Eur J Secur Res (2016) 1:135–150
DOI 10.1007/s41125-016-0008-y

ORIGINAL ARTICLE

A Framework for a Uniform Quantitative Description of Risk with Respect to Safety and Security

Jürgen Beyerer[1,2] · **Jürgen Geisler**[1]

Received: 29 August 2016 / Accepted: 6 September 2016 / Published online: 7 October 2016

Abstract A mathematical framework is presented that describes risk in the context of safety and security problems quantitatively and in an integrative way. Great importance is laid on a clear notation with a sound semantics. Essentially, this seminal contribution is a substantially expanded version of our short paper "*A quantitative risk model for a uniform description of safety and security*", which we presented to the 10th Future Security 2015 in Berlin (A quantitative risk model for a uniform description of safety and security. In: Proceedings of the 10th Future security—security research conference, pp 317–324, 2015). The key concept of this paper is a quantitative formulation of risk. Uncertainties are modelled based on probability distributions. Risk due to purely stochastic sources of danger is based on objective notions of probabilities and costs whereas risks of individuals (intelligent agents) are described from their own points of view, i.e. in a fully subjective manner, since individuals draw their decisions based on their subjective assessments of potential costs and of frequencies of event occurrence. Therefore, probability is interpreted in a Bayesian context as a degree of belief (DoB). Based on a role model for the involved agents with the three roles »source of danger«, »subject of protection« and »protector«, risk is modelled quantitatively using statistical decision theory and game theory. 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

✉ Jürgen Beyerer
juergen.beyerer@iosb.fraunhofer.de

Jürgen Geisler
juergen.geisler@iosb.fraunhofer.de

[1] Fraunhofer Institute of Optronics, System Technologies, and Image Exploitation IOSB, Fraunhoferstr. 1, 76131 Karlsruhe, Germany

[2] Institute of Anthropomatics and Robotics, Karlsruhe Institute of Technology KIT, Adenauerring 4, 76131 Karlsruhe, Germany

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. Two approaches for determining DoBs, the Maximum Entropy Principle (MEP) and the Conditioning On Rare Events (CORE), are presented and discussed. The model can be used to simulate and evaluate the endangerment of subjects of protection quantitatively, e.g. using a software agent implementation, where the agents are endowed with the cost functions and the DoBs of the presented framework.

Keywords Agents · Safety · Security · Risk · Bayesian statistical decision theory · Game theory · Degree of belief · Role model · Vulnerability · Flanks of vulnerability · Subjective and objective cost functions and probabilities · Maximum entropy principle

1 Introduction

Safety and security share many 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.

2 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 (Berger 1993). In combination with attack trees, game theory has been already applied to model rational attackers (Buldas et al. 2006). Some aspects of the approach presented in this paper have been already proposed in a preliminary qualitative formulation in Beyerer et al. (2009) and Beyerer (2009).

3 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.

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

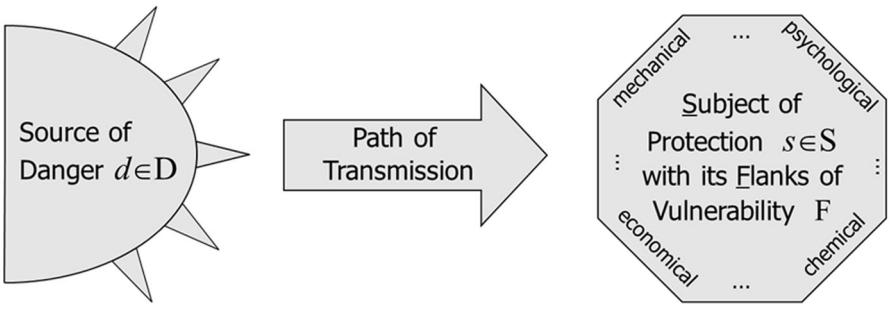

Fig. 1 Relation between a source of danger d and subject of protection s. D and S denote the sets of sources of danger and the set of subjects of protection, respectively

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). Figure 2 illustrates this categorization.

