X

Safety Concepts

Concepts de sécurité

Sicherheits-Konzepte

Leere Seite
Blank page
Page vide

Xa

Sicherheit als sozio-ökonomisches Optimierungsproblem

Safety – a Socio-Economic Decision Problem

Sécurité – un problème de décision socio-économique

Th. SCHNEIDER
Dipl. Ing.
Basler & Hofmann, Ingenieure und Planer AG
Zürich, Schweiz

ZUSAMMENFASSUNG
Es wird diskutiert, warum sich heute eine grundsätzlichere Auseinandersetzung mit der Sicherheit technischer Systeme aufdrängt. Die Entwicklung und der Stand der Bauwerksicherheit werden in diesem Rahmen kurz beleuchtet. Die Frage "Was ist Sicherheit?" wird in ihrer allgemeinsten Form besprochen, und es werden Überlegungen angedeutet, wie Risiken gemessen und beurteilt werden können. Im Vordergrund stehen dabei die Schäden, welche ein System erzeugt, sowie die Kosten, welche für eine Reduktion der Schadenerwartung aufgewendet werden müssen.

SUMMARY
The need for a basic discussion of technical safety is brought forward. The development and state of the art in the field of structural safety are shortly mentioned in this context. The question "What is safety?" is discussed in a broad sense and some ideas on how to measure and appraise risks are presented. The actual damage or loss produced by a technical system and the costs of reducing this anticipated damage are considered to be the decisive facts.

RESUME
La nécessité d'une discussion fondamentale de la sécurité technique est mise en évidence. Le développement et l'état actuel de la sécurité des constructions sont mentionnés sous cet aspect. La question "Qu'est-ce que la sécurité?" est discutée dans un sens général. Des considérations pour évaluer et apprécier des risques sont présentées. Les dégâts qu'un système technique pourrait produire et les frais qu'on devrait engager pour réduire ces risques sont considérés comme les éléments décisifs.

1. EINLEITUNG

1.1 Zur Aktualität der Sicherheitsfrage in der Technik

Die Frage der Sicherheit war seit je her eng mit der technischen Entwicklung verknüpft. In jüngster Zeit jedoch hat sie an Aktualität besonders gewonnen. Dies ist vorerst erstaunlich, da kaum irgendwelche messbaren Fakten auf eine zunehmende Verunsicherung unseres Lebensraumes hinweisen. Wenn die Sicherheitsfrage dennoch vermehrt ins Rampenlicht rückt, so dürfte dies verschiedene Gründe haben:

Vorerst ist zu erwähnen, dass man in den letzten Jahrzehnten in verschiedenen technischen Bereichen zu einer grundsätzlicheren Auseinandersetzung mit dem Sicherheitsproblem gezwungen war. Allem voran sei hier die Raumfahrt genannt. Das bisherige, mehrheitlich empirische Vorgehen reichte dort für die Lösung der komplexen Sicherheitsfragen ganz einfach nicht mehr aus.

Auch die Sicherheitsprobleme von Kernenergieanlagen waren mit der traditionellen Methode von "trial and error" nicht mehr zu bewältigen. Gerade dieser Zweig der Technik weist uns dabei gleichzeitig auch auf einen anderen Grund für die Aktualisierung der Sicherheitsfrage hin: Während bisher die Technik weitgehend nur den Fachleuten überlassen wurde, wird vermehrt wieder nach einem Einbezug der Technik in die übergeordneten sozialen und psychischen Kategorien gestrebt. Sicherheit ist dabei ein besonders sensibles Thema.

Bedeutsam an dieser Entwicklung ist vor allem, dass sich plötzlich auch Nichttechniker mit dem Sicherheitsproblem befassen. Dabei treten sehr bald Verständigungsprobleme auf. Der Laie fragt: "Ist das überhaupt sicher?" Was soll ihm der Fachmann darauf antworten? Mit einem blossen "Ja" gibt sich der Frager kaum zufrieden.

Was sich hier vorerst als reines *Verständigungs*problem zu manifestieren schien, ist aber unterdessen zu einem massiven *Verständnis*problem geworden. "How safe is safe enough?" fragt man heute. Die Artikel zu diesem Thema häufen sich, Ideen werden aufgeworfen; die Antwort ist bis jetzt ausgeblieben.

Ein weiterer Grund für den Ruf nach einer besseren Klärung der Sicherheitsfrage sei hier aufgeführt. Trotz steigendem Wohlstand ist fast überall eine zunehmende Verknappung der öffentlichen Finanzmittel festzustellen. Dies bedeutet, dass auch für Sicherheit, selbst wenn sie an sich ein unbestrittenes Anliegen darstellt, nicht unbeschränkt Mittel zur Verfügung stehen. Umso mehr müssen wir uns die Frage stellen, wie wir die verfügbaren Mittel am besten einsetzen können. Dazu müssen wir aber die Wirksamkeit und den Nutzen verschiedener möglicher Sicherheitsmassnahmen und Strategien überhaupt vergleichen können, was heute in den meisten Fällen erhebliche Schwierigkeiten bereitet.

Zusammenfassend stellt man fest, dass wir mit beschränkteren Mitteln immer komplexere Probleme zu lösen haben und gleichzeitig höhere Sicherheitsanforderungen erfüllen müssen. Dies kann wohl nur gelingen, wenn wir mit einer differenzierteren Betrachtungsweise an das Sicherheitsproblem herantreten.

1.2 Was tut sich auf dem Gebiet der Bauwerkssicherheit?

Fragen wir nach der Sicherheit im Bauwesen, so stellen wir vorerst folgendes fest: Zwischen der Sicherheit bei der Herstellung von Bauwerken und der Sicherheit fertiger Bauwerke besteht ein enormer Unterschied. In der Schweiz kommen heute noch jährlich nahezu 200 Beschäftigte im Bauwesen ums Leben, also rund einer von tausend. Hingegen wissen wir nicht einmal, wieviele Personen durch das Versagen fer-

tiger Bauwerke zu Schaden kommen, so klein ist ihre Zahl.

Bis heute stellen in den meisten Ländern Arbeitsunfälle offenbar kaum ein Thema dar, welches wissenschaftlicher Untersuchungen und Tagungen würdig ist. Im Gegensatz dazu hat sich bei Bauwerken das Streben nach absoluter Sicherheit weitgehend behauptet.

Nun, es gibt nur drei Möglichkeiten: Entweder sind unsere Bauwerke zu wenig sicher, gerade sicher genug oder zu sicher. Dabei müssen wir eigentlich zuerst fragen, ob überhaupt alle Bauwerke gleich sicher sind. Sollten sie alle gleich sicher sein? Bis heute sind unsere Sicherheitsanstrengungen vor allem darauf ausgerichtet, Mängel und Fehler auszumerzen. Andere Anstrengungen sollen uns bessere Modelle für das Verhalten von Tragwerken und Materialien liefern. Dies erlaubt uns, die Zuverlässigkeit unserer Berechnungen zu steigern und damit unter Umständen, den gleichen Tragwerkswiderstand unter Verwendung von weniger Material nachzuweisen. Ueber die Frage nach dem Ziel unserer Anstrengungen scheint jedenfalls so etwas wie ein stillschweigender Konsensus zu bestehen.

Seit etwas mehr als zwanzig Jahren hat sich eine zunehmende Zahl von Wissenschaftlern bemüht, der Sicherheit von Bauwerken etwas systematischer und rationaler nachzugehen. Den Ausgangspunkt bildete dabei die Feststellung, dass die Sicherheit eines Bauwerkes gar nicht mit Bestimmtheit vorausgesagt werden kann. Zahlreiche Grössen, welche für eine solche Voraussage bekannt sein müssten, lassen sich in Wirklichkeit nicht mit Bestimmtheit ermitteln, da sie einer unbeabsichtigten, zufälligen Streuung unterworfen sind. Sowohl die Eigenschaften von Materialien, die Abmessungen eines Bauwerkes, vor allem aber die zu erwartenden Belastungen sind von dieser Ungewissheit betroffen. Diese Ungewissheit in den Grunddaten der Bauwerksbemessung setzt sich fort bis in die Gesamtbeurteilung der Sicherheit.

Dementsprechend wurde versucht, durch geeignete mathematische Modelle, diese Grunddaten der Bemessung und die "Sicherheit" des Bauwerkes adäquater in Zusammenhang zu bringen. Wesentlich war es dabei, den Zufallscharakter all dieser Daten berücksichtigen zu können. Folgerichtig stiess man dabei schliesslich auf die Versagenswahrscheinlichkeit als Mass für die Sicherheit eines Bauwerkes. Damit stand gleichzeitig Sicherheit erstmals als messbare Grösse da.

Gegenüber Ansätzen dieser Art ist von vielen Seiten her Kritik geübt worden. Auf alle dabei vorgebrachten Argumente soll hier nicht eingegangen werden. Es scheint jedoch, dass in letzter Zeit die Bedeutung dieser Betrachtungsweise immer klarer gesehen wird. Dies betrifft einerseits die unbestreitbaren Vorteile und Einsichten, welche eine logische und systematische Betrachtungsweise mit sich bringt. Anderseits hat sich aber auch gezeigt, wo - zumindest heute noch - ihre Grenzen liegen. Als eine dieser Grenzen wird immer häufiger genannt, dass zwar der Bemessungsvorgang von Tragwerken durch diese Modelle einigermassen sinnvoll erfasst wird, dass dabei aber eines der Hauptprobleme der Bauwerksicherheit unberücksichtigt bleibt: Die menschlichen Fehler bei der Planung und Ausführung von Bauwerken.

Auf dieses Problem soll hier nicht näher eingegangen werden. Die nachfolgenden Beiträge werden sich eingehender damit beschäftigen. Immerhin sei erwähnt, dass mit dieser Kritik nicht ein grundsätzlicher Mangel statistischer Betrachtungsweisen aufgedeckt wird. Hingegen muss wohl eingestanden werden, dass die entsprechenden Modelle bis heute zu eng gefasst sind.

1.3 Ziel dieses Beitrages

Der vorliegende Beitrag versucht das Sicherheitsproblem von einer ganz anderen Seite her anzugehen. Wir wollen hier nicht nach Mitteln und Massnahmen zur Verbesserung der Sicherheit fragen. Dem Laien ist es letzten Endes gleich, mit welchen Mitteln wir die Sicherheit von Bauwerken erreichen. Er fragt nur, wie sicher Bauwerke sind und ob sie sicher genug sind.

Alle heute verfügbaren Modelle zur Beschreibung der Sicherheit von Bauwerken durch quantitative Grössen wie z.B. Wahrscheinlichkeiten, liefern zwar eine wichtige Grundlage für die Beurteilung der Sicherheit, bilden uns aber nicht die Antwort auf die Frage des Laien. Wir wissen zwar damit, mit welchen Grössen "Sicherheit" beschrieben werden kann, können Versagenswahrscheinlichkeiten ermitteln; was aber "sicher" heisst, wissen wir damit immer noch nicht. Dieses Problem soll im folgenden näher diskutiert werden.

2. WAS IST SICHERHEIT ?

2.1 Müssen wir diese Frage stellen ?

Es mag provokativ klingen, wenn wir die Frage "Was ist überhaupt Sicherheit?" gerade im Zusammenhang mit Bauwerken stellen. Kaum ein anderer Bereich der Technik kann auf eine derart lange Erfahrung zurückblicken und sich rühmen, durch seine Werke in fast symbolhafter Weise Sicherheit zu verkörpern.

Die ganze bisherige Entwicklung im Bauwesen hat sich abgespielt, ohne dass eine explizite Antwort auf die Sicherheitsfrage gegeben wurde. Ständig verbesserte Kenntnisse der physikalischen Zusammenhänge, Erfahrung und Beurteilungskraft der Ingenieure sowie die Wechselwirkung zwischen Fachleuten, Bauherren, Benützern und der allgemeinen Oeffentlichkeit waren bestimmend für die Festlegung von Regeln und Massstäben, nach denen Bauwerke erstellt wurden.

