Zeitschrift: Schweizer Ingenieur und Architekt
Herausgeber: Verlags-AG der akademischen technischen Vereine
Band: 111 (1993)
Heft: 47

Artikel: Risikoanalyse technischer Systeme: Methoden, Modelle, Verfahren und Hilfsmittel
Autor: Giampiero, E.G. / Kröger, Wolfgang
DOI: https://doi.org/10.5169/seals-78285

Sicherheit und Risiko

Risikoanalyse technischer Systeme

Methoden, Modelle, Verfahren und Hilfsmittel

In den letzten zwei Jahrzehnten wurden für die Analyse des Risikos technischer Systeme (chemische Anlagen, Transportsysteme, Systeme zur Erzeugung elektrischer Energie u.a.) verschiedenste Anleitungen, Handbücher und Computersysteme entwickelt. Diese beziehen sich zum einen auf die umfassende Risikoabschätzung, zum anderen aber auch auf deren Teilaspekte wie Ereignis-, Ausbreitungs- und Expositionsanalyse. Gemeinsam ist ihnen aber, dass sie alle auf bestimmten methodischen Ansätzen – in den nachfolgenden Ausführungen «Methoden» genannt – sowie Modellen beruhen.

VON GIAMPIERO E. G. BEROGGI, DELFT (NL), UND WOLFGANG KRÖGER, ZÜRICH

Generelles Verfahren der Risikoanalyse

Das generelle Verfahren der Analyse technischer Risiken ist ziemlich uneingeschränkt akzeptiert und wird je nach Problemstellung mit unterschiedlichem Detaillierungsgrad durchgeführt. Es handelt sich dabei um einen aktiven und dynamischen Prozess, der vom Risikoanalytiker viel Engagement und Initiative verlangt.

Wegen der Vielfalt der vorhandenen Systeme kann kein universell gültiges, starres Ablaufschema entworfen werden. Es ist die Verantwortung und Herausforderung des Sicherheitsfachmannes, innerhalb der vorgeschriebenen Schranken eine aussagekräftige, sauber dokumentierte und für andere nachvollziehbare Risikoanalyse durchzuführen. Das Vorgehen bei einer umfassenden Risikoanalyse kann grundsätzlich in die Schritte gemäss Bild 1 gegliedert werden. Zur praktischen Durchführung der Risikoanalyse nach diesem Verfahren werden Modelle (z.B. Fehlerbäume), Methoden (z.B. Probabilistik), Verfahren (z.B. Handbücher) und Hilfsmittel (z.B. Computersysteme) eingesetzt.

Methoden und Modelle zur Risikobestimmung

Wie die Schritte der Risikoanalyse bereits andeuten, setzt sich das Risiko aus mehreren Teilereignissen zusammen, die sich gegenseitig beeinflussen. Diese Ereigniskette oder dieses Ereignisnetzwerk wird in einem Risikomodell dargestellt. Ein vereinfachtes Risikomodell ist in Bild 2 in Form eines Influenzdiagramms illustriert.

Die Analyse der ovalen Ereignisse entspricht den Teilschritten einer Risikoanalyse, mit den Ereignissen in abgerundeten Rechtecken als deren Einflussgrössen. Das Resultat eines Teilschritts ist jeweils mit Ungewissheiten behaftet, die ebenfalls einen Einfluss auf das Resultat des nächsten Teilschritts haben. Der letzte Teilschritt besteht dann in der Bestimmung des möglichen Schadens, der zusammen mit der entsprechenden Ungewissheit (Wahrscheinlichkeit) das Risiko ergibt. Die in Bild 3 angegebenen Grössenordnungen dieser Ungewissheiten im Risikomodell sind bei einer Risikoanalyse stets zu beachten [11].

Nicht nur die Wahrscheinlichkeit eines bestimmten Störfalls setzt sich aus vielen Teilwahrscheinlichkeiten zusammen. Der Schaden besteht aus mehreren Schadensarten (z.B. Anzahl Tote und Verletzte, Fläche verseuchten Bodens), die verknüpft den totalen Schaden ausmachen. Um diese Verknüpfung von qualitativen oder quantitativen Grössen zur Bestimmung des totalen Risikos bewerkstelligen zu können, müssen Prinzipien vorgegeben werden, nach denen sich die Teilungewissheiten und die verschiedenen Schadensarten verbinden lassen. Im folgenden werden kurz die wichtigsten Methoden der Verknüpfung von quantitativen und qualitativen Grössen in der Risikoanalyse vorgestellt.

Methoden zur Verknüpfung von qualitativen Grössen

Wenn Grössen rein qualitativ beschrieben werden, dann benützt man verbale Ausdrücke, wie «klein», «mittel» und «gross». Mit diesen Ausdrücken können sowohl Ungewissheiten (Häufigkeiten) wie auch Schadensausmasse beschrieben werden. Verbale Risiken werden oft in einer Ausmass-Häufigkeits-Tabelle dagestellt.

Die Methode zur Verknüpfung von verbalen Ausdrücken kann mittels Regeln erstellt und in wissensbasierte Systeme abgespeichert werden. Die Verknüpfung von Regeln erfolgt oft gemäss der Prädikatenlogik, wobei auch andere etablierte und neue Methoden immer

