Die sicherheitstechnische Auslegung wassergekühlter Kernreaktoren in der Bundesrepublik Deutschland

F. Mayinger

Paris, 20. Oktober 1987

1. Internationale Vergleichbarkeit des Sicherheitsstandards.

Nach der Reaktorkatastrophe in Tschernobyl wurde im politischen Raum wiederholt und mit Nachdruck die Forderung nach einem international gleichhohen Standard für alle Reaktoren der westlichen und östlichen Welt laut. Offen gelassen wurde dabei die Frage, wie man diesen Standard mißt, was konkret im sicherheitstechnischen Sinn Vergleichbarkeit bedeutet und wie man die verschiedenen Möglichkeiten und Wege, die Umwelt vor Reaktorkatastrophen zu schützen, bewertet. Von verschiedenen Seiten wurde auch versucht, Rangfolgen zu kreieren, ja den verschiedenen Reaktorkonzepten unterschiedliches Risikopotential zu unterstellen.

Wenn ich heute über die sicherheitstechnische Auslegung deutscher Reaktoren zu berichten habe, so möchte ich dies keineswegs im Sinne einer gegenseitigen Aufwägung sicherheitstechnischer Einrichtungen oder gar in einer vergleichenden Bewertung sicherheitstechnischer Strategien tun, oder verstanden wissen, sondern ich will lediglich das deutsche Konzept und die Überlegungen, die dazu führten, vorstellen, in der Hoffnung, daß gegenseitige Information und konstruktive Diskussion uns allen, insbesondere auch der deutschen Seite neue und wertvolle Denkansätze für noch bessere Sicherheitsstrategien und noch zuverlässigere Maßnahmen zur Vermeidung katastrophaler Unfälle liefert. Es gibt verschiedene Wege, wie man in einem so komplizierten System wie einer

kerntechnischen Anlage ein Optimum an Sicherheit erzielen kann und es wäre nicht nur vermessen sondern auch dumm, behaupten zu wollen, der eigene sei der beste oder gar einzig richtige Weg.

2. Deterministische oder probabilistische Betrachtungsweise

In der Vergangenheit beruhte das Genehmigungsverfahren und die sicherheitstechnische Beurteilung von Kernkraftwerken ausschließlich auf dem deterministischen Konzept, wobei man in früheren Jahren sogar nicht ganz korrekt von einem "Größten Anzunehmenden Unfall" sprach, während man heute unter dem Auslegungsstörfall eine Vielzahl verschiedener Versagensmöglichkeiten und Fehlfunktionen des Reaktorsystems versteht. In Abb.1 sind solche Versagensmöglichkeiten und Fehlfunktionen als Beispiele für einen "Störfall" zusammengestellt.

Wie international üblich ist unterschieden zwischen Störfällen mit und ohne Kühlmittelverlust, Reaktivitätsstörfällen durch Fehlfunktionen der Regelsysteme, Fehlern in der Energieversorgung und auch Fehlern, die bei der Handhabung und Speicherung der Brennelemente auftreten können. Von diesen internen Störfällen sind Einwirkungen von außen zu unterscheiden. Als solche werden im deutschen Genehmigungsverfahren der Absturz eines Flugzeuges bis zu großen Verkehrsmaschinen, Erdbeben, Explosionen freigesetzter brennbarer Gase und auch Sabotage durch Einzeltäter und Tätergruppen betrachtet.

Die ausschließlich deterministische Sicherheitsbeurteilung war sicher gerechtfertigt, solange nicht genügend Betriebserfahrung mit laufenden Anlagen verfügbar war. Bereits die ersten Risikostudien führten zu Fragen nach der Zweckmäßigkeit eines probabilistischen Vorgehens, das auch hypothetische Unfälle und ihre Folgen miteinschließt und damit über den "Auslegungstörfall" hinausgeht. Ein solches probabilistisches Vorgehen könnte für die Definition und Festlegung von Sicherheitszielen sehr wertvoll sein. Wie bekannt wurden Risikostudien schon lange vor dem Unfall in Three Mile Island vorgelegt und diskutiert. In der Bundesrepublik Deutschland führte das Ergebnis der Risikostudie Phase A dazu, daß Maßnahmen zum Abfahren bzw. zum Abblasen der Dampferzeuger für den Fall eines kleinen Lecks oder eines Ausfalls der Stromversorgung vorgesehen wurden, bevor der Unfall in Three Mile Island auftrat. Als Konsequenz des Unfalls in Three Mile Island wurden dann damals lediglich Möglichkeiten für ein

automatisches Abfahren der Dampferzeuger in deutschen Druckwasserreaktoren gefordert und installiert, da die Risikostudie menschliches Fehlverhalten mit hoher Wahrscheinlichkeit bewertete.

Bei jeder Risikostudie muß man jedoch darauf achten, wie vollständig die Probleme definiert werden können und selbst bei weitgehend vollständiger Definition bleibt immer noch die Frage, ob alle wichtigen Ereignisse und Ereignismöglichkeiten nicht nur in Betracht gezogen sind, sondern auch hinsichtlich der Häufigkeit ihres Eintretens richtig beurteilt wurden. Schließlich ist jede Risikoanalyse mit subjektiven Elementen behaftet, die ich keineswegs als Willkür beurteilt oder betrachtet haben möchte, sondern die darauf beruhen, daß die analysierenden Fachleute mehr oder weniger große Erfahrung mitbringen.

Deshalb gibt es auch heute noch viele gute Argumente, bei dem bewährten deterministischen Prinzip für Auslegung und Sicherheitsbeurteilung von Kernkraftwerken zu bleiben. Wichtige Gründe dafür sind die Genauigkeit und Zuverlässigkeit der sicherheitstechnischen Beurteilung und die Effektivität, mit der deren Richtigkeit nachgewiesen werden kann. Daneben aber ist es sicherlich nützlich, ein Konzept für die Definition und Anwendung probabilistischer Sicherheitskriterien zu erarbeiten, das die deterministischen Regeln ergänzt.

Zweifellos sind Risikostudien eine extrem wertvolle und wichtige Hilfe, Schwachpunkte in der Anlage zu finden und dadurch deren Zuverlässigkeit und Sicherheit zu verbessern. Jede Risikostudie ist aber nur für eine ganz bestimmte Anlage relevant, da sie auf speziellen Konstruktionsmerkmalen, auf dem Grad der Redundanz wichtiger sicherheitstechnischer Komponenten und auf deren Qualitätssicherheit aufbaut. Als Mittel zur Verbesserung der öffentlichen Akzeptanz von Kernkraftwerken halte ich Risikostudien für ungeeignet.

3. Sicherheitsstrategien

Das Konzept der deutschen Sicherheitsstrategie ist mehrdimensional und im Sinne mehrerer Verteidigungslinien tief gestaffelt. Die Strategie beginnt mit der Qualitätssicherung der Reaktorkomponenten und -systeme , beinhaltet die Redundanz und Diversität sicherheitstechnisch wichtiger Einrichtungen, nutzt die weitgehende Automatisierung der Störfallvermeidung und Störfallbeherrschung, beachtet die räumliche Trennung der Sicherheits- und

Notfalleinrichtungen und stützt sich schließlich auf eine ausreichend, ja überdimensionierte Struktur der Primär- und Sekundärkomponenten (Abb.2).

Beispielhaft sei hier die Qualitätsicherung, wie sie beim Bau und Betrieb deutscher Kernkraftwerke gehandhabt wird, herausgegriffen und etwas im Detail diskutiert (Abb.3). Schon bei der Wahl der Werkstoffe wird auf hohe Zähigkeit und Widerstand gegen Korrosion geachtet; dies ist der erste Schritt, um z.B. einen großen Riß oder gar einen doppelendigen Bruch der primärkühlmittelführenden Leitungen ausschließen zu können. Der nächste Schritt wird dann bei der Konstruktion getan, nicht nur durch sorgfältige Berechnung der Beanspruchung und durch mit großen Sicherheitsmargen versehener Auslegung, sondern insbesondere auch dadurch, daß man Schweißnähte soweit wie möglich vermeidet. Ein Beispiel für die Reduzierung der Zahl und Länge der Schweißnähte von Biblis A bis zum Bau des Kernkraftwerkes Philippsburg 2 mag Abb.4 verdeutlichen. Durch konstruktive Verbesserung konnte die Zahl der Rundnähte am Reaktordruckbehälter von 8 auf 5 verringert werden und die gesamte Länge der Schweißnähte am Reaktordruckbehälter, die bei Biblis A noch 143 m betrug, wurde bei Philippsburg 2 auf 78 m reduziert. Ein Vergleich der in Abb.4 angegebenen Wandstärken zwischen Biblis A und Philippsburg 2 zeigt auch, daß die auftretenden Spannungen im Zuge dieser konstruktiven Verbesserungen verringert wurden. Besondere Aufmerksamkeit wurde auf die leichte Zugänglichkeit der Schweißnähte für Wiederholungsprüfungen gelegt. Beispielhaft dafür ist die Anordnung und Einbringung der großen Stutzen für die Hauptkühlmittelleitungen. Ähnliche Verbesserungen wurden auch bei den Dampferzeugern vorgenommen, so verringerte sich dort die Zahl der Schweißnähte in der Druckschale von 51 bei Biblis A auf 21 bei Philippsburg 2.

Es klang bereits an, daß bei der Qualitätssicherung auch die Wiederholungsprüfung der Komponenten eine wichtige Rolle spielt, selbstverständlich wird bei der Herstellung peinlich genau auf hohen Qualitätsstandard geachtet und dieser während der gesamten Bearbeitung durch zahlreiche Prüfungen verschiedener und unabhängier Institutionen überwacht.

Die geringe Fehlerrate beruht natürlich auch auf dem ausgewählten Material - z.B. 20 MnMoNi 55 - das verarbeitungsfreundlich ist. Die Verwendung von ferritischem Stahl anstelle von austenitischem Material für die Primärrohrleitungen hat sich über die Jahre bewährt. Es ist heute möglich, nahtlose ferritische Rohre

induktiv zu biegen und sie dann mit einem austenitischen zweilagigen Cladding innen zu versehen. Bei so konstruierten und gefertigten Rohrleitungssystemen besteht praktisch keine Einschränkung für die zerstörungsfreie Wiederholungsprüfung. In bestimmten Bereichen z.B. an einigen Stellen der Frischdampfeinleitung, also im Sekundärbereich von Druckwasserreaktoren, ist die Oberfläche der Schweißnähte geschliffen. Im einzelnen sind die Maßnahmen und Empfehlungen für dieses Konzept der "Basis Sicherheit" in den RSK-Leitlinien und in der KTA-Regel 3201 niedergeschrieben.

Jede Maßnahme bringt Vor- und Nachteile mit sich und obwohl Betreiber wie Hersteller mit diesem Konzept der Basis Sicherheit gute Erfahrungen machten, muß man doch darauf achten, daß der Aufwand an Papier - Zertifikaten, Bescheinigungen und Berichten - nicht zu groß wird. Die Aufmerksamkeit des Ingenieurs könnte sonst zu sehr auf die Erfüllung der formalen Vorschriften, also auf die Beibringung und Erstellung der Aktenunterlagen, als auf die Komponente selbst gerichtet sein und zum anderen können übertriebene Formalitäten das Bewußtsein der Eigenverantwortung einschläfern, dadurch daß sich der Ingenieur zu sehr auf das Ausfüllen von Formularen und das Erstellen von Schriftstücken verläßt.

Eine zweite Dimension der Sicherheitsstrategie ist die sogenannte "gestaffelte Verteidigung" (defense-in-depth). Dies bedeutet, daß bei Transienten und Störfällen verschiedene Ebenen von Regel- und Sicherheitseinrichtungen zur Verfügung stehen, die im Anforderungsfall nacheinander und unabhängig voneinander eingreifen. In Abb.5 ist der Versuch gemacht, diese gestaffelte Verteidigung gegen Stör- und Unfälle zu veranschaulichen.

Bei geringen Abweichungen vom Betriebszustand wird zunächst das betriebliche Regelsystem ansprechen und die Anlage in den vorgegebenen Betriebszustand bringen. Sollten die Störungen zu groß sein oder die Möglichkeiten des betrieblichen Regelsystems nicht ausreichen, so greift im Sinne einer zweiten Verteidigungsebene das Begrenzungssystem, das durch Kontrollmaßnahmen - immer noch ohne Reaktorschnellabschaltung - den Anlagenzustand wieder stabilisiert. Erst wenn die Maßnahme dieser zweiten Ebene nicht ausreicht, greift die dritte Ebene, es tritt das Reaktorschutzsystem in Aktion, das zunächst eine Reaktorschnellabschaltung bewirkt. Abhängig von der Art der Störung - also zum Beispiel ohne oder mit Kühlmittelverlust - werden dann die entsprechenden Not- oder Nachkühlsysteme aktiv, bei intaktem Primärkreis die

Druckentlastung der Dampferzeuger und die sekundärseitige Nachspeisung, oder bei einem Leck im Primärkreis die Hochdruckeinspeisepumpen, die Druckspeicher und schließlich die Niederdrucknachkühlpumpen.

Diese tiefgestaffelte Verteidigung soll auch Abb.6 nochmals demonstrieren, wobei dort jedoch zusätzlich zu den bereits diskutierten drei Schutzebenen eine vierte Barriere gegen unzulässige Auswirkungen von nuklearen Stör- oder Unfällen aufgezeigt ist. Abb.4 unterscheidet deutlich zwischen den drei Ebenen der Genehmigungsanforderungen und der erwähnten vierten Ebene außerhalb des Genehmigungsverfahrens, die zur Verringerung des Risikos aus einem schweren Störfall, der über die Auswirkungen des Auslegungsstörfalls hinausgeht, beiträgt. Eine wichtige Funktion in dieser vierten Verteidigungsebene spielt das sogenannte "accident management", worunter man das Verfügbarmachen und den Einsatz von Systemen versteht, die ursprünglich nicht als Sicherheitssysteme vorgesehen sind und somit auch nicht automatisch im Störfall angefordert werden, und worunter auch die Reaktivierung zeitweise ausgefallener Sicherheitssysteme durch Hand- oder Überbrückungsmaßnahmen fällt. Wir werden anhand einiger Beispiele noch auf die Möglichkeiten dieser vierten Verteidigungsebene zurückkommen.

4. Sicherheitstechnische Einrichtungen

Deutsche wie französische Reaktoren haben die üblichen sicherheitstechnischen Einrichtungen, wie sie in Abb.7 beispielhaft an einem Druckwassereaktor dargestellt sind. Im Kreise von Fachleuten ist es sicher nicht notwendig, auf diese Sicherheitseinrichtungen im allgemeinen einzugehen. Nur kurz diskutiert werden soll anhand der Abb.7, welche dieser Sicherheitseinrichtungen während des Betriebes einer Inspektion zugänglich sind, also welche theoretisch täglich in Augenschein genommen werden könnten. Inspektionen durch das Betriebspersonal haben sich als äußerst wichtig und förderlich für den zuverlässigen Betrieb von Maschinen und Apparaten erwiesen. Deshalb kommt der Zugänglichkeit wichtiger sicherheitstechnischer Systeme große Bedeutung zu.

Man erkennt aus Abb.7, daß das gesamte Notkühlsystem einschließlich der Nachwärmeabfuhrkette, aber auch die sekundärseitigen Druckentlastungsventile während des Betriebes zugänglich sind. Nur kleine Bereiche des Reaktors, wie das Primärsystem selbst

mit dem Reaktordruckbehälter und den Dampferzeugern, erlaubt keine unmittelbare Inaugenscheinnahme während des Betriebes. Dies ist aber auch nicht nötig.