Ist all dies heute in Frage gestellt? Sicher nicht! Aber die Frage, ob es in jedem Fall noch genügt, wird man sich heute stellen müssen. Im Bauwesen ist die Entwicklung zwar auch in den letzten Jahrzehnten nicht so stürmisch verlaufen wie in manch anderem Bereich der Technik. Dennoch sind wir auch hier mit zahlreichen Neuerungen konfrontiert worden: Neue Materialien, neue Konstruktions- und Bauweisen lassen sich nicht mehr alle ohne weiteres in den bisherigen Erfahrungsbereich einreihen. Wie soll hier über die notwendigen Regeln und Anforderungen entschieden werden?

Unser traditionelles Sicherheitsdenken stösst aber auch dort an seine Grenzen, wo Bauwerke immer mehr nur noch Komponenten grösserer, umfassenderer technischer Systeme darstellen. Dies trifft nicht nur im Energiebereich zu, wo Kernkraftwerke, Oel- und Gasgewinnungsanlagen (vor allem "off-shore"-Anlagen) die Einpassung baulicher Elemente in ein Gesamtkonzept erfordern. Auch in der übrigen Industrie ist man mit immer grösseren Gefahrenpotentialen konfrontiert, denen man nur mit wohlabgestimmten Sicherheitskonzepten begegnen kann. Diese Aufgaben können nicht ohne interdisziplinäre Zusammenarbeit verschiedenster Bereiche der Technik bewältigt werden. Verfügen aber diese verschiedenen Fachleute über die gemeinsame Sprache und genügend klare Sicherheitsvorstellungen für ihre Zusammenarbeit? Wer ist heute in der Lage, die Sicherheit solcher Anlagen gesamthaft zu überblicken und liefert uns daraus die Anforderungen an die baulichen Komponenten?

Ein besonderes Problem stellen dabei in zunehmendem Masse Gefahren dar, deren Potential zwar sehr gross ist, die Chance, dass dieses Potential zur Wirkung kommt, aber sehr gering ist. Hier sind neben Anlagen der Energiewirtschaft wieder Industrien zu nennen, welche mit ständig wachsenden Mengen gefährlichster Stoffe auch in unmittelbarer Umgebung grösster Ballungszentren arbeiten. Wer legt hier die Anforderungen fest? Auf welcher Basis? Die Erfahrung fehlt hier jedenfalls weitgehend, und es ist ja gerade unser Ziel, diese Erfahrungen nicht zu machen.

2.2 Wie beschreibt man Sicherheit ?

Stellen wir uns wiederum auf den Standpunkt des Laien. Wie manifestiert sich für ihn Sicherheit? Wohl kaum in Spannungen, Faktoren oder Materialstärken. Der Laie kann nur erkennen, ob ein Bauwerk Schäden erzeugt oder nicht! Für ihn ist Schadenfreiheit Sicherheit. Das Auftreten von Schäden oder die Prognose möglicher Schäden ist also die entscheidende Basis für die Sicherheitsfrage.

Es gibt selbstverständlich viele Arten von Schäden, welche Bauwerke oder andere technische Systeme erzeugen können. Man kann diese Schadenarten z.B. grob in die Kategorien "Sach- oder Personenschäden" sowie "reparabel oder irreparabel" einteilen. Zu den irreparablen Sachschäden wären dabei z.B. Umweltschäden oder Schäden an Kulturgütern zu zählen. Wenn von Sicherheit die Rede ist, steht aber vor allem der Schutz von Leib und Leben von Personen im Vordergrund. Im folgenden soll deshalb nur von tödlichen Unfällen die Rede sein. Für alle anderen Schadenkategorien können analoge Ueberlegungen gemacht werden.

Betrachtet man irgend ein technisches System ganz aus der Sicht der Personengefährdung, so lässt sich diese an sich recht einfach beschreiben (Figur 1): Für jede potentiell betroffene Person ist ihre Gefährdung vollumfänglich durch die Wahrscheinlichkeit beschrieben, durch dieses System tödlich zu verunfallen. Dieses sogenannte *individuelle Risiko* kann dabei auf ein Jahr, die ganze Lebensdauer oder eine andere Grösse bezogen werden. Für die Sicherheit eines Einzelnen ist es an sich irrelevant, wieviel andere Personen in welchem Masse gleichzeitig gefährdet sind.

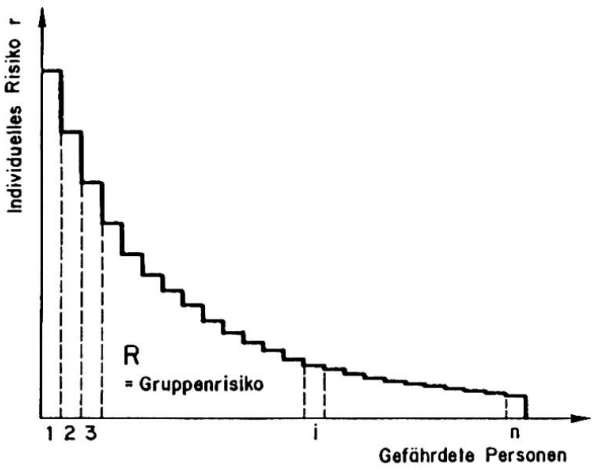

Fig. 1

Ein System erzeugt in der Regel verschiedene individuelle Risiken für die einzelnen gefährdeten Personen. Die Summe dieser individuellen Risiken ergibt das Gruppenrisiko, also die gesamthaft zu erwartende Anzahl Opfer. Diese Zahl finden wir in der Unfallstatistik.

Trägt man das individuelle Risiko aller Betroffenen, wie in Figur 1 dargestellt, auf, so erkennt man eine zweite Risikogrösse: Die Fläche, welche so entsteht, wird oft als *Gruppenrisiko* bezeichnet. Sie gibt an, wie gross das Personenrisiko dieses Systems gesamthaft ist und entspricht der Grösse, welche in unseren Unfallstatistiken auftritt. Solche Statistiken geben ja in der Regel nur an, wieviele Opfer eine bestimmte Aktivität als ganzes erzeugt, ohne zu sagen, wie dieses Risiko über die Beteiligten verteilt ist.

Das Gruppenrisiko kann übrigens auch auf andere Weise als durch die Summation der individuellen Risiken berechnet werden: Wenn wir alle möglichen Schadenereignisse j in einem System definieren, anschliessend deren Wahrscheinlichkeit w_j sowie die Anzahl Opfer A_j im Ereignisfall ermitteln und diese miteinander multiplizieren resp. addieren, so erhalten wir genau dieses Gruppenrisiko ($\sum w_j \cdot A_j$).*

Zusammenfassend seien die beiden soeben beschriebenen Risikogrössen hier nochmals in symbolischer Schreibweise festgehalten. Vereinfachend sei dabei von einem System ausgegangen, in welchem nur ein einziges Schadenereignis zur Diskussion stehe.

Individuelles Risiko einer Person i : $r_i = w_V \cdot w_{Pi}$

Gruppenrisiko über alle Personen* : $R = \sum_i r_i = \sum_i w_V \cdot w_{Pi} = w_V \cdot A$

w_V = Ereigniswahrscheinlichkeit

w_{Pi} = Wahrscheinlichkeit, dass Person P_i beim Ereignis anwesend ist

A = mittlere Anzahl Opfer im Ereignisfall

Welche dieser beiden Grössen ist nun massgebend für die Sicherheit? In welcher Beziehung stehen diese Grössen zu dem, was wir uns bisher unter der Sicherheit von Bauwerken vorgestellt haben? Auf diese Fragen soll später zurückgekommen werden.

2.3 Zum Nutzen von Sicherheitsmassnahmen

Die Definition des Sicherheitsbegriffes ist selbstverständlich eng mit der Beurteilung des Nutzens von Massnahmen verknüpft. Definieren wir Sicherheit durch Schadenrisiken, so ist es klar, dass der Nutzen von Sicherheitsmassnahmen sich durch eine entsprechende Reduktion des Schadenrisikos ergibt.

Für Personenrisiken lässt sich die Frage nach dem Nutzen von Sicherheitsmassnahmen besonders prägnant ausdrücken: Wieviele Personen werden durch eine bestimmte Massnahme gerettet? Diese klare und unausweichliche Frage mag uns in dieser allgemeinen Form vielleicht befremden. Stellen wir uns aber vor, wir hätten zwei verschiedene Sicherheitsmassnahmen (oder Normenwerke!) gegeneinander abzuwägen: Ist dies dann nicht die Grundfrage, die wir uns stellen sollten?

Wie sieht dies nun bei der Planung und Festlegung von Sicherheitsmassnahmen aus? Betrachten wir dazu den Fall eines bestimmten Bauwerktypes und stellen uns die Frage, welche Verbesserungen der Sicherheit möglich bzw. notwendig sind. In Figur 2 sei auf der Ordinate der Graphik das Gruppenrisiko eines solchen Bauwerkes aufgetragen, auf der Abszisse hingegen die Kosten verschiedener möglicher Sicherheitsmassnahmen. Diese möglichen Massnahmen sind dabei so geordnet, dass das Verhältnis zwischen Risikoabminderung und Kosten kontinuierlich abnimmt.

*Es muss hier der Vollständigkeit halber angedeutet werden, dass mit dieser Definition des Gruppenrisikos ein Effekt vernachlässigt wird, der in der Realität nachweislich auftritt. Ob nämlich jede Person in Figur 2 einzeln gefährdet ist, oder ob mehrere Personen gleichzeitig durch ein Ereignis betroffen werden, wird im allgemeinen nicht gleich beurteilt. Dieser Effekt, welcher in der formalen Entscheidungstheorie als Risikoaversion bezeichnet wird, ist unbedingt zu beachten, soll aber hier nicht weiter diskutiert werden.

Das Gruppenrisiko von Bauwerken fällt bei gleicher Versagenswahrscheinlichkeit ebenfalls sehr unterschiedlich aus. Zusätzlich zur Versagenswahrscheinlichkeit des einzelnen Bauwerkes kommt hier die Anzahl Bauwerke dieses Types ins Spiel, sowie die mittlere Zahl der anwesenden Personen.*

Es hat sich bei der praktischen Anwendung solcher Ueberlegungen in verschiedenen anderen Bereichen gezeigt, dass sowohl das individuelle Risiko der einzelnen Betroffenen zu beachten ist als auch der zu erwartende Gesamtschaden, d.h. das Gruppenrisiko. Aufgrund von Figur 1 ist dies auch plausibel, da ja die Fläche unter der Kurve unabhängig von der Form dieser Fläche ist.

Tabelle 1 zeigt eine Gegenüberstellung von individuellen und Gruppenrisiken ververschiedener Aktivitäten. Man erkennt, dass diese beiden Grössen keineswegs parallel zueinander verlaufen.

Arbeitsgattung	Tote/Jahr über alle Vollbeschäftigten = Gruppenrisiko	Tote/1000 Vollbeschäftigte und Jahr = mittl. indiv. Risiko
- Holzfällen und Holztransport	2	6
- Engeres Baugewerbe	204	1
- Chemische Industrie	17	0.3
- Fabrikm. Metallbearbeitung	10	0.1
- Kaufm. und techn. Büros	16	0.05

Tab.1 Vergleich von individuellen und Gruppenrisiken in der Schweiz

Es ist nun anderseits selbstverständlich, dass beide Risikogrössen abnehmen, wenn die Wahrscheinlichkeit von Schadenereignissen reduziert wird. Sowohl das individuelle Risiko als auch das Gruppenrisiko können also durch die Versagenswahrscheinlichkeit gesteuert und auf beliebig kleine Werte gebracht werden. Wozu also noch diese Grössen beachten?