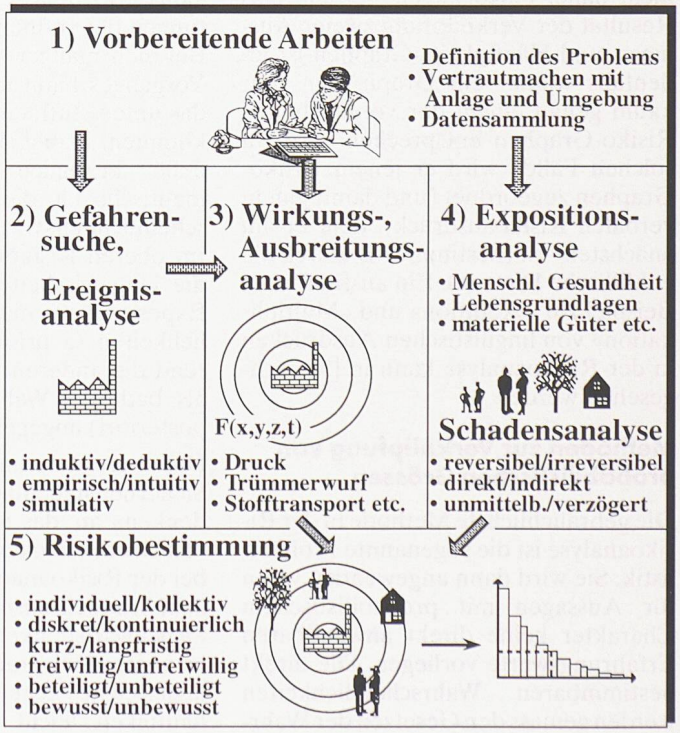

Bild 1. Generelles Vorgehen bei einer umfassenden Risikoanalyse

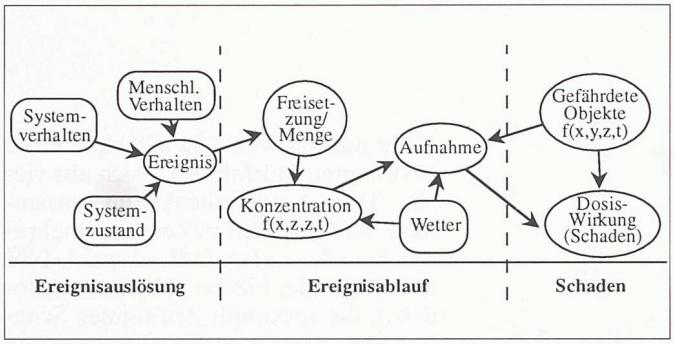

Bild 2. Vereinfachtes Risikomodell in Form eines Influenzdiagramms

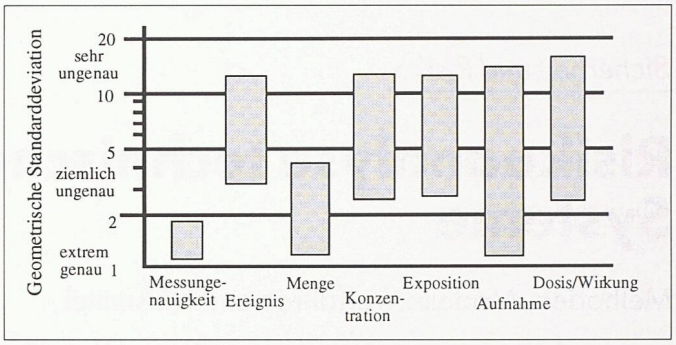

Bild 3. Grössenordnungen der Ungewissheiten im Risikomodell

mehr gebraucht werden. Die bekanntesten Hilfsmittel, die sich auf diese Methoden abstützen, sind die HazOp und FMEA, die im nächsten Abschnitt kurz besprochen werden.

Eine andere Art, um qualitative oder verbale Grössen zu verknüpfen, ist die Fuzzy-Logik. Während in einer Tabelle die Trennung von z.B. «kleinem» und «mittlerem» Schadensausmass scharf ist, handelt es sich bei der Fuzzy-Methodik um einen schleichenden Übergang (vgl. Bild 4). So können z.B. 15 km² verschmutzter Boden einem «mittleren» Schaden mit Zugehörigkeitswert 0.6 und gleichzeitig einem «kleinen» Schaden mit Zugehörigkeitswert 0.4 entsprechen.

Hier interessiert nun, wie sich einer der verschiedenen verbalen Schadensausdrücke mit einem der verbalen Häufigkeitsausdrücke zu einem Risikoausdruck verknüpfen lässt (z.B. «multipliziert»), wobei die Risikoausdrücke auch durch einen entsprechenden Graphen definiert sind. Auf die Einzelheiten einer solchen Verknüpfung soll hier nicht näher eingegangen werden. Das Resultat der Verknüpfung zweier Ausmass- und Häufigkeits-Graphen ist jedenfalls wieder ein Graph, der aber kaum genau einem der vorgegebenen Risiko-Graphen entsprechen wird. In solchen Fällen wird er jenem Risiko-Graphen zugeordnet (und damit jenem verbalen Risikoausdruck), dem er am «nächsten» ist (bestimmt z.B. durch die euklidische Distanz). Ein ausführliches Beispiel zur «Addition» und «Multiplikation» von linguistischen Ausdrücken in der Risikoanalyse kann in [5] nachgesehen werden.

Methoden zur Verknüpfung von probabilistischen Grössen

Die gebräuchlichste Methode in der Risikoanalyse ist die sogenannte Probabilistik. Sie wird dann angewendet, wenn für Aussagen mit probabilistischem Charakter keine direkt anwendbaren Erfahrungswerte vorliegen. Die direkt bestimmbaren Wahrscheinlichkeiten werden gemäss den Gesetzen der Wahrscheinlichkeitsrechnung (Axiomen von Kolmogorow) zu «top events» superponiert. Von diesen Axiomen leitet sich das bedeutende Gesetz von Bayes zur Bestimmung von A-posteriori-Wahrscheinlichkeiten ab. Es beschreibt, wie eine gegebene Wahrscheinlichkeit eines Ereignisses, P(E), nach Hinzukommen weiterer Zusatzinformation (ZI) revidiert werden muss:

$$P(E \mid ZI) = \frac{P(E)\,P(ZI \mid E)}{P(ZI)} \qquad (1)$$

Der Logarithmus dieses Ausdruckes kann folgendermassen interpretiert werden, wobei P(ZI) ein Normierungsfaktor ist:

A-posteriori-Häufigkeit = A-priori-Häufigkeit + Zusatzinformation

Die Zusatzinformation wird auch als Information des Experimentes oder als Wahrscheinlichkeit der Daten angesehen. Mit diesem Gesetz und unter Berücksichtigung weiterer Randbedingungen, auf die hier nicht näher eingegangen wird, lassen sich nun die Richtungen der Influenzen (Pfeile) ändern. Bei mehrmaliger Wiederholung dieses Vorganges kann man vom oberen auf das untere Influenzdiagramm in Bild 5 kommen. Dabei sind beide Risikomodelle bezüglich Informationsgehalt identisch; d.h. die gemeinsame Wahrscheinlichkeitsverteilung ist dieselbe. Im oberen Risikomodell (Bild 5) sind die Ungewissheiten von Ereignis und Exposition als marginale Wahrscheinlichkeiten (a priori) angegeben, während die anderen vier Ungewissheiten als bedingte Wahrscheinlichkeiten (a posteriori) angegeben sind.

Das obere Diagramm (Bild 5) leitet den Sicherheitsfachmann zum «Vorwärtsdenken» an, das untere hingegen zum «Rückwärtsdenken». Vor allem wenn bei der Risikoanalyse Erfahrungswerte zum Schadensausmass vorliegen, ist ein «Rückwärtsdenken» angebracht. Wie im unteren Diagramm angedeutet wird, lässt sich in solchen Fällen die Ereignishäufigkeit leicht aus Schadens- und Mengenhäufigkeit bestimmen. Kann jedoch die Ereignishäufigkeit gut, die Schadenshäufigkeit aber schlecht abgeschätzt werden, ist ein «Vorwärtsdenken», wie im oberen Diagramm angedeutet, angebracht.

