Gesellschaft für
Reaktorsicherheit (GRS) mbH

Entwicklungen zur Leittechnik in Kernkraftwerken

9. GRS-Fachgespräch
München,
7.–8. November 1985

GRS 61

Gesellschaft für
Reaktorsicherheit (GRS) mbH

Entwicklungen zur Leittechnik in Kernkraftwerken

9. GRS-Fachgespräch
München,
7.–8. November 1985

GRS 61 (Februar 1986)
ISBN 3 - 923875 - 09 - 6

Herausgeber: Gesellschaft für Reaktorsicherheit (GRS) mbH, Köln
Redaktion: B. Laue, GRS, Köln

Diese Beiträge wurden gleichzeitig in der Zeitschrift „Technische Mitteilungen" Heft 1 · 1986 im Vulkan-Verlag Dr. W. Classen Nachf. GmbH & Co. KG, Postfach 10 39 62, 4300 Essen 1, veröffentlicht.

Inhaltsverzeichnis

Entwicklungen zur Leittechnik in Kernkraftwerken

9. GRS-Fachgespräch vom 7. und 8. November 1985 in München

Eröffnung

Von O. Kellermann[1])

Die Bundesrepublik Deutschland hat vor 30 Jahren mit der friedlichen Nutzung der Kernenergie begonnen. Wenige Wochen nach der ersten Genfer Atom-Konferenz erhielt Franz Joseph Strauß im Oktober 1955 aus der Hand von Professor Heuß seine Ernennungsurkunde zum Bundesminister für Atomfragen. Der Start war frei für die deutschen Atomprogramme, für die Errichtung von Kernforschungsanlagen und für das erste Kernkraftwerk Kahl, das in der kommenden Woche den 25. Jahrestag seiner Betriebsaufnahme feiert.

Für die Ingenieure in München und Köln waren damals die Startbedingungen in beiden Ländern etwa gleich. In Bayern und in Nordrhein-Westfalen waren je ein 15-MW-Kernkraftwerk und eine Kernforschungsanlage sicherheitstechnisch zu bewerten.

Wenn wir heute über die Kernenergieentwicklung in den beiden Sitzländern unserer Institute Bilanz ziehen, ergibt sich folgendes Bild:

- in Bayern ist in den zehn Jahren von 1974 bis 1984 die Stromerzeugung um 50 % gestiegen, der Kernenergieanteil von 6 auf 49 %,
- in Nordrhein-Westfalen stieg die Stromerzeugung um 28 %, der Kernenergieanteil stieg lediglich von 0,4 auf 3 %.

Die GRS hatte sich auf die differenzierte Haltung der Bundesländer zur Kernenergie einstellen müssen. Inzwischen ist unsere Mitwirkung in den Genehmigungsverfahren allerdings stark zurückgegangen. Wir sehen derzeit und in den kommenden Jahren unsere Hauptaktivitäten bei der Auswertung von Betriebserfahrungen und bei der Verbesserung der Schadensvorsorge. Die Bewertung neuer Konzepte und die Optimierung von Sicherheitsanforderungen sind eine weitere mittelfristige Aufgabe. Die Entsorgung und Wiederaufarbeitung haben wir als GRS-Aufgabe im vergangenen Jahr vorgestellt.

Schließlich soll hier erwähnt werden, daß unsere Gesellschafter, der Bund, die Sitzländer und die Sachverständigenorganisationen im Mai dieses Jahres eine Änderung des Gesellschaftsvertrages beschlossen haben, die uns in die Lage versetzt, die gewonnenen Erkenntnisse und Erfahrungen auch für den Umweltschutz zu nutzen. Wir haben auf diesem neuen Arbeitsgebiet bereits einige Aufgaben übernommen und wir werden uns in engem Kontakt mit den Gesellschaftern um sachgerechte Lösungen bemühen.

Das Thema des diesjährigen Fachgespräches lautet

„Entwicklungen zur Leittechnik in Kernkraftwerken".

Es gibt kaum eine industrielle Anlage, in der so viele Daten erfaßt, gesammelt, verarbeitet und umgesetzt werden wie in einem Kernkraftwerk. Seine Instrumentierung umfaßt mehr als 10 000 Meßstellen. Aus den vielen in der Warte vorliegenden Anzeigen und Daten auch

[1]) Dipl.-Ing. Otto Kellermann ist Geschäftsführer der Gesellschaft für Reaktorsicherheit (GRS) mbH

bei gestörtem Betrieb die richtigen Handlungen herzuleiten, ist eine Aufgabe, die nur bei guter Informationsaufbereitung und -darstellung gelöst werden kann.

Den Prozeßrechnern kommt dabei die wichtigste Aufgabe zu. Durch frühzeitige Reaktion auf Störungen lassen sich Aktionen des Reaktorschutzsystems verhindern. Jede Schnellabschaltung bringt eine Belastung der Komponenten und Systeme mit sich. Das Verhindern einer Reaktorschnellabschaltung durch frühzeitigen, weichen Eingriff trägt also zur Schonung der Anlage bei und kann die Lebensdauer des Kraftwerks verlängern.

