SSI-SPEZIAL

Sonderausgabe zum Thema «Sicherheitsplanung» 1/06

Sicherheits-planung

Methodik der Risikoanalyse,

Vorgehensschritte und Begriffsbestimmung

Inhaltsverzeichnis

Anhang

SSI – Schweizerische Vereinigung unabhängiger Sicherheitsingenieure und -berater

VORWORT

Liebe Leserin, lieber Leser

Die vorliegende Sonderausgabe des SSI-Bulletins stellt die erste Publikation einer geplanten Reihe dar. Diese Publikationen haben im Sinne einer neuen Dienstleistung der SSI zum Ziel, unseren Partnern in der Wirtschaft, Politik und Verwaltung vertiefte Hintergrundsinformationen zu fachlich oder politisch aktuellen Themen zu bieten. Sie stellen das Ergebnis einer engagierten Zusammenarbeit unserer SSI-Mitgliedsfirmen dar. Diese erste Ausgabe befasst sich mit der Thematik der «Sicherheitsplanung». Begriffe wie Sicherheit, Risikomanagement, Restrisiko und Kostenwirksamkeitsanalyse werden sowohl in Fachkreisen als auch in der Öffentlichkeit mit grosser Selbstverständlichkeit verwendet. Aber sprechen wir wirklich alle vom Gleichen? Und welche Methoden stehen uns in der Sicherheitsplanung zur Auswahl? Die vorliegende Publikation gibt einen Überblick, ohne dabei den Anspruch zu erheben, abschliessend zu sein. Gerne hoffen wir, dass diese Sonderausgabe als Argumentations- und Entscheidungshilfe, Erinnerungsstütze oder einfach als Denkanstoss von Nutzen sein wird.

Der SSI-Vorstand

IMPRESSUM

Herausgeber:

SSI, Schweizerische Vereinigung unabhängiger Sicherheits-ingenieure und -berater
Güstrasse 46
8700 Küsnacht
Telefon 044 910 73 06
Telefax 044 910 73 96
Internet: www.ssi-ch.info
E-Mail: ssi@mediasec.ch

Autoren:

Peter Christen, Dipl. Ing. ETH, Leiter Sicherheit von Bauten und Anlagen bei Ernst Basler+Partner AG, Sicherheitsberater SSI, langjährige Beratungstätigkeit in Fragen Risiko und Sicherheit.

Annemarie Dorenbos Theler, Dr. sc. techn. ETH, Dipl. Kulturingenieurin, Projekt-leiterin Neosys AG Gerlafingen, Sicherheits-beraterin SSI, Schwerpunkte: Gefahrstoff-management, Störfall- und Risikoanalysen, Sicherheitskonzepte.

Achim Ernst, Dipl. Chemieing. TU, dipl. Wirtschaftsing. FH, Projektleiter der Bereiche Gebäudesicherheit, Arbeitssicherheit und Gesundheitsschutz bei der Gruner AG, Basel.

Rolf Walther, Dipl. El.-Ing. HTL/NDS, Geschäftsführer Amstein + Walthert Sicherheit AG, SSI-Sicherheits-Berater/- Planer, Tätigkeitsschwerpunkte seit 1985: Entwick-lung und Umsetzung von Sicherheits-konzepten (Safety, Security) für Verwaltungen, Gefängnisse, Rechenzentren, Industrie etc.

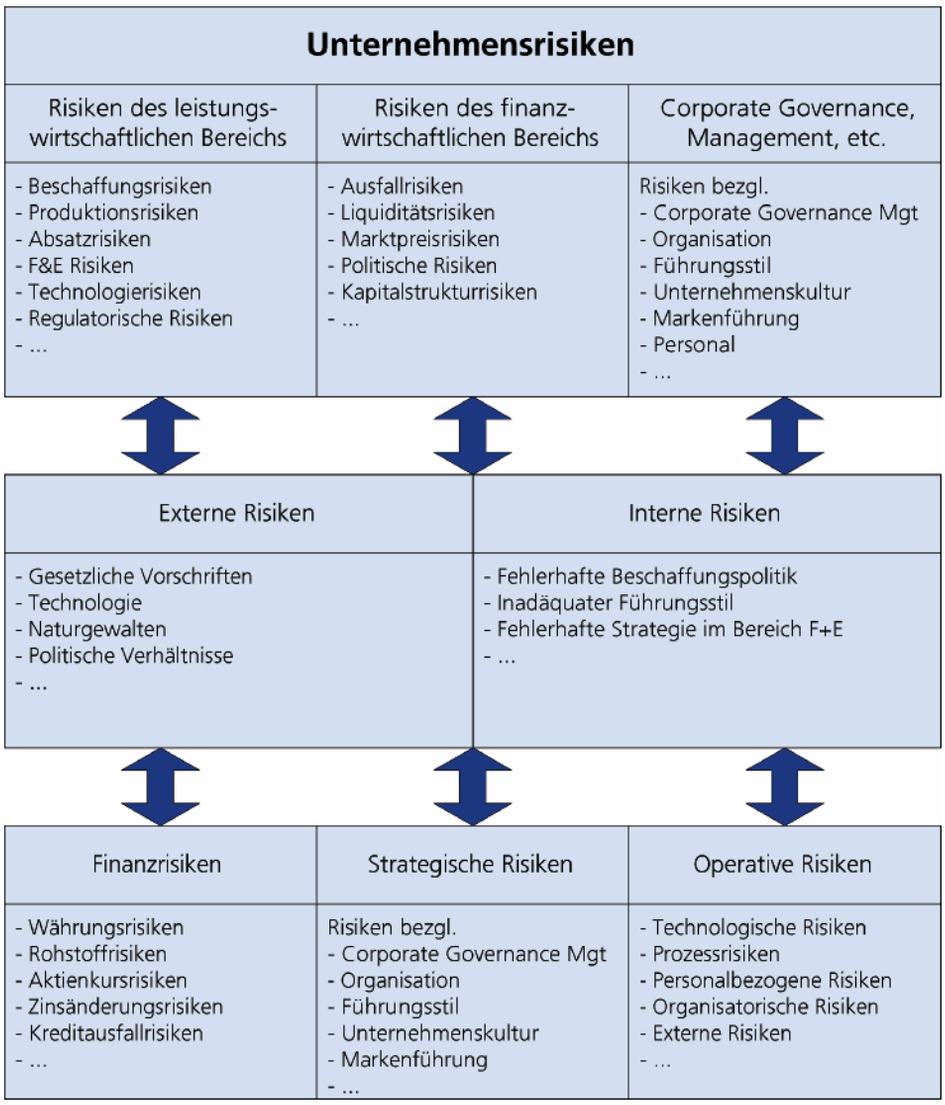

Abbildung 1: Kategorisierung der Unternehmensrisiken in Analogie zu ROMEIKE 2004.

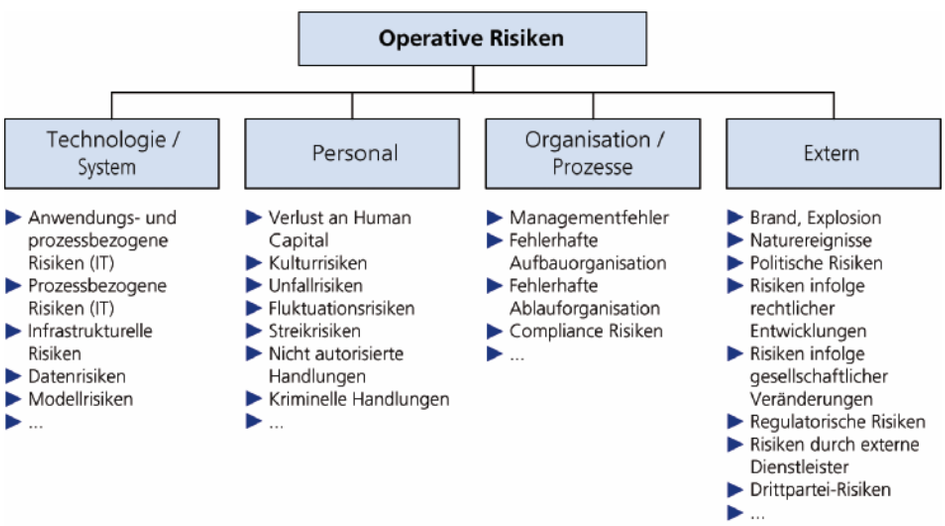

Abbildung 2: Operative Risiken (ROMEIKE UND FINKE 2003).