Wir wollen nun unsere Betrachtungen der Sicherheitssysteme im wesentlichen auf den Druckwassereaktor beschränken und den Siedewasserreaktor nur kurz streifen. Denkt man schutzzielorientiert, also in dem Sinne, daß die Abgabe von Radioaktivität an die Umwelt im Falle eines Störfalles auf ein technisch mögliches Minimum reduziert werden muß - wie es übrigens das deutsche Atomgesetz vorschreibt - so ist das erste Schutzziel, den Reaktor sicher und schnell abzuschalten und unterkritisch zu halten. Dies wird durch die Abschaltstäbe und auch durch das Borier-System bewirkt. Das zweite Schutzziel richtet sich dann auf die sichere Abfuhr der Nachwärme aus dem Reaktorkern und auf die Einhaltung einer Kerntemperatur, die eine Beschädigung der Brennelemente ausschließt.

Aus Risikostudien, aber auch aus der praktischen Erfahrung wissen wir, daß Störfälle, die durch große Leckagen im Primärkreis verursacht sind, eine um Größenordnungen geringere Wahrscheinlichkeit haben, als solche, bei denen das Primärsystem keinen oder nur wenig Kühlmittelverlust aufweist, bei denen also der Druck im Primärsystem hoch bleibt. Es gilt dann die Nachwärme über das Sekundärsystem abzuführen, wobei nach Ausfall der Turbine, also wenn es nach einem Netzzusammenbruch zum Beispiel nicht gelingt, die Turbine auf Eigenversorgung zurückzuregeln, zunächst der Kondensator als Wärmesenke zur Verfügung steht. Sollte auch die Nutzung des Kondensators nicht möglich sein, so werden, wie bekannt, die Dampferzeuger sekundärseitig über Ventilstationen abgeblasen. Insbesondere die Vorsteuerventile dieser Ventilstationen waren in den vergangenen Monaten ein Diskussionspunkt in den Fachgremien, insbesondere in der Reaktorsicherheitskommission, da an einigen Anlagen Unregelmäßigkeiten aufgetreten waren. Bei den neuesten Anlagen wurden nun diese Vorsteuerarmaturen diversitär ausgeführt, bzw. nachgerüstet, d.h. ihre Öffnungsmechanismen folgen unterschiedlichen Konstruktionsprinzipien. Für die Abkühlung des Reaktors genügt es, zwei von vier Dampferzeuger abzublasen, für die Abfuhr der Nachwärme reicht ein Dampferzeuger aus.

Ebenso wichtig wie die sichere Druckentlastung ist das rechtzeitige und ausreichende Nachspeisen von Wasser auf die Sekundärseite der Dampferzeuger. Hierfür stehen, wie in Abb.8 skizziert, verschiedene Speisewassersysteme zur Verfügung. Zu nennen ist

zuerst das betriebliche Speisewassersystem mit drei Speisewasserpumpen, von denen eine für die Nachspeisung während der Notkühlphase ausreicht. Redundant hierzu stehen weitere Einspeisesysteme zur Verfügung, nämlich das An -und Abfahrsystem mit zwei Speisepumpen und vier unabhängigen Strängen, und das Notspeisesystem, von denen jedes aus einem Vorratsbehälter, einer dieselgetriebenen Speisepumpe und den dazugehörigen Armaturen besteht. Das gesamte Speisewassersystem ist also hochgradig redundant, was insbesondere daher rührt, daß im deutschen Genehmigungsverfahren davon ausgegangen wird, daß im Anforderungsfall ein Teilsystem versagt, ein zweites sich in Inspektion befindet und die verbleibenden Systeme in der Lage sein müssen, nicht nur die Nachwärme sicher abzuführen, sondern auch den Reaktor auf einen Zustand nahe dem Umgebungszustand zu bringen. Diese Forderung wird auch bei dem Notspeisewassersystem gestellt, deshalb besitzt es vier Stränge, von denen zwei zur Abkühlung des Reaktors ausreichen müssen.

Der Wärmetransport aus dem Core zu den Dampferzeugern erfolgt durch freie Konvektion, wobei Versuche nachwiesen, daß dieser Wärmetransport auch gewährleistet ist, wenn sich Dampf im Primärsystem befindet, ja selbst wenn dieser Dampf nichtkondensierbare Spaltgase enthält.

Bei einem Leck im Primärsystem muß das ausströmende Wasser, bzw. der ausströmende Dampf durch Einspeisung wieder ersetzt werden, wofür bei kleinen Leckagen das Volumenregelsystem, das nicht zu den Sicherheitseinrichtungen zählt, ausreicht. Bei Absinken des Druckes im Primärkreis unter 111 bar oder wenn der Wasserspiegel im Druckhalter unter 2,2 m liegt, werden die Hochdruckeinspeisepumpen aktiv, die zunächst aus vier Vorratsbehältern boriertes Wasser ansaugen. Diese vier Hochdruckeinspeisepumpen sind, wie Abb.9 zeigt, sowohl auf die kalte wie auf die heiße Seite der Primärrohrleitungen geschaltet.

Sinkt der Druck im Primärsystem trotz Zuspeisung aus den Hochdruckpumpen wegen der Größe des Lecks weiter ab, so öffnen bei einem Primärdruck von etwa 27 bar acht Druckspeicher automatisch und entleeren ihren Wasserinhalt von je 47 m^3 in den Reaktordruckbehälter. Auch die Niederdrucknachkühlpumpen sind, wie Abb.9 zeigt, vierfach redundant vorhanden, auch sie beziehen ihr Notkühlwasser aus den vorher genannten Vorratsbehältern. Sobald genügend, aus dem Primärkreis ausgeströmtes Wasser im Sumpf des Sicherheitsbehälters angesammelt ist, schalten sich die Ansaugleitungen automatisch auf diesen Zulauf um. Dabei wird das ange-

saugte Sumpfwasser über einen Kühler gedrückt. In Abb.9 sind die verschiedenen Schaltungs- und Anforderungsweisen des Not- und Nachkühlsystemes so dargestellt, daß der erste Strang auf Hochdruckeinspeisung, der zweite Strang auf Umwälzkühlung aus dem Sumpf, der dritte auf Niederdruckeinspeisung aus dem Vorratsbehälter und der vierte auf die Druckspeichereinspeisung skizziert ist. Auch bei diesen Sicherheitssystemen gilt die genehmigungstechnische Annahme, daß eines im Anforderungsfalle ausfällt, eines in Inspektion ist, und zusätzlich wird noch unterstellt, daß ein drittes teilweise auf die gebrochene Primärkühlmittelleitung speist. Damit stünden unter diesen konservativen Annahmen nur 1 1/2 Notkühlsysteme für die Kühlung des Kernes zur Verfügung, die so wirksam sein müssen, daß die Temperatur im Kern unterhalb dem von der Reaktorsicherheitskommission gesetzten Limit von 1200° C bleibt. Aus Experimenten und theoretischen Analysen weiß man, daß selbst bei einem so umfangreichen, in Realität nie zu erwartenden Ausfall von Notkühlsträngen die Temperatur im Kern weit unter diesen 1200° C bliebe, nämlich noch unter 800° C.

Für die Kühlung der Brennelemente im Lagerbecken stehen zusätzlich drei Pumpen zur Verfügung, die sowohl aus dem Vorratsbehälter als auch aus dem Sumpf gespeist werden können. Langfristig muß für die Notkühlung des Kernes soviel Wasser in den Reaktordruckbehälter eingespeist werden können, daß die fühlbare Wärme des Wassers allein in der Lage ist, die Nachwärme abzuführen, daß also kein merkliches Verdampfen auftritt. Dies bewirkt, daß die Austragung von Aerosolen aus dem Kern in den Sicherheitsbehälter auf ein Minimum reduziert wird.

Auch die Wärmeabfuhr im Umwälzbetrieb nach außen ist hoch redundant ausgelegt. Wie man aus Abb.10 erkennt, wird der Kühler jedes Nachkühlstranges sekundärseitig von zwei Pumpen in einem geschlossenen Kreislauf gespeist, wobei aus diesem geschlossenen Kreislauf wieder über einen Kühler die Wärme schließlich an den Fluß oder einen Kühlturm abgegeben wird.

Zur Sicherstellung der Funktionsweise dieser Not- und Nachkühlsysteme, auch bei Einwirkungen von außen wie Flugzeugabsturz, chemische Explosionen und Sabotage, sind diese Systeme verbunkert, bzw. innerhalb des Betonschildes des eigentlichen Reaktorgebäudes untergebracht und zusätzlich noch räumlich voneinander getrennt, wie Abb.11 zeigt. Diese räumliche Trennung ist insbesondere auch eine Maßnahme gegen Brandeinwirkung, da sie verhindert, daß mehr als 1 Teilsystem durch Brand außer Funktion ge-

setzt werden kann. Der Schutz gegen Erdbeben erfolgt durch erdbebensichere Fundamente und Befestigungen.

Bei großen Leckagen, insbesondere beim doppelendigen Bruch kommt den Druckspeichern die Hauptaufgabe für die Kühlung der Brennstäbe in den ersten 100 bis 200 s zu. Obwohl die Druckspeicher völlig passive Systeme sind, deren Wasserinhalt mit Stickstoff auf einen Druck von 27 bar vorgespannt ist und die sich, wie bereits erwähnt, über Rückschlagklappen automatisch öffnen wenn der Druck im Primärkreis unter diese 27 bar gefallen ist, wird im Genehmigungsverfahren unterstellt, daß nur fünf der vorhandenen acht Druckspeicher tatsächlich ihr Wasser in das Primärsystem einspeisen. In Wirklichkeit werden sieben Druckspeicher voll aktiv und nur der achte, der ebenfalls öffnet, speist seinen Inhalt auf das Leck. Abb.12 zeigt, wie sich diese konservative Annahme im Genehmigungsverfahren, nämlich daß nur fünf von acht Druckspeichern kühlwirksam werden, auf die Temperatur der Brennelementhüllen im höchstbelasteten Bereich des Kernes auswirken. Aber selbst unter der physikalisch völlig irrealen Annahme, daß keiner der acht Druckspeicher einspeist und von allen vorhandenen Not- und Nachkühlpumpen nur eine Niederdrucknachkühlpumpe arbeitet, steigt die Temperatur der Brennelementhüllen im Kern, wie Abb.12 zeigt, nicht über 1200° C und bliebe damit auch unter diesen, jenseits aller Genehmigungsbedingungen liegenden Zuständen, innerhalb der im Genehmigungsverfahren noch tolerierten Temperatur.

Bei Siedewasserreaktoren sieht das Nachkühlsystem naturgemäß etwas anders aus. Die Speisewasserzuführung sowohl im Normalbetrieb als auch im Störfall erfolgt, wie bekannt, in den Reaktordruckbehälter. Bei Ausfall der Turbine und des Kondensators, und damit auch der Hauptspeisewasserpumpen, stehen für die Not- und Nachkühlung, wie aus Abb.13 ersichtlich, im Hochdruckbereich zwei diversitäre Systeme zur Verfügung, nämlich das dampfgetriebene Einspeisesystem TJ und das elektromotorisch angetriebene Nachspeisesystem TM. Im Niederdruckbereich können fünf Flutsysteme bzw. Stränge aktiviert werden, nämlich das Kernflutsystem TK und vier Nachkühlstränge. Durch Handmaßnahmen kann im Notfall weiterhin das dreisträngige Rückfördersystem aus dem Sicherheitsbehälter zum Fluten eingesetzt werden. Für die Nachkühlung steht das viersträngige TH-System zur Verfügung. Bei allen Störfallabläufen ist für die Nachkühlung bis zu einer maximalen Temperatur von 80° C in der Kondensationskammer des Sicherheitsbehälters 1 Nachkühlstrang ausreichend. Diese Angaben und die Informationen der Abb.13 gelten für das Kernkraftwerk Krümmel.

Notfalls könnte auch für eine begrenzte Zeit der Wasservorrat des Speisewasserbehälters, der ja unter erhöhtem Druck steht, als Überbrückungsmaßnahme zur Verfügung stehen. Man erkennt daraus, daß die Speisewasserzufuhr beim Siedewasserreaktor in noch höherem Maße redundant ist als beim Druckwasserreaktor.

In Abb.14 ist schließlich noch das Nachkühlsystem der neueren Baulinie, der sogenannten Baulinie 72, von deutschen Siedewasserreaktoren dargestellt, so wie sie z.B. im Kernkraftwerk Gundremmingen verwirklicht wurde. Man erkennt je drei Nachkühlstränge für den Nieder- und den Hochdruckfall, wobei jeder dieser Stränge in der Lage ist, die Nachwärme aus dem Kern zu 100 % abzuführen und darüber hinaus noch die Anlage abzukühlen. Die Druckentlastung und damit die Wärmeabfuhr erfolgt, wie bei allen Siedewasserreaktoren, durch Einblasen von Dampf in die Wasservorlage der Kondensationskammer, die dadurch aufgeheizt wird. Deshalb ist es notwendig, die Wärme aus dieser Kondensationskammer langfristig auch wieder abzuführen, was durch Umwälzen über einen Wärmetauscher mittels einer Vorpumpe und der Niederdruckpumpe in jedem der drei Niederdrucknachkühlstränge erfolgt.

Einwirkungen von außen begegnet man, wie bereits erwähnt, einerseits durch Verbunkerung der wichtigen Sicherheitssysteme und andererseits durch räumlich getrennte Anordnung. Abb.15 erläutert diese Maßnahmen am Beispiel eines modernen Druckwasserreaktors. Die Notspeisewassersysteme und die Notstromdiesel sind in verbunkerten Gebäuden untergebracht und auch die außerhalb des Reaktorgebäudes befindlichen Schaltanlagen sind durch Betonwände und -decken gegen Flugzeugabsturz gesichert. Jedes der Teilsysteme ist konsequent von dem anderen getrennt und abgeschottet, um zu vermeiden, daß Brände mehr als ein Teilsystem außer Funktion setzen können.

5. Klassifizierung hypothetischer Unfälle.

Jenseits des "Auslegungsstörfalls" kann man drei verschiedene Kategorien hypothetischer Unfälle unterscheiden, wie sie in Abb.16 scheinbar willkürlich, aber für die Sicherheitspraxis doch adäquat klassifiziert sind. Störfälle, die in der Klassifikation der Abb.16 zur 1. Kategorie zählen, werden automatisch durch die vorhandenen Sicherheits- und Notkühlsysteme ohne die Notwendigkeit irgendwelcher zusätzlicher Maßnahmen beherrscht und das Hüllmaterial der Brennstäbe bleibt innerhalb des Temperaturlimits von 1200°C, wie in den Leitlinien der Reaktorsicher-

heitskommission in Anlehnung an die internationalen Gepflogenheiten festgelegt. Wir müssen uns hier nochmals in Erinnerung rufen, daß die Rechnungen im Genehmigungsverfahren bis heute auf konservativen Annahmen beruhen. Würde man sogenannte best-estimate Analysen durchführen, so würde man Temperaturspitzen von höchstens 750° C vorhersagen und feststellen, daß bereits 100 s nach dem Störfalleintritt, die Brennelemente wieder von Wasser benetzt sind, also ihre Oberflächentemperatur entsprechend dem Druck im Sicherheitsbehälter bei rund 150° C liegt. Der hauptsächliche Unterschied zwischen konservativer und best-estimate Vorhersage rührt von der Annahme im Genehmigungsverfahren her, daß einer der vier Notkühlstränge versagt, einer in Inspektion ist und schließlich der dritte teilweise auf die Leckstelle speist, womit also nur die Kapazität von 1 1/2 Notkühlsträngen beim Druckwasserreaktor aktiv für die Kühlung und die Abfuhr der Nachwärme zur Verfügung steht.

