Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB

Beitrag zur Formulierung einer

„Querschnittstheorie Sicherheit“

Prof. Dr.-Ing. habil. Jürgen Beyerer

Leipzig, 04. Dezember 2015


Ettlingen


Karlsruhe


Ilmenau


Lemgo

© Fraunhofer IOSB

Sicherheit

- Multidisziplinär: Technik-, Rechts-, Geistes- und Sozialwissenschaften
  → Keine gemeinsame, durchgängige Sprache
- Vielschichtig: Safety, Security, Zuverlässigkeit
- Komplex: Extrem große Konfigurations- und Zustandsräume

Es fehlt eine abstrakte Rückgratwissenschaft für die Sicherheit zur:

- Formalen Beschreibung (Deskription)
- Analyse
- Synthese (Design)
- Optimierung

der Sicherheit komplexer Systeme.

© Fraunhofer IOSB

Was kann eine solche Theorie der Sicherheit leisten?

- Disziplinenübergreifendes Verständnis und Behandlung komplexer Sicherheitsfragestellungen.
- Herausarbeitung und Bereitstellung technologieunabhängiger Grundtatsachen und Wirkungsmechanismen.
- Beherrschung der Komplexität realer Sicherheitsaufgaben.
- Abdeckung von *Safety* und *Security*.
- Quantifizierung der Risikominderung durch Schutzmaßnahmen
  → Quantifizierung von Resilienz
- Quantitativer, optimaler Entwurf von Sicherheitssystemen

© Fraunhofer IOSB

Spieltheoretische Sicht auf Safety und Security

„Safety“ »Spiel gegen den Zufall«

→ Stochastisch eintretende Schadensereignisse
→ Statistische Analyse der Gefährdung
→ Passive Maßnahmen reichen oft aus.

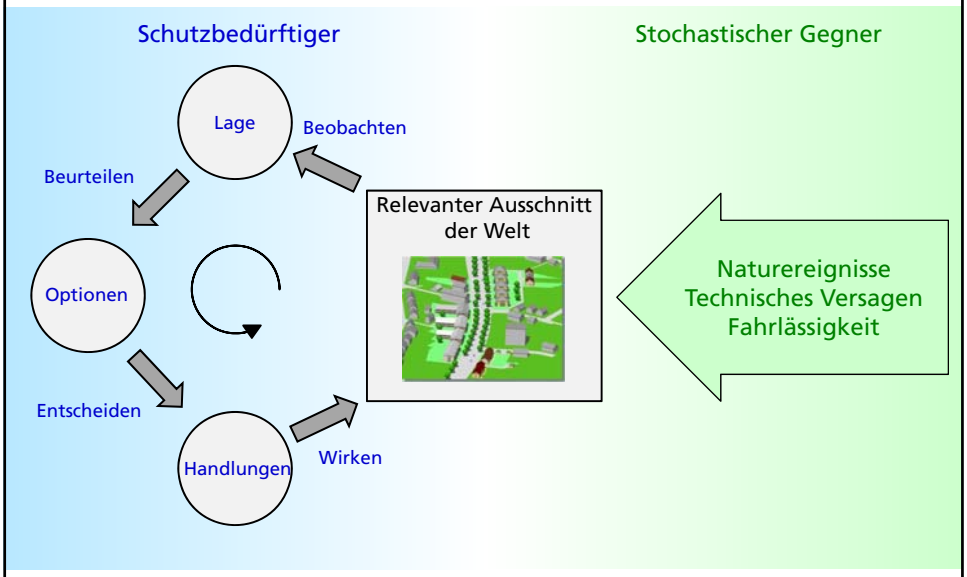
„Security“ »Spiel gegen die Absicht«

→ Gegner entzieht sich dem Verstandenwerden, handelt taktisch.
→ Auf Maßnahmen folgen Gegenmaßnahmen, folgen Maßnahmen, ….. usw.
→ Aktive, d.h. rückgekoppelte, adaptive und lernende Prozesse sind notwendig.