Unternehmer müssen Chancen und Risiken in ihrer Unternehmenssteuerung berücksichtigen, um sich am Markt behaupten zu können und ihren Unternehmenswert zu steigern. Das Erkennen und Steuern des eigenen Chancen-Risiken-Profils wird durch ein Risikomanagement unterstützt. Ein Risikomanagement erlaubt nicht nur das Erkennen bestehender Risiken, sondern auch das frühzeitige Erkennen und – im besten Fall – das Vermeiden kritischer Zustände.

Die Abbildung 1 zeigt drei mögliche Kategorisierungen der Unternehmensrisiken (in Analogie zu ROMEIKE 2004). Risiken können durch externe wie auch durch interne Ereignisse verursacht werden. So kann zum Beispiel ein Beschaffungsrisiko durch ein externes Ereignis wie Überschwemmungen und die daraus resultierende Ressourcenknappheit, aber auch durch ein internes Ereignis wie Engpässe im internen Beschaffungsprozess verursacht werden.

Im technischen Bereich stehen oft die Bewertung der operativen Risiken im Brennpunkt, da sich hier insbesondere die Wertungsfragen der Risiken (Grösse des Schadensausmasses und/oder der Eintretenswahrscheinlichkeit) stellt: «Welches Risiko ist für ein Unternehmen oder die Gesellschaft noch tragbar?»

Die so genannten operativen Risiken können wie in Abbildung 2 dargestellt, untergliedert werden.

Eine wichtige Aufgabe der Sicherheitsingenieure und -berater der SSI liegt in der Betreuung ihrer Kunden beim Risikomanagement. Je nach Situation und Kundenbedürfnis erfolgen die einzelnen Schritte des Risikomanagements jeweils in mehr oder weniger engen Zusammenarbeit mit dem betreffenden Kunden. Die Gliederung des Risikomanagementprozesses wird nachfolgend umschrieben.

RISIKOMANAGEMENTPROZESS

Die in der Praxis verwendeten Vorgehensweisen und Abläufe lehnen sich in der Regel an die aus der Theorie bekannten theoretischen Abläufe (z.B. CCPS 1989, CCPS 1992, HARDAKER et al. 1997, ROMEIKE 2004) einer Risikoanalyse an. Nicht nur in der Theorie, aber vor allem auch in der Praxis, zeigt sich das Risikomanagement immer wieder als kontinuierlicher Anpassungsprozess und nicht als Einzelaktivität. Für den Kunden bedeutet dies somit, dass die Schritte des Risikomanagements in allen relevanten betrieblichen Entscheidungsfindungsprozessen integriert werden sollten.

Die Abbildung 3 zeigt eine gute allgemeine Darstellung des Risikomanagementprozesses (Quellen: AS/NZS 4360:1999, sowie HARDAKER et al. 1997):

Nachfolgend werden die einzelnen Schritte des Risikomanagementprozesses erläutert. Die Identifikation, Analyse und Bewertung der Risiken bilden dabei die zentralen und zugleich anspruchvollsten Schritte im gesamten Risikomanagement, da auch zukünftige Risiken mit den entsprechenden Unschärfen berücksichtigt werden müssen. Es ist es jedoch wichtig, zu beachten, dass es je nach Situation und Kundenwunsch nicht notwendig ist, immer alle Schritte durchzuführen.

1. Kontext bestimmen

- Strategischen Kontext des Unternehmens bestimmen (Stärken, Schwächen, Chancen, Gefahren)
- Organisatorischen Kontext des Unternehmens und Verantwortlichkeiten für das Risikomanagement festlegen
- Risikopolitik festlegen: Sicherheitsziele festhalten, Kriterien zur Risikobewertung inkl. Akzeptanzgrenzen festlegen
- Relevante Gesetzesbestimmungen beschaffen (legal compliance)
- Sich über Schadenfälle in der betreffenden Branche informieren
- Daten und Dokumente über den betreffenden Produktionsprozess sammeln

2. Risiken identifizieren

- Mögliche Beeinträchtigungen der Unternehmenstätigkeit, des Prozesses und/oder des Umfeldes ermitteln
- Mögliche Ursachen für eine Beeinträchtigung der Unternehmenstätigkeit, des Prozesses und/oder des Umfeldes ermitteln
- Mögliche Auswirkungen der Unternehmenstätigkeit auf das Umfeld bestimmen
- Sowohl Normalbetrieb als auch Störfall berücksichtigen

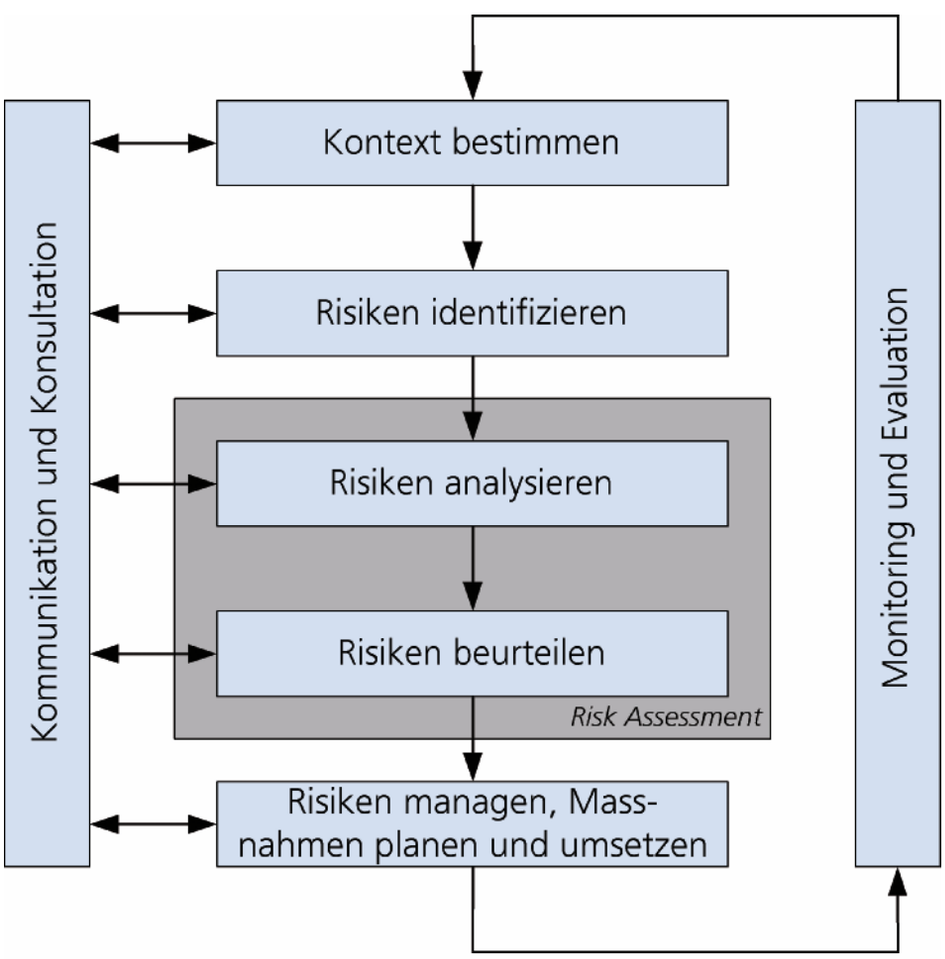

Abbildung 3: Risikomanagement Prozess.