Es entspricht der langen Tradition deutscher Kraftwerksbetreiber, in Eigeninitiative um hohe Sicherheit und Verfügbarkeit ihrer Anlagen bemüht zu sein. So ist es eindrucksvoll, welche Aufwendungen unsere Energieversorgungsunternehmen aufgrund der Betriebserfahrungen in den vergangenen zwanzig Jahren für zusätzliche Sicherheit geleistet haben.

Die Betriebserfahrungen und die Ergebnisse von Analysen haben immer wieder zu Aufrüstmaßnahmen geführt, die zwar im Moment Kosten verursachten, sich aber langfristig auszahlen. Als Gegensatz soll hier das Verhalten mancher amerikanischer Betreiber herausgestellt werden, die selbst gravierenden Fehlern im Primärsystem mit Reparaturmaßnahmen abhelfen, die bei uns überhaupt nicht zur Diskussion stehen. Beispiele sind Auftragsschweißungen auf Rohrleitungen und Klemmverbindungen zur Entlastung fehlerhafter Schweißnähte. Vergleichbare Fehler in den Rohrleitungen hiesiger Anlagen haben zum völligen Austausch des Primärsystems geführt, wobei Betreiber und Hersteller freiwillig über die jeweiligen Forderungen der Genehmigungsbehörden hinausgegangen sind.

Alle deutschen Kernkraftwerke sind Schritt für Schritt nachgerüstet worden. Sie haben Wertzuwachs und eine höhere Verfügbarkeit erreicht. Auch bei einer geplanten Anlagenlebensdauer von 40 Jahren bestehen keine Bedenken, insbesondere was Werkstoffermüdung, Korrosion und Strahlenversprödung angeht.

Die hohe Verfügbarkeit bedeutet aber nicht, daß die Sicherheitsfragen vernachlässigt werden dürfen. Wir freuen uns, daß der Bundesminister des Innern das ebenso sieht wie wir. Neben den Aktivitäten zur Schadensvorsorge und Optimierung muß im Zusammenhang mit dem Thema unseres Fachgespräches hier besonders erwähnt werden: Die Leittechnik.

Echte Verbesserungen lassen sich noch erzielen und auch bei in Betrieb befindlichen Anlagen mit vertretbarem Aufwand realisieren. Diese Verbesserungen werden auf die Langzeitsicherheit einen positiven Einfluß haben.

Unsere Bemühungen um Qualifizierung der Leittechnik im Blick auf Sicherheitsziele laufen durchaus mit den Interessen der Elektrizitätswirtschaft zur Verbesserung der Wirtschaftlichkeit parallel.

In dieser Woche ging eine Nachricht durch die Medien, wie es sie in den dreißig Jahren Kerntechnik noch nie gegeben hat: Ein deutsches Kernkraftwerk, das KKW Emsland, kann ein halbes Jahr früher ans Netz gehen als geplant. Eine fast unglaubliche Nachricht für alle, die die Irritationen, Verzögerungen, Eskalationen der 70er Jahre erlebt haben.

Der Bundesinnenminister und sein Haus haben maßgeblichen Anteil daran, daß so eine Nachricht möglich wurde.

Für die GRS und für die Kerntechnische Gemeinschaft ist der Besuch des Bundesinnenministers eine besondere Ehre und Ermunterung. In den vergangenen Jahren waren wir häufig die Zielscheibe der Kritik und persönlicher Angriffe. Die Gedanken und Beschlüsse mehrerer Politiker waren und sind manchmal für uns unerforschlich. Umsomehr tut es uns gut, heute Unterstützung durch den zuständigen Bundesminister zu erhalten, und daraus zu lernen, daß unsere Arbeit und der Nutzen der Kernenergie für die Bundesrepublik Deutschland und ihre Bewohner anerkannt wird.

Begrüßungsansprache

Von Bundesinnenminister Dr. Friedrich Zimmermann

Mit ihren Fachgesprächen stellt die Gesellschaft für Reaktorsicherheit (GRS) alljährlich einem größeren Publikum ihre Aufgabenschwerpunkte vor. Sie tritt damit den Beweis für ihre Qualifikation und ihre Kompetenz auf dem Gebiet der kerntechnischen Sicherheit ebenso an wie für ihre an rein naturwissenschaftlichen Kriterien orientierte Arbeitsweise. Sie unterwirft sich damit dem Urteil der Fachwelt, und ich meine, sie kann dies getrost tun.