Wie erwähnt wird beim kleinen Leck die Wärme aus dem Core mittels freier Konvektion zu den Dampferzeugern geführt und dort durch sekundärseitiges Abblasen der Dampferzeuger an die Umgebung getragen. Es besteht keinerlei Gefahr einer Kernschädigung, solange der Wasserspiegel im Reaktordruckbehälter, oder zumindest der Gemischspiegel, die Brennelemente bedeckt. Diese Wasserspiegelsituation ist solange gewährt, solange wenigstens zwei Sicherheitseinspeisepumpen in das Primärsystem einspeisen und die Sekundärseite von zwei Dampferzeugern mit einer Abkühlgeschwindigkeit von 100 K/h abgeblasen wird.

Eine Situation entsprechend der Kategorie II in Abb. 16 würde dann eintreten, wenn alle Notkühlsysteme für eine gewisse Zeit ausfallen, was eine Beschädigung der Brennelemente zur Folge haben könnte, aber durch rechtzeitiges Wiederingangsetzen der Notkühlung Kernschmelzen verhindert wird, eine langfristige Wärmeabfuhr sichergestellt ist und der Kern auf niedrige Temperatur gebracht werden kann. Das Unfallszenario in Three Mile Island ist in diese Kategorie II einzuordnen.

Kategorie III- Unfälle wären schließlich Abläufe mit vollständigem Coreschmelzen und einem Durchdringen des geschmolzenen Kernmaterials durch die Druckbehälterwand und dessen Eintrag in den Sicherheitsbehälter. Dies setzt voraus, daß alle Notkühlsysteme vollständig und für lange Zeit ausfallen.

Bevor eine solche Situation eintreten kann, müssen zahlreiche Sicherheitsbarrieren versagen, wie wir bei der Diskussion des

Prinzips "gestaffelte Verteidigung" gesehen haben. Im Falle eines Stromausfalls z.B. würde die Turbine automatisch auf Eigenbedarf zurückgeregelt. Sollte diese Prozedur nicht erfolgreich sein, so stehen für jedes deutsche Kernkraftwerk zumindest zwei unabhängige Zuspeiseleitungen für elektrischen Strom von außen zur Verfügung, die nicht mit der Leistungsabgabe nach außen verknüpft sind. Diese Stromeinspeisesysteme könnten dann die Sicherheitssysteme im Reaktor mit Energie versorgen. Sollte diese Einspeisung von außen auch ausfallen, so sind - wie erwähnt - vier Dieselmotoren verfügbar, von denen im Falle des äußersten Notfalls nur einer benötigt würde. Sollte auch keiner dieser vier Notstromdiesel starten, was extrem unwahrscheinlich wäre, so könnte in dem hier skizzierten Szenario, also bei "station black out", die Wärme aus dem Kern durch Öffnen der sekundärseitigen Abblaseventile abgeführt werden, was mittels Batterie erfolgt und durch Nachspeisen von Sekundärwasser mittels der vorher erwähnten Notspeisewasserpumpen, von denen jede einen eigenen Dieselmotor zum Antrieb hat, gewährleistet wird.

Wie erwähnt, sieht die Sicherheitsstrategie des Genehmigungsverfahrens verschiedene gestaffelte Verteidigungslinien gegen einen Störfall und seine Auswirkungen vor. Das Genehmigungsverfahren beinhaltet aber nur die Betrachtung des sogenannten Auslegungsstörfalles, bleibt also innerhalb der Kategorie I, wie sie in Abb.16 kurz skizziert ist, d.h. bei diesem Störfall bleibt das Core voll kühlbar, selbst mit dem in den Sicherheitsregeln geforderten Minimum an Sicherheitssystemen, ja die Temperatur der Brennstabhüllen überschreitet nicht die vorgegebene Obergrenze von 1200° C.

Die Ergebnisse der Risikostudien und, im politischen Bereich, insbesondere auch die Ereignisse von Tschernobyl warfen die Frage auf, was passiert und welche weiteren Verhütungs- und Schutzmöglichkeiten existieren, wenn mehr Sicherheits- und Notkühlsysteme ausfallen, als im Genehmigungsverfahren angenommen, oder wenn gar die gesamte Kette der Sicherheits- und Notkühlsysteme nicht arbeiten würde. Für solche Situationen wurde und wird weltweit über Maßnahmen im Rahmen des sogenannten "accident management" nachgedacht, wodurch weitere Barrieren gegen katastrophale Folgen eines nuklearen Unfalls aufgebaut werden können. Bei diesen "accident management"-Maßnahmen muß man unterscheiden zwischen solchen, die der Verhütung (Preventing) der weiteren Eskalation des Störfalls dienen und solchen, welche versuchen, die Folgen eines Unfalls zu begrenzen bzw. zu verringern (Mitigation). Man kann sicher unterschiedlicher Meinung

sein, wo bei der "Prevention" oder bei der "Mitigation" die Notfallmaßnahmen, also das "accident management" schwerpunktmäßig einsetzen sollen. Im politischen Raum wird gerne der Schwerpunkt auf die "Mitigation" verlegt, da diese Maßnahmen dem Laien leichter verständlich sind. Der Ingenieur und Physiker wird aber versuchen, zuerst den Kern so weit wie möglich intakt zu halten, also sein Augenmerk auf das Ziel "Prevention" zu richten, als zu sehr auf Rückhaltemaßnahmen für bereits freigesetzte radioaktive Stoffe zu vertrauen. Die deutsche Reaktorsicherheitskommission gibt deshalb einhellig den Maßnahmen zur Unfallverhütung, also in Zielrichtung "prevention" den Vorzug.

6. Notfallmaßnahmen und Mensch-Maschine-Wechselwirkung

Jeder schwere Störfall bzw. Unfall geht von einer Situation aus, in der für eine gewisse Zeit im Primärkreis Zustände der Kategorie I herrschen. Die Dauer dieser Zeitspanne wächst mit abnehmender Leckgröße, wie sich anhand von zahlreichen theoretischen und experimentellen Sicherheitsanalysen ergab und wie Abb.17 demonstriert. Bei kleinen Leckagen besteht eine Stunde Toleranzzeit, und bei Störfällen ohne Kühlmittelverlust vergrößert sich diese Toleranzzeit sogar auf zwei Stunden, bis ausgefallene Notkühlsysteme wieder in Betrieb sein müssen oder bis zusätzliche Maßnahmen ergriffen sind. Die Wiederinbetriebnahme bzw. Reaktivierung von ausgefallenen Sicherheitssystemen muß durch die Bedienungsmannschaft mittels Handeingriffe in das Sicherheitssystem erfolgen, ist also ein Vorgang der Mensch-Maschine-Wechselwirkung. Für eine prompte und richtige Aktion bzw. Reaktion der Bedienungsmannschaft im Falle eines hypothetischen Unfalles müssen zwei Bedingungen erfüllt sein:

- Die Bedienungsmannschaft muß korrekt und zuverlässig über die Situation im Primärkreis und insbesondere im Reaktordruckbehälter informiert sein und
- die Bedienungsmannschaft muß klare Vorstellungen haben über die geeignetsten Maßnahmen, eine weitere Eskalation des Stör- bzw. Unfalls zu verhindern und die Unfallfolgen einzudämmen.

Zur Erfüllung der ersten Bedingung sind weitere Verbesserungen derjenigen Instrumentierung von Vorteil, welche die Zustände des Kernes im Reaktordruckbehälter anzeigt. Deshalb wurde bei allen deutschen Druckwasserreaktoren eine Einrichtung in den oberen Teil des Druckbehälters eingebaut, welche den Wasserspiegel von Kernoberkante aufwärts bis in den Bereich des Druckbehälterdomes

mißt. Siedewasserreaktoren haben ohnehin seit langem Meßeinrichtungen, welche den Wasser- bzw. Gemischspiegel im Druckbehälter feststellen lassen. Mit diesen Meßeinrichtungen hat die Bedienungsmannschaft eine eindeutige, zuverlässige, und wie ich meine sicherheitstechnisch auch ausreichende Information über die Kühlbedingungen des Reaktorkernes. Damit ist es für die Bedienungsmannschaft nicht mehr nötig, aus mehreren Signalen wie Druck, Neutronenfluß oder Temperatur auf den Kernzustand zu schließen, oder daraus Kombinationsüberlegungen anzustellen.

Für die Erfüllung der zweiten, oben genannten Bedingung benötigt jeder Reaktorfahrer - also die Bedienungsmannschaft - ein möglichst gutes Training, indem er bzw. sie lernt, wie man hypothetische Unfälle eindämmen und überwinden kann. Dies bedeutet, daß in Zukunft die Ausbildung und das Training an neu zu gestaltenden Simulatoren eine wichtige Rolle spielt. Neue Simulatoren müssen insbesondere in der Richtung entwickelt und zur Verfügung gestellt werden, daß sie in der Lage sind, ein möglichst breites Spektrum von denkbaren Störfällen und Unfällen nachzubilden, wobei die Simulationsanlage auf Aktionen der Bedienungsmannschaft realistisch reagieren muß. Selbstverständlich muß die Unfallentwicklung und auch die Reaktion auf Maßnahmen der Bedienungsmannschaft in Echtzeit simulierbar sein. Diesen Simulatoren kommt insbesondere für Maßnahmen zur Beherrschung von Zuständen der Kategorie II und zur Rückführung des Reaktorzustandes aus der Kategorie II in den der Kategorie I große Bedeutung zu. Eine Situation der Kategorie II bedeutet z.B., daß die Notkühlsysteme oder auch, bei kleinen Lecks oder Störfällen ohne Kühlmittelverlust, alle Speisewassersysteme einschließlich des Notspeisewassersystems für eine gewisse Zeit ausfallen. Dies hätte die Folge eines zunächst begrenzten Coreschadens, aber durch Wiedereinbetriebnahme der Kühlung kann eine Wärmeabfuhr und eine Temperaturabsenkung der Brennstäbe wieder erreicht werden. Die Szenarien des Three Mile Island-Unfalles entsprechen der Definition dieser Kategorie II.

In Abb.18 sind Beispiele für tolerierbare Zeiten des Ausfalles von Wärmeabfuhrsystemen bei Situationen eines großen Lecks aufgelistet. Die erste Zeile in dieser Tabelle demonstriert, daß nur 1 Niederdrucknachkühlpumpe notwendig ist, um die Maximaltemperatur der Brennelementhüllen unter 1200° C zu halten, was auch schon bei der Diskussion der Abb.12 kurz anklang. Dies gilt auch, wenn alle acht Druckspeicher nicht öffnen sollten, was, wie bereits erwähnt, physikalisch unmöglich ist. Sind, wie physikalisch realistisch, sieben Druckspeicher verfügbar und unter-

stellt man, daß alle Notkühlpumpen ausfallen, so besteht, wie man aus der zweiten Zeile von Abb.18 entnehmen kann, eine Zeittoleranz von etwa einer halben Stunde, bis eine der vier Niederdruck-Nachkühlpumpen wieder in Betrieb sein muß, um Wasser in den Kern zu speisen und so ein Schmelzen des Kernes zu verhindern. Der Beginn des Kernschmelzens ist nach zahlreichen Untersuchungen bei 1900°C zu erwarten.

Bei Störfällen mit kleinen Leckagen ist die Situation zwar etwas komplexer aber dafür zeitlich entspannter. Hier muß man zunächst fragen, wie lange dauert es, bis das Sicherheitssystem das Leck entdeckt. Drei unterschiedliche Signale signalisieren das Leck, wie in Abb.19 gezeigt. Es sind dies der Druck im Primärkreis, der Druck im Sicherheitsbehälter und der Wasserstand im Druckhalter. Es ist physikalisch leicht einsichtig, daß die Ansprechzeit dieser Signale eine Funktion der Leckgröße ist, wie Abb.19 ebenfalls demonstriert. Wenn wir die Abhängigkeit der Anzeigezeit von der Leckgröße in Abb.19 betrachten, so müssen wir uns vor Augen führen, daß für sehr kleine Leckagen, die einer Ersatzleckgröße von weniger als 1,5 cm Durchmesser entsprechen, kein Notkühlsystem benötigt wird, da das betriebsmäßige Volumenregelsystem genügend Wasser in den Primärkreis fördert, um den Wasserspiegel im Druckbehälter hoch genug zu halten. Man kann deshalb aus Abb.19 ableiten, daß die automatische Zuschaltung der Hochdruckeinspeisepumpen, also der Hochdrucknotkühlpumpen in jedem Falle früh genug erfolgt. Für die Aktivierung des sekundärseitigen Abblasens, also für das Öffnen der Druckentlastungsventile, ist dann immer noch Zeit, selbst wenn nur eine von vier Hochdruckeinspeisepumpen arbeiten würde.

Wie Abb.20 zeigt, reicht die tolerierbare Verzugszeit für die Aktivierung des sekundärseitigen Abblasens der Dampferzeuger bis zu drei Stunden beim Arbeiten von nur einer Hochdruckeinspeisepumpe und erhöht sich auf fünf Stunden, wenn zwei Hochdruckeinspeisepumpen in Betrieb sind. Die Nachwärme würde dann in jedem Fall, ohne die Temperatur von 1200°C an den Brennelementhüllen zu überschreiten, an die Dampferzeuger abgeführt werden. Würde man ein erstes Anschmelzen der Brennstäbe als oberes Limit betrachten, so würde die tolerierbare Verzugszeit noch wesentlich größer. Erst dann würden Zustände im Kern erreicht, die jenseits des Kategorie II Szenarios liegen.

Der Wärmetransport vom Core zum Dampferzeuger benötigt keine Umwälzung durch Pumpen, sondern erfolgt durch freie Konvektion, die sich automatisch einstellt. Elektrische Energie ist nur not-

wendig für das Öffnen der sekundärseitigen Druckentlastungsventile, was mit Hilfe der Batterie im Falle eines totalen Stromausfalls erfolgen kann. Zusätzlich wird dann allerdings innerhalb einer halben bis einer Stunde elektrische Energie oder der Antrieb eines Dieselmotors benötigt, um zumindest eine der Speisewasserpumpen wieder in Betrieb zu setzen und so das vollständige Ausdampfen der Dampferzeuger zu verhindern, was zu einem Zusammenbruch der Wärmeabfuhr führen würde.

Man kann nun in völlig irrealistischer Annahme unterstellen, daß es innerhalb einer halben bis einer Stunde nicht gelingt, diese elektrische Energie zur Verfügung zu stellen oder wenigstens einen Dieselmotor zu starten. Es würde dann im Primärkreis der Druck steigen, bis das primärseitige Sicherheitsventil öffnet. Durch Abblasen von Primärdampf in den Sicherheitsbehälter kann wieder etwa eine Stunde lang - eventuell auch länger - Wärme aus dem Kern abgeführt werden, ohne daß Schmelzen eintritt. Nach dieser Zeit würde der Wasser- bzw. Gemischspiegel die Oberkante der Brennelemente erreichen, wobei in der folgenden Zeit nun die Gefahr des Kernschmelzens besteht. Bis zu dieser Situation steht aber eine Zeitspanne von mindestens zwei Stunden für Überlegungen und Maßnahmen zur Verfügung.