Gewährleistung von Security ist ein dynamischer Prozess!
→ Schutzprozesse werden Regelkreise.

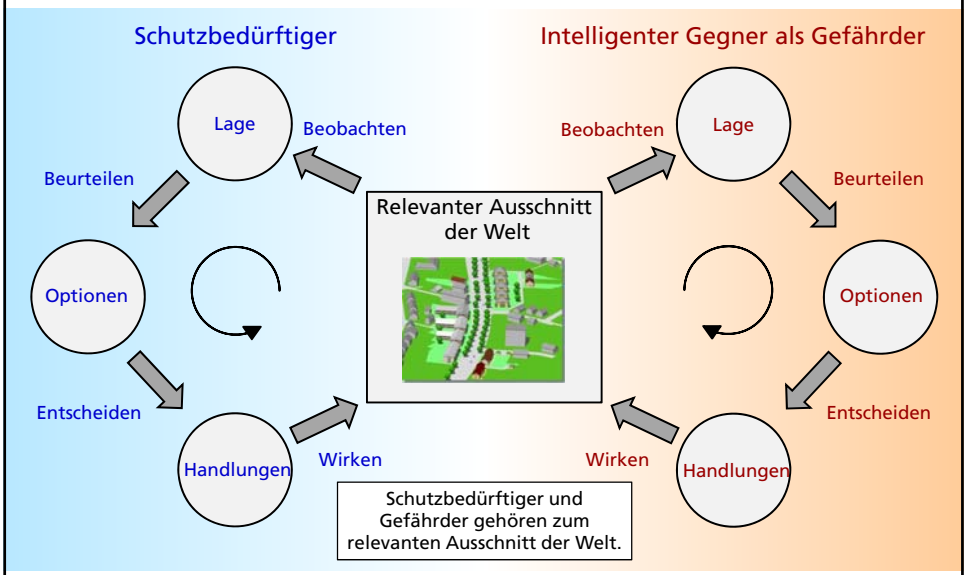
© Fraunhofer IOSB

Spieltheoretische Sicht auf Safety



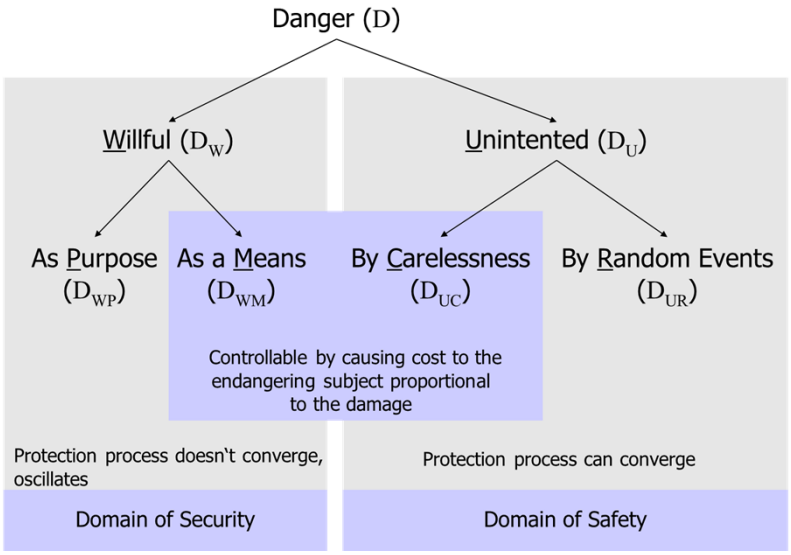
© Fraunhofer IOSB
5
Fraunhofer IOSB KIT

Spieltheoretische Sicht auf Security



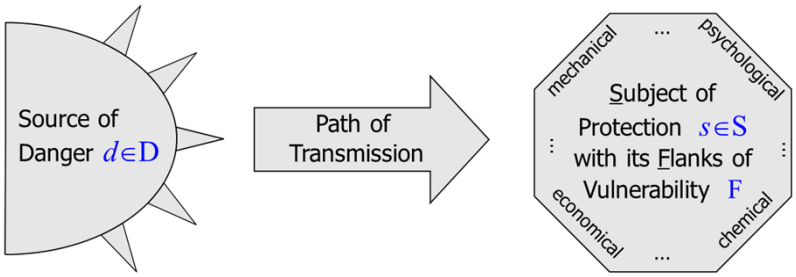
© Fraunhofer IOSB
6
Fraunhofer IOSB KIT

Aufschlüsselung der Gefährdung/Gefährder



© Fraunhofer IOSB

Von der Gefahrenquelle zur Gefahrensenke

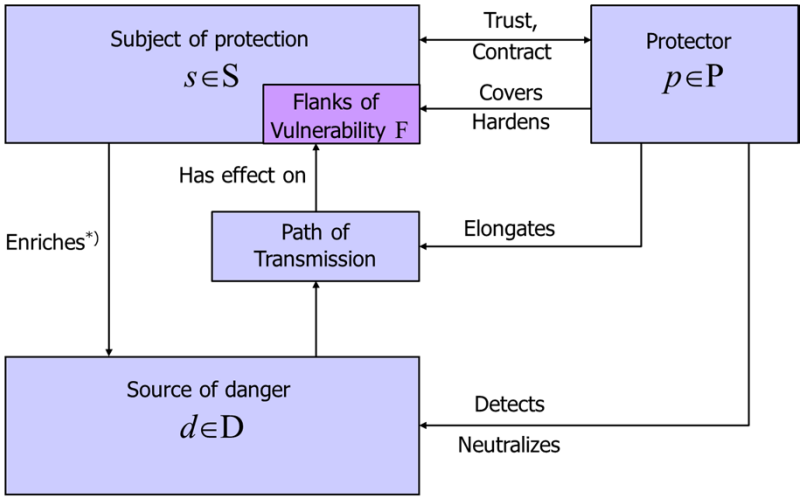


Minimalprinzip der Security:
Die schwächste Flanke ist bestimmend für die Verwundbarkeit.

Safety oder **Security**:
Nur an der Gefahrenquelle unterscheidbar.

© Fraunhofer IOSB

Rollenmodell



* Not for danger from random events

Bemerkung: Unterschiedliche Rollen müssen nicht zwingend getrennte physische Entitäten sein.

© Fraunhofer IOSB

Fraunhofer IOSB KIT Karlsruhe Institute of Technology

Modellierung

Menge D der Gefährder (dangers) d :

$$D = D_{WP} \cup D_{WM} \cup D_{UC} \cup D_{UR}$$

- WP: Willful danger: als Zweck (Vandalismus, Amok, Terrorismus …)
- WM: Willful danger: als Mittel (Diebstahl, Raub, …)