Seit vielen Jahren ist die solide Arbeit der GRS eine wesentliche Voraussetzung dafür, daß unsere kerntechnischen Einrichtungen sicher und umweltfreundlich betrieben werden. Sie wissen, daß ich vor kurzem dem Deutschen Bundestag wieder berichten konnte, daß es 1984 in deutschen Kernkraftwerken keine Störfälle oder gar Unfälle gegeben hat. Auch in diesem Jahr war der Betrieb von Kernkraftwerken frei von besorgniserregenden Störungen. Hieran haben die grundlegenden Arbeiten der GRS gewichtigen Anteil. Ich begrüße es deshalb, daß zwischen den Gesellschaftern der GRS, nämlich den TÜV, den Ländern Nordrhein-Westfalen und Bayern sowie dem Bund Übereinstimmung erzielt werden konnte, daß die GRS ihr im Bereich der Kerntechnik erworbenes Know-how nunmehr auch im allgemeinen Umweltschutz einsetzen wird. Das Markenzeichen GRS, ihr bewährtes ingenieurtechnisches und analytisches Potential erschließt sich damit für einen Bereich, der mir als Umweltminister des Bundes naturgemäß besonders am Herzen liegt.

Zum Schutz des Menschen und seiner Umwelt zähle ich auch den Schutz vor ionisierenden Strahlen, gleichwohl ob es sich dabei um die Strahlenbelastung aus Baustoffen, aus der medizinischen Therapie oder aus der friedlichen Nutzung der Kernenergie handelt. Hier möchte ich an die GRS appellieren, ihre Tätigkeit auf diesem Felde zu intensivieren. Es geht mir dabei um die Lösung von grundsätzlichen strahlenschutztechnischen Fragen, wobei wir selbstverständlich bei dem Erreichten, das auch und gerade im internationalen Vergleich einen besonders hohen Standard aufweist, nicht haltmachen dürfen.

Aber so sehr wir danach trachten müssen, die Strahlenbelastung auch unterhalb der durch die Rechtsordnung ausdrücklich zugelassenen Schwelle weiter zu senken, müssen wir dies auch mit Augenmaß tun, nämlich unter Abwägung des Aufwandes und des Sicherheitsgewinns. Deshalb möchte ich hier, weil dies bei vielen immer noch mißverstanden wird, ausdrücklich feststellen:

Das international anerkannte ALARA-Prinzip (as low as reasonably achievable) gilt selbstverständlich auch bei uns, es heißt nur in unserer Rechtssprache etwas anders, nämlich „Ausübung des pflichtgemäßen Ermessens nach erfolgter Güterabwägung der einzusetzenden Mittel im Verhältnis zum angestrebten Zweck". Ich erwarte, daß dieser Punkt bei den jetzt angestellten Überlegungen zur Novellierung der Strahlenschutzverordnung ebenso präzisiert wird wie die Definitionen zur Störfall-Unfall-Abgrenzung.

Die GRS hat für ihr diesjähriges Fachgespräch das Thema „Entwicklungen zur Leittechnik in Kernkraftwerken" gewählt. Ich halte dies für eine gute Wahl, weil heute in der Tat die Beobachtung von Weiterentwicklungen der Sicherheitstechnik zur Optimierung von Betriebsabläufen im Vordergrund steht gegenüber den grundsätzlichen Überlegungen zur Auslegung der Leichtwasserreaktoren. Die Auslegung hat einen hohen Reifegrad erreicht, jetzt heißt es die Lehren zu ziehen, die sich aus der Betriebserfahrung ergeben können.

Die Bundesregierung hat ihren Beitrag dazu geleistet. Am 1. Oktober 1985 habe ich neue Kriterien für die Meldung von besonderen Vorkommnissen in Kraft gesetzt. Präziser und detaillierter als in der Vergangenheit legen sie fest, welche Vorkommnisse den atomrechtlichen Aufsichtsbehörden innerhalb welcher Fristen anzuzeigen sind. Es ist nun Sache der Betriebstechniker, daraus Erfahrungen zu gewinnen.

Unabhängig davon müssen Überlegungen angestellt werden, welche weiteren Technologien zur Sicherung eines störungsfreien Betriebs eingesetzt werden können. Dabei scheinen mir gerade die Entwicklungen auf dem Gebiet der Leittechnik besonders zukunftsweisend zu sein. Ich denke dabei vor allem an die Mikrocomputer, die mit Riesenschritten immer weitere Gebiete der Technik und unseres täglichen Lebens erobern. Auch bei der Überwachung und Steuerung eines so komplexen Gebildes, wie es ein Kernkraftwerk darstellt, werden sie ihren Einsatz finden. Sie können helfen, den Anlagenbetrieb zu optimieren, die Bedienungsmannschaft von Routineaufgaben zu befreien, und sie können für schwierige Entscheidungen exakt aufbereitete Informationen liefern. Was bei der Raumfahrt und der Luftfahrt möglich und nutzbringend ist, sollte auch in Kernkraftwerken erreichbar sein. Allerdings dürfen wir Computern sicherheitstechnische Aufgaben in Kernkraftwerken erst dann übertragen, wenn sie nachweisbar fehlerfrei arbeiten. Wir dürfen uns nicht der Gefahr von „quasi vorprogrammierten Störfällen" aussetzen. Es bedarf deshalb einer sorgsamen Entwicklung. Ich bin sicher, daß sich unsere Gutachterorganisationen und die Industrie dieser Herausforderung stellen werden.