Unterstellt man nun noch irrealistischer, daß es innerhalb dieser zwei Stunden nicht gelingt, eine Notspeisepumpe und eine Hochdruckeinspeisepumpe in Betrieb zu nehmen, so könnte man weitere Zeit - etwa fünf bis sieben Stunden - dadurch gewinnen, daß man Druckentlastungsventile des Primärkreises ansteuert und den Druck im Primärkreis durch Abblasen auf ein Niveau senkt, das unterhalb des Einspeisedruckes der Druckspeicher, also unterhalb 27 bar liegt. Das von den Druckspeichern in den Primärkreis und in den Reaktordruckbehälter gelangende Wasser reicht dann für die genannten fünf bis sieben Stunden aus, bis es verdampft wäre. Damit würde sich die verfügbare Toleranzzeit bis zur Aktivierung von Not- und Nachkühlpumpen auf sieben bis neun Stunden verlängern. Selbstverständlich wird es oberstes Ziel der Bedienungsmannschaft sein, den Reaktor und seinen Kern ohne Öffnen der primärseitigen Druckentlastungsventile, also bei geschlossenem Primärkreis in einem unbeschädigten Zustand zu halten und die sekundärseitigen Speisewasserpumpen rechtzeitig zu aktivieren.

Bei Temperaturen der Brennelementhüllen oberhalb 800°C setzt, wie wir wissen, eine heftige Wasserstoffbildung durch chemische Reaktion des Zirkons mit Wasser bzw. Wasserdampf ein. Bei sehr

hohen Temperaturen und Kernschmelzen kann diese Wasserstoffbildung durch Bindung des Sauerstoffes des Wassers an Eisen noch erhöht werden. Es wurden deshalb Maßnahmen diskutiert den entstandenen Wasserstoff wieder zu Wasser zu rekombinieren, oder den Wasserstoff im Sicherheitsbehälter frühzeitig zu zünden, bevor sich eine Menge angesammelt hat, welche bei unkontrollierter Zündung zu zu hohen Druckwellen führen würde. Wasserstoffexplosionen wären besonders für den Sicherheitsbehälter von Siedewasserreaktoren gefährlich wegen dessen geringeren Rauminhalts im Vergleich zu denen der Druckwassereaktoren. Die deutsche Reaktorsicherheitskommission empfahl deshalb vor einigen Monaten, alle Sicherheitsbehälter der Siedewasserreaktoren der Baulinie 69 mit Stickstoff zu inertisieren.

Druckwasserreaktoren besitzen seit langem ein Wasserstoffrekombinationssystem, das jedoch nicht für die hohen Wasserstofffreisetzungsraten ausreichen würde, die bei einem Störfall der Kategorie II oder gar einem Unfall der Kategorie III auftreten würden. Nach neuesten sicherheitstechnischen Überlegungen würde erst die Wasserstoffreisetzung während der Kategorie III bei sehr später Zündung zu einer so starken Explosion führen, daß sie den Sicherheitsbehälter der modernen Druckwasserreaktoren gefährden könnte. Man kann dann noch argumentieren, daß eine anfangs nach der Zündung deflagrativ anlaufende Wasserstoffverbrennung infolge Turbulenz in eine Detonation mit den damit verbundenen wesentlich höheren Drücken übergeht. Neueste Messungen zeigten, daß bei einem Wasserdampfanteil von mehr als 33 bis 35% im Reaktorsicherheitsbehälter ein Umschlag von Deflagration in Detonation unter allen strömungstechnisch denkbaren Bedingungen ausgeschlossen ist. Dies legt es nahe, dafür zu sorgen, daß möglichst viel Dampf im Sicherheitsbehälter existiert.

Postuliert man schließlich in Verkennung aller ingenieurmäßigen Möglichkeiten und physikalischen Gegebenheiten, daß alle Maßnahmen zur Verhütung des Kernschmelzens nicht greifen, so würde die Kernschmelze den Reaktordruckbehälter durchdringen und schließlich auf das Betonfundament gelangen. Man müßte dann Maßnahmen zur Eindämmung (Mitigation) der Unfallfolgen in Betracht ziehen und anwenden. Es gibt dann vier verschiedene Pfade, über die die Integrität des Containments verletzt werden könnte und durch die das radioaktive Material in die Umgebung gelangen könnte, nämlich :

- Dampfexplosionen
- Durchschmelzen des Betonfundaments
- Wasserstoffexplosion oder Detonation

- Überdruckversagen des Sicherheitsbehälters.

Die Frage der Beschädigung des Sicherheitsbehälters durch Wasserstoffexplosionen bzw. Detonationen haben wir bereits oben diskutiert.

In der Literatur und bei Institutionen, die sich mit Reaktorsicherheit beschäftigen, konnte und kann man lange Diskussionen verfolgen, ob Dampfexplosionen den Sicherheitsbehälter oder gar den Reaktordruckbehälter zustören können. Unter Dampfexplosion versteht man bekanntlich die thermische Wechselwirkung zwischen Schmelze und Wasser. Es sind zwei Situationen vorstellbar, während deren eine explosionsartige Wechselwirkung zwischen Kernschmelze und Wasser auftreten könnte. Im Falle eines großen Lecks könnte eine Dampfexplosion während der Zeitspanne initiiert werden, während der die Schmelze aus dem Kern in die noch teilweise mit Wasser gefüllte untere Kugelschale des Druckbehälters fließt. Bei einem kleinen Leck oder bei totalem Stromausfall, wo ja der Primärkreis unter hohem Druck steht, würde, wie wir aus Messungen wissen, eine so hohe Trigger-Energie für die Initiierung der Dampfexplosion nötig sein, daß sie in dieser Phase kaum aufgebracht werden kann. Hier ist anzumerken, daß während der Three Mile Island Unfalles Kernschmelze in das im unteren Plenum noch vorhandene Wasser floß, daß jedoch dabei keine Dampfexplosion eintrat.

Eine zweite mögliche Situation für eine Dampfexplosion ergibt sich, wenn beim Druckwasserreaktor die Kernschmelze die Betonabschirmung um den Druckbehälter durchdringt und mit dem außen liegenden Wasserring in Berührung kommt. Bei diesem Vorgang ist jedoch die Mischungsenergie zwischen Schmelze und Wasser sehr klein, da das Wasser langsam über den Schmelzsee fließen wird, bzw. die Schmelze unter das Wasser kriecht. Dieser Zustand kann nicht zu einer heftigen Dampfexplosion führen.

Aus den zahlreichen experimentellen und theoretischen Analysen wurde in der Bundesrepublik Deutschland der Schluß gezogen, daß eine Dampfexplosion, die heftig genug wäre, um den Druckbehälter oder die Wand des Sicherheitsbehälters zu zerstören, eine so große Menge an Schmelze benötigen würde, daß diese unter physikalisch realistischen Annahmen in der kurzen Zeit, die dafür zur Verfügung stünde, nicht bereitgestellt werden kann. Wir haben dabei uns vor Augen zu halten, daß nur wenige Sekunden Zeit verfügbar sind, innerhalb deren eine sehr große Schmelzmenge homogen mit Wasser zu mischen ist ohne daß dabei bereits

Separations- bzw. Absetzeffekte merkbar werden. Dies ist nur denkbar bis zu Schmelzmengen von einigen 100 kg. Diese Mengen sind aber selbst bei spontaner Reaktion für den Druck- bzw. Sicherheitsbehälter ungefährlich. Für deren Zerstörung müßten mehrere Tonnen Schmelze gleichzeitig innerhalb Bruchteile einer Sekunde reagieren, nachdem sie vorher homogen mit Wasser vermischt wurden.

Es ist sehr wahrscheinlich, daß kleine Dampfexplosionen im Laufe eines solchen Unfalles auftreten, sie sind jedoch die beste Garantie dafür, daß keine größeren Wasser-Schmelze-Mischungen entstehen können, da sie immer für einen hohen Dampfanteil im Wasser sorgen, der Dampfexplosionen verhindert, oder zumindest deren Wirkung stark verringert.

Wegen der Auslegung gegen Erdbeben, Flugzeugabsturz und chemische Explosionen von außen ist das Fundament der deutschen Druckwasserreaktoren sehr dick ausgeführt. Es würde deshalb einige Tage dauern, bis nach einem katastrophalen Versagen des Kernes die Schmelze dieses Betonfundament durchdringen könnte. Bis dahin wäre ein Großteil der Radioaktivität in der Schmelze bereits abgeklungen, ein anderer Teil hätte sich an festen Wänden und an Flüssigkeitsfilmen abgelagert. Theoretische Analysen basierend auf einigen Experimenten zeigten, daß die Schmelze nach Durchdringung des Betonfundamentes im Erdreich ausfrieren würde, wobei sie eine glasartige Schale von dichtgepacktem Feststoff um sich bildet.

Hauptsächlich durch Wasserverdampfung aber auch durch Bildung von Kohlendioxyd beginnt der Druck im Sicherheitsbehälter 10 Stunden nach Eintritt des Unfalls zu steigen. Das produzierte CO_2, aber auch der Wasserstoff und Kohlenmonoxyd rühren von Wechselwirkungen zwischen der Schmelze und dem Beton her. Die Verdampfung ist eine Folge des thermischen Kontaktes zwischen Schmelze und Sumpfwasser. Abb. 21 zeigt den zeitlichen Druckverlauf im Sicherheitsbehälter, wie er für den s.g.Niederdruckpfad, also im wesentlichen nach einem großen Bruch im Primärsystem, sich ausbilden würde. Man kann diesem Bild entnehmen, daß stets der Partialdruck des Wasserdampfes den Gesamtdruck im Sicherheitsbehälter maßgebend bestimmt. Nach einer Zeit von 4 bis 5 Tagen hat der Gesamtdruck im Sicherheitsbehälter einen Wert erreicht, der in etwa dem Versagenswert der Sicherheitshülle entsprechen würde.

Dieser zeitliche Druckverlauf ist für den Hochdruckpfad, also

bei kleinem Leck oder bei Ausfall der gesamten elektrischen Energieversorgung, ganz ähnlich, wie man aus Abb.22 sieht. Die Druckspitze, etwa drei Stunden nach Beginn des Unfalles, ist dabei etwas stärker ausgebildet als im Niederdruckpfad, was daher rührt, daß in diesem Augenblick der Reaktordruckbehälter versagt und die Druckspeicher ihr Wasser über die Schmelze strömen lassen. Bei dem in Abb.22 diskutierten Druckverlauf ist anzumerken, daß hierbei keine Druckentlastung des Druckbehälters vor dessen Versagen infolge Einwirkungen der Schmelze angenommen wurde.

In beiden Fällen würde jedoch der von der Sicherheitsbehälterwand abtragbare Druck nach einigen Tagen überschritten werden. Erste Überlegungen gingen davon aus, daß der Sicherheitsbehälter an einer durch die Konstruktion gegebenen Schwachstelle örtlich begrenzt versagt, also daß z.B. eine Durchführung oder auch eine Schleuse soweit öffnet, daß der Druck durch begrenztes Abblasen von Dampf absinkt. Untersuchungen an neueren Anlagen zeigten nun, daß die Konstruktion des Sicherheitsbehälters so vollkommen ist - was sich hier als Nachteil erweist -, daß keine Schwachstellen existieren. Es bestünde also die Gefahr, daß der Sicherheitsbehälter unkontrolliert und mit einem langen Riß öffnet. Es wurden deshalb bereits vor dem Unfall in Tschernobyl in der deutschen Reaktorsicherheitskommission Überlegungen angestellt, den Sicherheitsbehälter durch gezielten Handeingriff rechtzeitig, aber auch nicht zu früh, einer Druckentlastung zuzuführen. In der Zwischenzeit haben die Betreiber hierzu Vorschläge erarbeitet und die Reaktorsicherheitskommission hat sowohl für die deutschen Druckwasserreaktoren als auch für die deutschen Siedewasserreaktoren Notfallmaßnahmen zur Druckentlastung des Sicherheitsbehälters empfohlen.

Bei Druckwasserreaktoren wird, wie Abb.23 am Beispiel des Kernkraftwerkes Unterweser zeigt, hierzu die Durchdringung des Sicherheitsbehälters verwendet, die normalerweise zur Überdruckprüfung dient, an die also die Kompressoren bei dieser Überdruckprüfung angeschlossen sind. Diese Leitung wird innen im Sicherheitsbehälter, wie in Abb.23 links erkenntlich, durch eine Berstscheibe abgeschlossen und an diese Berstscheibe schließt sich dann im Ringraum eine Doppelarmatur an. Im Notfall wird zur Druckentlastung diese Berstscheibe von außen mittels Stickstoffdruck zerstört, es werden dann die Doppelarmaturen geöffnet und das Dampf-Gas-Gemisch strömt über zum großen Teil festverlegte Leitungen einem Metallfaserfilter zu. Dieses Metallfaserfilter scheidet die Aerosole in dem Gemisch ab. Hinter

dem Filter gelangt das Gemisch in den Kamin der Anlage.

Die Druckentlastung würde vorgenommen , wenn der Druck im Sicherheitsbehälter etwa den bei der Druckprobe aufgebrachten Prüfdruck erreicht. Im Sinne einer Minimierung der radioaktiven Belastung der Umgebung erfolgt die Druckentlastung nicht bis zum Umgebungsdruck, sondern nur bis etwa zum halben Prüfdruck des Sicherheitsbehälters. Die Armaturen müssen deshalb auch zuverlässig wieder schließbar sein. Für die Druckentlastung kann ein Zeitraum von ein bis zwei Tagen in Anspruch genommen werden. Langfristig sind darüber hinaus Vorkehrungen zu treffen, daß der infolge Druckentlastung ausströmende Dampf wieder durch Wasser im Sicherheitsbehälter ersetzt wird und gleichzeitig diese Wasserzugabe eine Temperaturabsenkung bewirkt.

Bei Siedewasserreaktoren muß die Druckabsenkung wegen des geringeren Rauminhalts des Sicherheitsbehälters früher erfolgen. Dadurch ist die Jodaktivität höher als bei der Druckentlastung eines Druckwasserreaktors. Die Filterung muß deshalb in der Lage sein, nicht nur Aerosole, sondern im begrenzten Maße auch Jod abzuscheiden. Deshalb wurde eine Filtereinrichtung gewählt, wie sie in Abb.24 zusammen mit den Druckentlastungsvorrichtungen skizziert ist. Die Abströmung erfolgt aus dem Dampfraum der Kondensationskammer des Sicherheitsbehälters und das Dampf-Gas-Gemisch strömt zunächst einem Naßwäscher zu, bevor es, ähnlich wie beim Druckwasserreaktor, in ein Metallfaserfilter gelangt. Hinter der Filtereinrichtung befindet sich eine Drosselstelle, um die ausströmende Menge zu begrenzen. Die gesamte, bisher diskutierte Druckentlastungsstrecke ist hinter der Drosselstelle durch eine Berstscheibe abgeschlossen. Diese Berstscheibe wird im Notfall durch Stickstoff aufgedrückt. Da das ausströmende Gemisch hohe Anteile an Wasserstoff enthält, der beim Einleiten in den Kamin - nach Mischung mit der dort vorhandenen Luft - zünden könnte, wurde die Ausströmöffnung neben den Kamin in eine Höhe von 50 bis 100 m gelegt.

Damit können die Folgen von hypothetischen Störfällen wirksam eingedämmt werden.

Es scheint zweckmäßig und sinnvoll, bei zukünftigen Überlegungen zur Verbesserung der Sicherheit von Kernreaktoren Augenmerk auf die Möglichkeiten des "accident management", also der ingenieurmäßigen Notfallmaßnahmen zu legen. Die Betriebsmannschaft ist gewohnt und gehalten, nach Vorschriften vorzugehen, die bisher im Betriebshandbuch festgelegt sind. Bei Störfällen sind diese

Vorschriften im Betriebshandbuch meist ereignisorientiert formuliert, was bedeutet, daß sich die Bedienungsmannschaft erst klar darüber werden muß, welches Fehlverhalten den Reaktorstörfall auslöste. Dies kann Zeit kosten, kann aber auch zu Trugschlüssen führen. Deshalb sind Vorbereitungen im Gange, parallel zu ereignisorientierten Maßnahmen auch schutzzielorientierte Maßnahmen in das Betriebshandbuch aufzunehmen.

