satw it's all about technology

SATW-Workshops der Themenplattform «Risiko»

Umgang mit Risiko – Alte und neue Herausforderungen

Nach wie vor wird der **Risikobegriff** unterschiedlich weit gefasst, je nach Community auf die Konsequenzen unerwünschter Ereignisse, das heisst auf das Wagnis, beschränkt oder die positiven Aspekte und die Chancen miteinschliessend. Eine allgemeingültige Definition fehlt; die wesentlichen Elemente des Risikos, insbesondere die «Wahrscheinlichkeit», und deren Zusammenspiel mit anderen Elementen stossen oft auf Unverständnis. Verbleibende Unsicherheiten, die aus Mangel an Wissen oder der dem Ereignis innewohnenden Zufälligkeit resultieren können – man denke an Erdbeben –, steht man oft ratlos gegenüber, ebenso dem Umgang mit dem **Restrisiko**. Das simple **Risikokonzept** mit multiplikativer Verknüpfung von Häufigkeit und Konsequenzen wird für Ereignisse extremer Schadenshöhe, trotz zugestandener Seltenheit, oft als untauglich erachtet, Risikoaversion geltend gemacht – wie etwa gegenüber dem Nuklearbereich üblich.

Zudem ist angesichts zunehmender Integration und gegenseitiger Abhängigkeiten im Bereich lebenswichtiger Infrastrukturen ein komplexes **«System von Systemen»** entstanden, das in seinem Verhalten stark vom operativen-organisatorischen Umfeld abhängt und Störungsmuster einschliesslich Kaskaden aufweist, die wir derzeit nur schwer verstehen, geschweige denn voraussehen können. Klassische quasi-statische Methoden wie Fehler- und Ereignisbäume reichen dafür nicht aus. **Extremereignisse** treten in vielen Bereichen häufiger auf und laufen anders ab als gedacht: Sie liegen ausserhalb gängiger Verteilungsfunktionen. Manche betrachten sie, selbst bei Betonung so genannter «heavy tails», als sich abzeichnende Ausreisser; für andere sind sie überhaupt nicht prognostizierbar, das heisst, es sind so genannte «Schwarze Schwäne».

«Resilienz» taucht als **neues Paradigma** auf, was das bisherige auf Erhöhung der Widerstandskraft ausgerichtete Risikokonzept um das Verhalten eines Systems nach Störereignissen bis zur Wiederherstellung der Funktionsfähigkeit erweitert. **Risikomanagement** sollte beispielsweise geografisch integriert erfolgen, bei Problemstellungen erheblicher Tragweite in Richtung **«Governance»** entwickelt werden und bei grossen Unsicherheiten und Ambiguitäten die Hauptakteure einbeziehen.

Zu diesen teils alten, teils neuen Herausforderungen und gepriesenen Möglichkeiten fand im November 2013 ein Workshop statt. Dieses Diskussionspapier hat zum Ziel, ausgewählte Beiträge zusammenfassend darzustellen und an Interessierte heranzutragen.

Ausführlichere Versionen der einzelnen Beiträge können (in englischer Sprache) als PDF unter **www.satw.ch/risiko** heruntergeladen werden.

Risikobausteine, traditionelle Methoden der Risikoanalyse

Wolfgang Kröger, ETH Zürich

Unterschiedliche Quellen von **Unsicherheiten** spielen eine wichtige Rolle bei der Risikobeurteilung. Üblicherweise werden die **Risikoelemente**, das heisst die Frequenz und die Folgen eines unerwünschten Ereignisses, multipliziert und im Falle von mehr als einem Ereignis anschliessend aufsummiert.

Restrisiko wird entweder als beschreibender Begriff verwendet, mit dem nach Umsetzung aller geplanten Sicherheitsmassnahmen das übrigbleibende Risiko zusammengefasst wird, oder als normativer Begriff, um das zulässige Risiko nach vorgegebener Akzeptanz-Beurteilung zu bezeichnen.

Das **systemische Risiko** bettet Risiken in einen grösseren Kontext von sozialen, finanziellen und wirtschaftlichen Folgen und erhöhten gegenseitigen Abhängigkeiten ein. Der Begriff **Sicherheit** kann absolut (Abwesenheit von Gefahr), relativ (vergleichsweise niedriges oder akzeptables Risiko, Umgang mit normativen Anforderungen) oder als wahrgenommene Sicherheit definiert werden.