- UC: Unintended danger: aufgrund Fahrlässigkeit (Unachtsamkeit, Pflichtverletzung, …)
- UR: Unintended danger: mit Zufallscharakter (Technisches Versagen, Naturereignisse)

$$D = D_W \cup D_U \qquad D_W := D_{WP} \cup D_{WM} \qquad D_U := D_{UC} \cup D_{UR}$$

Gefährder mit Intention haben ein Budget b:

$$d \mapsto b(d) \quad \text{mit} \quad d \in D_W$$

© Fraunhofer IOSB

Fraunhofer IOSB KIT Karlsruhe Institute of Technology

Modellierung

Gefährder mit Intention $d \in \mathrm{D_W}$ verüben Angriffe (attacks) $a \in \mathrm{A}$

A: Menge der Angriffe (attacks)

A_d: Menge der von d durchführbaren Angriffe

$$\mathrm{A}_d \subseteq \mathrm{A}$$

Unabsichtliche Gefährder $d \in \mathrm{D_U}$ erzeugen Vorfälle (incidents) $i \in \mathrm{I}$

I: Menge der Vorfälle (incidents)

I_d: Menge der durch $d \in \mathrm{D_U}$ verursachbaren Vorfälle

$$\mathrm{I}_d \subseteq \mathrm{I}$$

Der Erfolg eines Angriffs bzw. der Schadensgrad eines Vorfalls wird mit

$$\beta \in [0,1]$$

quantifiziert. $\beta = 0$ bedeutet "Erfolglosigkeit" bzw. "kein Schaden", $\beta = 1$ bedeutet "vollständiger Erfolg" bzw. "vollständiger Schadenseintritt".