Die Schritte 3 und 4 werden zusammen oft mit dem Begriff «Risk Assessment» umschrieben:

3. Risiken analysieren

- Ursachen-Konsequenzen-Ketten aufzeigen
- Eintretenswahrscheinlichkeiten der erkannten Ursachen einschätzen
- Konsequenzen für Unternehmen und Umfeld/Umwelt ermitteln
- Risiko darstellen

4. Risiken bewerten

- Basierend auf der Risikopolitik (Sicherheitsziele, Risikobewertungskriterien, Akzeptanzgrenzen) Handlungsbedarf aufzeigen
- Risiken priorisieren

5. Risiken managen, Massnahmen planen und umsetzen

- Handlungsalternativen aufzeigen, priorisieren und vergleichen: In der Abbildung 4 sind die verschiedenen Handlungsalternativen dargestellt.
- Zugehörige Massnahmen evaluieren und selektieren, zum Beispiel
  - Voraussetzungen schaffen, dass Mitarbeiter risikogerecht handeln können
  - Technische und bauliche Massnahmen treffen
  - Notfallplanung für Ereignisfälle vorbereiten (inkl. Risikokommunikation)
  - Bestehende finanzielle Lösungen (z.B. Versicherung) überprüfen

6. Monitoring und Evaluation einführen

- Frühwarnsystem installieren und Massnahmen überwachen;
- Schadenereignisse und beinahe eingetretene Ereignisse sowie Ursachen und Auswirkungen festhalten;
- Erkenntnisse periodisch auswerten (IST/Soll-Vergleich);
- Erkenntnisse den betroffenen Personen/Stellen im Betrieb weiterleiten;
- Überprüfen, ob das Risikomanagement richtig funktioniert.

7. Kommunikation und Konsultation sicherstellen

- Sensibilisierung des Personals für Gefährdungen von Personen, Sachen, des Vermögens/Gewinns oder der Umwelt;
- Regelmässig über die Ergebnisse der einzelnen Schritte sowie über das Risikomanagement als Ganzes kommunizieren und mit internen und externen Stakeholders den Kontext prüfen (siehe Schritt 1).

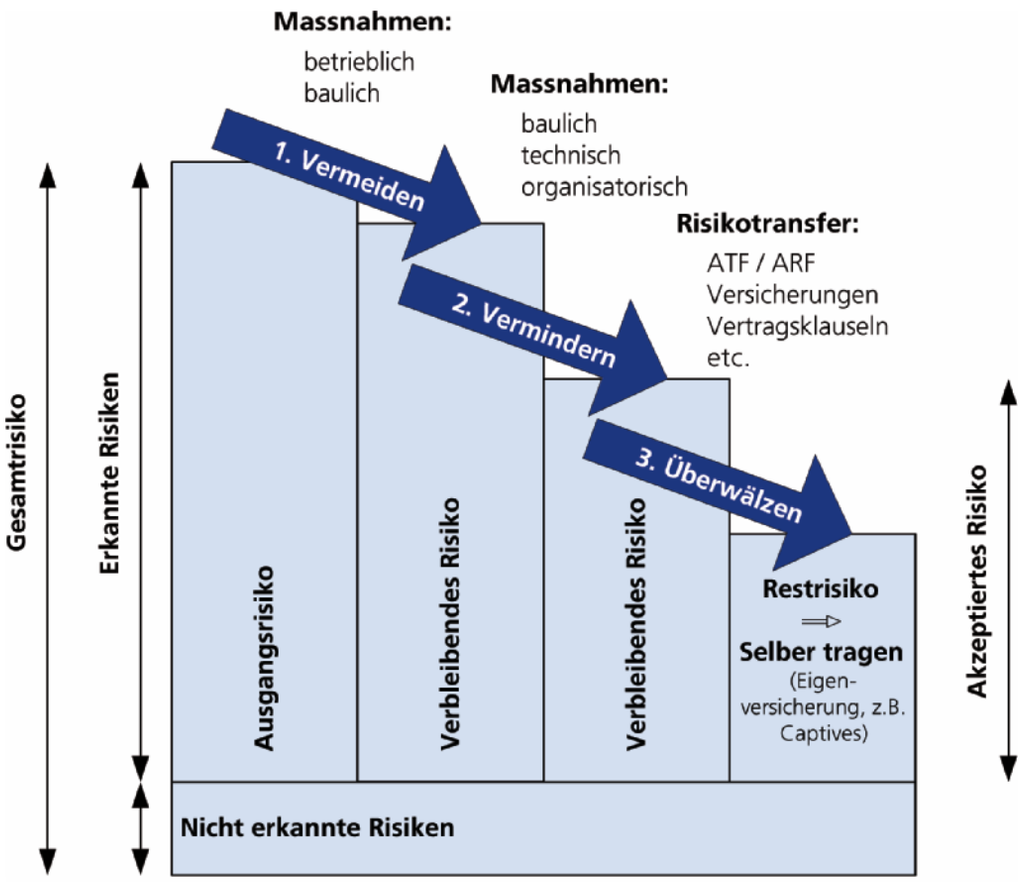

Abbildung 4: Risikopolitische Handlungsalternativen (ROMEIKE 2004).

3.1 Problem- und Situationsanalyse (Kontext bestimmen)

Eine systematische Problem- und Situationsanalyse erhöht die Chance, eine tragfähige Lösung zu finden. Das Systems Engineering stellt eine der erfolgsversprechenden Basismethoden für die systematische Problem- und Situationsanalyse dar (HABERFELLNER et al. 1997). Speziell hervorzuheben ist dabei die Wichtigkeit der Zielsuche im Rahmen des Problemlösungszyklus (siehe Abbildung 5).

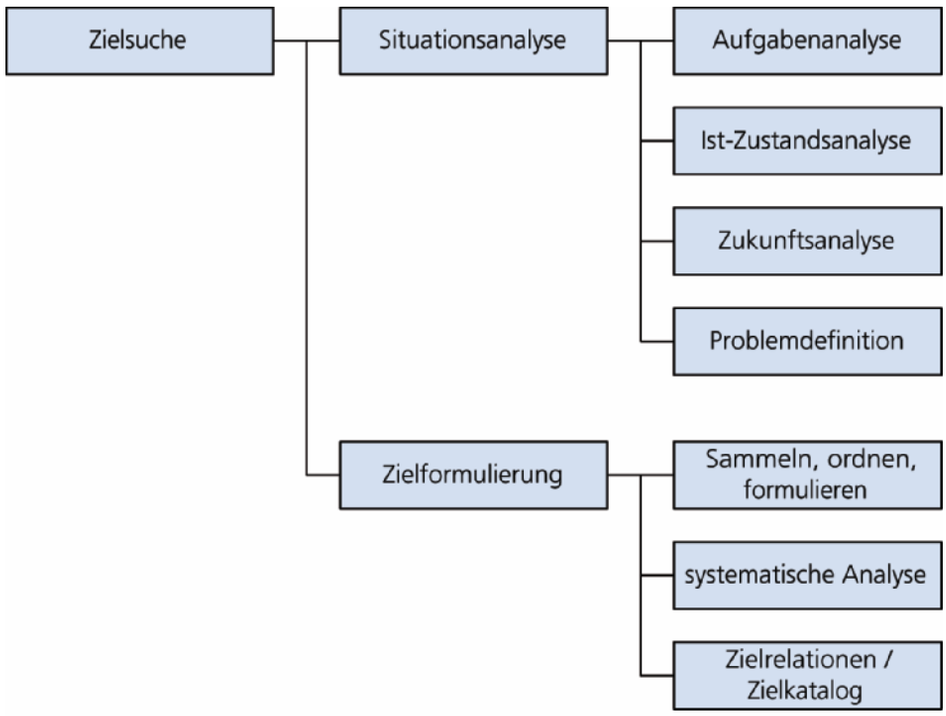

Abbildung 5: Zielsuche aus dem Problemlösungszyklus nach Systems Engineering

3.2 Gefährdungs- und Risikoanalyse (Risiken identifizieren und analysieren)

Eine bewährte und häufig angewendete Methode der Gefährdungsanalyse stellt der empirische Ansatz der Szenarienanalyse dar. Grundsätzlich sind unendlich viele Möglichkeiten denkbar, wie ein System/Objekt einen Schaden erleiden kann. Bei der Szenarienanalyse geht es darum, eine Strukturierung der Gefährdung zu erreichen, beispielsweise passive Gefährdungen versus aktive Gefährdungen oder von Menschen verursachte Ereignisse versus Naturereignisse. Diese Strukturierung erlaubt, die massgebenden Ereignisse schnell und möglichst vollständig zu erfassen. Bei der Szenarienanalyse handelt es sich um eine kreative Technik, der keine strengen Regeln zu Grunde gelegt sind. Das Resultat der Szenarienanalyse ist ein so genannter Szenarienbaum (Abbildung 6).

Dieser Schritt der systematischen Ermittlung der massgebenden Gefährdungen ist nicht zuletzt für die Systemabgrenzung wichtig. Aus dem Szenarienbaum lässt sich leicht erkennen, welche Bereiche untersucht werden sollen. Ebenso kann die Bearbeitungstiefe durch die Anzahl der Verfeinerungsschritte (Verästelungen im Szenarienbaum) dem Problem angepasst werden.

