A QUANTITATIVE RISK MODEL FOR A UNIFORM DESCRIPTION OF SAFETY AND SECURITY

Jürgen Beyerer[1] and Jürgen Geisler[2]

[1] *juergen.beyerer@iosb.fraunhofer.de*
Fraunhofer Institute of Optronics, System Technologies, and Image Exploitation IOSB,
Fraunhoferstr. 1, 76131 Karlsruhe (Germany)
and
Karlsruhe Institute of Technology KIT
Institute of Anthropomatics and Robotics
Adenauerring 4, 76131 Karlsruhe (Germany)

[2] *juergen.geisler@iosb.fraunhofer.de*
Fraunhofer Institute of Optronics, System Technologies, and Image Exploitation IOSB,
Fraunhoferstr. 1, 76131 Karlsruhe (Germany)

Abstract

A mathematical framework is presented that allows to describe quantitatively and in an integrative way the risk of safety and security constellations. Thereby, great importance is attached to a clear notation with a sound semantics.

Based on a role model with the three roles »source of danger«, »subject of protection« and »protector«, risk is modelled quantitatively using statistical decision and game theory. Uncertainties are modelled based of probability distributions, whereupon probability is interpreted in a Bayesian context as a degree of belief DoB.

The set D of sources of danger is endowed with a DoB-distribution describing the probability of occurrence. D is partitioned into subsets that describe dangers which are due to random causes, carelessness and intention.

A set of flanks of vulnerability F is assigned to each subject of protection. These flanks characterize different aspects of vulnerability concerning mechanical, physiological, informational, economical, reputational, psychological, ... vulnerability. The flanks of vulnerability are endowed with conditional DoBs that describe to which degree an incidence or an attack will be harmful. Additionally, each flank of vulnerability is endowed with a cost function that quantifies the costs which are charged to the subject of protection, if it is affected by a harmful incidence or attack.

With these ingredients the risk for the subject of protection can be quantified based on an ensemble functional with respect to all sources of danger and to all flanks of vulnerability. Depending of the respective subset of dangers such a functional is an expectation (case of random causes and carelessness) or a selection operation (case of intention), where in the latter case the attack will presumably take place at the weakest flank of vulnerability.

The calculated risk can be opposed to the cost of protection measures that are offered by the protector in order to foster an effective and economical invest decision.

From an attacker's point of view a utility function is formulated which a rational attacker presumably would use to evaluate his cost-benefit ratio in order to decide whether he attacks and which of his options he exercises.

The challenges of the approach are the determination of the cost functions and especially the estimation of the probabilities (DoBs) of the model.

The model can be used to simulate and evaluate the endangerment of subjects of protection quantitatively.

Keywords: Safety, Security, Risk, Bayesian Statistical Decision Theory, Game Theory, Degree of Belief, Role Model, Vulnerability, Flanks of Vulnerability

1 INTRODUCTION

Safety and security share a lot of commonalities. Nevertheless, measures and systems to provide and ensure safety and security are planned and implemented often independently by different experts. If both aspects were treated in an integrated manner, synergies could be realized and costs could be reduced.

If we want to ensure safety and security of such complex systems like critical infrastructures and socio-technical systems, many disciplines will be stakeholders: engineering, law, economics, humanities, social sciences etc.

Up to now, there is no established common formal language concerning safety and security and no common language across all involved disciplines. The aim of this paper is to propose a quantitative mathematical approach that could serve to describe and to analyze safety and security problems in a unified fashion and to plan and optimize dedicated measures and systems.

1.1 Related Work

The frameworks of statistical decision and game theory are mature and approved methodologies which have been applied to many different domains, foremost to economics [1]. In combination with attack trees, game theory has been already applied to model rational attackers [2]. Some aspects of the approach presented in this paper have been already proposed in a preliminary qualitative formulation in [3] and [4].

1.2 Safety and Security

The terms of safety and security only make sense in the face of some danger that is supposed to be able to cause damage. It emanates from some »source of danger« d, propagates over a certain »path of transmission« and has effect on a »subject of protection« s (see Fig. 1). The path of transmission is everything between d and s that is needed to transport the hazardous effect. It belongs neither to d nor to s.