From a game theoretic point of view there is another interesting interpretation of safety and security (Beyerer et al. 2009). With respect to safety the subject of protection *s* plays a game against nature (see Fig. 3). 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. The protection process can converge (see Figure 2, on the right).

In contrast, regarding security, the adversary behaves intelligently (see Fig. 4). 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. The protection process oscillates necessarily (see Fig. 2, on the left).

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 most promising for him to achieve his goal.

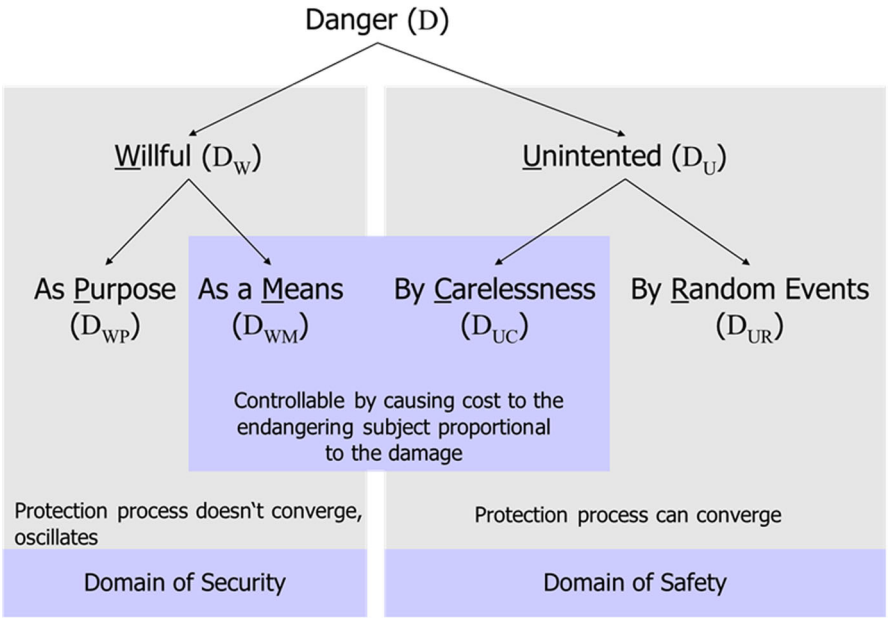

Fig. 2 Categorization of dangers with respect to safety and security. $d \in D_W$ are called "attackers" and $d \in D_U$ are called "causers". In the cases of an attacker $d \in D_{WM}$ or a causer $d \in D_{UC}$ the pertaining risk can be influenced by costs charged to *d* (penalties, money,…), so that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