Im Allgemein besteht eine Risikoanalyse aus folgenden drei Schritten:

- **Ereignisanalyse (Prozess- und Gefährdungsanalyse):**

  Sie befasst sich mit der Entstehung und der Entwicklung von unerwünschten Ereignissen. Das Resultat der Ereignisanalyse umfasst im Minimum einen Szenarienbeschrieb und eine Abschätzung der Grundhäufigkeit des Ereigniseintritts.

- **Wirkungsanalyse:**

  Sie befasst sich mit den chemischen, physikalischen, physiologischen, psychologischen oder ggf. anderen Wirkungen eines Ereignisszenarios. Das Resultat der Wir-

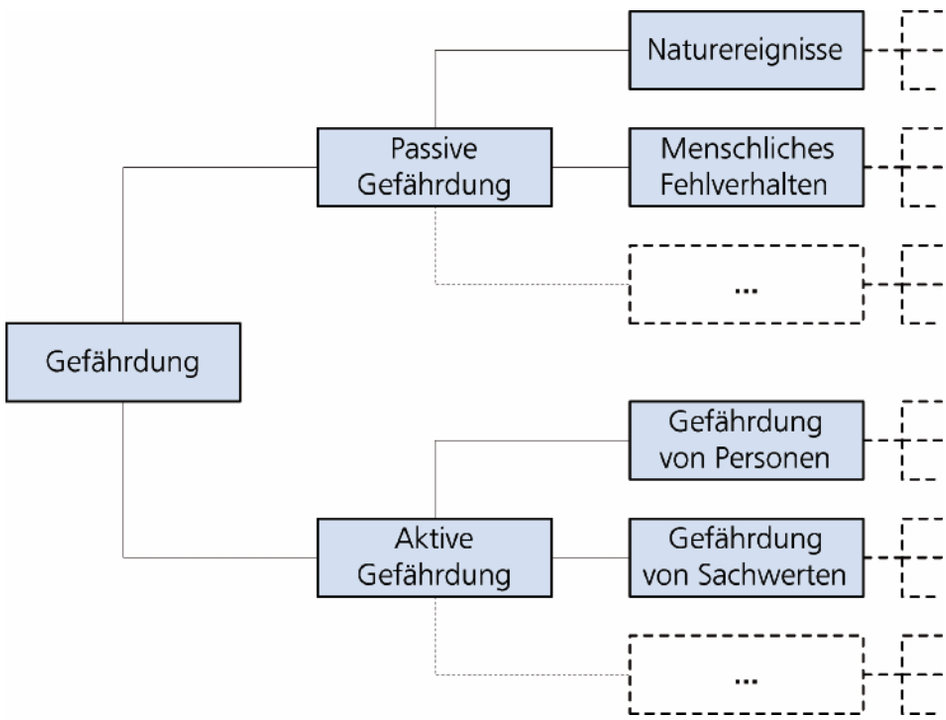

Abbildung 6: Skizze eines Szenarienbaums

kungsanalyse umfasst gefährdungsspezifische Wirkungsreichweiten, beispielsweise Letalitätszonen.

- **Expositionsanalyse:**

  Sie befasst sich mit der Lage, Dauer und Anzahl oder Ausdehnung von gefährdeten Schutzobjekten wie Personen, Objekte oder Umweltelemente im Bereich der möglichen Wirkungsreichweiten. Das Resultat der Expositionsanalyse umfasst neben den Inputgrössen für die Ausmassberechnungen auch bedingte Wahrscheinlichkeiten (z.B. Aufenthaltsdauer von gefährdeten Personen) für die Präzisierung der Grundhäufigkeit der Ereignisszenarien.

Für die massgebenden Ereignisszenarien werden als Resultat der Ereignis-, Wirkungs- und Expositionsanalyse die Häufigkeiten bzw. Wahrscheinlichkeiten der massgebenden Szenarien sowie das Schadenausmass hinsichtlich der massgebenden Schadenindikatoren ermittelt oder abgeschätzt. Die Resultate können in einer Risikodatentabelle zusammengefasst werden (siehe Tabelle 1). In dieser Tabelle werden in der Senkrechten alle identifizierten massgebenden Szenarien, und in der Waagrechten für jedes Szenario der zutreffende Häufigkeitswert sowie die Schätzungen zum zutreffenden Schadenausmass (Einheiten: Anzahl, Flächen- oder Volumenmass oder Franken) eingetragen.

- anhand von analytischen Methoden (z.B. Fehler und Ereignisbäume) sowie
- aufgrund von Schätzungen durch Fachleute.

Bei der Abschätzung der Häufigkeiten oder Wahrscheinlichkeiten der Szenarien sind alle verfügbaren Informationen in geeigneter Weise einzubeziehen. Wenn beispielsweise für ein konkretes Objekt keine direkten Angaben vorliegen, so kann es zweckmässig sein, unter Berücksichtigung objektspezifischer Faktoren Rückschlüsse aus Angaben anderer Objekte oder vergleichbarer Organisationen zu ziehen. Andererseits kann es zweckmässig sein, von objektspezifischen Schätzungen eine Hochrechnung auf alle vergleichbaren Objekte der Schweiz zu machen, um die Schätzung zu verifizieren.

Für alle definierten massgebenden Szenarien wird das mutmassliche Schadenausmass bei den festgelegten Schadenindikatoren ermittelt oder geschätzt. Dies lässt sich ebenfalls auf drei Arten vornehmen:

- aufgrund der statistischen Auswertung von konkreten Ereignissen im betrachteten oder vergleichbaren System,
- anhand von analytischen Methoden (z.B. Schadensimulationsmodelle),
- aufgrund von Schätzungen von Fachleuten.

Szenario	Häufigkeit (pro Jahr)	Schadenausmass (Schadenindikatoren)			
		Todesopfer	Verletzte	Sachschaden	.....
SZ 01	H_{SZ01}	$N1_{SZ01}$	$N2_{SZ01}$	$N3_{SZ01}$	.....
SZ 02	H_{SZ02}	$N1_{SZ02}$	$N2_{SZ02}$	$N3_{SZ02}$	.....
SZ 03	H_{SZ03}	$N1_{SZ03}$	$N2_{SZ03}$	$N3_{SZ03}$	.....
.....	.....	.....	.....	.....	.....

Tabelle 1: Risikodatentabelle

Das kollektive Risiko, oftmals auch als jährlicher Schadenerwartungswert bezeichnet, stellt eine erste Vergleichsgrösse dar. Es kann für alle definierten Szenarien angegeben werden. Das kollektive Risiko R_i eines Szenarios i ergibt sich aus dem Produkt der Häufigkeit H_i eines Ereignisses und dem dazugehörigen Schadenausmass A_i.

Häufigkeiten oder Wahrscheinlichkeiten von Ereignisszenarien lassen sich grundsätzlich auf drei Arten ermitteln oder abschätzen:

- aufgrund statistischer Daten (inkl. incident reporting),

3.3 Risikobewertung (Risiken beurteilen)

3.3.1 Einleitung

Die kollektiven Risiken der massgebenden Szenarien sind bei einer Darstellung in der oben erwähnten Risikodatentabelle nicht oder nur schwer miteinander vergleichbar. Erst wenn festgelegt ist, wie sich die verschiedenen Schadenindikatoren untereinander vergleichen – also beispielsweise wie der Schaden infolge eines Funktionsausfalls von 30% während 10 Stunden im Vergleich zu einem Sachschaden von 2 Mio. Franken oder zu einer verletzten Person zu bewerten ist – wird die unterschiedliche Bedeutung der verschiedenen Szenerien ersichtlich. Deshalb ist es notwendig, die verschiedenen Schadenindikatoren auf eine gemeinsame Schadenzahl umzurechnen. Dies kann mit den zwei Elementen «Monetarisieren anhand der Zahlungsbereitschaft» und «Gewichten mit Aversionsfaktoren» erreicht werden. Selbstverständlich gibt es weitere Bewertungsmethoden wie beispielsweise Utility Function oder Life-Cost-Index.