In case of e.g. a radio-controlled explosive device this path comprises the radio link between trigger and device as well as the air between the device and the target that the bomb fragments have to pass. In case of a tsunami it is the water between the epicenter of an earthquake and the shore.

The danger hits the subject of protection s at some of its »flanks of vulnerability« F that can be of different quality (mechanical, chemical, psychological, financial, informational, ...). The flanks of vulnerability do belong to the subject of protection and are under its control.

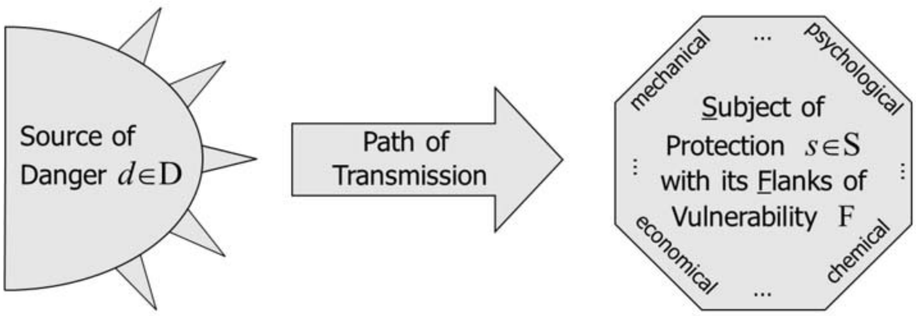

Fig. 1: Relation between a source of danger d and subject of protection s. D and S denote the sets of sources of danger and the set of subjects of protection, respectively.

The two examples mentioned above – explosive device and tsunami – illustrate two fundamental categories of dangers: willful and unintended. If a danger is willfully applied, we are in the domain of security. If it is unintended, we are in the domain of safety. A willful endangerment by human beings can be used on the one hand as a means to achieve some (material) goal, e.g. in the case of robbery. Or it can be executed as a purpose of itself, e.g. in the case of vandalism or amok. The source of unintended danger may on the one hand be human carelessness that may underestimate or even ignore damage. Or the origin may be a random event such as an unforeseeable technical fault or a natural event (e.g. an earthquake). Fig. 2 illustrates this categorization.

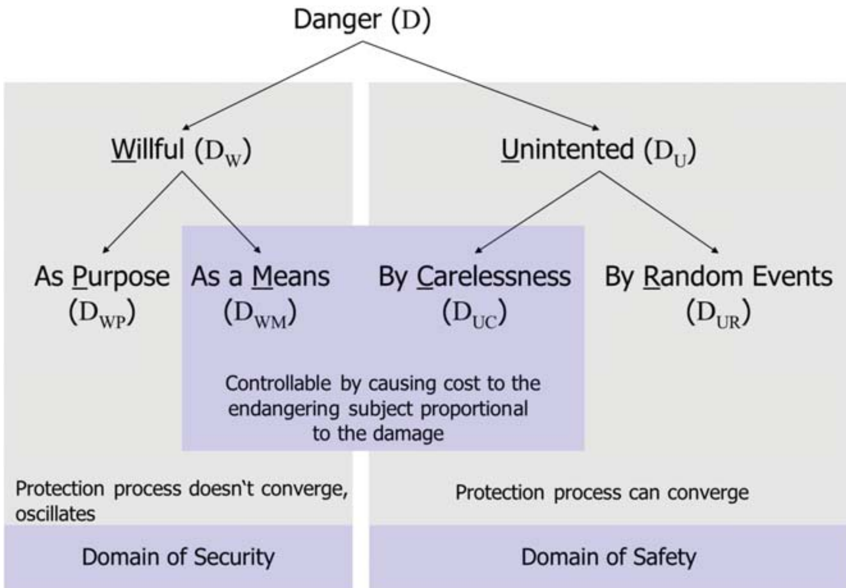

Fig. 2: Categorization of dangers with respect to safety and security. $d \in \mathrm{D_W}$ are called "attackers" and $d \in \mathrm{D_U}$ are called "causers". In the cases of an attacker $d \in \mathrm{D_{WM}}$ or a causer $d \in \mathrm{D_{UC}}$ the pertaining risk can be influenced by costs charged to d (penalties, money,…), so that d will be deterred from attacking or so that d is urged to act more carefully, respectively.