Wie bei allen Regeln, gibt es auch bei der Aussage über eine grundsätzliche Verlagerung von den Sicherheitsfragen bei der Auslegung der Anlage zur sicherheitstechnischen Optimierung des Betriebs Ausnahmen. Ich denke hier insbesondere an die fortgeschrittenen Reaktorlinien und die Wiederaufarbeitung von Kernbrennstoffen.

Die Bundesregierung hat nie einen Zweifel daran gelassen, daß im Sinne einer vorausschauenden Energiepolitik die Weiterentwicklung des Schnellen Brüters ebenso erforderlich ist wie die des Hochtemperaturreaktors. Deshalb wird sie auch auf die Inbetriebnahme des SNR 300 drängen.

Es ist in diesen Tagen so oft davon die Rede, daß das Genehmigungsverfahren „streng nach Recht und Gesetz" durchgeführt werde. Ich frage mich, warum dies – eine bare Selbstverständlichkeit – immer wieder betont wird. Wenn ich das so häufig höre, fühle ich mich fatal an jenen „Dienst nach Vorschrift" erinnert, den vor Jahren Fluglotsen ausgeübt haben und der bekanntlich eine erhebliche Beeinträchtigung des Flugverkehrs mit sich brachte. Ich hoffe sehr, daß ähnliches mit solchen Wendungen heute nicht gemeint ist.

Die Bundesregierung wird jedenfalls das Ihre dazu tun, daß über den Antrag des Betreibers frei von politischen Einflüssen unverzüglich nach Vorliegen der sicherheitstechnischen Voraussetzungen in den dafür seit Jahren bewährten Verfahren entschieden wird. Für mich als den Sicherheitsminister des Bundes, der über die korrekte Ausführung des Atomgesetzes zu wachen hat, ist dies das alleinige Entscheidungskriterium. Das gilt selbstverständlich ebenso für die Wiederaufarbeitungsanlage in Wackersdorf, für die die Bayerische Staatsregierung am 27. September 1985 die 1. Teilerrichtungsgenehmigung erteilt hat.

Internationale Erfahrungen – auch in den Staaten, die wie wir die Kernenergie zu ausschließlich friedlichen Zwecken nutzen – zeigen, daß die Wiederaufarbeitungstechnologie in einer Weise beherrscht werden kann, daß jedwede Gefahr für die in der Anlage Tätigen ebenso ausgeschlossen ist wie für die Umgebungsbevölkerung.

Auch in der Umgebung der britischen Wiederaufarbeitungsanlage Sellafield hat es entgegen den Behauptungen in Presse und Fernsehen keine Strahlenbelastungen von Personen gegeben, die – gemessen an den strengen Grenzwerten unseres Strahlenschutzrechts – das vertretbare Maß überschritten hätte. Dies, obwohl im Vergleich zum deutschen Anlagenkonzept einer Wiederaufarbeitungsanlage radioaktive Stoffe mit dem Abwasser in die

Irische See eingeleitet werden. Anders in Wackersdorf; hier werden die radioaktiven Reststoffe dem Abwasser entzogen und im künftigen Endlager entsorgt. Aber selbst in Sellafield haben sich Behauptungen über hohe Sterblichkeit an Leukämie und Krebs in der Umgebung als unwahr herausgestellt.

Auch nach den Erfahrungen unserer deutschen Wiederaufarbeitungsanlage im Kernforschungszentrum Karlsruhe ergibt sich eindeutig, daß die Wiederaufarbeitung von Kernbrennstoffen ebenso sicher und umweltfreundlich betrieben werden kann wie unsere Leichtwasserreaktoren.

Ich werde dem Deutschen Bundestag in wenigen Tagen einen Bericht über besondere Vorkommnisse in der Wiederaufarbeitungsanlage Karlsruhe vorlegen, aus dem sich ergibt, daß es auch hier im Jahre 1984 bei einer ohnehin geringen Zahl erwähnenswerter Vorkommnisse in keinem Fall zu einer radiologischen Belastung der Bevölkerung oder der Umgebung gekommen ist.

Alle wesentlichen Industrienationen setzen in ihrer langfristigen Energiepolitik auf die Wiederaufarbeitung. Da kann sich auch die Bundesrepublik Deutschland keinen technologischen Fadenriß leisten, sonst müßten wir eines Tages möglicherweise dafür teuer bezahlen. Unabhängig davon ist aber nach dem derzeitigen technischen Kenntnisstand die Wiederaufarbeitung ein unverzichtbarer Teil unseres Entsorgungskonzepts. Die Bundesregierung hat aufgrund einer sorgfältigen Untersuchung des Kernforschungszentrums Karlsruhe im Rahmen des „Projekts Andere Entsorgungstechniken (PAE)" am 23. Januar 1985 folgendes festgestellt:

1. Die direkte Endlagerung abgebrannter Brennelemente aus Leichtwasserreaktoren hat keine entscheidenden sicherheitsmäßigen Vorteile gegenüber der Entsorgung mit Wiederaufarbeitung.
2. Die direkte Endlagerung erscheint zwar grundsätzlich technisch realisierbar, kann jedoch aus heutiger Sicht für den Nachweis der Entsorgungsvorsorge bei Leichtwasserreaktoren nicht in Anspruch genommen werden und ist daher zunächst weiter zu entwickeln.