3.3.2 Monetarisierung anhand der Zahlungsbereitschaft

Um die verschiedenen Schadenindikatoren vergleichbar zu machen, werden sie monetarisiert, d.h. mit der Zahlungsbereitschaft in Geldeinheiten umgerechnet. Die Zahlungsbereitschaft muss spezifisch für alle Schadenindikatoren festgelegt werden. Die Zahlungsbereitschaft gibt an, wie viel Geld eine Gesellschaft oder Organisation bereit ist auszugeben, um das Risiko um eine bestimmte Einheit zu verringern. Die Festlegung der Höhe der Zahlungsbereitschaft stellt eine Bewertung dar, die – unter gebührender Berücksichtigung des Umfelds – in jedem Einzelfall und in enger Zusammenarbeit mit dem betreffenden Unternehmen explizit vorgenommen werden muss. Es gibt in diesem Sinne keinen objektiv richtigen Wert für die Zahlungsbereitschaft. Allerdings muss man sich bewusst sein, dass die Festlegung der Zahlungsbereitschaft indirekt die Risikoakzeptanz steuert: je höher die Zahlungsbereitschaft festgelegt werden, desto höher werden die Risiken bewertet und desto dringlicher werden Sicherheitsmassnahmen.

Die Zahlungsbereitschaft variiert – in Anlehnung an zahlreiche Untersuchungen – mit der Wahrnehmung von Risiken und deren entgegengebrachten Risikoakzeptanz. Je höher die Risikoakzeptanz ist, desto geringer ist die Zahlungsbereitschaft zur Verhinderung eines Schadens. Folgende Kriterien liegen der Festlegung der Höhe der Zahlungsbereitschaft zugrunde:

- **Selbstbestimmung / Fremdbestimmung**

  Je höher der Grad der Selbstbestimmung, desto mehr kann eine gefährdete Person das Risiko durch ihr eigenes Verhalten beeinflussen und desto höher fällt die Risikoakzeptanz aus. Das Verhältnis von Selbstbestimmung und Fremdbestimmung ist abhängig von der Kenntnis, der Vermeidbarkeit und der Beeinflussbarkeit des Risikos.

- **Nutzenempfindung**

  Je höher der unmittelbare Nutzen, desto höher ist die Risikoakzeptanz. Die Nutzenempfindung ist dort am unmittelbarsten, wo der Mensch Tätigkeiten zur persönlichen Befriedigung betreibt (z.B. Freizeitaktivitäten) bzw. dort am geringsten, wo es um Aktivitäten der Gesellschaft geht, deren Bedeutung man sich immer wieder verstandesmässig bewusst machen muss.

3.3.2 Gewichten mit Risikoaversionsfaktoren für grosse Schäden

Hohe und katastrophale Schadenausmasse werden in der Regel von der Gesellschaft unverhältnismässig gross und stark wahrgenommen und empfunden. In der Literatur wird dabei von einem risikoaversen Verhalten gegenüber Grossereignissen gesprochen. Um diesem Umstand Rechnung zu tragen, wird bei der Risikoberechnung formal ein so genannter *Aversionsfaktor für Grossschäden* eingeführt, der mit einer *Risiko-Aversionsfunktion* definiert wird. Diese Risiko-Aversionsfunktion «vergrössert» das Risiko in Abhängigkeit von der Grösse des Schadenausmasses.

Die Einführung von Risikoaversionsfaktoren, insbesondere für Grossschäden, hat sich im Bereich der technischen Risiken mittlerweile etabliert. Es gibt eine grosse Zahl von Beispielen für solche Risikoaversionsfunktionen, beispielsweise im Zusammenhang mit der schweizerischen Störfallverordnung. Die Festlegung der Grösse dieser Risikoaversionsfaktoren stellt ebenfalls eine Bewertung dar, die – unter gebührender Berücksichtigung des Umfelds – explizit vorgenommen werden muss. Es gibt in diesem Sinne keinen objektiv richtigen Wert für Risikoaversionsfaktoren. Allerdings muss man sich auch hier bewusst sein, dass die Festlegung von Risikoaversionsfaktoren indirekt die Risikoakzeptanz steuert: je höher die Risikoversionsfaktoren festgelegt werden, desto höher werden die Risiken bewertet und desto dringlicher werden Sicherheitsmassnahmen.

Folgende Elemente sollen durch Risikoaversionsfaktoren berücksichtigt werden:

- **Signalwirkung:** Katastrophale Ereignisse finden unverhältnismässig hohe Beachtung und führen oft zu unverhältnismässig heftigen Reaktionen der Gesellschaft (z.B. bezüglich Forderungen nach Massnahmen, Vorwürfe an die Verantwortlichen etc.).
- **Existenzielle Bedrohung:** Katastrophale Ereignisse sind oft kritisch für das betroffene System. So ist beispielsweise bekannt, dass rund 50% aller Firmen, die in den USA von einem Grossbrand heimgesucht wurden, innerhalb von zwei Jahren vom Markt verschwanden.
- **Überforderung bei der Ereignisbewältigung von Katastrophen:** Zur Behebung der Schäden infolge katastrophaler Ereignisse ist immer ein unverhältnismässig grosser Aufwand erforderlich: Zum einen sind es grosse Schäden, zum andern treten sie oft örtlich und zeitlich konzentriert auf. Dies bringt meist eine temporäre Überforderung aller Hilfsorganisationen mit sich.
- **Hohe Verantwortlichkeit:** Grossereignisse betreffen meist Risiken, die im Verantwortungsbereich von Institutionen liegen. Diesbezüglich wird von diesen also eine besonders hohe Sorgfaltspflicht erwartet. Die Reaktion der Öffentlichkeit gegenüber den Verantwortlichen ist beim Eintreten solcher Ereignisse entsprechend heftig.
- **Unsicherheit hinsichtlich der Eintretenswahrscheinlichkeit:** Katastrophen sind naturgemäss sehr selten, womit die Beurteilung ihrer Eintretenswahrscheinlichkeit mit erheblicher Unsicherheit verbunden ist. Wenn solche Ereignisse eintreten, wirft dies fast immer die Frage auf, ob die Wahrscheinlichkeiten richtig eingeschätzt wurden.
- **Unsicherheit hinsichtlich der Auswirkungen:** Grosse Unsicherheiten sind auch mit der Abschätzung der Auswirkungen solcher Ereignisse verbunden, insbesondere was indirekte und langfristige Schäden anbelangt. Oft zeigt sich das wahre Ausmass der Katastrophe erst allmählich, womit die Diskussion um solche Ereignisse lange anhält.

3.3.4 Vergleiche und Darstellung der Risiken

Die monetarisierten Ausmasswerte werden in die Risikodatentabelle (siehe Tabelle 1) eingetragen, womit einerseits die Ausmasse der verschiedenen Schadenindikatoren eines bestimmten Szenarios miteinander vergleichbar gemacht und zu einem totalen Risiko des Ereignisszenarios addiert werden können. Andererseits können auch die Risiken der verschiedenen Szenarien untereinander verglichen und zu einem Gesamtrisiko der untersuchten Bereiche eines Objektes addiert werden.

Sie lassen sich auf verschiedene Weise darstellen, beispielsweise:

- in Form von grafischen Darstellungen (Kuchendiagramme, Balkendiagramme), welche die Verteilung des totalen Risikos auf die Ereignisszenarien oder auf die Schadenindikatoren zeigen.
- in Form von (komplementär kumulativen) Wahrscheinlichkeits-Ausmass-Diagrammen, wie sie insbesondere im Bereich der technischen Risiken verwendet werden, beispielsweise im Rahmen der Störfallverordnung. Diese Darstellungsmöglichkeit erlaubt einen Vergleich mit Risiken von anderen Systemen, z.B. Vergleich der Risiken eines Zugreisenden mit den Risiken eines Fluggastes.