From a game theoretic point of view there is another interesting interpretation of safety and security [3]. With respect to safety the subject of protection s plays a game against nature. His opponent behaves like a random process. Based on a statistical analysis the distribution which characterizes the opponent can be learned and counter measures can be applied to reduce the risk. Especially if the distribution does not change with time, a stationary safety level can be attained with passive measures.

In contrast, regarding security, the adversary behaves intelligently. In this case, the subject of protection s plays against a strategically acting opponent who evades of being understood, who analyzes the weaknesses of s and who selfishly tries to maximize his benefit. Therefore, measures will be answered with counter measures and no stationarity will be achieved (see Fig. 2).

A further issue becomes clear from the discussion so far: an attacker who is a rationally acting agent does not randomly attack any of the flanks of vulnerability. Instead he will attack the flank which is must promising for him to achieve his goal. Relating to security, this directly leads to the following **minimum principle**: The weakest flank determines the degree of vulnerability.

Moreover, whether we are in the domain of security or of safety only depends on the source of danger d and does neither depend on the path of transmission nor on the subject of protection s (see Fig. 1). E.g. if a fire was caused by an arsonist, we would have a security case. If however the fire was caused by an electric shortcut, we would assign it to safety. Relating to the path of transmission and to the subject of protection both cases need not to be distinguished, since both lead to the same consequences.

2 ROLE AND RISK MODEL

2.1 Roles

The goal of each measure to increase safety as well as to increase security is to prevent the subject of protection from harm caused by dangers. Therefore, we define a third role beneath the already introduced source of protection s and the source of danger d: The »protector« p. It is first of all a role, not necessarily an entity separate from s. When any s protects itself without any external help, p and s are coined by the same entity. With the introduction of p we can concentrate all measures of protection onto this role. That are (see Fig. 3): To detect and possibly neutralize the source of danger directly, to elongate the path of transmission in order to weaken the hazardous effect, to cover the subject of protection and to harden its flanks of vulnerability. A necessary precondition for the relation between the subject of protection and its protector is trust, in case of s and p are separate entities often confirmed by a contract.

To complete the relations between the three roles in Fig. 3 it should be made clear, that except for unintended danger by random events (see. Fig. 2) there is always some flow of value from s to d. That is expressed by the relation s »enriches« d.

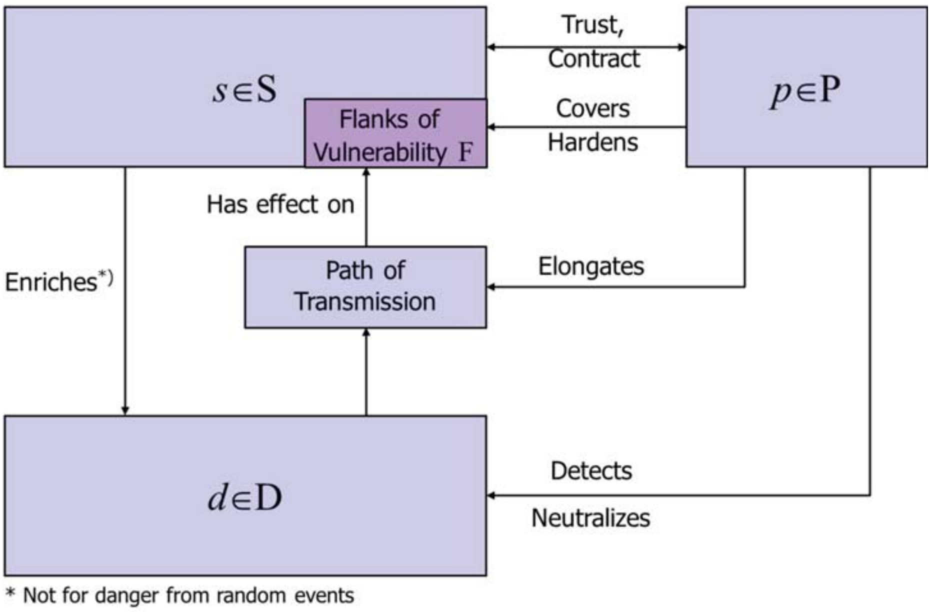

Fig. 3: Roles and relations between them. Note that the different roles can be played by different entities but coincidences are also possible. E.g. someone can be a danger for himself or someone can protect himself.