Ein «vorwärtsgerichtetes» Influenzdiagramm, bei dem jedes Ereignis jeweils nur binäre Zustände annehmen kann (Ja oder Nein) entspricht einem Ereignisbaum. Ein «rückwärtsgerichtetes» Influenzdiagramm, bei dem die Ereignisse (in der Regel) nur binäre Zustände annehmen und bei dem Kombinationen von Zuständen besonders hervorgehoben werden müssen durch UND- und ODER-Verbindungen, entspricht einem Fehlerbaum. Die marginalen Ereignisse werden dann Primärereignisse genannt und das letzte Ereignis Topereignis. Obwohl Ereignis- und Fehlerbäume in der Regel innerhalb der probabilistischen Methode gebraucht werden, können sie auch zusammen mit anderen quantitativen (z.B. die Fuzzy-Logik) oder auch qualitativen Methoden eingesetzt werden. Das Verfahren und die am häufigsten gebrauchten Hilfsmittel bei der Durchführung eines Fehlerbaumes werden im nächsten Abschnitt behandelt.

Die gebräuchlichsten Softwarepakete für probabilistische Influenzdiagramme sind DPL (MS-DOS, US$ 500) und DAVID (Macintosh, US$ 600). Beide Programme erlauben nebst der Berabeitung von probabilistischen Ereignisknoten auch den Einbezug von Entscheidungs- und Wertungsknoten. Damit können nebst den Ungewissheiten auch Entscheidungsstrategien unter Einbezug der Risikoaversion analysiert werden. Die gebräuchlichsten Softwarepakte für Ereignis- und Fehlerbäume werden bei der Besprechung der Hilfsmittel (weiter unten) angegeben.

Die statistische Methode

Wenn genügend historische Daten zur Bestimmung der Wahrscheinlichkeit eines Teilschritts der Risikoanalyse vorhanden sind, wird die statistische Me-

thode eingesetzt. Bei Grossereignissen ist in der Regel nicht genügend statistisch signifikantes Datenmaterial vorhanden. In solchen Fällen wird in der Praxis trotzdem oft die statistische Methode angewendet, vermutlich um die vielleicht etwas kompliziertere probabilistische Methode zu umgehen.

Wahrscheinlichkeiten werden dann durch Simulationen bestimmt oder mittels Expertenwissen abgeschätzt. Ein weitverbreitetes Computerprogramm für Monte-Carlo-Simulationen ist @Risk (MS-DOS, Macintosh, rund US$ 400). Der Benützer kann mit einem Lotus oder EXCEL ähnliche Menus arbeiten. Ein anderes oft verwendetes Monte-Carlo-Simulationsprogramm ist Crystal Ball (Macintosh, rund US$ 200). Klassische Simulationspakete zur interaktiven visuellen Simulation sind SIMAN (MS-DOS) und IThink (Macintosh).

In einem ersten Schritt wird das Risikomodell in Form eines Influenzdiagramms erstellt. Danach werden die Wahrscheinlichkeitsverteilungen definiert, womit dann die Simulation durchgeführt werden kann. Besonders wertvoll bei diesen Systemen ist, dass während der Simulation die Ereignisse am Bildschirm im Zeitraffer visualisiert werden können.

Methoden zur Verknüpfung von Schadensmessgrössen

Die Verknüpfung von unterschiedlichen (qualitativen und quantitativen) Schadensmessgrössen kann auf verschiedene Arten bewerkstelligt werden. Die drei gebräuchlichsten Methoden sind Gewichtung, Indikatorisierung und Monetarisierung.

Gewichte

Die Methode der Gewichtung basiert auf der Nutzwert-Theorie und besteht darin, dass man den verschiedenen Schadensarten Gewichte zuordnet und die gewichtete Schadenswerte zum totalen Schaden aufsummiert.

Zur Bestimmung des optimalen Standorts für die Endlagerung radioaktiver Abfälle in den USA wurde folgende additive Schadensfunktion zur Beurteilung der Bauphase verwendet [7]:

$$\text{Totaler Schaden} = 121\text{-}0.05\Sigma K_i C_i(X_i), \quad (2)$$

wobei die Faktoren 121 und 0.05 nötig sind, um die Funktion zwischen 0 und 100 zu skalieren. Die C_i's sind die «Schadensnutzen» der 14 verschiedenen Schadensarten (Mensch, Umwelt, Infrastruktur, ästhetische Degradation, sozioökonomische Schäden usw.) und die K_i's die entsprechenden Gewichte. Die in der Studie gewählten Grössen lassen u.a. auf folgende Präferenzen schliessen: Ein (probabilistischer) Toter durch Transportunfall beim Bau entspricht US$ 4 Mio. Konstruktionskosten, 1% zusätzliche ästhetische Degradation entspricht US$ 1 Mio. zusätzlicher Kosten, und US$ 1 Mio. Transportkosten entsprechen US$ 1 Mio. Lagerungskosten.

Indikatoren

Die Umwandlung von verschiedenen Schadensmessgrössen in dimensionslose Indikatoren (von 0 bis 1) wird im Handbuch I zur Störfallverordnung vorgeschlagen [3]. Werte zwischen 0 und 0.3 repräsentieren den Unfall, Werte zwischen 0.3 und 0.5 den Grossunfall und Werte zwischen 0.5 und 1 die Katastrophe. Die Wahrscheinlichkeiten der Ausmasse werden numerisch dargestellt und könnten mit dem statistischen oder probabilistischen Ansatz bestimmt worden sein.

Der totale Risikoindikator über alle Schadensarten kann auf mehrere Arten bestimmt werden. Verschiedene Ansätze dazu sind aus der sogenannten Fuzzy-Logik bekannt. Ein sehr rudimentärer Ansatz sagt, dass der totale Risikoindikator dem Maximum der Einzelindikatoren entspricht. Ein Ansatz, auf den im Handbuch I der Störfallverordnung hingewiesen wird, berechnet den totalen Risikoindikator aus den Einzelindikatoren n_i zu:

$$\text{Tot. Risikoindikator} = \min\left\{1, \left[\sum_{i=1}^{m}(n_i)^p\right]^{1/p}\right\}, \quad (3)$$

wo p ein Parameterwert ist und m die Anzahl verschiedener Schadensarten [12]. Der Parameter p muss zwischen 1 und ∞ gewählt werden. Je grösser der Parameter p ist, desto kleiner der totale Risikoindikator. Wenn p = 1 ist, dann handelt es sich um die einfache Summation der Risikoindikatoren (tot. Risikoindikator aber höchstens = 1). Wenn p unendlich gross ist, dann ist der tot. Risikoindikator gleich dem maximalen Einzelindikator. Wie gut sich dieser Ansatz bewährt, muss sich aber erst noch in der Praxis zeigen.