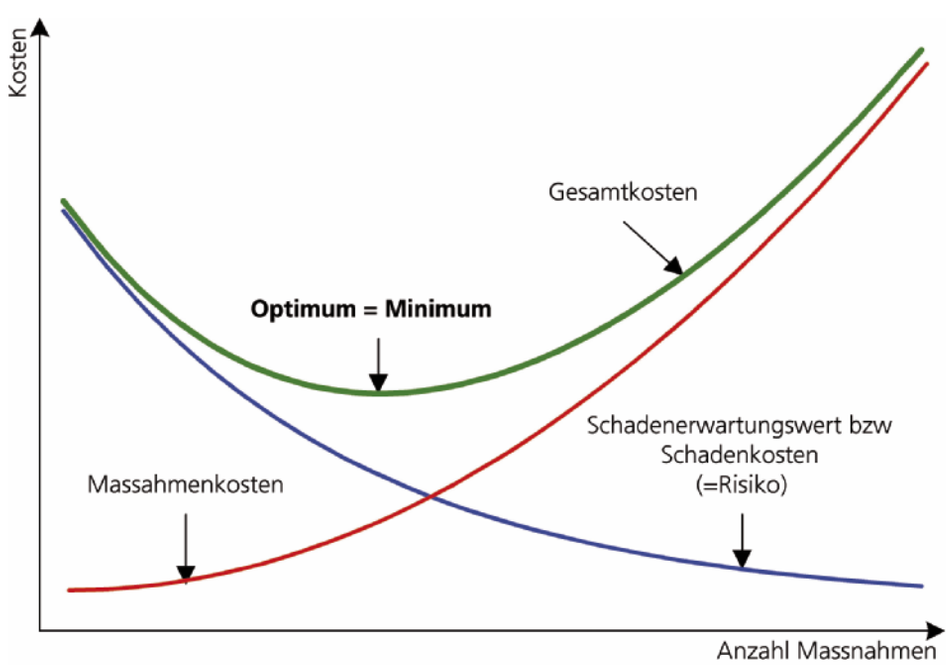

Abbildung 7: Prinzip der Kostenwirksamkeit.

- in Form einer Häufigkeits-Schadenausmass-Matrix, in der die verschiedenen Szenarien in Funktion von Häufigkeitskategorien und Schadenkategorien eingetragen werden. Diese Darstellung wird manchmal verwendet, um entsprechende Schutzziele zu definieren.
- in Form von normierten Risikozahlen, beispielsweise Risiko pro Handlungsausführung oder Risiko pro Besucher. Mit geeignet normierten Zahlen lassen sich auch verschiedene Objekte unterschiedlicher Grösse und Ausprägung im Hinblick auf bestimmte Risikoeigenschaften miteinander vergleichen.

3.4 Massnahmenplanung (Risiken managen, Massnahmen planen und umsetzen)

3.4.1 Bedeutung der monetären Risikogrösse

Die monetäre Risikogrösse, die in Franken pro Jahr ausgedrückt wird, stellt eine zentrale Grösse für die mittel- und langfristige Investitionsplanung für risikosenkende Massnahmen dar. Die Frage, ob eine Massnahme geeignet ist, kann aufgrund der Gegenüberstellung der ermittelten Risikoreduktion in monetären Einheiten mit den jährlichen Kosten (Annuitäten) im Kostenwirksamkeitsverhältnis beantwortet werden.

Bei der Beurteilung von Massnahmen ist zunächst zu unterscheiden zwischen Massnahmen, die rechtlich vorgeschrieben sind (z.B. in verbindlichen Vorschriften) und Massnahmen, die primär aus eigenen Interessen z.B. des Betreibers ins Auge gefasst werden.

3.4.2 Beurteilung von Massnahmen aufgrund rechtlich definierter Schutzziele

Wenn Massnahmen aufgrund von rechtlich definierten Schutzzielen zu treffen sind, dann besteht in der Regel kein Handlungsspielraum seitens der Objektverantwortlichen. In solchen Fällen ist jedoch immer zu beachten, dass es oft mehrere Möglichkeiten geben kann, um ein rechtlich definiertes Schutzziel zu erreichen. In solchen Fällen sind jene Massnahmen zu treffen, welche die geringsten Gesamtkosten (Investition, Betrieb, Unterhalt) erzeugen.

3.4.3 Beurteilung von Massnahmen aufgrund der Kostenwirksamkeit

Wenn aufgrund der eingeschätzten Risiken zusätzliche Sicherheitsmassnahmen angebracht scheinen oder wenn die Sicherheitsmassnahmen als unverhältnismässig empfunden werden, so kann das Kostenwirksamkeitsverhältnis als Entscheidungsgrundlage wie folgt ermittelt werden:

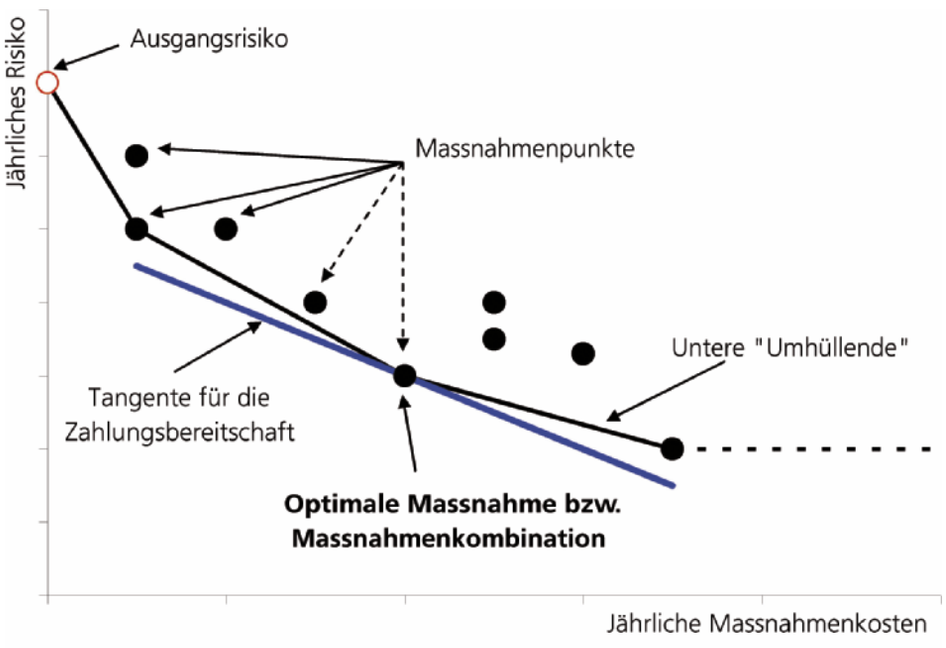

Abbildung 8: Risiko-Kosten-Diagramm.

- **Wo?**
  Bei welchen Gefährdungen und welchen Schadenindikatoren wirkt diese Massnahme? Konkret heisst das, dass in der Risikodatentabelle (siehe Tabelle 1) die durch diese Massnahme betroffenen Felder zu markieren sind.
- **Wie?**
  Wie wirkt diese Massnahme in den bezeichneten Feldern, d.h. wie stark wird der ursprüngliche Schadenausmasswert reduziert? Konkret heisst das, dass in der Risikomatrix die entsprechenden Werte in den markierten Feldern zu ändern sind.
- **Was kostet die Massnahme?**
  Welches sind die jährlichen Kosten der Massnahme? Dabei sind die Investitionskosten, die Betriebs- und Unterhaltskosten, die Lebensdauer sowie die Diskontierung zu berücksichtigen.

3.4.4 Bedeutung der Kostenwirksamkeitsbeurteilung

Mit den veränderten Schadenausmasswerten kann nun die durch die Massnahme erzeugte bzw. prognostizierte Veränderung des Gesamtrisikos ermittelt werden. Diese Risikoreduktion, die in Franken pro Jahr ausgedrückt ist, kann direkt mit den jährlichen Kosten der Massnahme verglichen werden. Sind diese kleiner als die monetarisierte jährliche Risikoreduktion kann die Massnahme als kostenwirksam bezeichnet werden. Übertreffen diese Kosten jedoch die monetarisierte jährliche Risikoreduktion, dann kann eine Massnahme nicht als kostenwirksam bezeichnet werden. Da sowohl das Risiko als auch die Massnahmenkosten auf eine einheitlichen, monetäre Basis gebracht wurden (z.B. Franken pro Jahr) geht es beim Prinzip der Kostenwirksamkeit darum, die Gesamtkosten aus Risiken und Massnahmen zu minimieren. Vereinfacht ausgedrückt ist das Optimum an Sicherheit dann erreicht, wenn die Gesamtkosten minimal sind (siehe Abbildung 7).

3.4.5 Darstellung der Massnahmen im Risiko-Kosten-Diagramm

Eine gebräuchliche Darstellung der Resultate der risikobasierten Massnahmenplanung stellt das Risiko-Kosten-Diagramm dar (siehe Abbildung 8). In diesem Diagramm werden sämtliche, nach Kosten und Risikominderung untersuchten Massnahmen bzw. Massnahmenkombinationen als Punkte dargestellt. Die untere «Umhüllende» stellt den Pfad der wirksamsten Massnahmen dar. Die −45°-Tangentenpunkt, wenn die Risiken bereits mit Hilfe der Zahlungsbereitschaft monetarisiert wurden, stellt den im Sinne der Abbildung 7 optimalen Punkt dar, an welchem die Gesamtkosten minimal werden.