2.2 Formalization of Ingredients

In this section the entities, attributes and relations of the considerations above are formalized and quantified using the well-established approach of Bayesian statistical decision theory [1]. Probability is used in the broader sense as a degree of belief (DoB). This interpretation is a generalization of the classical frequentistic meaning of probability, which however is still compliant with the axioms of Kolmogorov [5], [6]. All quantities relate to a time interval of length T, within which they are assumed to remain constant.

$\mathrm{S} = \mathrm{S}_{\text{Persons}} \cup \mathrm{S}_{\text{Objects}} \cup \mathrm{S}_{\text{Systems}} \cup \mathrm{S}_{\text{Legal Interests}}$ denotes the set of subjects of protection. These subjects $s \in \mathrm{S}$ have budgets $b(s)$ for safety and security measures and flanks of vulnerability $f \in \mathrm{F}_s$.

Dangers (attackers, causers) d are elements of the set of sources of danger $\mathrm{D} = \mathrm{D}_{\text{WP}} \cup \mathrm{D}_{\text{WM}} \cup \mathrm{D}_{\text{UC}} \cup \mathrm{D}_{\text{UR}}$, where the indices have the following meaning:

WP: Willful danger as a purpose (vandalism, amok, …)

WM: Willful danger as a means (burglary, robbery, …)

UC: Unintended danger due to carelessness or negligence (inattention, breach of duty)

UR: Unintended danger with random characteristic (technical failures, natural disasters)

We define two further subsets $\mathrm{D}_{\text{U}} := \mathrm{D}_{\text{UC}} \cup \mathrm{D}_{\text{UR}}$ and $\mathrm{D}_{\text{W}} := \mathrm{D}_{\text{WP}} \cup \mathrm{D}_{\text{WM}}$ that structure the dangers $\mathrm{D} = \mathrm{D}_{\text{W}} \cup \mathrm{D}_{\text{U}}$ into a willful and an unintended subcategory.

In the following $d \in \mathrm{D}_{\text{W}}$ are called »attackers«. Attackers perpetrate attacks a which are pooled in the set of attacks A, $a \in \mathrm{A}$. An attacker has a budget $b(d)$ with which he finances the effort of an attack. The attacks a an attacker d is able to perform are summarized in the subset $\mathrm{A}_d \subseteq \mathrm{A}$.

Sources of danger $d \in \mathrm{D}_{\text{U}}$ due to carelessness generate incidents i, which are pooled in set of incidents I , $i \in \mathrm{I}$. In the following $d \in \mathrm{D}_{\text{U}}$ are called »causers«, because they cause incidents. The set of incidents referred to a causer $d \in \mathrm{D}_{\text{U}}$ are summarized in the subset $\mathrm{I}_d \subseteq \mathrm{I}$.

If an attack or incident happens, the success (harm) of such an event is quantified by the degree of success $\beta \in [0,1]$.

An attack or an incident on s via flank f with success β costs s: $c(s, f, \beta) \in [0, \infty)$. Vulnerability with respect to attacks or incidents is modelled as a DoB-density. $p_{\text{V}}\left(\beta \middle| i, s, f\right)$ and $p_{\text{V}}\left(\beta \middle| a, s, f\right)$ describe the DoB-densities for the degree of success β, if a respectively i hits s via f .

Remark: In the case that the costs $c(s, f, \beta)$ are proportional to the success β , i.e. $c(s, f, \beta) = \beta \cdot c(s, f)$, costs and vulnerability can be factorized:
$\int_0^1 c(s, f, \beta) \cdot p_V(\beta \mid i, s, f)\, \mathrm{d}\beta = c(s, f) \cdot v(s, f, i)$, where $v(i, s, f) := \mathrm{E}_{\beta|i,s,f}\{\beta\}$
$= \int_0^1 \beta \cdot p_V(\beta \mid i, s, f)\, \mathrm{d}\beta$ is the mean success-DoB of an incident i.

