Schutzziele für kritische Infrastrukturen

Würdigung von Kosten-Nutzen-Ansätzen und weiteren Konzepten

Global Risk Forum GRF Davos
Promenade 35
7270 Davos

Davos, 17. Sept. 2013

Impressum

Auftraggeber

Bundesamt für Bevölkerungsschutz
Monbijoustrasse 51A
3003 Bern

Vertrag Nr

Forschungsauftrag

Nr. 353003897-SFA

Projektbegleitgruppe

Dr. Stefan Brem, Bundesamt für Bevölkerungsschutz BABS

Christoph Werner, Bundesamt für Bevölkerungsschutz BABS

Nick Wenger, Bundesamt für Bevölkerungsschutz BABS

Auftragnehmer/ Verfasser der Studie

Global Risk Forum
GRF Davos
Promenade 35
7270 Davos
Telefon: 081 414 16 00
Fax: 081 414 16 10
walter.ammann@grforum.org
www.grforum.org

Zitiervorschlag

GRF Davos (2013): Schutzziele für kritische Infrastrukturen – Würdigung von Kosten-Nutzen-Ansätzen und weiteren Konzepten. Forschungsauftrag Nr. 353003897-SFA des Bundesamtes für Bevölkerungsschutz BABS, Bern. Global Risk Forum GRF Davos, Davos, 60 p.

Bezugsquelle

Der Bericht kann kostenlos von www.babs.admin.ch heruntergeladen werden.

Die in diesem Bericht wiedergegebenen Aussagen sind nicht zwingend repräsentativ für das Bundesamt für Bevölkerungsschutz und für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport. Die in diesem Bericht gemachten Aussagen stellen in diesem Sinn die Ansichten des Auftragnehmers dar und sind für den Auftragnehmer nicht bindend.

Inhalt

Abbildungs- und Tabellenverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Executive Summary

Das Bundesamt für Bevölkerungsschutz BABS hat im Rahmen der Umsetzung der nationalen Strategie des Bundesrates zum Schutz kritischer Infrastrukturen (SKI) das Global Risk Forum GRF Davos beauftragt, methodische Fragen zur Festlegung von Schutzzielen für kritische Infrastrukturen zu klären. Die Arbeiten sollen insbesondere Grundlagen und Hintergrundinformationen für die Erarbeitung des SKI-Leitfadens liefern. Dieser zeigt auf, wie der integrale Schutz von kritischen Infrastrukturen überprüft und bei Bedarf verbessert werden kann. Dabei behandelt er unter anderem auch Fragen bezüglich Schutzzielen. Das BABS wird Erkenntnisse aus diesem Bericht in den Leitfaden einfliessen lassen. Der vorliegende Bericht ist dementsprechend als Grundlagenpapier zu verstehen und hat somit keine (Rechts-) Verbindlichkeit.

Der Bericht umfasst eine kritische Würdigung bestehender Ansätze zum Umgang mit Risiken im Allgemeinen und zu den Schutzzielen im Besonderen. Während bekanntlich bei den individuellen Risiken mit der Angabe des individuellen Todesfallrisikos ein klarer Grenzwert festgelegt werden kann, ist der Stand der Erkenntnisse bei den kollektiven Risiken bedeutend weniger fortgeschritten und in der Vergangenheit kontroverser diskutiert. Dabei wird aber deutlich, dass die Kosten-Wirksamkeit der Schutzmassnahmen und die Verhältnismässigkeit der eingesetzten Mittel und Ressourcen in den verschieden Risikobereichen und den damit verbundenen behördlichen Fachbereichen immer stärker ins Zentrum rücken und als Entscheidungsgrundlage für Schutzmassnahmen Akzeptanz finden.

Die nachfolgend eingeführte Schutzziel-Pyramide mit ihren vier Levels ermöglicht die Einbettung in bereits bestehende Sicherheitsbestrebungen. Die Pyramide beinhaltet von Level 1 bis Level 4 einen aufsteigenden Grad expliziter Risiko-Wirksamkeits-Betrachtungen bei der Schutzzieldefinition. Level 1 und Level 2 decken dabei die klassischen Schutzziele in Form von normierten und standardisierten Massnahmen und Mindestanforderungen ab, während mit Level 3 und Level 4 der Paradigma-Wechsel zu einem risikobasierten Vorgehen nach den Grundsätzen der Verhältnismässigkeit und der Zahlungsbereitschaft vollzogen wird.

Der Bericht schliesst mit der Empfehlung, im Bereich der kritischen Infrastrukturen dem Grenzkosten-Ansatz zu folgen. Dieser ermöglicht eine einheitliche Anwendung über alle kritischen Infrastrukturen und Risiken. Die Umsetzung bietet neben grossen Vorteilen selbstverständlich noch zahlreiche Herausforderungen. In den nachfolgenden Kapiteln ist der Umgang mit diesem Ansatz grob skizziert.

1. Ausgangslage

„If our priorities in managing risks are not cost-effective, we are, in effect, killing people whose premature deaths could be prevented."

David Okrent, 1980[1]

Leitfaden für Erarbeitung integraler Schutzkonzepte

Der Bundesrat hat am 27. Juni 2012 die nationale Strategie zum Schutz kritischer Infrastrukturen (SKI) verabschiedet und das Bundesamt für Bevölkerungsschutz BABS mit der Koordination der Arbeiten beauftragt.[2] Die nationale SKI-Strategie bezeichnet insgesamt 15 Massnahmen. Eine davon betrifft die Stärkung der Widerstandsfähigkeit der Kritischen Infrastrukturen. Zu diesem Zweck werden die zuständigen Stellen (Fachbehörden, Betreiber usw.) beauftragt, integrale Schutzkonzepte zu erarbeiten und umzusetzen. Als diesbezügliches Hilfsmittel hat das BABS einen Leitfaden erarbeitet, der in einem Entwurf vorliegt.[3]

Forschungsauftrag zur Festlegung von Schutzzielen an GRF Davos

Verschiedene Teile des Leitfadens bedürfen noch einer Prüfung und Vertiefung. Ein zentrales und besonders anspruchsvolles Thema betrifft die sog. Schutzziele. Für die Bearbeitung dieser Frage wurde ein Projektauftrag für eine Forschungsstudie an das „Global Risk Forum GRF Davos" erteilt. Ziel dieser Forschungsstudie war die Entwicklung einer Methodik, die ein einheitliches Konzept zur Festlegung von Schutzzielen bei kritischen Infrastrukturen gewährleistet. Diese Methodik soll die heute bestehenden, sehr unterschiedlichen Ansätze berücksichtigen, werten und den Bedürfnissen der SKI anpassen.

Schutzziele sind im Gesamtkontext des integralen Risikomanagements zu sehen

Es sei hier schon betont, dass die Schutzzielfrage nicht isoliert betrachtet werden kann, sondern immer im Gesamtkontext eines integralen Risikomanagements zu sehen ist. Mit dem Begriff des integralen Risikomanagements wird das Gesamtsystem von Risikoanalyse, Risikobewertung und Massnahmenplanung umschrieben. So hängt die Definition von Schutzzielen u.a. davon ab, welche Informationen die Risikoanalyse zu liefern vermag. Anderseits werden Schutzzielbetrachtungen von der Massnahmenplanung beeinflusst, wenn Nutzen-Kosten-Überlegungen einzubeziehen sind.

Schutzziele legen die Sicherheit von Menschen, sozialen Systemen, Umwelt und Sachwerten fest

Schutzziele befassen sich in erster Linie mit der Sicherheit von Menschen in ihrem (technisch-ökonomischen) Umfeld. Es geht aber natürlich auch um den Schutz von sozialen Systemen, der Umwelt, von (Nutz-)Tieren und von Sachwerten. Im Zusammenhang mit der SKI-Strategie kommt dabei insbesondere auch der Erhaltung von für die Bevölkerung und die Volkswirtschaft lebenswichtiger Funktionen grosse Bedeutung zu.

Die Mittel im Umgang mit Sicherheit sind stets begrenzt, was bedeutet, dass bestimmte (Rest-) Risiken akzeptiert werden müssen und daher auch der Umgang mit ihnen vorbereitet sein will. Von zentraler Bedeutung ist, dass Risikoabschätzungen und Entscheide möglichst transparent gemacht und gut dokumentiert werden, zumal allenfalls im Schadenfall ethische und rechtliche Aspekte (fehlende Vorgaben, Haftungsfragen etc.) ins Spiel kommen.

---

1 David Okrent (1980), *„Comment on Societal Risk"*; in: Science, Volume 208, Issue 4442, 25.4.1980

2 Nationale Strategie zum Schutz kritischer Infrastrukturen vom 27. Juni 2012, BBl 2012 7715.

3 BABS (2012a): *Leitfaden Schutz Kritischer Infrastruktur*. Entwurf, 23. Juli 2012. Bundesamt für Bevölkerungsschutz, Bern.

2. Strategische Vorgaben für die Schutzziel-methodik

"To expect the unexpected shows a thoroughly modern intellect"

Oscar Wilde, 1854 – 1900

2.1 Einleitung

Auftragsziel

Das Ziel dieses vom BABS erteilten Forschungsauftrages besteht in der Erstellung von folgenden zwei Produkten:

- Erarbeitung einer „Methode Schutzziele auf Stufe KI-Objekt[4]"[5]
- Erstellung eines Berichts im Sinne einer Erläuterung der Methode als eigenständiges Dokument (vorliegendes Dokument).

Methode zur Festlegung von Schutzzielen

Die zu erarbeitende Methode soll den zuständigen politischen Behörden (Bund, Kantone) und KI-Betreibern eine Anleitung liefern, um im Rahmen von Schutzkonzepten Schutzziele für KI-Objekte festzulegen. Diese Methode soll Bestandteil des eingangs erwähnten Leitfadens Schutz Kritischer Infrastrukturen (Leitfaden SKI des BABS) werden.

Die Methode als Handlungsanweisung zur Festlegung von Schutzzielen auf Stufe KI-Objekt soll dem Anwender folgende Fragen beantworten:

- Wie ist vorzugehen?
- Was ist zu beachten?
- Wer ist beizuziehen?

Aufgabe und Fragen, die es zu klären gilt

Die Studie hat hauptsächlich zu prüfen, welche Art von Schutzzielen am besten geeignet ist, die Vorgaben der SKI-Strategie zu erfüllen. Basierend auf diesen Erkenntnissen ist ein Vorschlag zu formulieren, welcher das methodische und organisatorische Vorgehen zur Festlegung von Schutzzielen festhält. Die Erkenntnisse sind in einem eigenständigen Bericht zu erläutern. Zudem wünscht der Auftraggeber, dass im Bericht auf die zahlreichen nachstehenden Fragen eingegangen wird. Dies geschieht zum Teil explizit, in der Mehrzahl der Fragen aber implizit in den nachfolgenden Kapiteln. Erläuterungen werden erwartet zu Fragen wie:

- Wie lassen sich KI-Schutzziele in den bestehenden politischen und organisatorischen Rahmenbedingungen umsetzen?
- Welche rechtlichen Rahmenbedingungen sind dabei speziell zu berücksichtigen? Müssen neue Rahmenbedingungen allenfalls erst geschaffen werden?
- Sollen die Schutzziele als „Minimal-" oder „Maximalanforderung" formuliert werden?
- Wie kann die Bedeutungsermittlung pro KI-Objekt (nationale, regionale, lokale Bedeutung) auf die Verfügbarkeit der Objekte angewendet werden?
- Welche Indikatoren neben der Verfügbarkeit sind zu beachten? (siehe Schadenindikatoren im Entwurf Leitfaden SKI).
- Welchen Stellenwert hat die Unterscheidung der PLANAT zwischen strategischen und operativen Schutzzielen und Massnahmenzielen?

---

[4] KI-Objekt: im Folgenden stets als Abkürzung für „kritisches Infrastruktur–Objekt" verwendet.

[5] Die Methode zur Festlegung von Schutzzielen wird im SKI-Leitfaden integriert und bildet einen integralen Bestandteil des gesamten Leitfadens. Die Methode wird nicht als eigenständiges Dokument publiziert.

- Könnte auch ein Grenzkosten-Ansatz gewählt werden?
- Ist die Festlegung von Zielbereichen anstelle klar festgelegter Grenzwerte zielführend?
- Der Methodenbericht soll generische Ansätze zur Anwendbarkeit auf Stufe Teilsektoren enthalten.

2.2 Nationale Strategie zum Schutz Kritischer Infrastrukturen

Nationale Strategie

Die nationale Strategie zum Schutz Kritischer Infrastrukturen, die der Bundesrat am 27. Juni 2012 verabschiedet hat, hält in Bezug auf Schutzziele folgende Prinzipien fest:

Vision

„Die Schweiz ist im Hinblick auf die Funktionsfähigkeit der kritischen Infrastrukturen resilient, sodass grossflächige und schwerwiegende Ausfälle der kritischen Infrastrukturen und der damit verbundenen Güter und Dienstleistungen möglichst verhindert werden, beziehungsweise das Schadenausmass im Ereignisfall begrenzt bleibt."

Übergeordnete Schutzziele

Aufeinander abgestimmte, verbindliche Schutzziele

„Die Schutzziele geben Auskunft über das angestrebte Schutz- und Leistungsniveau. Die Festlegung der Schutzziele erfolgt auf politisch-gesellschaftlicher Ebene. Es ist anzustreben, dass für die verschiedenen kritischen Infrastrukturen in einem politischen Prozess aufeinander abgestimmte und verbindliche Schutzziele vorgegeben werden. Aufgrund der Heterogenität der kritischen Infrastrukturen und der politischen Bedeutung der Thematik stellt dies ein äusserst schwieriges Unterfangen dar. Aus diesem Grund dient die in der Strategie beschriebene Vision als Schutzziel im KI-übergreifenden Bereich. Die Konkretisierung der Schutzziele erfolgt bei der Erarbeitung der integralen Schutzkonzepte im Bereich der kritischen Infrastrukturen. Nach Möglichkeit werden dafür Revisionen von bestehenden Rechtsgrundlagen genutzt. Bereits bestehende Schutzziele sind dabei zu berücksichtigen."

Integraler Schutz

„Der integrale Schutz der kritischen Infrastrukturen ist auf allen relevanten KI-Ebenen (kritische Sektoren, kritische Teilsektoren und kritische Einzelelemente) gewährleistet. Alle relevanten Risiken sind erkannt und gestützt auf Schutz- und Leistungsziele, die auf politischer Ebene vereinbart wurden, nach einem risikobasierten Kosten-Wirksamkeits-Ansatz reduziert. Dabei wird ein umfassendes Gefahren- und Massnahmenspektrum berücksichtigt."

2.3 Fazit

Die aufgeführten Anforderungen an die Schutzziele halten sich naturgemäss auf allgemeiner Ebene. Für die im Folgenden zu konkretisierende Umsetzung werden folgende Vorgaben aus den vorstehenden Dokumenten als zentral erachtet:

Risiko-basierter Kosten-Wirksamkeits-Ansatz im Zentrum

- Die Anwendung eines risikobasierten Kosten-Wirksamkeits-Ansatzes
- Die Erarbeitung finanzierbarer, politisch akzeptierter und aufeinander abgestimmter Schutzziele
- Es sind für jeden Infrastruktursektor aufeinander abgestimmte Schutzziele zu erarbeiten und durch die Politik zu verabschieden. Die Festlegung der Schutzziele erfolgt auf politisch-gesellschaftlicher Ebene. Nach Möglichkeit werden dafür Revisionen von bestehenden Rechtsgrundlagen genutzt.
- Grossflächige und schwerwiegende Ausfälle der kritischen Infrastrukturen und der damit verbundenen Güter und Dienstleistungen sollen möglichst verhindert

werden, beziehungsweise das Schadenausmass im Ereignisfall begrenzt bleiben.

- Die Konkretisierung der Schutzziele erfolgt bei der Erarbeitung der integralen Schutzkonzepte. Die Schutzziele geben Auskunft über das angestrebte Schutz- und Leistungsniveau. Schutzziele selber sind nicht absolut.
- Alle relevanten Risiken sind erkannt und gestützt auf Schutz- und Leistungsziele, die auf politischer Ebene vereinbart wurden, nach einem risikobasierten Kosten-Wirksamkeits-Ansatz reduziert. Dabei wird ein umfassendes Gefahren- und Massnahmenspektrum berücksichtigt.

3. Grundsätzliches und Grundlagen zum Thema Schutzziele

"Humans should learn how to overcome the distance between knowledge, perception and common myths. The key to the integration is probably wisdom."

Aaron Wildavsky, 1930 – 1993, amerikan. Politik-Wissenschafter

3.1 Einleitung

Technische Entwicklungen erfordern Sicherheits-Strategien.

Menschliche Aktivitäten stützen sich seit langem und zunehmend auf immer vielfältigere, technische Errungenschaften, welche durch ihre Komplexität und ihre Einbettung in komplizierte Systeme zu Störanfälligkeit und zu immer grösseren Verletzlichkeiten von Gesamtsystemen führen. Sicherheitsfragen sind dementsprechend eng gekoppelt mit diesen Aktivitäten und den benutzten Technologien.

Das Alter dieser technischen Entwicklung im Blick haltend, könnte man annehmen, dass der Umgang mit den entsprechenden Risiko- und Sicherheitsfragen auf eine umfangreiche und fundierte Tradition und Erfahrung zurückgreifen kann. Dies ist aber weitgehend nur implizit der Fall. Eine explizite Auseinandersetzung oder gar Regelung der Frage nach einem erforderlichen Sicherheitsmass bzw. nach akzeptierten Risiken hat erst in den letzten Jahrzehnten eingesetzt. Anlass dazu waren vorerst Grosstechnologien wie Kernkraftwerke, Raumschifffahrt, Hochgeschwindigkeitszüge, oder Grossraumflugzeuge.

Neuartige Technologien erfordern Risikoanalysen

Diese neuartigen und komplexen Technologien, verbunden mit dem Potential für katastrophale Verluste an Menschenleben und Sachwerten, liessen ein empirisches Vorgehen nach dem Prinzip „trial and error" nicht mehr zu. In der Folge wurden deshalb zunächst Methoden zur Analyse von Risikoproblemen entwickelt - die Geburtsstunde von expliziten Risikobetrachtungen in Form sog. Risikoanalysen. Diese Risikoanalysen führten zu explizit ermittelten, quantitativen Risikogrössen und in der Folge unweigerlich zur Frage nach der Zulässigkeit dieser Risiken, d.h. zur Frage „Wie sicher ist sicher genug?"[6].

Mit einiger Zeitverzögerung führten einerseits schwere Unfälle in der chemischen Industrie (Seveso, Flixborough, Bophal, Schweizerhalle), aber z.B. auch grosse Bahnprojekte im Hochgeschwindigkeitsbereich zur erweiterten Anwendung einer risiko-orientierten Denkweise.

Umfassende Lösungen für Schutzziele fehlen

Fragestellungen wie diejenige der SKI Strategie, welche wesentlich umfassendere Risikobetrachtungen und -beurteilungen beinhalten, sind erst in neuerer Zeit (auch international) zu einem Thema geworden. Sie wurden zwar von Beginn weg auf der Basis von Risikobetrachtungen angegangen. Umfassende Lösungsansätze, insbesondere zum Thema Schutzziele, liegen aber bis heute nicht vor.

6 Ch. Starr, Science Nr. 165, 1969

3.2 Stand der Risikomethodik

Der Risikoansatz als starkes Instrument im Umgang mit Gefährdungen

Der risikobasierte Umgang mit Gefährdungen zielt neben der einleitend aufgeführten Grundsatzfrage „Wie sicher ist sicher genug?“ vor allem auf die Szenarien-basierte Frage „Was kann passieren?“ (Risikoanalyse) und auf die Schutzziel-basierte Frage „Was darf passieren?“ (Risikobewertung) ab.

Lange Zeit hat eine Kontroverse stattgefunden, inwiefern der Risikoansatz nur qualitativ[7], oder aber quantitativ angewendet werden soll. Grund dafür waren vor allem die Zweifel an einer genügenden Zuverlässigkeit solcher Risikoanalysen, aber auch ihre Komplexität und der damit verbundene Aufwand. Einerseits konnte dank IT-Hilfsmitteln der letztgenannte Punkt entschärft werden. Anderseits wurde immer bewusster, dass die Entscheide zur Sicherheit (Massnahmen, Investitionen) letztlich immer quantitativ sind und daher auch quantitative Entscheidungsgrundlagen aufzuzeigen sind.

Quantifizierung der Risiken mit der Farmer-Kurve

Die quantitative Risikoanalyse hat ihre Wurzeln in der in den 1950er Jahren aufkommenden Zuverlässigkeitsanalyse technischer Systeme. In den 1960er Jahren wurden erstmals Risiken mit Wahrscheinlichkeiten w und Ausmass A in einem Diagramm, der sog. Farmer-Kurve[8] dargestellt (vgl. Fig. 10 in Anhang A1) . Als ein Pionier der quantitativen Risikobewertung schuf Farmer mit der Risiko-Grenzkurve eine wesentliche, methodische Grundlage für die quantitative Risikobewertung industrieller Anlagen. Farmer wies auch darauf hin, dass in der Risikobewertung (z.B. eines Kernkraftwerkes) das gesamte Spektrum möglicher Unfälle zu betrachten ist und nicht nur ein "maximales" Unfallereignis - der GAU (grösster anzunehmender Unfall), wie es bis dahin in der Kerntechnik üblich war.

Die Risikoanalyse ist natürlich auf adäquate Daten und Modelle zur Erfassung der Gefährdungs- und Auswirkungssituationen angewiesen[9]. Neben der eigentlichen Gefährdung, charakterisiert durch Intensität und Eintretenswahrscheinlichkeit, tragen u.a. die Exposition von Personen, Sachwerten, Infrastrukturen etc. und deren Verletzlichkeit und Interdependenzen zum Gesamtrisiko bei. Stark Risiko-verschärfend wirkt die Risikoaversion, sofern sie berücksichtigt wird.

Unschärfen und Unsicherheiten sind in die Risikoanalyse einzubeziehen

Die damit verbundenen Unschärfen und Unsicherheiten gilt es in Risikoanalyse und -bewertung zu bedenken, um keine Scheingenauigkeiten vorzutäuschen. Als zusätzlich erschwerende Umstände für eine aussagekräftige Risikoanalyse kommen die sich ständig verändernden Randbedingungen, z.B. der Einfluss der Klimaveränderung auf Gefährdungsszenarien (Eintretenswahrscheinlichkeit und Intensität der Gefährdung), oder die zunehmenden und schwierig abzubildenden Interdependenzen in Infrastruktur- und Wirtschaftssystemen hinzu. Die Zweckmässigkeit und unbestrittenen Stärken der Risikoanalyse und des nachfolgend dargelegten Grenzkosten-Kriteriums deswegen in Frage zu stellen, wäre jedoch verfehlt, da methodische Kompromisse diese Unsicherheiten nicht beseitigen. Die Ermittlung von expliziten, quantitativen Risikowerten stellt eine ausserordentlich bedeutsame Erweiterung der Entscheidungsgrundlagen für Schutzplanungen dar.

---

7 Gängige Risikomanagementsysteme, z.B. ISO 31000 beinhalten in der Regel nur qualitative Beurteilungen.

8 F.R. Farmer, (1967) *“Safety Criterion, Containment and Siting of Nuclear Power Reactors"*, IAEA Vienna.

9 CSS ETHZ (2012). *Fukushima und die Grenzen der Risikoanalyse*, CSS ETH Zürich

Risikobewertung und Risikomatrix als Tool zur Priorisierung

Wesentlich schwerer als mit der Risikoanalyse tut man sich bis heute immer noch mit der Risikobewertung als logische Fortsetzung der Risikoanalyse. Dabei sind zwei grundsätzlich verschiedene Dimensionen des Risikos zu unterscheiden: das individuelle und das kollektive Risiko. Dies betrifft primär Personenrisiken (vgl. dazu nachfolgendes Kap. 3.3):

Für die Beurteilung einer Risikosituation aus Sicht des kollektiven Risikos ist die sog. Risikomatrix (siehe Abb. 6) nützlich und gebräuchlich. Sie zeigt anschaulich die Lage der Risikobeiträge der verschiedenen Gefährdungs- und Schadensszenarien einer Gesamtsituation aus der Sicht der Eintretenswahrscheinlichkeit w einer bestimmten Gefährdung und des damit verbundenen potentiellen Schadenausmasses A. Die Risikomatrix wird in diesem Kontext v.a. dazu verwendet, den relativen Stellenwert verschiedener Risikokomponenten und damit allfällige Prioritäten bezüglich des Handlungsbedarfs zu visualisieren. Darauf wird in Kapitel 5.2 näher eingegangen.

3.3 Individuelles und kollektives Risiko

Das Risiko hat 2 Dimensionen

Zwei Dimensionen des Risikos sind zu unterscheiden (vgl. Abb. 1 und Abb. 2), das individuelle Risiko und das kollektive Risiko. Abb. 1 zeigt eine Risikosituation mit einer Vielzahl von Personen(-Gruppen), die unterschiedlich gefährdet sind und demnach das individuelle Risiko unterschiedlich ist. Die Gesamtheit der individuellen Risiken summiert sich zum kollektiven Risiko. Für den Bereich SKI sind in der Regel primär die kollektiven Risiken ausschlaggebend.

Individuelles Risiko

Grenzwerte zum individuellen Risiko auf der Basis von Todesfallwahrscheinlichkeiten

Beim individuellen Personenrisiko geht es um die Wahrscheinlichkeit, mit der das einzelne Individuum einen Schaden erleiden kann. Es geht also um das persönliche Risiko eines Einzelnen, durch eine Gefahr zu Schaden zu kommen, insbesondere um die Wahrscheinlichkeit eines einzelnen Individuums von einer Gefährdung tödlich betroffen zu werden. Für das individuelle Todesfallrisiko von Personen existieren heute bereits fundierte und relativ breit akzeptierte Grenzwerte. Das Kriterium für das Schutzziel besteht in einer Begrenzung des maximal zulässigen individuellen Risikos; es wird ausgedrückt durch die jährliche Todesfall-Wahrscheinlichkeit. Diese Grenzwerte garantieren, dass keine einzelne Person einem spezifischen übermässig Risiko ausgesetzt ist. Sie gewährleisten einen einheitlichen Mindestschutz für alle Personen. Situations- oder Gebiets-bezogene, ungerechte Verteilungen von Risiken können damit vermieden werden. (Details vgl. Anhang A2)

Das individuelle Risiko dürfte aber im Rahmen der SKI in der Regel nur ausnahmsweise massgebend sein. Die SKI-Strategie betont, dass es um grossflächige und schwerwiegende Ausfälle geht. Es geht also tendenziell um seltene Ereignisse, was bestärkt, dass das individuelle Risiko wohl selten massgebend werden dürfte.

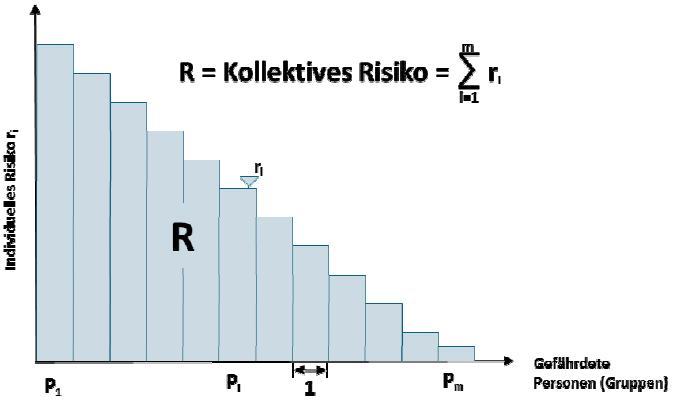


Abbildung 1: Die zwei Dimensionen des Risikos: individuelles und kollektives Risiko (nach Merz et al.[10])

Kollektives Risiko

Das kollektive Risiko als Summe der Individuellen Risiken und als Ausdruck des Gesamtrisikos für eine Gesellschaft.