Weiterhin ist ein Notfallhandbuch in Vorbereitung, das gemeinsam mit dem Hersteller KWU und den Betreibern ausgearbeitet wird. Es dürfte in seinen Maßnahmen überwiegend schutzzielorientiert sein. Die Schutzzielorientierung hat den Vorteil, daß die Bedienungsmannschaft nur auf wenige Schutzzielzustände achten muß, nämlich Unterkritikalität, Kühlung des Kerns, zulässigen Druck und zuverlässigen Sicherheitsabschluß. Alle Maßnahmen brauchen also nur an diesen Zielen gemessen zu werden. Ihre Überwachung ist einfach, insbesondere auch dadurch, daß alle deutschen Reaktoren die Möglichkeit der Wasserstandsanzeige, zumindest oberhalb des Kernes, besitzen.

7. Internationale Kooperation in der Reaktorsicherheit

Für die Zukunft scheint eine engere internationale Kooperation auf dem Gebiet der Reaktorsicherheit fachlich wie politisch geboten zu sein. Fachlich empfiehlt sich diese Kooperation vor allem zum Austausch von Betriebserfahrungen der weltweit stromerzeugenden Kernkraftwerke, um daraus rechtzeitig und frühzeitig sicherheitstechnische Maßnahmen und Anweisungen für das Betriebspersonal ableiten zu können. Politisch ist eine solche Kooperation anzuraten, um sicherheitstechnische Regelwerke im internationalen Rahmen zu harmonisieren und eventuelle neue sicherheitstechnische Anforderungen auf ihre internationale Kompatibilität zu prüfen.

Seit Jahren besteht eine gute Zusammmenarbeit und ein fruchtbarer, reger Erfahrungsaustausch zwischen der Group Permenant eacteurs, dem Advisory Committee for Reactor Safety der Vereinigten Staaten und der deutschen Reaktorsicherheitskommission. Seit etwas über einem Jahr hat sich erfreulicherweise auch die japanische Reaktorsicherheitskommission in diese Beratungen und in diesen Erfahrungsaustausch eingeschaltet. Die Gespräche in und zwischen diesen Kommissionen haben sehr viel zu dem hohen internationalen Standard der Reaktorischerheit beigetragen. Es wäre sicher sinnvoll und nützlich auch andere Nationen, die Kernreaktoren bauen und Kernenergie nutzen, in

diesen Erfahrungsaustausch einzubeziehen.

Reactivity Incidents and Malfunction of Control Elements

Loss of Auxiliary Power Supply

Loss of Coolant from the Reactor Coolant System

- inside the Containment with/without Necessity of Heat Removal on the Secondary Site
- outside the Containment (Failure of an Instrument Line)

Loss of Coolant from the Secondary System

- with Operational Leakages from the Reactor Coolant System
- with Defective Steam Generator Heating Tubes

Steam Generator Heating Tube Failure

Malfunctions in Auxiliary and Ancillary Systems

Malfunctions and Incidents during Fuel Element Handling and Storage

Internal Plant Floodings

Internal Plant Fires and Explosion

External Natural Impacts

External Man–induced Impacts

Fig.1 Design Basis Incidents

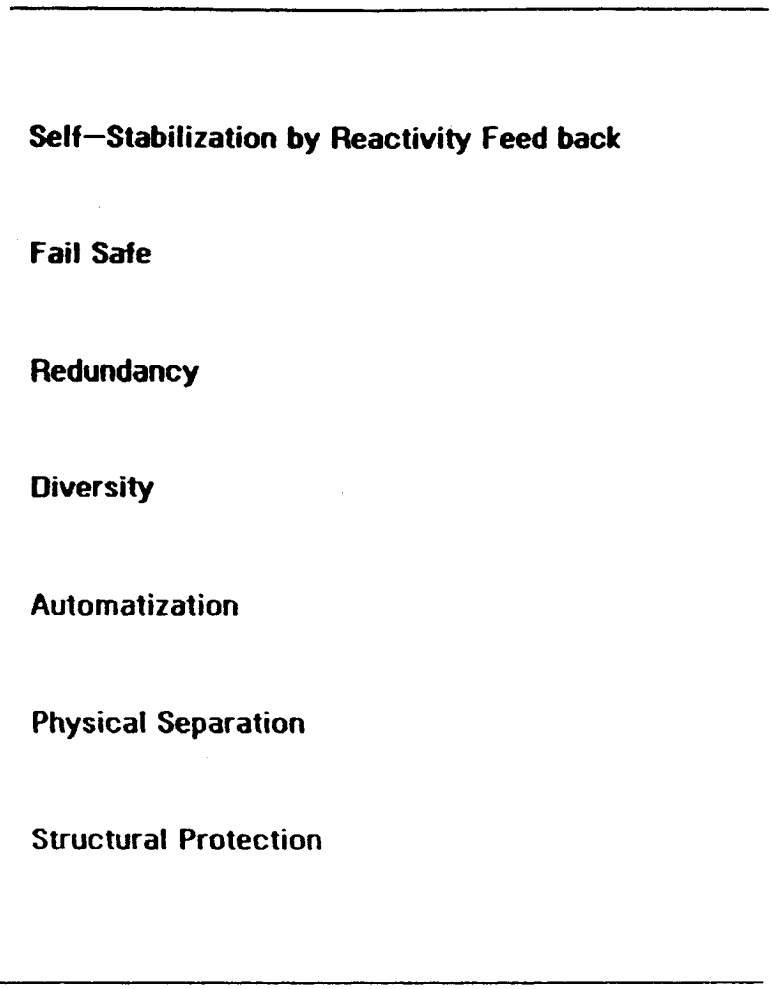


Fig.2 Main Principals of Safety Engineering

- Design Materials and Manufacturing

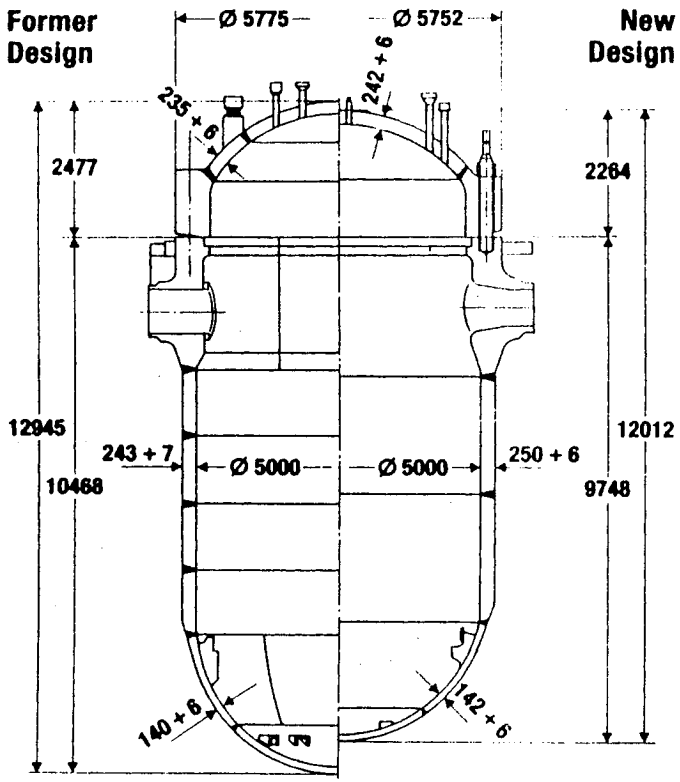
  - use of licensed material
  - high toughness of material
  - corrosion resistance
  - reduced number of welds
  - logitudinal welds avoided
  - reliable manufacturing methods
  - low nominal stresses during operation

- Validation of Design Assumptions (Calculations)

- Inservice Inspections
  - access and possibility for non destructive examination

- Quality Assurance

Fig.3 High Quality Measures for Pressure Retaining Components



	Biblis A	KKP 2
Number of circumferential welds	8	5
Number of longitudinal welds	10	0
Total length of welds	143 m	78 m

Fig.4 Reduction of Number and Length of Welds by Improved Reactor Pressure Vessel (PWR)

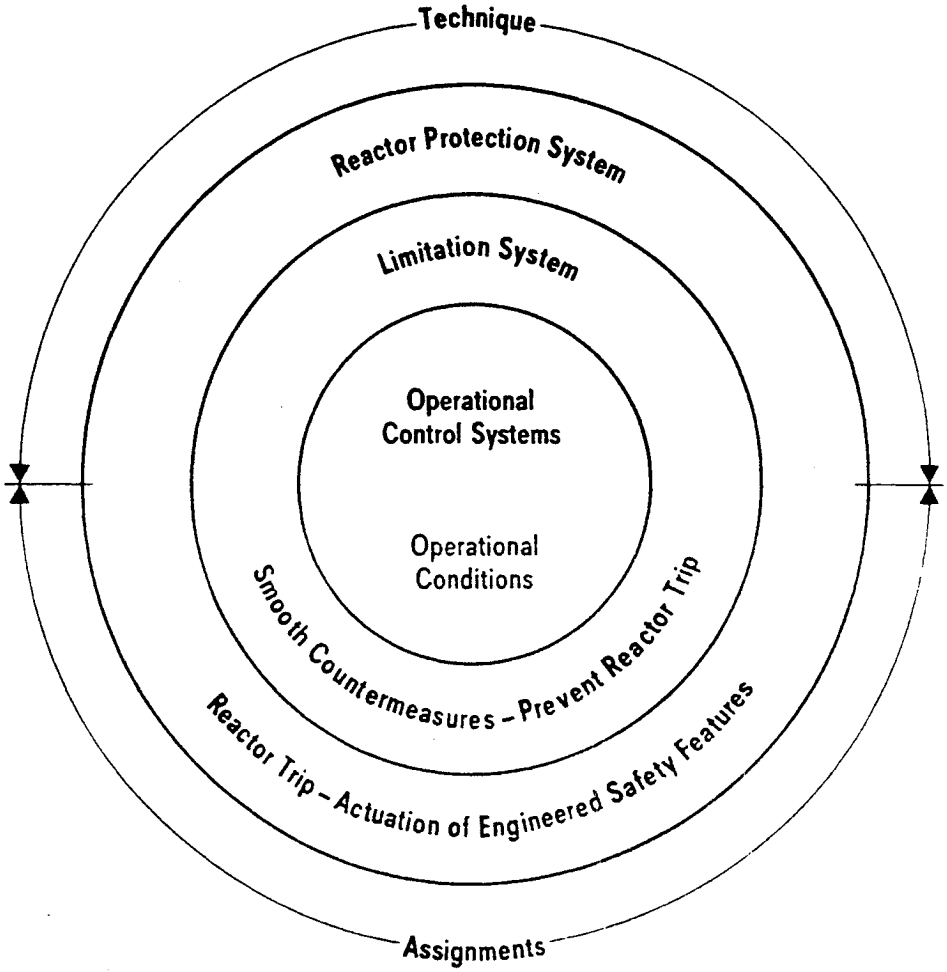


Fig.5 Concept of "Defense-in-Depth"