Die Steuerung der Sicherheit über die Ereigniswahrscheinlichkeit allein ist ausserordentlich undifferenziert. Sie führt aus der Sicht der effektiven Sicherheitsgrössen zu einem unausgewogenen Resultat. Einer konstanten Verteilung der Versagenswahrscheinlichkeit aller Bauwerke entspricht nämlich eine sehr stark streuende Verteilung der erwähnten Risikogrössen. Spielt dies aber eine Rolle solange wir die erforderliche Sicherheit erreichen?

Hierauf kann eine ganz klare Antwort gegeben werden: Solange es unwesentlich ist, wieviel Geld wir für Sicherheit ausgeben, ist dies in der Tat nicht wichtig. Sobald wir aber fordern, dass die erforderliche Sicherheit mit minimalem Aufwand erreicht werden soll, stehen wir hier vor einem entscheidenden Punkt. Noch deutlicher ist vielleicht die Aussage, dass wir mit den heute eingesetzten Mitteln nicht die maximal mögliche Sicherheit erreichen, wenn wir die Versagenswahrscheinlichkeit als Mass für die Sicherheit nehmen.

* Bei Einführung einer Aversion gemäss Fussnote in Abschnitt 2.2 ist auch die maximal mögliche Zahl exponierter Personen von Bedeutung.

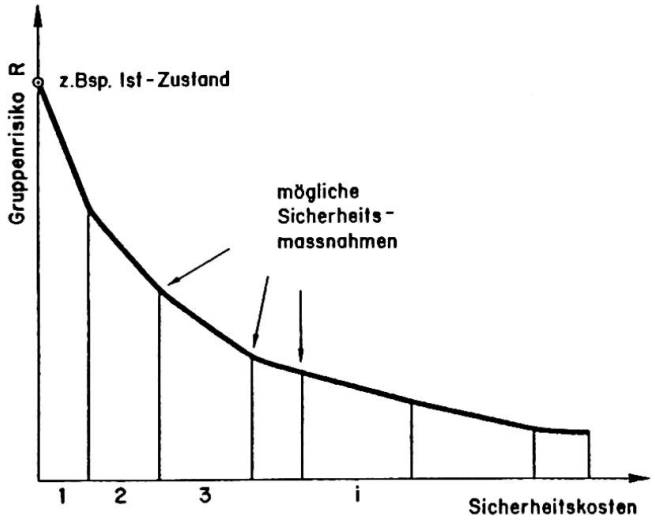

Fig. 2

Jedes technische System kann vom bestehenden Zustand oder irgend einem Ausgangspunkt aus durch mehr Aufwand für Massnahmen sicherer gemacht werden. Ordnet man die Massnahmen nach ihrer Effizienz, so erhält man eine Kurve wie nebenstehend gezeigt.

Es ist nun typisch für jedes technische System, dass man mit zunehmendem Aufwand die Sicherheit immer weiter steigern kann. Dabei werden aber immer unwahrscheinlichere Ereignisse abgedeckt und der Aufwand für eine weitere Risikoreduktion wird immer grösser. Schliesslich zeigt sich auch die bekannte Tatsache, dass das Risiko solcher Systeme nie null sein wird. Dass wir absolute Sicherheit nicht als Massstab nehmen können, ist damit klar. Für jeden aber wird, wenn er dieser Kurve entlang die Sicherheit eines Systems verbessert, einmal der Punkt kommen, wo er sich fragt: Lohnt es sich noch? Ist es noch gerechtfertigt mehr Geld auszugeben? Wo ist der Punkt, an dem das System sicher genug ist?

3. DIE BEURTEILUNG VON PERSONENRISIKEN

3.1 Beurteilung aufgrund der Versagenswahrscheinlichkeit

Alle systematischen Ansätze, die Sicherheit von Bauwerken präziser zu erfassen, bringen direkt oder indirekt die Sicherheit mit der Versagenswahrscheinlichkeit des Bauwerkes in Verbindung. Wie weit dies auch für das traditionelle, implizite Sicherheitsdenken gilt, ist schwer zu beurteilen.

Gehen wir im folgenden davon aus, das Sicherheitsstreben bei Bauwerken sei im wesentlichen auf eine konstante Versagenswahrscheinlichkeit w_V ausgerichtet. Stellen wir nun diese Zielgrösse den beiden Begriffen des individuellen Risikos ($=w_V \cdot w_{P_i}$) und des Gruppenrisikos ($=w_V \cdot A$) gegenüber, so ist leicht einzusehen, dass bei konstantem w_V keiner dieser beiden Werte konstant für alle Bauwerke sein wird.

In einem Wohnhaus beispielsweise hält man sich verhältnismässig lange auf. Die Chance, dass die Bewohner beim Auftreten der kritischen Belastung anwesend sind, ist also gross. Die Versagenswahrscheinlichkeit liegt hier wohl nahe beim individuellen Risiko der Bewohner. Bei einer Brücke hingegen liegen die Verhältnisse ganz anders. Die Chance, dass ein bestimmtes Individium im Zeitpunkt eines allfälligen Einsturzes gerade anwesend ist, ist sehr gering. Das individuelle Risiko für einen Benützer dürfte also verschwindend klein sein, wenn die Versagenswahrscheinlichkeit der Brücke gleich gross wie diejenige des Wohnhauses ist.

3.2 Die Bewertung von Gruppenrisiken

Figur 2 zeigt deutlich, wie sich die Sicherheitsfrage auf der technisch-ökonomischen Ebene präsentiert. Davon ausgehend soll vorerst gefragt werden, wie ein Sicherheitskriterium überhaupt aussehen sollte.

Die häufigste Antwort auf diese Frage lautet wohl so: Die Kosten sind für die Festlegung der erforderlichen Sicherheit irrelevant. Es muss auf irgendeine Weise - z.B. durch Risikovergleiche - ein Wert für das akzeptierbare Risiko gefunden werden. Die erwähnte Kurve zeigt uns dann lediglich, wieviel es kostet, das Risiko auf diesen Wert zu reduzieren.

Diese Antwort scheint auf den ersten Blick zwar einleuchtend. Kommen wir aber so tatsächlich zur besten Lösung des Sicherheitsproblemes? Dass dies nicht der Fall ist, soll das Beispiel von Figur 3 andeuten. In dieser Figur werden drei Systeme betrachtet, wobei jedes durch seine Risiko-Kosten-Kurve charakterisiert ist. Auf der linken Seite der Figur wird ein reines Risikokriterium angewendet. Das akzeptierbare Risiko R* führt dabei zu Gesamtkosten K* für alle drei Systeme.

Man kann nun aber leicht zeigen, dass mit Kosten K* ein geringeres Risiko als 3R* erzielt werden kann. Die rechte Hälfte von Figur 3 deutet an, wie man bei Kosten K* das kleinste Restrisiko erhält. Die drei Lösungspunkte sind so zu wählen, dass alle drei Kurven in diesem Punkt die gleiche Neigung aufweisen. Dass dies so sein muss, lässt sich mathematisch leicht nachweisen.

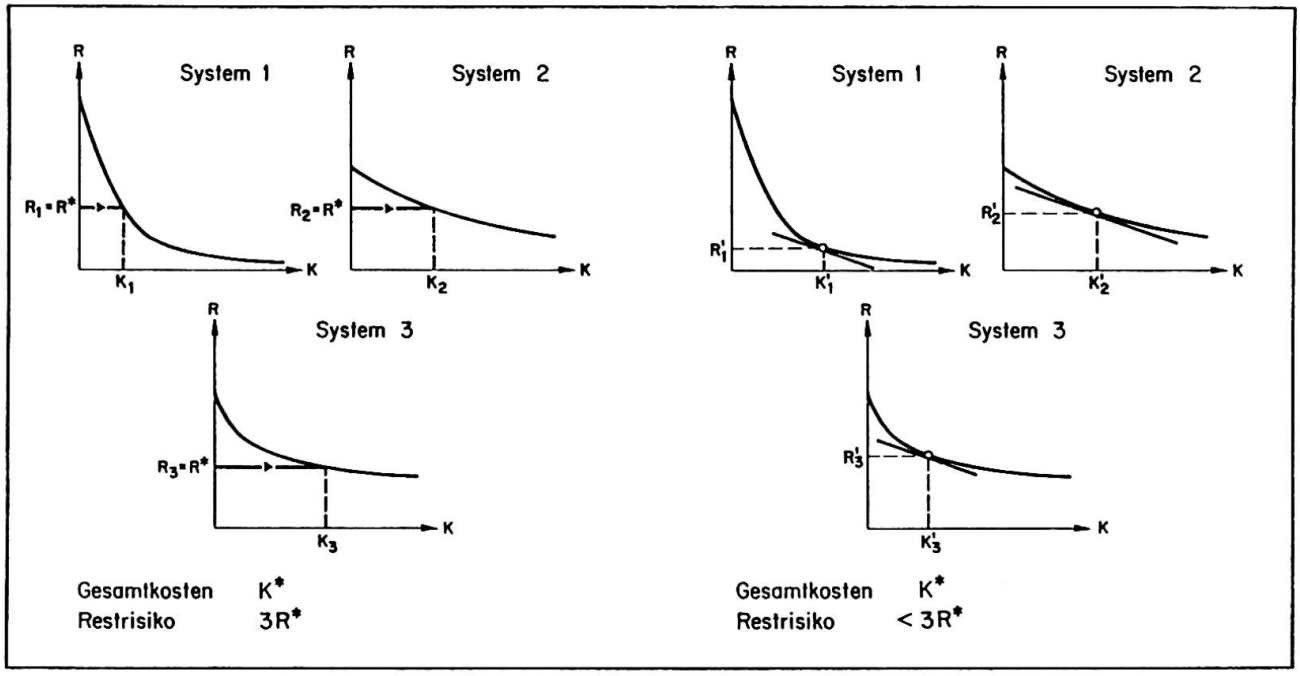

Fig. 3 Um in einer beliebigen Anzahl von Systemen für gegebene Gesamtkosten K* das kleinste Restrisiko zu erhalten, ist nicht ein Risikokriterium (links) sondern ein Grenzkostenkriterium (rechts) einzuführen

Was ist die konkrete Bedeutung eines solchen "Tangentenkriteriums"? In der Oekonomie spricht man von Grenzkosten oder marginalen Kosten und meint damit die Kosten, welche aufgebracht werden müssen, um den Nutzen einer Aktivität um einen Schritt zu steigern. Im Falle unseres Sicherheitsproblemes lässt sich dies ganz konkret ausdrücken: Es sind die Grenzkosten, welche wir für die Rettung eines Menschenlebens ausgeben.

Wer die Entwicklung allgemeiner Sicherheitsmodelle etwas eingehender verfolgt hat wird nun denken, dass wir damit wieder beim längst bekannten und oft angefochtenen Problem der ökonomischen Bewertung von Menschenleben angelangt sind. Dazu zwei Bemerkungen:

Vorerst ist festzuhalten, dass uns die Forderung nach optimalem Einsatz der verfügbaren Mittel zwangsweise zu diesem Grenzkostenkriterium führt. Ist dies aber nicht ein deutlicher Hinweis, dass man sich mit dieser Grösse auch inhaltlich eingehender befassen sollte?

Auf Widerstand ist aber die ökonomische Bewertung von Menschenleben vor allem aus einem anderen Grund gestossen. Immer wieder ist versucht worden, aufgrund versicherungstechnischer oder allgemeiner ökonomischer Ueberlegungen einen quasi objektiven Wert für ein Menschenleben zu berechnen. Davon wird hier klar Abstand genommen. Wieviel wir für die Rettung eines Menschenleben ausgeben wollen, ist ein rein subjektives Problem, eine Sache unserer Wertvorstellungen. Wir stehen hier vor einer ähnlichen Frage, wie wenn wir entscheiden müssen, wieviel wir für unsere Landesverteidigung ausgeben sollen, wieviel für das Gesundheitswesen, die Schulen etc.