Das heißt doch im Klartext: Würden die politischen Totalverweigerer der kommerziellen Wiederaufarbeitung Erfolg haben, so wäre – mangels entsprechender Entsorgungsvorsorge – der Weiterbetrieb unserer Kernkraftwerke gefährdet. Dann hätten die Gegner der friedlichen Nutzung der Kernenergie in unserem Lande weitgehend ihr Ziel erreicht und unseren Staat energiewirtschaftlich ins vorige Jahrhundert zurückgeworfen. Dies darf die Bundesregierung nicht zulassen.

Es ist nun Aufgabe der Sachverständigen, der Technischen Überwachungsvereine, der Gesellschaft für Reaktorsicherheit und all derjenigen Stellen, die Erfahrung und Know-how auf diesem Gebiet haben, darüber zu wachen, daß dem Atomrecht und dem Strahlenschutzrecht entsprechend alle notwendigen sicherheitstechnischen Voraussetzungen geschaffen werden.

Wenn ich die Felder sehe, auf denen in den kommenden Jahren Strahlenschutz und kerntechnische Sicherheit zu beurteilen sein werden, ist mir um die Beschäftigungslage auf diesem Gebiet nicht bange. Wir alle brauchen die Kenntnis der Zusammenhänge und den technischen Sachverstand der hier Versammelten, und wir brauchen – das möchte ich mit Nachdruck betonen – ihre Unabhängigkeit von gesellschaftspolitischen Einflüssen jeder Art. Sie allein garantiert letztlich die Glaubwürdigkeit und sachliche Überzeugungskraft der Wissenschaft.

Über die Glaubwürdigkeit von Expertenaussagen

Von W. Wild[1])

Durch den Beschluß, bei Wackersdorf in der Oberpfalz eine Wiederaufbereitungsanlage zu bauen, ist die in den letzten Jahren etwas abgeflaute Kernenergiedebatte neu entflammt, und wie seit jeher stehen sich die Lager der Gegner und der Befürworter der Kernenergie unversöhnlich gegenüber. Der tiefere Grund dieser Konfrontation dürfte wohl darin liegen, daß es bei der Kernenergiedebatte gar nicht so sehr um die Kernenergie selbst, sondern um grundsätzliche Normen des Handelns und der Wertsetzung geht.

Carl-Friedrich von Weizsäcker hat in einem Vortrag vom 9. März 1978 „Die friedliche Nutzung der Kernenergie. Chancen und Risiken" die unterschiedlichen Wertvorstellungen, die in der Kernenergiedebatte aufeinander treffen, sehr anschaulich beschrieben: „Mehrfach haben mich altgediente Kernenergieexperten, fassungslos angesichts der gegnerischen emotionalen Lohe, die ihnen ins Gesicht schlug, gefragt: „Ist eigentlich der Menschheit die kühle Überlegung abhanden gekommen? Kein technisches Verfahren ist in bezug auf Gefahren und Vorsorge gegen Gefahren schon vor seiner Einführung so minutiös studiert worden wie die Kernenergie. Jedes Beispiel möglicher Unfälle, das unsere Gegner vorbringen, stammt aus unseren eigenen Studien. Aber bei jedem Beispiel dreht man uns das Wort im Munde herum, liest eine behutsame Gefahrenabwägung wie einen Versuch, eine drohende Katastrophe zu verharmlosen, und behandelt uns wie egoistische Interessenvertreter, ja wie entlarvte Verbrecher. Aus welchen seelischen Tiefen steigen eigentlich diese Angstvorstellungen? Denn der manifeste politische Mißbrauch dieser Ängste ist doch nur möglich, wenn die Ängste den Menschen wirklich Eindruck machen." Ebenso fassungslos angesichts der Zuversicht der Technokraten fragen ihre Gegner: „Sind diese Leute wirklich ihrer Gottähnlichkeit so sicher? Wagen sie im Ernst, auf Grund ihrer jedes Jahr wieder korrigierten Abschätzungen eine Technik einzuführen, die unwiderruflich das Schicksal von dreißig Generationen nach uns bestimmt und vielleicht ihr Leben zugrunde richtet? Sind wir, die Betroffenen, nicht die Opfer einer Verschwörung derjenigen, die sich für Wissende halten? Kann ein Experte sich noch zu seinen Fehlern bekennen, der jahrzehntelanger Arbeit im Dienste dieser Sache seine Karriere, sein Ansehen, seine Villa, seine Italienreisen und das Geld für das Studium seiner Kinder verdankt?"