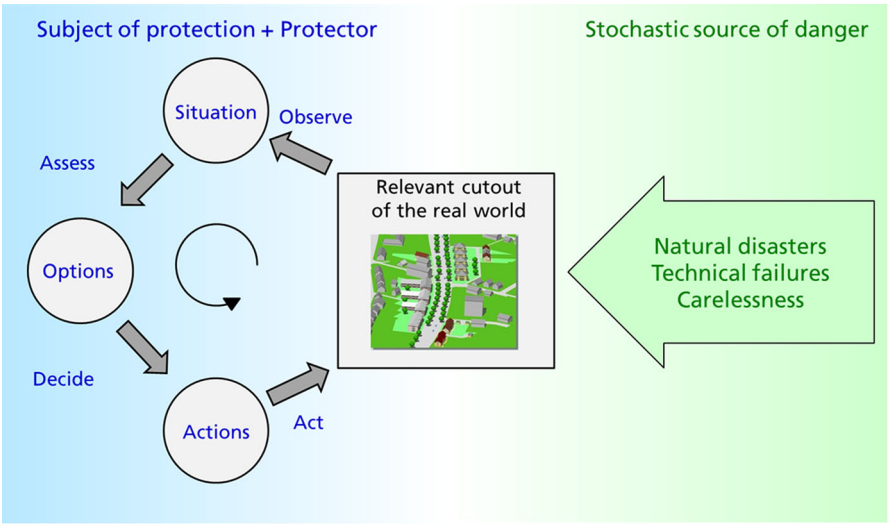

Fig. 3 Game theoretic view on safety

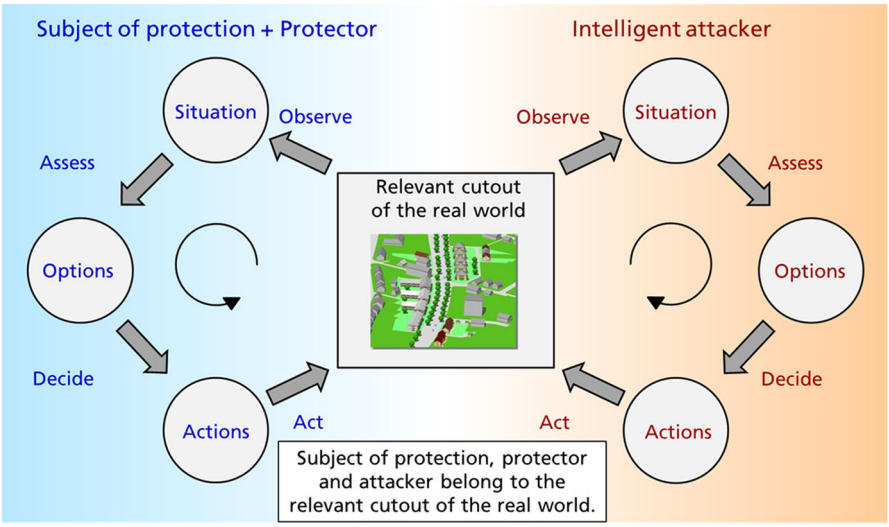

Fig. 4 Game theoretic view on security

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). For example, 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.

4 Role and Risk Model

4.1 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. 5): 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. 5 it should be made clear, that except for unintended danger by random events (see Figs. 2, 3) there is always some flow of value from *s* to *d*. That is expressed by the relation *s* »enriches« *d*.

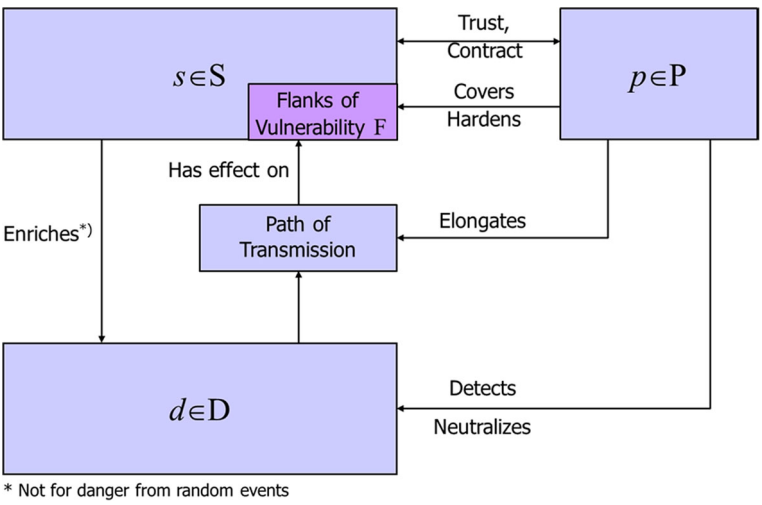

Fig. 5 Roles and relations between them. Note that the different roles can be played by different entities but coincidences are also possible. For example, someone can be a danger for himself or someone can protect himself

4.2 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 (Berger 1993).

4.2.1 Degree of Belief Interpretation of Probabilities

Following the compellent argumentation of (Lindley 1982) all uncertainties are modelled based on the probability calculus.

In this paper, 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 (Bernardo and Smith 1994; Beyerer 1999).