Monetarisierung

Ein recht oft gebrauchtes Modell zur Verknüpfung von Schadensmessgrössen unterschiedlicher Natur ist das Kostenmodell. Begründet wird dieser Ansatz dadurch, dass die meisten Entscheide in Organisationen auf Kosten beruhen und dass die traditionellen Schadensmessgrössen (z.B. Lethalität) zu komplex für die praktische Handhabung sind. Weiter wird betont, dass kostengünstige Sicherheitsmassnahmen besser identifiziert und deren Nutzen besser abgeschätzt werden können. Die

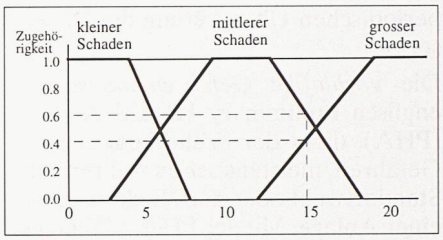

Bild 4. Fuzzyklassen für verbale Schadensgrössen

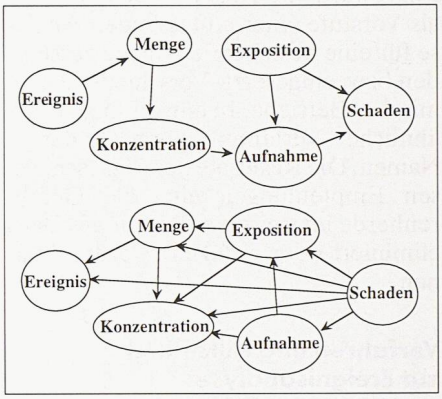

Bild 5. Zwei Influenzdiagramme mit gleichem Informationsgehalt

Versicherungen haben verständlicherweise ein grosses Interesse am Kostenmodell, können doch dadurch Versicherungsfragen besser angegangen und die nötigen Mittel zur Schadensdeckung beiseite gelegt werden.

Verfahren und Hilfsmittel zur Risikoanalyse

Eine sehr gute Übersicht der gebräuchlichsten Verfahren zur Risikoanalyse kann in [2] nachgelesen werden. Die verschiedenen in der Praxis verwendeten Methoden lassen sich in der Regel von einem oder von Kombinationen mehrerer dieser Verfahren ableiten.

Verfahren und Hilfsmittel zur Gefahrensuche

Die gebräuchlichsten Verfahren zur Gefahrensuche sind Checklisten und die vorläufige Gefahrensuche. *Checklisten* dienen der Überprüfung des Betriebsablaufs und der Gefahrenerkennung während Bau und Betrieb. Sie sind sehr einfach zu gebrauchen und dienen vor allem der Sicherstellung, dass gewisse Minimalanforderungen bezüglich Sicherheit eingehalten werden. Der Anwendungsbereich von Checklisten ist sehr gross. In der Entwurfsphase einer Anlage werden Checklisten zur schnellen und zuverlässigen Überprüfung möglicher Gefahrenherde eingesetzt. Während der Konstruktion werden Checklisten zur Qualitätssicherung eingesetzt und während des Betriebes zur

periodischen Überprüfung der Prozesse.

Die *vorläufige Gefahrenanalyse,* auf englisch Preliminary Hazard Analysis (PHA), dient der Früherkennung von Gefahren, meistens schon während der Standortwahl oder der Neukonzeption einer Anlage. Mit der PHA können potentielle Gefahrenherde schon in der Entstehungsphase des Betriebes möglichst effektiv und kostensparend lokalisiert werden. PHAs werden aber auch als Vorstufe einer umfassenden Analyse für eine bestehende Anlage verstanden bzw. eingesetzt. Verschiedene chemische Betriebe benützen der PHA ähnliche Verfahren unter anderem Namen. Die Resultate der PHA schliessen Empfehlungen ein, wie Gefahrenherde im weiteren Verlauf des Baus eliminiert oder reduziert werden können.

Verfahren und Hilfsmittel zur Ereignisanalyse

Die gebräuchlichsten Verfahren zur Ereignisanalyse sind die Gefahren- und Fehlererkennungsanalyse und die Versagensarten und Wirkungsanalyse. Die *Gefahren- und Fehlererkennungsanalyse,* auf englisch Hazard and Operability Study (HazOp), dient der Gefahren- und Fehlererkennung in einem Betrieb. Die HazOp wird sowohl bei der Erstellung der Anlage wie auch bei deren Betrieb in irgendeiner Phase eingesetzt.

Das Charakteristische der HazOp ist, dass es sich um eine Gruppenarbeit handelt, bei der Experten aus den verschiedensten Bereichen im Sinne mehrerer Brainstormings die Anlage mittels Leitwörter analysieren. Die Resultate der HazOp umfassen Identifikationen von Gefahren und Operationsprobleme, Empfehlungen für Änderungen, Vorschläge zur Sicherheitserhöhung und Empfehlungen für weitere Studien.

Die *Versagensarten und Wirkungsanalyse,* auf englisch Failure Modes and Effects Analysis (FMEA), besteht in einer tabellarischen Festhaltung von Versagensmöglichkeiten von Betriebselementen und Auswirkungen der Versagensmöglichkeiten auf die gesamte Anlage. Die Versagensmöglichkeiten beziehen sich nicht nur auf potentielle Gefahren, sondern es werden auch kleinere Fehler und Defekte berücksichtigt. Die FMEA wird auch als Vorstufe für die Fehlerbaumanalyse eingesetzt. Die Resultate der FMEA werden in solchen Fällen z.B. für die HazOp gebraucht (die FMEA ist ein Spezialfall einer HazOp). Die FMEA wird aber auch zusammen mit anderen Hilfsmittel der Risikoanalyse (z.B. Ereignis- und Fehlerbaumanalyse) eingesetzt.

Einige der kommerziell verfügbaren Softwarepakete für die HazOp und FMEA sind: CAHAZOP (MS-DOS, rund US$ 2 000); HAZOPtimizer (MS-DOS, unter US$ 400), für PHA, HazOp und FMEA; HAZSEC (MS-DOS).

Verfahren und Hilfsmittel zur Bestimmung von Häufigkeiten

Die wichtigsten Modelle in der quantitativen Risikoanalyse sind die Ereignis- und Fehlerbaumanalyse. Die Ereignisbaumanalyse dient dazu, mögliche Versagensarten von einem spezifischen Initialereignis ausgehend zu studieren und dessen Wahrscheinlichkeiten zu bestimmen. Das Initialereignis kann anlageintern oder -extern durch technisches Versagen, Naturereignisse oder menschliches Fehlverhalten ausgelöst werden.

Ereignisbäume zwingen den Sicherheitsingenieur in eine «Vorwärtsrichtung» zu denken, da vom Initialereignis ausgehend alle Folgeereignisse bis zum letztlichen Grossereignis (topevent) untersucht werden. Das Resultat der Ereignisbaumanalyse besteht in der Angabe verschiedener Initialereignisse/ Ereignisabläufe, inkl. der Angabe der Zwischenereignisse.