Die Befürworter der Kernenergie gehen in der Regel von wohldefinierten, exakt beschriebenen und säuberlich abgegrenzten Teilproblemen aus. Sie bringen empirische Fakten ins Spiel und bemühen sich um quantitative Abschätzungen. Die Zahlen werden mit vergleichbaren Zahlen für andere Energieträger verglichen und die Bilanz, die sich aus der Vielzahl detaillierter Analysen ergibt, ist dann letztlich für die Kernenergie positiv: Die friedliche Nutzung der Kernspaltung ist eine umweltfreundliche, in ihren Risiken beherrschbare und kostengünstige Form der Energieerzeugung.

Der Ansatzpunkt der Kernenergiegegner ist ein gänzlich anderer, sie führen politische, weltanschauliche und moralische Argumente ins Feld. Zwar sind auch sie bereit, die Auseinandersetzung gelegentlich im technischen und wissenschaftlichen Detail zu führen. Der Ausgang solcher Detaildebatten ist aber für sie letztlich wenig relevant, denn es geht ihnen nicht um den konkreten Aufweis von Mängeln, die sich ja fast immer durch verbesserte technische Maßnahmen beseitigen lassen. Motivation und Blickwinkel der Kernenergiegegner sind vielmehr getragen von einer Grundhaltung des Skeptizismus gegenüber dem bestehenden System wissenschaftlich-technischer Entwicklung als ganzem.

---

[1]) Professor Dr. Wolfgang Wild ist Präsident der Technischen Universität München.

Demgegenüber sehen zwar die Befürworter die allgemeinen Probleme durchaus, die den Gegnern als Ausgangspunkt ihrer Argumentation dienen, bedingt jedoch durch eine Grundhaltung des Vertrauens in die bestehenden Strukturen auf dem Sektor der Wissenschaft und Technik und darüber hinaus auch der Wirtschaft und Politik halten sie diese Probleme für lösbar und sehen in ihnen keine brisanten Fragen oder gar Existenzprobleme der Menschheit.

Die unterschiedliche weltanschauliche Basis, von der aus Befürworter und Gegner der Kernenergie operieren, macht es verständlich, warum die Spaltung bis in das Lager der Experten hineinreicht. Und diese Spaltung ist keineswegs auf die Kernenergie beschränkt; sie begegnet uns in ähnlicher Form in der Debatte um die Gentechnologie und in vielen anderen Bereichen. Der Glaube an den Fortschritt ist ins Wanken geraten, nicht nur bei den wissenschaftlichen Laien, sondern auch bei vielen Wissenschaftlern selbst. Der Freiburger Politologe Wilhelm Hennis hat in einem Brief an den Physiker Heinz Maier-Leibnitz seine Wissenschaftsskepsis mit den Worten beschrieben: „Ich glaube nicht, daß wir mehr wissen als je. In welcher für den Menschen entscheidenden Frage wissen wir denn mehr als je? Jeder Wilde weiß von seiner Umwelt, der Art, wie er mit ihr umgehen muß, mehr als wir, die wir für jede Lappalie einen Spezialisten bemühen müssen. Wo gibt es Hilfen, um in den entscheidenden Fragen mit dem Wissen umzugehen? Das Wissen, von dem Sie sprechen, ist doch nur das Mittelwissen, instrumentelles Wissen. Wo hilft uns dieses Wissen in den entscheidenden Fragen?. . . Sind wir nicht eher in allen entscheidenden Fragen, beim Bedenken der Ziele, überall, wo praktische Vernunft gefordert wird, dümmer geworden?"

Das Gefühl der Orientierungslosigkeit in einer undurchschaubar gewordenen Welt, das Wilhelm Hennis beschreibt, paart sich mit dem Gefühl der Enttäuschung darüber, wie wenig selbst die Verwirklichung der Ziele, die Generationen als Leitvorstellungen dienten, zum Glück und zur Befriedigung der Menschen beigetragen hat. Am Beginn seines Buches „Haben oder Sein" schreibt der Sozialpsychologe Erich Fromm: „Die große Verheißung unbegrenzten Fortschritts – die Aussicht auf Unterwerfung der Natur und auf materiellen Überfluß, auf das größtmögliche Glück der größtmöglichen Zahl und auf uneingeschränkte persönliche Freiheit – das war es, was die Hoffnung und den Glauben von Generationen seit Beginn des Industriezeitalters aufrechterhielt. . . .

Diese Trias von unbegrenzter Produktion, absoluter Freiheit und uneingeschränktem Glück bildete den Kern der neuen Fortschrittsreligion, und eine neue irdische Stadt des Fortschritts ersetzte die „Stadt Gottes". Ist es verwunderlich, daß dieser neue Glaube seine Anhänger mit Energie, Vitalität und Hoffnung erfüllte?

