heart of decision making whether or not it is explicitly future-oriented. This process can, for example, advance the decision maker’s attention management or improve his understanding of relations between factors in the environment (Klayman 1984). Knowledge acquisition can be inter alia supported by direct feedback specific to one’s actions: “If action-outcome-feedback links are *short* and *frequent* the individual is in a good position to learn about, and thus comprehend, the probable effects of action on outcomes” (Hogarth and Makridakis 1981:120, emphasis in original, see also: Sterman 1994). However, unfortunately the opposite holds true if feedback loops are infrequent, protracted or if the feedback received is distorted and thus invalid.

The experienced decision maker is equipped with a large background of domain-specific knowledge allowing him to handle the demands of the decision environment, no matter whether this knowledge is seen to be organized in a repertoire of patterns, a set of learned prototypes, or in schemas and mental models. Higher levels of expertise and greater knowledge increase the chance of decisions to be correct and thus successful. However there is also a negative side to this: If the preparation for a future event requires out of the box thinking, there is a danger that "overconfidence in our experience [...] may lead us to [...] miss something new" (Klein et al. 2010:237). Consequently, creativity can play an important role, if decision makers find themselves in situations where they have to make assumptions about possible states of the future. This aspect will be addressed in Section 4.

4. Creativity and Knowledge

This section refers to a topic that was already dominant in the previous section, i.e. the interrelatedness of the human being and the environment. It will be treated here from a different perspective. In this section human creativity will be the main point of focus. The concept of creativity plays a major role in future-oriented airport security, the fact that the security threat is continuously evolving is based on the malevolent creativity capacities on the attacker's side. This creativity is thus producing a demand for proactive security management. In this section, the theoretical foundation of creativity research will be outlined and models relevant to the pursued approach will be described. Special emphasis will be placed on the relation between learning, knowledge and creativity.

4.1 Theoretical Background in Creativity Research

More than 60 years ago, J. P. Guildford, a U.S. psychologist, spoke to the American Psychological Association (APA) in his APA presidential address. He chose creativity as topic, and emphasized the need for research in this area (Feldman et al. 1994a). In his talk he provided a rational and a research agenda for the study of creativity (Mayer 1999) and created "almost single-handedly [...] psychometric interest in the study of creativity" (Sternberg and O'Hara 1999:252). In the following years Guildford himself identified aspects relevant to creative problem solving and developed a number of tests of creativity, mainly using divergent-thinking tasks. These psychometric tests allowed a comparison of everyday subjects on a standard creativity scale (Sternberg and Lubart 1999). Torrance built upon the work of Guildford and developed the Torrance Test of Creative Thinking, which consists of verbal and figural tasks and can be scored for fluency, flexibility, originality and elaboration (Sternberg and Lubart 1999). Currently, the test remains "the most widely used assessment of creative talent" (Sternberg 2006a:87).

Despite Guildford's appeal to the research community, Feldman observed in 1999 that "the amount of research on creativity has increased during the past two decades but still lags far behind most mainstream topics in psychology" (1999:169f.). A more recent account by Sternberg suggests that this situation still persists: "What is perhaps most notable about creativity research around the world is how little there is [...], and what research there is seems to be poorly systematized" (2006b:2). Nevertheless, there are a number of methodologies and views beyond psychometric approaches that researchers commit themselves to. In the following section a short overview of models relevant for the scope of this dissertation is provided.

4.2 Models

Whereas Mayer (1999) structures existing views on creativity according to the methodologies that are employed, Sternberg and Lubart (1999) focus on approaches and underlying concepts of creativity. Among these approaches are the psychometric approaches which relate to the assumption that creativity is a trait that can be measured using paper-and-pencil tasks (this view is shared, for example, by Guildford and Torrance). This approach has been criticized for using trivial and inadequate measures, and thus failing to capture creativity. Cognitive approaches to the study of creativity seek "to understand the mental representations and processes underlying creative thought" (Sternberg and Lubart 1999:7). Personality and motivational variables as well as the sociocultural environment are seen as the source of creativity in the so-called social-personality approaches. Sternberg and Lubart argue that the understanding of creativity has so far been largely dominated by unidisciplinary approaches, focussing only on single aspects within the overall concept. They promote a multidisciplinary perspective on creativity which they believe can be found in confluence approaches. From this perspective "multiple components must converge for creativity to occur" (Sternberg and Lubart 1999:10). Two confluence approaches will be presented in more detail in the following paragraphs.

The Investment Theory of Creativity (Sternberg 2006a, 2006c) is a theory, according to which creative people are those who are able and willing to buy low and sell high. This means that creative individuals pursue ideas that are unpopular or new but demonstrate a certain growth potential. The individual insists on keeping to the idea, even when facing resistance, and eventually succeeds. There are a number of resources that present a necessary prerequisite for creativity, including intellectual abilities, knowledge, thinking styles, personality, motivation and environment (Sternberg 2006c). According to the Investment Theory, these components interact in the process of creativity. For example, a particular strength in one aspect can compensate a weakness in another and two strong components can enhance their effect on creativity multiplicatively (Sternberg 2006a). Sternberg furthermore stresses the active role of the individual in pursuing a creative idea: "Creativity is as much a decision about and an attitude toward life as it is a matter of ability" (Sternberg 2006c:7).

Another confluence approach that claims an even broader focus was developed by Csikszentmihalyi (2006). He stresses that creativity cannot be seen as an exclusively mental process and that, besides psychological aspects, social as well as cultural events need to be taken into account. In his Systems Theory of Creativity he describes the interaction between the environment in which creativity takes place and the individual and points out that "the audience is as important to its constitution as the individual to whom it is credited" (Csikszentmihalyi 2006:3). According to Csikszentmihalyi, the environment consists of domains and fields. Domains are topic-related, organized bodies of knowledge and relate to the cultural context. Fields specify groups of people capable of affecting the structure of a domain (Csikszentmihalyi 1988, cited in Feldman et al. 1994b) and, thus, relate to the social context. According to Csikszentmihalyi, creativity can only occur when these components interact:

> "For creativity to occur, a set of rules and practices must be transmitted from the domain to the individual. The individual must then produce a novel variation in the content of the domain. The

> variation must be selected by the field for inclusion in the domain." (2006:3)

Learning plays an important role in this concept as basic instructions for actions within the domain are transmitted to the individual through learning (Csikszentmihalyi 2006). This issue is also relevant in the Social Psychology of Creativity Theory developed by Amabile (1996). She views creativity as the confluence of domain-relevant knowledge and skills, creativity-relevant skills and task motivation. The aspect of knowledge in relation to creativity will be focussed on in the following section.

4.3 Knowledge

Without neglecting the general need for a confluence approach one can, nevertheless, focus on certain aspects of creativity. The study of single components of creativity, such as knowledge, can support the development of overarching theories by providing a better understanding of underlying concepts and assumption. In accordance with the confluence approaches described above, Weisberg exclusively focusses on the aspect of knowledge, but recognizes it as being "necessary, not sufficient, for creative achievement" (Weisberg 1999:248).

In an attempt to trace the approaches pursued by other researchers interested in the relation between knowledge and creativity Weisberg found that there is "a consistency in opinion concerning the need for creative thinking to go beyond the bounds of knowledge in order to produce true advances" (Weisberg 1999:229). He, furthermore, summarizes that it is assumed that changes in the environment of individuals demand this adaptation capability. Knowledge of a field is presumed to be a prerequisite when one aims at producing something novel within that field. However, it is widely accepted that too much experience can inhibit free, creative thought. In this so-called Tension View the relation between creativity and knowledge is assumed to be curvilinear, shaped like an inverted U. According to this view, the peak of creativity of a person should occur after some familiarisation with the field and before a deep immersion (Weisberg 1999).

Weisberg (1999) proposes an alternative conception of the relation between creativity and knowledge which he labelled Foundation View. He suggests that knowledge and creativity are positively related to one another and that deep domain-specific knowledge is a requirement for creative thought. In support of this view, he presents a set of studies, mainly from fields such as painting and musical composition. These studies suggest that a large amount of time has to be invested in practice, internalising the advancements of others, until a noteworthy contribution to the field can be observed. Thus, they document a positive relation between creativity and knowledge.

The next section will introduce the field of airport security and describe challenges to the efficient operation of the security system. Aspects of NDM and theories of creativity will be linked to this field of application and the relevance of knowledge-acquisition and expertise as well as the role of creativity in forestalling possible future threats will be emphasised.

5. Supporting Decision Making in Airport Security

Challenges specific to decision making within the airport environment will be the main focus of this chapter and links to the presented approaches of decision making and creativity will be provided. Moreover, methodological bases of a future-oriented approach to airport security addressing these challenges will be outlined.

5.1 The Airport Security System as Decision Environment

In this section, aspects of airport security are investigated further and related to issues touched upon in the NDM and creativity sections. It is argued, that deep knowledge of the structure of the airport security system as well as the creative development of new threat scenarios are prerequisites to successfully counteract possible future threats to the air transport system.

5.1.1 Airport Security and Complexity

Airport security as a system consists of a number of different entities, such as security technologies and activities, security personnel or the airport infrastructure, as well as underlying rules and regulations. Together they form a complex socio-technical system, aiming at preventing security incidents in the air transport system. Generally, complexity can be defined as being “first and foremost a matter of the number and variety of an item’s constituent elements and of the elaborateness of their interrelational structure” (Rescher 1998:1). As indicated above, airport security is composed of a larger number of widely varying elements that are interrelated in many areas. Airport security, thus, fulfils these ontic criteria for complex systems. From the epistemic point a view the “most plausible measure of the complexity of a phenomenon [...] is given by the *cognitive effort* we must afford in order to *adequately grasp the phenomenon descriptively and explanatorily*” (Leiber 2007:195, emphasis in original). Hofinger (2003) adds to this view by highlighting the fact that the necessary cognitive effort depends on the knowledge and expertise available to a person and draws the conclusion that the notion of complexity is always subjective (see also Brehmer 1992).

Effects of complexity on human decision making were already addressed in the NDM section, where NDM researchers were described as being interested in aspects relating to complex real-world settings (Klein et al. 1993). It was, furthermore, argued, that many of the challenges decision makers face in the real-world can be facilitated by the acquisition of knowledge within their own domain. Dörner describes this notion as inherent to complex environments: "It is characteristic of complex situations that one doesn't have complete knowledge of the situation, but rather that one must acquire this information while acting" (Dörner 1980:101). Learning to deal with the large number and variety of elements within the airport security system and to (at least partially) understand the underlying dependences determining the system's behaviour can only be accomplished gradually. Based on the argument that the airport security system can be classified as a complex environment, the next section will analyse in more detail how the field of airport security relates to the body of research in NDM.

5.1.2 Airport Security and Decision Making

The combination of complex field settings and experienced decision makers describes the main focus of research in the realm of NDM. In Section 3.2.2.1, aspects characterising such decision contexts were described. They included, for example, uncertain and dynamic environments, time stress, high stakes and multiple players (Orasanu and Connolly 1993). These aspects were identified in typical NDM environments such as fire fighting or military operations in emergency situations. Such settings are similar to the environment which decision makers encounter at an airport during the occurrence of a security incident. However, the ultimate goal cannot be reduced to handling incidents efficiently but should be directed to preventing attacks in the first place. This is acknowledged through, for example, the introduction of strict regulations on open fires in dry areas or the implementation of security checks.

To be simultaneously effective and efficient, preventive measures should always include aspects of backward- as well as forward-oriented reasoning. They should be capable of analysing past attacks as well as dealing with potential future threats. From this aspect, Endsley's level three SA (1997) and the concept of anticipatory thinking discussed by Klein et al. (2010) come to the fore again. Klein et al. (2010) have pointed out that the imagination of possible future events can provide a basis to prepare for potential threats. This aspect is particularly relevant in airport security as security measures have typically been introduced as reactions to incidents (Sweet 2002, Salter 2008a, Poole 2009, Sweet 2009), allowing attackers to continuously remain one step ahead.

Necessary requirements towards a proactive improvement of the airport security system are a large domain-specific knowledge-base with regard to system components and underlying dependences, the ability to anticipate possible future threats and the means to adapt the system according to one's insights and expectations. Once adaptions are implemented, whether the changes improved the defensive capabilities of the security system or whether they had negative influences must be determined. Unfortunately, there are a few obstacles to this course of action in the field of airport security, particularly related to knowledge acquisition, action-outcome-feedback loops, and the evaluation of effects of one's action.

As demonstrated in Section 3.2.2, expertise and training are important prerequisites to successfully deal with decision tasks in complex environments. Expertise is acquired through learning, which is often guided by direct feedback on one's actions. This would require constant observation in order to evaluate whether the system continues to behave in the expected and desired way (despite or because of the implemented changes) and to take action if this is not the case. Within the scope of airport security, changes to the system could be based on the discovery of a possible new threat or type of threat. The main difficulty becomes apparent in the evaluation phase following the implementation: Security incidents occur so seldom that changes made to an airport security system in anticipation of possible future threats (or even as reaction to attacks which have already occured) cannot be tested empirically for effectiveness. The action-outcome-feedback links are not only infrequent, in most cases they are simply non-existent. Another aspect further complicates this notion. The ultimate goal of an airport security system is to prevent attackers from even trying to conduct an attack because they feel that the system is so well protected that it is not worthwhile. In this case the success of an improved security system would become apparent in the fact that its reliability is never tested at all.

The approach developed in the course of this dissertation offers the opportunity to systematically create single threat scenarios as well as scenario clusters and analyse the security measures related to them. It is based on the systematic documentation of elements and relationships of possible threat scenarios as well as airport security measures. A software tool, the so-called Scenario Builder, provides the interface for the user und guides stepwise through the process of scenario generation. As soon as a scenario is completed the Scenario Builder automatically derives security measures specific to the chosen scenario elements. This approach offers intuitive access to the underlying structure of threat elements as well as to the interrelations between these elements and the airport security system. Users of the tool can interact with the security system, explore dependences and learn to better understand its behaviour.

Moreover, the Scenario Builder has a further function: The tool offers the possibility to move security measures to other areas of the airport or to eliminate them in a virtual manner and then trace resulting changes in the relation to threats and security measures. For example, the walk-through metal detector could be moved to the entrance of an airport. Consequently, also meeters and greeters or people intending to shop at the airport would have to undergo a body control. That would mean that attacks in the public area employing, for example, guns and grenades could be forestalled more effectively. The Scenario Builder can thus not only (partially) substitute the missing action-feedback-loops but can, furthermore, support the investigation of effects of changes in the structure of the security system. This allows the user to acquire a better understanding of the system's structure, element interrelations and the overall system behaviour.

5.1.3 Airport Security and Creativity

Creativity is a central driving force within the field of airport security. However, as the reactive adaptation of security measures in the aftermath of incidents described above suggests, it is not so much the creativity on the defending side (e.g. regulator or security technology industry) but more the creativity on the side of the attackers. Threats to the air transport system have greatly evolved over recent decades reflecting political and societal developments as well as tightening security regulations. From the 1930s onwards attacks were mostly conducted by people fleeing their home countries and seeking political asylum. They were thus directed at hijacking aeroplanes (Wells and Young 2004). Terrorists became attracted to aircraft (especially flag-carriers) as targets during the 1960s. Hijacking continued to be the dominant modus operandi but now aimed at conveying political statements (Salter 2008b). In the following decades the focus shifted to aircraft bombings and almost 50 bombs were placed on aircraft between 1970 and 1990. Misusing the aircraft itself as a weapon of mass destruction was a new procedure in the 9/11 attacks (Feakin 2011). In the last decade a shift towards an attempted exploitation of perceived weaknesses in the security chain (e.g. shoe bombs, liquid bombs, printer toner bombs) has taken place. Reviewing the evolution of past incidents Baum concludes that "the best lesson the past has taught us is that the next time it will be different" (2011:1).

The aspects of creativity and innovation in terrorism research have so far been neglected and currently remain "relatively undeveloped ideas in the context of terrorist behaviour" (Gill et al. 2013). One clear exception to this observation is the book "Understanding Terrorist Innovation:

Technology, Tactics and Global Trends" authored by Dolnik (2007). Building on detailed examples, he examines how terrorist organizations innovate, what strategies they employ, what means they have available and how successful the endeavours are.

The terms creativity and innovation are often used interchangeably as far as studies on terrorism are concerned. Gill et al. base their understanding of the two concepts on Amabile (1996), and define them as follows: "creativity refers to the generation of ideas and novel concepts, innovation involves implementing these ideas" (Gill et al. 2013:130). Consequently, creativity and innovation are two interrelated aspects of the development process of a new product or solution. Malevolent creativity preceding terrorist innovation is conducted with the awareness of negative consequences of the developed solution for others.

In a conference held 2010 at the U.S. Naval Postgraduate School the attending terrorism experts agreed on the notion that terrorist innovation is regularly driven by the ambition to overcome installed countermeasures (Rasmussen and Hafez 2010). Thus, counter-terrorism policies can be seen as "*imposing* the need for innovation on a terrorist organisation" (Gill et al. 2013:136, emphasis in original). The more creative the developed solutions are and the more radical the resulting innovations, the harder they are to anticipate:

> "Radically creative products possess the surprise factor of being rarely anticipated and thus provide a competitive advantage [...]. In the same way as businesses compete with one another, the war on terror is seen as a dynamic struggle between law enforcement officials and terrorists to out-perform one another" (Gill et al. 2013:134).

Gill et al. (2013) present the 2006 transatlantic liquid bomb plot as an example for these dynamics. In the aftermath of 9/11 many security procedures were tightened and new measures, such as the bulletproof cockpit doors, were introduced. Thus the chance of conducting attacks in the manner of 9/11 became very slight. This brought forth the impulse for jihadist cells to design new means by which the air transport system could be attacked. Bomb plots using liquid explosives in civil aircraft on suicide missions were developed but could, in these cases, be prevented through intelligence.

As demonstrated in the example, terrorist creativity is strongly influence by the environment. The confluence approaches presented in Section 4.2 were developed to take such interactions into account. From the confluence perspective, creativity can only take place when a number of different aspects converge. Csikszentmihalyi (2006) focussed on social, cultural and psychological aspects, and Sternberg (2006c) identified six components, such as personality, motivation and environment, on which creativity is based. Gill et al. (2013) analyse the conditions under which creativity takes place in terrorist organisations and find broad evidence for the need of a supportive environment, as well as motivation and ability on the terrorist side. It is a major challenge in the field of airport security to not only curtail the damage of a resulting new threat in the aftermath through emergency measures but also to proactively adapt the security system in order to principally prevent the threat. To reach this goal, the creative potential of regulators, security companies, and airport operators has to exceed the high degree of creativity displayed by the opponents.

It can be difficult to think out of the box about possible future developments when one is caught in daily business and routine. The Scenario Builder can support the creative process leading to the generation of possible new threat scenarios. The tool guides the user stepwise through the creation of a scenario, offering specific types of scenario elements to choose from at each step. Once a choice is made, the Scenario Builder automatically continues with the next category of elements, until a scenario is completed. The elements offered at each step are always consistent with those already chosen, thus limiting the user in his choice. Consequently, it is only possible to select elements that can be combined in a plausible threat scenario. This scenario building procedure supports the creativity of the user mainly because of the range of elements that are displayed at each step. To assemble a scenario, the user must actively choose one element and dismiss others, envisaging the effects of the choice made on the resulting type of threat scenario. He might be led to choose elements he would not have thought of himself and to test out different possibilities to see how the resulting scenario unfolds.

The structure of domains and elements and the functionality of the Scenario Builder as well as examples for assembled scenarios and ways to analyse the results are presented in the publications compiled in Section 6. Throughout the publications it becomes apparent how the acquisition of knowledge regarding the underlying system elements and relations can be supported through the use of the Scenario Builder and how creativity is fostered in the course of the scenario building process. In the following section the methodological background of the approach developed in the course of this dissertation will be described.

5.2 Methodological Basis of the Developed Approach

The proactive approach to airport security developed in the course of this dissertation is mainly based upon two established methodologies: matrix-based complexity management and scenario technology. In the following sections these will be introduced. More comprehensive accounts can be found throughout the publications in Section 6.

5.2.1 Matrix-Based Complexity Management

The elements and interdependences underlying the airport security system, consisting of threat scenario elements as well as airport security measures, are modelled according to a method known as Multiple-Domain Matrix (MDM) (Lindemann et al. 2009, Eppinger and Browning 2012). It is a matrix-based approach aiming at facilitating complexity management in large systems.

A structured acquisition of system elements as well as their mutual dependences is supported by this approach. The system's elements are grouped in domains and transferred to a matrix as row and column headings, both in identical order. Two types of matrices can be differentiated: Design Structure Matrices (DSM) represent elements within one domain, and Domain Mapping Matrices (DMM) connect intra-domain relationships (Steward, 1981; Danilovic and Browning, 2007). All DSMs and DMMs of a system together form the complete MDM. The structure of a documented system can be analysed visually since specific characteristics of a system, such as hierarchies and feedback loops, form defined visual patterns in the matrix. One feature of a matrix-based approach is that only bilateral dependences can be documented. This shortcoming had to be addressed in the course of the dissertation because the airport security system cannot be reduced to interdependences between element pairs. To enable scenario modelling, dependencies between more than two elements had to be captured. This methodological advancement is described in detail in Section 6.2. To include a future-oriented perspective, relevant aspects from the scenario technology approach were identified. Fundamentals of this field are presented in the following section.