Die *Fehlerbaumanalyse* ist eine deduktive Methode, die für ein ausgewähltes Ereignis (Grossereignis) die Ursachen und deren Zusammenhänge analysiert. Die Ursachen umfassen technische und menschliche Fehler. Die Stärke dieses Ansatzes liegt darin, dass ein potentielles Ereignis in seine verursachenden technischen und menschlichen Komponenten zerlegt werden kann, wodurch auch mittels gezielter Massnahmen die Wahrscheinlichkeit des potentiellen Ereignisses reduziert werden kann.

Im Gegensatz zur Ereignisbaumanalyse zwingt die Fehlerbaumanalyse den Sicherheitsingenieur zu einem «Rückwärtsdenken». Das Resultat der Fehlerbaumanalyse ist eine Liste von Kombinationen technischer und menschlicher Versagensarten, die das zu untersuchende Grossereignis auslösen können. Diese Kombinationen von Versagensarten stellen die minimale Zusammensetzung von Komponenten dar, die bei kombiniertem Versagen zum Grossereignis führen können.

Einige der gebräuchlichsten Softwarepakete für Ereignis- und Fehlerbäume sind: CAFTA+ (MS-DOS, unter US$ 8 000), für Fehlerbäume; CARA (MS-DOS, rund US$ 10 000), für Ereignis- und Fehlerbäume; CHEMRISK (MS-DOS, rund US$ 2 500), für Ereignis- und Fehlerbäume; ETA II (MS-DOS, rund US$ 5 000), für Ereignisbäume; FaultrEASE (Macintosh, rund US$ 400), für Fehlerbäume; NUSSAR-II (MS-DOS, rund US$ 3 500), für Fehlerbäume; UNCERT (MS-DOS, rund US$ 6 000), zur Bestimmung von Ungewissheiten von Systemversagen.

Verfahren und Hilfsmittel zur Ausbreitungsanalyse

Die Ausbreitung eines Stoffes hängt natürlich stark vom seinem Aggregatzustand und vom Ausbreitungsmedium ab. Bei Explosionen (Druckausbreitung) und Bränden (Hitzestrahlausbreitung) breitet sich nicht der Stoff selber aus, sondern physikalische und chemische Wirkungen als Folge des Ereignisses. Massgebend für die Risikoanalyse sind Wirkdistanzen, Wirkflächen und die entsprechende Konzentration in Funktion der Zeit. Wirkdistanzen bei Feuerbällen sind konzentrisch und basieren auf dem Punktquellenmodell. Der Durchmesser von Feuerbällen hängt von der Menge des Stoffes ab. Die Druckausbreitung von Explosionen im Freien wird stark vom Terrain und von den Hindernissen beeinflusst. Auch Wirkdistanzen der Drücke werden mit dem Halbkugelmodell bestimmt und hängen von der Menge des Stoffes ab. Die Ausbreitung von giftigen Gasen in der Luft hängt stark von der Art des Austritts und von den vorhandenen klimatischen Verhältnissen ab. Wichtiger als die Wirkdistanz ist hier die Wirkfläche. Die Ausbreitung von Chemikalien in Boden und Wasser kann auf verschiedenen Pfaden erfolgen. Verfolgt werden jene Pfade, die schliesslich in die Trinkwasserfassung führen.

Wirkradien, Wirkflächen und Konzentrationen von verschiedenen Substanzen und Mengen können in verschiedenen Tabellen nachgeschlagen werden. Eine im Hinblick auf den Vollzug der Störfallverordnung erstellte Sammlung solcher Tabellen ist die «Schadensausmass-Einschätzung», erstellt durch die Koordinationsstelle für Störfallvorsorge des Kantons Zürich [9]. Verschiedene kommerziell verfügbare Softwarepakete können Wirkdistanzen berechnen und graphisch darstellen, einige davon sogar als Wirk-Isolinien auf einer digitalisierten Karte. Einige Beispiele dafür sind die folgenden Programme: EFFECTS (Freisetzung von Flüssigkeiten und Gasen) der TNO in den Niederlanden; ATMS (Air Toxic Modelling System, MS-DOS, unter US$ 15 000) der U.S. EPA, das fünf Transport- und Diffusionsmodelle enthält; CAMEO (Computer Software for Emergency Responders and Emergency Planners, MS-DOS, Macintosh, über US$ 1 000), vom U.S. National Safety Council, das in den U.S. stark verbreitet ist; InterCLAIR (in Entwicklung

beim U.N. Interagency Programme), ein Umwelt-Informationssystem basierend auf «Procedural Guidance for Integrated Health and Environmental Risk Assessment and Safety Management in Large Industrial Areas»; ChemPlus (MS-DOS, unter US$ 1 000), das vorwiegend für Notfallplanung eingesetzt wird; EPIcode (MS-DOS, unter US$ 1 000), das ebenfalls vorwiegend für die Notfallplanung gebraucht wird; IMES (Integrated Model Evaluation System, MS-DOS), MIDAS (Meteorological Information and Dispersion Assessment System, über US$ 20 000, MS-DOS, UNIX), zur Unterstützung des Personals einer Anlage durch graphische Darstellung der Daten in Echt-Zeit; PHAST (Process Hazard Analysis Software Tools, MS-DOS, über US$ 15 000); QCRR (Quantification of Chemical Release Risk, MS-DOS, über US$ 5 000), RISKPRO (MS-DOS, über US$ 500), das durch die U.S. EPA genehmigt wird; TECJET (Free Jet and Plume Dispersion Model, MS-DOS, über US$ 5 000); VAPACT (MS-DOS, über US$ 15 000), das W/A Diagramme erzeugen kann; WHAZAN (World Bank Hazard Analysis Software, MS-DOS, über US$ 1 750), das auf dem Handbuch «Techniques for Assessing Industrial Hazards: A Manual» basiert. Weitere Softwares zur Schadstoffausbreitung können in [1] gefunden werden.

Verfahren und Hilfsmittel zur Expositionsanalyse

Bei der Expositionsanalyse geht es um die Identifikation und Lokalisierung der gefährdeten Objekte. Die Expositionsanalyse kann natürlich nicht losgelöst von den berücksichtigten Wirkungen gemacht werden. Bei direkt einwirkenden Einflüssen auf den Menschen, wie z.B. Explosionen oder Gaswolken, ist die zeitliche und räumliche Verteilung der Menschen um die Schadensquelle ausreichend. Bei indirekten (z.B. via Nahrungskette) oder verzögerten (z.B. durch lange Transportstrecken) Gefahren können nicht nur die Menschen um die Gefahrenquelle betrachtet werden. Die gefährdeten Objekte müssen zeitlich und räumlich umfangreicher erfasst werden. Zudem muss der Risikoanalytiker je nach zeitlichem und räumlichem Verlauf der Ausbreitung neue Objekte hinzunehmen und andere wieder ausschliessen.