Figure 6 illustrates this concept. The famous axioms of Kolmogorov formally define the syntax of probability as a measure theoretic concept. But they only determine how to calculate with probabilities in a sound manner, i.e. they only determine the syntax of probabilistic calculations. They do not explain the meaning of probability. Indeed, to a formal system like Kolmogorov's axioms multiple interpretations (i.e. multiple semantics) can coexist as long as they are consistent with the axioms (Hofstadter 1979).

One the one hand, there is the frequentistic interpretation of probability. Probability here is treated like a physical quantity that can be measured by performing experiments; at least thought experiments should be conceivable for this endeavor. For example, if a die is given and the probabilities for its six numbers should be determined, the die can be thrown N times and the relative frequencies of the numbers can be used as estimates for the pertaining probabilities. If N goes to infinity, the law of big numbers guaranties that the relative frequencies converge to the probabilities.

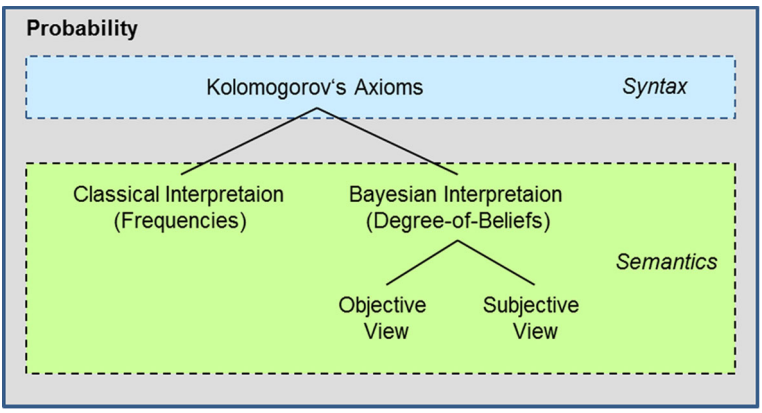

Fig. 6 Different meanings of probability

On the other hand, if someone is asked about the probability of life on Mars, after some intensive considerations his answer could be: 0.0001 or maybe 0.5 for example. Obviously, these answers have no frequentistic meaning (Lehner et al. 1996). Either there is life on Mars or not. The point is, it is unknown. No repeated experiment, even no reasonable thought experiment, is conceivable in which trails can be performed in order the count the cases in which there was life on Mars or not.

The first answer 0.0001 could be the result of some thorough considerations about the physical conditions on Mars and their consequences for the existence of biological life. It quantifies an individual belief. The second answer 0.5 could express that there is no idea about the possibility of life on Mars at all and therefore expresses complete ignorance (Lehner et al. 1996). Again, it quantifies a belief, or to be more specific, a degree of belief (DoB). DoBs are consistent with the axioms of Kolmogorov and furthermore generalize the frequentistic interpretation. If a frequentistic experiment can be performed and relative frequencies are calculated, of course this result can be adopted as DoB, which in this special case is determined empirically.

DoBs can be subdivided into objective and subjective DoBs. In the first case, given evidence is transformed into DoBs in an objective way so that two individuals faced with the same facts and having the same knowledge would derive the same DoB. In the latter case, each individual can derive its own subjective DoBs about all relevant factors.

Objective DoBs are of special interest, because there are well understood approaches to establish DoBs individually in an impartial way such as, e.g. the Maximum Entropy Principle (MEP) (Jaynes 1968); see also Sect. 4.4 for more details. It takes all given facts and knowledge as constraints and calculates that DoB which has the maximum entropy by simultaneously fulfilling all constraints. MEP–DoBs therefore are minimum prejudiced and do not implicitly introduce any additional assumptions i.e. no additional bias. If risk is to be quantified from an objective point of view, the MEP is a suitable approach for importing given facts and knowledge formally into DoBs and thus into the probability calculus.

On the other hand, subjective DoBs allow that each agent within a scenario has his own point of view and his own belief about the probabilities of events and realizations of variables. Individual beliefs may differ very much from one individual to other individuals and also may strongly deviate from objective DoBs. But the decisions of each agent clearly depends on that the agent's beliefs. For example, if an agent intends to commit a burglary in a house, he evaluates his personal risk based on his subjective DoBs about vulnerability and the probabilities of being successful and being caught and punished, instead of considering the objective, to him usually unknown values of those quantities.