5.2.2 Scenario Technology

Scenario technology is a methodology directed towards the analysis of possible future developments. In the course of a scenario process, a set of future states is derived, reflecting plausible futures within a chosen field. The method has gained wide acceptance in recent years and is a prominent approach in the toolbox of futures research methodologies collected by Glenn and Gordon (2009). The approach can be defined as

> "a process of positing several informed, plausible, and imagined alternative future environments in which decisions about the future may be played out for the purpose of changing current thinking, improving decision making, enhancing human and organization learning, and improving performance" (Chermack and Lynham 2002:376).

In a typical scenario process, a number of drivers for the specific field in question are analysed in terms of both their possible future developments and their influences on one another. Since this is a time-intensive task, in most cases the number of drivers taken into account does not exceed more than twenty. Three or five scenarios are generally constructed as outcome of such a scenario process. A more detailed introduction to the basic steps of a scenarios process is provided by de Jouvenel (2000).

The advantage of the scenario approach lies in the fact that scenarios "stimulate the imagination, reduce inconsistencies, create a common language, structure collective thought, and enable appropriation by decision makers" (Godet 2000:8). However, application of this approach to airport security is accompanied by two major shortcomings. Firstly, the elements which are relevant for modeling the threat cannot be reduced to an amount manageable in a standard scenario process. Secondly, the few scenarios that result from this process are not sufficient to reflect the vast variety of possible future threats to airport security. To overcome these limitations, elements of the scenario technology were merged with the MDM approach to complexity management.

5.2.3 Combination of the Two Methods

The airport faces a large variety of potential future threats due to the creative potential of opposing organisations. To be able to proactively adapt the security system to address anticipated new threats, the nature of relevant threats and their interrelation to available airport security measures has to be understood in great detail. To fulfil this requirement, an approach has been developed in the course of this dissertation which combines elements from scenario planning and matrix-based complexity management methods. This permits merging the capability of systematically dealing with a large variety of system elements and complex underlying system structures with the competence to provide a sound understanding of requirements of future-oriented thinking. This new approach can produce a large number of threat scenarios and automatically lists all security measures related to each scenario. The large amount of generated data poses a new challenge to the user, means of comparing and interpreting the data and of deriving valid conclusions have to be specified. Different possibilities to deal with this challenge will be discussed in the publications in the next section.

6. Publications on Methodological Aspects of Proactive Airport Security Management

This section constitutes the core of the dissertation. Different facets of the central theme - the proactive handling of complexity in airport security management - are discussed in four publications. The approach on which the publications are based was developed in the course of a research project named SiVe, which was supported by funding from the German Federal Ministry of Education and Research (BMBF). The publications will be introduced in the following paragraphs and their different focus areas will be highlighted.

6.1 Introduction to the Following Publications

The papers presented in this dissertation have been released in publications from diverse disciplines, reflecting the highly interdisciplinary character of the approach. Paper number 1 (Cole and Kuhlmann 2012) was published in FUTURES, a journal specializing in medium- to long-term future developments and methodologies of futures studies. The Journal of Air Transport Management, in which publication number 2 (Cole 2014) has been released, focusses on economic, policy and management issues of the air transport system. Paper number 3 (Cole and Maurer 2014) has been published by The International Journal of Knowledge-Based and Intelligent Engineering Systems. This journal addresses the application of intelligent systems to complex problems. The fourth publication (Maurer and Cole 2012) is a chapter in the basic work on MDM methodology by Eppinger and Browning (2012). The case of the airport security system is incorporated as an application example for multidomain architectures in MDM. The fact that each paper is published in a book or journal representing a different discipline demonstrates that the approach, in spite of being fundamentally interdisciplinary, fulfills the standards of the single disciplines it relates to. In the following all four publications are briefly introduced.

Publication number one mainly focuses on scenario process-related aspects. A standard scenario process is presented as a starting point and the shortcomings of this methodology regarding airport security are highlighted. Elements of the MDM approach are integrated into the scenario process to overcome these drawbacks and the Scenario Builder is introduced as a means to deal with the large data base developed. First suggestions are made as to how the resulting threat scenarios can be analysed. This paper was published at an intermediate state of the research project SiVe and some of the details presented here differ from later publications (such as the number of domains and elements constituting the airport security system). A preliminary version of this paper has been published in the proceedings of the "Security in Futures - Security in Change" conference of the Finland Futures Research Centre (Cole and Kuhlmann 2011).

The second publication represents the status at the end of the project. It takes up a MDM perspective and presents a structured framework for the approach developed. The different phases in building the complete model are described and the additional information generated with each subsequent step is illustrated. Phases range from the first data acquisition efforts to a detailed analysis of the results. Furthermore, the application of the approach in the context of decision making in complex systems is addressed.

Publication number three was also prepared at the end of the project. Its main focus lies in the analysis of the data generated through the application of the Scenario Builder. The relevance of scenario clusters (a group of threat scenarios that have some identical elements) for the analysis of the security system is highlighted. Two types of security measures can be differentiated: pass-through and potentially effective measures. A detailed example is provided, demonstrating the usefulness of these two concepts as well as the overall applicability of the approach. Some of the aspects elaborated in this paper were initially presented at the Air Transport Research Society World Conference in 2011 (Cole and Maurer 2011).

As an example of multidomain architectures, the fourth publication concentrates on a core area of MDM research: the interpretation of visual patterns in a matrix. Here is demonstrated how the logical structure of the scenario building process can be traced visually, reflecting the stepwise specification of different kinds of elements until a scenario is considered complete and the security measures triggered at the airport are derived.

6.2 Publications

The order of the publications presented in this section was chosen on the basis of their content as well as their overall complexity. The first two papers provide a general introduction to the approach pursued, while the remaining publications mainly focus on means to analyse the resulting data base. As mentioned above, discrepancies between the publications with regard to the general approach relate to the fact that the publications present different stages of work in progress. References can be found directly after each publication and are not transferred to the overall bibliography.

6.2.1 Publication Number 1: Cole and Kuhlmann (2012)

Cole, M. and Kuhlmann, A. (2012). A Scenario-Based Approach to Airport Security. In: Futures, 44:319-327.

A SCENARIO-BASED APPROACH TO AIRPORT SECURITY

Abstract

Mobility, particularly air transport, is vital to the economic stability and growth of a nation. It symbolizes national self-confidence and self-conception. As a result commercial aviation remains a preferred target for attacks by terrorists and other offenders. Security measures intended to render these threats harmless have mostly been introduced in response to specific occurrences, thus allowing the potential attackers to always remain one step ahead. As this approach seems inappropriate for dealing with future security threats, this paper provides a proactive approach to identification of future threats and their coverage by airport security processes and technologies. To meet the requirements of a highly complex and at the same time critical system, such as airport security, a standard scenario process has been enhanced by matrix-based methods of complexity management. This approach allows analysis of threat scenario clusters with respect to the number of potentially effective security measures. The method developed allows proactive detection of weak points in the security architecture and thus reveals potential for improvement.

1. Introduction

Mobility, particularly air transport, is vital to the economic stability and growth of a nation. Air transport symbolizes national self-confidence and self-conception, which has made commercial aviation a preferred target for attacks by terrorists and other offenders. Airports are part of the critical infrastructure of a country and provide a gateway for the majority of terrorist attacks on the air transport system. In the past, political and related scientific approaches aiming to cope with airport security matters were primarily of a reactive nature [1,2]. New security measures have regularly been introduced in a political ad-hoc process as a consequence of specific security incidents. The well-coordinated terrorist attacks on September 11 are the most prominent examples [3]. The liquid ban after the transatlantic aircraft plot in 2006 is another example of this costly and often inefficient process of reactive action.

A good alternative to this reactive procedure would be an anticipatory approach, which would allow exploration of the different characteristics of potential threats and adaption of appropriate security processes. This would not only require an in-depth understanding of the many interlinked and complex airport processes, but also a systematic assessment of threat aspects or elements, as well as, a related analysis of possible and plausible future threats. The methods of futurology might, in principle, be applicable in bridging the present gap. The use of the well-established scenario technique can provide new insights into possible future threat situations and, thus, can serve as an important prerequisite for any assessment of current and future security measures.

The typical scenario-building process is, however, insufficient for these purposes as it only results in a small number of plausible future scenarios with a rather global focus (see next section). Furthermore, such an approach only allows dealing with a relatively small number of elements in order to keep the process manageable. This is not appropriate for analysing a clearly defined system which has to deal with a large variety of possible threats and whose processes are to be improved at a level with a high amount of detail. This scope requires an approach for the development of a very high number of standardised scenarios which show a detailed level of abstraction.

In this paper, we propose a method which allows generation of the required large variety of consistent scenarios and analysis of them in a systematic way. A matrix-based method adapted from system analysis and complexity management methods is applied in order to analyse the airport security system. The combination of different threat aspects to form a valid threat scenario and their link to related security measures have been assessed and implemented in a matrix. From such a database, structurally consistent scenarios can be produced in a standardised form. Analysis of the resulting scenarios enables the user to better anticipate possible future threats, identify weak points in the security structures and, thus, to proactively improve the respective processes.

First, the standard scenario approach with its advantages and shortcomings in the context of airport security will be described. Next the enhanced approach, which allows inclusion of a high level of detail and complexity of the respective system without compromising the manageability for decision makers, will be introduced. This includes system capture, scenario building and related analyses. The last section summarises the results and provides an outlook for further research tasks.

2. The standard scenario approach

In order to deal with prospective challenges in a proactive way, futurology or foresight methods are increasingly gaining acceptance and relevance for companies and politics alike. The scenario process is one of the most prevalent techniques in the toolbox of futurological methodology. Chermack and Lynham have defined it as ‘a process of positing several informed, plausible, and imagined alternative future environments in which decisions about the future may be played out for the purpose of changing current thinking, improving decision making, enhancing human and organization learning, and improving performance’ [5]. Scenarios broaden the scope of decision makers by providing a range of possible outcomes and insight into the underlying drivers of change. Furthermore they uncover already well developed trends or predetermined outcomes such as demographic developments and they help to avoid biased and lopsided group results by facilitating contrarian thinking. Godet described scenarios as useful in a fivefold way, as they ‘stimulate the imagination, reduce inconsistencies, create a common language, structure collective thought, and enable appropriation by decision makers' [6]. However, scenarios are also prone to misinterpretation and abuse. Some have described scenarios as counterproductive for developing a clear vision and, therefore, not suited for leadership tasks [7]. Such a position neglects the fact that a goal can also be robust under several different scenarios. Decision makers, however, confronted with scenarios when they are actually searching for a one-dimensional vision or prognosis often choose one or two scenarios which are closely related to their own image of reality. Ignoring the outer scenarios leaves leaders exposed to all kinds of dramatic change. The potential of scenarios can, therefore, only be exploited if they are correctly understood and applied.

2.1. The procedure

In the 1970s, scenarios entered the field of strategic planning both in public and private sectors, with the methodologies developed and made popular by consultancy groups such as Battelle [8]. The Battelle approach (e.g. [9]) is structured in eight steps, where a problem specification (1) is followed by environmental screening (2), which then requires a specification of the relevant parameters and characteristics (3). This is followed by a clustering of assumptions (4), an interpretation of selected scenarios (5), an analysis of wild cards (6) and implications (7), which then leads to concrete action planning (8). Thirty years later de Jouvenel [10] provided a comprehensive review of scenario methods and described the prospective procedure in a similar way but condensed it to five basic steps: defining the problem and choosing the horizon (1); constructing the system and identifying key variables (2); gathering data and drafting of hypotheses (3); exploring possible futures, often with the help of tree structures (4); and outlining strategic choices (5). In the following, these steps will be referred to as the standard scenario process. The system analysis (in steps 2 and 3) also includes an assessment of the interrelations within the system, which is generally implemented by a cross-impact analysis [11]. Apart from similarities in the different standard processes described above, it is obvious that every scenario generation process varies with the specific topical context, the experience and the tools of the respective moderator.

2.2. Characteristics of standard scenario problems

Before starting the scenario generation process, the following question has to be asked in order to choose the appropriate methodological steps: To what purposes are scenarios generally well-suited and what are the relevant features in the respective system or topical context? In cases of large uncertainty and, thus, numerous and quite different possibilities for future developments in the respective environment, scenarios cannot be built reliably at any level of detail. However, even if this is not the case, it is problematic to structure “the unknown”. A reasonable and helpful way to approach this problem is to identify and describe the scenarios by means of a small number of decisive variables. Scenarios can, thus, be characterized by the two most important driving forces, resulting in an illustration of scenario-axes with the four quadrants representing four related scenarios [12]. Such a structure, which allows the making of seemingly unrelated data operationally useful, proved to be quite valuable in environments where a few decisive variables characterise an economic sector or certain political developments sufficiently. However, even for issues where many variables are needed to describe the environment, the number of resulting scenarios rarely exceeds four. This is mainly for simplicity reasons in order to avoid overwhelming the decision maker [10].

2.3. Morphological analysis and scenario building

One approach to deal with more detail and a larger variety of scenarios has been introduced with the Morphological Analysis (MA). It was originally developed by Fritz Zwicky (1898–1974) in the mid 1960s in course of his work for the California Institute of Technology [13] and rests on a matrix based representation of the considered system. The basic methodology has been improved in recent decades, mainly through computer-supported implementations, and has been successfully used for scenario development [14]. In the context of security issues, this approach allows us to decompose potential threats into key components [15]. These can then be more closely examined in order to identify the combinatorial rules between these components. This allows exploring of the event space in search of specific threat scenarios or related scenario clusters that may reveal vulnerabilities and, therefore, become of special interest. In order to attain scenarios, it is necessary to identify consistent configurations of the relevant system components. This is achieved by a pair wise comparison within a cross-consistency matrix [14], which allows to eliminate inconsistent configurations or scenarios.

In order to assess available airport security measures with respect to relevant threat scenarios, the matrix based system representation needs to include many airport related components as well as threat elements. This results in a very high number of relevant elements. A pair wise comparison, as conducted in the MA approach described above, is very difficult, because of the extremely high amount of theoretically possible configurations. Therefore, our approach goes beyond a standard MA-based scenario procedure and draws on methods from the field of product development capable of dealing with high structural system complexity. We introduced an additional matrix on a higher level of abstraction, the so-called “Multiple Domain Matrix”, which allows handling the large number of elements as well as the corresponding system complexity. The resulting enhanced scenario process is described in Section 3.

3. The enhanced structural complexity scenario approach

In the context of airport security it is neither sufficient to use a small number of descriptive variables, nor is a small number of scenarios adequate to cover the possible varieties of future threats. Here a clearly defined complex security system (characterized by a variety of utilized processes, technologies and involved actors) has to deal with a large variety of threat aspects and, therefore, many variables or critical uncertainties. An approach to dealing with airport security in a proactive way would, therefore, require a process which includes the advantages of scenario planning without compromising the specific requirements of the airport security system. Such requirements include the development of numerous standardised scenarios which still offer a high level of abstraction. This is necessary as scenarios – in this context – serve to identify as many security threats as possible and do not just give an idea of the most plausible lines of development. These requirements are not in line with the standard scenario approach delineated above. The following sections describe an approach, which allows fulfilment of these requirements in a prospective and, therefore, proactive way and thus overcomes the shortcomings of standard scenario planning in the context of airport security.

3.1. System coverage, data gathering and structuring

As mentioned above most scenario processes approach the topic in question in a structured way, with clear steps. The procedure may vary in detail from one scenario project to another but the basic steps mostly stay the same. Moats et al. express it in the following way: 'Although there are numerous variations on how to conduct a scenario planning exercise [. . .], all have certain elements in common' [16]. This section will demonstrate how the adaptation of standard scenario methods helps to overcome the constraints faced when dealing with large, complex systems on a very detailed level. The procedure will be demonstrated by drawing on examples from a scenario process conducted at Bauhaus Luftfahrt concerning airport security, which was performed by means of matrix based methods of structural complexity management, originating from product development methodology [17].

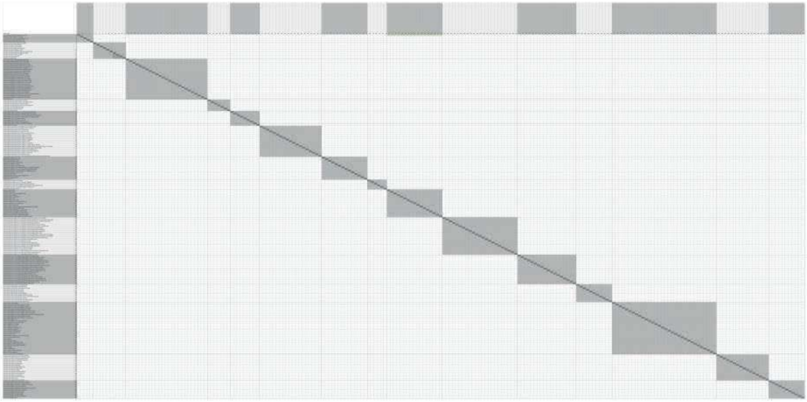


Fig. 1. MDM on element level.

The first step of the standard scenario process (see previous section) is conducted to define the problem as well as to choose the horizon. Environmental scanning can help to detect important influencing factors as well as to define the limits of the system in question [18]. In the case described in this section, expert discussions as well as literature reviews helped to identify potential influencing elements of the airport security system. During this process the borders of the system were clearly defined or, in de Jouvenel's words, the horizon was chosen [10].

Once the system's borders had been defined, the variables influencing airport security were compiled–a procedure corresponding to step two of the standard approach. To be able to analyse interdependences within the airport security system from an integral point of view, security measures as well as elements of threat scenarios were gathered. To escape the danger of subjectivity, elements were collected by experts from different backgrounds and with different interests in the process. Structuring the collected elements was the next step in the scenario process conducted. The terms were clustered and structured hierarchically. In this first version, 210 elements constituted the system on the lowest hierarchy level, structured by up to seven hierarchy levels and subsumed under 15 top level categories. Nine of these categories refer to threat elements including characteristics of the "potential offender" and his possible "intentions". Furthermore, different types of "tools or weapons" are included as well as their respective "application possibilities" (such as remote or manual release). Different ways of "approaching the airport", "inserting the weapon" and the "location of the offender" at the time of his attack form three more categories. The "target of the attack" as well as "resulting threats" completes the comprehensive description of a threat scenario. Two other categories describe countermeasures for security threats at an airport. "Preventive measures" include, on the one hand, processes such as hand-luggage checks and on the other hand technologies such as metal detectors, whereas "reactive measures" contain mostly processes such as evacuation. Remaining categories include other influencing factors in the airport context such as "actors" (e.g. different airport users and employees, police, legislation) involved, their respective "interests", and "human factors" affecting the quality of security processes.

Following a standard scenario process, the next step would have been to transfer the elements to a matrix to be able to carry out a cross-impact analysis of all elements gathered. Transfer of the collected terms to a matrix allows the elements to serve as row headings and as column headings – both in the same order – resulting in a Multiple Domain Matrix (MDM). Diagonal matrix cells thus represent self-reflexive dependences. Since the system shows a very high level of detail this would have required specifying 44,100 relations (see Fig. 1).

Since this is an impossible task with respect to time resources, another way had to be found to approach the cross-impact analysis. At this point, it was necessary to alter the standard scenario process and adapt the approach to the specific requirements of the airport security system. Thus, an intermediate step was introduced to reduce the relations to the logically necessary connections. This is generally necessary if a system consists of too many single elements (and thus element interrelations) to be considered within a reasonable timeframe. To gain a more general impression of the system, it is vital to change the level of abstraction. Up to this point, the focus has been laid on the element level, the perspective is now broadened, focussing on the highest level (the "domain level") of the system. On this level of abstraction, which of the domains are directly linked to each other can be verified and which of them are not connected at all. The latter domain-pairs can later be excluded when performing a cross-impact analysis on the element level. This interim step significantly reduces the element connection considered to a feasible number.

After identifying the domain-linkages, the direction and specific quality of each relation was discussed and named. With the help of a flowchart these connections were illustrated (see Fig. 2). The arrows in Fig. 2 represent the direction as well as the quality of a relation between two domains (e.g. "potential offender" has "intention"; "tool/weapon" is suitable for "target").

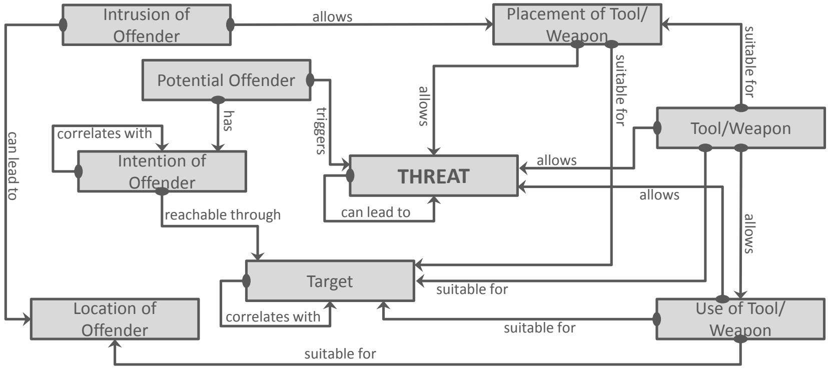
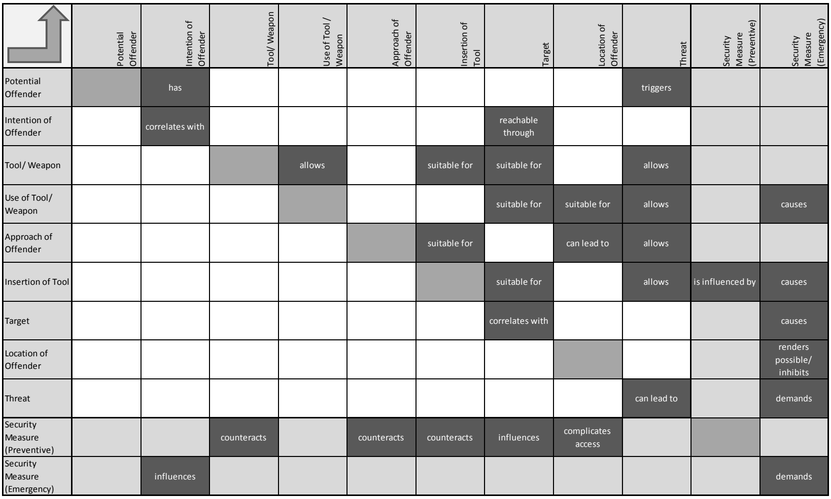


Fig. 2. Detail of flowchart (showing 9 out of 15 domains).