Mit diesem abschliessenden Schritt des Risikomanagementprozesses liegen dem Kunde i.d.R. genügend Entscheidungsgrundlagen im Hinblick auf das weitere Vorgehen und eventuell auf die Einführung eines betriebseigenen Risikomanagements vor.

BEGRIFFSBESTIMMUNGEN

Präambel

Über die Richtigkeit und Präzision von Begriffsbestimmungen liesse sich lange diskutieren. Wichtig ist jedoch, dass eine Begriffsdefinition erfolgt, damit eine gemeinsame Basis geschaffen wird. Die nachfolgenden Begriffsdefinitionen sollen helfen, eine gemeinsame Sprache zu finden. Sie erheben keinen Anspruch auf Vollständigkeit und wissenschaftliche Genauigkeit.

Gefahr

- Latente negative Umwelteigenschaft
- «Was kann passieren»?
- einer Gefahr ist man «passiv» unterlegen
- Gefahr ist eine Sachlage, bei der das Risiko grösser als das Grenzrisiko ist. VDE 31000/ VDE1987
- Gefahr:
  - Als Gefahr wird die Möglichkeit bezeichnet, durch ein Ereignis einen Schaden zu erleiden. Der Zeitpunkt des Eintritts, die Art und das Ausmass des Schadens sind nicht bekannt.
  - Gefahr steht für eine unbestimmte und nicht orientierte (also nicht gezielt auf Menschen und/oder Sachen gerichtete) Gefährdung.
  - Gefahr ist ein Zustand, Umstand oder Vorgang, aus dem ein Schaden entstehen kann.
- Aktive Gefahr (Security):
  Gefahr, die durch beabsichtigte, gezielte Handlungen herbeigeführt wird.
- Passive Gefahr (Safety):
  Gefahr, die durch menschliches oder technisches Versagen oder durch Naturereignisse hervorgerufen wird.

Gefährdung

- potentielle Schadensquelle [ISO/IEC Guide 51:1990]
- Gefährdung (Bedrohung):
  Als Gefährdung wird eine auf eine bestimmte Situation, ein bestimmtes Objekt oder eine bestimmte Person bezogene Gefahr bezeichnet.

Gefährdungssituation

- Zustand, in dem Menschen, Güter oder die Umwelt einer oder mehreren Gefährdungen ausgesetzt sind [ISO/IEC Guide 51:1999, Definition 3.6].

Gefährlicher Vorfall

- Gefährdungssituation, die zu einem Schaden führt.

Risiko

- Erwartete Schadenshöhe durch ein Ereignis x Eintrittwahrscheinlichkeit des Ereignisses.
- Ein Risiko geht man «aktiv» ein.
- Das Risiko ist ein Mass für die Grösse einer Gefährdung. Es ist eine nach Häufigkeit und Auswirkungen erfasste Gefährdung und wird in der Regel in Franken pro Jahr gemessen. Es stellt im mathematischen Sinn einen Schadenerwartungswert dar.

Grenzrisiko

- Das grösste noch vertretbare Risiko eines bestimmten technischen Vorganges oder Zustandes. Im Allgemeinen lässt sich das Grenzrisiko nicht quantitativ erfassen.

Tolerierbares Risiko

- Risiko, das basierend auf den aktuellen gesellschaftlichen Wertvorstellungen in einem gegebenen Zusammenhang tragbar ist.

Restrisiko

- Risiko, das nach der Anwendung von Schutzmassnahmen verbleibt [ISO/IEC Guide 51:1999, Definition 3.9].
- Als Restrisiko wird das Risiko bezeichnet, das nach der Realisierung aller vorgesehener Sicherheitsmassnahmen noch verbleibt. Es setzt sich zusammen aus.
  - Risiken, die bewusst akzeptiert wurden,
  - Risiken aus objektiv unbekannten und subjektiv unerkannten Gefährdungen,
  - Risiken aus fahrlässig oder vorsätzlich vernachlässigten Gefährdungen,
  - Risiken aus ungeeigneten bzw. fehlerhaften angewendeten Sicherheitsmassnahmen.

Risikoanalyse

- Systematische Auswertung verfügbarer Informationen, um Gefährdungen zu identifizieren und RISIKEN abzuschätzen [ISO/IEC Guide 51:1999, Definition 3.10].
- Bei der Risikoanalyse werden die Risiken der Ereignisszenarien mit geeigneten Methoden ermittelt bzw. berechnet. Die Risikoanalyse stellt einen weitgehend objektiven Vorgang dar.
- Einsatz von verfügbaren Informationen mit dem Ziel, gefährliche Vorfälle vorgängig zu erkennen und das Risiko einzuschätzen.

Risikobewertung

- Beurteilung auf der Grundlage einer RISIKOANALYSE, ob auf der Basis der von der Gesellschaft anerkannten Werte ein vertretbares RISIKO in einem gegebenen Zusammenhang erreicht worden ist (ANMERKUNG Auf der Grundlage von ISO/IEC Guide 51:1999, Definition 3.11 und 3.7).
- Bei der Risikobewertung werden die ermittelten Risiken mittels Risikokriterien vergleichbar gemacht und/oder gewichtet, um die empfundene Grösse der Gefährdung zu bestimmen. Die Risikobewertung stellt einen subjektiven Vorgang dar.
- Verfahren, bei dem auf der Grundlage der Risikoanalyse und unter Berücksichtigung von Faktoren wie soziale, wirtschaftliche und Umweltaspekten darüber entschieden wird, ob ein Risiko tragbar ist.
- Die Risikobewertung ist die Beurteilung der Risiken auf der Basis der Risikoanalyse. Sie bezeichnet sowohl den Vergleich mit einem definierten Wertesystem als auch den Entscheid über die Tragbarkeit der Risiken.

Risikobewusstsein

- Mass der Sensibilisierung für die Gefährdung von Personen, Sachen, Umwelt oder Vermögen.

Risikokommunikation

- Kommunikationsprozess, der der Informationsvermittlung und dem Informationsaustausch zwischen Personen, Gruppen und Institutionen über die Beschaffenheit, Bewertung und Bewältigung von Risiken für Mensch und Umwelt dient.

Risikokontrolle

- Prozess, durch den Entscheidungen herbeigeführt und Sicherheitsmassnahmen implementiert werden, um Risiken zu reduzieren oder um sie in festgelegten Grenzen zu halten.

Risikomanagement

- Systematische Anwendung von Managementgrundsätzen, Verfahren und Praktiken auf die Analyse, Bewertung und Kontrolle von Risiken.

Risikowahrnehmung (dreistufig)

1. Risikoperzeption (das unmittelbare, intuitive Erkennen von Risiko)
2. Risikoevaluation (normative Bewertung, wie bedeutsam das Risiko für Mensch/Umwelt ist)
3. Risikoakzeptanz (willentliche oder bewusste Zustimmung zum Risiko)

Schaden

- Physische Verletzung oder Schädigung der Gesundheit von Menschen, entweder direkt oder indirekt als ein Ergebnis von Schäden von Gütern oder der Umwelt [ISO/IEC Guide 51:1990 (modifiziert)].
- Schaden ist ein Nachteil durch Verletzung von Rechtsgütern auf Grund eines bestimmten technischen Vorganges oder Zustandes. (VDE 31000 /VDE1987).
- Physische Verletzung und/oder Beeinträchtigung der Gesundheit von Personen, Zerstörung oder Beschädigung von Sachen, Verhinderung oder Einschränkung der Funktionstüchtigkeit von technischen Systemen, Beeinträchtigung von Ökosystemen.

Schutz

- Als Schutz bezeichnet man Massnahmen, welche die zu schützende Sache oder Person vor der Wirkung einer Gefährdung bewahren.
- Als Schutz bezeichnet man das Abhalten der Wirkung einer Gefährdung von der zu schützenden Sache oder Person.

Schutzziel

- Ziel, das erreicht werden muss, damit die nötige Sicherheit gewährleistet ist. Sicherheit liegt vor, wenn
  - das Risiko vertretbar gering ist,
  - unvertretbare Risiken fehlen.