Zu erläutern wie man zur Festlegung eines solchen subjektiven Wertes für ein Menschenleben kommen kann, würde hier zu weit führen. Immerhin sei als Hinweis erläutert, dass jeder Entscheid über eine bestimmte technische Lösung für ein Sicherheitsproblem implizite eine Festlegung dieses Wertes beinhaltet; nur wissen wir dabei normalerweise nicht wie gross der gewählte Wert ist.

Akzeptiert man die Grenzkosten für die Rettung eines Menschenlebens grundsätzlich als Sicherheitskriterium, so bleibt immer noch eine Frage offen: Soll dieses Kriterium für alle Aktivitäten denselben Wert annehmen? Ein Blick auf die heutige Realität zeigt deutlich, dass wir offenbar nicht bereit sind, überall die selben Sicherheitsanstrengungen zu machen. Längst ist es z.B. bekannt, dass freiwillig höhere Risiken eingegangen werden, als wenn uns Risiken auferlegt werden - und zwar bis zu einem Faktor Tausend.

Allerdings kann es kaum gelingen, die Vielfalt aller zivilisatorischen Tätigkeiten nur nach den Kategorien "freiwillig" und "unfreiwillig" zu unterscheiden. Es sei im folgenden nur andeutungsweise ein Beurteilungsmodell vorgestellt, wie es seit einigen Jahren im Zusammenhang mit der Planung explosionsgefährlicher Anlagen entwickelt und angewendet worden ist. Figur 4 zeigt, dass dabei vorerst vier Hauptkategorien von Risiken gebildet worden sind. Als Unterscheidungsmerkmale wurde das Verhältnis zwischen den

- Betroffenen (durch die Risiken einer Aktivität)
- Beteiligten (an der Aktivität und damit auch Nutzniesser)
- Verantwortlichen (für die Sicherheit der Aktivität)

eingeführt. Weitere Parameter innerhalb der einzelnen Hauptkategorien sind in Figur 4 angedeutet. Die quantitative Festlegung der Kurve in dieser Figur beruht auf einer Auswertung zahlreicher theoretischer Studien, aber auch Fallstudien zu diesem Thema.

Das Diagramm ist so zu verwenden, dass eine Aktivität vorerst einer Risikokategorie zuzuteilen ist. Der dazugehörige Grenzkostenwert bildet das gesuchte "Tangentenkriterium", wie es in Figur 3 diskutiert wurde. Bauwerke gehören entsprechend ihrem Zweck in verschiedene Kategorien. Ein Schwergewicht liegt aber sicher beim Uebergang zwischen den Kategorien 3 und 4.

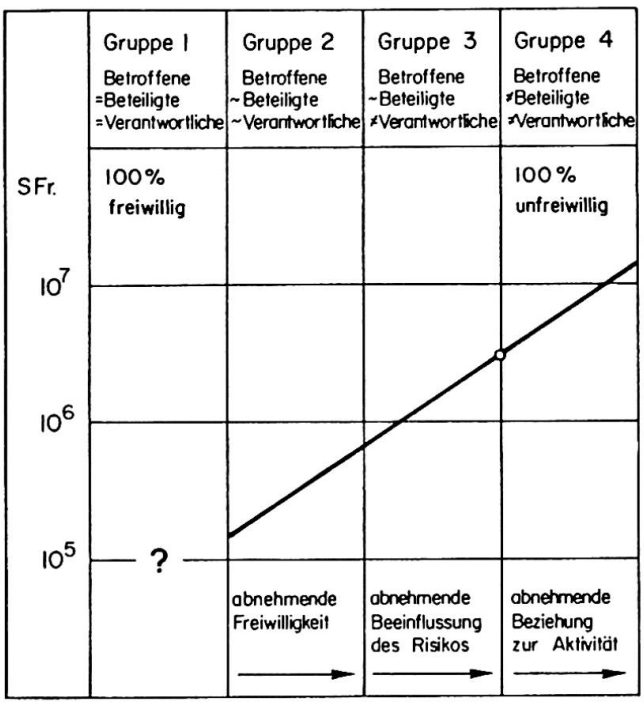

Fig. 4 Grenzkostenkriterium für das Gruppenrisiko (= Kosten pro gerettetes Menschenleben)

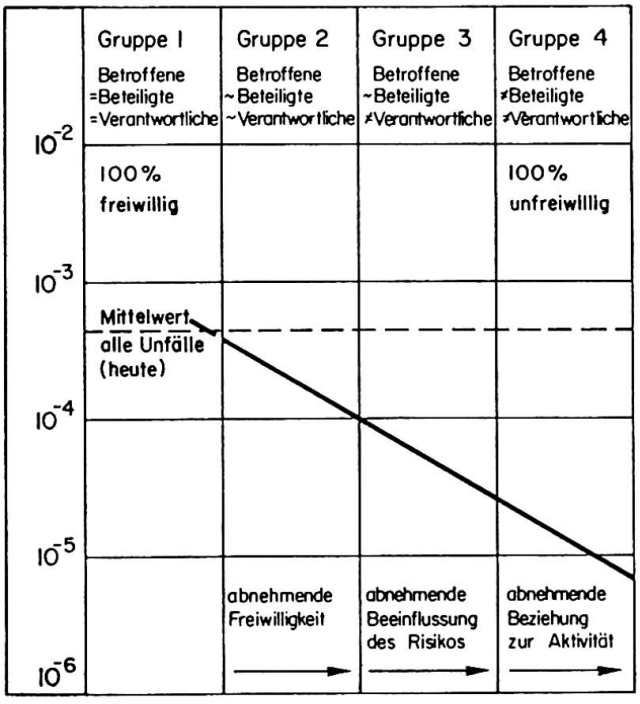

Fig. 5 Risikogrenze für das individuelle Risiko (=Wahrscheinlichkeit für tödlichen Unfall pro Jahr)

3.3 Die Bewertung von individuellen Risiken

Der wesentliche Unterschied zwischen der Bewertung von Gruppenrisiken und individuellen Risiken beruht auf folgender Tatsache: Bei Gruppenrisiken besteht das Ziel in der Rettung möglichst vieler Personen für die eingesetzten Mittel; die Zahl in der Unfallstatistik soll möglichst klein werden. Daraus ergibt sich, dass die Mittel dort einzusetzen sind, wo sie am meisten Nutzen abwerfen. Für das Risiko eines Einzelnen sieht dies aber anders aus: Die Person A wird für sich kaum ein höheres individuelles Risiko akzeptieren, nur weil es billiger ist, das individuelle Risiko von Person B zu reduzieren.

Im Gegensatz zu vorher stellt sich hier nun also tatsächlich die Frage nach einem akzeptierbaren Risiko. Für die Beurteilung dieses Problems hilft ein Blick auf die heute vorhandenen individuellen Risiken. Mittlere individuelle Risiken für verschiedene Aktivitäten lassen sich vergleichsweise einfach aus Unfallstatistiken ermitteln und sind schon in zahlreichen Publikationen zusammenfassend dargestellt worden. Auch hier dürften dabei wohl nicht alle Tätigkeiten mit einer Elle gemessen werden. Figur 5 zeigt hierzu einen analogen Vorschlag, wie ihn Figur 4 für das Gruppenrisiko darstellt.

Erwähnt sei hier, dass der Entwurf für eine Tragwerkssicherheitsnorm, welcher zur Zeit in der Schweiz bearbeitet wird, folgende Richtwerte für die Sicherheit von Tragwerken festhält:

- für die Beschäftigten im Bauwesen (nur infolge Tragwerksversagen im Bauzustand, also nicht alle Bauunfälle!) 10^{-4} pro Jahr
- für die allgemeine Bevölkerung (nur infolge Tragwerksversagen, also nicht alle Unfälle in und um Bauwerke) 10^{-6} pro Jahr

Mit diesen Werten wird erstmals versucht, eine Zielvorstellung zu formulieren, wie sicher Tragwerke für die Benützer und Ersteller sein sollten.

4. SCHLUSSBEMERKUNGEN

Die Kluft zwischen den hier dargelegten Ueberlegungen und dem, was normalerweise im Rahmen der Bauwerkssicherheit diskutiert wird, mag ziemlich gross erscheinen. Man wird sich dabei automatisch fragen, ob es überhaupt gelingen kann, eine Brükke zwischen diesen allgemeinen Ueberlegungen und den Ueberlegungen auf der rein technischen Ebene zu schlagen.

Schadenwirkungen und Sicherheitskosten sind aber diejenigen Grössen innerhalb des ganzen Sicherheitsproblemes, welche sich letztlich in der Realität manifestieren. Man tendiert aber dennoch dazu, diese Ueberlegungen als abstrakt zu bezeichnen. Sollten wir uns aber nicht vielmehr vermehrt vor Augen halten, wie wirklichkeitsfremd oft unsere Modelle auf der technischen Ebene sind?

In einem Sicherheitsdenken, das von den tatsächlich möglichen Ereignissen ausgeht, deren Wahrscheinlichkeit und Auswirkung als Basis nimmt und Massnahmen nach ihrer schadenmindernden Wirkung beurteilt, kann jedes Sicherheitsproblem erfasst werden. Alle Sicherheitsprobleme der Technik haben hier ihre gemeinsame Basis. Ist es aber nicht notwendig, dass Sicherheit nicht mehr nur als lästiges Nebenproblem vieler einzelner Aktivitäten betrachtet wird? Ist "life saving" nicht ein Bereich, der es verdient, für sich selbst einmal konzeptionell durchdrungen zu werden? Wessen Aufgabe wäre dies?

Sicherheit ist letztlich eine Frage der Wertvorstellungen unserer Gesellschaft. Diese können nicht berechnet werden, sondern kommen nur in einem langfristigen Entwicklungsprozess zum Ausdruck. Vielen Aktivitäten fehlt dieser langfristige Prozess. Sicherheit im Energiesektor ist daher zu einem Tappen im Dunkeln geworden. Wer aber könnte die notwendigen Erfahrungen für die Bewertung von Sicherheit besser liefern als die traditionellen Tätigkeiten der Technik, wie z.B. das Bauwesen? Ein solcher Erfahrungsaustausch ist aber ohne einheitliche Betrachtungsweise gar nicht möglich.

Dürfen wir uns aber selber im Bauwesen wegen unserer langen Erfahrung als erhaben über all diese Fragen betrachten? Viele Baufachleute, z.B. aus dem Wohnungsbau, wundern sich vielleicht, dass man sich überhaupt solange über die Sicherheitsfrage aufhalten kann. Für sie sind wohl meistens ganz andere Faktoren als die Versagenswahrscheinlichkeit des Bauwerkes für die Bemessung massgebend. Aber die Probleme liegen wohl nicht in allen Bereichen des Bauwesens gleich. Es gibt jedenfalls auch eine ganze Reihe von Ingenieuren, die mit ihren Bauaufgaben an oder gar über die Grenzen unserer abgesicherten Erfahrungen gestossen sind.

Abschliessend möchte ich aber provokativ noch eine andere Frage stellen: Sind nicht gewisse Bauwerke vielleicht auch zu sicher? Dürfen wir finanzielle Mittel beanspruchen, die anderswo einen viel grösseren Nutzen bringen würden? Wer aber überblickt dies überhaupt? Sollten wir diesen grösseren Ueberblick nicht anstreben?

Fragen, Fragen! Dieser Einführungsbericht stellt unzählige Fragen. Ich hoffe, dass in Wien auf einige dieser vielen Fragen Antworten gegeben werden.