© Fraunhofer IOSB

Modellierung

Fahrlässige Gefährder $d \in \mathrm{D_{UC}}$ erleiden durch ihre Vorfälle Kosten κ:

$$\kappa(s, f, \beta) \in [0, \kappa_{\mathrm{Ruin}}(d)]$$

Diese Kosten entsprechen einer Strafe für d bei Verursachung eines Vorfalls, der s über f betrifft und den Schadensgrad β hat.

Annahme:
Je höher diese Kosten, desto geringer die Eintrittswahrscheinlichkeit eines Vorfalls (wirkt als „Abschreckung").

© Fraunhofer IOSB

Modellierung

Menge S der Schutzbedürftigen s :

$$\mathrm{S} = \mathrm{S}_{\text{Personen}} \cup \mathrm{S}_{\text{Objekte}} \cup \mathrm{S}_{\text{Systeme}} \cup \mathrm{S}_{\text{Rechtsgüter}}$$

Schutzbedürftige haben ein Budget:

$$s \mapsto b(s) \quad \text{mit} \quad s \in \mathrm{S}$$

Schutzbedürftige haben Flanken der Verwundbarkeit:

$$f \in \mathrm{F}(s)$$

Angriff auf oder Vorfall an Flanke der Verwundbarkeit f von s mit Erfolgs- bzw. Schadensgrad β kostet s:

$$c(s, f, \beta) \in [0, \infty)$$

© Fraunhofer IOSB

Modellierung

Erfolgs- bzw. Schadensgrad β eines Angriff a auf oder Vorfalls i an Flanke der Verwundbarkeit f von s wird als Zufallsvariable mit den DoB-Dichten

$$p_{\mathrm{V}}(\beta | i, s, f) \quad \text{bzw.} \quad p_{\mathrm{V}}(\beta | a, s, f)$$

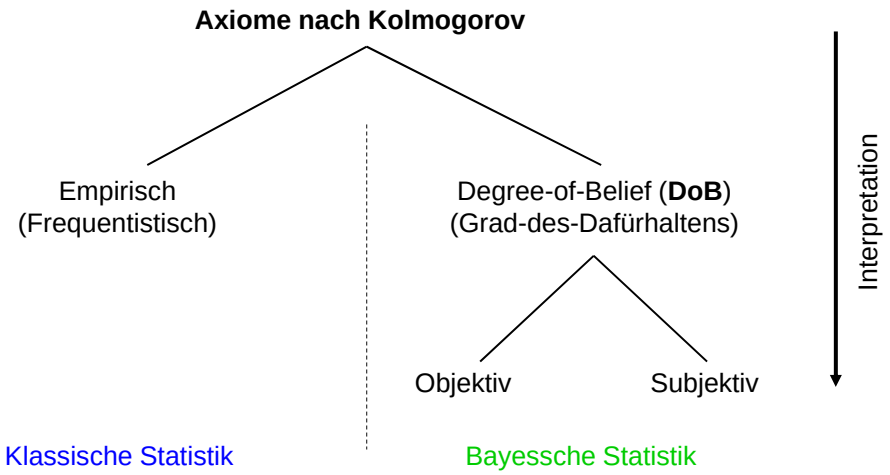
modelliert.

Diese Dichten beschreiben die Vulnerabilität des Schutzbedürftigen s über seine Flanken der Verwundbarkeit.