Man muß sich die Tragweite dieser großen Verheißung und die phantastischen materiellen und geistigen Leistungen des Industriezeitalters vor Augen halten, um das Trauma zu verstehen, das die beginnende Einsicht in das Ausbleiben ihrer Erfüllung heute auslöst. Denn das Industriezeitalter ist in der Tat nicht imstande gewesen, seine große Verheißung einzulösen, und immer mehr Menschen werden sich folgender Tatsachen bewußt:

- daß Glück und größtmögliches Vergnügen nicht aus der uneingeschränkten Befriedigung aller Wünsche resultieren und nicht zu Wohl-Sein (well-being) führen;
- daß der Traum, unabhängige Herren über unser Leben zu sein, mit unserer Erkenntnis endete, daß wir alle zu Rädern in der bürokratischen Maschine geworden sind;
- daß unsere Gedanken, Gefühle und unser Geschmack durch den Industrie- und Staatsapparat manipuliert werden, der die Massenmedien beherrscht;
- daß der wachsende wirtschaftliche Fortschritt auf die reichen Nationen beschränkt blieb und der Abstand zwischen ihnen und den armen Nationen immer größer geworden ist;
- daß der technische Fortschritt sowohl ökologische Gefahren als auch die Gefahr eines

Atomkrieges mit sich brachte, die jede für sich oder beide zusammen jeglicher Zivilisation und vielleicht sogar jedem Leben ein Ende bereiten können."

Es soll dahingestellt bleiben, ob und inwieweit Wilhelm Hennis und Erich Fromm recht haben. Im Zusammenhang mit unserem Thema, das sich ja mit der Glaubwürdigkeit von Expertenaussagen beschäftigen soll, haben diese Zitate nur die Funktion, zu verdeutlichen, wie stark auch bei vielen hochgebildeten Wissenschaftlern das Gefühl ist, der Weg der industriellen Zivilisation führe in eine Sackgasse. Aus diesem Gefühl entspringt dann oft die Überzeugung, man diene dem Heile der Menschheit, wenn man sich mit allen Mitteln dem herrschenden Trend entgegenstemme und auf eine Umkehr hinwirke. Man glaubt, zur Rettung der Menschheit verpflichtet zu sein und räumt dieser Verpflichtung einen höheren ethischen Rang ein als dem traditionellen wissenschaftlichen Ethos der Nüchternheit, Objektivität und Unparteilichkeit.

Bei den Gegnern der Kernenergie und anderer moderner Technologien ist es zumeist der moralische Impetus, der bis an ein quasireligiöses Missionierungsbedürfnis heranreichen kann, der zu einseitigen Darstellungen, ja gelegentlich sogar zu falschen Aussagen führen kann. Aber auch die Befürworter versündigen sich nicht selten am Gebot der wissenschaftlichen Objektivität. Ihre Motive sind weniger moralischer als pragmatischer Art. Sie wissen, daß mögliche Risiken von der Gegenseite aufgebauscht und aus dem Zusammenhang gerissen werden. Man hat ihnen allzu oft das Wort im Munde herumgedreht nach dem Motto: , Auch der als Befürworter der Kernenergie (Gentechnologie, etc.) bekannte Herr X hat zugegeben, daß . . . ." Da liegt es nahe, Erkenntnisse, die die eigene Position schwächen könnten, zu verschweigen. Bei Experten, deren wirtschaftliche Existenz von der Realisierung technischer Projekte abhängt, ist überdies die Versuchung groß, die Vorteile solcher Projekte herauszustreichen und die Nachteile zu verharmlosen.

Neben die moralischen oder pragmatischen Motive, die ein Abweichen vom Gebot der wissenschaftlichen Objektivität verursachen, tritt bei manchen Wissenschaftlern die Überzeugung, daß es wissenschaftliche Objektivität nicht gibt. Erkenntnis sei gesteuert durch Interesse und überdies werde jeder Mensch durch Emotionen geleitet, die ihm großenteils gar nicht bewußt seien. Darüber hinaus prägten Lebenserfahrungen nicht nur die Persönlichkeit, sondern auch die wissenschaftliche Einstellung und mit ihr die Erkenntnisfähigkeit des Forschers. Aus all dem zieht man den Schluß: Es gibt keine objektiv wahren Aussagen, in jeder Aussage spiegelt sich das Interesse und die Persönlichkeit des aussagenden Subjekts wider.

Wenn man eine erkenntnistheoretische Position vertritt, die die Möglichkeit objektiver Erkenntnis bestreitet und dem erkenntnisleitenden Interesse entscheidende Bedeutung zumißt, dann wird man auch vom Experten bewußte Parteilichkeit fordern. Der Fachmann soll sich nach dieser Auffassung für eine bestimmte Zielsetzung engagieren und wie ein Anwalt nur Argumente vorbringen, die dieser Zielsetzung förderlich sind. Die Entscheidungsfindung soll sich dann als Ergebnis eines Diskussionsprozesses zwischen den Anhängern unterschiedlicher Zielsetzung ergeben.