4.2.2 Subjects of Protection, Sources of Danger and Protectors

All quantities relate to a particular time interval of length T, within which they are assumed to remain constant.

$$\mathrm{S} = \mathrm{S}_{\text{Persons}} \cup \mathrm{S}_{\text{Objects}} \cup \mathrm{S}_{\text{Systems}} \cup \mathrm{S}_{\text{Legal interests}}, \tag{1}$$

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

$$\mathrm{D} = \mathrm{D}_{\mathrm{WP}} \cup \mathrm{D}_{\mathrm{WM}} \cup \mathrm{D}_{\mathrm{UC}} \cup \mathrm{D}_{\mathrm{UR}}, \tag{2}$$

where the indices have the following meaning: WP is the willful danger as a purpose (vandalism, amok,), WM is the willful danger as a means (burglary, robbery, …), UC is the unintended danger due to carelessness or negligence (inattention, breach of duty), UR is the unintended danger with random characteristic (technical failures, natural disasters).

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

In the following $d \in \mathrm{D}_{\mathrm{W}}$ 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 $d \in \mathrm{D}_{\mathrm{U}}$ due to carelessness generate incidents i, which are pooled in set of incidents I, $i \in \mathrm{I}$. In the following $d \in \mathrm{D}_{\mathrm{U}}$ are called »causers«, because they cause incidents. The set of incidents referred to a causer $d \in \mathrm{D}_{\mathrm{U}}$ 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 $\beta \in [0, 1]$. $\beta = 1$ denotes total success and $\beta = 0$ stand for no success at all.

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. $p_{\mathrm{V}}(\beta|i,s,f)$ and $p_{\mathrm{V}}(\beta|a,s,f)$ describe the DoB-densities for the degree of success β, if a respectively i hits s via f (see Fig. 7).

Remark In the case that the costs $c(s,f,\beta)$ are proportional to the success β, i.e.

$$c(s,f,\beta) = \beta \times c(s,f), \tag{3}$$

costs and vulnerability can be factorized:

$$\int_0^1 c(s,f,\beta) \times p_V(\beta|i,s,f)\mathrm{d}\beta = c(s,f) \times v(s,f,i), \tag{4}$$

where

$$v(s,f,i) := E_{\beta|i,s,f}\{\beta\} = \int_0^1 \beta \times p_{\mathrm{V}}(\beta|i,s,f)\mathrm{d}\beta, \tag{5}$$

is the mean success-DoB of an incident i.

Causers of danger due to carelessness $d \in \mathrm{D}_{\mathrm{UC}}$ are charged with costs $\kappa(s, f, \beta) \in [0, \kappa_{d\_\mathrm{Ruin}}]$. These costs correspond to a penalty for d for generating

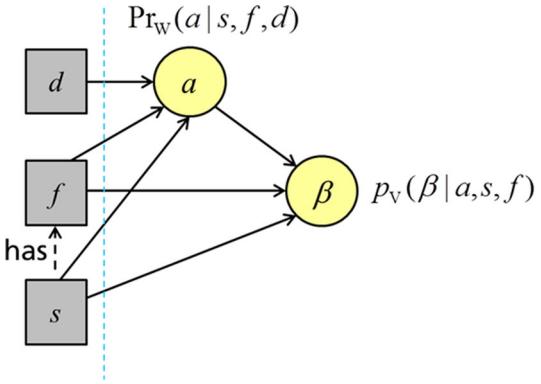

Fig. 7 Vulnerability is modeled the by the DoB-density of the success β of a certain attack a on the subject of protection s via its flank of vulnerability f [with the discrete probability $\Pr_w$ for a willful threat; see Eq. (11)]. Thus the vulnerability does not depend on the source of danger but only on the attack a, that an attacker d performs. Analogously, the same holds if attackers are replaced by causers $d \in \mathrm{D_U}$ and attacks by incidents i