After both the quality of the logically necessary interrelations and their direction of influence have been specified, domains can be transferred back to a matrix design. Fig. 3 shows the result for those domains of airport security which are relevant in the context of this paper. Each filled matrix cell represents an arrow from the flow chart and, thus, the connection of one domain to another. In the matrix cells, each type of connection is specified. Just as in the element matrix (see Fig. 1), the domains in the rows influence the domains in the column heading. This representation method makes it possible to document the direction as well as the specific kind of relation in a very clear way and thus allows for an intuitive access to the data. The section of this domain matrix presented can be subdivided into two major areas: the red represents the elements necessary to form a valid threat scenario and the blue represents the preventive and reactive (i.e. emergency) countermeasures an airport can apply.



	Potential Offender	Intention of Offender	Tool/ Weapon	Use of Tool / Weapon	Approach of Offender	Insertion of Tool	Target	Location of Offender	Threat	Security Measure (Preventive)	Security Measure (Emergency)
Potential Offender		has							triggers		
Intention of Offender		correlates with					reachable through				
Tool/ Weapon				allows		suitable for	suitable for		allows		
Use of Tool/ Weapon							suitable for	suitable for	allows		causes
Approach of Offender						suitable for		can lead to	allows		
Insertion of Tool							suitable for		allows	is influenced by	causes
Target							correlates with				causes
Location of Offender											renders possible/ inhibits
Threat									can lead to		demands
Security Measure (Preventive)			counteracts		counteracts	counteracts	influences	complicates access			
Security Measure (Emergency)		influences									demands

Fig. 3. Detail of MDM on domain level (showing 11 out of 15 domains).

After the domain's relations have been reduced to the logically necessary ones, the standard scenario process can be picked up again. According to de Jouvenel [10] a cross-impact matrix is often employed at this stage to analyse the relations between elements. It is typically used as 'a schema for collating and systemizing [...] expert judgments, so as to make it possible to construct a conceptual substitute, however imperfect, for a wished-for but nonexistent theory of how events affect each one another in a multidisciplinary context' [19]. At this point, the level of abstraction has to be changed back to the lowest hierarchy level of the system, the element level. Each matrix cell in the domain level represents a submatrix on the element level. For the following cross-impact analysis, only those element relations are considered that belong to a domain interrelation that is marked as logically necessary in the domain matrix.

To ensure a certain level of quality and to overcome the impending subjectivity, the determination of the connections has to be carried out by a certain number of researchers with different scientific backgrounds. Mostly binary decision (indicated by 0 and 1) sufficed to document the relationship between two elements. In some cases, a more detailed differentiation was necessary and the relation was specified by a weighted value (+2, +1, 0, 1, 2), indicating positive or negative influences. For example, a terrorist could have the intention of causing commercial damage, a high loss of human lives and, thus, demoralising the population. He could do this by attempting to smuggle explosives or a knife through the hand-luggage check. This is the point where the airport can render the whole threat scenario harmless. Security measures always address single aspects of threat scenarios and never the scenario as a whole. By detecting elements of the scenario one hopes to render the whole potential threat unsuccessful. If, for example, the explosives are detected during the hand-luggage check the whole scenario falls apart because the offender cannot complete the scenario without a weapon.

To cover evolving threats, it is sometimes necessary to adapt the documented system relations. There are three different possibilities to alter the database gathered. First, connections between elements can be changed so that elements that were previously not connected are related and vice versa. This could become necessary if, for example a known weapon was used in an innovative way that had not been anticipated. The introduction of new elements is the second possibility to change the system which is fairly easy to implement. Hereafter, the new elements have to be interlinked carefully according to the logic connection of their domains. The third possibility is to integrate a new domain, a step that entails far-reaching adaptations and should only be performed if a new, unexpected threat appears, requiring an adaption of system borders. A consequence of alterations on the domain level is that the underlying logic of the overall system also has to be adjusted to properly integrate the new aspects of either threat or security measures.

These modes of system alteration also allow injecting different levels of alleged implausibility into the system. Elements and respective connections, for example, may be deliberately added or related in a way which shows no logical connection from today's point of view. For example, prior to the events of 11th September 2001 an aircraft would not have been considered as an effective weapon of mass destruction, but only as a target. This procedure, however, serves to stimulate imagination in a structured way, thus facilitating the anticipation of different possible futures.

In a standard scenario process, the next step would be to collect data concerning the past, present and possible future development of the variables considered. As a consequence of the very high level of abstraction of the airport security system considered, the elements themselves are not subject to development. It is their interaction within the system that lets the system as a whole evolve. Thus the complexity and high detail does not allow approaching the compilation of scenarios with the help of plausible projections. Consequently, another way has to be found to extract the information gathered during the cross-impact analysis to generate consistent scenarios. This process, which is completely beyond the scope of the standard scenario process, will be described in the following section.

3.2. The scenario-building-process

The specified connections in the scenario-part of the matrix (illustrated by the red area in Fig. 3) build the base for generating structurally consistent and, thus, plausible scenarios. Assuming that the matrix comprises all possible threat elements and correct interconnections between them, one could theoretically claim that all possible threat scenarios are covered by this approach. All the different shapes a scenario can assume are documented through different combinations of the interlinked elements. The elements of a historic or fictive threat scenario can, then, be traced within the detailed system matrix (see Fig. 1). Two results arise from mapping scenarios on to the documented structure: by mapping historic scenarios, the quality of the documented system can be scrutinized and by mapping fictive scenarios on to the matrix the plausibility of the scenario itself can be validated regarding its structural consistency.

To verify the consistency of fictive scenarios, one has to take a close look at the system on the element level and check the interlinkage of the different element pairs one by one. Since the system does not only consist of threat scenario elements but also includes security measures, the relation between the scenario and potentially effective countermeasures can be traced. Again the connection of each element of the threat scenario to each element of the security measures has to be assessed. Because of the high structural complexity, it is very time-consuming to trace each connection. To make the system more easily accessible and to overcome these problems, the domains of the system were connected via an underlying process logic derived from the partitioning process and connected by the Boolean algebra operators AND and OR. This logic was applied to the whole dataset (the single matrix elements) in a tool based on MS Excel called “scenario builder”.

The “scenario builder” helps to compile threat scenarios and offers a clear representation of the scenario-specific countermeasures. It allows generation of (threat) scenarios by successively choosing consistent elements from different domains until a scenario is completed. The sequence is based on the underlying logic (starting with the “potential offender”, as illustrated in Fig. 2) and every successive choice or step only allows choosing from a reduced selection of elements in the next domain, according to the logical link from the previous choice. The scenario builder, thereby, guides the user through the process of compiling elements to form a consistent scenario. Besides creating scenarios in a very time-efficient way, this approach has the advantage of also producing scenarios that might seem to make no sense from a rational point of view but that are, at the same time, structurally consistent – e.g. scenarios a mentally disabled person might pursue.

After the scenario is compiled, the scenario builder automatically lists the security measures that are connected to the elements of the scenario. This helps to evaluate the effectiveness of existing security measures because the scenario and the related measures are directly opposed. Fig. 4 depicts the sequence of steps that have been described so far on the basis of the standard scenario approach as discussed in Section 2.1. The last step "analysis of data set" will be described in the following section.

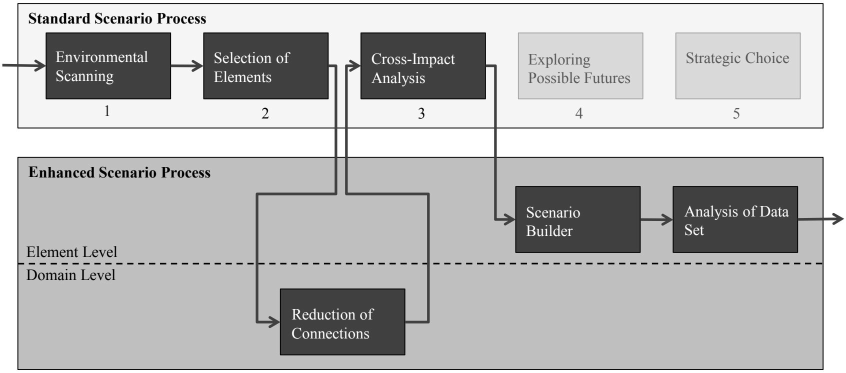


Fig. 4. Standard and enhanced scenario process.

3.3. The system analysis

The content of the matrix allows analysis of many structural aspects of the security system and their relation to specific threat elements. One possibility is to analyse the risk coverage by preventive security measures but single threat aspects or elements are not the relevant perspective, as their combination (or the scenario) creates the valid threat [20]. The scenario builder renders the broad space of all structurally consistent scenarios accessible in a rather intuitive way. To gather a certain amount of scenarios in order to analyse them, for example, with respect to the related security measures, is still a timeconsuming activity. The scenario-building process has been automatised in order to ensure that the evaluation of the function of the security measures in relation to different scenarios has a broad database. Through the automatic analysis, the span of the space of all structurally consistent scenarios can be fully exploited. The first analysis of the airport security system, which had to run under certain restrictions in order to match the available calculating capacity, resulted in more than 220,000 scenarios. With this large set of scenarios, it is possible to analyse structurally weak points in the airport security system. For this purpose the scenarios can be sorted according to the number of related security measures which potentially address the respective threat elements (see Fig 5).

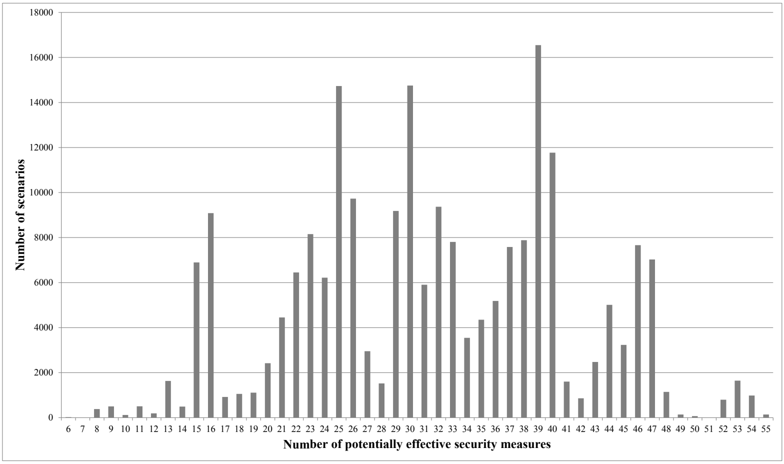


Fig. 5. Scenarios and potentially effective security measures.

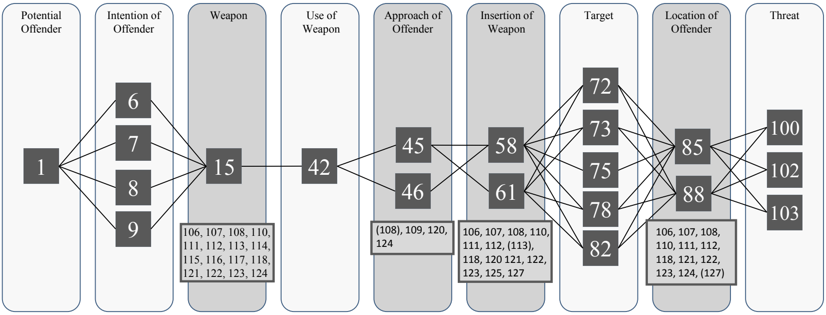
By clustering similar scenarios, in which in principle only a small number of countermeasures are able to address the threat (see the ellipse in Fig. 5), one can identify threats which are dangerous from a structural point of view.

Fig. 6 illustrates how the different parts of (standard) threat scenarios can be opposed to relevant counter-measures and consequently be visualized. This example shows a cluster of similar scenarios, in which a suicide bomber tries to smuggle explosives into the security zone of an airport to reach a specific target. The columns depict the nine domains of the threat scenarios. The numbers in the blue squares represent the scenario elements, while the ones in the red boxes indicate the elements of preventive counter-measures, which are part of the airport security system. When the terrorist tries to conceal the weapon on his body (item 58), the most relevant counter-measure is the passenger control (item 111), while concealing in the hand-luggage (item 61) is, amongst others, addressed by the hand-luggage check (item 113). Similar analyses can identify where redundancies in the system are very large, which might indicate a bad cost–benefit performance.

4. Discussion and outlook

In the past, new airport security measures have regularly been introduced in political ad-hoc processes, often as a consequence of specific security occurrences. A precondition to overcome this reactive procedure would be to apply an anticipatory approach. Scenario-planning methods could, in principle, be applied to address this problem. However, the typical scenario-building process is insufficient for this purpose since a large database of plausible scenarios is needed to be able to systematically improve the airport security system. Thus an approach merging elements from a standard scenarioprocess, system analysis and matrix-based complexity management has been developed and is described in this paper.

This approach allows combination of the advantages of a prospective foresight method, which is generally vague in terms of tangible developments in specific sub-systems, with the accuracy of an in-depth system analysis of airport security. Two adaptations of the standard scenario process are central: first, the logical reduction of possible links between elements for the cross-impact analysis which is necessary to handle large complex systems. The second major extension is the introduction of the “scenario builder”, allowing for a time-efficient analysis of the complex data. This kind of extended scenario analysis allows demonstration of effects of a specific scenario on other affected stakeholders or systems (in this case on airport security). Such an automatised approach is valuable when a large variety of scenarios has to be analysed. This, in turn, allows a better optimisation of the system concerned because the interrelations are documented and, thus, evaluable, for example, with respect to structurally weak points in the system.



1: Terrorist, 6: Economical damage, 7: Human lifes, 8: Attention, 9: Fear, Demoralization, 15: Explosives, 42: Manually – calculating personal death, 45: Street, 46: Rail, 58: Concealing weapon on body, 61: Concealing weapon in hand-luggage, 72: Aircraft flying, 73: Aircraft at ground level, 75: Fuel depot, 78: Restricted area, 82: People, 85: On-board, 88: Restricted area, 100: Hijacking, 102: Sabotage, 103: Renegade

Fig. 6. Threat scenario cluster with respective security measures.

The scenarios analysed still suffered from the restrictions described regarding the limited choice of threat elements. This largely reduced the resulting number of relevant scenarios which could be analysed. To overcome this constraint, it would be necessary to migrate the data to a more powerful software environment, such as a database developed to suit the specificities of the system. An automated analysis run through without the former restrictions would produce an exponentially increased number of logically possible scenarios. Given that millions of scenarios cannot be analysed with an appropriate effort, one has to define ways of extracting reasonable scenario clusters. These clusters could provide a better access to relevant threat categories, as they would combine similar threat characteristics which are treated alike by airport security measures.

For a general overview on the complete airport security analysis of the whole “SiVe” project, which includes simulations as well as cost-benefit-analyses, see Breiing et al. [21]. A more specific description of how the scenario builder is interconnected with simulation and risk quantification modules and how aggregated risk values are derived is given by Maurer et al. [22].

Acknowledgements

This article has been developed in the course of the research project “SiVe” which is funded by the Federal Ministry for Education and Research as part of the German Research Program for Civil Security, which in turn is part of the High-Tech- Strategy of the Federal Government of Germany. The authors would like to thank Dr. Maik Maurer, Teseon GmbH, for his valuable input to this article.

References

[1] M.B. Salter (Ed.), Politics at the Airport, University of Minnesota Press, 2008.

[2] K.M. Sweet, Terrorism and Airport Security, Edwin Mellen Press Ltd., 2002.

[3] ACRP Synthesis 3, General Aviation Safety and Security Practices, FAA, 2007.

[4] J.C. Glenn, T.J. Gordon (Eds.), Futures Research Methodology, Version 3.0, UNU Millenium Project, 2009.

[5] T.J. Chermack, S.A. Lynham, Definitions and outcome variables of scenario planning, Human Resource Development Review 1 (3) (2002) 366–383.

[6] M. Godet, The art of scenarios and strategic planning: tools and pitfalls, Technological Forecasting and Social Change 65 (1) (2000) 3–22.

[7] C. Roxburgh, The Use and Abuse of Scenarios, McKinsey Quarterly, November 2009.

[8] M. Godet, F. Roubelat, Scenario planning: an open future, Technological Forecasting and Social Change 65 (1) (2000) 1–2.

[9] U. von Reibnitz, S. Seibert, H. Geschka, Die Szenario-Technik als Grundlage von Planungen, Battelle-Institut, 1982.

[10] H. de Jouvenel, A brief methodological guide to scenario building, Technological Forecasting and Social Change 65 (1) (2000) 37–48.

[11] T.J. Gordon, H. Hayward, Initial experiments with the cross-impact matrix method of forecasting, Futures 1 (2) (1968) 100–116.

[12] S. van't Klooster, M.B.A. van Asselt, Practising the scenario-axes technique, Futures 38 (1) (2000) 15–30.

[13] F. Zwicky, Discovery, Invention, Research—Through the Morphological Approach, The Macmillan Company, 1969.

[14] T. Eriksson, T. Ritchey, Scenario development using computerized morphological analysis, adapted, in: Cornwallis International Operations Research Conference, 2002.

[15] H. Jimenez, I.C. Stults, D.N. Mavris, A Morphological approach for proactive risk management in civil aviation security, in: 47th AIAA Aerospace Sciences Meeting, 2009, AIAA 2009-1636.

[16] J.B. Moats, T.J. Chermack, L.M. Dooley, Using scenarios to develop crisis management: applications of scenario planning and scenario-based training, Advances in Developing Human Resources 10 (3) (2008) 397–424.

[17] U. Lindemann, M. Maurer, T. Braun, Structural Complexity Management, Springer, 2009.

[18] T.J. Gordon, J.C. Glenn, Environmental Scanning. Futures Research Methodology, Version 3.0, 2009 UNU Millenium Project.

[19] O. Helmer, Reassessment of cross-impact analysis, Futures 13 (3) (1981) 389–400.

[20] M. Cole, A. Kuhlmann, O. Schwetje, Aviation security—a structural complexity management approach, in: 13th Air Transport Research Society World Conference, 2009, Paper No. 96.

[21] M. Breiing, M. Cole, J. d'Avanzo, G. Geiger, S. Goldner, A. Kuhlmann, C. Lorenz, A. Papproth, E. Petzel, O. Schwetje, Optimisation of critical infrastructure protection: the SiVe project on airport security, Lecture Notes in Computer Science 6027 (2010) 73–84.

[22] M. Maurer, M. Cole, J. d'Avanzo, D. Dickmanns, Airport security: from single threat aspects to valid scenarios and risk assessment, in: 1st Global Conference on Systems and Enterprises, 2009.

6.2.2 Publication Number 2: Cole (2014)

Cole, M. (2014). Towards Proactive Airport Security Management: Supporting Decision Making Through Systematic Threat Scenario Assessment. In: Journal of Air Transport Management, 35:12-18.

TOWARDS PROACTIVE AIRPORT SECURITY MANAGEMENT: SUPPORTING DECISION MAKING THROUGH SYSTEMATIC THREAT SCENARIO ASSESSMENT[1]

Abstract

An airport is the gateway which facilitates access to air transport. As a reaction to very diverse attacks on the air transport system during the last decades a broad range of security measures has been introduced to mitigate possible threats. The challenge to provide a trouble free experience for the passenger and, at the same time, to operate more efficiently calls for a proactive approach. This requires the definition of future requirements that allow an adaptation of the security system. When dealing with uncertainty that future-oriented decisions inevitably display, it is important to gain as much knowledge as possible about a system's general structure. The approach described in this paper systematically documents elements and relationships of the airport security system. It consists of threat scenario elements as well as security measures. The development of a software tool, the so-called Scenario Builder, is described and its application for the identification of possible future threats explained. The presented approach offers intuitive access to the underlying structure of the airport security system. It provides decision makers

[1] The results presented in this paper are part of the research project SiVe, which was partially financed by the German Federal Ministry of Education and Research (BMBF). SiVe was part of the Security Research Program initiated in the context of the High-Tech Strategy by the German Federal Government.

with a possibility to interact with the system and anticipate effects of threat development, thereby enabling robust, future-oriented decisions.

Keywords: Airport security; Threat scenarios; Complexity management; Robust decision making

1. Introduction

The airport offers the interface between ground and air transport, functioning as a gate through which passengers, crew and employees must pass in order to access air transport. For various reasons, the air transport system has been a preferred target for attacks for many decades (Sweet, 2009), leaving airports "constantly under potential threat [...] from a variety of sources" (Kirschenbaum et al., 2012a). The airport security system in place today is supposed to mitigate potential threats. To this end, layer after layer of measures have been introduced, often as a direct reaction to specific incidents, creating a very complex socio-technical system. As threats have constantly evolved in the past and most likely will continue to do so in the future, the security system has to be improved constantly. Baum (2011) draws the conclusion that with regard to aviation security incidents "the best lesson the past has taught us is that the next time it will be different".