Neben dem Menschen werden auch weitere gefährdete Objekte berücksichtigt. Das Handbuch I zur Störfallverordnung schlägt neben dem Menschen noch Lebensgrundlagen (Ökosystem, Boden und Grundwasser) und Sachwerte als gefährdete Objekte vor [3]. Weitere Objekte (oder eher Aspekte) sind kultureller (historische Orte und Gebäude), sozio-ökonomischer (Infrastruktur) oder ästhetischer (wertvolle Orts- und Landschaftsbilder) Natur.

Die dynamische Inventarisierung und die graphische Darstellung der gefährdeten Objekte wird mit geographischen Informationssystemen (GIS) bewerkstelligt. Dank der offenen Architektur vieler GIS können relativ einfach weitere Berechnungsmodule (z.B. Schadstoffausbreitung) oder Datenbanken integriert werden, wodurch das GIS dann als Risikoinformationssystem (RIS) bezeichnet werden kann.

Neben den grossen GIS-Shels für Workstations (z.B. Arclnfo, InfoCam, Intergraph), die bis zu mehreren US$ 10 000 kosten, gibt es viele PC GIS-Shells für weniger als US$ 2 000, die in der Praxis und Forschung zu RIS ausgebaut werden können. Dazu gehören u.a. MAPINFO, GIS-Plus oder TransCad, das sich speziell für Transportsysteme eignet.

Verfahren und Hilfsmittel zur Schadensanalyse

Die Schadensanalyse folgt aus den Resultaten der Ausbreitungs- und der Expositionsanalyse. Mögliche Schäden durch Detonationen sind Trommelfellriss oder Schädigung der Lungen sowie Unfälle durch Wegschleudern bei Luftstössen, Trümmerwurf, Gebäudeeinsturz und Splitterwurf. Kurzzeitige Stösse sind in der Regel viel gefährlicher als schwache und lange Stösse. Brandschäden beim Menschen entstehen durch thermische Strahlung oder durch Kontatkt mit dem Feuerball. Bei Gaswolkenexplosionen ist die Energiestromdichte massgebend. Rund 65 kJ/m² ist die Schwelle zum Schmerz, ab 375 kJ/m² handelt es sich um eine Verbrennung dritten Grades. Giftgasausbreitungen führen zu Vergiftung durch Einatmung, Verschmutzung der Luft oder Vergiftung der Nahrungsgrundlagen. Die Schadenshöhe hängt von der Konzentration und der Expositionsdauer ab. So ist z.B. für den Menschen Chlorgas bei einer Konzentration von 1000 ppm bereits nach einigen Atemzügen tödlich, Schwefelwasserstoff bereits ab 900 ppm, hingegen Ammoniak erst ab einer Konzentration von 5000 ppm.

Eine Freisetzung radioaktiver Stoffe kann Direktstrahlungen aus der Wolke, Bodenstrahlung oder Bestrahlung des Menschen durch Inhalation oder Nahrungsaufnahme zur Folge haben. Sie können zu akuten oder Frühschäden (z.B. akute Strahlenkrankheit), nichtmalignen Spätschäden (z.B. fibrotische Gewebsveränderungen, Trübung der Augenlinsen), malignen Spätschäden (z.B. Leukämie und Tumoren) und genetischen Schäden führen [4].

Das Schadensspektrum beim Menschen umfasst Tote, Verletzte und psychologische Folgen. Verletzungen und psychologische Folgen sind je nachdem reversibel oder irreversibel. Die Schädigung der Gewässer als Lebensgrundlagen für Menschen, Pflanzen und Tiere wird als Volumen verschmutzten Wassers angegeben und hängt von der Substanz ab (Pflanzen und Tiere via dem LC_{50}-Wert, Menschen via dem Toleranzwert, dem Grenzwert oder durch Qualitätsziele). Die Schädigung des Grundwassers und des Bodens hängt vom k-Wert ab und wird (bei Erdölderivaten) als Fläche verschmutzten Grundwassers und als Volumen verschmutzten Bodens ausgedrückt. Für weitere gefährdete Objekte müssen eigene Schadensspektren eingeführt werden. So z.B. für biologische Degradation (von «keine Einflüsse» bis zu «Zerstörung von gefährdeten Lebewesen oder deren Lebensraum») oder sozioökonomische Einflüsse (von «keine Einflüsse» bis «grössere Zerstörung der Infrastruktur mit Evakuation»).

Was die Hilfsmittel anbetrifft, wird auch hier auf die Anleitung «Schadensausmass-Einschätzung» hingewiesen [9]. Kommerziell verfügbare Softwarepakete zur Schadensanalyse sind u.a.: ACSL (Advanced Continuous Simulation Language, MS-DOS, unter US$ 5 000), das zur Bestimmung der Aufnahme von Chemikalien bei Menschen und Tieren gebraucht wird; IRIS (Integrated Risk Information System, online service der U.S. EPA, MS-DOS, unter US$ 500), das Informationen über mehr als 400 Chemikalien enthält; Risk*Assistant (U.S. EPA, MS-DOS), mit dem der Benützer für verschiedene Konzentrationen relevante toxikologische Daten bestimmen kann; Risk*Rank (MS-DOS, über US$ 900), THRESH (MS-DOS, unter US$ 1 500); TOX-RISK (MS-DOS, rund US$ 5 000), das vor allem zur Abschätzung und Reihung von karzinogenen Risiken gebraucht wird; RAMAS/stage (MS-DOS, rund US$ 400), das zur Simulation von Populationsschwankungen eingesetzt wird.

Zur Durchführung einer umfassenden Risikoanalyse

Die Risikoanalyse stellt den ersten Schritt eines Entscheidungsprozesses dar, der insgesamt die Analyse der Risiken, deren Bewertung und Management umfasst. Während sich die *Risikoanalyse* mit der Gefahrenerkennung und Beschreibung der Risiken auseinandersetzt, bezieht sich die *Risikobewertung* auf Schutzziele, Akzeptanzfragen sowie rechtliche und ökonomische Randbedingungen. Das *Risikomanage-*

ment befasst sich vorrangig mit der Risikoreduktion, d.h. den nötigen Massnahmen, den Kontrollen, der A-jour-Haltung der Risikoanalyse und der Risikokommunikation. Deshalb muss bei der Wahl der Methoden, Modelle, Verfahren und Hillfsmittel der Risikoanalyse stets auch auf die Anforderungen der Risikobewertung und des Risikomanagements geachtet werden.

Da es erstrebenswert ist, eine grösstmögliche Vergleichbarkeit der Resultate der Risikoanalyse zwischen verschiedenen Systemen zu gewährleisten, sollte der methodische Ansatz zur Risikoanalyse soweit wie möglich unabhängig vom Zweck der Risikoanalyse, dem zu untersuchenden System und den vorhandenen Mitteln und Ressourcen sein. Zudem sollten die methodischen Ansätze zur Analyse, zur Bewertung und zum Management untereinander konsistent sein.