Sicherheit (Safety)

- Freiheit von unvertretbaren Risiken (Anmerkung uv: entspricht auch ISO/IEC Guide 51:1999, Definition 3.1).
- Sicherheit ist eine Sachlage, bei der das Risiko nicht grösser als das Grenzrisiko ist. VDE 31000 /VDE1987

Sicherheitsmassnahme

- Massnahme zur Beseitigung einer Gefährdung oder zur Verminderung eines Risikos.

Szenario (Ereignisszenario):

- Ein Szenario ist ein Ablauf von Handlungen oder Ereignissen, die an bestimmte Bedingungen gebunden sind.

Umweltrisiko

- Risiko einer Umweltbeeinträchtigung verursacht durch menschliches Handeln.
- Als Umweltbeeinträchtigung gilt die dauerhafte Störung des natürlichen Zustands von Luft, Gewässern (auch Grundwasser), Boden, Flora oder Fauna durch Immissionen, sofern als Folge dieser Störung schädliche oder sonstige Einwirkungen auf die menschliche Gesundheit, auf Sachwerte oder auf Ökosysteme entstehen können oder entstanden sind. Ebenfalls als Umweltbeeinträchtigung gilt ein Sachverhalt, der vom Gesetzgeber als «Umweltschaden» bezeichnet wird (Zürich Versicherungs-Gesellschaft 1999, Art. 26a; Winterthur Versicherungen 1991, Art. 6a).

LITERATURVERZEICHNIS

AS/NZS 4360 (1999): *Risk Management*, herausgegeben von der Standards Association of Australia, Strathfield, ISBN 0 7337 2647 X

CCPS, Center for chemical process safety (1989): *Guidelines for Quantitative Risk Analysis*, American Institute of Chemical Engineers, New York, ISBN 0-8169-0402-2

CCPS, Center for chemical process safety (1992): *Guidelines for Hazard Evaluation Procedures, Second edition with worked examples*, American Institute of Chemical Engineers, New York, ISBN 0-8169-0491-X

DIN VDE 31000-2 (1987): *Allgemeine Leitsätze für das sicherheitsgerechte Gestalten technischer Erzeugnisse, Begriffe der Sicherheitstechnik; Grundbegriffe.* VDE Verlag

EFD (2000): *Weisungen über den Schutz ziviler Immobilien vom 19. Juni 2000.* Eidgenössisches Finanzdepartement (EFD), Bern

HABERFELLNER, R. et al. (1997): *Systems Engineering. Methodik und Praxis.* 9. Auflage, Orell Füssli Verlag, Zürich, ISBN 3 85743 986 6

HARDAKER, J.B., R.B.M. HUIRNE und J.R. ANDERSON (1997): *Coping with Risk in Agriculture. Reprinted with corrections 1998*, CAB International, Wallingford, UK

ISO/IEC Guide 51 (1999): *Safety aspects – Guidelines for their inclusion in standards.* herausgegeben von der International Organization for Standardization (ISO), Genf

ISO/IEC Guide 73 (2002): *Risk management – Vocabulary – Guidelines for use in standards.* herausgegeben von der International Organization for Standardization (ISO), Genf

MERZ, H. et al. (1995): *Bewertung von technischen Risiken. Beiträge zur Strukturierung und zum Stand der Kenntnisse. Modelle zur Bewertung von Todesfallrisiken.* In: Kröger, W. (Hrsg.): Interdisziplinäres Forschungsprojekt «Risiko und Sicherheit technischer Systeme», Verlag der Fachvereine der ETH Zürich, Zürich, ISBN 3 7281 2178 9

ROMEIKE, F. und FINKE, R.B. (2003): *Erfolgsfaktor Risiko-Management.* 1. Auflage, Betriebswirtschaftlicher Verlag Dr. Th. Gabler GmbH, Wiesbaden, ISBN 3-409-12200-1

ROMEIKE, F. (2004): *Lexikon Risiko-Management.* 1. Auflage, Bank-Verlag GmbH, Köln, ISBN 3-527-50112-6

SCHNEIDER, J. et al. (1994): *Sicherheit und Zuverlässigkeit im Bauwesen. Grundwissen für Ingenieure.* Verlag der Fachvereine der ETH Zürich, Zürich, ISBN 3 7281 2037 5

SSI Schweizerische Vereinigung unabhängiger Sicherheitsingenieure und -berater
Association suisse des ingénieurs et conseillers en sécurité indépendants
Swiss association of independent safety and security consultants and engineers

Gefahren hat es immer gegeben – Lösungen auch!

In der SSI sind die kompetenten Problemlöser vereinigt

Amstein + Walthert Sicherheit AG
Mönchmattweg 5
CH-5036 Oberentfelden
Tel. +41 (0) 62 723 05 10
Fax +41 (0) 62 723 00 63
infoaa@amstein-walthert.ch
www.amstein-walthert.ch

Basler & Hofmann Ingenieure und Planer AG
Forchstrasse 395
CH-8032 Zürich
Tel. +41 (0) 44 387 11 22
Fax +41 (0) 44 387 11 00
basler-hofmann@bhz.ch
www.bhz.ch

Ernst Basler + Partner AG
Zollikerstrasse 65
CH-8702 Zollikon
Tel. +41 (0) 44 395 11 11
Fax +41 (0) 44 395 12 34
info@ebp.ch
www.ebp.ch

BDS Security Design AG
Muristrasse 96
CH-3006 Bern
Tel. +41 (0) 31 350 86 80
Fax +41 (0) 31 350 86 86
bds@bds-bern.ch
www.sicherheitsberatung.ch

BDS Safety Management AG
Segelhof, Postfach
CH-5405 Baden-Dättwil
Tel. +41 (0) 56 486 71 71
Fax +41 (0) 56 486 73 73
bds@bds-baden.ch
www.arbeitssicherheit.ch

BG Ingénieurs-conseils S.A.
BG Ingenieure + Berater AG
Avenue de Cour 61
CH-1007 Lausanne
Tel. +41 (0) 21 618 11 11
Fax +41 (0) 21 618 11 22
lausanne@bg-21.com
www.bg-21.com

Electrowatt Infra AG
Hardturmstrasse 161, Postfach
CH-8037 Zürich
Tel. +41 (0) 44 355 55 55
Fax +41 (0) 44 355 55 56
infra@ewi.ch
www.ewi.ch

Emch + Berger AG
Falkensteinstrasse 27
CH-9006 St. Gallen
Tel. +41 (0) 71 244 56 22
Fax +41 (0) 71 244 56 34
info@emchberger-sg.ch
www.emchberger.ch

Gruner AG
Gellertstrasse 55, Postfach
CH-4020 Basel
Tel. +41 (0) 61 317 61 61
Fax +41 (0) 61 312 40 09
mail@gruner.ch
www.gruner.ch

Ingenieurbureau Heierli AG
Culmannstrasse 56, Postfach
CH-8033 Zürich 6
Tel. +41 (0) 44 360 31 11
Fax +41 (0) 44 360 31 00
inbox@heierli.ch
www.heierli.ch

Neosys AG
RisCare
Privatstrasse 10
CH-4563 Gerlafingen
Tel. +41 (0) 32 674 45 11
Fax +41 (0) 32 674 45 00
info@neosys-ag.ch
www.neosys-ag.ch

RM Risk Management AG
Security & Risk Consultants
Blümlisalpstrasse 56
CH-8006 Zürich
Tel. +41 (0) 44 360 40 40
Fax +41 (0) 44 360 40 00
rm@rmrisk.ch
www.rmrisk.ch

Sicherheitsinstitut
Nüschelerstrasse 45
CH-8001 Zürich
Tel. +41 (0) 44 217 43 33
Fax +41 (0) 44 211 70 30
safety@swissi.ch
www.swissi.ch

SKS Ingenieure AG
Mitglied der suisseplan-Gruppe
Oerlikonerstrasse 88
CH-8057 Zürich
Tel. +41 (0) 44 315 17 17
Fax +41 (0) 44 315 17 18
mail@sks.ch
www.sks.ch

SRB Assekuranz Broker AG
Rautistrasse 11, Postfach
CH-8040 Zürich
Tel. +41 (0) 44 497 87 87
Fax +41 (0) 44 497 87 88
matjaz.ros@srb-group.com
www.srb-group.com

www.ssi-ch.info