A long term vision for the air transport sector has been recently published in the so-called "Flightpath 2050" report by the High-Level Group on Aviation Research under the leadership of the European Commission (European Union, 2011). In this document, a risk-oriented approach is called for to enable future airport security systems to simultaneously address relevant threats as well as to operate more efficiently. Decision makers will thus have to take possible future developments of the overall threat situation into account to proactively adapt the system's processes and technologies. This would imply a radical change of the component-oriented way airport security is structured today: Currently airport security measures mostly address objects that could be used in an attack. Accordingly, the walk-through metal detector is implemented to prevent guns or knives from being carried on board and sniffer tests are used to detect traces of explosive devices. This approach has been criticised in the past. Rather, processes searching for “bad people” instead of “bad objects” have been called for (IATA, 2012). But this is not sufficient as by themselves neither “bad people” nor “bad objects” pose a threat to passengers, airport or aircraft. A valid threat only arises from the combination of certain core elements, as risk can only be allocated to a threat scenario not to single components. For example, a knife itself does not pose a threat, but an offender smuggling a knife into the secured area of an airport to use it in an attack certainly does. Consequently, a risk-based improvement of security measures has to be based on the meaningful combination of threat elements.

Such an approach poses a major challenge for decision makers in the field of airport security. Everyday judgements are based on experience and best practices. However, in the case of a proactive, future-oriented approach there are no precedents. The objective of this paper is to present an approach that tackles this challenge by focussing on the systematic development of threat scenarios. It is described how possible future threat scenarios and their relationship to airport security measures can be collected, documented and analysed. To this end, elements and structural principles underlying the creation of valid scenarios are outlined and their connection to airport security measures is described. It is the aim of this paper to demonstrate how the knowledge of relationships between threat scenarios and security measures gained through the presented method allows decision makers to better understand the interaction of system components. The presented approach provides procedure to support proactive and more robust decision making in the field of airport security. The approach focuses deliberately on documenting objective dependencies and does not take the behavioural interactions and informal networks into account that security personnel rely in their everyday decision as these aspects have been addressed in depth by Kirschenbaum et al. (2012a; 2012b).

2. Structure of the Methodological Approach

In Section 2 a short literature overview dealing with decision making in complex situations, modelling of complexity and scenario techniques is presented. Furthermore, the underlying components and relationships of the airport security system are described. In this section the foundation is laid for a step by step description of the approach (Section 3) and the subsequent discussion of the findings in the context of decision making processes (Section 4).

2.1 Literature Review

Over the past decades the topic of decision making in complex situations or systems has attracted wide interest in different research areas. In 1983 Dörner et al. published their findings from an empirical study based on computer-simulated microworlds (see also: Brehmer and Dörner, 1993). Developments in computer technology allowed them to create dynamic simulation environments, reflecting real-world decision problems: complexity, dynamics and opaqueness (Brehmer, 1992). In an initially unpublished manuscript from 1973 Luhmann defined discretionary competence as the competence to adequately deal with complexity (Luhmann, 2009). However, creating robust strategies in a system where states of uncertainty and lack of knowledge are constituent (Willke, 2009) is a major challenge for decision makers. An important prerequisite for this task is a thorough understanding of the system's structure (Maani and Maharaj, 2004) allowing one to evaluate the effect of a decision taken on possible future developments of the system. The approach presented in this paper offers the possibility to gain insights into future threats and to learn about connections within the airport security system.

The system's dependencies are modelled mainly following a method known as Multiple-Domain Matrix (MDM) (Lindemann et al., 2009; Eppinger and Browning, 2012). It is a matrix-based approach for complexity management, supporting a systematic collection of system components as well as their respective dependencies. Different groups of elements – structured in so-called domains – are represented in a MDM. The method is furthermore designed for analysing system structures apparent after data acquisition. Characteristics of a complex system such as feedback loops or clusters can be visually identified as they form typical patterns in the matrix.

As the original MDM approach has not been developed to deal with future developments, insights from the field of scenario planning (Godet, 2000; de Jouvenel, 2000; Gordon and Glenn, 2009) have been included in the method presented in this paper. A detailed description of the steps necessary to integrate aspects of scenario planning with the MDM is provided by Cole and Kuhlmann (2012). The combination of methods allows benefiting from the knowledge acquisition provided by a structured complexity management approach as well as from a future-oriented perspective of the system addressed. In Section 2.2 basic areas that constitute the airport security system as well as the fundamental underlying system relationships are described.

2.2 Towards a Proactive Approach to Airport Security

The method presented in this paper supports the systematic gathering of elements as well as their interrelations relevant for the representation of an airport security system. Core areas that need to be considered are depicted in Figure 1. "Use Cases" represent the apparent use of the airport infrastructure (see Figure 1, box 1) and consist of two different subcategories, "Actor" and "Action". The category "Actor" includes elements such as passengers, employees or visitors. "Action" describes activities that can be pursued at the airport, for example boarding an aircraft, picking up somebody or working. A "Use Case" is thus composed from one element out of each category: e.g. a passenger boarding an aircraft or a meeter and greeter picking up friends or relatives. Each "Use Case" combination implies certain areas of the airport the actor is granted access to. Meeters and greeters, for example, are not allowed to access the secured area of an airport. Thus, the "Use Case" strongly influences the range of security measures a person has to undergo.

The "Use Case" furthermore reduces possible elements for the second core area, the threat scenario (see Figure 1, box 2). In this area over 100 threat scenario elements are subsumed under eight domains such as "Potential Offender", "Tool/Weapon" or "Intention of Offender". Dependencies between scenario elements are documented in a matrix: For each relevant combination of two threat elements it is specified whether or not they could logically occur in the same scenario. This data base allows assembling elements from the different domains that together form a valid threat scenario. As described above, the choice of elements for the threat scenario is restricted by the predefined "Use Case": If, for example, a potential offender pretends to be a visitor and consequently does not possess a valid ticket, it would (in most cases) not make sense to choose the aircraft as target of the scenario created. Once a set of elements is chosen, a structurally consistent threat scenario is assembled.

The specifications made in the first two areas predetermine the possible paths an attacker can pursue on his way through the airport (see Figure 1, box 3). In most cases the alternatives are narrowed down to two or three options. The clear definition of the path is the last piece of information necessary to indicate which security measures need to be taken into account in an analysis of the threat scenario outlined by elements from the three areas described above.

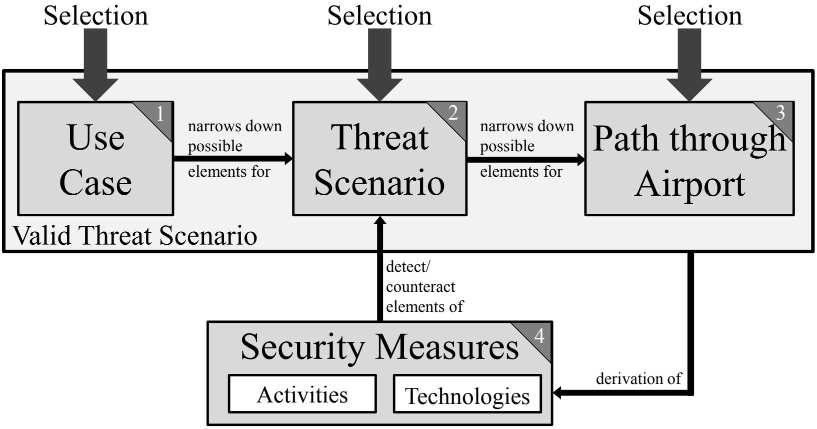


Figure 1: Core areas of threat scenario assessment

Airport security measures are addressed in the fourth box of Figure 1. They are split into security technologies and security activities. The latter relates to the processes that somebody might undergo, security technologies relate to the means by which the process is conducted. Security measures are not actively selected by the user, but automatically derived once a threat scenario is assembled according to the steps described above. Today's security measures are implemented to reveal certain aspects of the threat: They detect or counteract specific elements. The relationships between different security measures and threat elements are documented in the same matrix as the elements outlining the threat. Thus, if elements for a threat scenario are chosen, their interlinkage with relevant security measures can be directly derived.

The logical structure described in this section as well as many different components need to be taken into account to get a comprehensive impression of the airport security system. In order to handle the large number of elements a method has to be employed allowing systematic gathering of elements and interrelations, providing means by which the data can be analysed and enabling the incorporation of possible future developments. The method adapted for these tasks will be described in detail in the following section.

3. The Scenario Building Process

The presented approach can be divided into six phases. The first four phases constitute the data gathering and scenario building section of the approach. The analysis of the generated information takes place in phase five and six (see Figure 2).

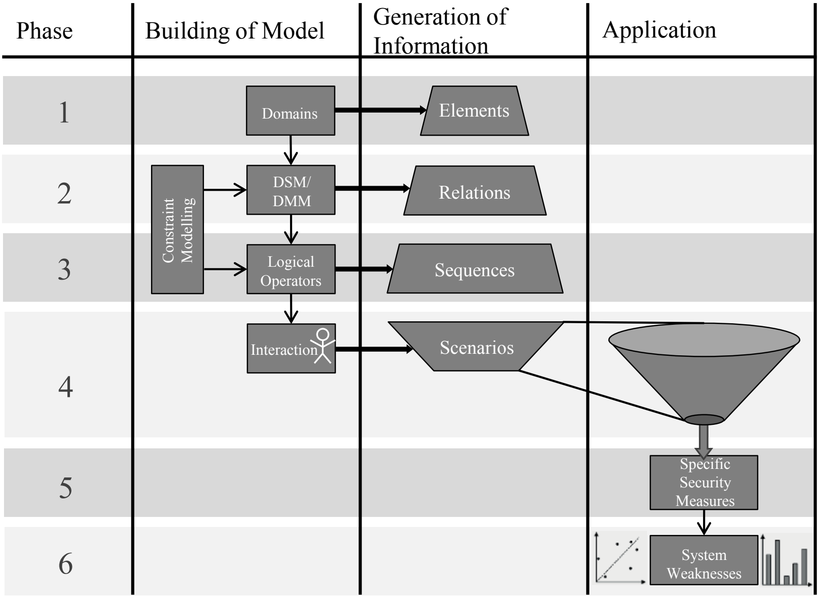


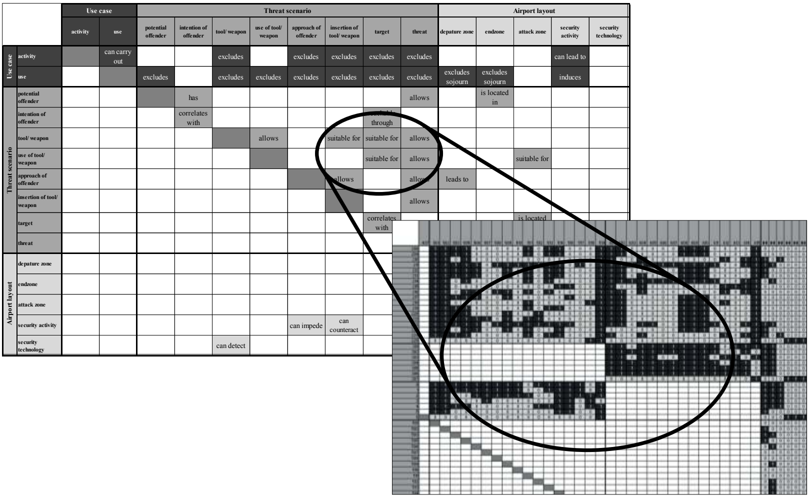
Figure 2: Framework for the developed approach

3.1 Definition of System Components

The first step when approaching a new system is to roughly specify relevant aspects that need to be incorporated as well as to define the system's borders. It is important to include different experts with an in-depth knowledge of the discussed subject during this data gathering to make sure that no important aspects are being overlooked. The collected aspects were regularly contrasted with historical incidents to make sure that all relevant aspects had been included in the data gathering phase. A mind map was used to systematically assemble and structure the data. Over the course of the project this first set of elements was iteratively redefined taking new insights into account. The final version the airport security system consisted of 235 elements, subsumed under 15 domains. These include the areas presented in Figure 1 (boxes 1-4). The hierarchical tree structure of the mind map supported the depiction of the gathered data in two different matrices: The first matrix was built from the factors of the main branches of the mind map, so-called domains. These were transferred in the matrix as row as well as column headings. The items on the most detailed level, so-called elements, were taken as row and column headings for the second matrix. The result of this first phase is the specification of necessary system components on the domain level (see Figure 2, Building of Model) as well as the population of the domains through the gathering of elements (see Figure 2, Generation of Information). In this phase the basis for all subsequent steps is generated.

3.2 Development of System Structure

The second phase aims at defining the mutual dependencies between the elements of the airport security system. In a systematic approach all possible combinations of elements would need to be considered. This is not possible in such a large system as this would have meant to specify more than 55.000 dependencies. The MDM approach offers a solution to this problem: Instead of directly specifying the element dependencies, the focus initially lies on the dependencies between domains. As the airport security system consists of 15 domains, this results in a matrix with 225 cells representing possible dependencies to be considered, with row domains influencing column domains (see Figure 3). In the next step logically necessary connections between the domains were specified. For example, the domains “potential offender” and “intention of offender” are connected by the dependency “has” (an offender has a certain intention), and the domains “tool/weapon” and “target” are connected through the dependency “suitable for” (a weapon is suitable for a specific target). Eventually, only 44 out of the 225 domains needed to be connected in this way, representing the system’s logical structure.



		Use case		Threat scenario								Airport layout				
		activity	use	potential offender	intention of offender	tool/ weapon	use of tool/ weapon	approach of offender	insertion of tool/ weapon	target	threat	depature zone	endzone	attack zone	security activity	security technology
Use case	activity		can carry out			excludes		excludes	excludes	excludes	excludes				can lead to	
	use			excludes		excludes	excludes	excludes	excludes	excludes	excludes	excludes sojourn	excludes sojourn		induces	
Threat scenario	potential offender				has						allows		is located in			
	intention of offender				correlates with					[illegible] through						
	tool/ weapon						allows		suitable for	suitable for	allows					
	use of tool/ weapon									suitable for	allows			suitable for		
	approach of offender								allows		allows	leads to				
	insertion of tool/ weapon										allows					
	target									correlates with				is located		
	threat															
Airport layout	depature zone															
	endzone															
	attack zone															
	security activity							can impede	can counteract							
	security technology					can detect										

Figure 3: Left: Dependencies on domain level (MDM); Right: Dependencies on element level (DSM/DMM)

Once the dependencies on the MDM level are specified the definition of the mutual dependencies on element level can be pursued further. However, connections between elements are now only specified if their respective domains are logically interlinked. Interdependence between two elements is indicated by a “1”, while “0” indicates no linkage. During workshops with different airport security experts the relationship of each relevant element pair was discussed and rated. Two different matrix areas exist on element level: the Domain Mapping Matrices (DMM) specify intra-domain dependencies and the Design Structure Matrices (DSM) connect elements within one domain, thus comprising the same elements in identical order on both axes (Steward, 1981; Danilovic and Browning, 2007).

This second phase results in the generation of a MDM matrix on domain level and the DSM/DMM matrix on element level (see Figure 2, Building of Model). Furthermore, based on these dependencies, different system components could be specified and documented (see Figure 2, Generation of Information). In Figure 2 a box labelled “Constraint Modelling” is placed across phases two and three. In phase two this indicates the reduction of possible element combinations: elements which show no connection (indicated by a “0” in the DMM/DSM) can not be part of the same threat scenario.

3.3 Introduction of Logical Constraints

In the third phase possible element combinations are narrowed down further through the introduction of logical operators and of further constraints. A first step towards the generation of valid scenario sequences is to define the order in which the scenario elements are specified (see Figure 2, Generation of Information). This is an important step to avoid circular reasoning in the assembly phase of a scenario. For example, if element *a* from domain *1* is specified before element *x* from domain *2* but domain *2* affects domain *1* (e.g. narrowing down the possible choice of elements) no definite choice can be made. To avoid these feedback loops a method named triangularization can be applied: Rows and columns of a MDM are reordered aiming at the grouping of all existing dependencies on one side of the diagonal (Browning, 2001). If not all filled matrix cells can be moved above the diagonal, this indicates the existence of a feedback loop. The MDM in Figure 3 visualises this step: All areas that have to be specified during the scenario building process (Use Case, threat scenario and path through airport) are located above the diagonal. Cells defining the security measures applied are located beneath as they are assumed to counteract components of the scenario.

The MDM approach is limited to the description of the relationship of exactly two elements. Maurer has named this limitation the “2-tupel constraint” (Maurer et al., 2009). Nevertheless, for the compilation of threat scenarios it is sometimes necessary to make sure that more than two elements are logically consistent. For example, elements from the following domains have to be consistent to allow a valid threat: “Potential Offender”, “Tool/Weapon”, “Use of Tool/Weapon”, “Approach of Offender” and “Insertion of Tool/Weapon”. These domains have been assigned the logical operator AND.

The last step before a logically consistent sequence of elements can be derived takes special cases into account that are not fully covered by the data assembled so far. Even after conducting all steps described above, some incongruous combinations could still be chosen to form a scenario. Thus, further rules had to be defined complementing the principles already documented. The following example gives an impression of the complexity of these implemented rules (see Figure 4): A certain security technology can only detect a tool/weapon if it (e.g. a knife) is inserted into the secured area in a way (e.g. hidden underneath the clothes) that a security activity (e.g. body control) employing a certain security technology (e.g. walk-through metal detector) can identify the relevant threat aspect (e.g. technical capability of metal detector to identify metal objects hidden underneath the clothes).

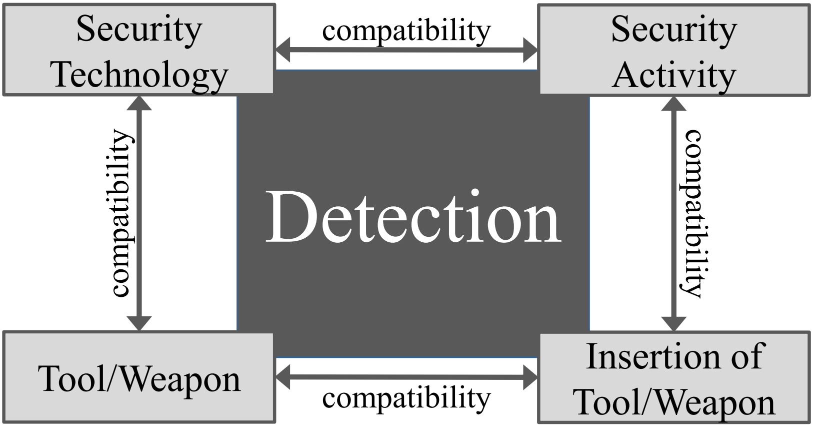


Figure 4: Definition of rules avoiding incongruous element combinations

The introduction of logical operators as well as further constraint mechanisms (see Figure 2, Building of Model) to be able to generate valid sequences of elements (see Figure 2, Generation of Information) was the main goal of phase three. With this step, the basic development phase of the approach was completed. The following steps focus on the generation of threat scenarios and the systematic analysis of related security measures.

3.4 Creation of Scenarios and Clusters

In phase four elements forming a consistent scenario are finally selected. To that end, a software tool, the Scenario Builder, has been developed. Because of the vast amount of elements constituting the airport security system and the many constraints adding to the complexity, assembling a consistent scenario is a very complex task in itself. To support this task the Scenario Builder, a software tool drawing on the assembled data base, guides the user through the process of element assembly, consecutively offering elements from the domains to choose from. The order in which the domains are presented follows the sequence defined in phase three. After one or more elements are chosen from a domain the Scenario Builder moves to the next domain but now only offers elements that are consistent with the previously defined elements. In this manner one domain after the other is specified until a complete, consistent scenario is assembled. The tool allows developing scenarios in an intuitive manner, encouraging the user to try out new combinations of elements.

The Scenario Builder can also be used to create scenario clusters. They consist of different scenarios that are identical in some aspects and differ in others and, thus, represent a certain type of threat but demonstrate possible variations. They can be created by leaving one or more domains unspecified during the process. The builder then automatically creates every possible variation. If two to three domains are left unspecified the resulting scenario cluster can easily comprise 70,000 or more scenarios.

The result of this fourth phase is the implementation of a tool that facilitates the interaction with the data base (see Figure 2, Building of Model) as well as the subsequent construction of structurally consistent scenarios and scenario clusters (see Figure 2, Generation of Information). The actual creation of scenarios is the first step towards the application of the developed model (see Figure 2, Application). Whereas the amount of gathered information continually grows during the first three phases, represented by the broadening boxes (see Figure 2, Generation of Information), phase four decreases the complexity of information to be dealt with in the application phase significantly. This is indicated by the tapering shape of the box.

3.5 Analysis of Scenarios and Clusters

Once every domain is specified and a scenario is created, the Scenario Builder automatically derives the related security measures (activities as well as technologies) that counteract or detect specific elements. This is represented by phase five in Figure 2 (Application). This step proceeds automatically and is the key for the overall approach as the link between the threat scenario and related measures finally becomes visible to the user.

In phase six the scenarios and clusters created during the previous phases are analysed (see Figure 2, Application). Because the amount of scenarios within a cluster can be rather high, methods for a systematic analysis have to be developed. Generally, it is the aim of this phase to identify weaknesses in a security system and to derive improvement strategies. If a set of scenario clusters is specified, a meta-analysis can be conducted, drawing on a range of different types of attacks on the airport security system and the measures triggered by them. Such an approach allows a more generalized statement on the performance of a security system in the light of future threats. A detailed account of strategies to analyse the resulting data has been published by Cole and Maurer (2011).