Causers of danger due to carelessness $d \in \mathrm{D}_{\text{UC}}$ are charged with costs $\kappa(s, f, \beta) \in [0, \kappa_{d\_\text{Ruin}}]$. These costs correspond to a penalty for d for generating an incident $i \in \mathrm{I}_d$ hitting s via f with success β. The higher the costs for d the lower the probability of an incident generated by d should be (deterrent effect).

A protector $p \in \mathrm{P}$ provides safety and security measures $m(s,f) \in \mathrm{M}$ for the flank *f* of *s*. M denotes the set of available and $\mathrm{M}^* \subseteq \mathrm{M}$ the set of implemented measures. A measure m costs s the amount $c(m(s,f))$. Of course, s can only effort measures according to his budget. This introduces the constraint $\sum_{m \in \mathrm{M}^*} c(m(s,f)) \leq b(s)$.

Measures $m(s,f)$ should reduce vulnerability, i.e. the success of attacks and/or incidents, and/or the probability of occurrence of attacks and/or of incidents. However, $m(s,f)$ is modeled such that it does not reduce $c(s,f,\beta)$.

The following quantities are to be understood from the attacker's point of view. $g(s,f,\beta)$ denotes the gain due to an attack on s via f with success β. $p_{\mathrm{Success}}(\beta \mid a,s,f)$ is the DoB-density for success β, if a hits s via *f*. $c_{\mathrm{Effort}}(a,s,f)$ describes the costs due to the effort for executing an attack a on s via *f*. $c_{\mathrm{Penalty}}(s,f,\beta)$ denotes the monetary equivalent to a penalty for an attack on s via *f* with success β.

And finally, $\Pr(\mathrm{Penalty} \mid s,f,\beta) = 1 - \Pr(\neg \mathrm{Penalty} \mid s,f,\beta)$ denotes the DoB for a punishment of an attack on s via *f* with success β.

2.3 Quantification of Risk

The total risk R_{s_total} of a subject of protection s from the point of view of s can be expressed as: $R_{s\_\mathrm{total}} := \underbrace{R_s}_{\mathrm{Model}} + \underbrace{R_0}_{\text{Outside modelling scope}}$, where R_S denotes the describable part of the risk and R_0 denotes that part of the risk, which cannot be modelled. Hopefully, measures m reducing the modelled part of the risk R_s should not increase R_0 for more than this reduction, i.e.: $\Delta R_{s\_\mathrm{absolut}}(m) := R_{s\_\mathrm{absolut}}(\text{without } m) - R_{s\_\mathrm{absolut}}(\text{with } m) \geq 0$ with $\Delta R_s(m) := R_s(\text{without } m) - R_s(\text{with } m) > 0$.

The risk R_s of s from the point of view of s can be expressed as:

$$R_s = \sum_{d \in \mathrm{D_U}} \sum_{i \in \mathrm{I}_d} \sum_{f \in \mathrm{F}_s} \int_0^1 c(s,f,\beta) \cdot p_{\mathrm{V}}(\beta \mid i,s,f)\, \mathrm{d}\beta \cdot \Pr_{\mathrm{U}}(i \mid s,f)$$
$$+ \sum_{d \in \mathrm{D_W}} \sum_{a \in \mathrm{A}_d} \int_0^1 c(s,\tilde{f},\beta) \cdot p_{\mathrm{V}}(\beta \mid a,s,\tilde{f})\, \mathrm{d}\beta \cdot \Pr_{\mathrm{W}}(a \mid s,\tilde{f}) \quad + \sum_{m \in \mathrm{M}^*} c(m(s,f))$$

$\Pr_{\mathrm{U}}(i \mid s,f)$ denotes the probability of occurrence (DoB) of an incident caused by d on s via *f*. $\Pr_{\mathrm{W}}(a \mid s,f)$ is the probability of occurrence (DoB) of an attack of d on s via f.

The first summand of R_s corresponds with the risk relating to safety, the second quantifies the risk relating to security and the third addend numeralizes the costs of deployed measures *m*. Thus, R_s unites the rating of safety and security and also considers the efforts for reducing the risk.