Bei der Durchführung der oben vorgestellten Schritte einer umfassenden Risikoanalyse werden die dazu benötigten Methoden, Modelle, Verfahren und Hilfsmittel in Kombination oder einzeln bei einem oder mehreren dieser Schritte eingesetzt. Der Risikoanalytiker muss klar erkennen, wo qualitativ und wo eher quantitativ vorzugehen ist und ob ein induktiver oder ein deduktiver Ansatz angebrachter ist und mit welchem Tiefgang die verschiedenen Hilfsmittel bei gegebenem Problem einzusetzen sind. Als Bestandteil der Risikoanalyse ist auch anzugeben, wo Einschränkungen, Vereinfachungen und Annahmen gemacht wurden.

Trotz der bereits vorhandenen Erfahrungen bei der Anwendung umfassender Risikoanalysen kann wegen der Komplexität kein generelles Rezept zum Vorgehen gegeben werden. Die Risikoanalyse ist nicht nur reine Wissenschaft, sondern auch eine «Kunst». Nur die Verbindung von Wissen und Erfahrung macht die Kompetenz des Sicherheitsingenieurs aus.

Im Handbuch I zur Störfallverordnung sind Ansätze zur umfassenden Risikoanalyse gegeben, die sich sowohl auf die qualitative als auch auf die quantitative Definition des Risikos abstützen [3]. Quantitative umfassende Risikoanalysen wurden zuerst im Nuklearbereich entwickelt und weltweit angewendet [8]. Die Studien von Canvey Island und Rijmond [4] sind Beispiele dafür, dass die umfassende Risikoanalyse auch in der chemischen Industrie Einzug gefunden hat, während in der Vergangenheit vorwiegend die Gefahrensuche und die Ereignisanalyse im Zentrum der Untersuchungen standen (zur quantitativen Risikoanalyse siehe auch [2]).

Softwarepakete, die die umfassende Risikoanalyse abdecken, sind u.a.: NUPRA (MS-DOS, rund US$ 17 000), das für probabilistische Risikoanalysen bei Level 1 und 2 eingesetzt wird. Es besteht aus sechs Analysemodulen und sieben Modulen zur Bestimmung von Nutzenfunktionen. RISKMAN (MS-DOS, rund US$ 45 000), das für die quantitative Risikoanalyse bei Nuklearanlagen eingesetzt wird (kann aber auch für andere technische Systeme benutzt werden). RiskPAC (MS-DOS, bis zu US$ 10 000), ein interaktives, automatisches System zur Risikoanalyse mit eingebautem Expertensystem. SAFETI (MS-DOS, Workstations, rund US$ 130 000), das zur Risikoanalyse von chemischen und petrochemischen Systemen gebraucht wird. Eine Beschreibung weiterer Software kann in [6] gefunden werden.

Schlussbemerkungen

Die umfassende Risikoanalyse ist ein dynamischer Prozess mit Querverbindungen zu Risikobewertung und -management. Die zunehmende Verdichtung des Lebensraums und der Zuwachs komplexer technischer Systeme verlangt aber auch immer mehr eine regionale Betrachtungsweise in Sicherheitsfragen. Die Risiken einer Region stammen von chemischen Anlagen, Nuklearanlagen, Gefahrenguttransporten u.a. Die Region kann dabei eine Gemeinde, ein Tal, eine Grossstadt oder ein Land sein. Einige der Gründe, weshalb die anlagespezifische Betrachtungsweise auf eine regionale Betrachtungsweise erweitert werden sollte, sind die folgenden:

- Bei der Standortwahl sowie für die anlagespezifischen Anforderungen einer neuen Anlage sollten die regionalen Gegebenheiten berücksichtigt werden.
- Schutzziele sollten das Gesamtrisiko einer Region sowie die Akzeptanz/Aversion der Bevölkerung innerhalb der Region berücksichtigen.
- Die Aufklärung der Öffentlichkeit in Sicherheitsfragen sollte nicht anlagespezifisch, sondern in einem übergeordneten, regionalen Rahmen geschehen.
- Entscheidungsgrundlagen für Politiker bilden nicht nur die Einzelanlagen, sondern die Gesamtheit der Anlagen innerhalb einer Region.

Eine der Voraussetzungen für eine regionale Betrachtungsweise ist aber ein konsistenter methodischer Ansatz der Risikoanalyse, der einen Vergleich nicht nur innerhalb, sondern auch zwischen verschiedenen Systemen zulässt.

Literatur

[1] *Ambrose R.B.* und *Barnwell T.O.:* Environmental Software at the U.S. Environmental Protection Agency's Center for Exposure Assessment Modelling, Environmental Software, Vol. 4, No. 2, 1989

[2] Guidelines for Hazard Evaluation Procedures: Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, 1992

[3] Handbuch I zur Störfallverordnung, StFV (zu beziehen bei Eidg. Drucksachen- und Materialzentrale, EDMZ, 3003 Bern)

[4] *Hauptmanns U., Herttrich M.* und *Werner W.:* Technische Risiken, Ermittlung und Beurteilung, Springer-Verlag, Berlin Heidelberg, 1987

[5] *Kangari R.* and *Riggs L.S.:* Construction Risk Assessment by Linguistics, IEEE - Transactions on Engineering Management, Vol. 36, No. 2, pp 126-131, 1989

[6] *Marrnicio R.J., Hakkinen P.J., Lutkenhoff S.D., Hertzberg R.C.* und *Moskowitz P.D.:* Risk Analysis Software and Databases: Review of Riskware 90' Conference and Exhibition Risk Analysis, Vol. 11, No. 3, 1991

[7] *Merkhofer M. W.* und *Keeney R.L:* A Multiattribute Utility Analysis of Alternative Sites for the Disposal of Nuclear Waste, Risk Analysis, 7/2, 173-194, 1987

[8] *Kröger W.* und *Chakraborty S.:* Risikobestimmung – Eine Bestandesaufnahme der Methodik für Kernkraftwerke, Schweizer Ingenieur und Architekt, Heft 37/90, S. 1022-1030, 1990

[9] Schadensausmass-Einschätzung: Referenzbeispiele und Hilfsmittel, Direktion des Kantons Zürich, Koordinationstelle für Störfallvorsorge, 8090 Zürich, 1992

[10] *Schneider J.:* Risiko und Sicherheit technischer Systeme, Auf der Suche nach neuen Ansätzen. Birkhäuser Verlag, 1991

[11] *Talcott F.W.:* How Certain is that Environmental Risk Estimate, Resources for the Future, No. 107, 10-15, 1992