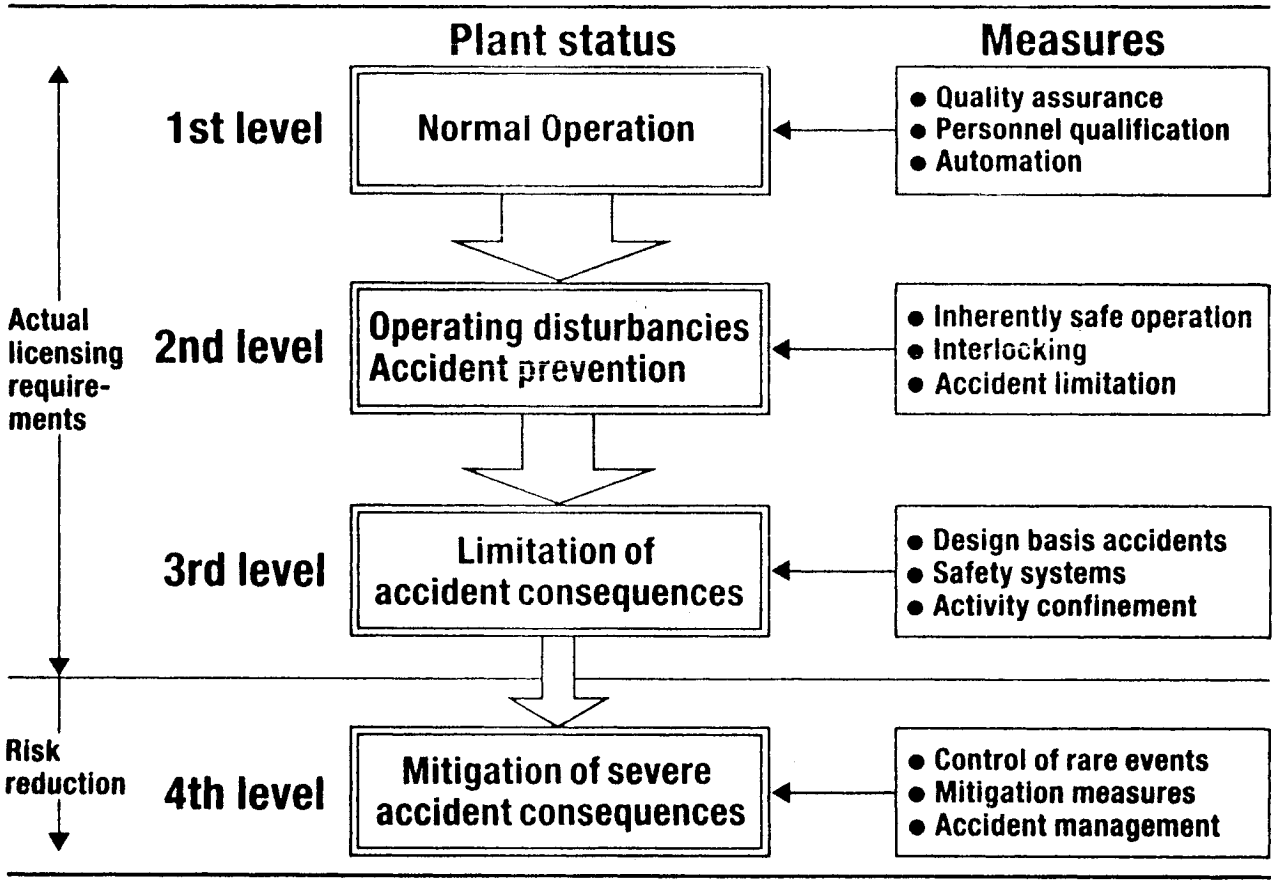


Fig.6 LWR Multilevel Concept of Plant Safety

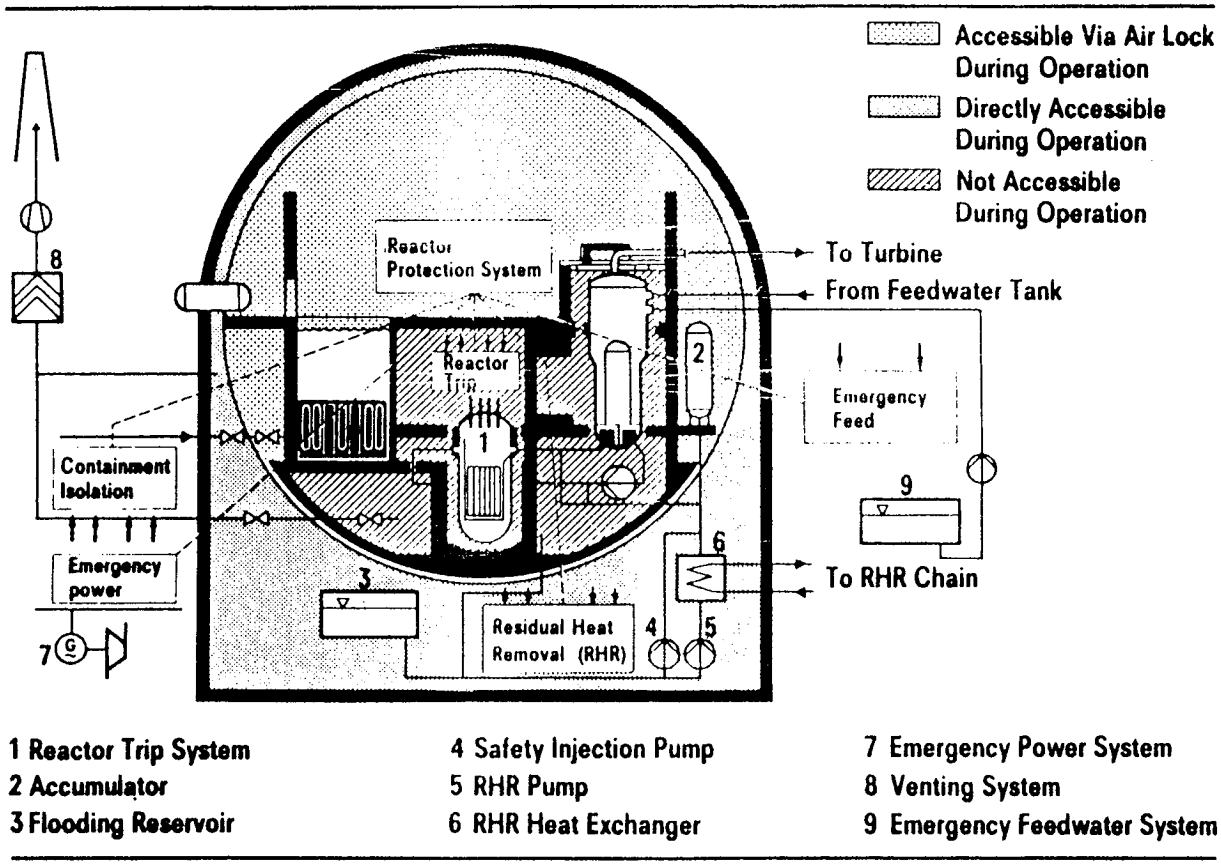


Fig.7 Engineered Safety Features

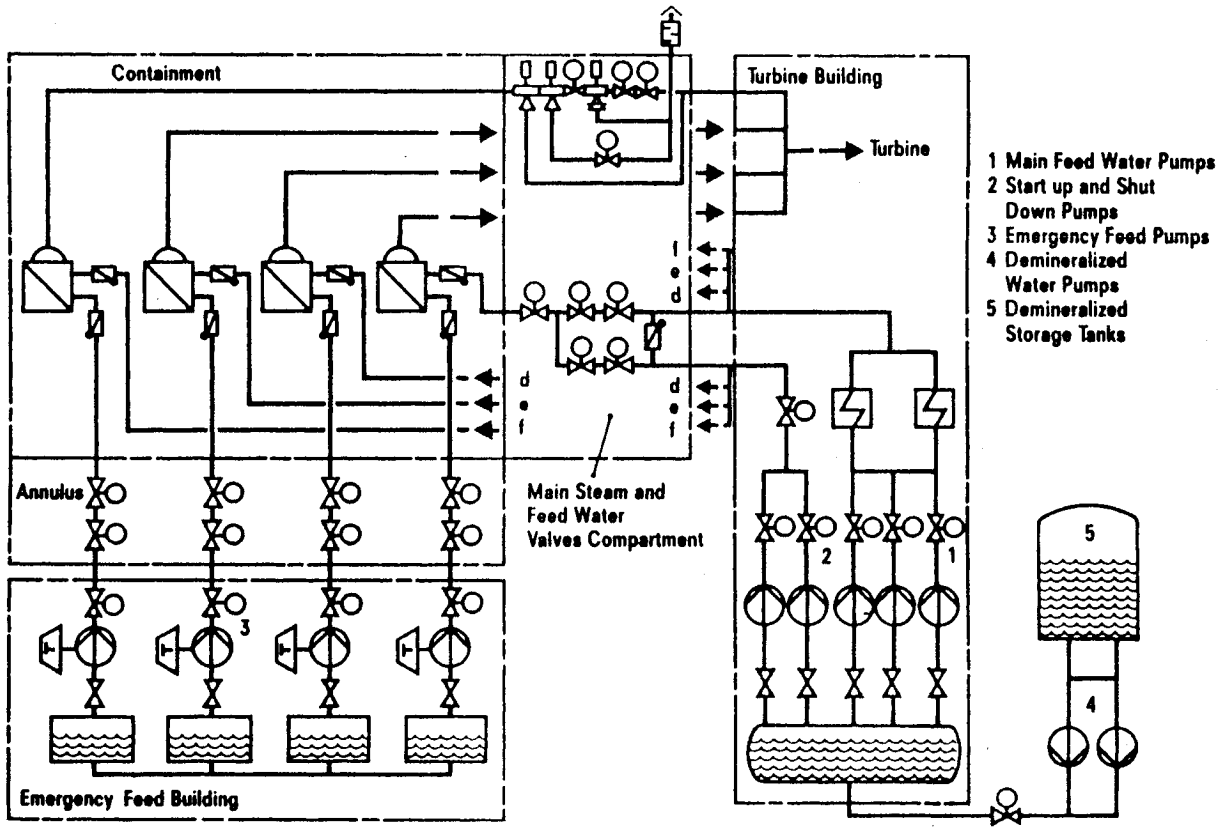


Fig.8 Main Steam System and Steam Generator Feeding

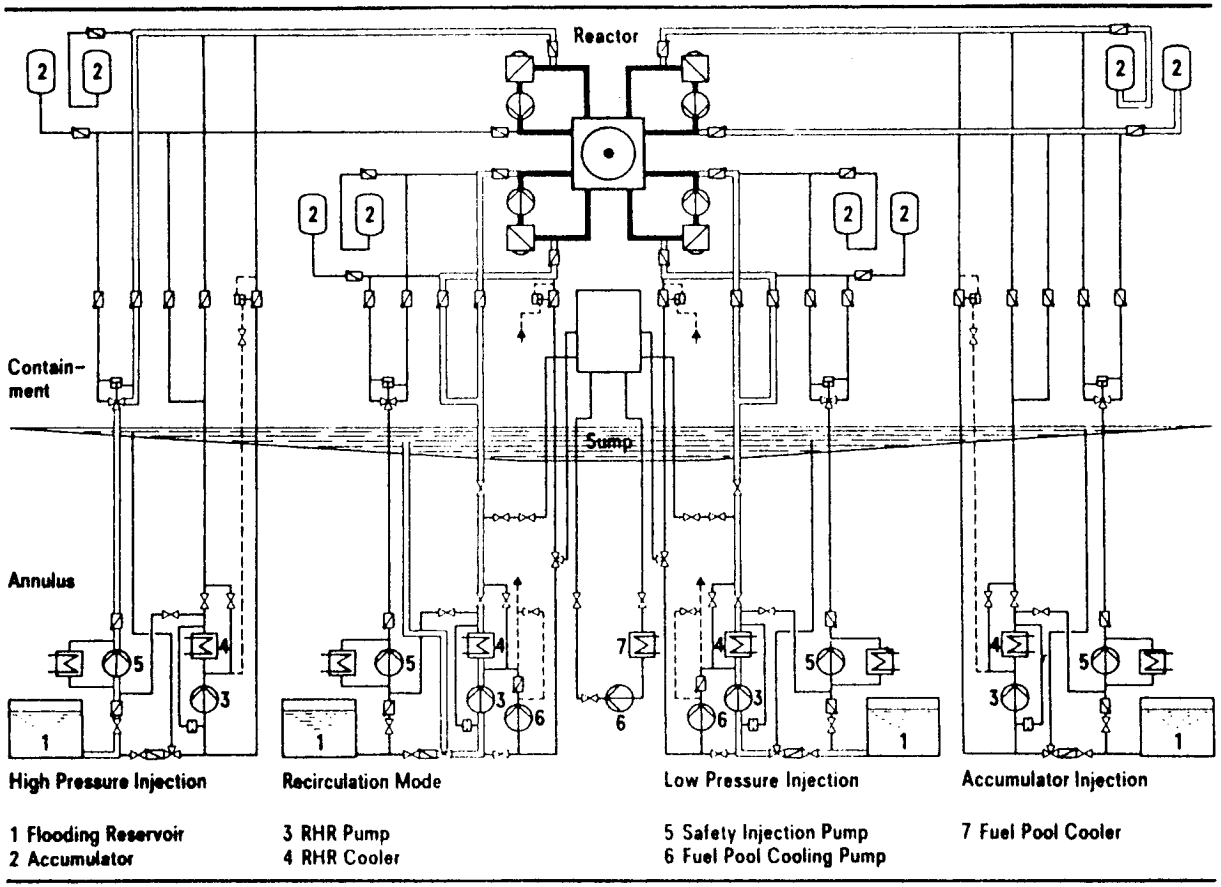


Fig.9 KWU-PWR 1300 MW
Emergency Cooling and Residual Heat Removal System

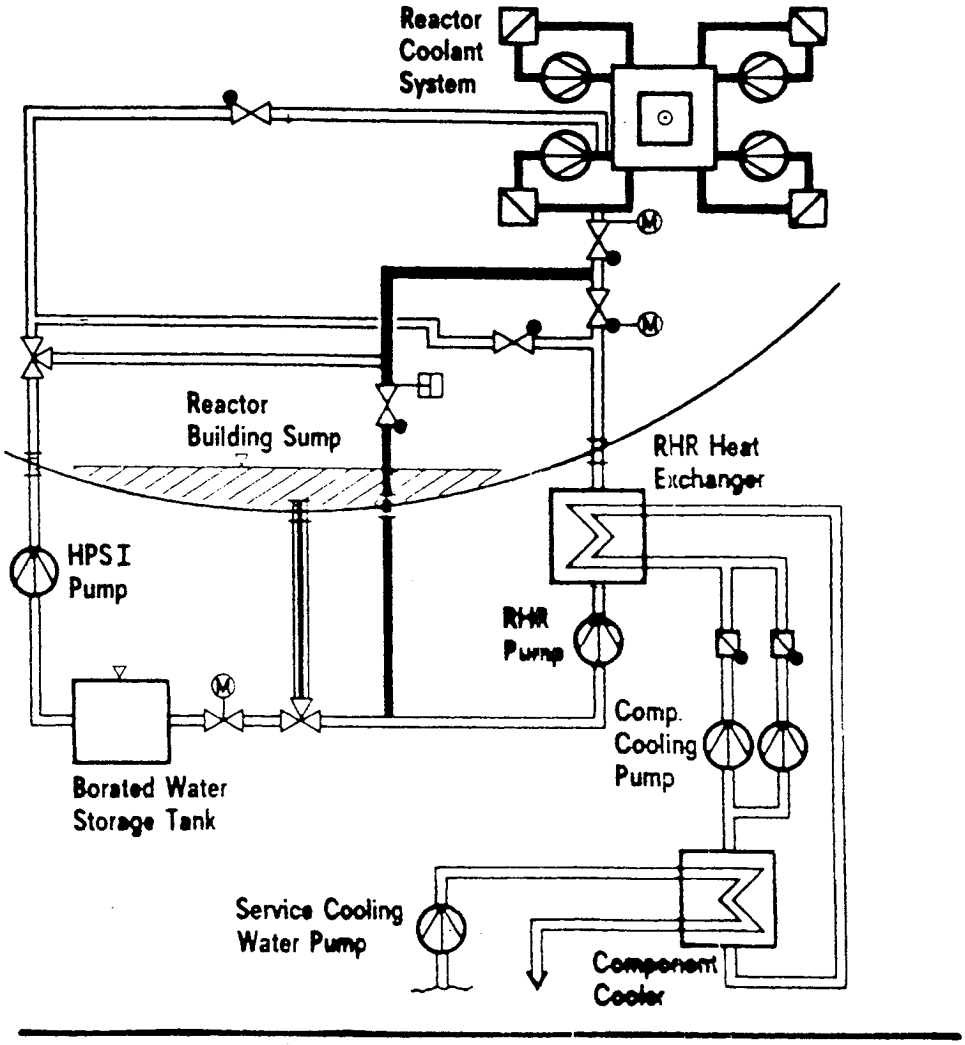


Fig.10 Schematic Diagram of a
Heat Removal Chain at Primary-Side
PWR 1300 MW-Convoy Plant