In the following section the application of the knowledge created in the scenario building process for responsible decision makers is discussed further.

4. Application of the Approach in the Context of Decision Making

Decision making in a complex system comprises all elements of a complex situation. They are characterized by manifold interlinked variables that develop without interference of an actor. The situation is, at least in some areas, intransparent and new to the decision maker. Additionally, goals need to be achieved simultaneously and are often somewhat vague (Schaub, 1996). Furthermore, the network structure leads to cascading effects. A minor mistake in one part of the system can lead to a disaster in other parts, spreading along the underlying links between variables and system areas (Helbing and Lämmer, 2008). A cascading effect potentially leading to a disastrous outcome could be triggered, for example, by security personnel not recognizing a knife smuggled into the secured area. All of these criteria can be transferred to the airport security system described above. Figure 3 and 4 demonstrate the interrelatedness of different components of the system.

The inability to make a decision can be based on insufficient knowledge about possible consequences while the fear of potential failures can lead to different avoidance strategies. Brehmer identifies two groups of these 'pathologies of decision making' (Brehmer, 1992): The first group comprises failures of target specification: 'Thematic vagabonding' describes a tendency to quickly shift targets without solving the problems tackled, while 'encystment' means to stick to a goal one feels comfortable with. The second group includes three different ways of refusal to learn from experience: The general refusal to make any decision is one element in this category. The second pathology is the tendency to blame others for own failures. The latter relates to the delegation of tasks. This includes delegating tasks one should not delegate as well as not delegating tasks that should be delegated. Another very basic mistake people tend to make when dealing with complex systems is that they “are not interested in finding out the existent trends and developmental tendencies at first, but are interested instead in the ‘status quo’” (Dörner, 1980).

A main reason for the development of the approach described in this paper is to enable decision makers to interactively deal with the dependencies between possible future threats and airport security measures. The scenario builder offers a possibility to develop a broad range of scenarios or clusters, to be inspired by the different element choices offered for each domain and to experiment with minor or major variations of scenarios as well as security measures.

A concrete example for such a variation is presented in the following paragraph. The aim of this example is to analyse how changes in the placement of security measures affect a specific category of scenarios. A rather straightforward scenario cluster could consist, for example, of a terrorist trying to attack people in the publicly accessible area of an airport by means of guns and grenades (a comparable attack took place in 1985 simultaneously in Vienna-Schwechat and Rome-Fiumicino). In the current layout such an attack would be addressed by patrol and intelligence service. To analyse a different layout, the database feeding into the Scenario Builder can be adapted to reflect the relocation of a specific security activity. For example, the security activity “body control” could be moved from the security checkpoint to the entrance of the airport. The screening could be conducted by using a walk-though metal detector and regular pat-down searches. This relocation would have a large effect on the groups of people having to undergo such a security check. In the “old” structure only people holding a valid plane ticket and employees working in the secured area of an airport had to undergo security checks, in such a “new” system everybody entering the airport building (meeters and greeters, people simply shopping at the airport etc.) would be screened. Scenarios in which an attacker planned a rampage in the public area of an airport would now be addressed by more security measures than just patrol and intelligence service. This historically inspired scenario as well as the rather simple change to the security system have been chosen deliberately as the presented example should not allude to possible weaknesses of today's security system. Of course, this procedure can be repeated with a broad range of scenarios or scenario clusters, any component of the security system and different security layouts.

Through the interaction with the Scenario Builder systemic structures of the security system can be better understood and the experiential basis – a fundamental to decision making – broadened. Effects of decisions made today can reach far into the future. If future developments are anticipated, actions can be aligned accordingly by letting the future become effective in the present (Willke, 2009). This is a very important prerequisite for robust decisions and to develop future-proof strategies.

5. Summary and Conclusion

In this paper an approach has been described that aims at identifying possible future threat scenarios and their relationship to airport security measures. To this end, threat elements and components of the security system were collected. The elements as well as structural principles underlying the system were documented following the Multiple-Domain Matrix method, a matrix-based approach to complexity management. It was complemented by insights from the field of scenario planning to account for future-oriented research questions. The paper outlines the various steps that lead from an initial involvement with the airport security system, to the development of the so-called scenario builder and, finally, to a broad data basis supporting proactive decision making. Furthermore, the application of the knowledge gained throughout the scenario building process has been discussed.

In the introduction it was mentioned that the Flightpath 2050 vision of the European Commission envisages a risk-based approach to airport security to be developed during the next decades. The method presented in this paper is a first step in this direction. However, a shortcoming in this term is that there is currently no possibility to rank threat scenarios or clusters according to their potential impact on human, financial or infrastructural losses. A major challenge for future research will thus be to link risk parameters to certain elements of the airport security system and to specify probable effects of a broad range of incidents on the overall system. This kind of information would provide an even better possibility for decision makers to gain insights into the system's structural principles and likely consequences of decisions taken.

Acknowledgements

The author would like to thank Dr Maik Maurer for fruitful discussions and valuable input, particularly concerning Figure 2. Dr John d'Avanzo and Dr Dirk Dickmanns provided interesting insights in the procedure of risk allocation. Furthermore, anonymous reviewers provided helpful comments on the draft version of this paper.

References

Baum, P., 2011. 80 Years of AVSEC: from Arequipa to Domodedovo. Aviat. Sec. Int. 17(1), 1.

Brehmer, B. 1992. Dynamic decision making: Human Control of Complex Systems. Acta Psychol. 81(3), 211-241.

Brehmer, B., Dörner, D., 1993. Experiments With Computer-Simulated Microworlds: Escaping Both the Narrow Straits of the Laboratory and the Deep Blue Sea of the Field Study. Comput. in Hum. Behav. 9, 171-184.

Browning, T.R., 2001. Applying the Design Structure Matrix to System Decomposition and Integration Problems: A Review and New Directions. IEEE Trans. Eng. Manag. 48, 292–306.

Cole, M., Kuhlmann, A., 2012. A Scenario-Based Approach to Airport Security. Futur. 44(4), 319-327.

Cole, M., Maurer, M., 2011. Sensitivity Analysis for a Future-Oriented Optimization of Airport Security. 15th Air Transp. Res. Soc. World Conf., Sydney, Australia.

Danilovic, M., Browning, T., 2007. Managing Complex Product Development Projects with Design Structure Matrices and Domain Mapping Matrices. Int. J. Proj. Manag. 25, 300-314.

Dörner, D., 1980. On the Difficulties People Have in Dealing With Complexity. Simul. & Games, 11(1), 87-106.

Dörner, D., Kreuzig, H.W., Reither, F., Stäudel, T. (Eds.), (1983). Lohhausen. Vom Umgang mit Unbestimmtheit und Komplexität, Verlag Hans Huber, Bern.

Eppinger, S.D., Browning, T.R., 2012. Design Structure Matrix Methods and Applications, MIT Press, Cambridge.

European Union, 2011. Flightpath 2050: Europe's Vision for Aviation, Maintaining Global Leadership & Serving Society's Needs, Report of the High Level Group on Aviation Research. URL [http://ec.europa.eu/transport/modes/air/doc/flightpath2050.pdf], (accessed 03.04.2013).

Godet, M., 2000. The Art of Scenarios and Strategic Planning: Tools and Pitfalls, Tech. Forecast. and Soc. Chang. 65(1), 3-22.

Gordon, T.J., Glenn, J.C., 2009. Futures Research Methodology. Version 3.0, UNU Millenium Project.

Helbing, D., Lämmer, S., 2008. Managing Complexity: An Introduction, in: Helbing, D. (Ed.), Managing Complexity: Insights, Concepts, Applications, Springer, Berlin & Heidelberg. pp. 1-16.

IATA, 2012. Fact Sheet: Security, URL (accessed 05.04.2013.): [http://www.iata.org/pressroom/facts_figures/fact_sheets/pages/security.aspx.]

Jouvenel, H. de, 2000. A Brief Methodological Guide to Scenario Building. Tech. Forecast. and Soc. Chang. 65(1), 37-48.

Kirschenbaum, A., Rapaport, C., Lubasz, S., Mariani, M., van Gulijk, C., Andriessen, H., 2012a. Security profiling of airport employees: Complying with the rules. J. Airpt. Manag. 6(4), 373-380.

Kirschenbaum, A., Mariani, M., van Gulijk, C., Rapaport, C., Lubasz, S., 2012b. Airports at risk: the impact of information sources on security decisions. J. Transp. Sec. 5(3), 187-197.

Lindemann, U., Maurer, M., Braun, T., 2009. Structural Complexity Management – An Approach for the Field of Product Design, Springer, Berlin.

Luhmann, N., 2009. Zur Komplexität von Entscheidungssituationen. Soz. Syst. 15(1), 3-35.

Maani, K.E., Maharaj,V., 2004. Links between systems thinking and complex decision making. Syst. Dyn. Rev., 20(1), 21-48.

Maurer, M., Biedermann, W., Kuhlmann, A., Braun, T., 2009. The 2-Tupel-Constraint and How to Overcome It. Proc. of the 11th Int. DSM Conf., Greenville, USA.

Schaub, H., 1996. "Exception error": Über Fehler und deren Ursachen beim Handeln in Unbestimmtheit und Komplexität. gdi impuls. 14(4):3-16.

Steward, D., 1981. The Design Structure System: A Method for Managing the Design of Complex Systems. IEEE Transact. Eng. Manag. 28(3), 79-83.

Sweet, K.M., 2009. Aviation and Airport Security – Terrorism and Safety Concerns, CRC Press, Boca Raton.

Willke, H., 2009. Zur Komplexität der Entscheidungstheorie. Soz. Syst. 15(1), 62-72.

6.2.3 Publication Number 3: Cole and Maurer (2014)

Cole, M. and Maurer, M. (2014). Handling Complex Socio-Technical Systems: A Method for Proactive Optimization of Airport Security. In: International Journal of Knowledge-Based and Intelligent Engineering Systems, 18:191-200.

HANDLING COMPLEX SOCIO-TECHNICAL SYSTEMS: A METHOD FOR PROACTIVE OPTIMIZATION OF AIRPORT SECURITY[1]

Abstract

The purpose of security checks at airports is to achieve a reduction in the risk of malevolent attacks on the aviation system. The introduction of new security measures aims at reducing this perceived level of risk, and often takes place as a direct reaction to (attempted) attacks. This procedure means that offenders remain one step ahead of security agents. The aim of the approach presented here is to overcome this shortfall by supporting decision-making in the context of airport security by a systematically created knowledge base. The combination of two well-accepted methods – scenario analysis and structural complexity management – supports a structured knowledge acquisition process that serves as a basis for the proactive identification of system weaknesses. Furthermore, this combination of methods can be applied to the search for optimisation potentials concerned with possible future threats. The basis for the approach is composed of threat scenario components, security measures and dependencies between these elements. A Multiple-Domain Matrix is applied for system modelling. Clustering of threat

[1] The results presented in this paper are based on research conducted in the course of the project SiVe, which was partially financed by the German Federal Ministry of Education and Research (BMBF). SiVe was part of the Security Research Program initiated in the context of the High-Tech Strategy by the German Federal Government.

scenarios and intensity of relations to security measures are used for analysis. The interpretation of findings makes use of portfolio representations.

1. Introduction

1.1 Initial Situation: Aviation as a Preferred Target for Attacks

The first attacks on aviation security took place in the 1930s and ended non-fatal as most of them were hijackings conducted by people seeking political asylum [33]. Since then the threat originating from such attacks has been constantly evolving. From the 1960s on, civil aviation has been an attractive target for terrorists. One of the many reasons is that aircraft, especially so-called flag carriers, as well as airports are highly symbolic targets and physically vulnerable [29]. In the 1960s and 1970s, hijacking was the most common threat pattern, predominantly designed to make political statements. Between 1970 and 1990, the focus shifted to bombings: almost 50 bombs were successfully placed on aircraft during this period [7]. The 9/11 attacks demonstrated a completely different approach carried out by a group of people equipped with rather simple weapons but misusing the aircraft itself as a weapon of mass destruction [1]. Since 2001 a widespread exploitation of weaknesses in the security chain has taken place (e.g. shoe bombs, underwear bombs, printer toner bombs).

1.2 Problem: Reactive Implementation of Security Measures

Security measures are invented and implemented for preventing attacks on the aviation system. These days attackers have to pass through many layers of security technologies and processes in order to reach an aircraft and consequently attract maximum attention. The first attempt to counter these threats took place in 1968 when walk-through metal detectors and cabin baggage X-rays were introduced. They were installed as a reaction to an incident on an EL AL flight from Rome to Tel Aviv. Terrorists hijacked the aeroplane and redirected it to Algiers [7]. From this event onwards, layer after layer of security technologies and processes have been introduced, mostly as direct reactions to security incidents [26; 28; 31; 32].

A prominent example of the reactive implementation procedure is the 2001 shoe bombing incident conducted by Richard Reid. He unsuccessfully attacked an American Airlines flight on its way from Paris to Miami with explosive devices hidden in his shoes, and thus below the height of the area scanned by a standard walk-through metal detector. As an immediate result, all passengers had to take off their shoes during passenger screenings so that these could be X-rayed together with the hand luggage. This measure can still be part of the process today.

The incident described above shows how terrorists have been taking advantage of (perceived) weaknesses of the security technologies and processes. They plan their attacks intelligently and conduct them, employing innovative means [4]. Baum draws the conclusion that “the best lesson the past has taught us is that the next time it will be different” [1, p.1]. The reactive implementation procedure of security measures consequently allows the attackers to remain one step ahead of security measures. An anticipatory approach is needed to prepare decision makers responsible for airport security in the best possible way to not only deal with known attacks but also with innovative threats. Therefore, a knowledge-based approach is required, which aims at improving overall security instead of counteracting single risks.

1.3 Objective: An Anticipatory System Approach to Airport Security

The objective of the approach presented here is to provide a basis for decision-making in the field of airport security. The relevance, effectiveness and intensity of these security measures all need to be assessed and should serve as a basis for continuous system improvement. Through this kind of knowledge security agencies, for example, or airport operators can be supported in their daily decision-making process. To this end, structural complexity management methods are combined with scenario planning methods.

The paper is structured as follows: In Section 2, a literature overview shows the state of the art in structural complexity management and research in scenario analysis. A detailed description of the information acquisition process for the approach developed is provided. Subsequently, the performance analysis of specific measures in relation to single threat scenarios or groups of threat scenarios by means of the application-impact diagram is introduced. The application of the approach is demonstrated in Section 3. Here, results of a particular scenario group assessment are shown and interpreted with the help of the application-impact-diagram. Section 4 summarises the findings and provides an outlook on future work.

2. Methodological Approach

The following paragraphs present the state of the art in system structure modelling and analysis using matrix-based approaches as well as in scenario analysis. Thereafter, the methodological approach is described in detail.

2.1 Literature Review and State of the Art

Optimization of airport security requires an adequate system model description. The topic implies that quantified information is hardly available. This results from the number of stakeholders involved, split responsibilities, reasons for non-disclosure and generally vague information about potential attackers, their methods and tools. In this approach, quantitative modelling is applied, i.e. it is focused on system elements, their dependences and the resulting system structure. Consequently, specific characteristics (such as strength, amount), which would result in a detailed quantitative model, are not acquired.

The objective of the approach described in this paper is the identification of threat scenarios consisting of assembled system elements. Furthermore, security measures will be linked to these scenarios. To this end, a method known as Multiple-Domain Matrix (MDM) [19; 5] is applied. This matrix-based method is designed for systematic acquisition of system elements and their mutual dependences as well as for analysis and interpretation of the resulting system structures. An MDM integrates different groups of elements (called domains) and is composed of Design Structure Matrices (DSM) and Domain Mapping Matrices (DMM).

DSM (as part of the MDM method) was introduced in 1981 [30]. It is a square matrix representing elements and links between them. The matrix layout allows application of analysis algorithms by the switching of matrix rows and columns [18]. The DSM is applied for visual system analysis, because system structures such as hierarchies, clusters and feedback loops form characteristic constellations. The DMM enhances the DSM by linking elements of two domains instead of those of one domain only [3].

Eppinger and Browning make mention of the fact that an MDM can be useful for modelling “system of systems” models [5, p.240]. They note that “[a]nalysis techniques for the MDM are still being contemplated and developed”. Whereas the sub-matrices can be handled with established approaches, one enhancement of the MDM is the possibility to derive indirect system dependences [20].

Several applications of MDM have been implemented [5]. Hellenbrand et al. [11], Koga et al. [14] and Kreimeyer [17] show the identification of indirect system links for creation of specific system views. These views serve as a basis for analysis and interpretation. Despite these beneficial applications, holistic system analysis by MDM has not been documented so far. Furthermore, it must be mentioned that an MDM (as well as DSM and DMM) only allows modelling dependences between element pairs [23]. Attempts to integrate logic operators to matrices (and thus combine more than two elements) have been documented, but they hinder conduction of established system analyses [17; 21].

MDM is useful for modelling the structure of large systems and represents a new approach to proactive analysis in the field of aviation security. As matrix-based system representations are limited to interdependence between element pairs only, further development of the method is required to enable scenario modelling. Therefore, documentation of dependence among numerous elements is necessary (e.g. A and B are linked, if C exists). The need for creating scenarios for a proactive approach to airport security can be explained by the following example: Risk is an important evaluation parameter in airport security, but it cannot be specified for single threat elements, e.g. a knife. However, the combination of certain threat elements, e.g. a knife used by a person with a malevolent intention on an aeroplane, can lead to a risk incident. Thus, only the combination of system elements (as described in a scenario) can be related to a specific risk.

The scenario technique is a method applied in future oriented research since it facilitates dealing with uncertainty in future developments. A scenario offers insights into the underlying drivers of change and provides a range of possible futures. Godet [8, p.8] highlights the usefulness of scenarios as they “stimulate the imagination, reduce inconsistencies, create a common language, structure collective thought, and enable appropriation by decision makers”.

The standard scenario process, as described by Jouvenel [13], comprises five consecutive phases: First, the problem is defined and system borders are specified (1). The influencing key variables are then identified (2). The gathering of relevant data and an assessment of the interrelations between the system components comprise the next phase (3). A cross-impact analysis [9] is generally employed to document the relations between the gathered components. Possible futures can be explored through valid combinations of system elements (4). The specified scenarios can then be used as a basis when outlining strategies to cope with possible future developments (5).

Some authors have described risk based approaches for critical infrastructure protection [10] and aviation security policy [26]. Provitolo [27] applied Systems Dynamics to analyse risk and catastrophe systems. An interesting approach is, furthermore, presented by Jiminez et al. [12]: He suggests a proactive risk management based on the weighting of a large number of scenarios through a morphological approach followed by an in-depth analysis of the implications of the results. Ong et al. [24] have demonstrated how possible future failures of aero-engines can be detected on the basis of knowledge-based analysis and how subsequent aircraft downtime can be prevented.

Drawbacks of the standard scenario approach are, however, the difficulty of handling large numbers of key variables due to the resulting vast amount of possible valid combinations as well as the limitation of the outcome to only a small number of plausible scenarios. However, an airport has to stand up to a potentially large variety of threats and its system structures have to be analysed in great detail. The approach presented in this paper allows us to bridge this gap by combining ideas from scenario planning with the MDM methodology and, hence, to exploit the advantages of both approaches.

The application of this combination of methods can provide a high number of standardized scenarios which show relations between system elements on a very detailed level. The editing and interpretation of resulting data, however, as well as an easily accessible depiction pose new challenges. This paper proposes a procedure for analysis of data and interpretation of depicted of results. It supports decision-makers in gaining new insights into aviation security and possible future threat situations.

2.2 Capturing System Components

The approach presented here consists of three main steps (Figure 1). First, system elements and dependences must be captured and transferred to the model and, therefrom, valid threat scenarios are created

(Section 2.2). Secondly, different types of related security measures are derived (Section 2.3). In the third main step a diagram is developed for analysing and interpreting the usefulness of specific security measures against specific threat scenarios.

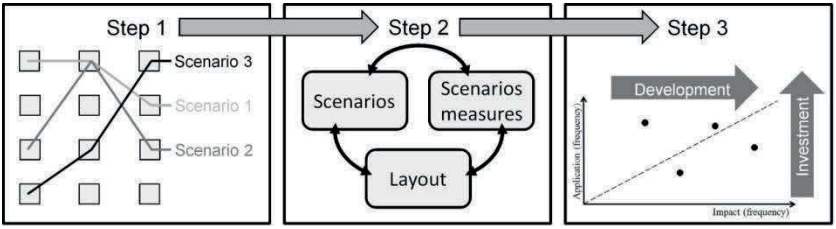
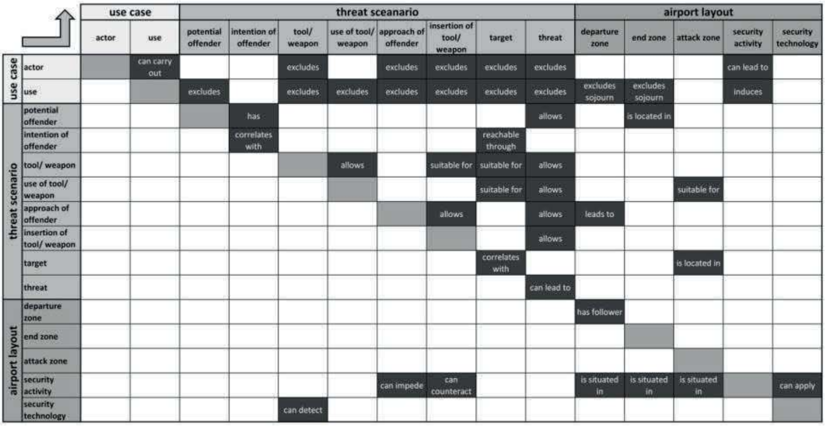


Figure 1: Main steps of approach

2.2.1 Capturing relevant elements and their interdependences

The first step when approaching a new system is to gather all kinds of elements that constitute the system and define its borders. The number of elements in the study totals about 200. These elements are split into 18 domains. The system structure comprises, on the one hand, domains that form a threat scenario such as “potential offender” or “tool/weapon”. On the other hand, the system structure comprises domains that represent the airport security measures (”security activity” and “security technology”) as well as the airport layout (e.g. “departure zone”). An MDM was set up with the domains serving as row and as column headings to determine the interrelation of these parts. The different types of relations were then specified (Figure 2). Cells that are blank indicate that the domains are independent of each other in the presented system view[2].