Xb

Risk Management — The Realization of Safety

Gestion des risques — réalisation de la sécurité

Risikobehandlung — die Verwirklichung von Sicherheit

CARSTEN BØE
Dr. Eng.
The Royal Norwegian Council for Scientific and Industrial Research
Oslo, Norway

SUMMARY
This report reviews major problem areas in safety concepts related to management of risks and realization of safety targets in practice. In particular the lack of overall safety assessment and attention to human error is pointed out.

RESUME
Ce rapport examine les aspects problématiques des concepts de sécurité relatifs à la gestion des risques et les moyens mis en oeuvre pour atteindre ces objectifs de sécurité. L'absence d'une conception globale de la sécurité est soulignée ainsi que l'attention à porter aux erreurs humaines.

ZUSAMMENFASSUNG
Dieser Bericht überblickt die grösseren Problemgebiete der Sicherheitsbegriffe, die mit der Risikobehandlung und Verwirklichung von Sicherheitszielen zu tun haben. Insbesondere wird auf den Mangel sowohl vom gesamten Sicherheitskonzept wie auch auf menschliches Versagen hingewiesen.

1. INTRODUCTION

Risks have emerged as real constraints to the introduction and development of new technology. This has happened in many fields of engineering. It will happen again in the future.

For several years now engineers have been asked - and sometimes forced - to consider risks related to design in a wider perspective than before. In this respect the engineering profession is changing. There is a mounting pressure from public authorities, and sometimes the general public itself, that risks be taken into account whenever a new installation is conceived and put into operation. In some instances the pressure becomes a demand for all conceivable risks to be controlled. People also anticipate the standards of risk control to be immaculate.

This awakening of our surroundings to risks from technology means that every engineer may eventually find himself responsible for analysing or managing risks in some way. The engineer who has not prepared himself for that moment is going to have problems.

At the root of these problems is the lack of broad experience with risk management in traditional design engineering. Of course such experience will be different in different fields of engineering. Those who are used to reliability engineering and quality assurance work will find it easier to cope with safety problems in a systematic way. The time has now come to exchange experience in how to handle safety problems. A discussion is needed and may in time create a broad basis for knowledge and understanding of risk problems related to design.

The purpose of this report is to focus on this issue, to indicate current major problems and to raise questions which may eventually be answered.

2. THE LACK OF OVERALL SAFETY ASSESSMENT

One of the biggest problems an engineer may run into is the question *'Is this installation safe ?'* Such questions are very difficult to answer for two specific reasons. Firstly, because the question in itself is imprecise and put forward in a language that the engineer does not normally speak. Secondly, because the question comprises the installation as a whole and not only the part for which there are design codes or where some detailed risk assessments have been made. The question, however, deserves a good answer and it deserves a precise answer. It is impossible to address this question, however, without considering some kind of overall safety assessment of the design as a whole.

The lack of overall safety assessment for any installation is a basic problem in engineering. It should really be interesting to know why. Perhaps the main reason is the fragmentary way professional responsibilities are taken care of in the design process? However, in this context the following two statements are important:

- Once a design solution or operational procedure has been decided on and is implemented, the composite installation and its operation represent a level of risk to people, investments and environment which depend on the decisions made from conceptual design to the commissioning of the installation.

- This level of risk is present whether it is analysed or not, whether it is ignored or not, and it is an attribute similar to structural strength or production capacity which can be appraised, changed and controlled.

So the starting point for any discussion on overall safety assessment will be the basic, superior safety requirements which are present at the outset of the design process. The starting point must also include the practical limitations in terms of people, nature and money which exist as boundaries to the actual solution of the design problem. These limitations and overriding requirements have clear and direct consequences for the risk control actions which are to be realized. Furthermore, every decision taken during the design and construction phases limit the scope and contents of the risk control actions.

Figure 1 is an attempt to illustrate how risk control depends on selection, choices and basic requirements. It really describes a risk management process.

In figure 1 there is an unbroken connection between the elements at the top and at the bottom of the figure. The important thing to remember is that every decision taken add to the boundaries on eventual risk control actions which have to be put into force to make the installation meet safety requirements. This is very easily forgotten.

One example of a crucial decision is the selection of a design alternative to be realized. Very often the selection is made according to economic criteria only. Later on one may discover that "*if you want economy, you've got to pay for it*". This happens when practical realities of risk control actions suffuse the design problem and it is discovered that another design alternative was really the better choice. One wonders whether or not for instance the North Sea offshore oil activities are filled with such discoveries. Perhaps the same wondering ought to apply to dam construction or bridge design sometimes?

There is another reason for why the selection of a design alternative is so important. Inherent to every design alternative is the range of risks which have to be controlled and those which one cannot control or does not wish to control. The latter risks are called residual risks. Once a particular design alternative has been chosen, one has also selected a specific range of risks which are to be controlled and a range of residual risks which are impossible or too costly to control. The residual risks one has to live with, and at least they have to comply with the superior safety requirements given at the outset. This is also easily forgotten and sometimes calls for grand mistakes.

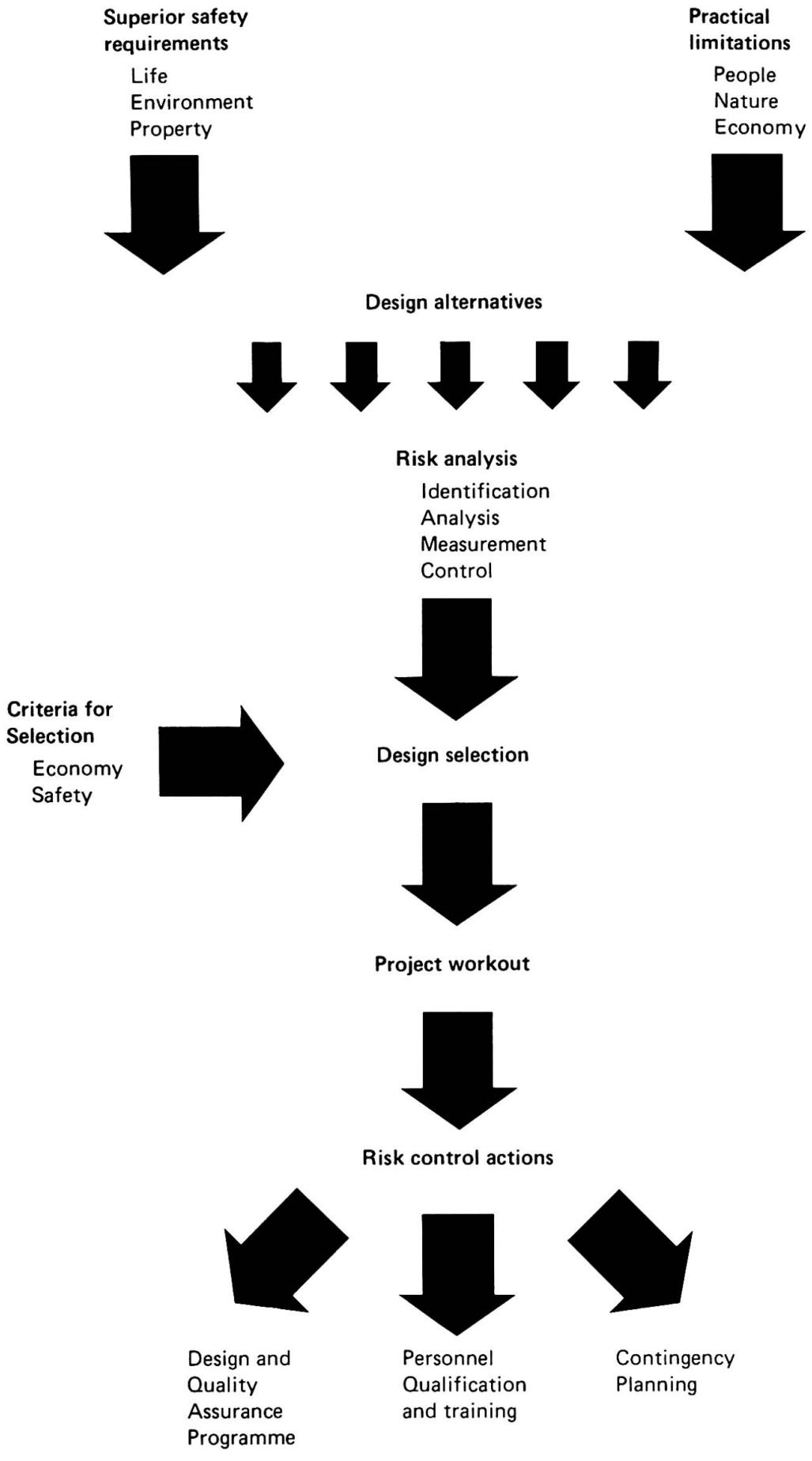

Fig. 1. Risk management process

3. THE IMPORTANCE OF THE CONCEPTUAL STAGE RISK ANALYSIS

To obtain some initial idea of what the overall safety of the different design alternatives may look like, a risk analysis at the very conceptual stage of a design is necessary. Such a conceptual stage risk analysis consists of a broad hazard identification at system level with corresponding analysis and assessment of the major risks to be found for each of the particular design alternatives. The result of this preliminary risk analysis will assist in deciding which risks are to be considered controllable risks and which are to be considered residual risks.

Very little statistical data are required in the conceptual stage risk analysis. The important thing to remember at this stage is that qualitative evaluation of the hazard spectrum is a necessary data base for deciding between residual and controllable risks for each particular design alternative.

It is of course important that the conceptual stage risk analysis is performed when the design is still at the conceptual stage. Then the alternative solutions may be assessed on an overall basis without serious economic consequences to the design project. The first stage risk analysis covers items such as preliminary main layout of the installation, simplified process diagrams, the initial planning of the various construction phases and preliminary outline of operational procedures and their limitations. One should be especially aware of basic design attributes where safety and economy may come into conflict. This allows for trade-offs to be performed at the earliest possible stages of the design.

One should also be aware that such a conceptual stage risk analysis cannot be performed without having a proper risk management organization. However, the experience with overall safety assessment is very small indeed and is found in very limited fields of engineering. A broader base of experience should be found and discussed. One will probably discover that both theoretical work as well as careful analysis of practical applications are required.

4. QUESTIONS RELATED TO RISK CONTROL

Anyone who is tempted to answer 'yes' to the question whether a design is safe, should be prepared to answer further questions related to risk control. Risk control actions are the necessary instruments actually put into force to ensure a certain level of safety. In practice risk control actions easily become ineffective and empty rituals because they are founded on wishful thinking or antediluvian codes - instead of realistic appreciations of actual risks from a design alternative. Realistic appreciations mean systematic risk control actions covering the full range of controllable risks based on causative patterns found in the results of risk analyses for a particular design.

Looking at the practice today, one is tempted to raise several questions. Firstly: *Why is the engineering design of a complex installation so totally independent of the design of the organization which is to run and maintain it ?* In practice there is a big gap between design engineers and those with experience in operating the installations being designed. In some areas this gap is more prominent than others. Perhaps those who

feel this gap to be very real and a hindrance to arrive at a proper design may learn something from those who have bridged this gap.

Another question: *Do codes in general lock design details to specific solutions which preferably instead should be tailored to meet the risks inherent to this particular design alternative ?* A new way to write codes might be to ask for risk assessments of a design. This has been attempted in some fields of engineering, but the experiences seem to be both good and bad.

Thirdly, the last question so far: *Why is the human being almost totally absent from the considerations on design and construction details ?* Too often one finds that the design has become so complex to maintain and operate that human errors seem to be built into the design. One should also give thought to the fact that the actual construction of a design is left to human beings for the most part. No matter how safe a design may look on the drawingboard, the finished product may end up as a quite different thing because the possibility of human error was forgotten. As a general statement it seems that design engineers have a poor understanding of human beings. After all the latter are responsible for operation and maintenance of the installation as well as all vital details in the construction phase.