Bevorzugt sollten Risikoschätzungen auf verfügbaren, direkt nutzbaren Daten und Erfahrungen mit ähnlichen Ereignissen basieren. Oft ist die Basis für eine solche **statistische Risikoschätzung** nicht gegeben und Modelle zur Voraussage von seltenen, noch nicht beobachteten Ausfallszenarien und Ereignissen müssen angewendet werden, die vorliegende empirische Daten auf der Komponenten-Ebene nutzen.

Unter der Annahme, dass Ereignisse einschliesslich ihrer Eintrittswahrscheinlichkeit im Voraus identifiziert werden können, wurde die systematische und umfassende Methodik probabilistischer Sicherheitsanalyse (PSA) entwickelt und hauptsächlich auf Kernkraftwerke angewandt. Daraus resultierende **prognostische Risikoabschätzungen** werden als anlagenspezifische Plattform für den Austausch von Sicherheitsfragen genutzt. Es gibt drei aufeinander aufbauende Stufen von PSA. In der Schweiz, wie in vielen Ländern auch, werden die Stufen 1 (Ermittlung der Kernschmelzhäufigkeit) und 2 (Ermittlung der Häufigkeit einer grossen Freisetzung radioaktiver Stoffe) eingesetzt, um zu prüfen, ob die getroffenen Schutzmassnahmen ausreichend zuverlässig und ausgewogen sind und die Zielwerte für die Sicherheit eingehalten werden. Sie sind nicht gedacht als Ermittlung tatsächlicher gesellschaftlicher Risiken, die aus dem Kernkraftwerksbetrieb resultieren. Dazu müssten traditionelle Methoden und Ansätze erweitert und Kenntnislücken geschlossen werden.

Integratives Risikomanagement und Resilienz

Hans R. Heinimann, ETH Zürich

Zunehmende Kopplungen und abnehmende Heterogenität innerhalb und zwischen sozio-technischen Systemen haben zu neuartigen Verhaltensmustern geführt, die neue Ansätze zur Risikobeurteilung erfordern. Zwei aufkommende Konzepte werden vorgestellt, deren Anwendung eine bessere Bewältigung von Störungen in einem «System von Systemen» verspricht.

Integratives Risikomanagement (IRM) ist ein Konzept, das darauf abzielt, simultan ein Portfolio natürlicher, technischer, wirtschaftlicher und sozialer Risiken für eine bestimmte geografische Region zu handhaben. Es sucht bei angestrebter Risikoreduzierung nach einer optimalen Balance zwischen Nutzen und Kosten, indem es eine Reihe von Aktionen öffentlicher und privater Mitwirkender initiiert und dabei traditionelle Grenzen beteiligter Disziplinen und Communities überwindet. IRM erfordert gemeinsame Anstrengungen, ein geändertes Bewusstsein und muss unterschiedliche Fachrichtungen aus den Ingenieur-, Wirtschafts- und Sozialwissenschaften zusammenbringen.

In den letzten zehn Jahren hat das so genannte **Resilienzkonzept** sehr an Aufmerksamkeit gewonnen und in den Bereich technischer Systeme Einzug gehalten. Resilienz bedeutet die «Fähigkeit eines Systems, Störungen (Schocks) zu absorbieren und sich zu reorganisieren/rekonfigurieren, um die ursprüngliche Struktur und Funktionsfähigkeit im Wesentlichen wieder zurückzuerhalten». Es ist also ein neues Paradigma im Unterschied zum klassischen Ingenieuransatz, der darauf abzielt, die Widerstandskraft eines Systems durch «Härtung» zu erhöhen.

Drachen-Könige: Die Natur von Extremereignissen begreifen

Spencer Wheatley und Didier Sornette, ETH Zürich

Extremereignisse dominieren die langfristige Qualität und Organisation der wichtigsten natürlichen und gesellschaftlichen Systeme: Die beiden grössten Kernkraftwerksunfälle haben fünfmal mehr Schaden verursacht, die fünf grössten Epidemien seit 1900 verursachten zwanzig Mal mehr Todesfälle, jeweils als alle anderen historischen Unfälle gleichen Typs zusammen. Entsprechende statistische Verteilungen zeichnen sich durch ausgeprägte «Schwänze» (heavy tails) aus; die schlimmsten Ereignisse stellen Ausreisser dar.