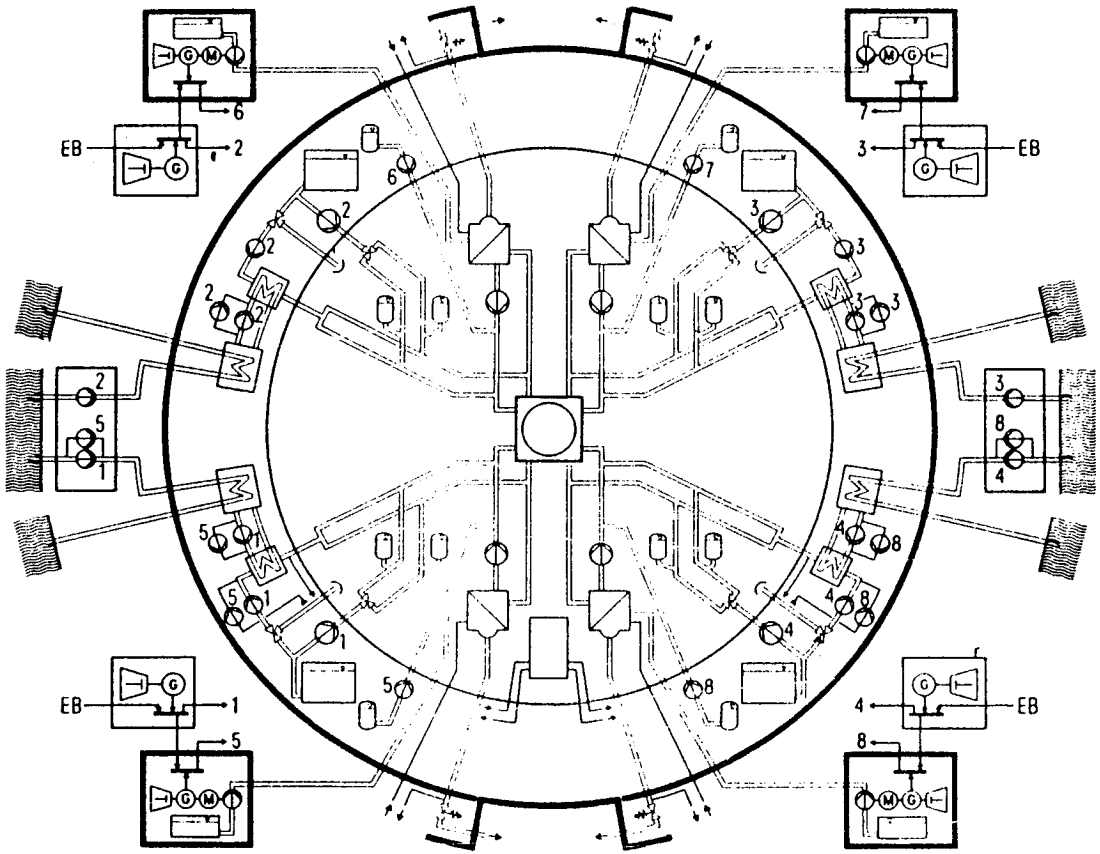


Abb.11 DWR 1300 MW Not- und Nachkühlung
4-Strang Konzept

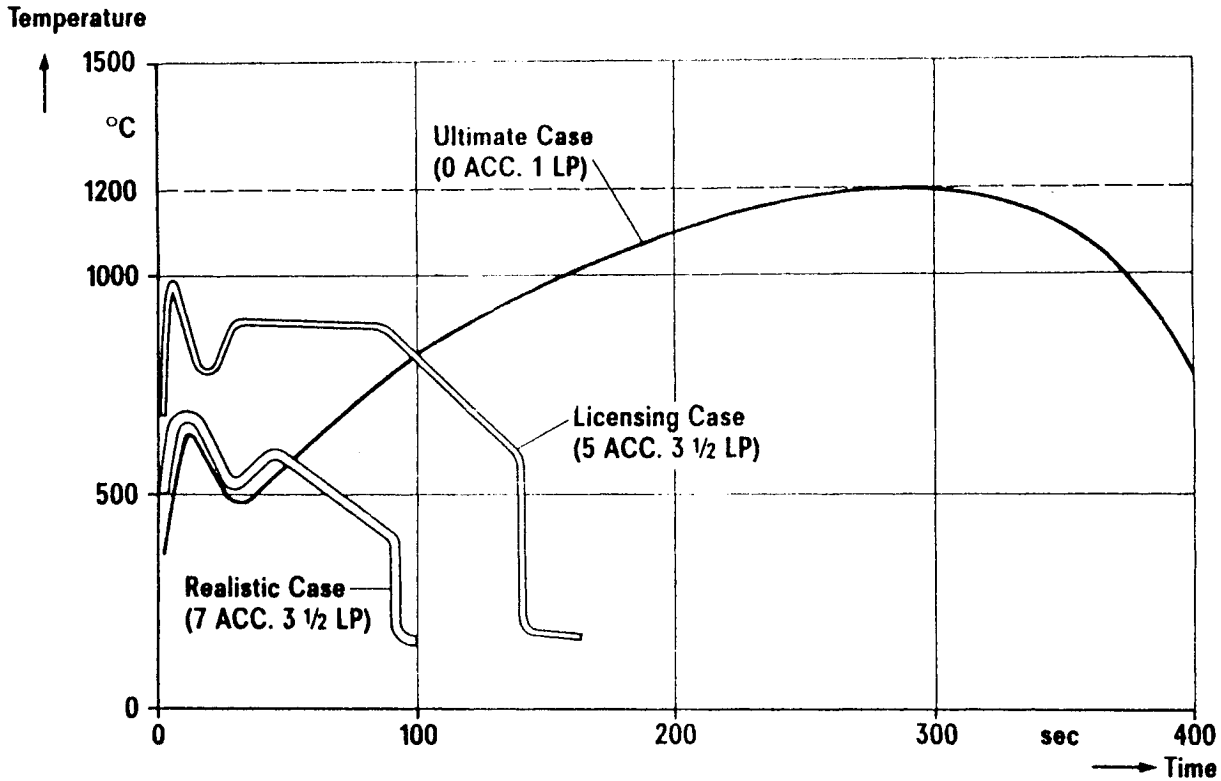


Fig.12 Maximal Cladding Temperature as a Function of Time for a large LOCA

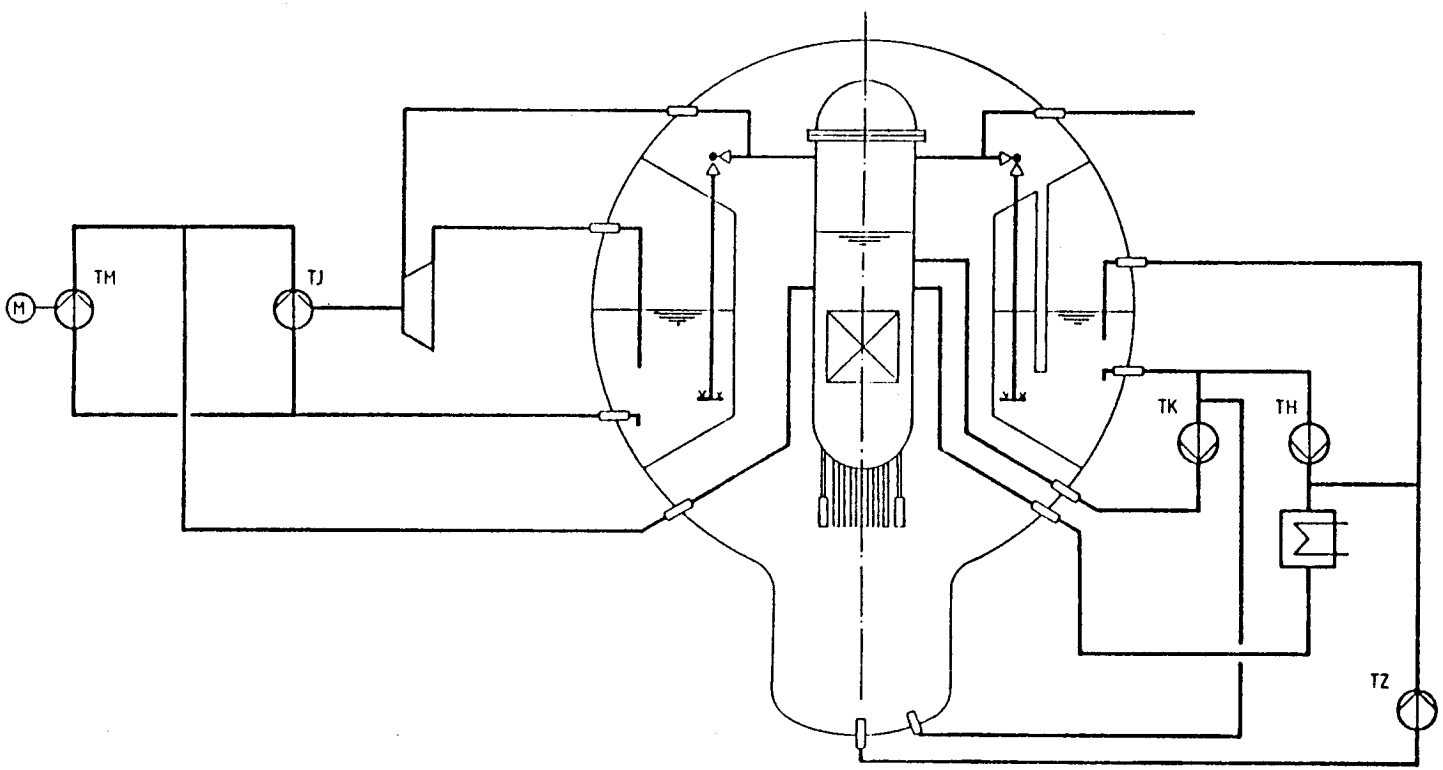


Abb.13 Not- und Nachkühlsysteme

1 Vorstufe
2 Niederdruckstufe
3 Hochdruckpumpe
4 Frischdampfleitung
5 Speisewasserleitung
6 Durchführungsabsaugsystem
7 Vergiftungssystem
8 Schnellabschaltsystem

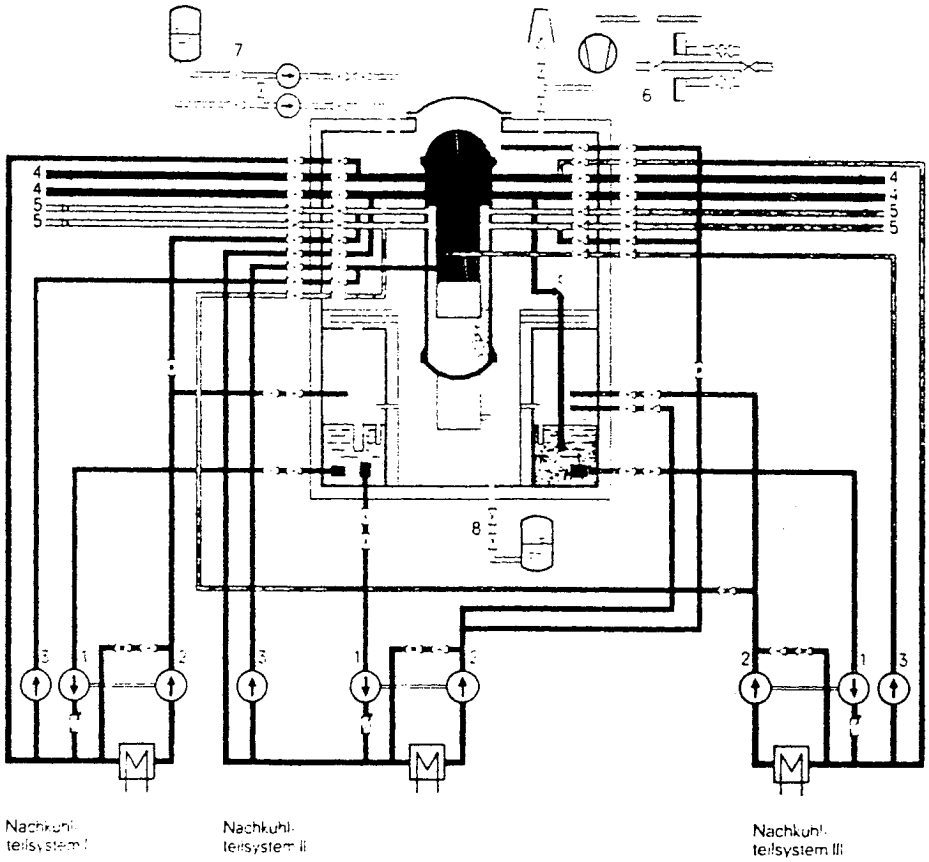


Abb.14 Nachkühlsystem vom SWR

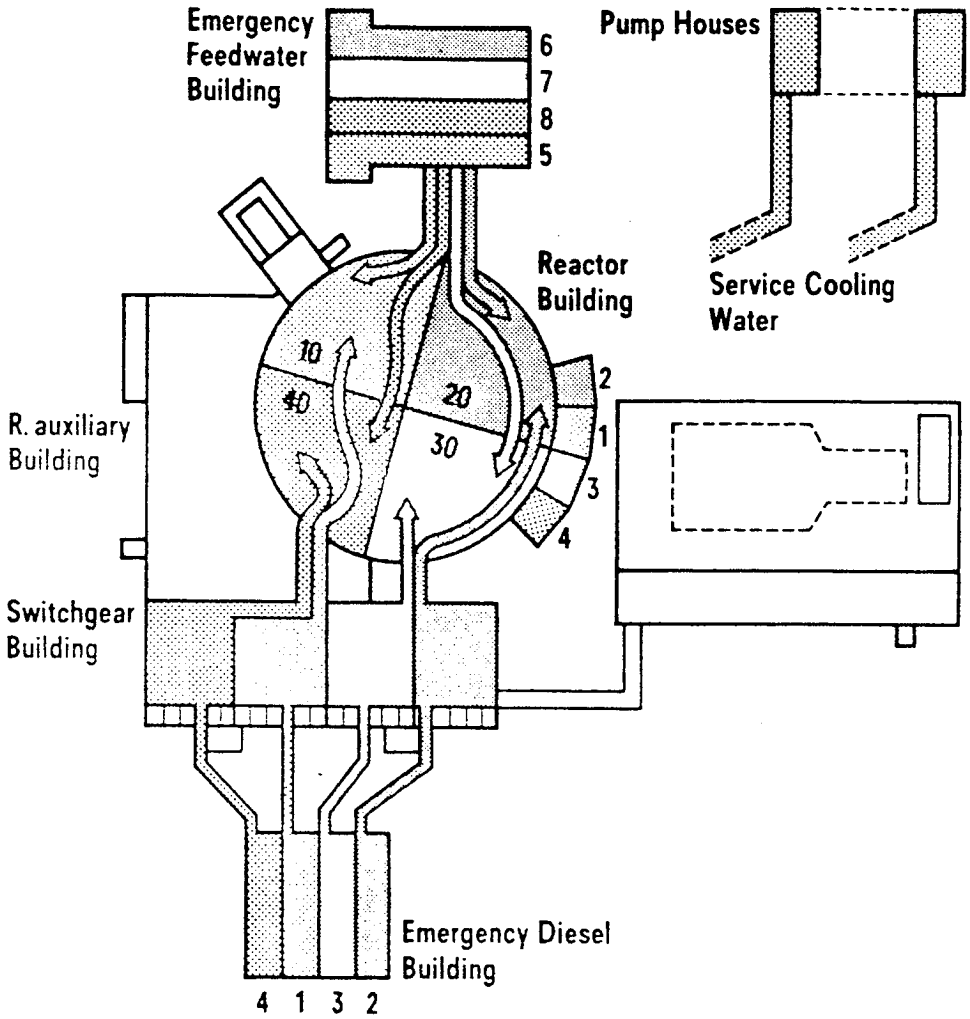


Fig.15 Protection against External Impacts and Redundancies KWU 1300 MW PWR

CATEGORY I : Requirements of licensing not fulfilled, but full coolability of the core possible with remaining safety systems. Temperature limits of licensing not exceeded.

CATEGORY II : Accident sequences with severe core damage. By reinforced cooling, however, a long-term decay heat removal can be reached. (TMI acc.)

CATEGORY III : Accident sequences with complete core melting and penetration of molten corium into the containment.