Im Unterschied zum individuellen Risiko bezeichnet das kollektive Risiko die insgesamt zu erwartende Zahl an Opfern und Schäden für die betroffene Gemeinschaft als Ganzes in einer spezifischen Risikosituation. Die Gesellschaft hat naturgemäss ein Interesse, das Schadensausmass niedrig zu halten, unabhängig davon, ob es sich um wenige Personen mit hohem, oder viele Personen mit niedrigem individuellem Risiko handelt. Da aber mit der Begrenzung des individuellen Risikos das Sicherheitsbedürfnis des Individuums abgedeckt ist, geht es hier nicht mehr um die Definition eines zulässigen Risikos für einzelne Risikosituationen, sondern um eine Minimierung des Schadensausmasses im betrachteten Gesamtsystem mit den insgesamt verfügbaren Mitteln.

Ansatz für das kollektive Risiko ist die Definition eines Risikobegriffes, welcher als Funktion der Wahrscheinlichkeit w und des Schadenausmasses A von möglichen Ereignissen definiert ist. Wie bereits im vorangehenden Kapitel 3.2 dargelegt, wird das Risiko üblicherweise als eindimensionales Produkt der beiden Grössen Wahrscheinlichkeit w und Schadenausmass A definiert. Mit Verweis auf Abb. 1 ist das kollektive Risiko R für die Gesellschaft die Gesamtsumme der individuellen Risiken r_i.

Störfallverordnung des BAFU als Beispiel einer Risikomatrix mit drei Handlungsbereichen.

Die Risikoermittlung ist die Grundlage für die Beurteilung der Tragbarkeit des Risikos. Ein theoretisch konsistentes, allgemeingültiges Konzept für Grenzwerte des kollektiven Risikos gibt es aber nicht. In einzelnen begrenzten Anwendungsbereichen existieren pragmatische Vorschläge. So definiert die Störfallverordnung des Bundes in einer Risikomatrix drei Bereiche. In den beiden äusseren Bereichen wird festgehalten, welche Risiken tragbar und welche nicht tragbar sind. Dazwischen ist ein Übergangsbereich definiert, in welchem die Vollzugsbehörde über die Tragbarkeit des Risikos zu entscheiden hat. Dabei wägt sie die Schutzbedürfnisse von Bevölkerung und Umwelt gegenüber privaten und öffentlichen Interessen an einer Anlage ab. Die Vollzugsbehörde entscheidet also, ob das von einer Anlage ausgehende Risiko für Bevölkerung und Umwelt tragbar ist, oder ob zusätzliche Sicherheitsmassnahmen nötig sind (BAFU 2013 Störfallverordnung[11]). Artikel 7 der Störfallverordnung und das

[10] Hans A. Merz, Thomas Schneider, Hans Bohnenblust (1995): *„Bewertung von technischen Risiken -Beiträge zur Strukturierung und zum Stand der Kenntnisse, Modelle zur Bewertung von Todesfallrisiken“*, Polyprojekt Risiko und Sicherheit Band 3, Dokumente, vdf Hochschulverlag, Zürich

[11] BAFU Störfallverordnung, Handbuch I zur StFV, 2008.

Handbuch 1 zur Störfallverordnung geben Hinweise auf die im Rahmen der Interessensabwägung zu berücksichtigenden Kriterien. Eine Risikosituation kann eine sehr unterschiedliche Charakteristik hinsichtlich des individuellen Risikos (Risikospitze) und des kollektiven Risikos (Risikofläche) haben. Wie aus Abb. 2 ersichtlich wird, resultiert für das Gefährdungsszenario 2 ein kollektives Risiko R2, welches bedeutend grösser ist als das kollektive Risiko R1, bei dem aber das maximal zulässige individuelle Risiko überschritten ist. Trotz Nicht-Überschreiten des individuellen Risikos muss auch R2 analysiert werden. Seltene Grossereignisse, wie sie im Rahmen SKI im Zentrum stehen, weisen eine grosse Fläche auf und naturgemäss eine geringe Risikospitze (Abb. 2).

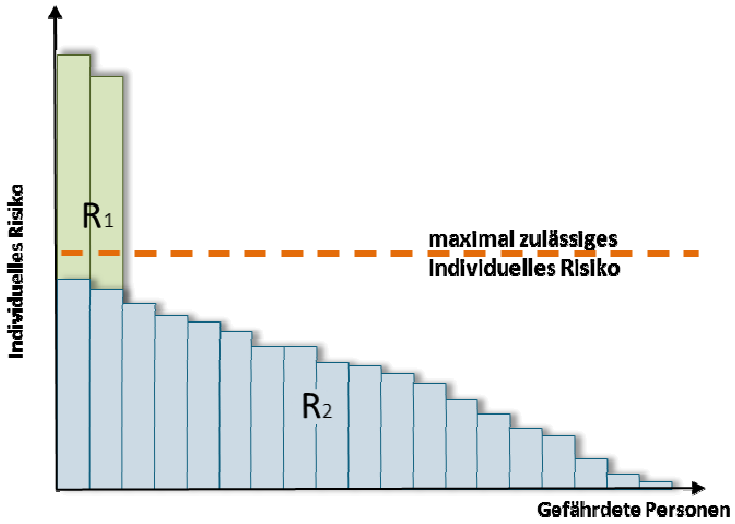


Abbildung 2: Zwei Gefährdungsszenarios mit unterschiedlich grossem individuellem (Einzelspitze) und kollektivem (Fläche) Risiko. Trotz Nicht-Überschreitens des individuellen Risikos muss auch das Gefährdungsszenario mit dem resultierenden kollektiven Risiko R2 analysiert werden (eigene Darstellung).

3.4 Risikoaversion

Risikoaversion als zusätzliche Komponente des Risikos (Risikowahrnehmung)

Mit der Risikobetrachtung parallel einher geht die Risikoaversion, ein Ansatz, der bis in die 70er-Jahre zurückreicht. Die Risikoaversion basiert auf der Feststellung, dass die Gesellschaft in ihrer öffentlichen Wahrnehmung einen einzigen Unfall mit 100 Todesopfern stärker gewichtet als 100 Unfälle mit jeweils einem Opfer. Damit geht einher, dass mit zunehmendem Ausmass eines Ereignisses seine gesamthaften Auswirkungen überproportional wahrgenommen werden und damit auch der Wunsch, ein Risiko zu verhindern, überproportional steigt. Seit über 20 Jahren bestehen Ansätze, welche auch in der Praxis Anwendung finden, um eine stärkere Gewichtung von grossen Schadenereignissen zu berücksichtigen, als es dem rein statistischen Erwartungswert w x A entspricht. Die Risikoaversion wird dabei als Skalierungsfaktor eingeführt, mit dem das (kollektive) Risiko multipliziert wird.

Verfeinerte Aversionskurve

Das Bundesamt für Bevölkerungsschutz 2008[12] hat zur Aversion eine Grundlagenarbeit veröffentlicht und zusätzlich einen Schadenergänzungsfaktor eingeführt. Der Aversionsfaktor berücksichtigt dabei neu die Unsicherheit bei der

[12] BABS Bundesamt für Bevölkerungsschutz (2008), *Risikoaversion – Ein Beitrag zur systematischen Risikobeurteilung*, BABS Bern, 31. Okt. 2008.

Eintretenswahrscheinlichkeit eines Ereignisses, die zunehmende Unsicherheit bei der Schadenprognose und die besondere Verantwortung bei Ereignissen mit ausserordentlichem Schadensausmass. Der Faktor ist als stetige Kurve in Funktion der Anzahl Toten definiert und liegt bis zu einer Gesamtzahl von 100 Toten bei einem Wert von 6.5 und ab 100‘000 Toten bei einem Wert von 40[13].

Aversionskurven sollten vereinheitlicht werden.

Allerdings wird andernorts, z.B. bei der Störfallverordnung, noch mit einer wesentlich grösseren Risikoaversion gearbeitet (wobei die Aversion erst im Rahmen der Risikobewertung zum Tragen kommt und die Risikoanalyse aus Gründen der Transparenz immer ohne Aversion durchgeführt wird). Eine homogenisierte Basis für die Berücksichtigung der Aversion bezüglich kollektiver Personenrisiken wäre grundsätzlich anzustreben.

Zu beachten ist ferner, dass die Frage der Aversion nicht nur aus Sicht der Öffentlichkeit, sondern auch der spezifischen Sicht sensibler Wirtschaftszweige und Institutionen thematisiert werden kann, bzw. muss (Reputationsschäden), was zu unterschiedlichen Einschätzungen führen kann. Gewisse Schadenformen und -ausmasse sollen dabei unbedingt vermieden werden. Es hat sich gezeigt, dass in solchen Situationen Wirtschaftszweige und Institutionen (Verkehrsbetriebe, Telecom-Firmen, etc.) in der Folge bereit sind, für ihre Massnahmenplanung u.U. sogar bedeutend strengere Massstäbe anzulegen.

Aversionsfaktor nur für Todesopfer, nicht aber für Sachwerte.

Da in den gängigen Rechenmodellen der Schadenerwartungswert mit dem Risikoaversionsfaktor multipliziert wird, sind zur Risikoaversion möglichst konkrete und einheitliche Vorgaben zu machen. Dabei sollte der Aversionsfaktor nur auf die Wertung der Todesopfer einen Einfluss nehmen, nicht aber auf die Sachwerte. Der Tod eines Menschen ist ein nicht ersetzbarer Verlust im Unterschied zu einem Sachwert-Verlust, so dass sich die ausschliessliche Anwendung eines Aversionsfaktors auf Todesfälle rechtfertigt. Dabei wird davon ausgegangen, dass die Ermittlung der zu erwartenden Sachschäden sowohl die direkten, wie auch die indirekten Schäden möglichst genau erfasst.

Die Risikoaversion ist also primär ein Element der Risikoquantifizierung und damit Teil der Risikoanalyse. Es zeigt sich aber auch hier, dass Risikoanalyse und Risikobewertung ineinander übergehen. Dabei stellt natürlich auch die Vernachlässigung der Risikoaversion eine Wertung dar. Im Rahmen des SKI ist der Risikoaversion gebührend Beachtung zu schenken.

3.5 Ansätze zum Risikomanagement in der Schweiz

Anfänge in den 70er Jahren

Seit Mitte der 90er Jahre finden in der Schweiz, die in Kap. 3.2 dargestellten quantitativen Arten der Risikoanalyse und Risikobewertung vermehrt auch Eingang in den Umgang mit Naturgefahren[14].

Zu erwähnen ist in diesem Zusammenhang insbesondere aber auch, dass im Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport VBS resp. in seinem Vorläufer EMD zu Beginn der 70er Jahre erstmals in der Schweiz ein Sicherheitskonzept auf quantitative Risikobeurteilungen der erwähnten Art ab-

[13] Es bleibt fraglich, ob derart hohe Werte gerechtfertigt sind, insbesondere wenn sie sowohl auf die Toten, wie auf die Sachschäden angewendet werden.

[14] Die PLANAT hat sich in ihrer Strategie von 2002 zu einer risikoorientierten Denkweise verpflichtet und 2004 erstmals Vorschläge für Schutzziele veröffentlicht (PLANAT, 2004a).

gestützt wurde. Dies betraf die Frage der sicheren Lagerung von Explosivstoffen und Munition.

Kosten/Nutzen-Ansatz im Zivilschutz

Im Bereich des Zivilschutzes wurde ebenfalls bereits in den 70er Jahren mit gewichteten Schadenszenarien die konzeptionelle Optimierung von Massnahmen unterstützt. Dabei ging es allerdings nicht um die Ermittlung zulässiger Risiken, sondern direkt um den optimalen Mitteleinsatz für Schutzmassnahmen mittels Kosten/Nutzen-Überlegungen. Diese Arbeiten wurden in der Folge einerseits im Rahmen des sog. KASKO[15] wieder aufgenommen und anderseits in den 90er-Jahren im BABS in breitem Rahmen mit der KATANOS[16]-Studie und deren Folgearbeiten weitergeführt. Zu erwähnen sind auch die frühen Ansätze zu gesamtschweizerischen Risikobetrachtungen, welche von der damaligen Zentralstelle für Gesamtverteidigung (ZGV) initiiert wurden und in der Folge stetig erweitert und vertieft wurden. An dieser Stelle sei auch die umfassende Behandlung der Risiko-Thematik in einem fundamentalen Buch von Fritzsche erwähnt[17]. Alle diese Arbeiten können als Vorläufer zu den nun im Rahmen des SKI aufgenommenen Arbeiten betrachtet werden.

Von einem breiten Durchbruch der methodischen Ansätze zu einem risikobasierten Entscheidungs- und Massnahmen-Umsetzungs-Prozess kann in der Schweiz trotz dieser zahlreichen bisherigen Arbeiten noch nicht gesprochen werden.

In einer zunehmenden Zahl von Bereichen (Störfallverordnung, Eisenbahn, Transport gefährlicher Güter, Strassenverkehr) fliessen aber in der Schweiz seit einiger Zeit Risikobetrachtungen in unterschiedlicher Form ein, da sie helfen, die entsprechenden Fragestellungen systematischer zu strukturieren und zu analysieren. Die dazu verwendeten Ansätze und Methoden der Risikoanalyse werden dabei laufend verbessert.

Ein wesentlicher Schritt, die Grundsätze der Verhältnismässigkeit und der konsequenten Kostenwirksamkeit im (Bau und) Unterhalt von kritischen Infrastrukturen zu verankern, ist auch mit der Einführung der neuen SIA Norm 269[18] im Jahr 2011 gelungen.

Schutzziele erst ansatzweise festgelegt

Auch zur Frage der Akzeptierbarkeit von Risiken bzw. der Risikobewertung und damit der Schutzziele sind zwar im Laufe der Zeit verschiedene Ansätze entwickelt und angewendet worden, von einem allgemein anerkannten Stand kann aber insbesondere hier nicht gesprochen werden. Dies hängt wesentlich damit zusammen, dass die entsprechenden Fragestellungen weit über das rein Technische und auch Ökonomische hinausgehen und rechtliche sowie politisch-gesellschaftliche Fragen zur Diskussion stehen.

Die Schweizer Gesetzgebung beginnt sich für risikobasierte Sicherheit zu interessieren.

Das Schweizer Recht hat sich bisher nur zurückhaltend und unverbindlich mit risikobasierten Sicherheitsfragen befasst. Doch auch hier kommt langsam Bewegung in die Frage, inwieweit Gesetzeswerke mit Blick auf risikobasierte Entscheide und Massnahmen anzupassen sind[19]. Auf gesellschaftlicher und politischer Ebene ist dies noch weniger der Fall, auch wenn dies immer wieder ge-

[15] KASKO = Koordinationsausschuss Schutzkonzept

[16] KATANOS = Katastrophen und Notlagen in der Schweiz (Folgestudie KATARISK)

[17] Fritzsche, A. F. (1986): *Wie sicher leben wir? Risikobeurteilung und –bewältigung in unserer Gesellschaft.* Verlag TÜV Rheinland GmbH, Köln.

[18] SIA Norm 269, 2011. *„Grundlagen zur Erhaltung von Tragwerken“,* Schweiz. Ingenieur- und Architektenverein, Zürich.

[19] Güngerich, A. und Walpen, A. (2011): *Rechtliche Aspekte eines risiko- und effizienzbasierten Sicherheitskonzepts.* Sicherheit & Recht 2 (2011).

fordert wird. Als implizites Signal der Zustimmung seitens der Politik für ein Vorgehen dieser Art kann die Akzeptanz entsprechender gesetzlicher Vorgaben (z.B. Störfallverordnung) gewertet werden.

3.6 Risikogrenzwerte und Grenzkosten

Risikogrenzwerte

Seit Sicherheitsprobleme mit dem auf einer Risikoanalyse basierenden Ansatz beurteilt werden (im Sinne von „Was kann passieren?“), steht bei der Risikobewertung die Frage „Was darf passieren?“ im Raum. Diese Frage führt zur Vorstellung, dass ein akzeptierbares Risiko festgelegt werden kann. Die im englischen Sprachbereich übliche Frage „How safe is safe enough?“ ist aus dieser Sicht offener. Dabei ist auch hier die Unterscheidung zwischen dem individuellen und dem kollektiven Risiko zu beachten (vgl. Kap. 3.2).

Explizite Risikorelevante Grenzwerte existieren nur für das individuelle Risiko.

Entscheidend ist dabei nach heutigem Stand des Konsensus, dass das individuelle Risiko von Personen, also die Wahrscheinlichkeit für eine einzelne Person, durch ein gefährliches Ereignis ums Leben zu kommen, durch einen entsprechenden Mindestgrenzwert zu limitieren ist. Damit ist dem Anspruch einer einheitlichen, „gerechten“ Begrenzung bzw. Verteilung von Risiken Genüge geleistet. Dieser Grenzwert wird je nach Art des Risikos bzw. dem Grad der Freiwilligkeit der Risikoexposition differenziert.

Im Gegensatz dazu ist die Diskussion um das kollektive Personenrisiko, also der Erwartungswert für Personenschäden innerhalb eines betrachteten Gesamtsystem, noch weit offener. Zwar setzt sich immer klarer die Auffassung durch, dass eine theoretisch konsistente Sichtweise zwingend zu einem Kriterium führt, bei dem die Verhältnismässigkeit der Sicherheitsanstrengungen im Zentrum steht, also die sog. Grenzkosten. Trotzdem wird immer wieder die Frage aufgeworfen, ob nicht auch für das kollektive Risiko Grenzwerte als ein sinnvolles Entscheidungskriterium definiert werden können und sollen.

Begrenzung der Wahrscheinlichkeit eines Ereignisses

Der Ansatz einer Risikobegrenzung durch Begrenzung der Wahrscheinlichkeit stammt vor allem aus den Anfängen der Risikobetrachtungsweise, welche zur Entwicklung von Grosstechnologien wie z.B. Raumfahrt, Grossraumfahrzeuge, Kernkraftwerke, etc. nötig wurde. Insbesondere bei Raketen und Flugzeugen bestand das unerwünschte Ereignis im Versagen des Objektes, womit das Schadenausmass bei Versagen quasi gegeben war. Auch bei kritischen Ereignissen, wie der Kernschmelze in einem KKW, ging es primär darum, solche Ereignisse grundsätzlich zu verhindern resp. eben deren Eintretens-Wahrscheinlichkeit so tief als möglich zu halten. Dementsprechend wurden damals primär Methoden zur differenzierten Berechnung von Wahrscheinlichkeiten entwickelt (z.B. die Fault Tree Analysis (FTA) etc.).

Eine Begrenzung der Wahrscheinlichkeit lässt keine Aussage zum verbleibenden Risiko zu.

Einerseits hat die zunehmend kritische Haltung gegenüber gewissen Technologien dieser Art (insb. KKWs), aber auch das Eintreten von Schadenereignissen trotz der angestrebten tiefen Eintretens-Wahrscheinlichkeiten, dazu geführt, dass auch Rechenschaft über die möglichen Schadensauswirkungen gefordert wird. Zudem wurden Risikobeurteilungen zunehmend auch in Bereichen durchgeführt, in denen das Argument minimer Eintretenswahrscheinlichkeiten aufgrund konkreter Erfahrungen a priori nicht verfängt (z.B. Chemiebetriebe, Eisenbahn).

Es muss zudem festgehalten werden, dass bei sehr kleinen Wahrscheinlichkeiten deren Nachweis trotz differenzierter Methoden mit beachtlichen Unsicherheiten behaftet ist. Dennoch basieren bis heute immer noch viele (technische) Systeme auf der Annahme einer genügend kleinen Eintretenswahrscheinlichkeit von Grossereignissen (z.B. Talsperren, grosse Gaslager etc.), ohne dass deren Auswirkungen eines Versagens in die Beurteilung einbezogen werden.

Begrenzung des Ausmasses eines Ereignisses

Eine Begrenzung des Ausmasses lässt keine Aussage zum verbleibenden Risiko zu.

Der Ansatz mittels Begrenzung des Schadenausmasses stammt primär aus der vor-Risiko-Zeit. Dabei wurden auf der Massnahmenebene Vorschriften definiert, die implizit das Schadenausmass begrenzen. Ein typisches Beispiel sind sog. Sicherheitsabstände zwischen Gefahrenherden und gefährdeten Objekten, wie sie z.B. bei der Lagerung gefährlicher Güter angewendet wurden. Hier wird im Gegensatz zum oben beschriebenen Vorgehen, die Wahrscheinlichkeit des Ereignisses vernachlässigt bzw. nicht in die Überlegungen einbezogen und lediglich darauf abgestellt, dass im Ereignisfall keine bzw. eine nur sehr beschränkte Schadenwirkung entsteht, indem der Gefahrenherd von den zu schützenden Objekten und Personen möglichst getrennt gehalten wird.

Aber auch dieser Ansatz einer reinen Beschränkung des maximalen Schadenausmasses hat sich in der Praxis immer häufiger als wenig zielführend erwiesen. Einerseits erweisen sich solche Vorschriften oft als sehr konservativ und damit (zu) einschneidend. Zunehmend sind sie nur schwer umsetzbar in einem Umfeld mit immer dichteren und intensiveren zivilisatorischen Aktivitäten und den resultierenden Interaktionen. Anderseits ist es bei den meisten Risikosituationen nur eine Frage der Phantasie, sich Szenarien vorzustellen, bei denen das Ausmass die als sinnvoll erachteten Grenzen doch übersteigt (z.B. ausserordentliche Personenansammlungen). Naturgemäss sind solche Szenarien mit kleinen Wahrscheinlichkeiten gekoppelt, was zeigt, dass ein Ausklammern von Wahrscheinlichkeitsüberlegungen nicht zweckmässig und letztlich nicht zu rechtfertigen ist.

Gleichzeitige Begrenzung von Wahrscheinlichkeit und Ausmass

Die einfachste Art, beide Risikogrössen w und A in eine Beurteilung einzubeziehen, wäre, für beide Grössen in der w-A-Risikomatrix je eine Grenze zu setzen und damit die zulässige Spanne des w-A-Feldes einzuschränken. Es ist jedoch offensichtlich, dass damit auch nicht plausible Beschränkungen eingeführt werden, insbesondere wenn bei sehr kleinem Ausmass die Wahrscheinlichkeit zusätzlich begrenzt wird. Es liegt daher auf der Hand nicht eine Begrenzung für die beiden Grössen getrennt zu definieren, sondern für ihre Kombination bzw. deren Produkt, also gemäss der üblichen Risikodefinition w x A. Dies bedeutet, dass die Begrenzung tendenziell einer Diagonalen im w-A-Feld folgt und damit einem konstanten Risiko.

Die Risikomatrix mit (drei) Zonen begrenzt gleichzeitig w und A

Auf dieser Basis hat sich in der Folge ein Ansatz etabliert, bei welchem im w-A-Feld resp. der sog. w-A-Risikomatrix drei Zonen unterschieden werden: *akzeptierbar, nicht akzeptierbar* sowie eine *Übergangszone,* mit unterschiedlicher Bezeichnung (z.B. tolerierbar). Die w-A-Matrix wird allerdings bis heute mehrheitlich nur qualitativ verwendet, womit eine Aussage über die effektiven Risiken und damit absoluter Risikogrenzwerte nicht gemacht wird. Der Wert dieser Beurteilungsweise besteht dann in einer qualitativen Abstufung der Risiken. Solange dies im Sinne einer ersten Prioritätenordnung erfolgt, ist dies durchaus

sinnvoll. Die Frage „How safe is safe enough?“ ist aber auch so nach wie vor nicht zu beantworten.

Die Störfallverordnung des BAFU als Beispiel einer zonalen Begrenzung der kollektiven Risiken.

Matrizen dieser Art werden aber auch mit quantitativen w- und A-Achsen vorgeschlagen, so in der Störfallverordnung des BAFU und im vorliegenden Fall im Leitfaden SKI des BABS. Eine wissenschaftlich hergeleitete und allgemein gültige Begründung für die Festlegung solcher Risikozonen ist nicht möglich und wird vermutlich in der Regel im Rahmen eines Konsensfindungsprozesses pragmatisch vorgenommen. Die Störfallverordnung des BAFU ist wohl die bekannteste Art einer gleichzeitigen w-A-Begrenzung. De facto liegt mit dem Ansatz der Störfallverordnung ein Grenzwertkonzept für das kollektive Risiko vor.

Grundsätzlich muss festgehalten werden, dass bis heute nur einige wenige pragmatische Ansätze, aber keine theoretisch fundierten Vorschläge für die Festlegung von Risikogrenzwerten für das kollektive Risiko existieren, obwohl die Frage nach einem solchen Ansatz immer wieder aufgeworfen und diskutiert wird. Zudem sind diese Ansätze immer nur für den jeweiligen engen Anwendungsbereich vorgesehen und gültig.

Möglichkeiten und Grenzen von Risikogrenzwerten

Es existieren keine eindeutigen Bezugsgrössen beim kollektiven Risiko, mit denen Grenzwerte festgelegt werden könnten.

Während die Festlegung von Risikogrenzwerten für das individuelle Risiko unbestritten ist, haben (vermeintliche) Grenzwerte für das kollektive Risiko zahlreiche Nachteile:

- Wenn Grenzwerte für ein Objekt definiert werden, ist dies nicht kompatibel mit der Forderung nach Verhältnismässigkeit, weil bis zur Erreichung des Grenzwertes in Sicherheit investiert werden, ohne dass Rücksicht auf die resultierenden Kosten genommen werden kann. Die zur Erreichung der Grenzwerte nötigen Massnahmen müssen getätigt werden, unabhängig von ihrer Kosteneffizienz.
- Es gibt keine eindeutige Bezugsgrösse für das Risiko. Es sind keine einheitlichen Risikogrenzwerte definierbar bzw. Risikogrenzwerte auf Ebene Objekt könnten aufgrund der Vielfalt bezüglich Grösse und Art der Objekte nicht einheitlich sein. Im Gegensatz zum individuellen Risiko, bei dem mit dem Individuum auf natürliche Art und automatisch eine Bezugsgrösse gegeben ist, bietet sich eine solche einheitliche Bezugsgrösse beim kollektiven Risiko nicht an.
- Grenzwerte sind – wenn überhaupt – nur sehr Objekt-spezifisch und rein pragmatisch festlegbar und beruhen auf einer Vielzahl von Erfahrungswerten, die in den allerwenigsten Fällen vorhanden sind (Ausnahme Munitionslagerung[20]). Ein einheitliches Prinzip für Grenzwerte für das kollektive Risiko kann deshalb bei der grossen Vielfalt an Infrastrukturen, Prozessen und den unterschiedlichsten Gefährdungsszenarien der KI-Objekte nicht definiert werden.

Grenzkosten

Die einzige, umfassend umsetzbare Alternative zu den verschiedenen Konzepten mit Grenzwerten stellen die Grenzkosten dar. Das zentrale Grundprinzip

[20] Bienz, A. (2006): *Revised Risk-Based Safety Criteria to be proposed for the Handling of Ammunition and Explosives in the Swiss Army and Military Administration*. ETH Zurich, Switzerland.

besteht darin, dass jede risikoreduzierende Massnahme nach dem Grundsatz der Verhältnismässigkeit beurteilt und umgesetzt wird. Dabei wird ebenfalls erwartet, dass die Sorgfaltspflicht aller an einem Prozess Beteiligten im „Rahmen des Zumutbaren“ wahrgenommen wird (vgl. Tab. 2).