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

4.3 Quantification of Risk

The total risk $R_{\mathrm{s\_total}}$ of a subject of protection s from the point of view of s can be expressed as:

$$R_{s\_\mathrm{total}} := \underbrace{R_{\mathrm{s}}}_{\text{Model}} + \underbrace{R_0}_{\text{Outside modelling scope}} \tag{6}$$

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.:

$$\Delta R_{s\_\text{absolut}}(m) := R_{s\_\text{absolut}}(\text{without } m) - R_{s\_\text{absolut}}(\text{with } m) \geq 0 \tag{7}$$

with

$$\Delta R_{\text{s}}(m) := R_{\text{s}}(\text{without } m) - R_{\text{s}}(\text{with } m) > 0. \tag{8}$$

The risk R_{s} of s from the point of view of s can be expressed as:

$$\begin{aligned} R_{\text{s}} = & \sum_{d \in \text{D}_{\text{U}}} \sum_{i \in \text{I}_d} \sum_{f \in \text{F}_s} \int_0^1 c(s,f,\beta) \times p_{\text{V}}(\beta|i,s,f)\text{d}\beta \times \Pr_{\text{U}}(i|s,f) \\ & + \sum_{d \in \text{D}_{\text{W}}} \sum_{a \in \text{A}_d} \int_0^1 c(s,\tilde{f},\beta) \times p_{\text{V}}(\beta|a,s,\tilde{f})\text{d}\beta \times \Pr_{\text{W}}(a|s,\tilde{f}) + \sum_{m \in \text{M}^*} c(m(s,f)), \end{aligned} \tag{9}$$

$\Pr_{\text{U}}(i|s,f)$ denotes the probability of occurrence (DoB) of an incident caused by d on s via f. $\Pr_{\text{W}}(a|s,f)$ 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 (Berger 1993), 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 (Baker 2005) and (Broder and Tucker 2012) whereas we formulate this third factor as a conditional DoB-density, so that compliance with probability theory is preserved. For example,

$$p_{\text{V}}(\beta|i,s,f) \times \Pr_{\text{U}}(i|s,f), \tag{10}$$

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, $\Pr_{\text{W}}(a|s,f)$ is modelled with a product of three DoB factors:

$$\Pr_{\text{W}} = \Pr_{\text{Motivation}} \times \Pr_{\text{Power}} \times \Pr_{\text{Occasion}}, \tag{11}$$

$$\tilde{f} := \arg\max_{f \in \text{F}_{\text{s}}} \{\max_{a \in \text{A}_{\text{d}}} \{U_d(a,s,f)\}\}, \tag{12}$$

denotes 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 $U_d(a,s,f) \in [U_{\text{min, d}},\ U_{\text{max, d}}]$ is modelled as:

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

$$U_d(a,s,f) = \int_0^1 \left[g(s,f,\beta) - c_{\text{Penalty}}(s,f,\beta) \times \Pr(\text{Penalty}|s,f,\beta)\right] \times p_{\text{Success}}(\beta|a,s,f)\,\mathrm{d}\beta - c_{\text{Effort}}(a,s,f), \tag{13}$$

whereupon $c_{\text{Effort}}(a,s,f) \leq b(d)$ 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 :$R_S = \sum_{s\in S} R_s$.

4.4 Determination of Probabilities

The crucial challenge of the presented framework is the determination of probabilities, or to be more specific, the DoBs which are constituents of the risk terms. This is especially difficult, if the probabilities are very low, so that there are not enough data to estimate the DoBs with statistical methods. From a methodological point of view, there are different options how to manage this task.