[2] See also [2] for a description of the procedure from a scenario planning perspective.



		use case		threat sceanario								airport layout				
		actor	use	potential offender	intention of offender	tool/ weapon	use of tool/ weapon	approach of offender	insertion of tool/ weapon	target	threat	departure zone	end zone	attack zone	security activity	security technology
use case	actor		can carry out			excludes		excludes	excludes	excludes	excludes				can lead to	
	use			excludes		excludes	excludes	excludes	excludes	excludes	excludes	excludes sojourn	excludes sojourn		induces	
threat scenario	potential offender				has						allows		is located in			
	intention of offender				correlates with					reachable through						
	tool/ weapon						allows		suitable for	suitable for	allows					
	use of tool/ weapon									suitable for	allows			suitable for		
	approach of offender								allows		allows	leads to				
	insertion of tool/ weapon										allows					
	target									correlates with				is located in		
	threat										can lead to					
airport layout	departure zone											has follower				
	end zone															
	attack zone															
	security activity							can impede	can counteract			is situated in	is situated in	is situated in		can apply
	security technology					can detect										

Figure 2: Multiple-Domain Matrix comprising domains and their respective relations (adapted from [22])

When the domains of the airport security system and their general relations have been defined, the focus is placed on the element level in the next phase. Each domain consists of several elements. If their respective domains are interlinked, some elements in this sub-matrix will possess dependences. The domain “tool/weapon” includes, for example, the element “improvised explosive devices” and the domain “threat” the element “hijacking of aeroplane”. These two domains are linked by the relation “allows”. Some tools or weapons will allow hijacking of an airplane. The dependences between system elements were acquired from experts in workshops. All relevant relations on the element level were specified either by “1” (existing relation) or by “0” (no relation). This procedure systematically evaluates the dependences between system elements that could either be part of the same threat scenario or, in the case of airport security elements, could impede the threat.

2.2.2 Compilation of valid threat scenarios and scenario clusters

Two necessary conditions have to be met to form a valid scenario: At least one element from each threat-related domain has to be chosen and these elements must be consistent according to the expert knowledge documented in the MDM. This extraction of scenarios is not supported by conventional MDM approaches, as only dependences between pairs of system elements can be modelled in such matrices. To facilitate the scenario-building process, a software tool has been developed that uses the MDM as input and guides the user through the scenario-building process. This “Scenario Builder” presents to the user elements from one domain after another to choose from. To this end, logic operators have been defined as connectors between the subsets of the MDM. The Scenario Builder then only lists elements that are consistent with the already chosen scenario parts to make sure that only matching elements are selected. The sequence in which the elements are offered was carefully deduced from the matrix structure to avoid circular reasoning [21].

The process of scenario building can be automatised: If only a few domains are specified by the user, the Scenario Builder generates all scenarios that can be formed on the basis of the preselection. Accordingly, the resulting so-called scenario clusters comprise only scenarios that show certain ex ante defined qualities. The fewer the elements that are specified beforehand the bigger the cluster. For example, if one would only specify the domains “potential offender” (e.g. terrorist), “tool/ weapon” (e.g. improvised explosive device) and the “threat” (e.g. hijacking of aeroplane) the Scenario Builder would automatically search for all possible combinations of scenario elements consistent with that choice. If the automatised scenario-building process is run through with no preselected elements, all structurally consistent scenarios are produced purely through permutation. The Scenario Builder, thus, provides an interface through which one can access the stored knowledge [15] without oversimplifying the complex structure of the airport security system [25].

2.3 Threat-Related Assessment of Security Measures

After a threat scenario is computed, the Scenario Builder automatically lists all related security measures (security activities and technologies). This information is taken from the MDM, where the impact of security measures on threat elements is modelled. There are two different types of security measures deduced in two different ways: pass-through measures and potentially effective measures.

The first two domains that influence the pass-through measures are "actor" and "use". They indicate what kind of disguise a potential offender displays: whether somebody pretends to be a meeter and greeter or to go on a long distance flight, fundamentally affects what kind of security activities he will have to face at the airport and which areas he is subsequently granted access to (arrow labelled "case-related" in Figure 3, part A). The scenario-specific measures are further narrowed down by the path the potential offender pursues through the airport. Different security activities are conducted either within particular areas of the airport (e.g. patrols in the publicly accessible area) or at the transition from one area to another (e.g. hand luggage checks on the border from the publicly accessible area to the departure area). The three domains "departure zone", "end zone" and "attack zone" describe the different areas an offender passes through in order to reach his final position (arrow labelled "path-related" in Figure 3, part A).

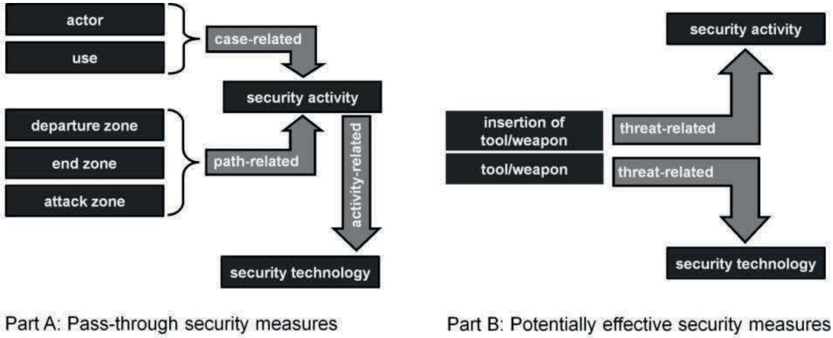


Figure 3: Two means of deducing scenario-oriented security activities and technologies

Which security activities have to be conducted at what point in the airport is specified by the regulator (e.g. Regulation (EC) No 300/2008 [6]). However, which security technologies are used to fulfil the required activities can differ between airports. For example, the follow-up check after the metal detector produced an alarm can either be conducted by means of a hand-held metal detector, a pat-down search or both. Thus, the security technologies which could be applied during the security activities must be specified (arrow labelled “activity-related” in Figure 3, part A). Finally, users assemble structurally consistent scenarios or scenario clusters and automatically derive related security measures with which an offender is confronted on his particular way through the airport.

Potentially effective security activities relate to the specific threat scenario based on the tool or weapon employed in a scenario and the way it is transported and possibly inserted into secured areas of the airport. Certain security activities can counteract specific ways of inserting a tool or weapon. For example, the fact that passengers have to pass through body control in the course of passenger screening is supposed to impede the insertion of a weapon hidden on the body into the secured area. Thus, security activities can at least complicate different ways of inserting a tool or weapon (arrow linking “insertion of tool/weapon” and “security activity” in Figure 3, part B).

The theoretical detection capability of a security technology does not depend on whether or not it is employed in a security activity conducted in the specific scenario (cluster). Security technologies have varying capabilities, e.g. a walk-through metal detector exclusively detects metal, whereas new-generation body scanners recognise different kinds of objects on the skin surface. Nevertheless, they could replace one another in the same security activity. If an explosives belt without a metal fuse is hidden underneath the clothing, a metal detector would not set off an alarm but the chances are that a body scanner would. This relation is displayed by the arrow linking “tool/weapon” and “security technology” in Figure 3, part B.

2.4 The Application-Impact-Diagram

Security activities and technologies that are applied in response to a specific scenario (cluster) do not necessarily address the relevant threat elements. Furthermore, security activities and technologies that have the potential to render the specific threat harmless are not necessarily applied. To make this relation more transparent the application-impact-diagram (Figure 4) was developed, setting these two aspects into relation. The description of extreme cases below lists the implications that can be drawn from the diagram:

- Position in the lower left corner of the diagram: Security measure is not applied and not effective, it is not relevant for the scenario cluster considered.
- Position in the upper left corner of the diagram: Security measure is applied but not effective, the application of the measure wastes resources (of airport security staff as well as passengers) in the context of the specific cluster; further technical development of the measure could improve the effectiveness, the position of the security measure would then move to the right.
- Position in the lower right corner of the diagram: Security measure is not applied but would be effective, e.g. for reasons of high procurement costs a measure is not applied. Investment could improve the impact against considered threat scenarios, the position of the security measure would then move upwards in the diagram.
- Position in the upper right corner of the diagram: Security measure is at the same time applied and effective.

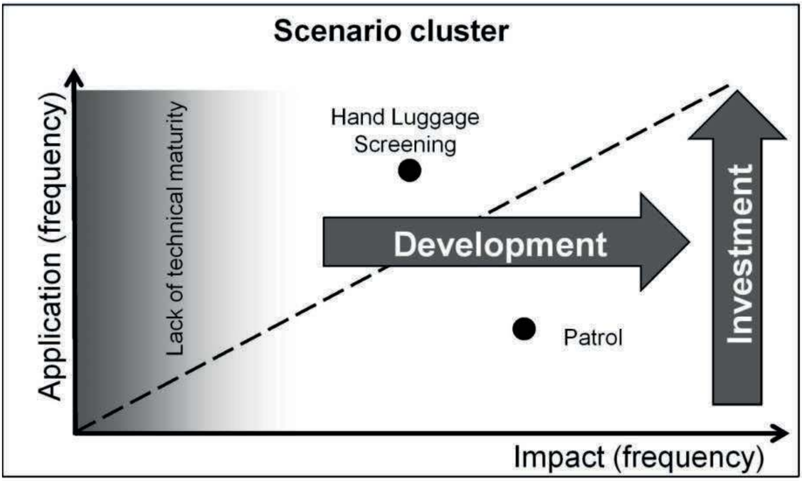


Figure 4: Application-impact-diagram

The highest efficiency regarding a particular scenario (cluster) can be reached if the frequency of application and the frequency of impact are equal. Thus, efficient security measures are located along the diagonal of the diagram. However, it has to be taken into account that both axes represent statistical values. Possible consequences are explained by the following example: If a security measure is effective in 10,000 threat scenarios and also is applied in 10,000 scenarios, it would be located on the diagonal of the diagram. However, if the scenario cluster consists of 20,000 scenarios in total, it is possible that the security measure is only applied against scenarios where it is not effective. This would mean no efficiency at all. Thus, the congruence between application and impact of a security measure must be known in order to rate the efficiency. To this end, one can take a set of random samples (statistical evaluation) or narrow down the scenario cluster. An adequate size of a scenario cluster is reached, if the impact of a security measure can be estimated as being identical for the entire cluster. For example, using a knife in the security area that was hidden underneath the clothing to bypass screening, forms a scenario cluster which is entirely impacted by pat-down search.

Changing impact or application of security measures results in their relocation in the diagram. Movements to the right indicate technical improvement by product development as more scenarios are addressed. Consequently, movements to the left do not normally appear, as this would mean a degradation of impact against scenarios. Vertical movement implies investment changes as the security mechanism is applied to more (or fewer) scenarios.

Figure 4 contains a grey shaded area at the left. Security measures located within this far left area lack a certain technical maturity or they are not well suited for the specific cluster because they only impact a very small number of scenarios within the cluster. Technical improvement could probably move the security measures out of this area.

2.5 Practical Application of the Approach

The following paragraphs show how, for example, security regulators, airport operators or security agencies could apply the approach beneficially. For instance, if a certain type of attack has occurred lately, using specific ways to disguise explosives, security agencies would probably assume a higher risk of similar attempts, since the modus operandi of attacks is often imitated. The following aspects can be highly relevant for decision-makers developing adequate actions:

- How many specific threat scenarios exist based on the use of the specific type of weapon? That means: How many valid scenarios does the scenario cluster contain?
- How well do the security measures protect the airport from threats posed by the scenario cluster considered? That means: Which security measures would theoretically address relevant threat elements and which are the ones applied (to which degree) against the scenario cluster considered?
- Which security measures should be improved and how? That means: Which security measures show the highest potential for

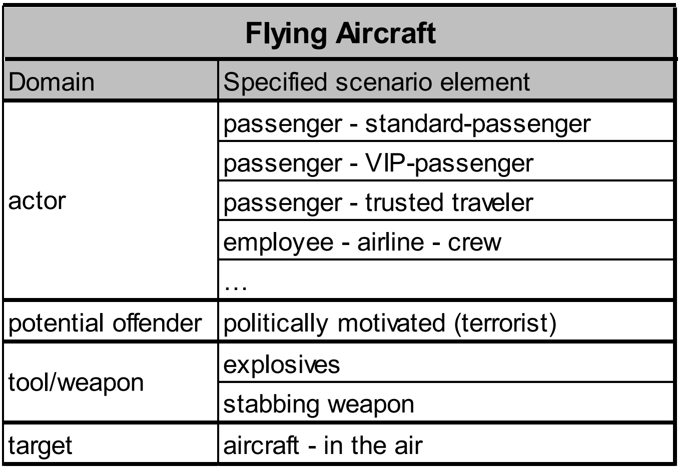
improvement and should they be applied more often or should their effectiveness be improved?

In section 3 these aspects will be discussed in more detail drawing on an example of a scenario cluster and the related application-impact-diagram.

3. Application Example "Flying Aircraft"

Each scenario cluster is specified by a preselection of certain scenario elements. Table I shows an extract of the elements specified for the scenario cluster "Flying Aircraft". Due to the need of non-disclosure some elements are hidden. Elements have been specified in four domains. Elements within the same domain (e.g. in the domain "actor") can be included alternatively in the scenarios (as has been done for two of the four domains). A valid scenario is composed if at least one element from each domain has been specified. The more elements are specified, the smaller the number of scenarios within the cluster.

Table 1: Specification of the scenario cluster "Flying Aircraft"



Flying Aircraft	
Domain	Specified scenario element
actor	passenger - standard-passenger
	passenger - VIP-passenger
	passenger - trusted traveler
	employee - airline - crew
	…
potential offender	politically motivated (terrorist)
tool/weapon	explosives
	stabbing weapon
target	aircraft - in the air

The cluster “Flying Aircraft” consists of scenarios that are all conducted by a terrorist, who tries to attack an aircraft in the air using explosives and a stabbing weapon.

3.1 Application-Impact Diagram for “Flying Aircraft”

The application-impact-diagram for the scenario cluster “Flying Aircraft” is shown in Figure 5. The legend lists some of the security measures considered such as “hand luggage control” or “check-in”. In total the cluster contains 97,416 scenarios based on the specification listed in Table I.

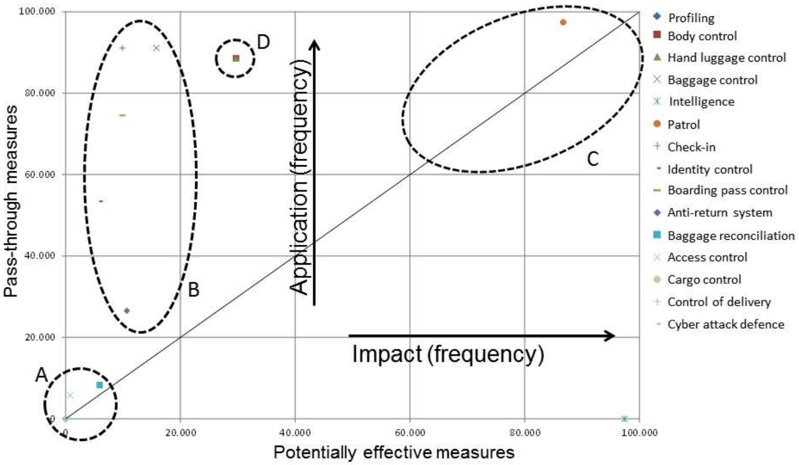


Figure 5: Application-impact-diagram for the scenario cluster “Flying Aircraft”

The positions of security measures in the diagram can be classified into three groups: Five measures (cargo control, control of delivery, baggage reconciliation, access control, cyber-attack defence) are located close to the zero point of the diagram (indicated by “A” in Figure 5). These measures do not address threat elements in this specific cluster and are also not applied. They are not designed for application in this scenario cluster and, therefore, do not need to be considered any further. However, it should be mentioned that these measures could be in more prominent positions if another cluster were to be considered (e.g. containing cargo or cyber threat elements).

Five security measures (baggage control, check-in, identity control, boarding pass control, anti-return system) are located close to the vertical axis (indicated by “B” in Figure 5). These measures are applied against scenarios of the cluster and, thus, require resources. But they only show very little impact. Of course, this statement only holds true with regard to the scenarios considered of the cluster considered. Regarding other scenarios, these measures could possess a high impact and contribute crucially to the overall security level, for example, if someone tried to access the aircraft without a valid ticket.

Two security measures (profiling, patrol) are located in the upper right corner of the diagram (indicated by “C” in Figure 5), which means they are applied to, and at the same time prove to be effective, against the scenarios in the cluster. Here, profiling and patrol are passed-through in all scenarios of the cluster and are potentially effective in almost 90% of the scenarios. Consequently, application and impact of measures must usually occur in the same scenarios and more detailed analyses of the scenario cluster (e.g. consideration of random samples) are not required. If a security measure were passed-through only in 60% of the scenarios within one cluster and the same measure were potentially effective in only 50%, it would be necessary to analyse whether application and effectiveness concern the same scenarios.

In Figure 5, body control and hand luggage control cannot be assigned to any of the before- mentioned areas. These measures must be passed-through in more than 90% of the scenarios in the cluster but are only potentially effective in 30% (indicated by “D” in Figure 5).

As explained in Section 2.5, the distance between the location of a security measure in the diagram and the diagonal is an indicator of the efficiency of this measure. If currently located above the diagonal, the efficiency of a measure would improve if more scenarios of the cluster were impacted. Typically, this would require further (technical) development of the measure. If located below the diagonal, the efficiency of a measure could be improved by its being applied to more scenarios. Typically, this means increasing the investment in application. In Figure 5, body control and hand luggage control are located above the diagonal and, thus, show a potential for technological and/or process-related improvement.

4. Conclusion and future work

In this paper, an approach towards a proactive identification of weak areas within the airport security system is presented which is based on methods drawn from structural complexity management and scenario planning. The model of airport security by MDM allows interaction with an extremely large number of possible threat scenarios. The concept of scenario clusters allows focussing on classes of similar threats, which can be analysed effectively and help answer the specific questions of security agents. The approach presented can support responsible decision-makers by providing insights into the relations within the socio-technical security system. The approach thus supports the preparation of the airport security against innovative threats and means a break with the sole implementation of reactive security measures.

The application-impact diagram has been introduced to visualize the derived potential for improvement of the overall security level. This diagram provides a simple visual link between a threat scenario cluster and security measures. The position of security measures in the diagram supports decision-making with regard to specific threats.

Future work will be based on the ongoing collection of different scenario clusters. These clusters can then be analyzed one by one and later merged to produce one large data base. The larger the variety of different clusters, the greater is the amount of multi-faceted information contained in the data base. Subsequently, this data base will allow the identification of structural weaknesses in the complex system of aviation security. This knowledge can support decision-makers in the identification of areas for proactive improvement and, thus, in improved handling of threats to this complex socio-technical system.

Acknowledgements

The authors would like to thank the participants of the 15th Air Transport Research Society World Conference 2011 (Sydney, Australia) for discussion and input to a preliminary version of this paper.

References

[1] P. Baum, 80 Years of AVSEC: from Arequipa to Domodedovo, Aviation Security International 17 (2011), 1.

[2] M. Cole and A. Kuhlmann, A Scenario-Based Approach to Airport Security, Futures 44 (2012), 319-327.

[3] M. Danilovic and T. Browning, Managing Complex Product Development Projects with Design Structure Matrices and Domain Mapping Matrices, International Journal of Project Management 25 (2007), 300–314.

[4] A. Dolnik, Understanding Terrorist Innovation: Technology, Tactics and Global Trends, Routledge, Abingdon, 2007.

[5] S.D. Eppinger and T.R. Browning, Design Structure Matrix Methods and Applications, MIT Press, Cambridge, 2012.

[6] European Parliament and Council, Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing, 2008,

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008R0300:EN:NOT, accessed 12/14/2012.

[7] T. Feakin, Insecure Skies? Challenges and Options for Change in Civil Aviation, Occasional Paper, Royal United Services Institute, London, 2011.

[8] M. Godet, The art of scenarios and strategic planning: tools and pitfalls, Technological Forecasting and Social Change 65(1) (2000), 3-22.

[9] T.J. Gordon and H. Hayward, Initial experiments with the cross-impact matrix method of forecasting, Futures 1(2) (1968), 100-116.

[10] Y.Y. Haimes and T. Longstaff, The Role of Risk Analysis in the Protection of Critical Infrastructures Against Terrorism, Risk Analysis 22(3) (2002), 439-444.