Grundsätzlich stellt sich bei jeder Sicherheitsplanung die Frage, warum man nicht quasi unbeschränkt Mittel investiert, um die Sicherheit weiter zu erhöhen. Bei dieser Frage ist es nützlich, sich über den Zusammenhang, welcher in Abb. 3 schematisch dargestellt ist, Rechenschaft abzulegen.

Mit einem Minimum an Kosten ein Maximum an Risikoreduktion erzielen.

Bei jeder Schutz- und Sicherheitsplanung stellt sich die Frage, mit welchen Massnahmen die (Ausgangs-)Risiken auf optimale Weise reduziert werden können. Dabei sind für jede Massnahme das Mass der erzielten Risikoreduktion und die dafür aufgewendeten Mittel zu beurteilen. Jede Massnahme kann dann in einem Risikoreduktions-Kosten-Diagramm eingetragen werden. Dabei ergibt sich zunächst eine Wolke von Massnahmen. Die untere Umhüllende dieser Wolke repräsentiert denjenigen Massnahmen, welche für die jeweiligen Kosten für eine Schutzmassnahme die grösste Risikoreduktion ergeben. So ergibt sich schliesslich, auf der Basis rein technisch-ökonomischer Fakten, die in Abb. 3 dargestellte Kurve. Die Kurve zeigt auf, wie viel Risikoreduktion in Abhängigkeit der investierten Kosten für Sicherheitsmassnahmen in einem System möglich ist. Die schwarze Kurve resultiert aus der Annahme, dass stets Sicherheitsmassnahmen gefunden werden können, die es erlauben, mit einem Minimum an Kosten ein Maximum an Risikoreduktion zu erzielen. Von diesen Fakten ist bei der Diskussion des angestrebten Sicherheitsniveaus auszugehen.

Grenzkosten Kriterium als Schutzziel

Die Monetarisierung der verschiedenen Schadengrössen zu einer einheitlichen Kostendimension und die damit erreichte Aggregierbarkeit der verschiedenen Risiken ist eine Voraussetzung für die Erstellung der genannten Kurve. Nur so hat man im Kosten-Wirksamkeits-Diagramm der Massnahmen auf beiden Achsen Geldeinheiten. Die Kosten für die Schutzmassnahmen sind auf der Abszisse und die Risikogrösse auf der Ordinate (vgl. Abb. 3). Im Rahmen dieser Monetarisierung wird dabei eine weitere wichtige Beurteilung vorgenommen, indem die verschiedenen Schadengrössen aufgrund der sog. Zahlungsbereitschaft bewertet werden. Darauf wird nachfolgend noch näher eingegangen.

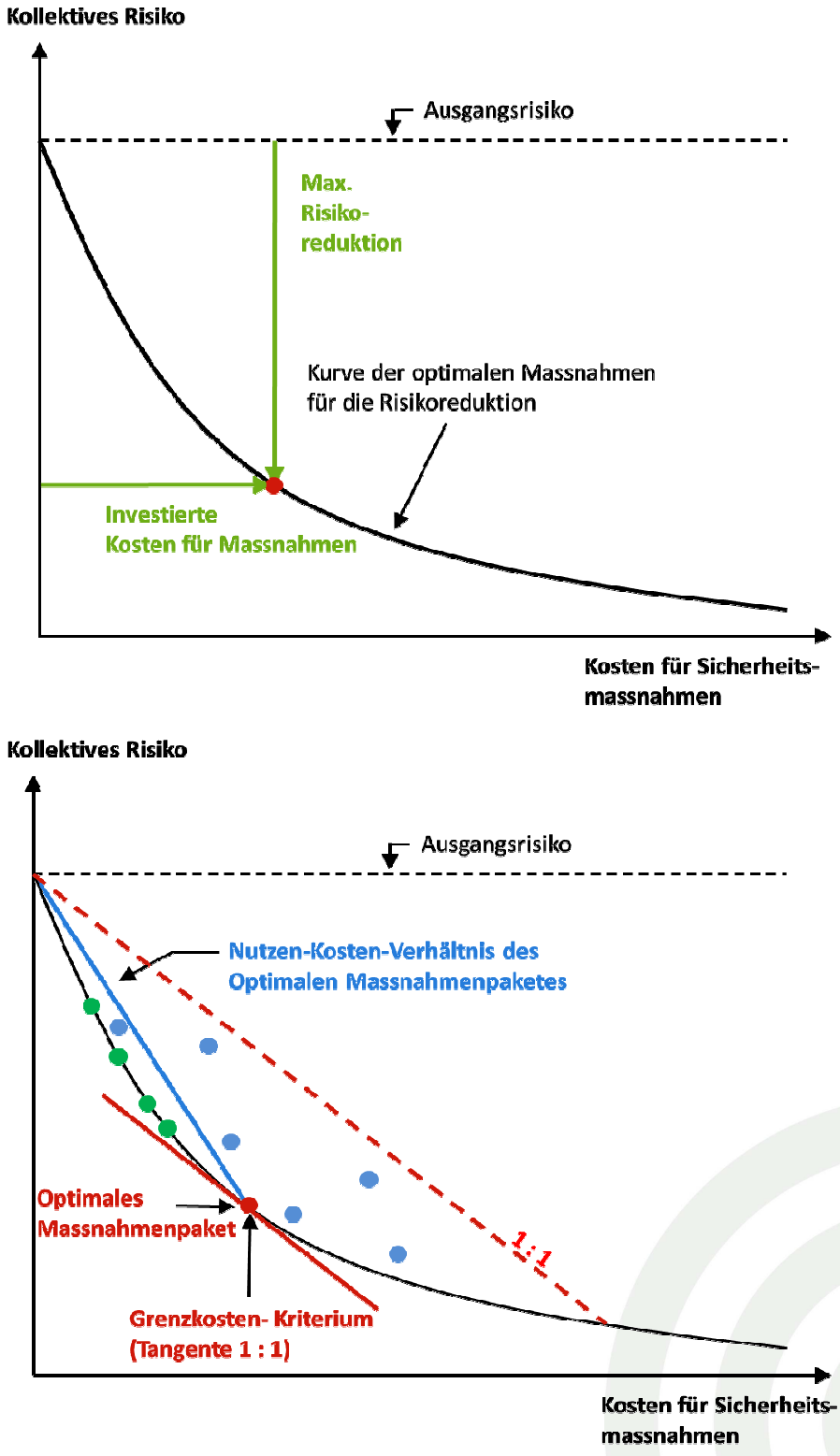


Abbildung 3: Das Prinzip der Grenzkosten. Die schwarze Kurve ist die untere Begrenzung sämtlicher Massnahmen. Auf ihr erzielen Massnahmen bei minimalen Kosten ein Maximum an Nutzen (=Risikoreduktion). Alle Massnahmen unterhalb der rot gestrichelten Linie (blaue Punkte) weisen zwar ein Nutzen-Kosten-Verhältnis über 1 auf, sind aber nur effizient bzw optimal, wenn sie auf der schwarzen Kurve bis zum roten Tangentenpunkt =Grenzkosten für Massnahmen liegen (grüne Punkte) (eigene Darstellung)

Eine solche Kurve ist naturgemäss zu Beginn am steilsten und verläuft mit zunehmenden Investitionen immer flacher, erreicht aber typischerweise nie die

Nulllinie. Die Frage ist, bis zu welchem Punkt man es als sinnvoll, angemessen, oder eben verhältnismässig *(Verhältnismässigkeit)* erachtet (oder Ressourcenmässig in der Lage ist), in eine weitere Reduktion der Risiken zu investieren. Die Kosten, die man (die Gesellschaft) für Sicherheitsmassnahmen gerade noch zu zahlen bereit ist, werden als *„Grenzkosten"* bezeichnet (vgl. Abb. 3).

Die Grundidee der Grenzkosten besagt nun, dass die Grenze der Verhältnismässigkeit dort erreicht ist, wo die Tangente mit der Neigung von -1 diese Kurve berührt. Man zahlt dort gerade 1 Franken für eine Massnahme pro 1 Franken Schadenreduktion (Abb. 3). Diese einfache Regel gilt allerdings nur, wenn die Bewertung des Schadens mittels der verschiedenen Schadenindikatoren in der Monetarisierung adäquat erfolgt ist. Dasselbe gilt auch für die Berücksichtigung der Risikoaversion. Abbildung 3 zeigt auch, dass alle Massnahmen unterhalb der rot gestrichelten Linie (blaue Punkte) zwar ein Nutzen-Kosten-Verhältnis über 1 aufweisen, aber nur effizient bzw optimal sind, wenn sie auf der schwarzen Kurve bis zum roten Tangentenpunkt, den Grenzkosten für Massnahmen liegen.

Grenzkosten vs. Nutzen-Kosten-Verhältnis

Die Grenzkosten sind dabei nicht zu verwechseln mit dem Nutzen-Kosten-Verhältnis (Sekante) des entsprechenden Massnahmenpaketes (vgl. Abb. 3). Solange die Grenzkosten noch nicht erreicht sind, ist die Neigung der Nutzen-Kosten-Kurve in jedem Falle grösser als die Neigung der Grenzkostentangente. Sicherheitsmassnahmen sind kostenwirksam (und somit eigentlich angemessen), wenn der Quotient aus Risikoreduktion und Sicherheitskosten über 1 liegt. Sie sind kostenneutral, wenn der Quotient aus Risikoreduktion und Sicherheitskosten gleich 1 ist, und sie sind nicht mehr kostenwirksam, wenn der Quotient aus Risikoreduktion und Sicherheitskosten unter 1 liegt. Dabei geht aus Fig. 3 hervor, dass zwar alle Massnahmen unterhalb der rot gestrichelten Linie kostenwirksam sind, aber dennoch weit vom optimalen Massnahmen-Paket liegen können und damit nicht ausgeführt werden sollten.

Unterschiedliches Restrisiko verbleibt – es gibt kein einheitlich akzeptiertes Restrisiko

Damit wird auch deutlich, dass im kollektiven Risiko das verbleibende Risiko sehr unterschiedlich hoch sein kann. Es gibt somit kein einheitlich definierbares „akzeptiertes Restrisiko", an dem die resultierende Sicherheit für Menschen, Sachwerte und die Umwelt festgemacht werden kann, wie dies beim individuellen Risiko mit der Festlegung einer Untergrenze der Todesfallwahrscheinlichkeit für ein Individuum möglich ist.

Grenzkosten verbinden technisch-ökonomische Aspekte mit gesellschaftspolitischen Aspekten

Die hier dargelegten Grundsätze der Verhältnismässigkeit der Grenzkosten und der Zahlungsbereitschaft als Basis für die Monetarisierung, aber auch die Risikoaversion beinhalten neben einer technischen und einer ökonomischen auch eine im Recht verankerte Komponente sowie eine eindeutig politische Komponente. Diese Sichtweise findet sogar weit über den Bereich der Sicherheitsplanung Anwendung und gilt ganz allgemein für die verschiedensten Bereiche gesellschaftlicher Aktivitäten (z.B. Gesundheitswesen[21], Umweltschutz etc.). Das Prinzip liegt letztlich (allerdings nur implizit) auch den Festlegungen auf den in Kap. 4 dargelegten Level 1 und Level 2 der Schutzziel-Pyramide zugrunde.

Zahlungsbereitschaft zur Rettung von Menschenleben

Die Zahlungsbereitschaft hängt naturgemäss vom zu schützenden Objekt bzw. von der Art des Schadens ab. Es sei hier bereits kurz auf die Zahlungsbereit-

[21] Gutzwiler et al. (2012): *Methoden zur Bestimmung von Nutzen bzw. Wert medizinischer Leistungen und deren Anwendung in der Schweiz und ausgewählten europäischen Ländern.* Akademien der Wissenschaften Schweiz. Bern.

schaft bei den zwei der wichtigsten Schadenkategorien bzw. Schadenindikatoren eingegangen:

- **Rettung von Menschenleben:** Seit längerem wird der Frage nachgegangen, wie viel die Gesellschaft bereit ist, für die Rettung eines Menschlebens auszugeben. Diese Frage ist nicht mit der Frage nach dem Wert eines Menschenlebens zu verwechseln. Derzeit schwanken die in der Schweiz diskutierten Werte zwischen 4 – 10 Mio. CHF. Der vom BABS im SKI Leitfaden favorisierte Wert von CHF 4 Mio. bildet somit die unteren Grenze.
- **Materielle Schäden:** In anderen Beispielen wurde dieselbe Fragestellung für materielle Schäden untersucht. Hier geht es also um die Frage, bis zu welchem Kostenaufwand man Sicherheitsmassnahmen gegen Risiken mit materiellen Schäden vorsieht. D.h.: Wie viel darf eine Sicherheitsmassnahme kosten, die einen Schadenerwartungswert von x Franken verhindert? Das Gebot der Verhältnismässigkeit gebietet, dass eine Massnahme nicht teurer sein sollte, als der mögliche Schadenerwartungswert, d.h. maximal 1 Franken an Massnahmen-Kosten für 1 Franken an Schadenreduktion.

Grundsätzlich gilt das Prinzip der Verhältnismässigkeit auch für das individuelle Risiko. Da hier aber die Einhaltung von Risikogrenzwerten für Personen Priorität hat, steht zunächst deren Einhaltung im Vordergrund. In Fällen, in denen übermässige Anstrengungen zu ihrer Einhaltung sich als erforderlich zeigten, wurden auch hier Grenzkostenkriterien angewendet (z.B. maximal 3-fache Grenzkosten für Personenrisiken).

Grenzkostenansätze werden oft als rein ökonomische Betrachtung resp. Optimierung verstanden und daher skeptisch aufgefasst. Es ist aber festzuhalten, dass der finanzielle (indirekt auch personelle) Aufwand, den man für die Erhöhung von Sicherheit aufwenden kann, immer beschränkt ist und in Konkurrenz zu anderen Anliegen der Gesellschaft steht. Ökonomisch-politische Fragen sind daher zwingende und massgebende Bestandteile von Sicherheitsentscheiden.

Sicherheit muss nicht teuer sein. Die Grenzkosten garantieren die Verhältnismässigkeit

Es gibt sowohl den Fall, in dem nicht realisiert wird, für wie wenig Geld die Verletzlichkeit von Systemen und damit die Sicherheit verbessert werden könnte (z.B. Einsturz von Fabrikationshallen beim Erdbeben von Modena 2011 wegen ungenügenden Auflageflächen der Deckenträger). Es gibt aber auch den Fall, in dem mit absoluten Sicherheitskriterien (Grenzwerte) implizit unbezahlbare Sicherheitsanforderungen postuliert werden. Die entsprechenden Massnahmen werden dann in der Praxis letztlich einfach nicht umgesetzt und damit die Schutzziele implizit tiefer angesetzt. Dies zeigt die grosse Bedeutung der Transparenz von Sicherheitsbeurteilungen.

Wie bereits mehrfach erwähnt, sind die drei Elemente der Sicherheitsplanung (Risikoanalyse, Risikobewertung und Massnahmenplanung) miteinander eng verknüpft sind (vgl. Abb. 7). Es wird zudem deutlich, wie sich bei diesem Vorgehen letztlich das verbleibende Risiko ergibt: nicht als Grenzwert, sondern als Folge dieser Kosten-Optimierung am Punkt, an dem eine weitere Risikoreduktion unverhältnismässig wird (vgl. Abb. 3).

Grenzkostenansatz

Grundsätzlich lässt sich festhalten, dass der Grenzkostenansatz ermöglicht:

- die begrenzten finanziellen Mittel richtig einzusetzen und für die eingesetzten Mittel ein Maximum an Personen- und Sachschäden verhindert werden kann.
- eine günstige Kostenwirksamkeit zu erreichen, bei der der Nutzen höher ist als der Aufwand.

- die Risiken aus verschiedenen Bereichen miteinander zu vergleichen resp. nach einem einheitlichen Massstab zu bewerten
- Resultate und Entscheide transparent und plausibel auf der Basis gesellschaftlicher Grundwerte darzustellen und nachvollziehbar zu dokumentieren
- dass verschiedene Anwender bei der gleichen Problemstellung weitgehend zum gleichen Resultat kommen, d.h. zu einem ähnlichen Mass an Risikoreduktion.

Der Grenzkosten-Ansatz stellt indessen nicht das alleine ausschlaggebende Entscheidungskriterium dar, ob und welche Massnahmen realisiert werden oder nicht. Divergierende Interessen von Politik, Gesellschaft, Wirtschaft oder Umwelt können ein Abweichen von der optimalen Massnahmenkombination nötig machen bzw. rechtfertigen. Dabei ist darauf zu achten, dass sich die geplanten Massnahmen trotzdem an der Grenzkosten-Kurve orientieren. Dies garantiert einen maximalen Kosten-Nutzen- (d.h. Risikoreduktions-) Effekt. Damit diese zusätzlichen politischen, sozialen, wirtschaftlichen und ökologischen Aspekte berücksichtigt werden können, und die Verhältnismässigkeit der Massnahmen beurteilt werden kann, ist eine fundierte, nachhaltige Güterabwägung nötig. Nur so können transparente und konsistente Entscheide getroffen werden (vgl. dazu auch Hepperle 2011)

3.7 Schadenindikatoren: Schutz- und Leistungsziele

Schutz- und Leistungsziele als zwei grundsätzlich verschiedene Ansätze, für Massnahmen

Die im Leitfaden SKI vorgesehene Risikoanalyse beruht auf dem Ansatz der Beurteilung von Risiken als Funktion von Wahrscheinlichkeit w und Auswirkungen A von ausgewählten Gefährdungen auf KI-Objekte und deren Komponenten. Dieser Ansatz ist der heute übliche, wenn von Risikoanalysen die Rede ist. In der Regel geht es darum, die Auswirkungen von schädlichen Ereignissen zu ermitteln und in Grenzen zu halten. Die Auswirkungen werden anhand von verschiedenen Schadenindikatoren beschrieben bzw. quantifiziert. Dazu werden im SKI-Leitfaden verschiedene Schadenindikatoren vorgeschlagen, die individuell je nach KI-Objekt angewendet werden sollen (z.B. Todesopfer, materielle Schäden, ökonomische Verluste, Umweltschäden etc.). Die Thematik der Einbussen in der Funktionstüchtigkeit von zivilisatorischen Systemen (Infrastrukturen), wie sie im Rahmen von SKI aufgeworfen wird, ist bisher kaum in die Diskussion von Schadenindikatoren eingeflossen.

Unabhängig von der Auswahl und Verwendung der verschiedenen Schadenindikatoren, stellt sich die Frage, ob und wie der Erhalt der Funktionstüchtigkeit bzw. der Leistungsfähigkeit von KI-Objekten, z.B. in Form einer Begrenzung von Ausfallzeiten bei IT-Systemen oder der Definition von minimalen Verfügbarkeiten bei Transportanlagen, zusätzlich zur Schadenminderung im Sinne von Schutzzielen festgelegt werden könnte.

Wie können Schäden und Nutzen direkt verglichen werden?

Damit stellt sich grundsätzlich die Frage, ob und wie die Problematik der klassischen Schadenminimierung und diejenige der Funktionserhaltung aneinander gekoppelt werden können. Schadenindikatoren sind an eine Risikoanalyse auf der Basis möglicher Gefährdungsszenarien gebunden, Leistungsindikatoren sind hingegen zusätzlich an Betriebszustände und daraus resultierende Funktion bzw. Nutzen gekoppelt, wobei diese Nutzen auch immaterieller Art sein können. Schäden und Nutzen müssen damit direkt miteinander verglichen werden können. Dabei steht die menschliche Sicherheit in der Regel und zu Recht im Zentrum, führt aber andererseits auch dazu, dass materielle Folgeschäden bzw. indirekte Schäden häufig ausgeblendet werden, weil sie schwierig zu erfassen

sind. Im Folgenden wird diese Kopplungs-Problematik dadurch gelöst, dass eine Nutzenreduktion als Schadengrösse eingeführt wird. Damit können Schäden und Nutzen in einer gemeinsamen Analyse zusammengeführt werden.

Bei den Auswirkungen bzw. Risiken für KI-Objekte infolge verschiedener Gefährdungsszenarien ist grundsätzlich zwischen zwei Schadenarten zu unterscheiden (vgl. Tab. 1):

1. Den direkten oder unmittelbar mit dem Schadenereignis verbundenen Auswirkungen bzw. Schäden, also im Besonderen den unmittelbaren Todesopfern eines Ereignisses und den direkten materiellen Schäden, wie z.B. die Zerstörung von Anlagen
2. Den indirekten Schäden oder Folgeschäden eines Ereignisses, also im Besonderen den Schäden infolge eines mehr oder weniger langen Ausfalls der Funktion oder der reduzierten Leistungs- bzw. Funktionsfähigkeit eines KI Objektes

Bisherige Risikobeurteilungen, sowohl bei Naturgefahren, aber auch bei technischen Anlagen konzentrieren sich in der Regel auf die direkten Schadenwirkungen. Als Beispiel sei die Gefährdung von Verkehrswegen infolge Naturgefahren (Lawinen, Steinschlag etc.) erwähnt. Hier ist die Risikobeurteilung primär auf Personenopfer und evtl. noch auf direkte Sachschäden ausgerichtet, erst ansatzweise aber auf die Auswirkungen als Folge einer eingeschränkten Benutzbarkeit (Funktion) des Verkehrsweges. Diese Vereinfachung wird nicht zuletzt mit Verweis auf die Schwierigkeiten einer solchen Beurteilung vorgenommen, ohne dass dabei aber die hohe Relevanz dieser zwei Aspekte sachlich geklärt ist. Als Folge fehlen heute entsprechende methodische Ansätze und Erfahrungen (monetärer Art) weitgehend.

Die Kenntnis über Folgeschäden ist heute noch rudimentär

Im Falle von SKI ist nun aber die Funktion der KI-Objekte von zentraler Bedeutung, und damit auch die Frage geeigneter Schutz- und Leistungsziele, welche gerade diese Folgeschäden betreffen. Dass diese Diskussion nun im Zusammenhang mit den Schutzzielen aufkommt, hängt damit zusammen, dass jede Schutzzieldiskussion damit beginnen muss, ob überhaupt Indikatoren gewählt wurden, die für eine Beurteilung der übergeordneten Ziele geeignet bzw. repräsentativ sind (vgl. Abb. 4).

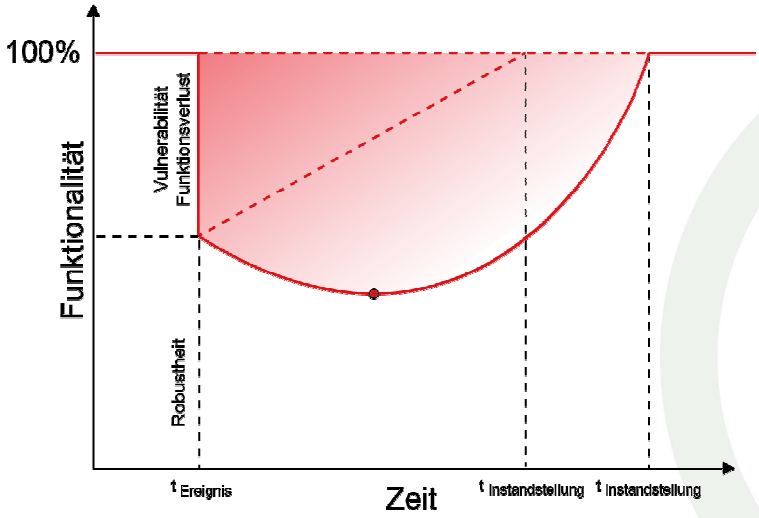


Abbildung 4: Ein Schadenereignis führt zu einem plötzlichen Funktionsverlust mit in der Regel reduzierter Funktionalität über längere Zeit(Folgeschäden) (eigene Darstellung).

Ein KI-Objekt erleidet zum Zeitpunkt des Eintritts eines Ereignisses einen bestimmten Funktionsabfall. Dieses Ausmass wird durch die Robustheit des Systems beeinflusst. Die Verletzlichkeit im Sinne dieses primären Funktionsverlustes kann durch vorbeugende Massnahmen beeinflusst werden. Der primäre Funktionsverlust führt in der dem Ereignis nachgelagerten Zeitspanne zu weiteren Ausfällen und Schäden.

Resilienz kann Folgeschäden stark eindämmen

Die Schäden in dieser nachgelagerten Phase können dabei bedeutend grösser sein, als die direkten Schäden aus dem primären Funktionsabfall. Je rascher ein System wieder seine ursprüngliche Funktionsfähigkeit erreicht hat, und je kleiner die nachfolgenden direkten und indirekten Schäden gehalten werden können, desto grösser ist die Resilienz dieses Systems. Resilienz wird primär durch Massnahmen in der Vorbeugungs-, Interventions- und der Wiederinstandstellungs-Phase beeinflusst. Schutzmassnahmen für KI-Objekte haben demnach zu berücksichtigen:

1. Das Ausmass eines Funktionsabfalls (primärer Schaden)
2. Das Ausmass der Folgeschäden durch Versagen weiterer Systeme, d.h. einer weiteren Abnahme der Funktionsfähigkeit
3. Das Ausmass indirekter Schäden (können auch noch auftreten, nachdem das primär ausgefallene System seine Funktionsfähigkeit wieder voll erreicht hat).
4. Die Zeitdauer, die benötigt wird, ein System wieder funktionsfähig zu machen (sog. „Recovery time“)

Eine umfassende und differenzierte Analyse dieser verschiedenartigen Wirkungen und ihrer jeweiligen Bedeutung bei Schadenereignissen hat bis heute nicht stattgefunden. Sie wäre aber eine nötige Grundlage für die Definition geeigneter Indikatoren und in der Folge entsprechender Schutzziele für eine Risiko- und Schutzplanung, wie sie im Rahmen von SKI erforderlich und gewünscht ist.

Versucht man, aufgrund der verschiedenen möglichen Situationen eine schematische Gliederung für die Wirkungen von Schadenereignissen festzulegen, bietet sich die in Tabelle 1 aufgeführte Matrix an:

Tabelle 1: Direkte und indirekte Schäden im Bereich Sicherheit und Nutzen (Funktionserhalt)

	Sicherheit	**Funktionserhaltung**
Direkte bzw. unmittelbare Schäden	Personenschäden Güter, Umwelt, immaterielle Werte	Unmittelbare Funktionseinbussen z.B. durch die Zerstörung von Anlagen
Indirekte bzw. Folgeschäden	Verzögerte Schäden Personen, Güter, Umwelt, immaterielle Werte	Reduzierte Funktion und Verfügbarkeiten bis zur Wiederherstellung

Unter Sicherheit wird dabei insbesondere der Schutz von Leib und Leben, aber auch von Gütern und immateriellen Werten verstanden. Mit Funktionserhaltung wird die Erhaltung der Leistung eines KI-Objektes verstanden. Sowohl Auswirkungen im Sicherheitsbereich wie auch Funktionseinbussen fallen aber letztlich unter den Oberbegriff „Schäden".

Die klassischen Risikobeurteilungen befassen sich typischerweise mit dem Feld „Sicherheit/direkte Schäden", wozu auch die meisten methodischen Ansätze und Erfahrungen vorliegen. Ein Mangel ist bis heute, dass der Aspekt der indirekten und Folgeschäden in der Regel nur ansatzweise und pauschal berücksichtigt wird[22]. Dementsprechend sind auch die methodischen Hilfsmittel für ihre Beurteilung weniger entwickelt.