Compared to statistical decision theory [1], additionally to the classical risk factors probability and cost, with p_{V}, which models the vulnerability, a third factor comes into play. This is in accordance with the approaches in [7] and [8] whereas we formulate this third factor as a conditional DoB-density, so that compliance with probability theory is preserved. E.g. $p_{\mathrm{V}}(\beta\,|\,i,s,f)\cdot \Pr_{\mathrm{U}}(i\,|\,s,f)$ is equal to the joint DoB-density $p(i,\beta\,|\,s,f)$ for the occurrence of an incident i with success β given s, f.

Only if an attacker coincidentally has motivation, power and occasion, he will undertake an attack. Therefore, $\Pr_{\mathrm{W}}(a\,|\,s,f)$ is modelled with a product of three DoB factors: $\Pr_{\mathrm{W}} = \Pr_{\mathrm{Motivation}}\cdot \Pr_{\mathrm{Power}}\cdot \Pr_{\mathrm{Occasion}}$.

$\tilde{f} := \arg\max_{f\in \mathrm{F}_s}\{\max_{a\in \mathrm{A}_d}\{U_d(a,s,f)\}\}$ is the most beneficial flank of vulnerability of s from the viewpoint of the attacker d.

To quantify the awaited benefit for the attacker d perpetrating an attack a on s via f, the utility $U_d(a,s,f)\in[U_{\min,\,d},\,U_{\max,\,d}]$ is modelled as:

$$U_d(a,s,f) := \int_0^1 g(s,f,\beta)\cdot p_{\mathrm{Success}}(\beta\,|\,a,s,f)\,\mathrm{d}\beta \;-c_{\mathrm{Effort}}(a,s,f)$$

$$-\int_0^1 c_{\mathrm{Penalty}}(s,f,\beta)\cdot \Pr(\mathrm{Penalty}\,|\,s,f,\beta)\cdot p_{\mathrm{Success}}(\beta\,|\,a,s,f)\,\mathrm{d}\beta$$

$$U_d(a,s,f) = \int_0^1\left[g(s,f,\beta)-c_{\mathrm{Penalty}}(s,f,\beta)\Pr(\mathrm{Penalty}\,|\,s,f,\beta)\right]p_{\mathrm{Success}}(\beta\,|\,a,s,f)\,\mathrm{d}\beta$$

$$-c_{\mathrm{Effort}}(a,s,f)$$

whereupon $c_{\mathrm{Effort}}(a,s,f)\le b(d)$ holds. Obviously, it is straight forward to apply the risk modelling approach also to sets S of subjects s of protection who are endangered by D. In this case, the risk simply can be calculated by summing over S: $R_{\mathrm{S}} = \sum_{s\in \mathrm{S}} R_s$.

2.4 Introduction of Temporal Dynamics

Up to now, all quantifies have been treated as they were constants relating to a time interval of duration T. In order to cover real world problems, it is necessary to equip the approach with a time dependency. If, for example, a measure m is implemented to improve the security level of s, this will influence the behavior of an intelligent opponent d. Within a longer time period T this would couple the different quantities implicitly and would make the interplay between s and d obscure.

A straight forward approach is to model all quantities as time series. An upper index $k\in\mathbb{N}_0$ denotes the discrete instant of time. Additionally, a transition operator Φ^k is introduced that maps the relevant quantities from time step k to $k{+}1$.

$$\left(b^k(s),m^k,\ldots,p_V^k,\Pr_{\mathrm{U}}^k,\Pr_{\mathrm{W}}^k,R_s^k,U_d^k\right)\xrightarrow[\Phi^k]{}\left(b^{k+1}(s),m^{k+1},\ldots,p_V^{k+1},\Pr_{\mathrm{U}}^{k+1},\Pr_{\mathrm{W}}^{k+1},R_s^{k+1},U_d^{k+1}\right)$$

It is assumed that the time discretization is fine enough to keep pace with the dynamics of the modelled system, so that all quantities can be assumed to remain constant within a time step k.

For example, the influence of a security measure m^k implemented at time k on $b\,(s), p_V, \Pr_{\mathrm{W}}, R_s$ and U_d is modelled by the change from $b^k(s), p_V^k, \Pr_{\mathrm{W}}^k, R_s^k$ and U_d^k to $b^{k+1}(s), p_V^{k+1}, \Pr_{\mathrm{W}}^{k+1}, R_s^{k+1}$ and U_d^{k+1} accomplished by the transition operator Φ^k.