4.4.1 Maximum Entropy Principle (MEP)

To define the DoBs in an objective manner, the Maximum Entropy Principle (MEP) can be applied (Jaynes 1968). Shannon's entropy

$$H := \sum_{\omega\in\Omega} -\Pr(\omega)\log(\Pr(\omega)), \tag{14}$$

in the discrete case and the differential entropy

$$h := \int_{\omega\in\Omega} -p(\omega)\log(p(\omega))\mathrm{d}\omega, \tag{15}$$

for continuous variables ω quantify the concentration of the DoB on the definition set ω. The lower the concentration the higher is the pertaining entropy. Without any constraint that DoB-distribution with constant DoB values for each $\omega \in \Omega$ achieves the maximum entropy. If we know any facts about $\omega \in \Omega$, those facts are employed as constraints with respect to which the DoB with maximum entropy is calculated. Thus, the resulting DoB maps the given facts into the probabilistic calculus in a way that avoids any additional implicit assumptions. Therefore, the MEP–DoB is impartial beyond the evidence of the considered facts.

The adoption of the MEP can be strongly justified by a set of axioms, from which the MEP can be derived unambiguously (Paris 1999). The axioms are formulated generally understandably and can be considered as commonsense reasoning principles. According to (Beierle et al. 2015) these principles are:

1. *Irrelevant information principle*: knowledge that is entirely irrelevant to the problem under consideration can be ignored.
2. *Renaming principle*: renaming all variables used to describe the problem does not influence the choice of the best model.
3. *Obstinacy principle*: receiving information that is already known is redundant and does not change the best model.
4. *Equivalence principle*: if two knowledge bases are semantically equivalent according to the axioms of probability theory, they should have the same best model.
5. *Relativization principle*: probabilistic knowledge about an event is not affected by knowledge that assumes that the event has not happened.
6. *Weak independence principle*: if two events A and B cannot occur together, then probabilistic knowledge about B does not affect the chosen probability for any event that happens together with A.
7. *Continuity*: very small changes in the factual probabilistic knowledge of the given probabilistic knowledge base can only result in very small changes in the resulting probabilities of the best model.

Best model means the probability distribution that is compliant to all given facts (i.e. to the above mentioned probabilistic data base) and compliant to the axioms (a)–(g). A rational agent (individual, reasoner) who uses probabilities and complies with these principles should choose the MEP to determine his probability distributions (Beierle et al. 2015).

4.4.2 Conditioning on Rare Events (CORE)

To cope with the problem to determine probabilities of extremely rare events (incidents or attacks) the estimation and/or assessment of them could also be completely omitted and risk could be formulated conditionally. I.e. for each event risk is expressed under the condition that an event i or a has occurred. Given e.g. an incident i has occurred the first summand of Eq. (9) changes to

$$\sum_{f \in \mathrm{F_s}} \int_0^1 c(s,f,\beta) \times p_{\mathrm{V}}(\beta | i,s,f) \mathrm{d}\beta, \tag{16}$$

and constitutes then a component to the conditional risk $R_s | \, i$.

4.5 Subjective Views of Agents

Objective cost functions and probabilities of occurrence must be clearly distinguished from subjective assessments of those quantities. A rational agent draws his decisions according to his subjective view, i.e. to his belief about costs in the case an incident or an attack would happen and about his DoBs with respect to the probability of occurrence. According to (Mainzer 2016), (Tversky and Kahnemann 2000) individuals rate costs and probability of occurrence with a cognitive bias. On the one hand the probabilities of very infrequent events are

usually overestimated and those of very frequent events are underestimated. On the other hand also the costs are distorted in a nonlinear manner, because an increment of costs is rated relatively to the absolute cost level, which approximately leads to a logarithmic scale and therefore to a strong flattening of the subjective cost functions for higher values. Furthermore, the readiness to assume risk, or otherwise, the risk aversion of an individual introduce asymmetries for positive and negative costs (i.e. profit). If $c_{\text{objective}}$ and $p_{\text{objective}}$ are the objective costs and objective probabilities respectively, the transition to subjective costs, subjective probabilities (DoBs) and thus to subjective risk can be accomplished mathematically using value functions $\upsilon(.)$ and $\pi(.)$:

$$c_{\text{subjective}} = \upsilon(c_{\text{objective}}), \tag{17}$$

$$p_{\text{subjective}} = \pi(p_{\text{objective}}), \tag{18}$$

$$R_{\text{subjective}} = \Psi\{\upsilon(c_{\text{objective}})\pi(p_{\text{objective}})\}, \tag{19}$$

where $\Psi\{.\}$ denotes an ensemble functional like, e.g. an integral or a selection operator. Within the presented framework, quantities from the point of view of an individual are always are to be understood as subjective quantities. In the case of probabilities the notion of DoB encapsulates the individual assessment of the frequency of events as well as the individual's cognitive bias.