5. THE HUMAN ERROR SYNDROME

In many areas of technology the basic element in the safety problem is found to be the confrontation between a very complicated technical and social system. After one or more accidents, public opinion creates a pressure on those responsible for something to be done. In such situations it is easy to take one specific problem, eliminate that particular risk and then believe that the causative pattern leading to the accident is broken. One also believes that overall safety has been increased.

In almost all cases one concentrates on concrete technical design problems. These are very easy to recognise: defect structure members, broken down machinery foundations, welding or material failures in piping, defect automation systems etc. By developing reliable technical components based on rigid codes, the risk that a technical failure can develop into a technical breakdown or catastrophy is diminished.

Of course this way of approaching things has a kind of logic of its own. By always increasing and developing technology the risks from technical design failures and defects will always diminish. However, the technical reliability sometimes can be so good that personal vigilance and the use of personal judgement of those operating and maintaining the installation can be deteriorated. It is possible to rely so much on the design of technical systems that one does not maintain the personal qualities of knowledge which are necessary to detect and control an unforeseen situation where the technical system has broken down, or more important, where it is about to break down.

Statistics and reports from the more serious accidents in industry tell us that human failure or lack of knowledge or experience are the main causes of accidents. This is of course only one part of the problem, but it illustrates that at the bottom of it all safety problems are based on human problems. It is difficult to give general recommendations of the human

aspects of safety because people are so different when it comes to abilities, precision, reactions, responsibility and many other qualities.

These difficulties make the study of human errors less exact and complete than studies of technical design failures. Something has nevertheless been learned through systematic studies of human behaviour in different situations. The most important is perhaps that human error is not subject to simple cause-effect relationships. In a hazardous situation many complicated and interactive events can be the consequences of a similar random pattern of events, which are called causes. Then to take one simple cause-effect relationship out of this complicated pattern may just as well serve to hide what actually happened in an accident as to tell the truth. In such undefined situations it is not easy to know what to do.

The thing one usually recommends to do is to emphasize development of safety routines and safety drills to promote selection and education, and of course to tighten responsibilities. This normally describes the extent of any risk control actions in practice today related to personnel. This approach may increase the vigilance and some of the personnel qualifications which are needed to cope with an abnormal situation. However, at the same time it may lead the attention and the actual safety work away from the technical conditions which were created on the drawingboard, and which may change by degree until they reach a point where there is no longer a balance between technology utilized and the human resources involved.

For instance, an installation may have reached such huge dimensions and the technical and physical chain reactions in a process may have become so fast that life saving equipment and contingency plans no longer are in balance with the rest of the technology creating the risks. This problem is well known in industry, offshore petroleum activities, shipping, and air transport.

6. THE ROLE OF EDUCATION AND TRAINING

When attacking the human error problem one may start at two different levels. The first level is the organisation. One may speak of an organisation with a safety conscious climate. An organisation with a safety conscious climate is an organisation which has the ability of internal self-regulation instead of relying on coordination and control from outside. This has the ultimate consequence that those who are concerned with safety, for instance those in the design department and those in the construction team, must work with safety themselves and also have influence and responsibilities in relation to their work.

The second level is the safe operator. He is easier to define than the organisation with a safety conscious climate. It can be done in a systematic way by stating the problem as two tasks:

- to minimize the probability of failure,

- to maximize the probability of correction when an error has occurred.

These two possiblities should be considered by every design engineer. However, there are two approaches to solve this problem. One is the philosophical approach where it is reasoned that no human being is perfect. This results in the belief that all human actions will be imperfect and it is human to fail. One anticipates that there will always be a component of failure in people, and that it sooner or later will show up.

The second approach is that of the ergonomist who tells that human error is caused by lack of adaptation between the abilities of the operator and the demands of the work situation. A human failure will occur when the relation between ability and demand is out of balance. The built-in potential for failure in all human beings is not released until a predisposing condition which creates unbalance acts as a catalyst to realise a potential failure.

This type of thinking has the advantage that - at least in theory - human errors can be completely eliminated simply by eliminating the predisposing condition. This is a challenging task for any design engineer, and current work on human failures and human engineering is performed at this level. The goal is to create the safe operator or the safe man-technology interface where human error can be tolerated. Over the years a lot has been learned in this field. Some of the problems with the safe operator are that too little of that knowledge is used in practice. Now is the time to share experience in this field.

The really difficult safety problem, however, is found at the organisational level. It is very important to solve the safety problem at the organisational level because the safety conscious climate in an organisation determines the possibilities for achieving the safe operator. This means that the simultaneous design of an installation and its operational organisation becomes very important.

Education and training are always necessary risk control actions in relation to human error. Especially important is to evaluate clearly the gap between the level of ability which can be achieved by selection and what is really needed to perform the work. It is also of vital importance to differentiate between training and education based on a complete understanding of the situation, and training based on fixed routines activated by external signals. One finds that in education it is difficult to differentiate between safety and professional matters. Very often a professionally first class work is also the best with regard to safety. However, how one chooses to approach the problem of education and training of people is not a random decision to be left to a personnel department. The approach to training and education should be determined after thorough appreciation of the risks involved with an installation and what kind of risk control measures one wants to take.

The role of education and training in risk control actions seems to be grossly underestimated.

7. SAFE ENOUGH - WHEN DO WE STOP ?

In all safety work one has to stop at some stage for many reasons. One reason is that total and absolute safety cannot ever be achieved for any design. The second is that there are limited amounts of money to be spent on safety evaluation, safety assessment, and improvement of safety. 'Safe enough' becomes a trade-off between what one can afford and what one can accept in terms of risk.

There are no ground rules for assessing how safe is safe enough. In spite of this the question of whether an installation is safe enough turns up every time safety is discussed. For some design details the answer may be found in codes. Codes may define the use of materials, construction procedures, design loads etc. To follow the code in some ways means that the design is safe enough. The codes very seldom give safety criteria for the installation as a whole. Therefore it is usually assumed that if the details are correct, and these are added up, the sum will be correct as well. Unfortunately, this is not the case, and it would be interesting to know how this dilemma has been solved in the various fields of engineering and at different levels of detail in the design of an installation.

Perhaps the only field where an attempt to arrive at an overall safety requirement has been made is the design of nuclear reactors. For reactors design and risk assessment procedures include not only hardware details of the design, but total considerations to the environment and people in the vicinity of the installation. Attempts have been made to quantify safety criteria for nuclear reactors of which perhaps the best known are the Farmer Criterion for radio-active releases and the subsequent site comparisons illustrated in two-dimensional risk diagrams.

8. CONCLUDING REMARKS - MAJOR PROBLEM AREAS

Looking back to Figure 1, it is admittedly difficult to envision a connection between 'superior safety requirements' and the practical realities of design work. It is not easy to be aware of social and political goals when one is struggling to meet with deadlines and codes. The main point in this report is that it really is difficult because risk management is an unknown word to most designers and design managers. Sooner or later, however, a design engineer will find that risk management tasks are put in front of him. Then he needs to know something about overall safety assessment and risk control actions. What is more, he is going to need a systematic way of doing safety work to ensure that a theoretical level of safety is really achieved in practice.

Safety conscious companies, authorities and political bodies have started to ask whether designs are safe. At present very few members of the engineering community can handle such questions.

If only to preserve the credibility of the engineering profession one should start to prepare oneself to answer questions on overall safety. Listening to those who have made attempts at answering is a very good start. Therefore we need exchange of experience and perhaps better education in this field.

The use of risk analysis as a basis for concrete risk control actions is at present a rare thing to find. It has been done, however, and the experiences so far seem to be very promising. The reasons for the scarce use of risk analysis are certainly plentiful. Some of the main reasons may be that this powerful tool is generally very little known, and that there is a belief that risk analysis is a complicated theoretical technique suitable for other people only. Experience with risk analysis, however, shows it to be an extremely flexible technique ranging from simple risk assessment to complicated analyses. Some people who have used risk analysis call it a scientific approach to common sense. The important thing is that the results are used to design risk control actions which are effective and to the point. How this is done ought to be common knowledge.

Human errors are given as causes to all kinds of accidents. However, it seems that too many people resign when it comes to take practical steps to avoid or ameliorate effects of human errors. The role of education and training seems to be grossly underestimated as a concrete risk control measure. Furthermore, design engineers do know too little about ergonomics, behaviour in stress situations, physiological attributes, the time people need to react, reversible failures, converging decision situations etc. This applies to the design work itself as well as construction and operation. Some fields in engineering have gained more experience than others in this respect. They should share their experiences and point out the practical 'tricks of trade' being used.

As one hundred percent safety can never be achieved, the question of how safe is enough always enters safety discussions at some point. Today, one can find several, quite different views on how this question should be handled. It is a field in rapid development. The interesting thing is that at present most of the development seems to follow a kind of trial and error pattern. One should expect that codes will play an important part in this development.

Xc

Safety, Building Codes and Human Reality

La sécurité, les codes de construction et la réalité humaine

Sicherheit, Baunormen und die menschliche Wirklichkeit

FRANZ KNOLL
Dr. Eng.
Roger Nicolet & Associates
Montréal, Canada

SUMMARY
This paper presents a review of the present state of advancement of structural safety concepts in research and practice, as seen by a practising design engineer. It describes the three levels of strategies which seem to emerge for the control of structural safety in civil engineering, including tools such as code design rules, the checking for human errors and the design to limit the scope of failure, should it occur.

RESUME
Cet article présente l'état actuel des connaissances – dans la recherche et dans la pratique – concernant la sécurité des structures, vu par un ingénieur projeteur. Trois stratégies contribuent à la sécurité des constructions de génie civil et comprennent des outils tels que les codes de construction, le contrôle de possibles erreurs humaines ainsi que la conception de structures pour le cas d'un effondrement éventuel.

ZUSAMMENFASSUNG
Der Beitrag gibt eine Übersicht über den Stand der Forschung und der Praxis im Zusammenhang mit der Sicherheit der Tragwerke, vom Standpunkt eines praktizierenden Ingenieurs. Die drei Strategien, die für den Zweck Anwendung finden, werden kurz behandelt. Sie umfassen solche Hilfsmittel wie Baunormen, die Kontrolle von menschlichen Fehlern und das Konzept der Begrenzung des Versagens von Tragwerken.

1. INTRODUCTION

Safety from collapse is one of the basic essentials any structure must provide during all of its history, besides such other functions as serviceability, pleasing appearance etc. Structural safety has traditionally been the task of the design engineer although more recently it has found a place on the scientists' desk, to be analysed and understood. Substantial efforts, in particular during the past 20 years or so, have succeeded in resolving part of the problem while another part still evades our comprehension and direction.

In this account the author shall try to identify and describe that part of the problem of structural safety which sofar has largely escaped analysis, and remains full of questions unanswered. Although talked about rather frequently, some of these questions themselves are still rather fuzzy and, as we shall attempt to show, it is man himself who is at the root of the problem, and it is the knowledge about our own actions and their morphology which is still lacking, quite contrary to the principles of ancient philosophers like Socrates, who advised to begin with man himself in order to understand the world.

Other ages had their try at the problem of structural safety and mostly the means to control or improve matters have been on the plane of jurisdiction. The first systematic attempt to transpire into our day is contained in the laws of the Babylonians, as formulated in the writing on Hammurabi's Stone. It provides a rather explicite, as well as draconic schedule of restitution duty, or of bodily punishments should the individual identified as the builder fail to provide a safe structure. It is perhaps not the most significant aspect of this law that its severity is aimed at removing the unfortunate builder from the scene, should he be found wanting, by ruining him financially or physically, nor even the fact that the incentives provided are so exclusively and dramatically negative. The very essence of the law would seem to be that it is directed towards the human individual exclusively, indicative of the conviction of the legislators of the time that this is where the roots of structural safety are to be found; that the failings of humans in their duties are the real reason for things to go wrong. Long before any scientific leverage existed to analyse problems away from the realm of faith, religion, mores or customs, the sober conclusion of common sense was that the human builder is the element in the history of the structure where structural safety is decided and where it can be influenced by the ultimate recipient, namely the public.