Die direkten Schäden sind primär bedingt durch die Vulnerabilität eines KI-Objektes und seiner Komponenten, während die indirekten Schäden oder Folgeschäden nach dem eigentlichen Ereignis bis zur Wiederinstandstellung des Ausgangszustandes resultieren (vgl. Abb. 4).

Bei der Funktionserhaltung wird primär an die Folgeschäden gedacht. Diese Art von Beurteilung ist bis heute eher Gegenstand von betrieblichen Risikomanagementsystemen, wie ISO 31000 u.a.m.. Während im Bereich Sicherheit heute zunehmend quantitative, probabilistische Beurteilungen durchgeführt werden, sind die betrieblichen Risikomanagementsysteme noch weitgehend qualitativ und weniger systematisch strukturiert[23].

Schadenrisiko als indirekte, inverse Messgrösse für den Leistungsverlust

Der Leitfaden SKI sieht vor, die Risiken bei KI-Objekte aufgrund der Schadenauswirkungen zu beurteilen. Die Risiken werden dazu nach üblicher Manier mit dem Produkt aus w x A ermittelt, wobei das Ausmass A mit verschiedenen Schadenindikatoren gemessen wird. Dementsprechenden wird dann unter dem Thema Schutzziele nach Kriterien für die Limitierung des Schadenrisikos gesucht. Implizit wird dabei wohl angenommen, dass je geringer das Schadenrisiko ist, umso grösser die Widerstandsfähigkeit (Robustheit) des Objektes ist und damit auch die zu erwartende Funktionswahrscheinlichkeit oder Leistungsfähigkeit. Das Schadenrisiko wird somit als indirekte, inverse Messgrösse für den Leistungsverlust genommen.

Die Quantifizierung des Ausmasses A setzt voraus, dass die auf einen Prozess respektive die jeweilige Gefährdung anzuwendenden Schadenindikatoren quantifiziert und aggregiert werden können, d.h. addierbar gemacht werden. Als verbreitetste Methode zur Quantifizierung des Ausmasses wird die Monetarisierung empfohlen. Damit ist eine auf Franken reduzierte Aggregation der verschiedenen Risikobeiträge möglich. Dies ist insbesondere auch mit Blick auf die Beurteilung der Kosten-Wirksamkeit von Massnahmen notwendig.

Ein unvollständiges Set an Indikatoren führt zu einer ungenügenden Risikobeurteilung

Der Festlegung der Schadenindikatoren kommt daher eine zentrale Bedeutung zu, sowohl bei der Risikoanalyse, wie auch bei der Risikobewertung. Letztlich beziehen sich die Schutzziele auf diese Schadenindikatoren. Ein unvollständiges Set an Indikatoren kann im Rahmen der Festlegung von Schutzzielen nicht korrigiert werden. Der SKI-Leitfaden gibt einige Indikatoren vor, mit denen ein Funktionsverlust erfasst werden kann. Die ersten Erfahrungen im Umgang da-

[22] Der in Risikoanalysen oftmals berücksichtigte Effekt einer sog. Risikoaversion beinhaltet implizit u.a. auch den Aspekt der indirekten und Folgeschäden (vgl. Bericht BABS/Planat (2008): Risikoaversion)

[23] Erwähnt sei immerhin die bekannte Methode FME = failure mode and effect

mit werden zeigen, ob das an sich wichtige Anliegen der Funktionserhaltung durch die im Leitfaden vorgeschlagenen Indikatoren genügend erfasst ist.

Sicherheit und Funktionserhalt als zwei separate Oberziele?

Eine separate Beurteilung der beiden Oberziele „Sicherheit“ und „Funktionserhaltung“ könnte u.U. eine grössere Transparenz im Umgang mit diesen beiden doch grundsätzlich sehr verschiedenen Zielen ermöglichen. Es fragt sich dabei, ob man auch bei der Funktionserhaltung mit monetären Nutzengrössen arbeiten will, oder ob nun Ausfallzeiten, Leistungsniveaugrössen etc. als Ziele zum Zuge kommen sollen. Bei der Frage der Nutzen/ Kosten-Optimierung und damit auch der Schutzziele würde man damit allerdings weitgehend Neuland betreten und nicht wie bei der klassischen Risikoanalyse auf eine bereits recht breite Erfahrungen zurückgreifen können. Mittels Monetarisierung der entsprechenden Grössen könnte auch hier mit Grenzkostenkriterien gearbeitet werden und jede Massnahme für sich getrennt optimiert werden. Auf der Basis einer genügenden Anzahl solcher Einzeloptimierungen könnten diese Erfahrungen schliesslich zu branchenbezogenen Zielen auf der Massnahmenebene Level 2 der Schutzzielpyramide (siehe Kap. 4) führen.

Methodisch wären deshalb beide Oberziele (Sicherheit und Nutzen/Funktion) grundsätzlich gleich zu behandeln, aber mit zwei getrennten Indikatorensets zu beurteilen und bis und mit Schutzzielen resp. Nutzen/Kosten-Optimierung separat zu bearbeiten. Der Hauptnachteil eines solchen Konzeptes würde darin bestehen, dass wahrscheinlich diverse Massnahmen beiden Zielen dienen, d.h. sowohl für die Schadenreduktion, als auch für die Funktionserhaltung wirksam sind, und deshalb eine zweigeteilte Beurteilung und Optimierung die gewünschte Übersichtlichkeit wieder (zer)stört.

Eine auf maximale Übersichtlichkeit ausgelegte und differenzierte Gesamtanalyse und Resultatdarstellung vermag deshalb vermutlich die geforderte Transparenz zweckmässiger zu erreichen. Schutz- und Leistungsziele, welche in einem hierarchischen Ansatz entsprechend der Schutzzielpyramide zu definieren sind, können dabei gezielt auf die zwei Oberziele ausgerichtet werden.

Vorderhand ein gemeinsames Indikatoren-Set und auf Grenzkosten basierende gemeinsame Massnahmen

Angesichts der sehr komplexen Fragestellung scheint ein Vorgehen mit einem einzigen Indikatorenset für Sicherheit und Funktionserhaltung und einer auf Grenzkosten basierenden, gemeinsamen Massnahmenplanung für den gegenwärtigen Zeitpunkt am sinnvollsten. Die Planungsinstrumente müssen so strukturiert werden, dass die Entstehung der Resultate jederzeit rückverfolgt werden kann. Die Monetarisierung der Indikatoren zur Beurteilung der Funktionserhaltung hat als Konsequenz strikte in Form des Ausmasses an Schäden infolge Funktionseinbussen zu erfolgen.

Das Primat der Verhältnismässigkeit der Investitionen für die zu tätigenden Massnahmen mittels der Grenzkosten bleibt als einheitliches übergeordnetes Schutzziel für die Einhaltung der Sicherheit und den Erhalt der Funktionen bestehen. Analog wie im Bereich Sicherheit auf der Basis einer umfassenden Beurteilung letztlich Aussagen zu den Restrisiken gemacht werden können, werden sich im Bereich der Funktionserhaltung analoge Aussagen zur verbleibenden Funktionstüchtigkeit von Objekten machen lassen.

Zur Gewährleistung einer einheitlichen Beurteilung im Rahmen SKI sind entsprechende Vorgaben, sowohl was die Indikatoren (inkl. Monetarisierungsprinzip) als auch das methodische Vorgehen betrifft, erforderlich.

3.8 Übersicht über den Stand bestehender Risiko- und Sicherheitsansätze

Einige der heute gängigen Risiko- und Sicherheits-Ansätze finden in verschiedenen Bereichen ihre Anwendung, insbesondere in der Technik. Die zahlreichen Ansätze gehen aber nur andeutungsweise auf die Schutzziele ein. Als erfreulich ist festzustellen, dass immer wieder auf die Kosteneffizienz hingewiesen wird. Einzelne weitere risikobasierte Elemente (z.B. Grenzwerte für das individuelle Risiko) sind vorhanden.

So ist z.B. **ALARA** *(*As Low As Reasonably Achievable) eine Leitlinie, die primär für den Strahlenschutz konzipiert wurde. ALARA wird für die Minimierung von Strahlendosen und der Freisetzung von radioaktiven Stoffen durch den Einsatz aller angemessenen Methoden verwendet. Sinngemäß übersetzt fordert das ALARA-Prinzip, beim Umgang mit ionisierenden Strahlen eine Strahlenbelastung von Menschen, Tieren und Material (auch unterhalb von Grenzwerten) so gering zu halten, wie dies mit vernünftigen Schutzmassnahmen machbar ist. ALARA ist dabei nicht nur ein Sicherheits-Prinzip, sondern auch eine regulatorische Anforderung für alle Strahlenschutz-Programme, die obligatorisch sind in vielen Ländern. Das Prinzip lässt sich genauso auf jede Art des Umgangs mit schädlichen oder potentiell schädlichen Einflüssen übertragen, hat aber nur im Strahlenschutz wesentlichen Einfluss. In der Anwendung des ALARA-Prinzips als kritisch zu sehen ist die Tatsache, dass dieser Ansatz keine Informationen liefert, der eine Differenzierung nach Prioritäten erlauben würde. Offen bleibt auch die Frage, was als „so gering wie vernünftigerweise erreichbar“ anzusehen ist. Ein „Ranking“ von Risiken wäre aber für das Risikomanagement und für die Prioritätensetzung hilfreich und nötig. Schliesslich liegen damit keine vergleichbaren Aussagen über die Restrisiken und die Effizienz der Massnahmen vor.

Demgegenüber ist **ALARP** (As Low As Reasonably Practicable) ein im Risikomanagement verwendetes Prinzip, das aus der britischen Art der Festlegung von Sicherheit entstanden ist. Die Verpflichtung zur Einhaltung der Sicherheit liegt beim Verursacher des Risikos, der die Behörde überzeugen muss, dass beim Management der industriellen Aktivitäten das ALARP-Prinzip befolgt wird; d.h. dass die Sicherheit überwacht wird; und dass die Vorkehrungen für einen Unfall angemessen vorhanden und für die unmittelbare Umgebung auch Schutz geboten werden kann. Schliesslich beruht ALARP auf einem einfachen Kosten/Nutzen-Vergleich. Innerhalb eines Risikomanagementprozesses wird mit Hilfe einer Risikomatrix festgelegt, welche Risiken im akzeptablen Bereich liegen, welche Risiken im ALARP-Bereich liegen und welche im inakzeptablen Bereich liegen. Die Einstufung in der Risikomatrix erfolgt in der Regel projektspezifisch und setzt voraus, dass die beiden Parameter *Eintrittswahrscheinlichkeit* und *Schadensausmaß* definiert sind. In einem kontinuierlichen Risikomanagementprozess werden vorhandene Risiken fortlaufend überwacht und bewertet sowie neue Risiken identifiziert. Risiken, die im inakzeptablen Bereich liegen, müssen durch risikoverringernde Maßnahmen in den ALARP-Bereich gebracht werden. Ist dies nicht möglich, so ist mit Hilfe einer Kosten/Nutzen-Analyse (Cost-Benefit Analysis) zu klären, ob der zu erwartende Nutzen die Risiken überwiegt. Auch beim ALARP finden sich keine konkreten Angaben, was intolerabel etc. ist. Es muss sogar angenommen werden, dass zum Teil kein Unterschied zwischen individuellem und kollektivem Risiko gemacht wird.

Beim **GAMAB und GAME** (Globalement Au Moins Aussi Bon, oder GAME-Globalement Au Moins Equivalent) handelt es sich um Methoden, die v.a. im

frankophonen Raum angewendet werden. Hierbei ist nachzuweisen, dass ein neuartiges System mindestens so gut ist, wie das bisher verwendete System. In Bezug auf das Verkehrssystem basiert dieses Kriterium z.B. auf der Voraussetzung, dass das gesamte Risiko in einem neuen schienengebundenen Verkehrssystems das gesamte Risiko in vergleichbaren bestehenden Systemen nicht übersteigen darf. Die Nachteile dieses Ansatzes sind evident.

Die verschiedenen Ansätze machen zwar gewisse Angaben zum individuellen Risiko, lassen aber den Umgang mit dem kollektiven Risiko nur erahnen, oder lassen ihn gänzlich ausser Acht. Es lässt sich summarisch festhalten, dass eine konzeptionelle, umfassende Diskussion und Begründung von Schutzzielen nur andeutungsweise vorhanden ist. Damit ist deren Anwendbarkeit für die Thematik Schutzziele bei KI-Objekten nicht gegeben. Als erfreulich ist immerhin festzustellen, dass immer wieder auf die Kosteneffizienz hingewiesen wird.

Die mit der Erarbeitung des Kapitel 3 einhergegangene detaillierte Literaturreview (Liste der verwendeten Literatur s. Anhang) hat gezeigt, dass es kein umfassendes Verständnis des Terms ‚Schutzziele' oder verwandter Konzepte gibt (siehe z.B. CRN und CSS 2010a), auch wenn der Schutz kritischer Infrastrukturen in den meisten Industrieländern Teil der nationalen Sicherheitsstrategien ist (vgl. BABS 2012b, Government of Australia 2004, Government of Canada 2009, Government of the United States 2007, UK Cabinet Office 2009). Bestehende Aussagen zu Schutzzielen und Schutzstrategien sind deshalb generell vage, und in der Regel nur abstrakt formuliert. In den meisten Ländern sind die Risiken, die eingegangen werden können/dürfen, nur qualitativ definiert und werden nicht quantifiziert. Nur in wenigen Ländern werden Risiken wirklich quantifiziert, oder gar durch einen Parlamentsbeschluss festgelegt (z.B. Niederlande).

Eine Ausnahme bilden Risiken bei Industrieanlagen, wo die Diskussion über quantifizierte und vertretbare Risiken vergleichsweise weit fortgeschritten ist. Der Schwellenwert des nicht vertretbaren, jährlichen Todesfallrisikos scheint sich im Wesentlichen im Bereich von 10^{-4} bis 10^{-6} zu bewegen (CRN und CSS 2010a). Todesfallrisiken sind denn auch das überwiegende Kriterium, wenn es um die quantitative Festlegung von Grenzwerten geht (z.B. ESCIS 1996, SFK 2004, PLANAT 2008). Zusammengefasst kann gesagt werden, dass die bestehende Literatur zum Thema Schutzziele nur sehr wenig relevante Informationen bereithält.

4. Umfassende Sicht der Sicherheitsanstrengungen: Die Schutzziel-Pyramide

"Plan for the difficult whilst it is easy.
Act on the large while it's minute.
The most difficult things in the world begin with things that are easy."

Laozi, chinesischer Pilosoph, Begründer des Taoismus, 6. Jh. v. Chr.

4.1 Einleitung

Bei den im Rahmen von SKI zu beurteilenden KI-Objekten und Anlagen handelt es sich in der Vielzahl um bestehende Systeme. Der notwendige Schutz bzw. die Widerstandsfähigkeit dieser Systeme sollen aus Sicht SKI aufgrund einer breiteren Palette von Gefährdungen beurteilt werden. Dabei sind neben allenfalls neu vorzusehenden Schutzmassnahmen auch die zahlreichen, an den Objekten vorhandenen Schutz- und Sicherheitsmassnahmen und damit das bereits vorhandene Sicherheitsniveau für die Beurteilung relevant. Einerseits können sich auch bei den bestehenden Massnahmen Lücken zeigen, anderseits tragen die bestehenden Massnahmen u.U. auch zu den Sicherheitsanforderungen aus Sicht SKI bei.

Eine breite Sicht auf die Frage der Sicherheitsmassnahmen und damit der Schutzziele ist deshalb notwendig. Wie bereits in Kap. 3 erwähnt, werden Sicherheitsmassnahmen auf sehr verschiedene Art und auf verschiedenen Ebenen festgelegt. Dabei werden Schutzziele oft nur implizit definiert.

Schutzziel-Pyramide mit vier Levels

Für die Diskussion über und die Festlegung von Schutzzielen für kritische Infrastrukturen wird im Folgenden eine 4-stufige „Schutzziel-Pyramide“ vorgeschlagen. Folgende vier Levels der Schutzziel-Pyramide (Abb. 5 und Tab. 2) werden dabei unterschieden:

- Level 1: Etablierte Massnahmen
- Level 2: Mindestanforderungen
- Level 3: Risikobasierte Anforderungen und Grenzwerte
- Level 4: Kriterien der Verhältnismässigkeit, Grenzkosten

Diese vier Levels werden im Folgenden näher erläutert.

4.2 Level 1 – Etablierte Massnahmen

Festlegung konkreter Massnahmen nach dem Stand der Technik

Die älteste und nach wie vor verbreitetste Art, Sicherheit zu „definieren“ besteht in der Festlegung konkreter, gezielter Massnahmen, die sich nach dem „Stand der (Sicherheits-)Technik“ entwickelt haben. Diese Massnahmen können je nach Fall Gegenstand von offiziellen Normen und Vorschriften sein, oder auch quasi inoffiziell als gängige, „anerkannte Regeln der Technik“ Anwendung finden. Ein System gilt dementsprechend dann als „sicher“, wenn alle diese Massnahmen getroffen wurden. Sie lassen in der Praxis dementsprechend im Prinzip keinen Spielraum mehr. Auch heute noch kommt kein Bereich (zumindest in Teilbereichen) ohne diese impliziten „Sicherheitsziele“ aus.

Die Etablierung dieser Massnahmen erfolgt kontinuierlich, quasi „schleichend“, beruht auf Konsens von Fachleuten und ist erfolgsorientiert: Hat sich eine Massnahme zur Zufriedenheit aller Beteiligten über Jahre bewährt, wird sie von der involvierten Branche als „Stand der Technik“ akzeptiert. Andernfalls werden Korrekturen angebracht.

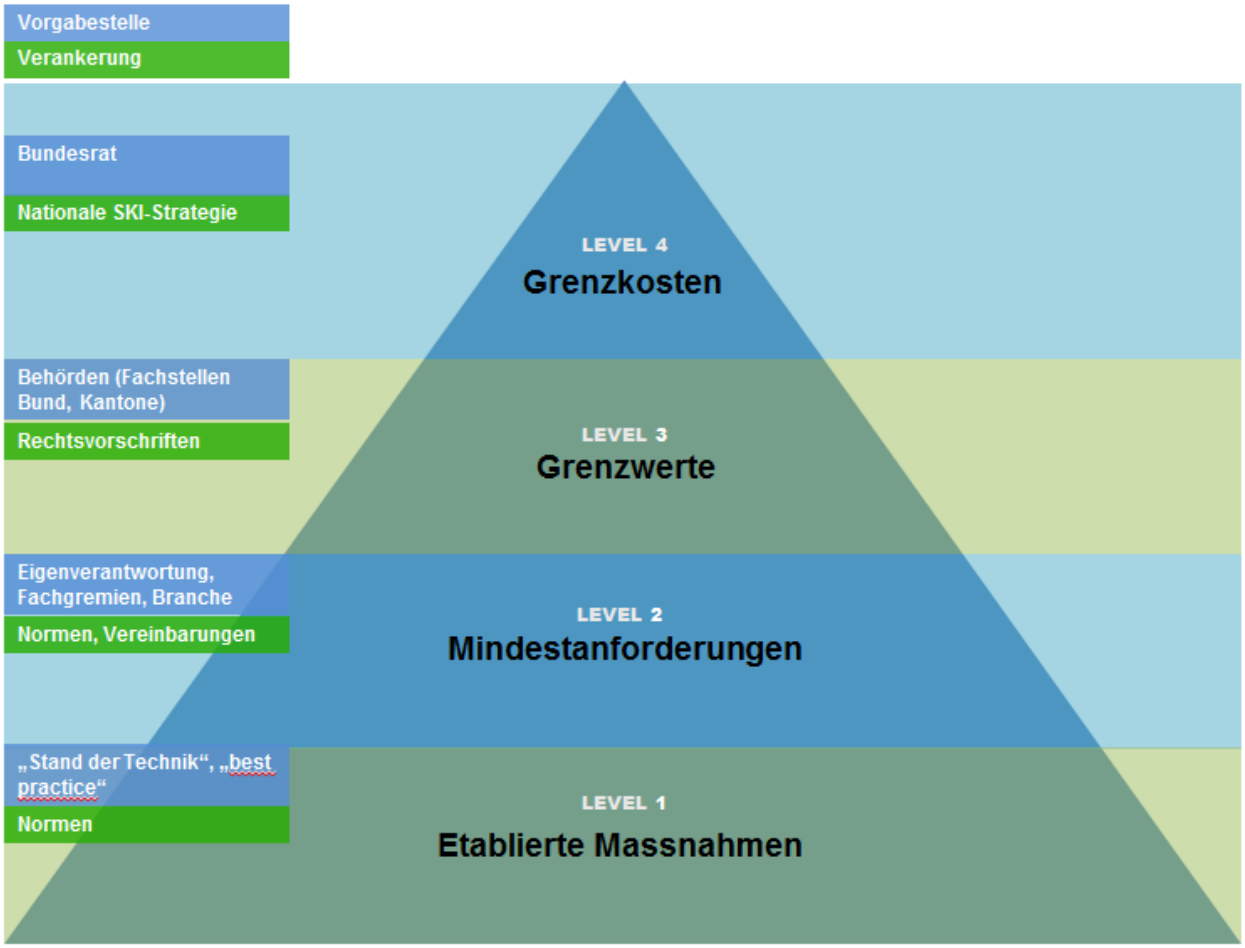


Abbildung 5: Die 4-stufige Schutzziel-Pyramide (eigene Darstellung)

4.3 Level 2 - Mindestanforderungen

Mindestanforderungen gemäss Normen und Standards

Level 2 bilden Regelungen, welche hier als Mindestanforderungen bezeichnet werden. Damit sind nicht mehr bereits etablierte Massnahmen wie in Level 1 gemeint, sondern Vorgaben, welche der Planung von erforderlichen Massnahmen zugrunde zu legen sind. Dazu gehören z.B. die Einhaltung der Nachweise der Tragsicherheit und der Gebrauchstauglichkeit, wie sie die Tragwerksnormen des Schweizerischen Ingenieur- und Architekten-Vereins SIA[24] festlegen, aber z.B. auch die Vorgabe bestimmter Periodizitäten für Hochwasser (Festlegung von „Bemessungs- und Sicherheits-Hochwasser im Wasserbau“[25]). Diese

SIA Normen

[24] SIA (2003). *SIA Norm 261 - Einwirkungen auf Tragwerke*, Schweiz. Ingenieur- und Architektenverein, Zürich.

[25] BfE (2008). *Sicherheit der Stauanlagen – Basisdokument zum Nachweis der Hochwassersicherheit.* Bundesamt für Energie, Bern. Juni 2008. 25p.

Normen und Regelungen dienen als Grundlage für die Planung von Massnahmenkonzepten.

Im Unterschied zum Level 1 wird im Level 2 typischerweise ersichtlich, gegen welche Art und Intensität von Einwirkungen die Massnahmen eine Anlage bzw. Bauwerk zu schützen haben. Dabei können unterschiedliche Massnahmen zur Erreichung des Schutzziels führen. In der Regel wird ein vollständiger Schutz gegen diese definierten Einwirkungen gefordert. Es besteht jedoch ein Spielraum für die Ausgestaltung der Massnamen, nicht aber hinsichtlich der geforderten Sicherheit.

Tabelle 2: Beschrieb der 4 Schutzziel-Levels in der Schutzziel- Pyramide.

Level	Art/Prinzip	Beschrieb
4	**Grenzkosten Verhältnismässigkeit Zahlungsbereitschaft zumutbare Sorgfaltspflicht**	Auswahl der optimalen Massnahmen auf der Basis von: • Sicherheitsebenen der KI-Objekte • Schadenindikatoren • Bedeutung von KI-Objekt/KI-Sektoren (Unterschiedliche Grenzkosten) • Allfälligen Risikokategorien analog „Freiwilligkeitsgrad“ (s. PLANAT) • Allfälliger Risikoaversion • Zahlungsbereitschaft • Kenntnis des verbleibenden Risikos
3	**Risikokonzept Grenzwerte**	Identifikation und Priorisierung des Handlungsbedarfs als Basis für die Massnahmenplanung auf Basis von: • Vorgaben für die Risikobeurteilung von KI (z.B. Tiefgang, Methodik für Risikoanalyse, Risikobewertung, Risiken in w –A – Diagramm) • Grenzwerte soweit anwendbar (für individuelles Risiko, Begrenzung des Ausmasses falls politisch gefordert und über Grenzkosten hinaus gehend
2	**Mindestanforderungen**	Mindestanforderung für Nachweis von Stand der Technik und gesetzlichen Vorgaben (Regelungen/Vorgaben, Standard, Normen, welche die Planung von Massnahmen bestimmen - z.B. Einhaltung der Nachweise der Tragsicherheit und der Gebrauchstauglichkeit der Tragwerksnormen des Schweizer Ingenieur und Architekten-Verein SIA. Keine Aussage über Grösse verbleibender Risiken ableitbar.

1	**Etablierte Massnahmen**	Konkrete, (technische) Massnahmen für den Nachweis des „Standes der Technik“ und gesetzlichen Vorgaben. Massnahmen nach „Stand der Technik“ vorgeschrieben. Massnahmen können je nach Fall Gegenstand von offiziellen Normen und Vorschriften sein, oder auch nur inoffiziell als anerkannte Regeln der Technik Anwendung finden, oder sind in Sicherheitsdokumenten (Dokumente die bei der Planung oder Beschaffung von Anlageteilen erstellt wurden) enthalten.

4.4 Festlegung von Standards bzw. impliziten Schutzzielen auf Level 1 und 2

Festlegung von Standards

Die Festlegung solcher Standards und Normen im Sinne der beschriebenen Massnahmen und Mindestanforderungen auf Level 1 und 2 erfolgt primär durch Fachleute. Dabei spielen Erkenntnisse aus der Wissenschaft, praktische Erfahrungen (insb. auch aufgetretene Schäden) und Konsens, aber auch „gesunder Menschenverstand“ eine wichtige Rolle. Hinzu kann, je nach Umstand, auch ein mehr oder weniger grosser Druck von wirtschaftlicher Seite kommen. Risikoüberlegungen, wie sie im nächsten Level 3 zum Tragen kommen, werden nur Ansatzweise und in der Regel nur implizit gemacht. Damit ist aber keine Aussage zum kollektiven Risiko gemacht. Nach schweren Unfällen kann auch ein gesellschaftlicher Druck ins Spiel kommen (z.B. . Tunnelbrand und Forderung nach Rettungstunnel, zweite Röhre).

Derartige Normen und Standards geben in der Regel über das verbleibende Risiko, wenn überhaupt, nur qualitativ und pauschal Auskunft. Eine beschränkte quantitative Aussage über die Restrisiken vermögen u.U. die Unfall- oder Schadenstatistiken zu erbringen.

Einhaltung der etablierten Massnahmen und Normen genügt in der Regel nicht.

Bereits an dieser Stelle ist wichtig, darauf hinzuweisen, dass die reine Einhaltung von etablierten Massnahmen und Normen in der Regel nicht genügt, einen adäquaten Schutz für kritische Infrastrukturen zu gewährleisten. Aussagen wie „Wir haben die Normen eingehalten“, ist mit dem Verweis auf die bereits angesprochenen, unbekannten Restrisiken zu begegnen.

4.5 Level 3 – Risikobasierte Sicherheitsbeurteilung

Mit Level 3 kommt Risikobasierte Sicherheitsbeurteilung zum Tragen

Ab Level 3 erfolgt die Sicherheitsbeurteilung rein risikobasiert. Level 3 legt die Methodik des risikobasierten Umgangs mit Gefährdungs- und Schadenszenarien und darauf basierenden Entscheidungskriterien fest. Dabei geht es einerseits um die eigentliche Risikoanalyse (Was kann passieren?) und anderseits um die anschliessende Risikobewertung (Was darf passieren?). Wie in Kap. 3 angedeutet, wurden in den letzten Jahrzehnten zunehmend und explizit Risikobeurteilungen vorgenommen und in einem beschränkten Kreis von Anwendungsbereichen eingeführt.