[11] D. Hellenbrand, H. Fiehl, S. Zirkler, M. Petermann and U. Lindemann, BMW Electric Sunroof, in: Design Structure Matrix Methods and Applications, S.D. Eppinger and T.R. Browning, MIT Press, Cambridge, 2012, pp. 271-276.

[12] H. Jiminez, I.C. Stults and D.N. Mavris, A Morphological Approach for Proactive Risk Management in Civil Aviation Security, Proceedings of 47th AIAA Aerospace Sciences Meeting, 5-8 January 2009, Orlando (FL, USA), vol. 29, 2009, pp. 19125-19136.

[13] H. de Jouvenel, A brief methodological guide to scenario building, Technological Forecasting and Social Change 65(1) (2000), 37-48.

[14] T. Koga, A. Hirao, K. Aoyama and Y. Iwata, 4G Mobile Phon LSI Chip Design. in: Design Structure Matrix Methods and Applications, S.D. Eppinger and T.R. Browning, MIT Press, Cambridge, 2012, pp. 294-299.

[15] P. Krbálek and M. Vacek, Teleology: A modern approach for knowledge mapping, International Journal of Knowledge-based and Intelligent Engineering Systems 17 (2013), 137-144.

[16] M. Kreimeyer, Audi AG Body-in-White Development, in: Design Structure Matrix Methods and Applications, S.D. Eppinger and T.R. Browning, MIT Press, Cambridge, 2012, pp. 300-307.

[17] M. Kreimeyer, S. Braun, M. Gürtler and U. Lindemann, Extending multiple domain matrices to allow for the modeling of Boolean opera-

tors in process models. in: Proceedings of the 17th International Conference on Engineering Design (ICED'09), M. Norell Bergendahl, M. Grimheden, L. Leifer, P. Skogstad and U. Lindemann, eds., vol. 1: Design Processes, pp. 1-12.

[18] A. Kusiak, Engineering Design – Products, Processes and Systems, Academic Press, San Diego, 1999.

[19] U. Lindemann, M. Maurer and T. Braun, Structural Complexity Management: An Approach for the Field of Product Design, Springer, Heidelberg, 2009.

[20] M. Maurer, Structural Awareness in Complex Product Design, Dr. Hut, München, 2007.

[21] M. Maurer, M. Cole, J. d'Avanzo and D. Dickmanns, Airport Security: From Single Threat Aspects to Valid Scenarios and Risk Assessment, Proceedings of 1st Global Conference on Systems and Enterprises, 2-4 December 2009, Washington (USA).

[22] M. Maurer and M. Cole, Airport Security System, in: Design Structure Matrix Methods and Applications, S.D. Eppinger and T.R. Browning, MIT Press, Cambridge, 2012, pp. 288-293.

[23] M. Maurer, M. Strattner, Using Boolean Operators in Multiple-Domain Matrices. 21st Annual INCOSE International Symposium, 20-23 June 2011, Denver (USA).

[24] M. Ong, X. Ren, G. Allan, V. Kadirkamanathan, H.A. Thompson and P.J. Fleming, Decision support system on the grid, International Journal of Knowledge-based and Intelligent Engineering Systems 9 (2005), 315-326.

[25] P.C. Panchariya, A.K. Palit, A.L. Sharma and D. Popovic, Rule extraction, complexity reduction and evolutionary optimization for fuzzy modling, International Journal of Knowledge-based and Intelligent Engineering Systems 8 (2004), 189-203.

[26] R.W. Poole, The Case for Risk-Based Aviation Security Policy, World Customs Journal 3(2) (2009), 3-16.

[27] D. Provitolo, Structural and Dynamic Complexities of Risk and Catastrophe Systems: An Approach by System Dynmics Modelling, in: Proceedings of the European Simulation and Modelling Conference, A. Nketsa, M. Paludetto and C. Bartelle, eds., 2006, p. 430-436.

[28] M.B. Salter, ed., Politics at the Airport, University of Minnesota Press, Minneapolis, 2008a.

[29] M.B. Salter, Imagining Numbers - Risk, Quantification, and Aviation Security, Security Dialogue 39 (2008b), 243-266.

[30] D. Steward, The Design Structure System: A Method for Managing the Design of Complex Systems. IEEE Transaction on Engineering Management 28(3) (1981), 79-83.

[31] K.M. Sweet, Terrorism and Airport Security, Edwin Mellen Press, Lewiston, 2002.

[32] K.M. Sweet, Aviation and Airport Security: Terrorism and Safety Concerns, Auerbach Publications, Boca Raton, 2009.

[33] A.T. Wells, and S.B. Young, Airport Planning & Management, McGraw-Hill, New York, 2004.

6.2.4 Publication Number 4: Maurer and Cole (2012)

Maurer, M. and Cole, M. (2012). Airport Security System. In: Eppinger, S. D. and Browning, T. R. (eds.). Design Structure Matrix Methods and Applications. MIT Press, Cambridge. pp. 288-293.

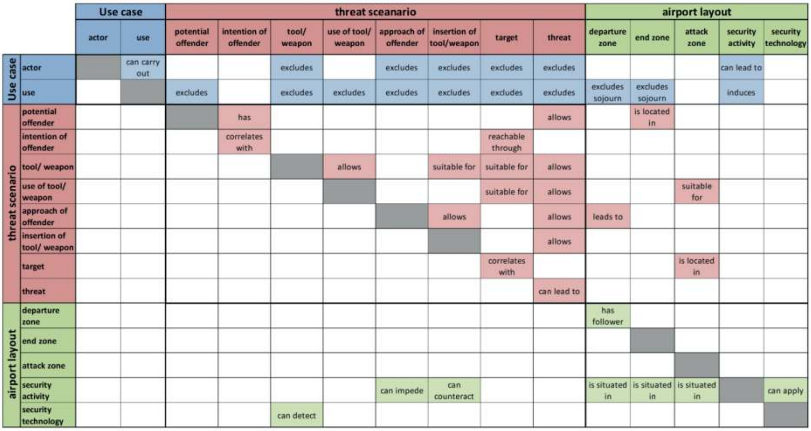
AIRPORT SECURITY SYSTEM

Problem Statement

Civil aviation faces a constant threat from terrorist attacks. The airport functions as a gateway, and installed security checkpoints are meant to reduce the occurrence of attacks. Being able to cope in an efficient way with both potential threats and increasing passenger volume is a highly demanding challenge. To prepare the airport for future threats, one needs to take a systems view in order to thoroughly understand the elements of possible future threat scenarios as well as their interrelation with existing security measures.

Data Collection

Bauhaus Luftfahrt is an international think tank founded by the Bavarian Ministry for Economic Affairs and three aerospace companies, EADS, Liebherr-Aerospace and MTU. Together with Teseon, a software development and consulting company, Bauhaus Luftfahrt constructed an airport security system MDM model containing approximately 300 elements grouped into 15 domains. Within this system there are approximately 11,000 possible relations, of which more than 3,200 direct dependencies were specified. At first, we identified the relevant elements in brainstorming sessions with up to six experts and a moderator. The identified elements were directly depicted in a mind map and then classified in a hierarchical tree structure. Elements describing the main branches of this structure served as the 15 domains for the MDM model, structured as shown in figure 9.9.1.

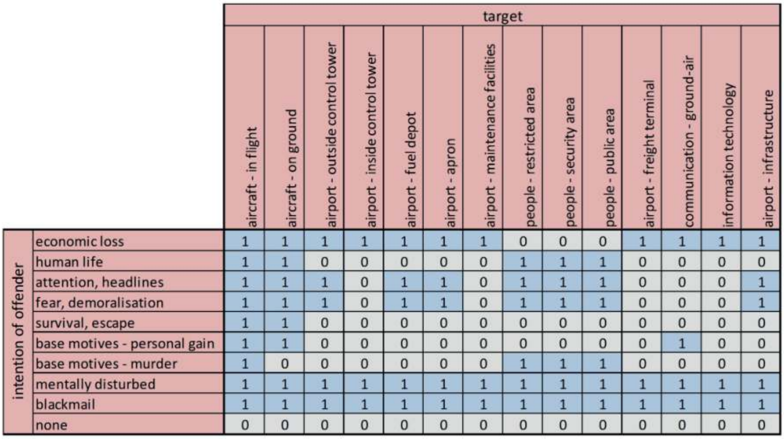


		Use case		threat sceanario								airport layout				
		actor	use	potential offender	intention of offender	tool/ weapon	use of tool/ weapon	approach of offender	insertion of tool/weapon	target	threat	departure zone	end zone	attack zone	security activity	security technology
Use case	actor		can carry out			excludes		excludes	excludes	excludes	excludes				can lead to	
	use			excludes		excludes	excludes	excludes	excludes	excludes	excludes	excludes sojourn	excludes sojourn		induces	
threat scenario	potential offender				has						allows		is located in			
	intention of offender				correlates with					reachable through						
	tool/ weapon						allows		suitable for	suitable for	allows					
	use of tool/ weapon									suitable for	allows			suitable for		
	approach of offender								allows		allows	leads to				
	insertion of tool/ weapon										allows					
	target									correlates with				is located in		
	threat										can lead to					
airport layout	departure zone											has follower				
	end zone															
	attack zone															
	security activity							can impede	can counteract			is situated in	is situated in	is situated in		can apply
	security technology					can detect										

Figure 9.9.1 Layout of the MDM for describing valid threat scenarios

The 15 domains in the square MDM resulted in 225 submatrices describing general dependencies within and between the domains. In a subsequent step, relevant submatrices with direct dependencies were identified and characterized. For example, the domain *tool/weapon* is linked directly to the domain *use of tool/weapon* (by the relation *allows*) but not to the domain *intention of offender*. It turned out that less than 20% of the submatrices were directly dependent and consequently utilized for the system modeling.

Finally, we transferred the system elements from the mind map to the MDM as row and column elements in their respective domains. In a series of workshops, the element dependencies indicated by the direct interrelation of the respective domains were specified. See figure 9.9.2 for an example DMM.



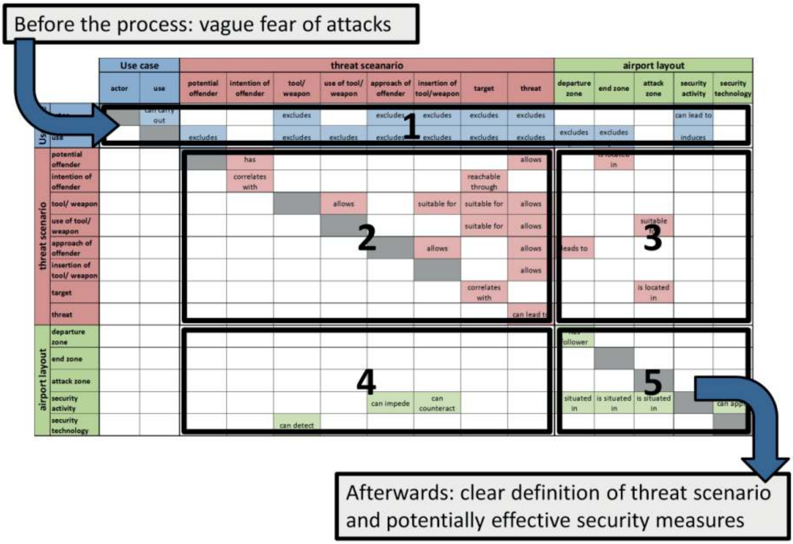
		target													
		aircraft - in flight	aircraft - on ground	airport - outside control tower	airport - inside control tower	airport - fuel depot	airport - apron	airport - maintenance facilities	people - restricted area	people - security area	people - public area	airport - freight terminal	communication - ground-air	information technology	airport - infrastructure
intention of offender	economic loss	1	1	1	1	1	1	1	0	0	0	1	1	1	1
	human life	1	1	0	0	0	0	0	1	1	1	0	0	0	0
	attention, headlines	1	1	1	0	1	1	0	1	1	1	0	0	0	1
	fear, demoralisation	1	1	1	0	1	1	0	1	1	1	0	0	0	1
	survival, escape	1	1	0	0	0	0	0	0	0	0	0	0	0	0
	base motives - personal gain	1	1	0	0	0	0	0	0	0	0	0	1	0	0
	base motives - murder	1	0	0	0	0	0	0	1	1	1	0	0	0	0
	mentally disturbed	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	blackmail	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	none	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 9.9.2 DMM showing direct dependencies between the intention of offender and target domains

Model

The identified domains can be aligned by triangularization, resulting in a clear sequence for the composition of valid threat scenarios, as illustrated in Figure 9.9.3. Starting the scenario-building process, the first two domains indicate a person's apparent use of the airport infrastructure. Whether somebody goes shopping or on an international flight affects which kind of security measures he might be confronted with and which areas of the airport he might have access to. This definition already narrows down the element choice for the subsequent scenario generation (figure 9.9.3, group 1). For example, somebody shopping at the airport will not be able to reach the target, *aircraft - on ground*, as he will not be granted access to secure areas.

After the elements of the first two domains are specified, the threat scenario can be assembled. The composition of a valid scenario without any circular logic in the building process can be assured by choosing the elements according to the sequence indicated by the MDM. Group 2 in figure 9.9.3 contains the relevant domains for this. Each selection affects the elements in the following domains; they are reduced to the ones consistent with the chosen scenario. When at least one element of each domain is settled (multi-selection of some elements is possible, such as in the *tool/weapon* domain), a structurally consistent scenario is completed. In addition to the scenario, it is important to know the attacker's way through the airport. Based on this information, scenario-specific security measures can be deduced. Possibilities are greatly reduced by specifying the use case (group 1). Additional choices have to be made in group 3 (the dependencies between threat scenarios and the airport layout).



Before the process: vague fear of attacks

		Use case		threat sceanario								airport layout				
		actor	use	potential offender	intention of offender	tool/ weapon	use of tool/ weapon	approach of offender	insertion of tool/weapon	target	threat	departure zone	end zone	attack zone	security activity	security technology
Us			can carry out			excludes		excludes	excludes	excludes	excludes				can lead to	
	use			excludes		excludes	excludes	excludes	excludes	excludes	excludes	excludes	excludes		induces	
threat scenario	potential offender				has						allows		is located in			
	intention of offender				correlates with					reachable through						
	tool/ weapon						allows		suitable for	suitable for	allows					
	use of tool/ weapon									suitable for	allows			suitable fo		
	approach of offender								allows		allows	eads to				
	insertion of tool/ weapon										allows					
	target									correlates with				is located in		
	threat										can lead t					
airport layout	departure zone											ollower				
	end zone															
	attack zone															
	security activity							can impede	can counteract			situated in	is situated in	is situated in		can app
	security technology					can detect										

Afterwards: clear definition of threat scenario and potentially effective security measures

Figure 9.9.3 MDM structured into groups of DSMs and/or DMMs

The remaining areas of the MDM contain security measures addressing single elements of the scenario (group 4) and information about the specific airport's security infrastructure (group 5). The information from these two parts of the MDM is needed to evaluate the airport's capacities to address the threat.

Results

An important result was a well-documented structure of the system and the interrelations of its elements – already achieved during the data acquisition phase. This clarified the definitions shared by all the participants.

Systematic data acquisition provided the basis for a structured assessment of threat scenarios. The system of airport security was too large for reasonably tracking the connection of each desired pair of scenario elements in the matrix, given the required level of detail. For this reason we developed a tool for facilitating the data access. A scenario builder draws on the data gathered in the MDM and guides the user through the process of building a plausible scenario. It provides the sequence in which the elements need to be specified: Elements can only be chosen if they are consistent with the pre-specified aspects of the scenario. Thus, it is impossible to assemble structurally inconsistent scenarios when working with the builder. Furthermore, after completing a scenario, the builder automatically indicates which security activities and technologies address elements of the respective scenario. The tool offers intuitive interaction with the complex structure, making the broad space of all structurally consistent scenarios accessible.

In planning airport checkpoints while taking possible future threats into account, it is desirable to account for as many scenarios as possible. As the manual creation of scenarios is time-consuming, the scenario builder has been automated, permuting through all possible element combinations and consequently producing all of the structural possibilities in the scenario design space.

Analyzing these data gave us hints concerning weak spots in the existing structure: Scenario clusters with few security technologies and activities addressing them might not be well protected. However, scenarios addressed by a large number of security measures might hint at possible redundancies in the airport layout. Such an analysis serves as a basis when testing the implementation of alternative techniques and layouts: If a poorly protected scenario cluster is addressed by new processes or technologies, then new measures seem appropriate.

References

Cole, Mara, Kuhlmann, Andreas, and Schwetje, Oliver, “Aviation Security – A Structural Complexity Management Approach,” *Proceedings of the 13th Air Transport Research Society World Conference*, Abu Dhabi, United Arab Emirates, June 2009.

Cole, Mara, and Kuhlmann, Andreas, “Preparing Today's Airport Security for Future Threats – A Comprehensive Scenario-Based Approach,” *Proceedings of the 12th Annual Conference of the Finland Futures Research Centre*, Turku, Finland, June 2010.

Maurer, Maik, Biedermann, Wieland, Cole, Mara, D’Avanzo, John, and Dickmanns, Dirk, “Airport Security: From Single Threat Aspects to Valid Scenarios and Risk Assessment,” *Proceedings of the 1st Annual Global Conference on Systems and Enterprises (GCSE)*, Washington, D.C., USA, December 2009.

Maurer, Maik, Biedermann, Wieland, Kuhlmann, Andreas, and Braun, Thomas, “The 2-Tupel-Constraint and How to Overcome It,” *Proceedings of the 11th International Design Structure Matrix Conference (DSM’09)*, Greenville, South Carolina, USA, October 2009.

8. Discussion and Future Work

The central aim of this thesis was to present an alternative to the reactive approach to airport security that is predominant today. The approach was motivated by developments in the field of decision making suggesting that expertise and knowledge-acquisition are fundamental preconditions for proficient decision making in complex environments. The constant need to adapt the security system has been related to the notion that the perceived threat to airport security is continuously evolving, based on the fact that attackers demonstrate a high level of creativity. Following an overview of the concepts, models and approaches referred to throughout this dissertation, possible directions of future work will then be outlined.

In Section 2, requirements for decision making in the context of airport security were specified. A figure was provided visualising these requirements as well as elements supporting the decision and possible actions based on the decision. It was argued that in order to understand underlying concepts such as knowledge acquisition and creativity one has to turn to research in the field of psychology. Section 3 dealt with decision making in complex environments. A short overview of the historical development of decision making within the context of psychology was provided before turning to current concepts. Naturalistic Decision Making and Fast and Frugal Heuristics were presented in more detail. A common characteristic of the two approaches is that they both build upon the notion that a decision can only be understood in the context of the environment in which it is made. Because Naturalistic Decision Making studies concentrate on decisions made in real-world settings by experienced decision makers, it was identified as being highly relevant in the context of airport security. The development of this line of research and related research models were described. Within the Naturalistic Decision Making framework, anticipatory thinking was introduced as a prerequisite to forestall and prevent possible future threats. The relevance of learning, knowledge-acquisition and expertise, not only for future-oriented decision making, is apparent throughout the whole section.

Closely interlinked with anticipatory thinking, creativity was recognized as a concept highly relevant in the context of proactive airport security management. The fundamental background of creativity as a concept within psychological research was presented and a number of different approaches introduced. Confluence approaches were identified as matching the understanding of creativity within the field of airport security. The basic assumptions of two such approaches – Investment Theory of Creativity and Systems Theory of Creativity – were presented. A special emphasis was put on the relation between creativity and knowledge. Two opposing views on the role of knowledge in the context of creativity research were presented, namely the Tension View and the Foundation View.

In the following section, insights from decision making research as well as research on creativity were related to aspects of airport security. The airport was described as a gateway through which access to the air transport system is granted. To prevent attackers from harming this system, security measures have been introduced, mostly in the aftermath of incidents. It was argued that airport security fulfils the criteria for a complex system, as it consists of a large number of varying and interrelated elements. Acquisition of extensive knowledge about such complex structures was described as being highly relevant in the context of decision making. However, feedback-loops, a basic requirement for learning, are generally missing in this decision environment because attacks on the airport security system occur very seldom. Thus, the effects of preventive actions taken can hardly ever be tested in the real-world setting. To compensate for this deficiency, a software tool, called Scenario-Builder, was introduced. This tool allows the user to construct threat scenarios and clusters and, once a scenario is completed, automatically lists security measures that are relevant to the specific choice. Furthermore, the tool offers a possibility to rearrange security measures within the airport context. In the next step, the effects of these virtual changes can be analysed and interpreted. It was suggested that the tool can (partially) substitute real-world experience and that a better understanding of the security system, effects of future threats as well as possible adaptations can be achieved.

Subsequently, how airport security and creativity relate to each other was traced. To this end, the evolution of the threat to the air transport system over the last decades was illustrated. The conclusion was drawn that the innovative potential inherent in each new attack presents a continuous challenge constituent to airport security. A dynamic interplay between the introduction of counter-measures and the exploitation of newly identified weaknesses was described. It was concluded that malevolent organisations need to be outpaced to effectively guard the transport system. The Scenario Builder was presented as a tool able to support the creative process of envisaging possible new threats by encouraging the user to reflect effects of different element choices throughout the process of scenario generation.

In conclusion of this section the methodologies underlying the developed approach, namely Multiple Domain Matrices and Scenario Technology, were introduced and shortcomings of both methodologies highlighted. It was argued, that through the combination of both approaches main drawbacks can be overcome.