This has not essentially changed in our times and the law still provides the means to reduce guilty individuals through restitution and loss of liberty. Incentives set are still purely negative although society has accepted a degree of redistribution of the financial burden deriving from failures throughout the community of builders, by means of insurance premiums. Even then, the engineer or builder found responsible for a structural failure will still be reduced to less than his former self, after the ordeal of lawsuits etc., morally and financially.

It would seem that a consensus still exists in our day's society to the effect that structural safety originates from humans, not from things or natural laws, although it could also be said that things do not respond to incentives,

negative or not and cannot be made to suffer in compensation. Therefore the only possible satisfaction for a failure can be had from the human individual with its emotions like fear, or the modern expression of the need for security, the wallet. Be this as it may, the effects of the traditional attitude and approach are still generally accepted as satisfactory and indeed, the safety of structures against collapse compares quite favorably with other fields of safety, or of risk.

Comparative annual probability of death by accident *

	Hours exposure/ annum	Approx. annual risk/person
Mountaineering	100	1×10^{-2}
Air travel (crew)	1000	1×10^{-3}
Car travel	400	2×10^{-4}
Home accidents	5500	1×10^{-4}
STRUCTURAL FAILURE	5500	1×10^{-7}

Foremost of all individuals in question, two people are traditionally most exposed to the negative incentives of the law. They are the structural engineer and the structural contractor who shall be called "designer" and "builder" in this paper. The responsibility for structural safety is almost exclusively assigned to these two, with the sharing variable to a certain extent, from country to country, indicating that the two functions can not easily and clearly be separated. Indeed, in many circumstances it is one organization or individual who directs design and construction, concept and execution of a structure.

Before proceeding to discuss how the activities making up design and construction are interrelated and guided by tools, let us give one thought to the history of a structure in its entirety which, besides the concept and execution will include usage and the physical fact of existence during its lifetime, up to the eventual demolition, or loss, and including alterations, overbuilding, change of use etc. It becomes clear then that the engineer and builder are by no means the only individuals interacting with the structure's safety, as it will be exposed to other stages of existence than the concept or construction for a much longer time, with a much larger number and variety of humans related to it. Considerations of structural safety ought to include all of this since a substantial portion of failures do occur and are generated in the latter part of the structures lifetime.

Therefore, the discussion of man and the effect of his activity on structures should not be limited to their creation but must encompass the users, as well as other persons in contact with the structure and capable to endanger it. This for instance includes such humans as the owner or tenant who overloads or alters the structure, or the executive of a utility company who

* From: CIRIA Report 63. Rationalization of safety and serviceability factors in Structural Codes

decides to assign insufficient personnel to the checking of gas and water lines which may eventually cause accidents. It will even include people who are only accidentally or indirectly inter-relating with the structure, such as the truck driver ramming a column with his vehicle, or a Code Committee who leaves gaps or erroneous statements in the building regulations, or merely compiles a Code that cannot be used because it is too complicated or lacks clarity. In this context the owner or promoter with a tight budget or schedule must not be forgotten who forces designers and builders to deliver skimpy or shoddy work, with insufficient supervision or the like. Although these individuals cannot always be reached by the legal system, structural safety is related to them and if the frequency of accidents ought to be controlled or reduced, their contribution must be dealt with, which means: designed for.

2. STRUCTURAL SAFETY IN CODES

One of the traditional tools designers or builders are able to employ for the generation of safe structures is the Building Code. A few notes shall be devoted to this type of instruments and the way they treat the problem of structural safety.

Building Codes exist in a wide variety of presentation, specificity and even legal status. Some are set-up as guidelines or suggestions, whereas others are accomplished structural design handbooks and/or carry the weight of law. This is not the place to discuss the pro's and con's of these variations but to recapitulate the common elements which in recent time have undergone rather dramatic changes in the semantic and logistic sense, some of which is still under way or merely planned for.

The most conspicuous changes relate to the very problem of structural safety and the way it appears written down in the form of, mostly minimum, standards. Traditionally a safe structure used to be one in which stresses calculated according to some theory, did not exceed certain limits stated in the Code. These limits or allowable maximum stresses then formed the basic trade coin of safety, covering virtually all questions of structural adequacy, from safety against manifest collapse down to all types of serviceability conditions. Values were mostly set by consensus of the leaders of the profession, without much rational basis.

More recently, the trade coin of allowable stresses has been found wanting and gradually, they became replaced, at least as far as design rules for safety against collapse are concerned. The well known design expression of the general type

$$k_o \cdot \underset{i=1}{\overset{m}{R}} (k_i\, r_i) \geq l_o \cdot \underset{j=1}{\overset{n}{Q}} (l_j\, q_j)$$

was introduced, with r_i and q_j, R and Q representing nominal contributions (functions) of resistance (r_i, R) and loading (q_i, Q) and modifying factors (k, l) to all or some of the parameters. Many variations of the expression exist, differing with country, construction materials or type and function of structures. Variations from the general form are mostly achieved by omission of some factors (k_i, l_j) or by splitting them up into products of subfactors. However, the general type of expression is always maintained

which, to the user and reader, conveys two basic functions of the expression: One general and one specific.

What is described in principle is the situation at the time of design when a concept of the structure is being generated. In this context, the basic properties of structure and load are expressed by estimated or nominal functions of

$$R\ (r_1 .. r_i ... r_m) \quad \text{and} \quad Q\ (q_1 ... q_j ... q_n)$$

(nominal from latin: nomen = name) as more exact knowledge about real values is not or not yet available. What the expression, simplified

$$R \geq L$$

then states is that the resistance of the structure shall exceed the loads the future has in store for it.

The second statement is contained in the factors k_i, l_j. They are intended to express the degree of uncertainty, which for every assumed nominal value of a building parameter, must be accounted for: Parameters that are well known in advance will be qualified and multiplied by a factor close to unity, whereas in a case of great uncertainty, the factor will modify the parameter considerably from its "nominal" value. At the same time the modification factors introduce the compensation thought necessary for that uncertainty, in the design expression, and together they convey the picture of a "worst possible case" to be considered in a design where a structure with a resistance already impaired by some deficiencies is overloaded by a combination of loads exceeding the nominal values. This unfavorable case as described by the modified parameters

$$(k_i\, r_i\ ,\ l_j q_j)$$

and functions

$$k_o R\ ,\ l_o Q$$

shall then still result in a structure that does not fail.

The more modern design methods and recipes are all grouped around some version of this safety expression. Under such names as "ultimate strength design", "Traglastverfahren", "charges majorées" etc. they have been used for some time, giving recognition to the fact that what a structure is really asked to do in the first place, is to stand up, rather than to comply with some arbitrary stress limits.

Sofar on the face of it and qualitatively, everything is allright: The designer is given a tool evidently representative of the true nature of the problem, introducing and at the same time compensating for the various things that can reasonably go wrong in the history of a structure. Code writers are given the means to adjust the safety rules according to the requirements of the day, such as economics or values assigned to human life. The public receives construction to a generally accepted degree of safety, with the possibility of modification, should some class of construction become conspicuous through frequent failures or waste of construction materials due to overdesign.

However, two aspects of the problem of design for structural safety still remain unanswered by the algebraic expression now being generally used for design. Firstly the design expression does not allow for direct, quantitative

introduction of data where and when it is becoming available on some building parameters. Much research effort has been devoted to the collection of such material and we shall review this research and what happened to it, as we shall see how the physical properties of a structure influence its safety.

The second aspect left unresolved by the design safety expression is the lack of relationship, even in the most general sense, to the real source of structural failure which remains with human individuals. It shall be discussed in a further chapter.

3. BLAMING THINGS. THE PROBABILISTIC CONCEPT.

Things lend themselves to be analysed and measured, interpreted and reproduced. Ostensibly, all construction is made up from things, like materials, elements and functional combinations of the two. All structures are also exposed to things like natural events, loading through wind, earthquake and the weight of materials, equipment etc.

The method of choice for the analysis and research which is and has been extensively used, is to gather statistical data on repeated similar or reproduceable events, and the use of such data as basis for a probabilistic approach to the safety problem. Thanks to the application of these methods a first definition of structural safety has been possible, it is the probability that a structure will not fail :

$$\text{Safety} = 1 - P_{\text{failure}}$$

as a specific case of the general notion of safety, which describes the probability that any unfavorable event will not occur. This probabilistic expression is now directly accessible to algebraic treatment in various ways. It can be related to a number of different possible modes of failure :

$$1 - P_{\text{failure}} = 1 - \Sigma P_i \text{ (different modes of failure)}$$

which allows to treat each possible failure mode separately. Probabilistic safety can be related to the design expression of the previous chapter

$$1 - P_{\text{failure}} = 1 - P\ (\overline{R} < \overline{Q})$$

by replacing nominal or design values for resistance and loading by true values, the probabilistic statistical properties of which can be gathered through research on building parameters.

Research efforts in the past twenty or so years have concentrated on the gathering of such statistical data, and its evaluation for use in adjusting the design safety expression. This has borne fruit and in many countries, such data is now being worked into the modification factors of the design expression, in an attempt to rationalize it, and to eliminate discrepancies that existed among different cases of structural design, with apparent overdesign on one side or excessive risk in other cases.

One step further, a relative adjustment of safety/risk has become possible which allows to reflect the value of losses related to prospective structural failure, for different conditions: Structures such as hospitals, or other buildings related to emergency services in case of disaster, are to be designed safer along with buildings likely to contain a great number of people,

as opposed to structures intended for storage or other like purposes not endangering many persons in case of a collapse. Conveniently structural safety in the form of probability can be transformed into different expressions, assuming certain probabilistic or statistical relationships to apply such as the symmetrical (Gaussian normal) distribution function, although the validity of such assumptions can not always be verified, or in some cases, is known not to be true. However, some simplification is proposed to be acceptable considering the tendency of the distribution of a function of many statistical variables to approach a Gaussian normal form, independent of the particular types of the individual distributions. For comparison of safety levels in various design cases, the factor β has recently been favored; it can be demonstrated most easily on the figure of a Gaussian normal distribution :

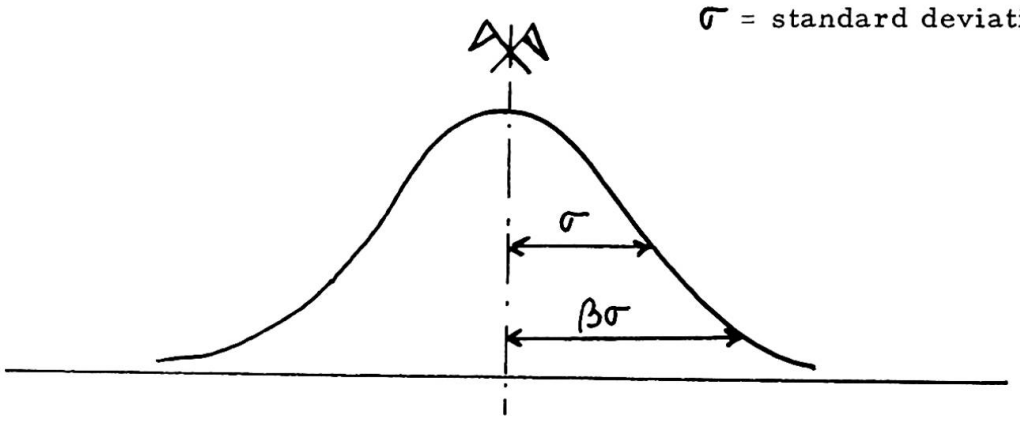

FIGURE 1.