In diesem Bericht wird eine besondere Art von Extremereignissen diskutiert: so genannte **Drachen-Könige**. Dies ist eine Doppel-Metapher für ein Ereignis, das – im Unterschied zu anderen Ereignissen aus dem gleichen System – betreffend Grösse oder Wirkung extrem ist (ein «König») und aus einem einzigartigen Prozess erzeugt wird (ein «Drachen»). In einem breiten Spektrum von physikalischen Systemen sind viele Extremereignisse bis zu einem gewissen Grad vorhersehbar, vorausgesetzt, dass man ein ausreichend tiefes Verständnis der Struktur und Dynamik des Fokussystems entwickelt und abbilden kann und dieses auch überwachen kann. Hier unterscheidet sich die Theorie der Drachen-Könige also grundlegend von der so genannter «Schwarzer Schwäne», die als unvorhersehbar gelten. Viele Ereignisse wie die Finanzkrise 2008 oder das Erdbeben 2011 in Japan sind auf den ersten Blick «Schwarze Schwäne», bei genauerer Analyse allerdings typische Beispiele für Drachenkönige.

Verstehen komplexer sozio-technischer Systeme

Giovanni Sansavini, ETH Zürich

Durchdringende Systemintegrationen und Strategieänderungen sowie unzureichende Investitionen in den letzten Jahren haben dazu geführt, dass grossflächige technisierte Netzwerke zunehmend voneinander abhängen und an den Grenzen ihrer Leistungsfähigkeit betrieben werden, wobei «der Mensch», zugleich Betreiber und Nutzer, die Komplexität gesamthaft steigert. Ein typisches Beispiel für ein solches Netzwerk ist das Stromversorgungssystem. Resultierende «Systeme von Systemen» tendieren zu unvorhersehbaren Verhaltensweisen mit Kaskaden und weitreichenden Konsequenzen, deren Verstehen und Charakterisierung entscheidend sind für die sorgfältige Analyse von deren Zuverlässigkeit und Verwundbarkeit.

Um die Folgen von Störereignissen unterschiedlicher Schwere abzuschätzen, muss – unter Ausnutzung meist weniger empirischer Beobachtungen – auf Modelle und Simulationen zurückgegriffen werden, die über gegenwärtige Standardansätze hinausgehen. Die **Complex Network Theorie (CNT)**, für die Erforschung struktureller/topologischer Eigenschaften komplexer sozio-technischer Systeme inzwischen allgegenwärtig, wurde auch auf das Schweizer Stromnetz angewendet und hat eine Reihe überraschender Ergebnisse und Einsichten hinsichtlich Kaskadenausbreitung geliefert. So können weitreichende Kaskaden ausbrechen, wenn die Systeme unter Stressbedingungen und in der Nähe von Sicherheitsmargen operieren. Dabei wirkt sich ein geringerer Vernetzungsgrad zunächst positiv aus; wenn allerdings die kritische Last erreicht ist, breitet sich die Ausfallkaskade schlagartig aus und lässt sich nur noch schwer mässigen. Umgekehrt sind stark vermaschte Netzwerke zwar anfälliger für eine Kaskadenausbreitung, die kritische Last ist allerdings höher.

Das «Risk Governance»-Konzept

Ortwin Renn, Universität Stuttgart

Der Begriff «Risk Governance» bezieht sich auf die unterschiedliche Art und Weise, wie mehrere Akteure, Einzelpersonen und Institutionen, öffentliche und private, in einem Umfeld von Unsicherheit, Komplexität und Mehrdeutigkeit mit Risiken umgehen beziehungsweise umgehen sollten. Eines der zugehörigen Konzepte wurde vom International Risk Governance Council (IRGC) entwickelt. Dieses adaptive Rahmenwerk verspricht begleitende Unterstützung beim Aufbau umfassender Strategien für die Beurteilung und Handhabung von Risiken; es integriert wissenschaftliche, ökonomische, soziale und kulturelle Aspekte und sieht ineinandergreifende Phasen vor, mit effizienter Kommunikation als zentraler Aufgabe.