© Fraunhofer IOSB

Bedeutung von Wahrscheinlichkeit

Mit den Kolmogorov'schen Axiomen verträgliche Interpretationen:

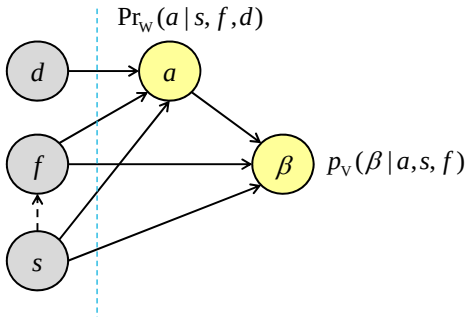


© Fraunhofer IOSB

Modellierung

Die Vulnerabilität wird als eine Eigenschaft des Schutzbedürftigen s modelliert, die vom Vorfall i bzw. vom Angriff a abhängt, aber unabhängig vom Gefährder d ist (bedingte Unabhängigkeit).

Beispiel im Falle eines Angreifers:



$\Pr_W(a \mid s, f, d)$: Wahrscheinlichkeit (DoB) eines Angriffs durch d auf s über f aus Sicht des Schutzbedürftigen.

© Fraunhofer IOSB

Modellierung

Menge P der Schützer liefert Schutzmaßnahmen m für die Flanke f von s:

$$m(s, f) \in \mathrm{M}$$

M: Menge verfügbarer Schutzmaßnahmen.
M^*: Menge implementierter Schutzmaßnahmen.

$$\mathrm{M}^* \subseteq \mathrm{M}$$

Eine Schutzmaßnahmen m kostet:

$$c(m(s, f))$$

Nebenbedingung:

$$\sum_{m \in \mathrm{M}^*} c(m(s, f)) \quad \leq \quad b(s)$$

Annahme: $m(s, f)$ vermindert die Vulnerabilität $p_{\mathrm{V}}(\beta \mid ., s, f)$ und/oder die Eintrittswahrscheinlichkeiten von Angriffen und/oder von Vorfällen. $m(s, f)$ vermindert hingegen nicht $c(s, f, \beta)$.

© Fraunhofer IOSB

Quantifizierung des Risikos

Risiko für den Schutzbedürftigen s:

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

$\mathrm{Pr}_{\mathrm{U}}(i \mid s, f, d)$: Eintrittswahrscheinlichkeit (DoB) eines Vorfalls durch d betreffend s über f.

$\mathrm{Pr}_{\mathrm{W}}(a \mid s, \tilde{f}, d)$: Wahrscheinlichkeit (DoB) eines Angriffs durch d auf s über $\tilde{f}$ aus Sicht des Schutzbedürftigen.

© Fraunhofer IOSB

Definition Risiko

$$\text{Risiko} := \text{Ensemble\_Functional}\{\ \text{Cost(Event)} \times \text{Probability(Event)}\ \}$$

$$\text{Risiko} := \text{Ensemble\_Functional}\left\{\begin{array}{l}\text{Cost(Event, Severity)}\\ \quad \times \text{Probability(Severity} \mid \text{Event)}\\ \quad \times \text{Probability(Event)}\end{array}\right\}$$

© Fraunhofer IOSB

Quantifizierung des Risikos

Risiko für den Schutzbedürftigen s:

$$R_s = \sum_{d \in \mathrm{D_U}} \sum_{i \in \mathrm{I}_d} \sum_{f \in \mathrm{F}_s} \int_0^1 c(s, f, \beta) \cdot p_{\mathrm{V}}(\beta \mid i, s, f)\, \mathrm{d}\beta \cdot \mathrm{Pr_U}(i \mid s, f, d) \quad \text{Safety}$$

$$+ \sum_{d \in \mathrm{D_W}} \sum_{a \in \mathrm{A}_d} \int_0^1 c(s, \tilde{f}, \beta) \cdot p_{\mathrm{V}}(\beta \mid a, s, \tilde{f})\, \mathrm{d}\beta \cdot \mathrm{Pr_W}(a \mid s, \tilde{f}, d) \quad \text{Security}$$

$$+ \sum_{m \in \mathrm{M}^*} c(m(s, f)) \quad \text{Costs of measures}$$

$$\tilde{f} := \arg\max_{f \in \mathrm{F}_s} \{\max_{a \in \mathrm{A}_d} \{U_d(a, s, f)\}\}$$