On this basis a comprehensive and consistent logical concept is being created presently to reflect the behaviour of "things" (essentially nonhuman quantities), as they work in or onto real structures, influencing safety. Rules are being derived from the theory and worked into the factors making up the design expression, which are being adjusted to reflect new findings. New general concepts such as "limit states design" are being introduced in building Codes, allowing the unification of structural design with different materials, or for different types of structures.

In spite of this evident success the probabilistic concept of safety which is essentially based on the "blaming of things", still fails to answer two salient questions which an ultimately successful concept of structural safety must resolve.

The theories built around statistical properties of building parameters have yet to be measured against the real frequency and make-up of structural failure. No algebraic relationship has been established between the population of structural failures and the statistical properties found for building parameters. Failures are, fortunately, rare events and - unfortunately - they are not always altogether and most of the time not clearly reported, a fact which relates quite closely to the practicalities of restitution and the working of the legal system which in most cases sets the incentives against comprehensive and public reporting. This has made it very difficult sofar to analyse failures in a systematic manner and therefore, the final word cannot be spoken yet on

the validity of the limit state theorems. This expresses itself in the fact that although the modification factors in the safety expression can and have been varied singly or in groups, no absolute calibration has been found possible, based on rational scientific fact and the overall magnitude of the combined modification factors is still entirely a matter of the consolidated judgement of the code committee.

The second weakness of the probabilistic concept, and hypothetically the same as the first one in essence, is that it still fails to include the human source of structural failure. Where human errors find mention at all they are notoriously attributed to the realm of "what must not happen, can not happen", with the excusing corollary that sufficient control and supervision would have prevented the human error to take effect.

But would it ? Or is it so that sufficient, or acceptable efforts are already being spent on control and supervision, checking and verification, with the manifest result that structural failure is, although rarely, still taking place ?

4. HUMAN REALITY

Is it not that humans direct most of the things contributing to a structure ? A designer determines structural system, material specifications, dimensions etc., the builder introduces construction sequence, organizes the labor to do the job, selects suppliers and materials, building elements and equipment. The user directs the exploitation of the structure as a load carrying device. The neighbour influences snow, wind, foundations of the structure through his own adjacent object. Dissatisfied workers or irresponsible people of all descriptions, including terrorists, expend their malevolence by sabotage or in other destructive ways. Eventually even accidents unrelated to the structural system must be considered, such as fire, collisions, explosions, the effects of war or events related to a future technology presently unknown.

All these possible causes of failure have a common origin, man. The action of individuals, or the inaction at a critical time and place, will always be the cause of the vast majority of structural failures. With the exception of such purely natural events as wind, rain, snow and earthquake, all "things" entering the building process will be selected, fabricated, or put together by humans. Humans will verify the activities of other humans, rectifying errors or omissions, or they will not, in a number of cases, and some of these will eventually develop into failures.

Human activity has sofar eluded attempts to statistical analysis, and research efforts in this direction have been discouragingly few and far between although the facts recited above have been exposed rather clearly for quite some time.

Is it that the secrecy of human activity should be protected in this manner, or is it merely that researchers are being deterred by the difficulty of the problem? Is it that success in research on "things" that cannot evade analysis is won more safely and easily than with the elusive working of the human mind which directs the "things" ? Let us not forget that structural failures are almost

never caused by one element alone but by combinations of a number of them : Even if it was the wind that blew down that roof, it was the designer who specified an insufficient number of nails, the builder who provided inferior quality or quantity, or the worker who cheated with the spacing in order to finish the day early. And again it was the foreman or superintendent who failed to check the worker, or the design, and let the deficiency slip through.

It is the checking function which is consistently cited as the only means in our power to control structural failure caused by human error or omission. Let us therefore devote some moments to the morphology of that checking function as it turns out, by elimination, to be the central element in the prevention of structural failure and, therefore, the principal tool for the achievement of structural safety.

Logically, the objective of supervision and checking is to eliminate in a second round what went wrong in the first one. This sounds rather simple but in practice, it is a very complex endeavour. In many cases, corrections can be made quite easily when an error has been recognized. Sometimes the time for recognition and correction is limited as for example in the case of concrete reinforcing faultily placed: As soon as the concrete has been placed, the error will be hidden from sight and corrections become very difficult and costly. The target of the checking (control, supervision) function is then, in trivial words :

For the right person to be there at the right time and paying sufficient attention.

Errors occur in an infinite variety of ways but they all have their history of development into conditions deleterious to the structure, during part of which they can be recognized and rectified. Eventually, real structural safety will therefore principally depend on the effectiveness of checking and supervision.

Let us consider how it is presently being performed, in order to understand how it works and why, in certain cases, it does not. Recapitulation of two facts appears to be justified at this point, in order to prepare the stage for the further discussion :

1. Structural failures are rare events and the number and variety of building parameters contributing is virtually infinite.

2. The amount of effort presently spent on checking and supervision is by and large what is considered adequate in today's social and economic conditions. It is not likely to change dramatically.

Various organizational mechanisms exist, varying from country to country and from case to case, to implement checking, review and supervision design, construction and sometimes the usage of structures. From state imposed institutions, like "Prüfingenieure" or "bureaux de contrôle", to the North American practice of leaving it more or less to the parties directly involved with the structure to decide on the intensity of control, many different systems are considered acceptable. No one has been proven to be superior

to others, where the only ultimate proof of course would be a relatively lower frequency of failures within the domain of a particular system, or inversely, by making possible higher economy by lowering safety margins (reduction in expenditure for building materials) without an increase in the frequency of failure. Therefore no "perfect" or "best" version has been found sofar.

In practice, checking is usually left to one or more individuals with not much more at their command than their personal experience, commonsense and inclination, and some furtive and unsystematic knowledge about what has gone wrong elsewhere. More or less systematic guides are rare to be found in the field of structural engineering, and they usually extend only over certain limited portions of the problem such as design calculations, consistency of shop drawings with plans and specifications, or quality of certain construction materials.

If one compares checking and supervision with a network set to catch errors of all kinds, then apparently, no particular type among a wide variety has been found to outcatch the others. With the average size of mesh sensibly invariable, as we have seen, improvements can be found only in one way, namely by finding and removing gaps and leaks in the mesh where errors still slip through, large enough to cause structures to fail. As good fisherman, we should go about mending our nets as we shall not be able to buy new or better ones. Gaps are not located in the same positions in all versions of the nets but one common property can be seen: They all need mending.

If the amount of thread available represents the total effort available then the best possible network is certainly the one with uniform mesh size throughout, and containing no gaps. This has always been implicitely recognized by the profession of engineers at large, the consequence having been that whenever a certain type of failure became conspicuous enough to cause concern, design methods and rules were adjusted and checking for the particular condition was intensified. Network mending is therefore a continuing process but, as experience shows, it normally takes place only after gaps have become evident through massive leakage, i.e. frequent accidents of a specific type. Earlier in history gaps in the net existed that could be filled by new developments in the theory of structures which subsequently were acquired such as the theory of stability, whose development and dissemination followed a number of large scale accidents due to instability of steel members or assemblies. Not much hope exists today that new theories will help us much further in controlling structural safety. Building Codes are in the process of fine adjustment and dramatic improvements in our knowledge about building parameters do not seem to be waiting around the corner.

What is it then that can be done in the sense of improving the consistency of the network, in order to prevent large fish from slipping through ?

Other fields of human endeavour have to deal with similar problems where the consequences of human failure to act appropriately at the right time is at the source of most of what goes wrong. Examples like the handling of airplanes or other complex technical equipment come to mind. All of them have in common that many elements or parameters work together for the final

result, such as a safe trip, faultless fabrication of industrial products, or in the case of structures, a fail safe history. One frequently used method of ensuring a gapless control or supervision has been the checklist to be performed before the start of the real run.

A great number of errors leading to failure, have been traced to a mere lack of attention of the right people at the right time. A few seconds of looking would have been needed to recognize the hazard of the missing bolt or the instable condition of a support: A gap in the mesh that was quite easy to see but still not noticed, because no one was looking in the right direction. With this in mind, a tool like the checklist appears to be quite promising as it forces the performer to focus his attention for a minimum of time onto each and every item. Of course, the performer will have to be equipped with the necessary knowledge and authority to correct errors which will make him the most highly qualified individual among the designers and builders: in airplanes it is the pilot himself who attends to the performance of the checklist.

As a tool for the verification that everything necessary for the success of the operation (or design) has been considered, the checklist is the simplest form of systematic prevention of errors of random character. If set up properly it can make any effort spent on checking decisively more consistent and efficient. In its simplicity, it lends itself to easy adjustment and completion whenever needed.

Perhaps it is time to equip the engineering profession with something more systematic than today's rather random methods of supervision in design and construction.

5. LIMITING THE INEVITABLE, CONCLUSION

On the 1978 joint Conference of the ASCE, ICE and CSCE, the subject of design against hazards was formulated, with one half of the conference devoted to the problem of human hazards. It is the engineers after all, or designers, who are in a position or ought to be, to influence the resistance of structures under the assault of hazards, or of the unforeseen.

Human errors, as they were named for convenience in this paper, do of course include human hazards in the narrower sense and strategies aimed at the prevention of errors or their consequences will have to extend to all adverse conditions the structure will meet during its history, no matter what their particular nature or classification may be. In Hammurabi's time a structure had to resist failure without any ifs or questions asked. This is still essentially the case despite all probabilistics and the "blaming of things", as it were.

To achieve this, different approaches have been found to provide part of the answer: A first and classic strategy has been seen to be the application of the design expression which includes safety margins to cover "reasonable" deviations of the building parameters from their assumed nominal values.

A second strategy was found to consist in an improvement not so much of the intensity as of the consistency of checking and supervision. It is quite obvious that this activity is limited practically to the duration of design and construction, unless certain controlling functions are extended beyond those stages, as is the case for certain types of structures such as railway bridges, power dams or structures of similar scope. The majority of structures however, will be left to itself and its users after the construction crew has left.

Other strategies will therefore have to be found to compensate for errors and hazards occurring after construction, as well as those that escaped the first two approaches to structural safety. In recent years, the beginnings of such strategies has been recognizable, with earthquake resistant design leading the field. Notions like design against progressive collapse, toughness or ductility of structures have made their appearance, triggered for example by the famous partial collapse of the Ronan's Point apartment building. They are what this author would like to call strategies of the third line of defense and they all have a common aim, to design a structure in such a way that failure, where it inevitably occurs, will be limited in scope, geometrically, in terms of value or danger to life.

In conclusion then, three types of strategy are presently being applied for the control of structural safety; by their state of advancement, they can be ordered:

1. Design safety margins, as represented by the typical expression
   $$\text{minimum Resistance} \geq \text{maximum Loading}$$
   This method is established and included in building codes and is being generally used in structural design and construction. Its development is very advanced and fine adjustments are presently being implemented. It is based on statistical recognition of the variation of building parameters, not considering random influence of human (or gross) errors.

2. Checking and supervision during design and construction. This strategy is generally applied in practice, with substantial effort but little consistency from case to case. A greater intensity not seeming to be probable in the near future, improvement will have to be found in the direction of making it more systematic and by directing the available effort onto where it counts. Research efforts in this field have been hesitant and much is left to be improved. The second strategy is mainly aimed at the elimination of human errors which are recognized to cause the majority of structural failures. The use of checklists for guidance seems indicated.

3. The beginnings of a third line defense strategy have been recognized in certain fields. It is aimed at equipping the structure with reserves for the case of accident or where the first and second lines of defense have failed to prevent structural failure. Specifically, types of initial failures possible or probable are established and limited in their scope through the choice of appropriate structural systems. Notions like earthquake resistant design, design against progressive collapse, ductility or toughness of structures, failure mechanics belong to this general approach. To make it into an effective and systematically used tool will be one of the tasks of the future.