Fig.16 Classification of accidents

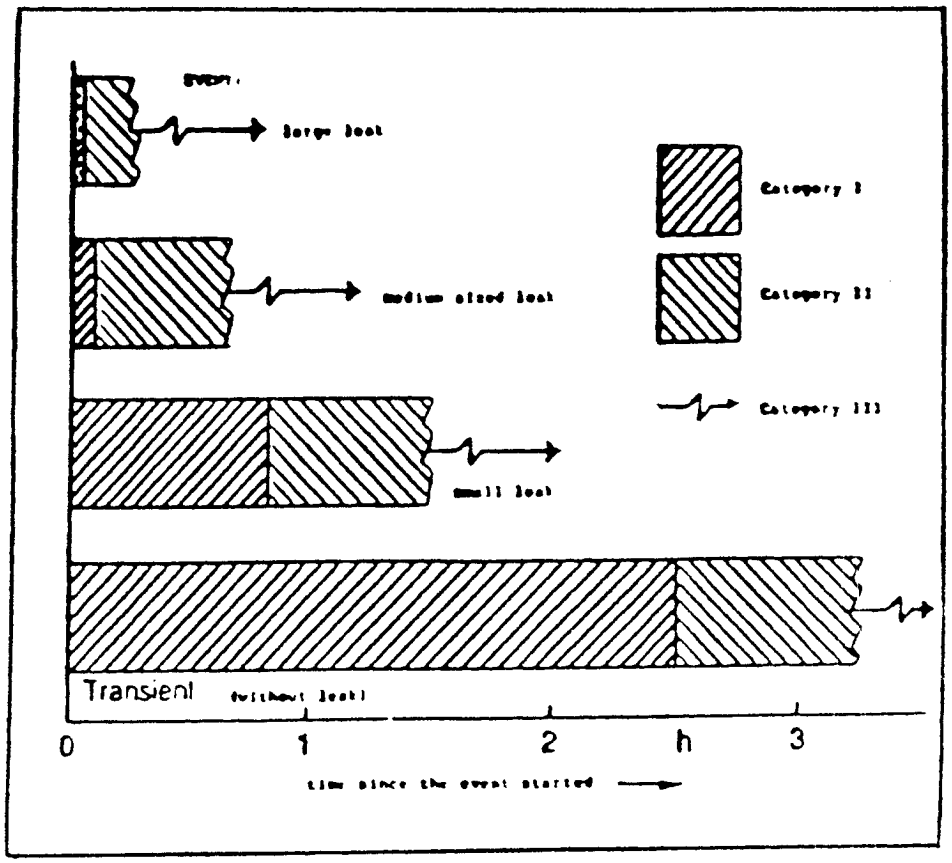


Fig.17 Time history of hypothetical accidents and time of tolerance for reinforcing safety systems

LARGE BREAK

break size	location	availability of systems SIP	Accum.	RHR-pump	activation delay of RHR-pumps
2.A	cold leg	0 of 4	0 of 8	1 of 4	none
2.A	cold leg	0 of 4	7 of 8	1 of 4	0.5 h

Fig.18 Tolerable activation delay of residual heat removal (RHR) pumps to avoid local core melting

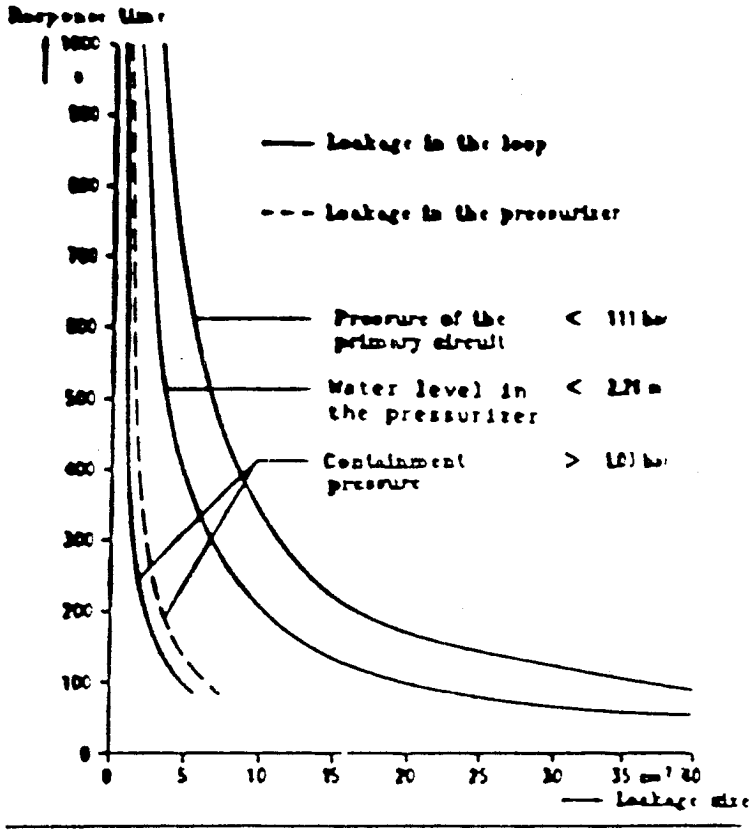


Fig.19 Response time of safety signals of a 1300 MW PWR

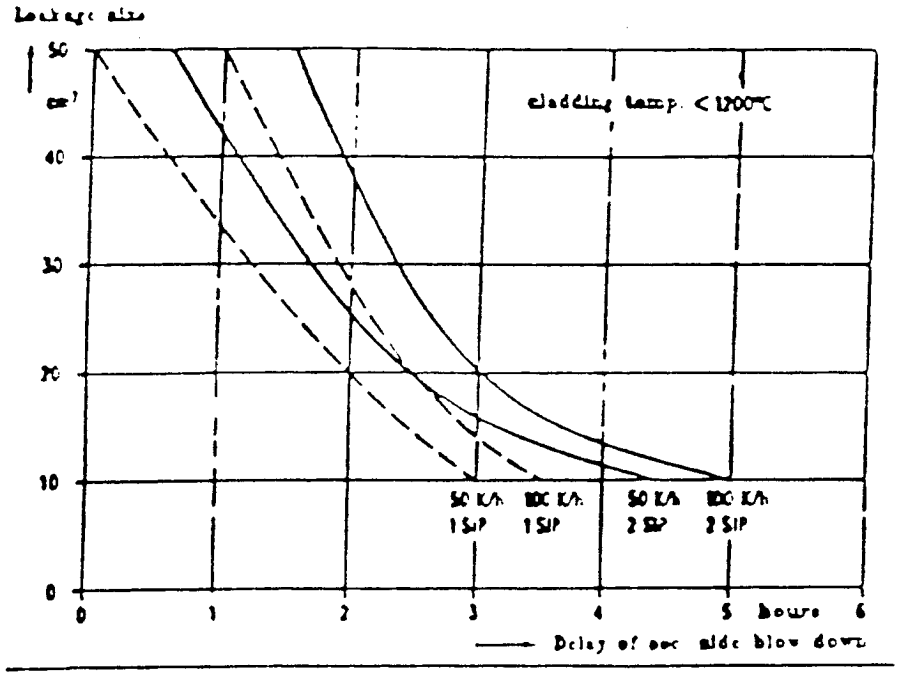


Fig.20 Emergency cooling analysis in case of reduced system availability and delayed sec.side blow-down (1300 MW PWR)

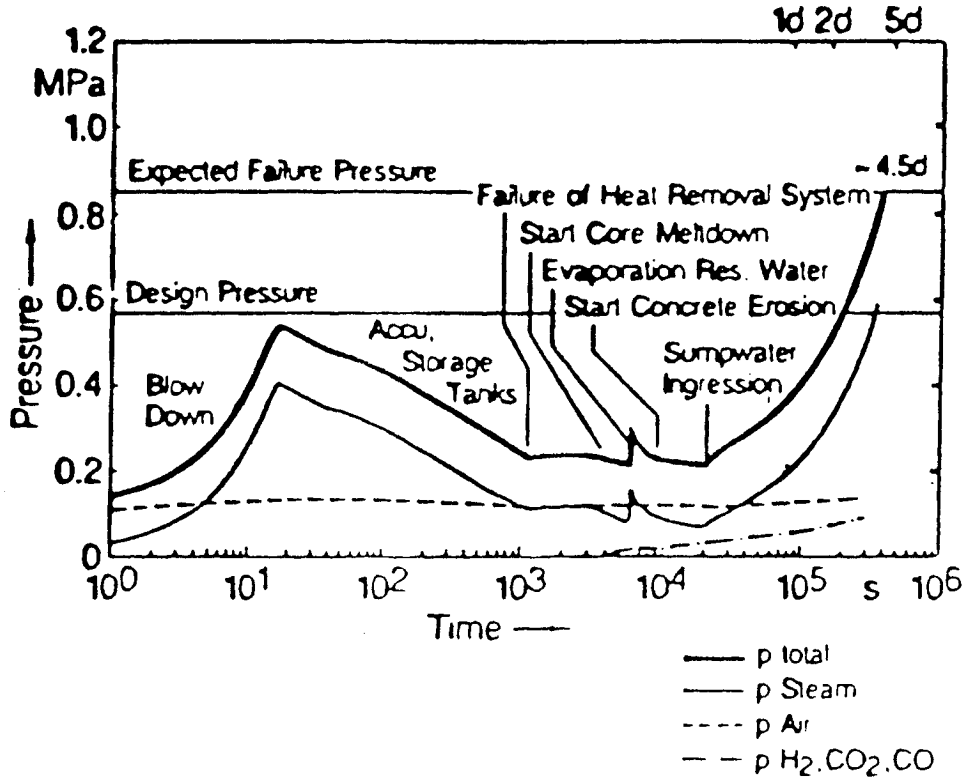


Fig.21 Containment pressure-time history (Low pressure case)

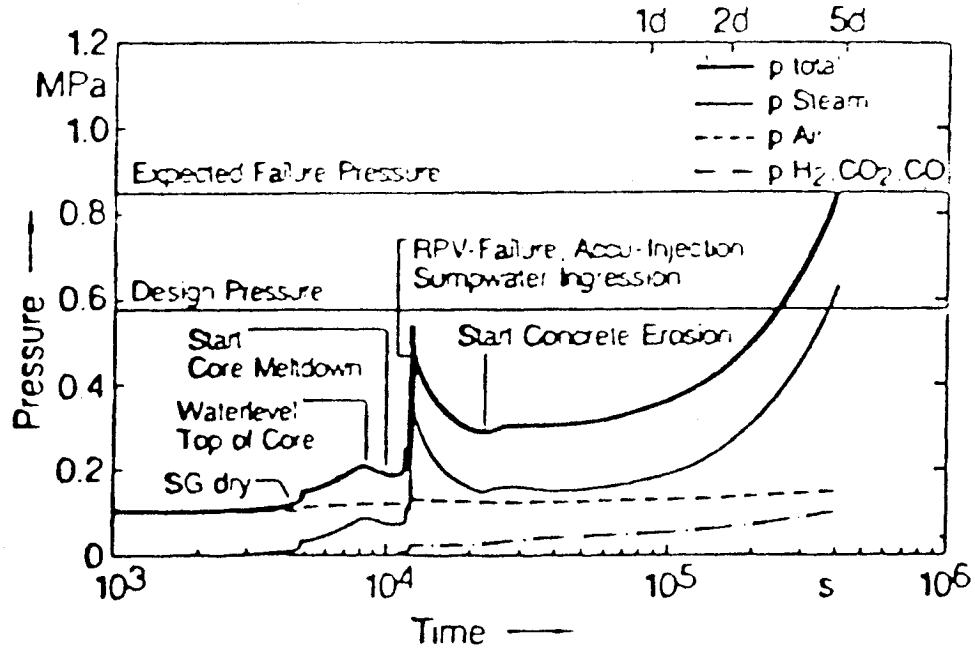


Fig.22 Containment pressure-time history (High pressure case)

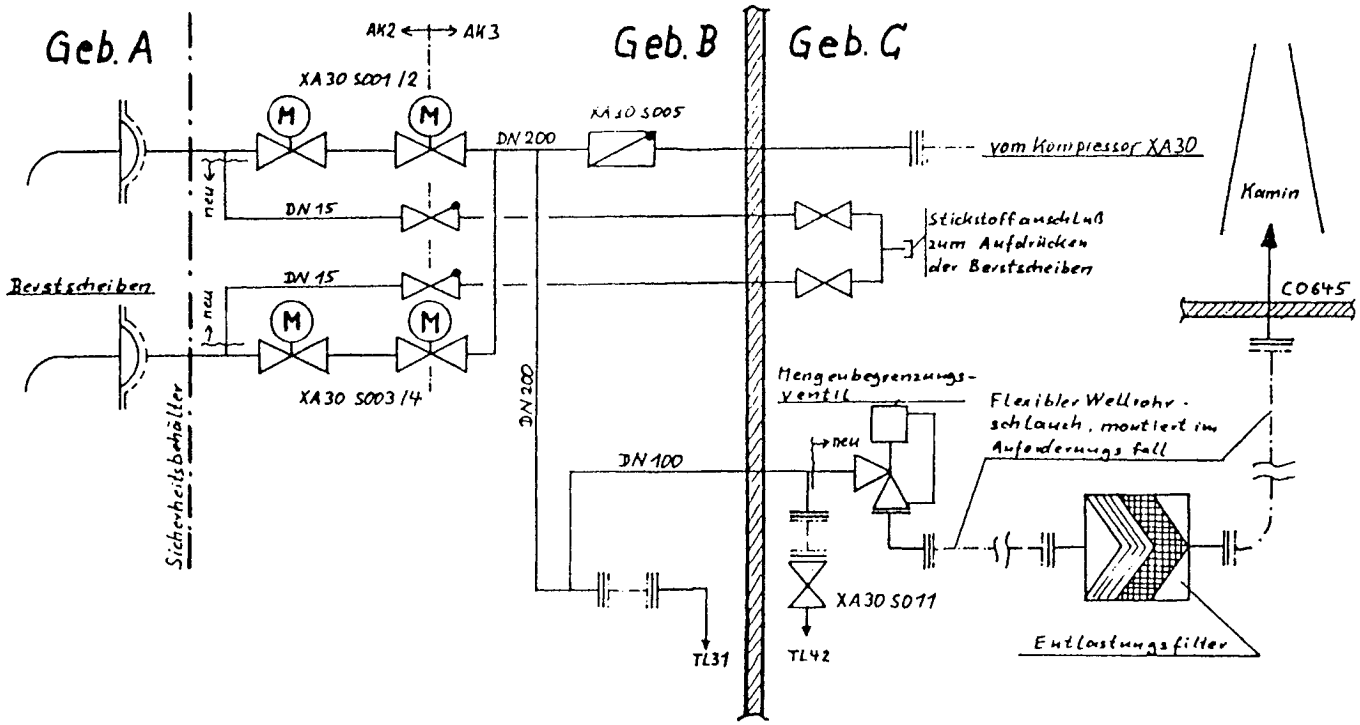


Abb.23 Kernkraftwerk Unterweser
Leitungen zur Druckentlastung des Sicherheitsbehälters

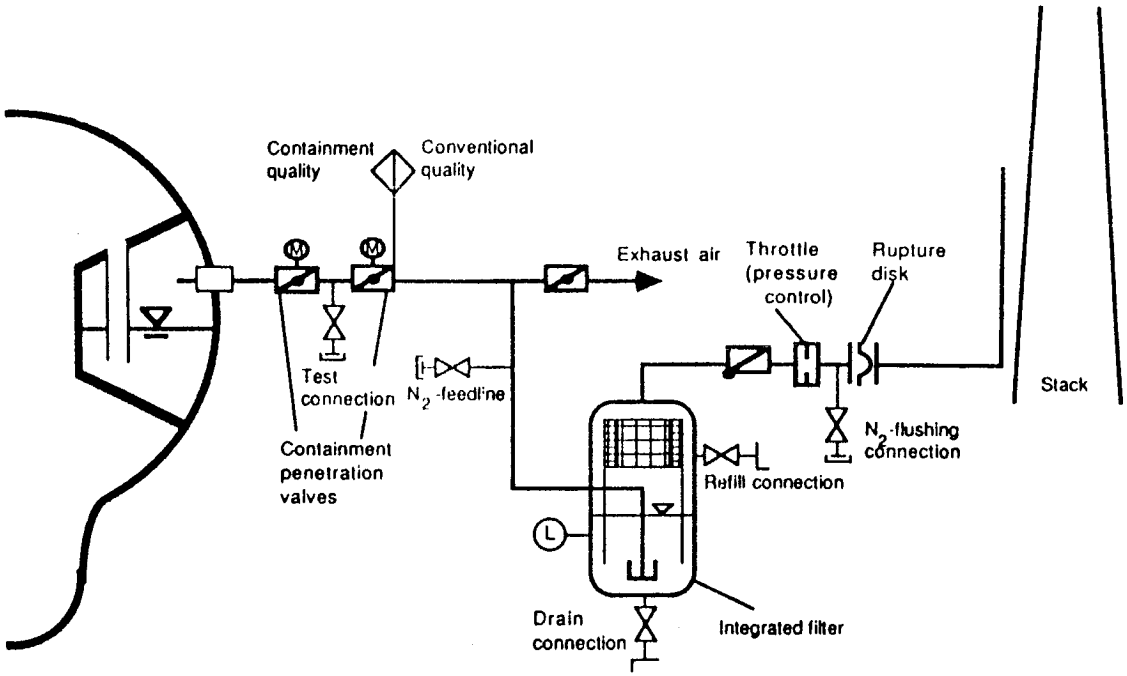


Abb.24 Containment Pressure Relief and Filtered Venting KKK