Flanke der Verwundbarkeit mit der größten Nützlichkeit aus Sicht des Angreifers $d \in \mathrm{D_W}$

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

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

Nützlichkeit (*Utility*) aus Sicht des Angreifers. $d \in \mathrm{D_W}$

© Fraunhofer IOSB

Modellierung

$g(s, f, \beta)$: Gewinn (gain) des Angreifers bei Angriff auf f von s mit Erfolg β

$p_{\text{Success}}(\beta \mid a, s, f)$: DoB-Dichte des Erfolgs β bei Angriff a auf s via f

$c_{\text{Effort}}(a, s, f)$: Kosten für Angriff a auf s via f

$c_{\text{Penalty}}(s, f, \beta)$: Monetäres Äquivalent einer Strafe für Angriff auf s via f mit Erfolg β

$\Pr(\text{Penalty} \mid s, f, \beta) = 1 - \Pr(\neg\text{Penalty} \mid s, f, \beta)$: DoB der Bestrafung eines Angriff auf s via f mit Erfolgs β

Budgetbeschränkung: $c_{\text{Effort}}(a, s, f) \leq b(d)$

© Fraunhofer IOSB

Modellierung

Qualitative Argumentation: Nur wenn der Angreifer zu einem Angriff motiviert ist und die Fähigkeit (*Power*, Mittel und Fähigkeiten) hat und die Gelegenheit (*Occasion*) hat, wird er einen Angriff durchführen.

Quantitative Modellierung: Zerlegung der Eintrittswahrscheinlichkeit (DoB) eines Angriffs in drei Faktoren (implizite Unabhängigkeitsannahme).

$$\Pr_W = \Pr_{\text{Motivation}} \cdot \Pr_{\text{Power}} \cdot \Pr_{\text{Occasion}}$$

© Fraunhofer IOSB

Modellierung

- Bisherige statische Betrachtung bezieht sich auf vorgegebenen Zeitraum der Länge T.
- Dynamisierung des Modells, Einführung einer diskreten Zeit $t = k\Delta T$, $k \in \mathbb{N}_0$ mit konstanten Zeitschritten ΔT.
- Alle bisher eingeführten Größen werden zu Zeitfolgen.

Anmerkung und Hypothese:

Bei statischer Betrachtung und längeren Zeiträumen der Dauer T lassen sich Abhängigkeiten z.B. zwischen Angriffswahrscheinlichkeit und Vulnerabilität nicht vermeiden.

Tastet man das Problem zeitlich aber fein genug ab, so kann man die Veränderung der Angriffswahrscheinlichkeit als Reaktion auf eine vulnerabilitätssenkende Schutzmaßnahme beim Übergang zum nächsten Zeitpunkt berücksichtigen.

Innerhalb des aktuellen Zeitintervalls modelliert man die beiden Größen jedoch konstant und entkoppelt.

© Fraunhofer IOSB

Modellierung

Dynamisierung des Modells; Zeitpunkte k:

$a \rightarrow a^k$

$m \rightarrow m^k$

$\vdots$

$\mathrm{Pr}_{\mathrm{W}} \rightarrow \mathrm{Pr}_{\mathrm{W}}^k$

$\mathrm{Pr}_{\mathrm{U}} \rightarrow \mathrm{Pr}_{\mathrm{U}}^k$ usw.