[12] *Wyler E.* und *Bohnenblust H.:* Disaster Scaling, A Multi-Attribute Approach Based on Fuzzy Set Theory, in Apostolakis G. (ed.), Probabilistic Safety Assessment and Management, Volume 1, Proceedings of the International Conference on Probabilistic Safety Assessment and Management, 1991

Verschiedene Bestrebungen in dieser Richtung sind vor allem in Europa im Gang.
An der ETH Zürich läuft seit 1991 ein mehrjähriges Polyprojekt «Risiko und Sicherheit technischer Systeme», das als zentrales Element methodische Fragen der regionalen Sicherheitsplanung hat. Es unterteilt sich in die drei Bereiche *Risikoanalyse, Risikobewertung und Risikomanagement.* Die Absicht ist, eine Schriftenreihe zu erstellen, die einem Sicherheitsfachmann helfen soll, eine regionale Sicherheitsanalyse durchzuführen. Dabei wird eine enge Zusammenarbeit zwischen Hochschule, Industrie und Verwaltung angestrebt. Nicht zuletzt geht es im Polyprojekt der ETH auch darum, eine Brücke zu den nichttechnischen Disziplinen zu schlagen, die für den richtigen Umgang mit technischen Risiken von nicht zu unterschätzender Bedeutung sind [10].

Adresse des Verfassers: *G. Beroggi,* Dr. dipl. Ing. ETH, Assistant Professor of Policy Analysis, Delft University of Technology, P.O.Box 5015, NL-2600 GA Delft, Netherlands; und Prof. Dr. W. Kröger, Paul Scherrer Institut, CH-5232 Villigen PSI.

Sicherheit und Risiko

Störfallrisiken technischer Anlagen

Bezug zur Raum- und Umweltplanung

Störfallrisiken technischer Anlagen werden seit Jahren intensiv diskutiert (vgl. u.a. unsere Artikelreihe «Sicherheit und Risiko», rund 30 Beiträge seit 1988). Verschiedene Schadenereignisse sowie die zunehmende Komplexität technischer Anlagen erfordern einen systematischen Umgang auch ausserhalb der Kerntechnik. Ein Resultat dieser Diskussion ist die Verordnung über den Schutz vor Störfällen (StFV) vom 27. Februar 1991. Im Mittelpunkt stehen dabei vor allem die betrieblichen und baulichen Aspekte der Sicherheitsplanung sowie die Notfallplanung. Welchen Beitrag könnte nun die Raumplanung zum verbesserten Umgang mit Störfallrisiken leisten? Nachfolgende Ausführungen stellen auch einen Ansatz dazu vor.

VON RENZO SIMONI, ZÜRICH

In den folgenden Ausführungen ist von Anlagen und deren Risiken gemäss Störfallverordung die Rede. Von den Betrachtungen ausgenommen sind insbesondere die der Kernenergie- und Strahlenschutzgesetzgebung unterstellten Anlagen. Weiter ausgeklammert bleiben die Naturgefahren, soweit sie nicht als Auslöser für einen technischen Störfall in Betracht kommen. Schliesslich ist im folgenden auch nicht die Rede von gesundheitlichen und ökologischen Risiken, die durch chronische, den gesetzlichen Anforderungen genügende und dem Normalbetrieb entsprechende Immissionen entstehen. Deren Bedeutung wird jedoch keineswegs verneint. Es wird unumgänglich sein, diese Risiken im Sinne einer ganzheitlichen Betrachtungsweise ebenfalls zu berücksichtigen.

Die Schwerpunkte der Störfallverordnung

Die Störfallverordnung [1] beginnt mit folgendem Satz: «Diese Verordnung soll die Bevölkerung und die Umwelt vor schweren Schädigungen infolge von Störfällen schützen.» Die sich daraus ableitenden Schwerpunkte für den Verordnungsvollzug sind gemäss Handbuch I zur Störfallverordnung [2]:

- Das Erfassen der Risiken für Bevölkerung und Umwelt
- Eigenverantwortliches Treffen der zur Verminderung des Risikos geeigneten Massnahmen durch den Betriebsinhaber
- Bewältigung von Störfällen durch den Inhaber
- Kontrolle durch die Behörden
- Verbesserung der Information der Bevölkerung

Der Vollzug der Störfallverordnung beinhaltet zu einem wesentlichen Teil risikoanalytische Fragestellungen [3]. Es obliegt der Eigenverantwortlichkeit eines Betreibers abzuklären, ob seine Anlage unter den Geltungsbereich der StFV fällt und wie allenfalls die Risiken zu beurteilen sind. Um diese Beurteilung zu ermöglichen, ist in einer ersten Stufe ein «Kurzbericht» und allenfalls in einer zweiten Stufe eine weiterführende «Risikoermittlung» durchzuführen [2]. Die Resultate dieser Untersuchungen fallen in der Regel objektbezogen aus. Das heisst, die vom Objekt ausgehenden Risiken werden anhand eines oder mehrerer Schadenindikatoren (z.B. Todesopfer, Sachschaden, geschädigte Ökosysteme...) sowie der Häufigkeit ihres Auftretens beschrieben. Diese Aussagen erlauben die Beurteilung der untersuchten Anlage.

Ein aus planerischer Sicht wesentliches Resultat des StFV-Vollzugs dürften die kantonalen Risikokataster sein. Darin werden sich die Aussagen voraussichtlich in einer Auflistung der erkannten Gefahrenpotentiale erschöpfen, allenfalls werden Risiken in einer Karte mittels unterschiedlich grossen Kreisen dargestellt [4]. Dies ist aus raumplanerischer Sicht einer der wichtigsten Punkte der StFV.

Die Anliegen der Raumplanung

Folgende allgemeine Anliegen und Aufgaben der Raumplanung scheinen im Zusammenhang mit Störfallrisiken technischer Anlagen wichtig zu sein:

☐ Die Raumplanung koordiniert Tätigkeiten mit räumlichen Auswirkungen, wo dies nötig erscheint, stellt Konflikte dar und zeigt Möglichkeiten (Massnahmen) zu deren Entflechtung oder zu deren Vermeidung auf. Die Situationsanalyse bildet die Grundlage dafür, welche es erlaubt, einerseits bestehende, anderseits künftige Konfliktbereiche, die durch Projekte entstehen könnten, zu erkennen.

Dies bedeutet, dass die raumrelevanten Aspekte von Störfallrisiken hinsichtlich ihrer Beeinträchtigung sowohl vorhandener wie auch gemäss Nutzungsplanungen vorgesehener Nutzungen beurteilt werden müssen. Dies gilt für bestehende Anlagen wie auch für Projekte.

☐ Bei der Standortevaluation von Anlagen der öffentlichen Hand (Infrastrukturanlagen) mit überörtlichem Charakter kommt der Richtplanung zentrale Bedeutung zu. Die Aufgabe der Richtplanung ist es unter anderem,