The major part of the thesis was focussed on four publications, three journal papers and one book chapter. The strong interdisciplinary focus of the approach is reflected by the different scientific backgrounds of the journals and the book. Each publication was introduced, and the different perspectives they offered on proactive airport security management were highlighted. The first paper employs the viewpoint of a scenario process and describes ways to enhance the standard process to be able to deal with large, complex systems. Paper number two deals with the airport security system from the perspective of matrix-based complexity management. A framework is presented that structures the relevant phases of the approach. Furthermore, methodological innovations necessary to reflect the complex structure of the airport security system are highlighted. The main focus of the third publication is placed on the analysis of the large data base that results from the scenario building process. A detailed example is presented, demonstrating possible ways of accessing and interpreting the generated data. Finally, the fourth publication traces the visual structure of the airport security system in the matrix representation of the airport security system.

In summary, it can be stated that this dissertation contributes to the fields of psychology, air transport and system engineering. Regarding the discipline of psychology, the main contribution relates to decision making in complex environments. This thesis proposes a procedure to support knowledge-acquisition in environments where absent feedback loops would otherwise impede learning processes. Adaptations of the system, reflecting expectations with regard to future developments based on anticipatory thinking, can be initially tested and compared. The approach, furthermore, indicates means by which the creative process of imagining possible future developments could be assisted, i.e. it suggests that the decomposition of the area in question into subcomponents and the presentation of reasonable element choices to the user can raise the level of creativity.

Security checks at airports are a major concern in the field of air transport, as they present a serious obstacle to the offering of a smooth and hassle-free journey to the passenger. From an airport management point of view, the reactive implementation procedure dominant today deprives airport operators of planning certainty since sudden regulatory changes could fundamentally change, for example, floor space necessary for security check points or costs evoked by security processes. A change in thinking towards proactive airport security management would first and foremost improve the overall level of security as innovative threats might already be counteracted when they first appear. Furthermore, a threat-oriented approach would help to identify redundant or unnecessary process steps and could finally lead to a more efficient setup of the airport security system.

The application of the Multiple Domain Matrix approach to the concerns of airport security introduced a new area of research to the methodology. The requirements of this field of application went beyond the borders of the methodology in a number of ways. For example, the restriction of the methodology to the documentation of pairwise interrelations had to be overcome. Furthermore, the large size and the complexity of the documented system made it necessary to develop a user interface that would guide the data extraction process. New ways of analysing the results were developed and tested. From the point of view of Scenario Technology it was also necessary to change the standard procedures to be able to accommodate the specific challenges of airport security. The enhanced approach demonstrates how large systems can be handled within the scope of Scenario Technology, despite their high number of elements.

The theoretical conceptions presented in this thesis, the creation of the Scenario Builder and the means suggested to analyse the resulting data provide the basis for subsequent steps towards proactive airport security management. Future work in this area should investigate the applicability of the approach in real-world settings. A necessary first step in this direction is the design of experimental settings to test how the Scenario Builder can add to the understanding of the system's components and interrelations. Furthermore, it is important to experimentally investigate how and to what extent the tool can lead to more creative ideas for possible future threats and their countermeasures. Once the capabilities of the approach have been determined, an exploration of how the methodology can be employed to the advantage of the objectives of the security system can be set in motion. To this end, the acknowledgement of the relevance of anticipatory thinking to address possible future threats by the stakeholders involved in airport security is of fundamental importance. A very interesting line of future research in this context would be to investigate how creativity is treated in organizational contexts and how its relevance can be promoted within corporate culture.

Another open question in the organizational context is how the security system should be adapted on the basis of identified possible future threats. Today the airport security system is strictly determined by national and international rules and regulations. The power of the airport operator or security provider to singlehandedly design elements of the security measures according to their own perception of current risk and possible future threats is almost nonexistent. In this context, who would be held responsible for failures of the system if binding regulations were relaxed would constitute an unanswered question. One of the major challenges to operators with regard to security is to run the airport system as efficiently as possible while at the same time permanently providing a high level of security. As the threat from malevolent organizations is constantly evolving, it might not be necessary to exert all security measures available at all times. In a modular approach to the airport security process, steps could be flexibly inserted or removed. With such an approach the measures executed could be adapted in accordance with the currently perceived level of risk and possible future threats identified as relevant. This security system would encompass as few restrictions as possible but, at the same time, be as extensive as current and future threats dictate.

This dissertation demonstrates how a proactive approach to airport security management can be grounded in psychological research on decision making and creativity. Fundamental requirements for such an approach have been discussed and the Scenario Builder presented as a possibility to address these challenges. How insights gained from a better understanding of underlying system interrelations and a supportive attitude to creativity can be habitually exploited on an organizational level still remains an unanswered question. It is a challenge for future research to provide empirical evidence for the suggested methodology and identify ways of incorporating anticipatory approaches into organizational structures.

9. Bibliography

Amabile, T. M. (1996). Creativity in Context. Update to: The Social Psychology of Creativity. Westview Press, Boulder and Oxford.

Baum, P. (2011). 80 Years of AVSEC: From Arequipa to Domodedovo. In: Aviation Security International, 17:1.

Beach, L. R. (1993). Image Theory: Personal and Organizational Decisions. In: Klein, G. A., Orasnu, J., Calderwood, R. and Zsambok, C. E. (eds.). Decision Making in Action: Models and Methods. Ablex Publishing Corporation, Norwood. pp. 148-157.

Bernoulli, D. (1954). Exposition of a New Theory on the Measurement of Risk. In: Econometrica, 22:23-36. (Translation of: Bernoulli, D. (1738). Specimen theoriae novae de mensura sortis. In: Commentarii Academiae Scientiarum Imperialis Petropolitanae, V:175-192.).

Brehmer, B. 1992. Dynamic Decision Making: Human Control of Complex Systems. In: Acta Psychologica, 81(X):211-241.

Chermack, T. J. and Lynham, S. A. (2002). Definitions and Outcome Variables of Scenario Planning. In: Human Resource Development Review, 1(3):366-383.

Cohen, M. S. (1993). Three Paradigms for Viewing Decision Bisases. In: Klein, G. A., Orasanu, J., Calderwood, R. and Zsambok, C. E. (eds.). Decision Making in Action: Models and Methods. Ablex Publishing Corporation, Norwood. pp. 36-50.

Cole, M. (2014). Towards Proactive Airport Security Management: Supporting Decision Making Through Systematic Threat Scenario Assessment. In: Journal of Air Transport Management, 35:12-18.

Cole M. and Kuhlmann A. (2011). Preparing Today's Airport Security for Future Threats – A Comprehensive Scenario-Based Approach. In: Auffermann, B. and Kaskinen, J. (eds.). Security in Futures – Security in Change: Proceedings of the Conference “Security in Futures – Security in Change”, 3 - 4 June 2010, Turku, Finland. pp. 206-216.

Cole, M. and Kuhlmann, A. (2012). A Scenario-Based Approach to Airport Security. In: Futures, 44:319-327.

Cole, M., and Maurer, M. (2011). Sensitivity Analysis for a Future-Oriented Optimization of Airport Security. In: 15th Air Transport Research Society World Conference, 29 June - 02 July 2011, Sydney, Australia.

Cole, M. and Maurer, M. (2014). Handling Complex Socio-Technical Systems: A Method for Proactive Optimization of Airport Security. In: International Journal of Knowledge-Based and Intelligent Engineering Systems, 18:191-200.

Csikszentmihalyi, M. (1988). Society, Culture, and Person: A Systems View of Creativity. In: Sternberg, R. J. (ed.). The Nature of Creativity. Cambridge University Press, New York. pp. 325-339.

Csikszentmihalyi, M. (2006). A System Perspective on Creativity. In: Henry, J. (ed.). Creative Management and Development (Published in Association with the Open University). Sage Publications, London. pp. 3-17.

Danilovic, M. and Browning, T. (2007). Managing Complex Product Development Projects with Design Structure Matrices and Domain Mapping Matrices. In: International Journal of Project Management, 25:300-314.

Dörner, D. 1980. On the Difficulties People Have in Dealing With Complexity. In: Simulation & Games, 11(1):87-106.

Dolnik, A. (2007). Understanding Terrorist Innovation: Technology, Tactics and Global Trends. Routledge, Abingdon.

Endsley, M. R. (1988). Design and Evaluation for Situation Awareness Enhancement. In: Proceedings of the Human Factors Society

32nd Annual Meeting. Human Factors Society, Santa Monica. pp. 97-101.

Endsley, M. R. (1997). Training the Naturalistic Decision Maker. In: Zsambok, C. E. and Klein, G. (eds.). Naturalistic Decision Making. Laurence Erlbaum Associates, Mahwah. pp. 269-283.

Eppinger, S. D. and Browning, T. R. (eds.) (2012). Design Structure Matrix Methods and Applications. MIT Press, Cambridge.

Feakin, T. (2011). Insecure Skies? Challenges and Options for Change in Civil Aviation. Occasional Paper, Royal United Services Institute, London.

Feldman, D. H. (1999). The Development of Creativity. In: Sternberg, R. J. (ed.). Handbook of Creativity. Cambridge University Press, New York. pp. 169-186.

Feldman, D. H., Csikszentmihalyi, M. and Gardner, H. (1994a). Preface. In: Feldman, D. H., Csikszentmihalyi, M. and Gardner, H. (eds.). Changing the World: A Framework for the Study of Creativity. Praeger, Westport. pp. xi-xv.

Feldman, D. H., Csikszentmihalyi, M. and Gardner, H. (1994b). A Framework for the Study of Creativity. In: Feldman, D. H., Csikszentmihalyi, M. and Gardner, H. (eds.). Changing the World: A Framework for the Study of Creativity. Praeger, Westport. pp. 1-45.

Gigerenzer, G. (1996). On Narrow Norms and Vague Heuristics: A Replay the Kahneman and Tversky (1996). In: Psychological Review, 103(3):592-596.

Gigerenzer, G. (2001). The Adaptive Toolbox. In: Gigerenzer, G. and Selten, R. (eds.). Bounded Rationality: The Adaptive Toolbox. MIT Press, Cambridge and others. pp. 37-50.

Gigerenzer, G. and Gaissmaier, W. (2011). Heuristic Decision Making. In: Annual Review of Psychology, 62:451-482.

Gigerenzer, G. and Goldstein, D. G. (2011). The Recognition Heuristic: A Decade of Research. In: Judgment and Decision Making, 6(1):100-121.

Gigerenzer, G. and Selten, R. (eds.) (2001). Bounded Rationality: The Adaptive Toolbox. MIT Press, Cambridge and others.

Gigerenzer, G. and Todd, P. M. (1999). Fast and Frugal Heuristics: The Adaptive Toolbox. In: Gigerenzer, G., Todd, P. M. and the ABC Research Group (eds.). Simple Heuristics That Make Us Smart. Oxford University Press, New York. pp. 3-34.

Gigerenzer, G., Todd, P. M. and the ABC Research Group (eds.) (1999). Simple Heuristics That Make Us Smart. Oxford University Press, New York.

Gill, P., Horgan, J., Hunter, S. T. and Cushenbery, L. D. (2013). Malevolent Creativity in Terrorist Organizations. In: The Journal of Creative Behavior, 47(2):125-151.

Glenn, J. C. and Gordon, T. J. (eds.) (2009). Futures Research Methodology, Version 3.0, UNU Millenium Project.

Godet, M. (2000). The Art of Scenarios and Strategic Planning: Tools and Pitfalls. In: Technological Forecasting and Social Change, 65(1):3-22.

Goldstein, D. G. and Gigerenzer, G. (2011). The Beauty of Simple Models: Themes in Recognition Heuristic Research. In: Judgment and Decision Making, 6(5):392-395.

Goldstein, W. M. and Hogarth, R. M. (1997). Judgement and Decision Research: Some Historical Context. In: Goldstein, W. M. and Hogarth, R. M. (eds.). Research on Judgment and Decision Making: Currents, Connections, and Controversies. Cambridge University Press, Cambridge. pp. 3-65.

Hertwig, R. Hoffrage, U. and the ABC Research Group (eds.) (2013). Simple Heuristics in a Social World. Oxford University Press, New York.

Hofinger, G. (2003). Fehler und Fallen beim Entscheiden in Kritischen Situationen. In: Strohschneider, S. (ed.). Entscheiden in kritischen Situationen. Im Auftrag der Plattform „Menschen in komplexen Arbeitswelten" e.V. Verlag für Polizeiwissenschaft Clemens Lorei, Frankfurt. pp. 115-136.

Hogarth, R. M. and Makridakis, S. (1981). Forecasting and Planning: An Evaluation. In: Management Science, 27(2):115-138.

de Jouvenel, H. (2000). A Brief Methodological Guide to Scenario Building. In: Technological Forecasting and Social Change, 65(1):37-48.

Kahneman, D. (2003). A Perspective on Judgment and Choice: Mapping Bounded Rationality. In: American Psychologist, 58(9):697-720.

Kahneman, D., Slovic, P. and Tversky, A. (1982). Judgment Under Uncertainty: Heuristics and Biases. Cambridge University Press, Cambridge.

Klayman, J. (1984). Learning From Feedback in Probabilistic Environments. In: Acta Psychologica, 56:81-92.

Klein, G. A. (1993). A Recognition-Primed Decision (RPD) Model of Rapid Decision Making. In: Klein, G. A., Orasanu, J., Calderwood, R. and Zsambok, C. E. (eds.). Decision Making in Action: Models and Methods. Ablex Publishing Corporation, Norwood. pp. 138-147.

Klein, G. (1997). An Overview of Naturalistic Decision Making Applications: A Global View. In: Zsambok, C. E. and Klein, G. (eds.). Naturalistic Decision Making. Laurence Erlbaum Associates, Mahwah. pp. 49-59.

Klein, G. (2008). Naturalistic Decision Making. In: Human Factors, 50(3):456-460.

Klein, G. A., Orasanu, J., Calderwood, R. and Zsambok, C. E. (1993). Preface. In: Klein, G. A., Orasanu, J., Calderwood, R. and Zsambok, C. E. (eds.). Decision Making in Action: Models and Methods. Ablex Publishing Corporation, Norwood. pp. vii-x.

Klein, G., Snowden, D. and Pin, C. L. (2010). Anticipatory Thinking. In: Mosier, K. L. and Fischer, U. M. (eds.). Informed by Knowledge: Expert Performance in Complex Situations. Taylor & Francis, Sussex. pp. 235-245.

Leiber, T. (2007). Structuring Nature's and Science's Complexity: System Laws and Explanations. In: Leiber, T. (ed.). Dynamisches Denken und Handeln. Philosophie und Wissenschaft in einer komplexen Welt, Festschrift für Klaus Mainzer zum 60. Geburtstag. Hirzel Verlag, Stuttgart. pp. 193-212.

Lindemann, U., Maurer, M. and Braun, T. (2009). Structural Complexity Management: An Approach for the Field of Product Design. Springer, Heidelberg.

Lipshitz, R. (1993). Converging Themes in the Study of Decision Making in Realistic Settings. In: Klein, G. A., Orasanu, J., Calderwood, R. and Zsambok, C. E. (eds.). Decision Making in Action: Models and Methods. Ablex Publishing Corporation, Norwood. pp. 103-137.

Lipshitz, R. and Ben Shaul, O. (1997). Schemata and Mental Models in Recognition-Primed Decision Making. In: Zsambok, C. E. and Klein, G. (eds.). Naturalistic Decision Making. Laurence Erlbaum Associates, Mahwah. pp. 293-303.

Lipshitz, R., Klein, G., Orasanu, J. and Salas, E. (2001). Taking Stock of Naturalistic Decision Making. In: Journal of Behavioural Decision Making, 14(5):331-352.

Marewski, J. N., Gaissmaier, W. and Gigerenzer, G. (2010). Good Judgments Do Not Require Complex Cognition. In: Cognition Process, 11:103-121.

Maurer, M. and Cole, M. (2012). Airport Security System. In: Eppinger, S. D. and Browning, T. R. (eds.). Design Structure Matrix Methods and Applications. MIT Press, Cambridge. pp. 288-293.

Mayer, R. E. (1999). Fifty Years of Creativity Research. In: Sternberg, R. J. (ed.), Handbook of Creativity. Cambridge University Press, New York. pp. 449-460.

Newell, B. R., Lagnado, D. A. and Shanks, D. R. (2007). Straight Choices - The Psychology of Decision Making. Psychology Press, Hove.

Orasanu, J. and Connolly, T. (1993). The Reinvention of Decision Making. In: Klein, G A., Orasanu, J., Calderwood, R. and Zsambok, C. E. (eds.). Decision Making in Action: Models and Methods. Ablex Publishing Corporation, Norwood. pp. 3-20.

Payne, J. W., Bettman, J. R. and Johnson, E. J. (1993). The Adaptive Decision Maker. Cambridge University Press, Cambridge.

Poole, R. W. (2009). The Case for Risk-Based Aviation Security Policy. In: World Customs Journal, 3(2):3-16.

Rasmussen, J. (1993). Deciding and Doing: Decision Making in Natural Contexts. In: Klein, G. A., Orasanu, J., Calderwood, R. and Zsambok, C. E. (eds.). Decision Making in Action: Models and Methods. Ablex Publishing Corporation, Norwood. pp. 158-171.

Rasmussen, M. and Hafez, M. (eds.) (2010). Terrorist Innovations in Weapons of Mass Effect: Preconditions, Causes and Predictive Indicators. Available at [http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA556986], last accessed 15.11.2013.

Rescher, N. (1998). Complexity. A Philosophical Overview. Transaction Publishers, New Brunswick.

Salter, M. B. (ed.) (2008a). Politics at the Airport. University of Minnesota Press, Minneapolis.

Salter, M. B. (2008b). Imagining Numbers - Risk, Quantification, and Aviation Security. In: Security Dialogue, 39:243-266.

Savage, L. J. (1954). The Foundations of Statistics. John Wiley & Sons, New York.

Simon, H. A. (1955). A Behavioral Model of Rational Choice. In: Quarterly Journal of Economics, 69:99-118.

Simon, H. A. (1990). Invariants of Human Behavior. In: Annual Review of Psychology, 41:1-19.

Sterman, J. D. (1994). Learning In and About Complex Systems. In: System Dynamics Review, 10(2-3):291-330.

Sternberg, R. J. (2006a). The Nature of Creativity. In: Creativity Research Journal, 18(1):87-98.

Sternberg, R. J. (2006b). Introduction. In: Kaufman, J. C. and Sternberg, R .J. (eds.). The International Handbook of Creativity. Cambridge University Press, New York. pp. 1-9.

Sternberg, R. J. (2006c). Creating a Vision of Creativity: The First 25 Years. In: Psychology of Aesthetics, Creativity, and the Arts, S(1):2-12.

Sternberg, R. J. and Lubart, T. I. (1999). The Concept of Creativity: Prospects and Paradigms. In: Sternberg, R. J. (ed.). Handbook of Creativity. Cambridge University Press, New York. pp. 3-15.

Sternberg, R. J. and O'Hara, L. A. (1999). Creativity and Intelligence. In: Sternberg, R. J. (ed.). Handbook of Creativity. Cambridge University Press, New York. pp. 251-272.

Steward, D. (1981). The Design Structure System: A Method for Managing the Design of Complex Systems. In: IEEE Transaction on Engineering Management, 28(3):79-83.

Sweet, K. M. (2002). Terrorism and Airport Security. Edwin Mellen Press, Lewiston.

Sweet, K. M. (2009). Aviation and Airport Security: Terrorism and Safety Concerns. Auerbach Publications, Boca Raton.

Todd, P. M. and Gigerenzer, G. (2012). What is Ecological Rationality? In: Todd, P. M., Gigerenzer, G. and the ABC Research Group (eds.). Ecological Rationality: Intelligence in the World. Oxford University Press, New York. pp. 3-30.

Todd, P. M. and Gigerenzer, G. (2007). Environments That Make Us Smart. In: Current Directions in Psychological Science, 16(3):167-171.

Todd, P. M., Gigerenzer, G. and the ABC Research Group (eds.) (2012). Ecological Rationality: Intelligence in the World. Oxford University Press, New York.

Tversky, A. and Kahneman, D. (1974). Judgment Under Uncertainty: Heuristics and Biases. In: Science, 185(4157):1124-1131.

von Neumann, J. and Morgenstern, O. (1947). Theory of Games and Economic Behavior. Princeton University Press, Princeton.

Wells, A. T. and Young, S. B. (2004). Airport Planning & Management. McGraw-Hill, New York.

Zsambok, C. E. (1997). Naturalistic Decision Making: Where Are We Now? In: Zsambok, C. E. and Klein, G. (eds.). Naturalistic Decision Making. Laurence Erlbaum Associates, Mahwah. pp. 3-16.

University
of Bamberg
Press

During the last decades the air transport system has been repeatedly under attack. As reactions to such incidents many layers of security measures have been introduced throughout the system, allowing potential attackers to continuously remain one step ahead. Against this background it is important to develop an approach aiming at proactive airport security management. This has to be based on in-depth knowledge of elements and interrelations of the security system and should allow inclusion of creative, out of the box ideas for novel incidents and attacks.

The development of a software tool fulfilling these challenges, the so-called Scenario Builder, has been pursued in the course of this dissertation. The methodological foundations, its functionality and use as well as possible ways to analyse the resulting data are presented in this work. The main part of the thesis is comprised of four publications dealing with different aspects of the developed methodology. Emphasis is placed on the strongly interdisciplinary character of the topic, mainly based in the fields of psychology and aviation management.

ISBN 978-3-86309-333-4
9 783863 093334
www.uni-bamberg.de/ubp/