Im Falle von KI-Objekten geht es grundsätzlich um folgende zwei Ebenen:

1. Sicherheitsmassnahmen, die sich aus Anforderungen der Öffentlichkeit/Gesellschaft ergeben, also Verhinderung von Schäden für Dritte, aber auch teilweise die Anforderungen an die Sicherheit des Personals.
2. Sicherheitsmassnahmen, die den reibungslosen und effizienten Betrieb gewährleisten sollen (inkl. Verhinderung allfälliger Imageschäden)

Dies entspricht einigermassen dem Unterschied zwischen „Sicherheit“ und „Funktionserhaltung“ (vgl. Kapitel 3.7).

Dabei stellt sich hier die Frage, welche Sicherheitsaufwendungen heute normalerweise Sache des Betriebes sind bzw. zur erwarteten Sorgfaltspflicht gehören und demnach auch durch ihn zu finanzieren sind, aber auch welche Forderungen unter Berücksichtigung der Bedeutung als KI-Objekt über diese reine Betriebssicherheit hinausgehen und zum Schutz der Allgemeinheit in einer Krisensituation dienen.

Damit stellt sich im Falle von SKI nicht nur die Grundfrage:

Wie weit wollen wir uns schützen, also die gängige Schutzziel-Frage „Was darf passieren?“

Vielmehr muss aus der speziellen Sicht SKI auch die Frage gestellt und beantwortet werden:

Wogegen ist zu schützen? Dabei handelt es sich um die Frage der Gefährdungsannahmen. Einerseits stellt sich die Frage, ob Risiken, wie sie ein Betrieb üblicherweise ohnehin in sein Risikomanagement einbezieht, im Rahmen SKI nicht mehr beurteilt werden müssen. Anderseits stellt sich die Frage, wie weit das Gefährdungsspektrum aus Sicht SKI zu erweitern ist. Grundlage für diese Auswahl an relevanten Gefährdungen, die in eine Risikoanalyse für ein KI-Objekt einzubeziehen sind, stellt der vom BABS erarbeitete „Katalog möglicher Gefährdungen“[26] dar.

Das Resultat der Risikoanalyse, wie sie im Leitfaden beschrieben wird, liefert für ein KI-Objekt eine Gesamtübersicht über die Teilrisiken des kollektiven Risikos für jeden Prozess und alle dafür relevanten Gefährdungen (vgl. auch Kapitel 5.4).

Ab Level 3 erfolgt eine konsequente, Risiko basierte Analyse der Gefährdungen und Planung der Massnahmen

Auf Level 3 werden aber soweit vorhanden auch **Grenzwerte** für Risiken eingeführt. Dies betrifft insbesondere den Grenzwert für das individuelle Risiko. Das Schutzziel-Modell der PLANAT schlägt als Grenzwert für die Wahrscheinlichkeit, mit der ein Mensch in einem bestimmten Objekt oder an einem bestimmten Ort zu Tode kommt, 10^{-5}/Jahr vor. Es handelt sich um einen Erwartungswert über die Dauer eines Jahres. Detaillierte Ausführungen zum Grenzwert des individuellen Risikos sind in Anhang 2 enthalten. Dieser Erwartungswert gilt für den, wie ihn die PLANAT nennt, institutionellen Verantwortungsbereich. Die PLANAT unterscheidet weitere Verantwortungsbereiche (professionell, individuell) und bezeichnet damit den unterschiedlichen Grad an Freiwilligkeit bzw. Selbstverantwortung, mit dem ein Individuum ein Risiko eingeht. Diese Grenzwerte sind höher.

In Anlehnung an die PLANAT integrieren beispielsweise die Norm SIA 269 (2011) „Grundlagen der Erhaltung von Tragwerken“ und das Merkblatt SIA 2018 (2004) „Überprüfung bestehender Gebäude bezüglich Erdbeben“ einen expliziten Grenzwert für das Todesfallrisiko von 10-5 pro Jahr, explizite Grenzkosten

[26] BABS (2013): Katalog möglicher Gefährdungen – Grundlagen für Gefährdungsanalysen. Bundesamt für Bevölkerungsschutz, Bern, April 2013, 20p.

für ein gerettetes Menschenleben sowie Vorgehensweisen zur Beurteilung der Verhältnismässigkeit von Massnahmen.

Allfällige weitere, technisch basierte Grenzwerte (z.B. Angaben zu minimalen Verfügbarkeiten, Angaben zur Zuverlässigkeit von Systemen, Festlegung von maximalen Ausfallzeiten etc.) können, wie bereits in Kapitel 3.6 ausgeführt, vielfach keine Aussagen zu den damit verbundenen Risikowerten machen und sollten deshalb für die Massnahmenplanung eigentlich nicht eingesetzt werden.

Derartige Grenzwerte können aber im Sinne von Schadenszenarien dazu beitragen, dass die Entscheidungsträger sich ein besseres Bild über mögliche unerwünschte bzw. „nicht akzeptable" Zustände machen können, für die dann mit der Methode der Grenzkosten gemäss Level 4 entsprechende Massnahmen geplant und umgesetzt und die verbleibenden Risiken ermittelt werden können. Stellt sich dann bei der Massnahmenplanung heraus, dass die Grenzkosten überschritten sind, gilt es diese vermeintlichen „Grenzwerte" kritisch zu hinterfragen. Derartige technisch basierte Grenzwerte werden in der Regel dazu verwendet, den Funktionserhalt eines KI-Objektes sicherzustellen (vgl. auch Tab. 1). Sie können deshalb u.U. auch Hinweise liefern für die Festlegung möglicher Schadenindikatoren für eine Risikoanalyse.

4.6 Level 4 – Grenzkosten

Strategische Schutzzielebene

Level 4 definiert die strategische Schutzzielebene. Sie beinhaltet das Grundprinzip für die Festlegung von Schutzzielen. Dies betrifft primär das kollektive Risiko, bei dem es um die Reduktion der Schadenerwartung für die Gesellschaft unter optimalem Einsatz der verfügbaren Ressourcen geht. Dabei ist die Verhältnismässigkeit für die Entscheidung über Schutzmassnahmen das massgebende Kriterium für das kollektive Risiko. Das Mass dafür wird als Grenzkosten bezeichnet. Dieses Kriterium der Grenzkosten weist mit Verweis auf Kap. 3.6 diverse wichtige Merkmale auf:

Verhältnismässigkeit

1. Zunächst ist die *Verhältnismässigkeit* ein im Recht verankertes Prinzip, das weit über den Bereich von Schutz und Sicherheit hinausgeht. Da es in unserer Gesellschaft immer darum geht, beschränkte Mittel möglichst nutzbringend einzusetzen und optimal auf die verschiedenen Bedürfnisse zu verteilen, ergeben sich entsprechende Grenzen immer da, wo ein weiterer Aufwand als unverhältnismässig erachtet wird.

Optimaler Ressourceneinsatz

2. Diese Überlegung schliesst unmittelbar an eine ökonomische Betrachtungsweise an, welche generell auf einen *optimalen Ressourceneinsatz* ausgerichtet ist. Dabei wird durch ein Handeln nach Grenzkosten nicht nur ein unverhältnismässiger Mitteleinsatz verhindert. Vielmehr kann gezeigt werden, dass bei einem Mitteleinsatz mit gleichen Grenzkosten in einem System insgesamt am meisten Nutzen erzielt wird. Man kann also nicht Geld von einem Teil des Systems in den anderen verschieben und so einen grösseren Gesamtnutzen erzielen[27].

Grenzkosten sind von der Systemgrösse unabhängig

3. Damit ergibt sich zusätzlich der Vorteil, dass sogar jede Einzelkomponente eines Systems isoliert nach einem einheitlichen Kriterium optimiert werden kann. Somit kann das Kriterium auf jede Einzelmassnahme, auf jedes Teilsystem, und sogar auf übergeordnete Systeme angewendet werden, unab-

[27] Entsprechend dem Pareto-Optimum

hängig von einem grösseren Zusammenhang. Das Grenzkostenkriterium ist also *unabhängig von der Grösse und Art des betrachteten Systems.*

4. Bei der konkreten Festlegung von Grenzkosten wird insbesondere von der Idee der *Zahlungsbereitschaft* ausgegangen. Damit ist eine Verankerung in einem zumindest impliziten, *gesellschaftlich-politischen Meinungsbildungsprozess* gegeben.

Grenzkosten als Ausdruck der Zahlungsbereitschaft der Gesellschaft

5. Da schliesslich die Grenzkosten diejenigen Anstrengungen repräsentieren, welche zur Steigerung der Sicherheit vorzunehmen sind, stellt die Forderung nach gleichen Grenzkosten auch die *Forderung gleicher Anstrengungen* für alle Beteiligten dar. Es ergänzt damit bezüglich Gleichbehandlung den Grenzwert des individuellen Risikos.

Der Grenzkostenansatz vermag somit die wichtigen Anforderungen der SKI-Strategie (die untereinander konsistenten Schutzziele, die risikobasierte Kosten-Wirksamkeit und die gesellschaftlich-rechtliche Verankerung) zu kombinieren und abzudecken.

Entscheidender Vorteil des Grenzkostenansatzes ist, dass er gleichermassen auf KI-Objekte, auf Teilsektoren und auf Sektoren angewendet werden kann.

Der Grenzkostenansatz vermag insbesondere (und dies ist wohl sein grösster und entscheidender Vorteil) die drei Ebenen KI-Objekte, Teilsektoren und Sektoren gleichermassen konsistent abzudecken. Damit wird eine einheitliche, durchgängige Sicherheitsphilosophie über alle drei Ebenen möglich.

4.7 Fazit

Level 1 und 2 ermöglichen noch keine Aussage zum Restrisiko

Die hier eingeführte Schutzziel-Pyramide mit den 4 Levels ist als Hintergrund für das Schutzzielkonzept SKI zu verstehen. Der Begriff des Schutzzieles soll also in einer breiten Interpretation verstanden werden, auch wenn sich die Studie letztlich konkret auf Level 3 und insbesondere Level 4 bezieht. Der Schutzzielbegriff deckt aber mit den in Abb. 5 dargestellten und in Tab. 2 näher beschriebenen Level 1 und Level 2 auch im Bereich SKI implizit bereits ein hohes Mass an Sicherheitsbedürfnissen ab. Der Grundsatz der Verhältnismässigkeit und der Zahlungsbereitschaft bleibt als oberstes Prinzip in jedem Falle erhalten. Er gilt grundsätzlich auch für Massnahmen, die zur Erfüllung der Levels 1 und 2 an bestehenden KI-Objekten zusätzlich zu ergreifen sind, damit die Schutzbemühungen im Rahmen von SKI erreicht werden können.

Während aus „Schutzzielen“ auf Level 1 und Level 2 keine expliziten Aussagen zu den verbleibenden Risiken gemacht werden können, liefern Level 3 und Level 4 explizite Aussagen dazu. Es können sich daraus Situationen einstellen, bei denen gesellschaftlich sogar weitergehende Schutzmassnahmen gefordert sein können. In diesen Situationen müssen sich die Entscheidungsträger bewusst sein, dass damit das optimale Schutzziel überschritten wird, und sie mehr Geld für Massnahmen ausgeben, als sie Schäden zu erwarten haben.

Grenzwerte und Grenzkosten ergänzen sich

Die obigen Ausführungen zeigen, dass Grenzkosten und Grenzwerte nicht als Alternativen zu verstehen sind, sondern sich gegenseitig ergänzen. Grenzkostenüberlegungen, das heisst Überlegungen zur Verhältnismässigkeit und zur Wirksamkeit der insgesamt gewählten Massnahmen müssen in jedem Fall gemacht werden. Letztlich geht es in einem KI-Sektor/Betrieb um eine Gesamtbeurteilung, wie viel Gesamtaufwand für den integralen Schutz insgesamt als tragbar erachtet wird und wie weit damit das Gesamtrisiko reduziert werden kann.

Risikogrenzwerte entsprechen zwar spontan eher den Erwartungen an ein Schutzziel, die Hauptnachteile sind aber, dass sie beim kollektiven Risiko keine

Bezugsgrösse haben (und damit gleiche Anforderungen an kleine und grosse Systeme stellen). Der zweite grosse Nachteil ist, wie oben erwähnt, dass solche Grenzwerte theoretisch keine Rücksicht auf die finanzielle Verhältnismässigkeit und damit Umsetzbarkeit nehmen (gerade im Bereich SKI liegen noch wenige Erfahrungen bezüglich des Aufwandes für Schutzmassnahmen vor).

In den bestehenden, klassischen Regelwerken werden bis heute nur in wenigen Fällen bereits quantitative und risikobasierte Sicherheitsbeurteilungen gefordert. Dies bedeutet, dass die meisten Branchen nicht oder erst ansatzweise mit diesen risikobasierten Methoden vertraut sind. Sie werden mit für sie neuartigen Methoden konfrontiert, wenn aufgrund übergeordneter (nationaler) Bedürfnisse deren Anwendung vermehrt gefordert wird.

Schulung und organisierter Erfahrungsaustausch wichtig

Mit entsprechender Schulung und dem zur Verfügung stellen entsprechender Hilfsmittel (evtl. EDV-gestützt) kann das erforderliche Fachwissen aber aufgebaut werden. Enorm wichtig wird auch hier ein regelmässiger Erfahrungsaustausch zwischen den verschiedenen KI-Betreibern und Branchen sein im Umgang mit risikobasierten Entscheiden für Schutzmassnahmen. Ebenso wichtig ist die Begleitung des Vorhabens durch die verantwortlichen Behörden auf kantonaler Ebene und auf Bundesebene im Sinne der Begutachtung der Zweckmässigkeit der gestellten Anforderungen und der bereitgestellten Grundlagen.

5. Festlegung von Schutzzielen im Rahmen der SKI-Strategie

„Der Mensch ist ständig in Gefahr, das nie dagewesene für undenkbar zu halten."

*Albert „Al" Gore (*1948), US Vizepräsident 1993-2001*

5.1 Einleitung

Auf der Basis der Schutzziel- Pyramide in Abb. 5 und Tab. 2 gilt es für einen KI-Betreiber sowohl die „klassischen" betrieblichen Risiken, als auch die SKI-relevanten Risiken abzudecken. Wie bereits kurz erwähnt geht es zum einen um Sicherheitsmassnahmen, die den reibungslosen und effizienten Betrieb eines KI-Objektes gewährleisten sollen (inkl. Verhinderung allfälliger Imageschäden), aber auch um die Einhaltung der gültigen gesetzlichen Bestimmungen Dazu kommen nun im Sinne SKI Sicherheitsmassnahmen, die sich aus Anforderungen der Öffentlichkeit bzw. zum Schutz der Gesellschaft ergeben, also um die Verhinderung von Schäden für Dritte. Dies entspricht einigermassen dem in Kap. 3.6 aufgezeigten Unterschied zwischen „Sicherheit" und „Funktionserhaltung" (vgl. Tab. 1).

Sicherheit für den Betrieb und für die Allgemeinheit

Im Zentrum steht dabei die Frage, welche Sicherheitsaufwendungen heute normalerweise Sache des Betriebes sind bzw. zur erwarteten Sorgfaltspflicht gehören und demnach auch durch ihn zu finanzieren sind, bzw. was im Sinne der SKI-relevanten Schutzmassnahmen darüber hinausgeht. Wenn für den KI-Betreiber weitergehende Kosten anfallen, die er der Allgemeinheit nicht weiterverrechnen kann und damit ihm aufgebürdet bleiben, dann belastet dies seine Wirtschaftlichkeit (ohne direkten Nutzen für den Betreiber) und damit indirekt auch seine Konkurrenzfähigkeit. Diese Volks- und Betriebswirtschaftlichen Zusammenhänge gilt es bei der Umsetzung von Schutzmassnahmen im Auge zu behalten. Mangelnde „Verrechenbarkeit" und damit Finanzierbarkeit von Schutzmassnahmen kann dazu führen, dass nicht alle möglichen Risikosituationen abgedeckt werden können (vgl. Kap. 4.5 – „Wogegen wollen/ können wir uns schützen?").

5.2 Die Schutzziele im Verbund von Risikoanalyse, Risikobewertung und Massnahmenplanung

Enge Interaktion der Schutzziele mit der Risikoanalyse, der Risikobewertung und der Massnahmenplanung.

Es ist zu berücksichtigen, dass eine strenge Trennung der Risikobewertung, und damit der Frage der Schutzziele, von der Risikoanalyse und der Massnahmenplanung nicht möglich ist. So werden z.B. mit der Festlegung der zu verwendenden Indikatoren zur Quantifizierung der Risiken, aber auch mit der allfälligen Berücksichtigung einer Risikoaversion aus methodischen Gründen bereits in der Risikoanalyse Wertungen eingeführt. Diese Wertungen fliessen auch bei der Beurteilung der Massnahmen und deren Wirksamkeit bezüglich ihrer Risikoreduktion ebenfalls schon ein, bevor es zur eigentlichen Bewertung durch das Grenzkostenkriterium kommt. Abbildung 6 verdeutlicht, dass die Schutzziele in einer engen Wechselwirkung mit der Risikoanalyse, der Risikobewertung und der Massnahmenplanung stehen. Die Schutzzielfrage beginnt mit der Festlegung der Schadenindikatoren. Wenn die möglichen Schadenwirkungen nicht

adäquat erfasst werden, zielt die Schutzzieldiskussion bereits teilweise am Ziel vorbei. Dasselbe gilt sogar bereits für vorzeitige, nicht genügend fundierte Beschränkungen bei der Berücksichtigung von Gefährdungen, durch welche letztlich die Schutzziele beeinflusst werden.

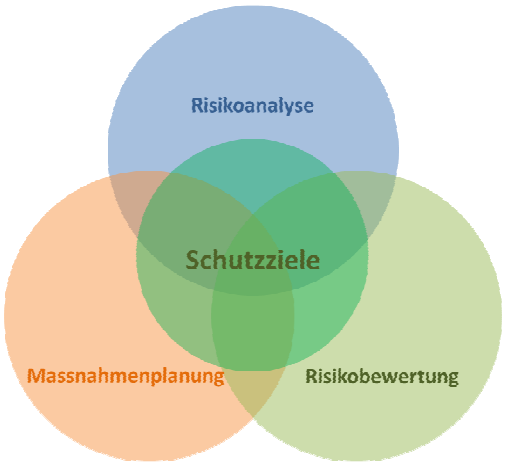


Abbildung 6: Schutzziele können nicht losgelöst von Risiko-Analyse, Risiko-Bewertung und Massnahmenplanung betrachtet werden. Alle Bereiche bilden eine integrale Einheit. (eigene Darstellung)

5.3 Kontrolle des Standes der Technik bzw. der Legal Compliance (Level 1 und 2)

Sicherheitsanalyse

Die konkreten Massnahmen und die einzuhaltenden Mindestanforderungen im Sinne der Levels 1 und Levels 2 bilden einen wichtigen Teil der Schutzplanung im Bereich SKI. Bei der Analyse der massgeblichen Prozesse werden unweigerlich für die Sicherheit relevante Mängel auf diesen Ebenen erkannt werden. Im Leitfaden wird bereits darauf hingewiesen, dass das Erkennen solcher Lücken bzw. Mängel Teil der Analyse der kritischen Prozesse ist, woraus bereits eine erste Liste von Massnahmen resultiert, die in der Folge in die Gesamt-Beurteilung risikoreduzierender Massnahmen einzubeziehen sind. Eine umfassende Überprüfung der Regelungen auf Level 1 und Level 2 kann hingegen nicht Gegenstand der SKI sein. Es muss davon ausgegangen werden, dass hier eigenständige Kontrollen bei der Erstellung und dem Betrieb der Anlagen durch die bestehenden Aufsichts- und Kontrollorgane greifen und die Sicherheit weitgehend gewährleistet ist; dies insbesondere für die Ebene KI-Objekt.

Teil dieser Analyse und der damit verbundenen Massnahmenplanung wird generell eine Auflistung aller relevanten Bestimmungen, Regelwerke bis hin zu Gesetzen und die Kontrolle ihrer Einhaltung sein[28]. Dies ist quasi eine Sicherheitsanalyse im herkömmlichen, klassischen Sinne (Kontrolle der Einhaltung des Standes der Technik) bzw. auch im Sinne des Nachweises der sog. Legal Compliance und ist eine ausgesprochen branchenbezogene bzw. sogar objektbezogene Aufgabe.

[28] Beispiele für derartige gesetzliche Bestimmungen, Normen und Richtlinien sind z.B.: Empfehlung der Kantone bezüglich Erdbebenschutz; technische Normen des IHS für Spitäler; Eisenbahngesetz Art. 8e Erteilung und Erneuerung der Sicherheitsbescheinigung; Stromversorgungsgesetz 2. Abschnitt: Sicherstellung der Versorgung, etc.

Diese Kontrolle inkl. die Anordnung und Umsetzung der daraus folgenden Korrekturen und ergänzenden Schutzmassnahmen sind für die Einhaltung der Schutzziele gemäss Level 1 und Level 2 der Schutzziel-Pyramide massgebend.

5.4 Grobbeurteilung der Risiken und Priorisierung des Handlungsbedarfs (Level 3)

Risikobeurteilung

Das Resultat der Risikoanalyse, wie sie im Leitfaden in Kap. 3.2 beschrieben wird, liefert für ein KI-Objekt eine Gesamtübersicht über die Teilrisiken des kollektiven Risikos für jeden Prozess und alle dafür relevanten Gefährdungen. Für die Wahrscheinlichkeit des Eintretens der verschiedenen Gefährdungen hatte der SKI-Leitfaden ursprünglich vorgeschlagen, die in „Katastrophen und Notlagen Schweiz“[29][30] aufgeführten Intensitäten: „erheblich“, „gross“, „extrem“ zu verwenden, d.h. dass für jedes KI-Objekt pro Gefährdungsart drei unterschiedliche Ereignisintensitäten beurteilt werden müssen. Es fragt sich allerdings, ob nicht auch eine nur zweistufige Gliederung verwendet werden könnte und dabei mit der einen Stufe das „Betriebsrisiko“ und mit der anderen Stufe das „SKI-Risiko“ eingeschätzt wird.[31]

Je nach KI-Objekt ergibt sich in der Folge aus einer Risikoanalyse gemäss Leitfaden eine sehr grosse Zahl von Risikopunkten, charakterisiert durch die Wahrscheinlichkeit des Eintretens und das potentielle Schadenausmass. Wenn z.B. in einem Spital 10 Prozesse zu unterscheiden sind und dabei 5 Gefährdungsszenarien mit jeweils drei Intensitäten zu berücksichtigen sind, so ergeben sich bereits 150 Punkte.

Maximal-Matrix

Um sich über diese Risikopunkte zunächst eine Übersicht zu verschaffen, werden sie in der Folge in der w-A-Risikomatrix dargestellt. Bis zu welchen Maximalwerten die Unterteilung auf den beiden Achsen w und A der Matrix gespannt werden soll, hängt vom KI-Objekt bzw. der KI-Ebene ab; als Basis dient die „Maximal-Matrix“ gemäss Leitfaden mit je 8 Gefährdungs- und Ausmassklassen. Die Vorstellungen über die quantitativen Werte der w- und A-Klassen sollen dabei den Klassen gemäss Leitfaden entsprechen, u.U. aber nicht die ganze Spanne von 8 Klassen ausschöpfen. Dabei sollen für die Ebene KI-Objekt, zumindest innerhalb der Teilsektoren bzw. Branchen, soweit möglich und sinnvoll die gleichen Abstufungen vorgenommen werden.

Für die Ebene KI-Objekt wird im Folgenden eine 6 x 6 – Matrix vorgeschlagen (Abb. 7). Für die drei Intensitäten der Gefährdung gemäss ursprünglichem Vorschlag im Leitfaden würden damit grundsätzlich je zwei Wahrscheinlichkeitsbereiche pro Niveau der Gefährdungsintensität zur Verfügung stehen.

Es ist erfahrungsgemäss für die Risiko- und Sicherheitsbeurteilung eines KI-Objektes sinnvoll, sich in einem ersten Schritt der Risikoanalyse Klarheit zu verschaffen über die maximal mögliche Bandbreite bei Ausmass und Wahr-

---

[29] BABS (2012). *Methode zur Risikoanalyse in „Risiken Schweiz“,* Technischer Bericht Version 1.01, 35p.

[30] BABS (2013). *Katastrophen und Notlagen Schweiz – Risikobericht 2012*, Bundesamt für Bevölkerungsschutz, Febr. 2013.

[31] Für die im Leitfaden ebenfalls aufgeführten, „mutwillig herbeigeführten Ereignisse“ an einem KI-Objekt (BABS, 2012) könnten die dort gelisteten 8 Plausibilitätsklassen allenfalls auch auf zwei Szenarien-Intensitäten zusammengeführt werden - vgl. p1 – p6 in Abb. 7.

scheinlichkeit möglicher Schadenereignisse bzw. Risikobeiträge und die qualitativen Einschätzungen von Ereignissen, insb. Extremereignissen, grob an den quantitativen Grössenordnungen der Klassen zu „eichen“. Eine grobe quantitative Beurteilung der Risiken kann sich in der Folge an den Mittelwerten der im Leitfaden vorgegebenen Wahrscheinlichkeits- und Ausmassklassen orientieren.

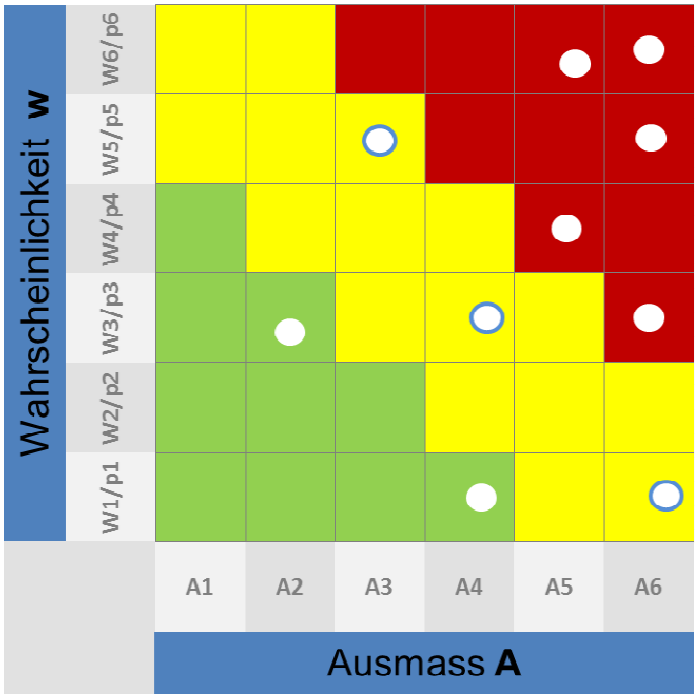


Abbildung 7: 6 x 6 Matrix mit eingetragenen drei (Schutzziel)-Bereichen zur Priorisierung des Handlungsbedarfs und mit fiktiven, exemplarischen Punkten (eigene Darstellung)

Die konsequente Einhaltung der Abstufungen der w- und A-Klassen über möglichst alle KI-Objekte ermöglicht eine über die Objekte vergleichbare Einschätzung. Diese Grobbeurteilung für ein Objekt hat Ähnlichkeiten mit der „Prozessgeleiteten Beurteilung“ der PLANAT (PLANAT 2008), resp. der im Rahmen der Risikoanalyse Schweiz erfolgten Delphi-Befragung von Experten (BABS Workshop 2012).