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

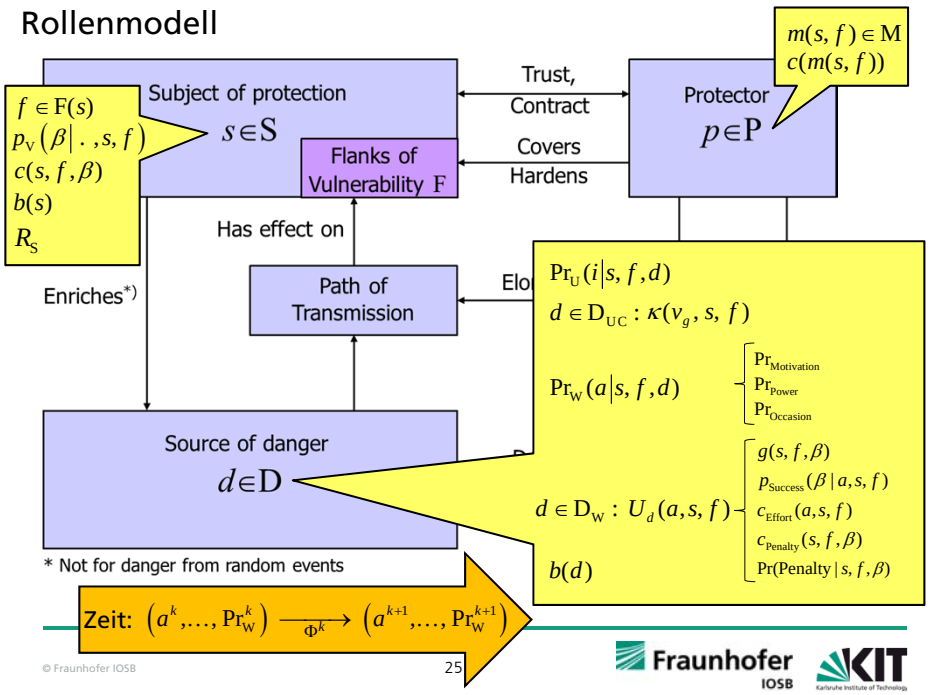
Φ^k : Transitionsoperator vom Zeitpunkt k zum Zeitpunkt $k+1$. Hängt von sich zeitlich ändernden Gegebenheiten ab und modelliert u.a. den Einfluss von ergriffenen Schutzmaßnahmen m^k. (Markov-Annahme)

Anmerkung: Mit dieser zeitlichen Modellierung lassen sich z.B. Fragen formalisieren wie:

Wie wirkt sich eine zum Zeitpunkt k implementierte Schutzmaßnahme im Zeitschritt $k+1$ auf Vulnerabilität, Eintrittswahrscheinlichkeiten usw. aus?

© Fraunhofer IOSB

Rollenmodell



© Fraunhofer IOSB

Simulation auf Basis des Modells

- MDP (*Markov Decision Processes*) und POMDP (*Partially Obsevable Markov Decision Processes*)
- Monte Carlo Verfahren
- Agentenbasierte Simulation (rationale sowie tlw. randomisierte Agenten)

Bemerkungen

- Modellierung ist Szenarien-übergreifend, da Ensemble von Szenarien betrachtet wird. Aussagen werden über Ensemble-Funktionale gewonnen.
- Sichere Zustände (Security) als stabile Nash-Gleichgewichte modellieren.
- Modellierung von Ensembles von Schutzbedürftigen: $R_{\mathrm{S}} = \sum_{s \in \mathrm{S}} R_s$
- DoBs subjektiv; Schätzung subjektiv; Rollenkonzept vereinbar mit der subjektiven Bayes'schen Deutung von Wahrscheinlichkeit.

→ Theorieentwicklung u.a. im *Themennetzwerk Sicherheit*, acatech

→ Antrag DFG SPP "*Transdisziplinäre Theorie der Verlässlichkeit*" eingereicht.

→ Forschungsprojekt gemeinsam mit PD Dr. Oliver Raabe KIT in KASTEL.

© Fraunhofer IOSB

11. Fraunhofer Conference Future Security 2016

International Scientific Security Research Conference

Berlin, 13.-15. September 2016

© Fraunhofer IOSB

Fraunhofer IOSB KIT Karlsruhe Institute of Technology