4.6 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 $k + 1$.

$$(b^k(s), m^k, \ldots, p_{\text{V}}^k, \text{Pr}_{\text{U}}^k, \text{Pr}_{\text{W}}^k, R_s^k, U_d^k) \underset{\Phi^k}{\rightarrow} (b^{k+1}(s), m^{k+1}, \ldots, p_{\text{V}}^{k+1}, \text{Pr}_{\text{U}}^{k+1}, \text{Pr}_{\text{W}}^{k+1}, R_{\text{s}}^{k+1}, U_d^{k+1}). \tag{20}$$

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_{W}, R_{s} and U_{d} is modelled by the change from $b^k(s)$, p_V^k, Pr_{W}^k, R_s^k and U_d^k to $b^{k+1}(s)$, p_V^{k+1}, $\text{Pr}_{\text{W}}^{k+1}$, R_s^{k+1} and U_d^{k+1} accomplished by the transition operator Φ^k.

5 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 of the different probabilities is far from trivial. If attacks or incidents occur very seldom, 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 (Bernardo and Smith 1994), 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 a UML-based conceptualization of all terms of the model according to the ideas proposed in Schnieder and Schnieder (2009, 2013). 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

Baker G (2005) A vulnerability assessment methodology for critical infrastructure sites. In: DHS symposium. R&D Partnerships in Homeland Security, Boston

Beierle C, Kern-Isberner G, Finthammer M, Potyka N (2015) Extending and completing knowledge and beliefs without bias. In: Künstliche Intelligenz, Band 29, Heft 3, pp 255–262, Springer, Heidelberg

Berger JO (1993) Statistical decision theory and bayesian analysis. Springer, New York

Bernardo JM, Smith AFM (1994) Bayesian theory. Wiley, Chichester

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

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

Beyerer J, Geisler J (2015) A quantitative risk model for a uniform description of safety and security. In Beyerer J, Meissner A, Geisler J (eds) Proceedings of the 10th Future security—security research conference, pp. 317–324, Berlin, 15th to 17th September 2015, Fraunhofer Verlag, Stuttgart

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

Broder JF, Tucker E (2012) Risk analysis and the security survey, 4th edn. Butterworth-Heinemann, Waltham

Buldas A, Laud P, Priisalu J, Saarepera M, Willemson J (2006) 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

Hofstadter DR (1979) Gödel, escher, bach: an eternal golden braid. Basic Books Inc., New York

Jaynes ET (1968) Prior probabilities. IEEE Trans Syst Sci Cybern 4(3):227–241

Lehner PE, Laskey KB, Dubois D (1996) An introduction to issues in higher order uncertainties. In: IEEE transactions on systems, man, and cybernetics—part a: systems and humans, 26, No. 3, pp. 289–293

Lindley DV (1982) Scoring rules and the inevitability of Probability. Int Stat Rev 50:1–26

Mainzer K (2016) Künstliche Intelligenz—Wann übernehmen die Maschinen?. Springer, Heidelberg Berlin

Paris J (1999) Common sense and the maximum entropy. Synthese 117:75–99

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

Schnieder E, Schnieder L (2013) Verkehrssicherheit—Maße und Modelle. Springer, Methoden und Maßnahmen für den Straßen- und Schienenverkehr

Tversky A, Kahnemann D (2000) Advances in prospect theory: cumulative representation of uncertainty. In: Kahnemann D, Tversky A (eds) Choices, values and frames. Cambridge University Press, Cambridge, pp 44–66