Grobkategorisierung

Alle ermittelten Risikopunkte bzw. -beiträge in der w-A-Matrix in eine Massnahmenplanung überzuführen bedeutet einen sehr grossen Aufwand. Die Matrixdarstellung soll daher eine erste Priorisierung des Handlungsbedarfs bezüglich der in den einzelnen Matrixfeldern aufgeführten Risiken (vgl. Abb. 7) ermöglichen. Eine grobe Kategorisierung der Risiken nach ihrer Grösse erfolgt sinnvollerweise durch 3 Zonen (vgl. in Abb. 7 die Zonen rot – gelb - grün), welche mehr oder weniger diagonal durch die Matrix von oben links nach unten rechts verlaufen. Dies bedeutet sinngemäss, dass Matrixpunkte in Diagonalrichtung entsprechen dem Produkt w x A ein ähnlich hohes Risiko repräsentieren.

Qualitative Grenzwerte

Die Abgrenzungen der drei verwendeten Farbbereiche rot – gelb – grün können zwar als qualitative „Grenzwerte“ interpretiert werden, von Bedeutung sind sie aber primär nur für eine Priorisierung der Risiken in Bezug auf den Handlungsbedarf. Diese Farbzuteilungen und die damit einhergehenden Priorisierungen der Risiken können als grob abgestufte provisorische „Schutzziele“ festgelegt werden (vgl. dazu auch (PLANAT 2008)). Eine solche Priorisierung ist stets bezogen auf das einzelne KI-Objekt zu sehen.

Folgende Bedeutung kann den Farben zugeordnet werden:

- **Rot** = hohes Risiko
- **Gelb** = mittleres Risiko
- **Grün** = geringeres Risiko

Diese Priorisierung von Risiken in den Matrixfeldern unterschiedlicher Farbstufen heisst nicht, dass neben Risiken im roten Bereich nicht gleichzeitig doch auch Massnahmen für Risiken im gelben Bereich oder gar im grünen Bereich zu prüfen sind, insbesondere wenn sie z.B. den gleichen Prozess betreffen. Letztlich entscheiden erst die in der Massnahmenplanung angewendeten Grenzkosten-Kriterien über die zu treffenden Massnahmen. Risiken im grünen Bereich können dabei tendenziell mit Massnahmen auf Level 1 und 2 der Schutzziel-Pyramide reduziert werden.

Massnahmen können auch im grünen Bereich Sinn machen – insbesondere, wenn sie Level 1 und 2 betreffen.

Die Anforderungen aus Level 1 und Level 2 (Abb. 5 und Tabelle 2) behalten Gültigkeit über sämtliche Matrixfelder, unabhängig von der Farbzugehörigkeit. Zudem ist davon auszugehen, dass nicht sämtliche Risiken voneinander unabhängig sind, so dass es gilt, die möglichen Abhängigkeiten ebenfalls mit geeigneten Massnahmen zu unterbrechen, damit nicht ein Risiko im roten Bereich ausgelöst wird (vgl. den Fall Fukushima). Auch in diesem Sinne darf die vorgeschlagene w-A-Matrix mit den drei ausgewiesenen Risikobereichen nicht als eine Festlegung von eigentlichen Risikogrenzwerten bzw. Schutzzielen betrachtet werden.

Der Massnahmenplanung vorgreifend sei bereits angedeutet, dass die Risikopunkte nach abgeschlossener Massnahmenplanung in der Risikomatrix neu positioniert werden können. Dies lässt erkennen, wie weit die „Wolke“ der Risiken sich z.B. aus dem roten Bereich über gelb nach grün verschoben hat. Dies kann auch Grundlage sein für eine allfällige, breitere gesellschaftlich-politische Diskussion der verbleibenden Risiken.

Risikoquantifizierung

Nach erfolgter Priorisierung anhand der Risikomatrix ist die Quantifizierung der ausgewählten Risiken im Rahmen der Massnahmenplanung detailliert zu überprüfen. Die Wahrscheinlichkeiten müssen prozessbezogen ermittelt werden. Abb. 8 zeigt dabei eine weitere mögliche Form der Aggregation der Risikobeiträge über die verschiedenen Prozesse und Gefährdungen. Dargestellt in Abb. 8 sind die Risikobeiträge der einzelnen Prozesse über alle Gefährdungen, bzw. die Risikobeiträge der einzelnen Gefährdungen über alle Prozesse.

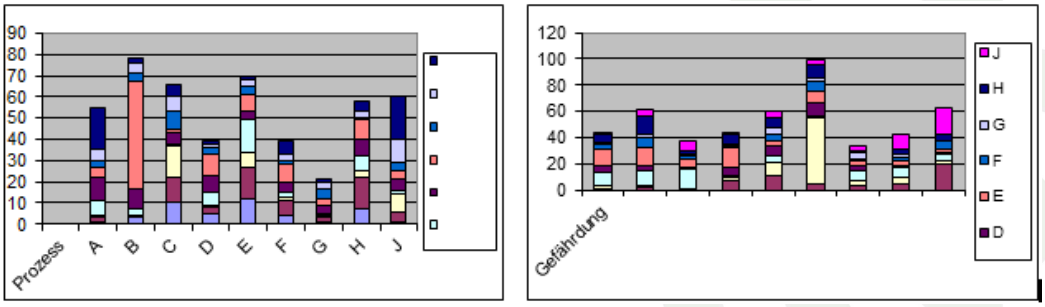


Abbildung 8: Übersicht und Struktur der Risiken für ein fiktives Beispiel mit 9 Prozessen und 3 Gefährdungsarten. Links: Risiken der Prozesse über alle Gefährdungen; Rechts: Risiken der Gefährdungen über alle Prozesse (eigene Darstellung)

Unabhängig von der Beurteilung der kollektiven Risiken mittels w-A-Matrix muss stets die Einhaltung der Grenzwerte für das individuelle Risiko gewährleistet bleiben. In der Regel dürfte das individuelle Risiko aber kaum der be-

stimmende Faktor für nötige Schutzmassnahmen sein. (vgl. Abb. 3). Für die Schutzziele bezüglich des individuellen Risikos besteht bereits ein gewisser Konsens.

5.5 Grenzkosten (Level 4)

Praktische Anwendung des Grenzkostenkriteriums – Monetarisierung

Monetarisierung als Basis zur Quantifizierung der Risiken

Der Grenzkostenansatz basiert auf quantifizierten Grössen für w und A. Wie erwähnt, wird für die erforderliche Quantifizierung eine vollständige Monetarisierung aller Indikatoren vorgeschlagen. Dies erfordert die Festlegung eines Geldwertes für alle Schadenindikatoren. Wie viele Franken ist man bereit auszugeben, um eine Risikoeinheit zu verhindern? Das ist die Frage, welche nachstehend näher erläutert wird.

Dies gilt insbesondere auch für Todesopfer, was bekanntlich oft als problematisch angesehen wird. Es wird hier allerdings nicht vom Verständnis eines „value of human life“ ausgegangen, sondern von der sog. „willingsness-to-pay to save a human life“ (= Grenzkosten für die Rettung eines Menschenlebens). Der Vorteil ist dabei, dass man sich bei diesem Wert heute zunehmend auf mehr oder weniger akzeptierte Werte aus verschiedensten Bereichen (z.B. technische Sicherheit, Unfallverhütung bis hin zu Gesundheitswesen, Umgang mit Naturgefahren) abstützen kann in der Meinung, dass letztlich die Bewertung eines Menschenlebens und seines Rettungsaufwandes nicht vom jeweiligen Kontext abhängig sein sollte. Es geht hier aber auch um die einfachere Frage, wie viel die Gesellschaft bereit ist, für die Verhinderung von materiellen Schäden auszugeben.

Schaden-dimensionen

Bei Schutz- und Sicherheitsproblemen geht es in der Regel um verschiedene Schadendimensionen, die nicht a priori vergleichbar sind. Wie können Verluste an Menschenleben und wirtschaftliche und ökologische Schäden miteinander verglichen werden? Es gibt zwei Vorgehensweisen, damit umzugehen:

1. Man behandelt jede Schadendimension für sich, indem entsprechende Grenzkosten, basierend auf der jeweiligen Zahlungsbereitschaft dafür definiert werden. Dieses Vorgehen hat den offensichtlichen und praktischen Nachteil, dass es schwierig ist mit Massnahmen umzugehen, welche für verschiedene Schadendimensionen wirken. Darüber hinaus ist es so nicht möglich, Risiken, die verschiedene Schadendimensionen umfassen, gesamthaft zu beurteilen.
2. Man verwendet ein Verfahren, bei welchen die verschiedenen Schadendimensionen zunächst alle auf eine gleiche Einheit transformiert werden, vorzugsweise die Geldeinheit (Monetarisierung) und nicht mit abstrakten Punktesystemen bewertet.

Monetarisierungs-prozess

Der **Monetarisierungsprozess** spielt sich dabei in der Regel wie folgt ab:

1. Ausgangspunkt ist ein Leitindikator, für den die besten Grundlagen inkl. Konsens für eine Monetarisierung mittels Zahlungsbereitschaft bestehen. Dies sind in der Regel die Todesopfer, für welche heute umfassende Grundlagen für eine Monetarisierung vorliegen.
2. An diesem Leitindikator werden die anderen Indikatoren geeicht. Dies kann z.B. so erfolgen, dass für den Leitindikator und die anderen Indikatoren eine gleiche Anzahl von Ausmassklassen definiert wird (z.B. die Ausmassklassen 1-8 wie im Leitfaden SKI des BABS vorgeschlagen). Der Geldwert des Leitindikators z.B. für Klasse 8 wird mittels der bekannten Grenzkosten

bestimmt und dient damit als Eichwert für die Klasse 8 der anderen Indikatoren. Wenn also Umweltschäden an der betroffenen Fläche gemessen werden, wird der Geldwert für Todesopfer der Klasse 8 durch den Flächenwert der Klasse 8 dividiert, woraus sich die Grenzkosten pro Schadeneinheit an Umweltschäden ergeben.

Die Quantifizierung der Wirksamkeit von Massnahmen kann schwierig sein

Auch die Kosten der Massnahmen bzw. deren Wirksamkeit sind stets im obigen Sinne zu quantifizieren. Das heisst, dass auch die Wirksamkeit der Massnahmen aufgrund der Veränderung dieser Grössen zu beurteilen sind, d.h. also auch alle organisatorischen Massnahmen inkl. Verkürzungen der Ausfallzeit einer Funktion. Dies kann bei gewissen Massnahmen schwierig sein (z.B. wenn eine Massnahme einfach nur eine bessere Regelung von Kompetenzen vorsieht, wird es schwierig sein, die Wirkung zu quantifizieren).

Schadenindikatoren

Der Leitfaden weist zahlreiche Schadenindikatoren aus für eine umfassende Ermittlung des Schadenausmasses („...geschätzte Auswirkung auf die Bevölkerung und deren Lebensgrundlagen...“, vgl. Leitfaden SKI). Diese Schadenindikatoren erlauben die Schadenermittlung mit realen Grössen (Todesopfer, Flächen, Franken etc.) und nicht nur mit Punktesystemen und qualitativen Bewertungen (z.B. gross – mittel – klein). Der Leitfaden unterscheidet und quantifiziert in jeweils 8 Auswirkungsklassen insgesamt 13 Schadenindikatoren für die Schadensbereiche Personen, Umwelt, Wirtschaft, und Gesellschaft. Beispiele aus diesem Katalog sind:

- Sicherheit von Personen (Anzahl Todesopfer)
- Verletzte/ Kranke (Anzahl Personen mit Gewichtungsfaktoren)
- Ökosystem (beeinträchtigte Fläche x Anzahl Jahre der Beeinträchtigung)
- Vermögen (Schäden an Anlagegütern und am finanziellen Vermögen, Kosten für Bewältigung des Schadens)
- Wirtschaftliche Leistungsfähigkeit (indirekte wirtschaftl. Auswirkung und Reduktion der nachfolgenden Wertschöpfung)
- Versorgung mit lebensnotwendigen Gütern und Dienstleistungen (Anzahl eingeschränkter Personen x Dauer der Einschränkung)

Der Monetarisierungsprozess angewendet auf die Unterlagen des BABS führt zu den in Tab. 3 aufgeführten Grenzkosten:

Tabelle 3: Grenzkosten für verschiedene Schadenindikatoren (die 4 Mio pro Toter werden im SKI-Leitfaden vorgeschlagen)

Schadenindikator	**Zahlungsbereitschaft Level 4**
Totesopfer	4 Mio CHF (Eichwert – kann von Regulationsbehörde angepasst werden)
Verletzte/Kranke	400'000 CHF / Schwerverletzen
Umweltschäden	260'000 CHF / km^2 u. Jahr
Vermögen	1 CHF / CHF
Wirtschaftliche Leistungsfähigkeit	1 CHF / CHF
Versorgung	100 CHF / Personentag

Dieser Schritt ist eindeutig mit einer Wertung verbunden und ist deshalb an sich Teil der Risikobewertung. Wie bereits verschiedentlich angedeutet, können aber Risikoanalyse und Risikobewertung hier nicht eindeutig getrennt werden (vgl. Abb. 6). So bedingt gerade das Vorgehen mittels Monetarisierung, dass die entsprechenden Indikatoren und Werte bereits in der Risikoanalyse verwendet werden.

Freiwilligkeitsgrad

Analog wie bei den individuellen Todesfallrisiken, wo unterschiedliche „Freiwilligkeitsgrade“ unterschieden werden könnten, liessen sich auch bei den Grenzkosten unterschiedliche Ansätze rechtfertigen. Dies wirkt sich aber nur auf den monetarisierten Risiko-Betrag aus. Bei einem allfälligen Vergleich mit Werten aus der Literatur ist dabei darauf zu achten, dass die Beträge und der Grad der Freiwilligkeit miteinander verglichen werden. Gemäss SKI Leitfaden (vgl. auch Tabelle 3) wird pro verhindertem Todesfall 4 Mio CHF eingesetzt. Damit befindet man sich bei verschiedenen Literaturangaben im Bereich der „freiwilligen“ Risiken. SKI-relevante Risiken sind aber der Stufe „unfreiwillig“ zuzuordnen. Eine Überprüfung dieses wichtigen Basiswertes scheint angezeigt.

Kritikalität als weiteres Element der Risikobewertung?

Kritikalität muss sich über das Schadenausmass zeigen – kein eigener Faktor angezeigt

Die unterschiedliche *Kritikalität* der verschiedenen KI-Objekte wird in verschiedenen Dokumenten, so insbesondere auch in der nationalen Strategie durch drei Niveaus (rot, orange, gelb) angedeutet. Es stellt sich also die Frage, ob die Kritikalitätsstufe zusätzlich gewichtet werden soll, bzw. in die Risikoanalyse und -bewertung einzubeziehen ist.

Grundsätzlich ist davon auszugehen, dass die Schadenwirkung selber die Bedeutung einer KI widerspiegelt und das potentielle Schadenausmass entsprechend grösser ausfällt, je wichtiger ein KI-Objekt ist. Zeigt sich dies in der Risikoanalyse nicht, so ist zu prüfen, ob wesentliche Aspekte mit den gewählten Indikatoren nicht erfasst werden, die Schadenbeurteilung also unvollständig ist. Auf eine zusätzliche Gewichtung mittels willkürlich gewählter Faktoren sollte u.E. aus Transparenzgründen verzichtet werden.

6. Zusammenfassung und Schlussbemerkungen

"Disaster reduction is everybody's business. We all have a moral, social and economic obligation to act now in building resilient communities and nations"

Ban Ki-moon

Das Bundesamt für Bevölkerungsschutz BABS hat im Rahmen der Vorbereitungen zur Umsetzung der Strategie des Bundesrates zum Schutz kritischer Infrastrukturen das Global Risk Forum GRF Davos mit einem Forschungsauftrag beauftragt, die methodischen Fragen zur Festlegung von Schutzzielen für kritische Infrastrukturen zu klären und dazu konkrete Vorschläge zu machen. KI-Betreiber sind verstärkt dazu angehalten und verpflichtet, neben den eher betrieblichen Risiken auch Verantwortung zu übernehmen für Risiken, Notlagen und Katastrophen von überregionaler und gar nationaler Bedeutung; also Risiken, die Leistungen des KI-Betreibers bedrohen, die für die Allgemeinheit in Krisen- und Notlagen entscheidend sind.

Bericht enthält kritische Würdigung bestehender Ansätze.

Der Bericht umfasst eine kritische Würdigung bestehender Ansätze zum Umgang mit Risiken im Allgemeinen und zu den Schutzzielen im Besonderen. Während bekannter Weise bei den individuellen Risiken mit der Angabe des individuellen Todesfallrisikos ein klarer Grenzwert festgelegt werden kann, ist der Stand der Erkenntnisse bei den kollektiven Risiken bedeutend weniger fortgeschritten und in der Vergangenheit kontroverser diskutiert. Dabei wird aber deutlich, dass die Kosten-Wirksamkeit der Schutzmassnahmen und die Verhältnismässigkeit der eingesetzten Mittel und Ressourcen in den verschieden Risikobereichen und den damit verbundenen behördlichen Fachbereichen immer stärker ins Zentrum rücken und als Entscheidungsgrundlage für Schutzmassnahmen Akzeptanz finden. Grenzkosten und Grenzwerte sind in diesem Sinne nicht als Alternativen zu verstehen, sondern sie ergänzen sich gegenseitig.

Grenzwerte und Grenzkosten ergänzen sich

Verhältnismässigkeit und Zahlungsbereitschaft der Allgemeinheit als Basis für die Festlegung von Schutzzielen

Die aufgezeigte Methode zur Festlegung einheitlicher Schutzziele für kollektive Risiken basiert auf dem monetarisierten Grenzkosten-Ansatz; d.h. dass festgelegt wird, wie viel für Schutz maximal auszugeben ist, um ein Risiko um eine Einheit zu reduzieren. Um die dafür notwenige Vergleichbarkeit der Risiken zu erreichen, wird der Ansatz der Zahlungsbereitschaft herangezogen, d.h. ein als akzeptiert betrachteter, über alle Risiken einheitlich geltender Betrag z.B. zur Rettung eines Menschenlebens oder anderer Schadenarten (Umweltschäden, Funktionseinbusse, etc.) festgelegt. Mit der Festlegung der Zahlungsbereitschaft der Allgemeinheit als Basis für die Schutzziele wird die Einbettung in einen gesellschaftlich-politischen Kontext gewährleistet. Diese Zahlungsbereitschaft der Gesellschaft kann sich über die Zeit verändern, insbesondere bei rückläufigem Wirtschaftswachstum oder Wohlstand, aber auch bei Gefährdungsarten, die ein ausserordentlich hohes Risiko beinhalten und die ganze Schweiz erfassen (z.B. Pandemiefall). Es gilt deshalb, diese Zahlungsbereitschaft ebenfalls periodisch zu hinterfragen.

Grenzwerte nur für das individuelle Risiko möglich

Das individuelle Risiko wird mit einer einheitlichen, jährlichen Todesfallwahrscheinlichkeit abgedeckt. Es dürfte im vorliegenden Fall nur ausnahmsweise relevant werden, weil Risiken und Katastrophen nationalen Ausmasses naturgemäss sehr selten sind.

Schutzziel- Pyramide: Level 1 und 2 können auch für SKI bereits einen massgeblichen Schutz bieten.

Aus der Sicht SKI sind Risiken dann relevant, wenn sie Gesellschaft und Wirtschaft der Schweiz existentiell treffen können. Das heisst aber nicht, dass die KI-Objekte nicht auch betriebliche Risiken abdecken müssen. Die hier eingeführte, sog. Schutzziel-Pyramide (Abb. 5) ist mit den 4 Levels als Hintergrund für das Schutzzielkonzept SKI zu verstehen. Die Pyramide beinhaltet von Level 1 bis Level 4 einen aufsteigenden Grad expliziter Risiko-Wirksamkeits-Betrachtungen bei der Schutzzieldefinition. Level 1 und Level 2 decken dabei die klassischen Schutzziele in Form von normierten und standardisierten Massnahmen und Mindestanforderungen ab. Sie sind zwar primär zur Abdeckung betrieblicher Risiken vorgesehen, decken aber implizit auch im Bereich SKI bereits ein beachtliches Mass an Sicherheitsbedürfnissen ab. Der Grundsatz der Verhältnismässigkeit und der Zahlungsbereitschaft bleibt als oberstes Prinzip gemäss Level 4 auch bei diesen beiden Levels in jedem Falle erhalten. Er gilt grundsätzlich auch für Massnahmen, die zur Erfüllung der Levels 1 und 2 an bestehenden KI-Objekten zusätzlich zu ergreifen sind, damit die Schutzbemühungen im Rahmen der SKI erreicht werden können. Während aus „Schutzzielen“ auf Level 1 und Level 2 keine expliziten Aussagen zu den verbleibenden Risiken gemacht werden können, ermöglichen Level 3 mit risikoorientierten Schutzzielen und schliesslich Level 4 mit Risiko-Wirksamkeits-Kriterien in Form von Grenzkosten explizite Aussagen zu den Restrisiken.

Für alle KI-Betreiber, Teilsektoren und Sektoren einheitliche Schutzziele auf der Basis des Grenzkosten-Ansatzes.

Der Grenzkosten-Ansatz ist damit in seiner Einfachheit und seiner über alle kritischen Infrastrukturen und Risiken einheitlichen Anwendung bestechend. Jedes KI-Objekt, jeder Teilsektor und jeder Sektor kann damit mit ein und demselben Schutzziel arbeiten. Der Ansatz bietet damit Gewähr, dass überall mit denselben Massstäben gearbeitet werden kann. Die erforderliche gesellschaftlich-politische Anbindung ist über die Festlegung der Grenzkosten gegeben. Revisionen von bestehenden Rechtsgrundlagen sind nur insofern nötig, als dass sie noch verstärkt die Risiko basierte Sichtweise in der Schadenbeurteilung berücksichtigen müssen. Dies ist aber nicht SKI spezifisch, sondern gilt für die Rechtsprechung ganz allgemein.

Schliesslich ist zu erwähnen, dass der Grenzkosten-Ansatz nicht das alleine ausschlaggebende Entscheidungskriterium darstellt, ob und welche Massnahmen realisiert werden oder nicht. Divergierende Interessen von Politik, Gesellschaft, Wirtschaft oder Umwelt können ein Abweichen von der optimalen Massnahmenkombination nötig machen bzw. rechtfertigen. Dabei ist aber darauf zu achten, dass sich die geplanten Massnahmen trotzdem an der Grenzkosten-Kurve orientieren. Dies garantiert einen maximalen Kosten-Nutzen- (d.h. Risikoreduktions-) Effekt. Damit diese zusätzlichen politischen, sozialen, wirtschaftlichen und ökologischen Aspekte berücksichtigt werden können, und die Verhältnismässigkeit der Massnahmen beurteilt werden kann, ist eine fundierte, nachhaltige Güterabwägung nötig. Nur so können transparente und konsistente Entscheide getroffen werden.

Inter-institutionelle Finanzierung von SKI relevanten Schutzmassnahmen nötig

Die Umsetzung bietet neben grossen Vorteilen selbstverständlich noch zahlreiche Knacknüsse, zumal auch der Umgang mit Risiken der eingangs erwähnten zweiten Verantwortungsebene für die KI-Betreiber grösstenteils neu ist und auch die Finanzierung von allfällig erforderlichen Massnahmen für die SKI relevanten Risiken erst ansatzweise geklärt ist. Umso wichtiger wird sein, die beschränkt vorhandenen Mittel und Ressourcen kostenwirksam für Schutzmassnahmen einzusetzen. Solange das Grenzkosten-Kriterium eingehalten ist, sind die Mittel – unabhängig von KI-Objekt und Risiko - stets vernünftig eingesetzt. Die Anwendung dieses integralen und risikobasierten Kosten-Wirksamkeits-Ansatzes bedingt aber auch eine inter-institutionelle Finanzierung der Schutzmassnahmen. Es ist daher nicht auszuschliessen, dass gewisse Subventions-

Tatbestände anzupassen sind, damit diese inter-institutionelle Mittelzuweisung zur Abdeckung SKI relevanter Risiken möglich wird.

Forschung zur Verletzbarkeit nötig.

Die Ermittlung der Schäden und deren Monetarisierung bedingt, dass genügend Kenntnis vorhanden ist über die Verletzbarkeit von Menschen, Sachwerten, Infrastrukturen und deren Prozesse, der Umwelt, oder von ökonomischen, gesellschaftlich-politischen Systemen unter der Einwirkung verschiedenster Gefährdungsarten. In zahlreichen Fällen sind diese Verletzbarkeit und die Bewertung ihrer Folgen in Funktion der Intensität der Einwirkung einer Gefährdung erst ansatzweise bekannt und bedürfen weiterer Forschung.

Abschätzung der Wirksamkeit von Massnahmen enthält Unsicherheiten.

Die Ermittlung der verbleibenden Risiken stützt sich primär auf die Frage der Wirksamkeit bzw. Zuverlässigkeit der eingesetzten Schutzmassnahmen. Nicht alle Massnahmen bieten die gleiche Zuverlässigkeit. Dies ist insbesondere dann der Fall, wenn Menschen Bestandteile dieser Massnahmen sind, d.h. wenn es um organisatorische Massnahmen geht und allfällige Fehlentscheide in Krisensituationen zu weiteren Schäden führen können. Aber auch technische Massnahmen bieten nicht 100prozentigen Schutz. Diese verschiedenen Unwägbarkeiten gilt es in einer Gesamtbeurteilung nicht aus den Augen zu verlieren.

Versicherungslösungen und Solidaritätsfond für die Abdeckung von Restrisiken

Wie aus Abb. 3 ersichtlich wird, besteht bei Erreichen der Grenzkosten nach wie vor ein u.U. (beachtliches) Restrisiko, welches mit kostenwirksamen Massnahmen nicht abgedeckt werden kann. Sollte sich dieses Restrisiko im Eintretensfall zumindest teilweise als tatsächlicher Schaden konkretisieren, ist es wichtig, bereits im Vorfeld eine Strategie im Umgang mit Restrisiken zu haben. Für betriebliche Risiken bieten sich Versicherungslösungen (Elementarschadenversicherung, Haftpflichtversicherung, Betriebsausfallversicherung, etc.) an, für SKI relevante Risiken müssen auch vorgesetzte Fachstellen in die Bewältigung derartiger Schäden eingebunden sein (ev. Schaffung eines Solidaritätsfonds auf Bundesebene?). Da es sich um Schäden handelt, von denen eine u.U. grosse Allgemeinheit betroffen ist, kann auch damit gerechnet werden, dass die Solidarität unter Geschädigten und Nicht-Geschädigten zum Tragen kommt.

Überprüfung der Machbarkeit des Zusammenfügens von Schutz- und Leistungszielen

Im Rahmen der Erfahrungen bei der Anwendung des SKI Leitfadens und damit der Schutzziele, wird auch deren Bewährung zu überprüfen sein und gegebenenfalls Präzisierungen und Anpassungen vorzunehmen sein. Insbesondere wird sich die Praktikabilität der Kombination von Schutz- und Leistungszielen und deren Monetarisierung mit einem einzigen, gemeinsamen Indikatoren-Set zu einem potentiellen Gesamtschaden noch weisen müssen. Da bei KI-Objekten u.U. die Erfüllung von Leistungszielen stärker und die Minimierung von Schäden weniger im Vordergrund stehen, empfiehlt es sich, diese Frage der allenfalls eigenständigen Behandlung der Leistungsziele nicht aus den Augen zu verlieren.