Das **«Risk Governance»-Konzept** wird einerseits im deskriptiven Sinn dafür verwendet, wie Entscheidungen gefällt werden, und anderseits im normativen Sinn, um Strukturen und Prozesse für politische Entscheidungen zu verbessern. «Risk Governance» lenkt die Aufmerksamkeit darauf, dass viele Risiken, insbesondere für grosse technische Systeme, im Umgang nicht einfach sind. Eine simple multiplikative Verknüpfung von Häufigkeit und Konsequenzen unerwünschter Ereignisse reicht nicht aus. Viele Risiken unterliegen komplexen Abwägungen von Kosten und Nutzen, die bei gesellschaftlich relevanten Entscheidungen angemessen, unter Beteiligung der Hauptakteure, einbezogen werden müssen.

Ausblick

Wir sehen uns auch zukünftig und vielleicht in zunehmendem Masse mit Entwicklungen und Fragestellungen konfrontiert, die für die Gesellschaft wirklich wichtige Risiken darstellen, zu deren Umgang und Beantwortung aber altbewährte Methoden und Herangehensweisen mit Blick auf mögliche Risiken nicht mehr taugen. Zu diesen Entwicklungen und Fragestellungen gehören einerseits die Integration von Systemen samt Steuerung über digitale Informations- und Kommunikationssysteme bis hin zum «Internet of Everything» und der autonomen Mobilität und anderseits «zukunftsweisende, smarte» Energieversorgungssysteme oder Verkehrs- und Bebauungskonzepte.

Angesichts der meist damit einhergehenden Komplexität des Systemdesigns und der Aufgabenstellung stossen unsere Fähigkeiten des Vorabverstehens, -simulierens und -beurteilens an ihre Grenzen. Es braucht neue Methoden und Ansätze.

Dazu gibt es aussichtsreiche Anregungen, aber auch bleibende Zweifel, ob uns das gelingen wird. Die Beiträge der Autoren zeigen Ansätze, die sich möglicherweise zu tragfähigen Methoden entwickeln lassen.

Als vielversprechendster Weg, unsere Systeme und Prozesse robuster und resilienter zu gestalten, wird oft deren Vereinfachung genannt, etwa durch Entkoppelung und Dezentralisierung, beispielsweise im Bereich der Stromversorgung. Wie weit das überhaupt möglich, machbar und erwünscht ist, wird sich zeigen.

Neuen, vor allem Cyber-induzierten Risiken ist entsprechende Aufmerksamkeit zu zollen, denn unsere Vorstellungskraft, welche Gefahr von böswilligen Systemmanipulationen ausgehen kann, ist noch begrenzt.

Wie man zu einem «guten» Umgang mit Risiken kommt, bedarf fortwährender Bemühungen. Für weitreichende Risiken von gesellschaftlicher Relevanz, die sich durch hohe Unsicherheiten und Ambiguitäten auszeichnen, ist die Anwendung des «Risk-Governance-Konzepts» sicher Versuche wert. Die Antwort auf die «alte» Frage «How safe is safe enough?» und dabei insbesondere bis zu welcher Höhe Schäden tolerierbar sind, muss letztlich die Gesellschaft entscheiden und dabei begreifen, dass es ein «Nullrisiko» nicht gibt. Die Wissenschaft kann höchstens die Beurteilungsbasis bereitstellen.

Autoren: Wolfgang Kröger (ETH Zürich) und weitere (siehe innen)

Beispiel eines Extremereignisses: Grosse Teile von New Orleans stehen nach dem Hurrikan Katrina unter Wasser. Die Gesamtschäden durch den Hurrikan beliefen sich auf über 100 Milliarden US Dollar.

Quelle: AP Photo/U.S. Coast Guard, Petty Officer 2nd Class Kyle Niemi (29.8.2005)

satw it's all about technology

Schweizerische Akademie der Technischen Wissenschaften SATW
Gerbergasse 5 | 8001 Zürich | 044 226 50 11 | info@satw.ch | www.satw.ch