3 CONCLUSIONS, CHALLENGES, AND SUMMARY

Based on a role concept we have introduced a mathematical framework that allows to model the risk of a subject of protection with respect to safety as well as with respect to security in a unified manner. The roles and quantities have clear semantics, which is a helpful prerequisite to determine the model parameters quantitatively, if the framework is applied to real problems. Nevertheless, in practice it is very challenging to estimate the involved quantities with sufficient precision. Especially the estimation the different probabilities is far from trivial. If attacks or incidents occur very seldomly, frequently there is not enough data available to perform a standard statistical analysis. The only way out is to adopt the wider interpretation of probabilities as degrees of belief (DoB). Within the Bayesian statistics this is the usual semantics of probability. It allows in the extreme case to use probabilities to express subjective beliefs of an agent [5], as long as the syntactic rules for the calculation with probabilities, i.e. Kolmogorov's axioms, are not violated.

The quantitative formulation of the risk of the subjects of protection and of the utility of attackers should allow to run simulations, e.g. Monte Carlo or agent based simulations, in order to compute the risk numerically and to generate plausible event sequences according to a simulated game between instances of the introduced roles.

Future work will be focused on methods to estimate the parameters of the model and to apply the approach to real world safety and security tasks. Furthermore, we strive for an UML-based conceptualization of all terms of the model according to the ideas proposed in [9] and [10]. The further development of the modelling approach will be especially pursued within the working group "*Themennetzwerk Sicherheit*" of the German National Academy of Science and Engineering *acatech*.

REFERENCES

[1] Berger, J.O.: *Statistical Decision Theory and Bayesian Analysis*. Springer (1993).

[2] Buldas, A.; Laud, P.; Priisalu, J.; Saarepera, M.; Willemson, J.: *Rational Choice of Security Measures via Multi-Parameter Attack Trees*. In: Critical Infrastructures Security, Lecture Notes in Computer Science Vol. 4347, pp. 235-248, Springer (2006).

[3] Beyerer, J.; Geisler, J.; Dahlem, A.; Winzer, P.: *Sicherheit: Systemanalyse und -design*. In: Winzer, P.; Schnieder, E.; Bach, F. (Hrsg.): Sicherheitsforschung – Chancen und Perspektiven. pp. 39-72, Springer (2009).

[4] Beyerer, J.: *Sicherheitstechnik, Sicherheitssysteme und Sicherheitsforschung – Aktuelle Herausforderungen*. In: Stober, R.: Sicherheitsgewerbe und Sicherheitstechnik – Von der Personalisierung zur Technisierung – 9. Hamburger Sicherheitsgewerberechtstag, pp. 1-10. Carl Heymanns Verlag (2009).

[5] Bernardo, J.M.; Smith, A.F.M.: *Bayesian Theory*. Wiley (1994).

[6] Beyerer, J.: *Verfahren zur quantitativen statistischen Bewertung von Zusatzwissen in der Meßtechnik*. VDI Fortschritt-Berichte, Reihe 8, Nr. 783, VDI Verlag, Düsseldorf (1999).

[7] Baker, G.: *A Vulnerability Assessment Methodology for Critical Infrastructure Sites*. DHS Symposium: R&D Partnerships in Homeland Security. Boston (2005).

[8] Broder, J.F.; Tucker, E.: *Risk Analysis and the Security Survey*. 4th ed. Waltham, MA, USA : Butterworth-Heinemann (2012).

[9] Schnieder, E.; Schnieder, L.: *Verkehrssicherheit – Maße und Modelle, Methoden und Maßnahmen für den Straßen- und Schienenverkehr*. Springer (2013).

[10] Schnieder, E.; Schnieder, L.: *Präzisierung des Normativen Sicherheitsbegriffs durch Formalisierte Begriffsbildung*. In: Winzer, P.; Schnieder, E.; Bach, F. (Hrsg.): Sicherheitsforschung – Chancen und Perspektiven. pp. 73-115, Springer (2009).