Komplexität der Aufgabenstellung erfordert die Entwicklung geeigneter (Software-)Tools und Hilfsmittel

Die Vielfalt der Risiken und Prozesse, die es zu berücksichtigen und zu bearbeiten gilt, wird die Bereitstellung entsprechender Hilfsmittel (z.B. Software-Tools) erfordern. Dies gilt nicht nur für das Stadium der Risikoanalyse, aber insbesondere auch für die kostenwirksame Massnahmen-Planung. Die Ermittlung der optimalen Massnahmenkette, d.h. das optimale „Aneinanderreihen der verschiedenen möglichen Massnahmen“ ist bei der Vielzahl von Risiken und Prozessen ohne ein derartiges Hilfsmittel kaum praktikabel. Praktische Beispiele und Schulungen werden helfen, den KI-Betreibern in dieser Risiko basierten Herangehensweise und in der Anwendung der Tools die nötige Sicherheit und Zuverlässigkeit zu vermitteln. Ein periodischer Erfahrungsaustausch zwischen

KI-Betreibern, den Branchen und Fachstellen wird diese „Unité de Doctrine“ weiter steigern können und weitere Optimierungsmöglichkeiten beim Schutz von KI-Objekten eröffnen.

Periodisches Risiko-Controlling ist wichtig

Die Realisierung von kosten-wirksamen Schutzmassnahmen ist das primäre Ziel im Umgang mit Risiken. Die Wirksamkeit dieser Massnahmen ist nicht nur zu Beginn ein Thema. Sie wird sich im Verlaufe der Jahre verändern. Neue Gefährdungen und Prozesse können dazu kommen. Es ist deshalb wichtig, den Umgang mit Risiken als dynamischen Prozess über die Jahre zu verstehen. Ein periodisches Risiko-Controlling ist deshalb wichtig, bei dem z.B. alle 5 Jahre die Gefährdungslage, die organisatorischen Abläufe und Prozesse, die Indikatoren, der Zustand der Schutzmassnahmen, etc. überprüft werden, Restrisiken ermittelt, und allenfalls nötige Massnahmen getroffen werden.

Incidence Reporting ist wichtig in den KI-Betrieben. Branchenweite Ansätze sind gefragt

In diesem Zusammenhang ist ebenfalls sehr wichtig, dass in dieser Zeit aufgetretene Ereignisse und Schäden in die Neubeurteilung einbezogen werden. Auch kleine Schadenereignisse können dabei wichtige Indikatoren sein, grössere Lücken in den Schutzmassnahmen zu detektieren. Es ist deshalb zu empfehlen, dass die KI-Betreiber nach Möglichkeit ein „Incidence Reporting“ einrichten, welches es den Mitarbeitenden erlaubt, Schadenmeldungen zu machen, ohne sofort Konsequenzen für ein allfälliges Fehlverhalten gewärtigen zu müssen. Ein solches Incidence Reporting könnte auch auf Branchenebene eingeführt werden. Jedenfalls müsste gewährleistet sein, dass sämtliche sicherheitsrelevanten Ereignisse innerhalb der Branche gesammelt und ausgewertet werden können. Derartige Meldesysteme sind in der Aviatik bereits seit vielen Jahren erfolgreich im Einsatz.

All diese zusätzlichen Abklärungen, Massnahmen und Tools sollen dazu beitragen, das Bewusstsein im Umgang mit Sicherheit in den KI-Betrieben zu verbessern und die KI-Betriebe befähigen, die geeigneten kosten-wirksamen Schutzmassnahmen zu treffen. Anpassungen beim Vorgehen und bei den Schutzmassnahmen werden dabei auf der Basis der zu sammelnden Erfahrungen unvermeidlich sein.

7. Literatur

Hinweis: die wichtigsten, dem Bericht zu Grunde liegenden Literaturstellen sind im vorstehenden Berichtstext auch als Fussnoten direkt aufgeführt. Die hier aufgeführte Literatur wurde auf ihren Gehalt bezüglich Aussagen zum Thema Schutzziele gesichtet.

AG Naturgefahren Kanton Bern (2010): Schutzziele bei gravitativen Naturgefahren. Arbeitsgruppe Naturgefahren des Kantons Bern, 8. September 2010, Bern.

Akademien der Wissenschaft Schweiz (2012): Methoden zur Bestimmung von Nutzen bzw. Wert medizinischer Leistungen und deren Anwendung in der Schweiz und ausgewählten europäischen Ländern. Bern.

Ammann, W.J, Schneider, Th. (2004): „Strategie Naturgefahren Schweiz – Bericht an das UVEK in Erfüllung des Auftrages des Bundesrates vom 20. August 2003“, PLANAT c/o BAFU Bern, 79 p.

Ammann, W. und Bründl, M. (2004): Strategie Naturgefahren Schweiz. Umsetzung des Beschlusses des Bundesrates vom 20. August 2003. Teilprojekt B: Methoden und Evaluation. Schlussbericht. Nationale Plattform Naturgefahren PLANAT, Bern.

Ammann, W.J., J. Barross, A. Bennett, J. Bridges, J. Fragola, A. Kerrest, K. Marshall-Bowman, H. Raoul, P. Rettberg, J. Rummel, M. Salminen, E. Stackebrandt, N. Walter (2012). „Mars Sample Return backward contamination – Strategic advice and requirements“. Report from the ESF-ESSC Study Group on MSR Planetary Protection Requirements, European Science Foundation/European Space Science Committee, Sept. 2012, 60 p.

Auerswald, P. et al. (2005): The Challenge of Protecting Critical Infrastructure. Working Paper No. 05-11, Risk Management and Decision Processes Center, Philadelphia, USA.

BABS (2008): Risikoaversion – Ein Beitrag zur systematischen Risikobeurteilung, Bundesamt für Bevölkerungsschutz,Bern, 31. Okt. 2008.

BABS (2012a): Leitfaden Schutz Kritischer Infrastruktur. Entwurf, 23. Juli 2012. Bundesamt für Bevölkerungsschutz, Bern.

BABS (2012b): Nationale Strategie zum Schutz Kritischer Infrastrukturen. Bundesamt für Bevölkerungsschutz, Bern.

BAFU (2008): Schutzauftrag und Subventionierung bei Naturgefahren. Rechtsgutachten. Bundesamt für Umwelt, Bern.

BAV (2013): Sicherheitskonzept BAV. Bern.

BKK (2012): Schutzkonzepte Kritischer Infrastrukturen im Bevölkerungsschutz. Ziele, Zielgruppen, Bestandteile und Umsetzung im BKK. Wissenschaftsforum, Band 11, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Bonn.

BBK (2011): Bevölkerungsschutz: Risikomanagement. Deutsches Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Berlin und Bonn.

BBK (2010): Methode für die Risikoanalyse im Bevölkerungsschutz. Wissenschaftsforum, Band 8. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK).

BBK (2009): Vulnerabilität Kritischer Infrastrukturen. Band 4 der Schriftenreihe Forschung im Bevölkerungsschutz. Deutsches Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Berlin und Bonn.

BKK (2008): Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus. Langfassung aus Band 2, Auflage 11/2008 S. 30 ff.

BfR (2005): Risikobewertung genotoxischer und kanzerogener Stoffe soll in der EU harmonisiert werden. Stellungnahme Nr. 029/2005 des BfR vom 18. Mai 2005.

Bienz, A. (2006): Revised Risk-Based Safety Criteria to be proposed for the Handling of Ammunition and Explosives in the Swiss Army and Military Administration. ETH Zurich, Switzerland.

Birkmann, J. et al. (2010): State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastruktur am Beispiel Strom/Stromausfall. Forschungsforum öffentliche Sicherheit, Schriftenreihe Sicherheit Nr. 2, Freie Universität Berlin.

Bohnenblust, H. und Schneider, T. (1983): Sicherheitskonzept für die Tunnel der Neubaustrecken. Fraunhofer IRB Verlag.

BMI (2007): Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden. Deutsches Bundesministerium des Inneren, Berlin und Bonn.

BMI (2011a): Schutz Kritischer Infrastruktur: Basisschutzkonzept – Empfehlungen für Unternehmen. Deutsches Bundesministerium des Inneren, Berlin und Bonn.

BMI (2011b): Nationale Strategie zum Schutz Kritischer Infrastruktur (KRITIS-Strategie). Deutsches Bundesministerium des Inneren, Berlin und Bonn.

Boin, A. and A. McConnell (2007): Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. Journal of Contingencies and Crisis Management, 15(1): 50-59.

Borter (1999): Risikoanalyse bei gravitativen Naturgefahren. Fallbeispiele und Daten. Bundesamt für Umwelt, Wald und Landschaft (BUWAL), Bern.

Braband, J. et al. (2006): Die CENELEC-Normen zur Funktionalen Sicherheit. Eurailpress T

Braband, J. (2005): Risikoanalysen in der Eisenbahn-Automatisierung. Eurailpress Tetzlaff-Hestra GmbH & Co. KG, Hamburg.

Brazier. J, J. Ratcliffe (2007): Measuring and valuing health benefits for economic evaluation.

Brühwiler, E. (2011): Das neue Schweizer Normenwerk zum Umgang mit bestehenden Tragwerken. Stahlbau 80 (2011), Heft 6.

Bründl, M. (2009): Strategie Naturgefahren Schweiz. Umsetzung des Aktionsplans PLANAT 2005-2008 / 2009-2011, Projekt A 1.1: Risikokonzept für Naturgefahren - Leitfaden. Nationale Plattform Naturgefahren PLANAT, Schlussbericht Phase 2, Testversion, Februar 2009, Bern.

Bundesamt für Verkehr (2010): Berechnung und Bewertung des individuellen Risikos für den öffentlichen Verkehr. SiT Workshop, TU Braunschweig.

Bundesnetzagentur (2012a): Versorgungsqualität - Übersicht SAIDI-Werte Strom 2006 – 2011. (http://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetGas/ Sonderthemen/SAIDIWerteStrom/SAIDIWerteStrom_node.html), Zugriff: 2. April 2013.

Bundesnetzagentur (2012b): Versorgungsqualität – SAIDI Wert Gas 2011. (http://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetGas/Sonderthemen/SAIDIWertGas2011/SAIDIWertGas2011_node.html), Zugriff: 2. April 2013.

Bundesrat (2009): Grundstrategie des Bundesrates zum Schutz Kritischer Infrastruktur. Basis für die nationale Strategie zum Schutz Kritischer Infrastrukturen. Der Bundesrat, Bern.

Burgess, J.P. (2007): Social values and material threat: the European Programme for Critical Infrastructure Protection. International Journal of Critical Infrastructures, 3(3-4): 471-487.

BUWAL (2003): Monetarisierung verkehrslärmbedingter Gesundheitsschäden. Umweltmaterialien, Nr. 166, Lärm. Bern.

BUWAL (1999a): Risikoanalyse bei gravitativen Naturgefahren. Fallbeispiele und Daten. Bern.

BUWAL (1999b): Risikoanalyse bei gravitativen Naturgefahren. Methode. Bern.

Cabinet Office UK (2012): National Risk Register for Civil Emergencies. 2012 Edition.

Canning, D. (2006): The Economics of HIV/AIDS in Low-Income Countries: The Case for Prevention. Program on the Global Demography of Aging, Working Paper Series. Boston.

Crisis and Risk Network (CRN) and Center for Security Studies (CSS) (2010a): Critical Infrastructure Protection. Protection Goals. Focal Report 4, CRN Report commissioned by the Federal Office for Civil Protection (FOCP), Zurich.

Crisis and Risk Network (CRN) and Center for Security Studies (CSS) (2010b): Der Schutz Kritischer Infrastrukturen. Gegenwart und Zukunft. CRN Report im Auftrag des Bundesamtes für Bevölkerungsschutz (BABS), Zurich.

Daskapan, S., W.G. Vree and R.W. Wagenaar (2006): Emergent information security in critical infrastructures. International Journal of Critical Infrastructures, 2(2-3): 247-260.

Dapra, D. (2009): Das ALARA - Prinzip in der Praxis. 4. Kärntner Ethik-Tag 'Der aufgeklärte Patient: Anspruch und Wirklichkeit' Casino Velden, 20. November 2009

De Bruijne, M., M. Van Eeten, E. Roe and P. Schulman (2006): Assuring high reliability of service provision in critical infrastructures. International Journal of Critical Infrastructures, 2(2-3): 231-246.

De Bruijne, M. and M. van Eeten (2007): Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment. Journal of Contingencies and Crisis Management, 15(1): 18-29.

Deutsche Bundesbahn (1983): Sicherheitskonzept für die Tunnel der Neubaustrecken. Schlussbericht. München.

Department of Homeland Security (2011): Strategic National Risk Assessment. The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation.

DePoy, J. et al. (2006): Critical Infrastructure Systems of Systems Assessment Methodology. Sandia Report, Sandia National Laboratories, New Mexico, USA.

DHS (2006): National Infrastructure Protection Plan. Building a Safer, more Secure, and more Resilient America. U.S. Department of Homeland Security, Washington, D.C.

Dunn Cavelty, M. and Mauer, V. (eds.) (2010): The Routledge Handbook of Security Studies. Routledge USA and Canada.

Dunning, H. (2004): A Mixed Method Approach to Quality of Life in Saskatoon. Saskatoon, Canada.

Drewitz, Y. (2011): Methodik zur Durchführung einer Quantitativen Risikoanalyse unter Berücksichtigung des Standes der Sicherheitstechnik bei Störfall-Anlagen in Deutschland. T

Egan, M.J. (2007): Anticipating future vulnerability: defining characteristics of increasingly critical infrastructure-like systems. Journal of Contingencies and Crisis Management, 15(1): 4-17.

European Union (2008): COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the n

Expertenkommission für Sicherheit in der chemischen Industrie der Schweiz (ESCIS) (1996): Einführung in die Risikoanalyse: Systematik und Methoden. Heft 4, 1996, 3. Überarbeitete Auflage. Basel.

Faber, M. H. and Maes, M. (2010): Sustainable Management of Life Safety Risks. International Journal of Engineering under Uncertainty, Hazards, Assessment, and Mitigation, 2 (1-2): 9-17.

Faber, M.H. and Virguez-Rodriguez, E. (2011): Supporting decisions on global health and life safety Investments. 11th International Conference on Applications of Statistics and Probability in Civil Engineering, ICASP11. August 1 – 4, 2011, Zurich, Switzerland. 2011.

FEDPOL (2004): Grundlagen für die Beurteilung von Risiken bei der Lagerung von Sprengmitteln für zivile Zwecke durch die Zentralstelle Sprengstoff und Pyrotechnik (ZSP). Vollzug Sprengstoffgesetzgebung (Art. 74 Abs. 5 SprstV), Bundesamt für Polizei (fedpol), Bern, Schweiz.

FEMA (2011): Critical Infrastructure: Long-term Trends and Drivers and Their Implications for Emergency Management. Strategic Foresight Initiative, US Federal Emergency Management Agency, Washington DC, 7 pp.

Foege, W. H. (2013): Preventive Medicine and Public Health. (http://web.archive.org/web/20071011061930/http://www.ihpnet.org/preventtxt.htm.), Zugriff: 25. April 2013.

Fritzsche, A. F. (1986): Wie sicher leben wir? Risikobeurteilung und –bewältigung in unserer Gesellschaft. Verlag TÜV Rheinland GmbH, Köln.

Fritzon, A., K. Ljungkvist, A. Boin and M. Rhinard 2007. Protecting Europe's critical infrastructures: problems and prospects. Journal of Contingencies and Crisis Management, 15(1): 30-40.

Fuchs, S. and McAlpin, M. C.: The Net Benefit of Public Expenditures on Avalanche Defence Structures in the Municipality of Davos, Switzerland, *Nat. Hazards Earth System Sciences,* 5, 319–330, 2005

Gamper, C.D., Thöni, M. and H. Weck-Hannemann (2006), "A conceptual approach to the use of Cost Benefit and Multi Criteria Analysis in natural hazard management", *Natural Hazards and Earth System Sciences*, 6:293-302.

Gordon, K. and M. Dion (2008): Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security. Organization for Economic Co-operation and Development, Paris, 11 pp.

Government of Australia (2004): Critical Infrastructure Protection National Strategy. Trusted Information Sharing Net¬work for Critical Infrastructure Protection. (www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/.../t0KMVCM4.pdf), Zugriff: 27. März 2013.

Government of Canada (2009): Working towards a National Strat¬egy and Action Plan for Critical Infrastructure. Public Safety Canada. (http://www.publicsafety.gc.ca/prg/em/cip/strat-part1-eng.aspx), Zugriff: 27. März 2013.

Government of the United States (2007): Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies. United States Government Accountability Office, Report to Congressional Re¬questers. (http://www.gao.gov/new.items/d08113.pdf), Zugriff: 27. März 2013.

Graham, J. and Kaye, D. (2006): A Risk Management Approach to Business Continuity. Aligning Business Continuity with Corporate Governance. Rothstein Associates Inc., Brookfield, Connecticut, USA.

Grünenfelder, L. (2006): Analyse der Kosten-Wirksamkeit organisatorischer Risiko-Schutzmassnahmen an ausgewählten Fallbeispielen aus dem Bereich Naturgefahren. ETH Zürich, Zürich.

Güngerich, A. und Walpen, A. (2011): Rechtliche Aspekte eines risiko- und effizienzbasierten Sicherheitskonzepts. Sicherheit & Recht 2 (2011).

Gutzwiler et al. (2012): Methoden zur Bestimmung von Nutzen bzw. Wert medizinischer Leistungen und deren Anwendung in der Schweiz und ausgewählten europäischen Ländern. Akademien der Wissenschaften Schweiz. Bern.

GVG (2012): Risikochecklisten Gemeinden (Bestandesaufnahme und Grobbeurteilung). Disentis/Mustér.

Habegger, B. (ed.) (2008): International Handbook on Risk Analysis and Management. Professional Experiences. Center for Security Studies, ETH Zurich, Zurich.

Haimes, Y.Y. and T. Longstaff (2002): The role of risk analysis in the protection of critical infrastructures against terrorism. Risk Analysis, 22(3): 439-444.

Hepperle, E. (2011): Rechtliche Verankerung des integralen Risikomanagements beim Schutz vor Naturgefahren. Rechtsgutachten. Bundesamt für Umwelt, Bern. Umwelt-Wissen Nr. 1117: 125 S.

Hess, J. (2011): Schutzziele im Umgang mit Naturrisiken in der Schweiz. Dissertation ETH Zürich, vdf Hochschulverlag, Zürich.

Hess, J. (2008): Schutzziele im Umgang mit Naturrisiken. Wandel auf dem Pfad der Gerechtigkeit. Interpraevent 2008 – Conference Proceedings, Vol. 2.

Hochrainer-Stigler, S., Kunreuther, H., Linnerooth-Bayer, J., Mechler, R., Michel-Kerjan, E., Muir-Wood, R., Ranger, N, Vaziri, P., and Young M.. (2010), "The Costs and Benefits of Reducing Risk from Natural Hazards to Residential Structures in Developing Countries," Wharton University of Pennsylvania. Working Paper 2011-01.

Homeland Security Council (2007): National Strategy for Homeland Security.Washington, D.C., USA.

Homeland Security Council (2009): National Infrastructure Protection Plan. Partnering to enhance protection and resilience. Washington, D.C., USA.

Hunziker, S. und Rintelen, C. (2005): Strategie Naturgefahren Schweiz. Umsetzung des Beschlusses des Bundesrates vom 20. August 2003. Teilprojekt C: Kommunikation. Zwischenbericht, März 2005. Nationale Plattform Naturgefahren PLANAT, Bern.

Hyslop, M. (2007): Critical Information Infrastructures: Resilience and Protection. Springer, Berlin, 277 pp.

ILK (2008): Grundlegende Sicherheitsanforderungen für Kernkraftwerke. Beilage zu ILK-31. Internationale Länderkommission Kernkraftwerke, Baden-Würtemberg, Bayern, Hessen.

International Commission on Radiological Protection (1977): IRCP Publication 26, Pergamon Press, Oxford 1977.

IRCG (2012): An Introduction to the IRGC Risk Governance Framework. Genf. (http://irgc.org/wp-content/uploads/2012/04/An_introduction_to_the_IRGC_Risk_Governance_Framework.pdf), Zugriff: 20. März 2013.

John, R. and Ross, H. (2008): Economic value of disability-adjusted life years lost to cancers.

Kanton Bern (2005): Risikostrategie Naturgefahren. Ergebnissicherung der Klausursitzung des Regierungsrates vom 10. August 2005. Bern.

Kanton Schwyz (2010): Naturgefahren im Kanton Schwyz. Kantonale Naturgefahrenstrategie (Revision 2010). Schwyz.

King, C. H. und Bertino. A.-M. (2008): Asymmetries of Poverty: Why Global Burden of Disease Valuations Underestimate the Burden of Neglected Tropical Diseases. PLoS Neglected Tr

KGG (2013): Kernkraftwerk Gundremmingen GmbH. (http://www.kkw-gundremmingen.de/kkw_s.php), Zugriff: 2. April 2013.

Koski, C. (2011): Committed to protection? Partnerships in critical infrastructure protection. Journal of Homeland Security and Emergency Management, 8: Article 25.

Kubler, O. and Faber, M.H. (2005). LQI: On the correlation between life expectancy and the gross domestic product per capita. Proceedings of ICOSSAR 2005, Rome, Italy.

Kühling, W. (2004): Risikomanagement im Rahmen der Störfall-Verordnung duch "Risikogrenzwerte"? Versuch einer kritischen Würdigung des Berichts „Risikomanagement im Rahmen der Störfall-Verordnung". KGV-Rundbrief, Nr. 4 (2004), S. 8-12 (ISSN 0949-8192).

LaPorte, T. R. (2007): Critical infrastructure in the face of a predatory future: preparing for

Lindström, M. 2009. The European Programme for Critical Infrastructure Protection. In S. Olsson (ed.), Crisis Management in the European Union. Springer, Berlin: 37-59.

Lovecek, T., J. Ristvej and L. Simak (2010): Critical infrastructure protection systems effectiveness evaluation. Journal of Homeland Security and Emergency Management, 7(1): Article 34.

Löfstedt, R. E. and Boholm, A. (eds.) (2012): The Earthscan Reader on Risk. Earthscan Publications Ltd, London, UK.

Masoli et al. (2012): The global Burden of Asthma. Developed for the Global Initiative for Asthma.

McDougall, A. (2009): Fragility: the next wave in critical infrastructure protection. Journal of Strategic Security, 2(2): 91-98.

McNeil, A. J. et al. (2005): Quantitative Risk Management. Concept, Techniques, Tools. Princeton Series in Finance, Princeton University Press, Princeton and Oxford.

Merz, H.A., Schneider, T, Bohnenblust, Hans (1995): Bewertung von technischen Risiken. Vdf Hochschulverlag an der ETH Zürich, Zürich.

Moteff, J. and P. Parfomak (2004): Critical Infrastructure and Key Assets: Definition and Identification. Report for Congress, Congressional Research Service, Washington DC, 16 pp.

Murray et al. (2010): Disability-adjusted life years (DALYs) for 291 diseases and injuries in 21 regions, 1990–2010: a systematic analysis for the Global Burden of Disease Study 2010. The Lancet, Vol. 308 Dec. 2012.

Nasterlack, M. (2005): Gesundheitsnutzen von REACH in industrieller Perspektive. Vortrag am 22. Januar 2005 auf dem Workshop der Evangelischen Akademie. Loccum: "Vorsorgende Chemikalienpolitik in der erweiterten EU: Wieviel Fortschritt bringt die REACH-Verordnung?

Nathwani, J.S., N.C. Lind and M.D. Pandey (1997): Affordable Safety by Choice: The Life Quality Method. Institute for Risk Research, University of Waterloo, Ontario, Canada.

NCRST (2002): Spatial Information Technologies in Critical Infrastructure Protection. National Consortium on Remote Sensing in Transportation, U.S. Department of Transportation, University of California, Santa Barbara.

NIAC (2010): A Framework for Establishing Critical Infrastructure Resilience Goals. Final Report and Recommendations by the Council. National Infrastructure Advisory Council, Washington, D.C.

Lorenz, D. (2010): Kritische Infrastruktur aus Sicht der Bevölkerung. Schriftenreihe Forschungsforum öffentliche Sicherheit, Berlin.

O'Riordan, T. und Stasch, A. (Hrsg.) (1994): Umweltwissenschaften und Umweltmanagement: Ein interdisziplinäres Lehrbuch. Springer, Berlin, Heidelberg, New York.

Okrent, D. und Whipple, C. (1977): An Approach to Societal risk Acceptance Criteria and

Ostermann, N. und Schöbel, A. (2004): Betrachtungen zur Risikoanalyse im Eisenbahnbau. TU Wien.

Pfnür, A. et al. (2010): Risikomanagement bei Public Private Partnerships. Springer Verlag, Heidelberg, Deutschland.

PLANAT (2009a): Strategie Naturgefahren Schweiz. Umsetzung des Aktionsplans PLANAT 2005-2008 / 2009-2011, Projekt B 2.2 Schutzziel-Modell. Nationale Plattform Naturgefahren PLANAT, Schlussbericht Phase 2, 29. Mai 2009, Bern.

PLANAT (2009b): Strategie Naturgefahren Schweiz. Aktionsplan PLANAT 2005-2008. Berichterstattung, Nationale Plattform Naturgefahren PLANAT, Bern.

PLANAT (2008): Strategie Naturgefahren Schweiz. Umsetzung des Aktionsplans PLANAT 2005-2008, Projekt B 2.2 Schutzziele. Nationale Plattform Naturgefahren PLANAT, Schlussbericht 1. Phase, 11. Februar 2008, Bern.

PLANAT (2004a): Strategie Naturgefahren Schweiz – Synthesebericht. Umsetzung des BRB vom 20. August 2003. Nationale Plattform Naturgefahren PLANAT, Eidg. Institut für Schnee- und Lawinenforschung, Davos.

PLANAT (2004b): Sicherheit vor Naturgefahren. Vision und Strategie. Von der PLANAT Plenarversammlung am 13. November 2002 genehmigt. Nationale Plattform Naturgefahren PLANAT, Bern.

Plattner, T.M. (2006): Risikoaversion als relevanter Faktor der Risikobewertung von Naturgefahren. ETH Zürich, Zürich.

Prezelj, I., E. Kopac, U. Svete and A. Iberna (2012): Cross-sectoral scanning of critical infrastructures: from functional differences to policy-relevant similarities. Journal of Homeland Security and Emergency Management, 9(1): Article 19.

Public Safety Canada (2008): Working Towards a National Strategy and Action Plan for Critical Infrastructure: Strategy. Ottawa, Canada.

Rasmussen, N. C. (1975): Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants. Main Report, WASH-1400, US NRC, Oct. 1975.

Renn, O. and Walker, K. (2008): Global risk Governance. Concept and Practice Using the IRGC Framework. Springer, The Netherlands.

Roberts, S. (2004): Tips and trends for homeland security and critical infrastructure protection. Journal of Homeland Security and Emergency Management, 1(4): Article 405.

Romang, H. et al. (2000): Wirksamkeit und Kosten von Wildbachschutzmassnahmen – ein Studienkonzept. Internationales Symposion INTERPRAEVENT 2000, Villach/A, Tagungspublikation, Band 3, S. 271-282.

Rowe, W. D. (1977): An Anatomy of Risks. John Wiley.

Sarriegi, J.M. et al. (2008): Towards a research framework for critical infrastructure interdependencies. International Journal of Emergency Management (IJEM), 5(3-4): 235-249.

Schäbe, H. (2005): Bestimmung von Risikogrenzwerten für Magnetschwebebahnen. Dresdner Fachtagung Transrapid, 29. Sept. 2005. Dresden.

Schnieder, E. et al. (2005): New and Conventional Measures for Quantifying Risk in Rail Transport. In: Journal of System Safety, 41(1).

Scholz, F. et al. (Hsg.) (2009): Risikomanagement der Öffentlichen Hand. Physica-Verlag, Heiderberg.

Schubert, M. und Faber, M.H. (2008): Beurteilung von Risiken und Kriterien zur Festlegung akzeptierter Risiken in Folge aussergewöhnlicher Einwirkungen bei Kunstbauten. ETH Zürich, Zürich.

Schwarze, J. (1997): Grundlagen der Statistik – Band 2: Wahrscheinlichkeitsrechnung und induktive Statistik. 6. Auflage, Berlin; Herne: Verlag Neue Wirtschaftsbriefe.

SFK (2004): Risikomanagement im Rahmen der Störfall-Verordnung. Arbeitskreis Technische Systeme, Risiko und Verständigungsprozesse der Störfall-Kommission, Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, Bonn.

Shi, P. et al. (2011): Integrated Risk Governance. Science Plan and Case Studies of Large-scale Disasters. Beijing Normal University Press, Beijing, China.

Siemens (2012): As Low As Reasonably Achievable (ALARA) planning. (http://m.plm.automation.siemens.com/en_us/Images/Siemens-PLM-Tecnomatix-As-Low-As-Reasonably-Achievable-ALARA-Planning-fs_tcm1224-200557.pdf), Zugriff: 20. März 2013.

Slovic, P. (2000): The Perception of Risk. Earthscan Publications Ltd, London, UK.

Stewart, M. (2009): Risk-informed decision support for assessing the costs and benefits of counter-terrorism protective measures for infrastructure. International Journal for Critical Infrastructure Protection, 3 (2010): 29-40.

Solano, E. (2010): Methods for Assessing Vulnerability of Critical Infrastructure. Research Brief, Institute for Homeland Security, North Carolina, USA.

SMB (Swiss Medical Board) (2009): Beurteilung medizinischer Verfahren. Gesundheitsdirektion des Kantons Zürich. (http://www.medical-board.ch/index.php?id=807), Zugriff: 20. März 2013.

Talbot, J. (2013): ALARP (As Low As Reasonably Practicable). http://www.jakeman.com.au/media/alarp-as-low-as-reasonably-practicable Zugriff: 12.03.2013.

The World Bank (2010): Natural Hazards, UnNatural Disasters. The Economics of Effective Prevention. Washington, D.C., USA.

UBA (2007): Ökonomische Bewertung von Umweltschäden. Methodenkonvention zur Schätzung externer Umweltkosten. Deutsches Umweltbundesamt, Dessau.

UK Cabinet Office (2011): Keeping the Country Running: Natural Hazards and Infrastructure. UK Government, London, 98 pp.

UK Cabinet Office (2010): Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards. UK Government, London, 26 pp.

UK Cabinet Office (2009): The National Security Strat¬egy of the United Kingdom: Update 2009 – Security for the Next Generation. UK Cabinet Office. Available at: (http://www.cabinetoffice.gov.uk/media/216734/nss2009v2.pdf), Zugriff: 27. März 2013.

URS (2010): Adapting Energy, Transport and Water Infrastructure to the Long-term Impacts of Climate Change (Ref. No RMP/5456). Report to the British Government, URS Corporation, London, 194 pp.

US Department of Homeland Security (2008): A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Level. Office of Infrastructure Protection, National Protection & Programs Directorate, U.S. Department of Homeland Security, Washington, DC.

UVEK (2009): Sicherheit des Verkehrssystems Strasse und dessen Kunstbauten. Rechtliche Aspekte eines risiko- und effizienzbasierten Sicherheitskonzepts. Forschungsauftrag AGB 2005/106 auf Antrag der Arbeitsgruppe Brückenforschung (AGB).

Wegmann, M. und Merz, H. (2004): Strategie Naturgefahren Schweiz. Umsetzung des Beschlusses des Bundesrates vom 20. August 2003. Teilprojekt A: Gesamtübersicht. Schlussbericht. Nationale Plattform Naturgefahren PLANAT, Bern.

WHO (2013a): Health Statistics and Health Information Systems: Disease and injury country estimates.(http://www.who.int/healthinfo/global_burden_disease/estimates_country/en/index. html), Zugriff: 25. April 2013.

WHO (2013b): Health Statistics and Health Information Systems: Metrics: Disability-Adjusted Life Year (DALY). (http://www.who.int/healthinfo/global_burden_disease/ estimates_country/en/index.html), Zugriff: 25. April 2013.

Wikipedia (2013a): Sicherheit von Kernkraftwerken. (http://de.wikipedia.org/wiki/Sicherheit_von_Kernkraftwerken), Zugriff: 2. April 2013.

Wikipedia (2013b): Liste historischer Stromausfälle. (http://de.wikipedia.org/wiki/Liste_historischer_Stromausf%C3%A4lle), Zugriff: 2. April 2013.

Wikipedia (2013c): Stromausfall. (http://de.wikipedia.org/wiki/Stromausfall), Zugriff: 2. April 2013.

Wikipedia (2013d): Versorgungssicherheit. (http://de.wikipedia.org/wiki/Versorgungssicherheit), Zugriff: 2. April 2013.

Winther, E. (2010): Kompetenzmessung in der beruflichen Bildung. W. Bertelsmann Verlag GmbH & Co. KG, Bielefeld.

Willke, B. (2007): A Critical Information Infrastructure Protection Approach to Multinational Cyber Security Events. Carnegie Mellon University, software Engineering Institute, Pittsbur

Zheng, S. (2004): Maximum Likelihood Estimation. Math 541: Statistical Theory II. Missouri State University, USA.

Zimmerman, R. and C.E. Restrepo (2006): The next step: quantifying infrastructure interdependencies to improve security. International Journal of Critical Infrastructures, 2(2-3): 215-230.

8. Anhang

A1 Vereinfachtes Beispiel zur Illustration

Im Folgenden wird ein stark vereinfachtes, fiktives Beispiel dargestellt. Es soll trotzdem erlauben, einige grundsätzliche Aspekte daran zu erläutern. Bei den aufgeführten Massnahmen wird davon ausgegangen, dass sie voneinander unabhängig sind, also nicht auch zur Risikominderung in einem anderen Gefährdungsszenario beitragen. Ausgangspunkt ist ein Spital mittlerer Grösse. Zudem werden folgende Annahmen getroffen:

- Betrachtet werden die Gefährdungen IT-Ausfall, Erdbebeneinwirkung und Pandemie.
- Die Aversion ist der Einfachheit halber analog dem PLANAT Vorschlag eingeführt, d.h. linearer Anstieg zwischen 1 bis 20 Toten vom Faktor 1 auf 10, und dann konstanter Aversionsfaktor von 10
- Grenzkosten pro Todesopfer: 4 Mio CHF
- Vereinfachend wird nur ein Gefährdungszustand betrachtet (für das gesamte Risiko müsste im Prinzip über die gesamte Farmer-Kurve integriert werden)
- Investitionen für Massnahmen werden über deren Laufzeit mit 4% hochgerechnet und dann auf einen Jahreswert reduziert.
- Massnahmenkosten und die angenommenen Risikoreduktionen sind fiktiv
- Als Faustformel für die Kostenwirksamkeit von Massnahmen sollten ihre auf die gesamte Wirkungsdauer bezogenen jährlichen Kosten maximal 1/3 des jährlichen Schadenerwartungswertes betragen.
- Eine Gesamtübersicht ist in Tabelle 4 und in Abb. 10 gegeben (wird nicht einzeln darauf verwiesen).

Die wichtigsten **Kenngrössen** des Spitals seien (Annahmen):

• Jahresumsatz (365 Tage)	250 Mio
• Mittlerer Tagesumsatz	0.70 Mio
• Stationäre Patienten pro Jahr	15‘000
• Anzahl Patienten bei 1 Woche Aufenthalt	288/Tag
• Ambulante Patienten	50‘000
• Anzahl ambulante Patienten pro Tag	140
• Patienten insgesamt pro Tag	430/ Tag
• Tagesumsatz pro Patient	1‘700 CHF
• Anzahl Angestellte	1‘800
• Vollzeit Äquivalent	1‘200

Gefährdungsszenario 1: IT Ausfall

Schadenszenario Annahmen: Ausfall führt während 1 Woche zu massiven Behinderungen, 2 Tote insgesamt

Risiko-Typ: Betriebs relevant

Ermittlung des jährlichen Schadenerwartungswertes:

- Umsatzeinbusse: 1 Woche auf 50% reduz.: 2.5 Mio.

- Anzahl Tote durch IT Ausfall: 2 (à 4 Mio.) 8 Mio.
- Totaler Schaden: 10.5 Mio.
- Ausfallwahrscheinlichkeit: 25 Jahre
- Jährlicher Schadenerwartungswert (1/25): 400‘000.-CHF
- Grenzaufwand gemäss Faustformel (1/3) 133‘000.-/Jh.

Mögliche Massnahmen: Ringleitung
Kosten CHF 475‘000 ergibt mit 4% auf 25 Jahre gerechnet rund 1.25 Mio., resp. rund CHF 50‘000.- jährliche Kosten (1/25), d.h. deutlich unter dem Grenzaufwand gemäss Faustformel.
Wirksamkeit der Massnahme: sie reduziere den Schadenerwartungswert um 75%, d.h. um CHF 300‘000.
Verhältnis von Risikoreduktion: Massnahmenkosten = 300‘000: 50‘000 = 6

Die in Tab. 4 und Abb. 10 aufgeführte weitere Massnahme (IT 2 – separate Räumlichkeit) fällt gerade noch knapp in den Bereich der Kostenwirksamkeit.

Gefährdungsszenario 2: Erdbeben

Schadenszenario Annahmen: Szenario mit :

- Magnitude 6.5 Erdbeben (500 Jahre Wiederkehrperiode), markante Schäden im Umkreis von 30 km.
- mit Schäden am Spital selbst (Bettenhaus mit 180 Betten teilweise beschädigt, 2 Tote, vorsorgliche Evakuation angeordnet, 2 Tote, eingeschränkte Chirurgie)
- 10 nachträgliche Tote wegen reduzierter Funktionsfähigkeit bzw Priorität für Erdbebenopfer)
- Insgesamt 50 Tote in Umkreis von 30 km und 200 Verletzte, davon 100 schwer.

Risikotyp: Betriebs und SKI relevant

Ermittlung des jährlichen Schadenerwartungswertes:

- Eingeschränkter Betrieb wegen Evakuation für drei Tage: 180 Betten x 3 Tage x 1‘700.- 1 Mio
- Instandstellung Bettenhaus 3 Mio
- Tote im Spital: 2 à 4 Mio 80 Mio
- Zusätzl.Tote mangelnde Versorgung 5 200 Mio
- Zusätzl.Tote mangelnde Kapazität 5 200 Mio

Totaler Schaden 484 Mio
Davon Betriebs relevanter Schadenanteil 84 Mio (exkl. 20 zusätzl. t)

Jährlicher Schadenerwartungswert (1/500): 1.0 Mio
Schadenerwartungswert in 50 Jahren (1 x 50) 50 Mio

Mögliche Massnahmen:
Anwendung der 1/3 Faustregel: Investition auf 50 Jahre 17 Mio
Gebäudeverstärkung: bei 4% Verzinsungsrate auf 50 Jahre dürfte die Massnahme nicht mehr als etwa 2.5 Mio CHF kosten (ergibt aufgezinst rund 15 - 17 Mio nach 50 Jahren und entsprechend jährliche Kosten (15 Mio auf 50 Jahre) = CHF 300‘000/Jahr

Wirksamkeit der Massnahme: sie reduziere den Schadenerwartungswert um 80%, d.h. um CHF 800‘000.

Verhältnis von Risikoreduktion: Massnahmenkosten = 800‘000:300‘000 = 2.7
Die in Tab. 4 aufgeführte weitere Massnahme betrifft die Verstärkungen an Einrichtungen (Erdbeben 2 in Abb. 11). Sie ist in unserem Falle ebenfalls wirksam.

Der **Betriebsrelevante** Schadenanteil beträgt in diesem exemplarischen Fall 84 Mio. d.h. rund CHF 170‘000/Jahr bzw. auf 50 Jahre rund 8. 5 Mio. Anwendung der 1/3 Faustformel ergibt rund 3 Mio. auf 50 Jahre, bzw. eine Investition von rund CHF 400‘000.-. Nehmen wir an, dass eine Überprüfung gemäss Level 1 und Level 2 ergeben hat, dass die Erdbebennorm nur teilweise eingehalten wurde, müssen zwingend Massnahmen getroffen werden, d.h. z.B. das Gebäude verstärkt werden. Nehmen wir an, dass diese Massnahmen rund 2 – 2.5 Mio. kosten, können damit zu einem sehr grossen Teil wohl auch die SKI relevanten Schäden abgewendet werden, so dass sich die Frage nach dem „Wer zahlt die Abdeckung des SKI relevanten Risikos“ im Falles des Erdbebens hier kaum stellt. (Theoretisch offen bleibt natürlich dann die Frage, ob allenfalls die geforderten Massnahmen nach Level 1 und Level 2 generell zu hoch angesetzt sind).

Nehmen wir allerdings an, dass die Normen eingehalten wurden und mit der aufgeführten 2. Massnahme die Betriebs relevanten Risiken abgedeckt werden können, stellt sich schon die Frage, wer die Verstärkungsmassnahmen am Spital zu finanzieren hat. In Analogie zu Finanzierung einer Lawinenverbauung, die eine Zufahrtsstrasse zu einem Dorf schützt, könnte man erwarten, dass dies gleichartig von Bund und Kanton getragen werden.

Gefährdungsszenario 3: Pandemie

Schadenszenario Annahmen:

• 1/3 der Belegschaft fällt aus	600 P
• Mittlere Ausfallzeit:	3 Monate
• Einzugsgebiet Patienten	50‘000 Einw.
• Pandemiebefall: 1/3	17‘000 P
• Hospitalisierte Personen: 1/6	3‘000 P
• Hospitalisierungszeit indiv. Patient:	2 Wochen
• Tagesbelegung auf 3 Monate	500 P
• Sterberaten: 1/10 der Hospitalisierten	300 Tote
• Auftretenswahrscheinlichkeit (100 J.)	1/100

Ermittlung des jährlichen Schadenerwartungswertes:

Betriebsausfall infolge Unterbesetzung	
1/3 Umsatzeinbusse auf 3 Monate:	20 Mio. CHF
Anzahl Pandemie-Tote infolge	
• mangelndem Personal 30 Tote à 4 Mio	1200 Mio.
• Ansteckung stationärer Pat. 30 Tote	1200 Mio.
• Fehlende Medikamente 30 Tote	1200 Mio.
Ungenügende Kapazitäten für Notfälle 20 Tote	800 Mio.
Totaler Schaden:	4420 Mio.
Jährl. Schadenerwartungswert:100 Jh.	44.2 Mio.
Grenzaufwand für Massnahmenkosten mit 1/3	15 Mio./Jahr

Mögliche Massnahmen:
Sind in Tabelle 4 exemplarisch aufgeführt. Dabei wird vereinfachend angenommen, dass die einzelnen Massnahmen unabhängig voneinander sind. Wie sich bei der Konstruktion des Polygonzuges zeigt, liegt einzig die Massnahme „Unterdruck-Räume“ in diesem Beispiel rechts vom Berührungspunkt der -45°Geraden an das Polygon und ist demzufolge nicht mehr kostenwirksam.

Konstruktion des Polygons zur Beurteilung der Massnahmen

Unter der Annahme, dass sämtliche der getroffenen Massnahmen voneinander unabhängig sind, sind sie in Tabelle 4 entsprechend ihrer abnehmenden Kostenwirksamkeit aufgelistet. In Abbildung 9 sind diese Massnahmen in ihrer Rangfolge der Kostenwirksamkeit übernommen, wobei jede Massnahme entsprechen ihrer Risikoreduktion an die vorangehende Massnahme angekoppelt wird.

Tabelle 4: Zusammenstellung der Gefährdungsarten und der möglichen Massnahmen

	Gefährdung	Jährl. Schadenerwartungswert R (CHF)	Massnahmenart	Laufzeit der Massnahme (Jh)	Risikoreduktion (CHF)	Jährl. Massnahmenkosten K (CHF)	Kosten-Wirksamkeit (R/K)	Rangfolge
Massnahmen	IT-Ausfall	400‘000	Ringleitung	25	300‘000	50‘000	6	1
			Separate Räumlichkeit	25	75‘000	50‘000	1.25	6
	Erdbeben	1‘000‘000	Gebäudeverstärkung	50	800‘000	300‘000	2.7	3
			Verstärkung Einrichtungen	25	50‘000	25‘000	2.0	5
	Pandemie	44‘200‘000	Information	jährlich	5‘000‘000	1‘000‘000	5	2
			Impfung	jährlich	20‘‘000‘000	8‘000‘000	2.5	4
			Unterdruckräume	50	5‘000‘000	6‘000‘000	0.85	7
	Total	**45‘600‘000**			**31‘225‘000**	**15‘425‘000**		

In Abbildung 9 sind die einzelnen Massnahmen aufgeführt und die mit Neigung -1 (unter -45°) rot eingezeichnete Grenzkosten-Gerade an das Polygon herangeführt. Die Reihenfolge der Massnahmen geht aus Tabelle 4 hervor. Es wird deutlich, dass die Massnahme „Unterdruckräume“ nicht mehr kostenwirksam

wird. In diesem exemplarischen Fall können somit bis zum Berührungspunkt mit rund 9 Mio. für jährliche Massnahmenkosten rund 26 Mio. an jährlichem Schadenerwartungswert reduziert werden, d.h. die Kostenwirksamkeit liegt insgesamt bei etwa 1:3.

Wendet man die Faustformel für das Optimum des gesamten Massnahmen-Paketes an, müssten für rund 45 Mio Schadenerwartungswert rund 15 Mio. an Massnahmen aufgewendet werden. Es könnte also durchaus sein, dass eine Evaluation weiterer Massnahmen dazu führen könnte, dass sich weitere kostenwirksame Massnahmen ergeben, sich die Rangfolge verändert resp. weitere Massnahmen dazukommen und das Polygon einen Verlauf zeigt, der dazu führt, dass die rote Gerade tiefer und nach rechts verschoben gelegt werden muss. Der Berührungspunkt wäre damit auch tiefer und mehr nach rechts verschoben.

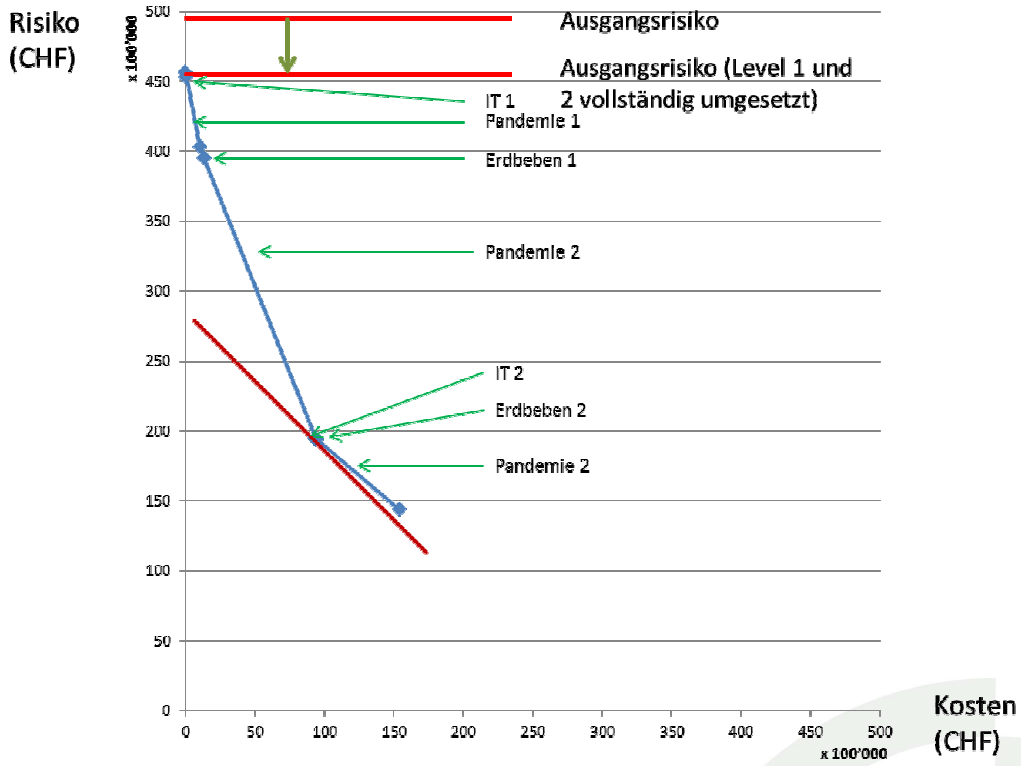


Abbildung 9: Verlauf der Massnahmen-Kurve für das fiktive Beispiel

A2 Individuelles Todesfallrisiko

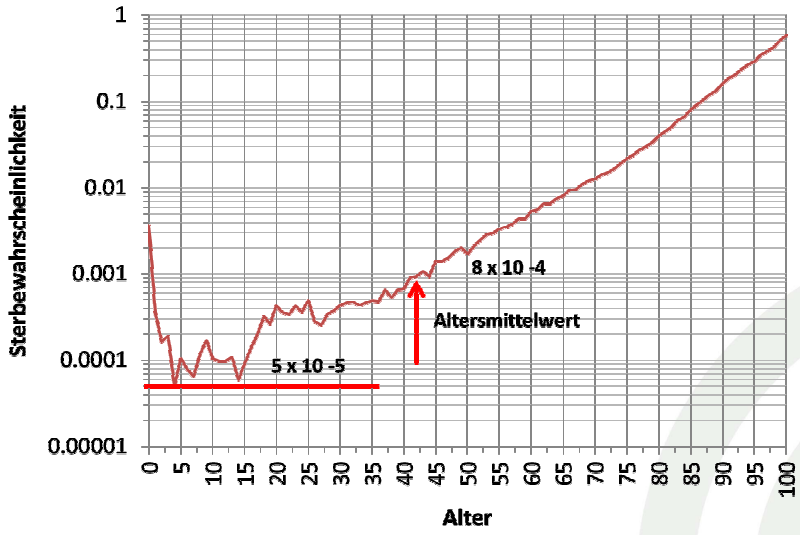
Individuelles Todesfallrisiko

Bereits in Kapitel 4 sind einige Ausführungen zum individuellen Risiko gemacht worden. Im Folgenden werden noch einige quantitative Angaben und Überlegungen ausgeführt.

Das Schutzziel-Modell der PLANAT[32] schlägt als Grenzwert für die Wahrscheinlichkeit, mit der ein Mensch in einem bestimmten Objekt oder an einem bestimmten Ort zu Tode kommt 10-5/Jahr vor. Es handelt sich um einen Erwartungswert über die Dauer eines Jahres. Dieser Erwartungswert gilt für den – wie ihn die PLANAT nennt – institutionellen Verantwortungsbereich. Die PLANAT unterscheidet weitere Verantwortungsbereiche (professionell, individuell) und bezeichnet damit den unterschiedlichen Grad an Freiwilligkeit, mit dem ein Individuum ein Risiko eingeht.

In einer früheren Publikation definiert die PLANAT für freiwillig eingegangene Risiken einen maximalen Wert für die Todesfallwahrscheinlichkeit pro Jahr von 10-2 bis 10-3 (Kategorie 1), und dann für drei weitere Risikokategorien mit abnehmendem Grad an Freiwilligkeit: 10-3 bis 2*10-4 (Kategorie 2), 2*10-4 bis 3*10-5 (Kategorie 3) und 3*10-3 bis 4*10-6 (Kategorie 4), (PLANAT 2008: 30).

Wie aus Abbildung 10 hervorgeht, liegt der von der PLANAT vorgeschlagene Grenzwert mit 10-5 deutlich unter der totalen Sterbewahrscheinlichkeit, insbesondere wenn man den Altersmittelwert in der Schweiz von rund 42 Jahren beachtet, der bei 8x10-4 liegt. Bei den Jugendlichen liegt die Sterbewahrscheinlichkeit deutlich tiefer (rund eine Zehnerpotenz).



Quelle: BfS

Abbildung 100: Totale Sterbewahrscheinlichkeit der Schweizer Bevölkerung 2011 (BfS 2011).

[32] PLANAT (2009a): *Strategie Naturgefahren Schweiz.* Umsetzung des Aktionsplans PLANAT 2005-2008/2009-2011, Projekt B 2.2 Schutzziel-Modell. Nationale Plattform Naturgefahren PLANAT, Schlussbericht Phase 2, 29. Mai 2009, Bern.

Abbildung 11 macht – neben einigen beachtlichen Unterschieden zur Sterbewahrscheinlichkeit von Mann und Frau – insbesondere deutlich, dass die Sterbewahrscheinlichkeit in den Generationen der letzten hundert Jahre um rund eine Zehnerpotenz gesunken ist. Diese Grenzwerte sind demnach „dynamische“ Grenzwerte und müssen gegebenenfalls periodisch den neuen Begebenheiten angepasst werden.

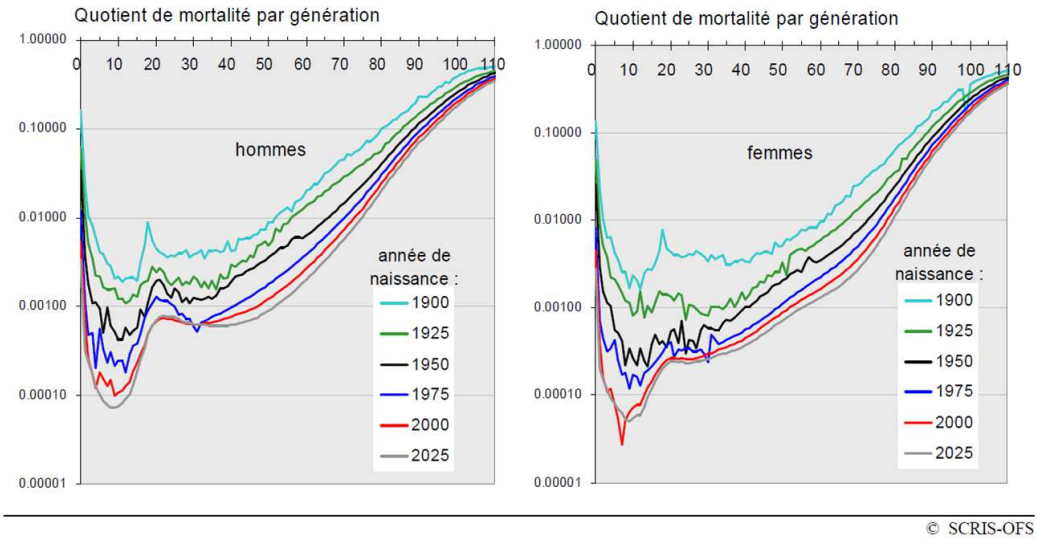


Abbildung 111: Sterbewahrscheinlichkeit der verschiedenen Generationen, getrennt nach Frauen und Männern (Quelle: Statistique Vaud SCRIS: Jacques Menthonnex 2009; BfS)