In der Theorie hat eine derartige erkenntnistheoretische Position, die vor allem von Jürgen Habermas und der Frankfurter Schule vertreten wird, etwas durchaus Bestechendes. In einem dialektischen Prozeß soll aus herrschaftsfreier Diskussion helleres Bewußtsein resultieren und zu rational verantwortbarem Handeln führen. In der Praxis aber sind die Folgen verheerend; die Wissenschaft hat in den Augen der Öffentlichkeit ihre Glaubwürdigkeit eingebüßt. Der Mann auf der Straße ist heute davon überzeugt, daß man bei jedem Problem für jede Auffassung einen Wissenschaftler gewinnen kann, der sich die gewünschte Auffassung zu eigen macht und sie mit Aplomb und im Brustton der Überzeugung vertritt. Noch schlimmer als dieser Prestigeverlust der Wissenschaft aber ist die allgemeine Unsicherheit, die sich ausgebreitet hat. Der Laie — und auch fast alle unsere Politiker sind in diesem Sinne Laien — weiß, wenn zwei Experten entgegengesetzte Meinungen vertre-

ten, im allgemeinen nicht, wem er glauben soll. Er wird sich oft für die Ansicht entscheiden, die rhetorisch überzeugender vorgetragen wird oder die seinen Überzeugungen näher steht; noch häufiger wird er eine anstehende Entscheidung hinausschieben mit dem Argument, die Wissenschaft sei sich in der betreffenden Angelegenheit nicht einig und darum sei diese Angelegenheit noch nicht entscheidungsreif. In Wirklichkeit aber ist in vielen Fällen die Sachlage völlig klar und durch unzweideutige Fakten belegbar; der Dissens kommt nur dadurch zustande, daß der sogenannte „Experte" der einen Partei von der Sache nichts versteht oder — vor sich legitimiert durch sein Engagement für ein vermeintlich höheres Ziel — bewußt die Wahrheit verschleiert.

Damit sind wir bei dem zentralen Thema unserer Untersuchung angelangt: Wie kommt der Politiker zu zuverlässigen wissenschaftlichen Informationen? Welche Kriterien hat er, um die Glaubwürdigkeit einer Expertenaussage zu testen?

Diese Frage ist leichter gestellt als beantwortet. Denn es gibt kein unfehlbares Kriterium, das es dem Laien gestatten würde, die Glaubwürdigkeit einer Expertenaussage festzustellen. Es gibt aber eine ganze Anzahl von Prüfungsmöglichkeiten, die auch dem Laien zu Gebote stehen und die ihm helfen, mit großer Wahrscheinlichkeit richtige von falschen Aussagen zu unterscheiden. Im folgenden soll versucht werden, solche Prüfungsmöglichkeiten in der Form von sechs Ratschlägen vorzuführen und auf ihre Brauchbarkeit hin zu analysieren.

Erster Ratschlag: *„Erkunde die wissenschaftliche Reputation der Experten und räume einem international angesehenen Wissenschaftler einen Vertrauensvorschuß ein."*

Eine objektive Feststellung der wissenschaftlichen Reputation ist natürlich schwierig, wenn nicht unmöglich, aber es gibt doch etliche Hinweise darauf, ob jemand, der mit dem Anspruch auftritt, ein Experte zu sein, in der wissenschaftlichen Welt Ansehen genießt. Ein Professorentitel ist heute sicherlich kein hinreichendes Kriterium mehr. Brauchbarer ist die Mitgliedschaft in wissenschaftlichen Akademien, denn diese Gremien haben ihre Mitgliedszahlen kaum erweitert. Eine akademische Karriere, die sich ausschließlich innerhalb einer einzigen Einrichtung vollzogen hat, spricht gegen eine Vielzahl von Rufen an verschiedene Hochschulen oder vergleichbare wissenschaftliche Einrichtungen für das Ansehen eines Wissenschaftlers. Das in diesem Zusammenhang beste Kriterium ist der internationale Bekanntheitsgrad, der sich etwa in der Wahl zum wirklichen oder korrespondierenden Mitglied ausländischer Akademien oder in der Zuerkennung internationaler Preise niederschlägt. All das kann auch der Laie durch Nachschlagen in einem Gelehrtenkalender ermitteln oder gegebenenfalls durch Nachfrage feststellen.

Selbstverständlich bietet eine hohe wissenschaftliche Reputation noch keine Gewähr für die Richtigkeit der Aussagen eines Experten. Die Wissenschaftsgeschichte bietet eine Fülle von Beispielen, daß in einer wissenschaftlichen Kontroverse anerkannte Autoritäten Unrecht und junge, noch ganz unbekannte Forscher Recht gehabt haben. Trotzdem ist der Laie in der überwiegenden Mehrzahl der Fülle gut beraten, wenn er einem international anerkannten Gelehrten einen größeren Vertrauensvorschuß einräumt als einem Wissenschaftler, der keine solche Reputation besitzt. Die in der Öffentlichkeit weit verbreitete Meinung, wonach die „etablierte" Wissenschaft nur ihre eigenen Parteigänger zu akademischen Würden zulasse und die Vertreter einer „kritischen" Wissenschaft, die andere Ansichten vertreten, bewußt diskriminiere, trifft in aller Regel nicht zu. Es gehört zum Wesen der Wissenschaft, daß sie kritisch ist und ihre Ergebnisse stets von neuem auf ihre Stichhaltigkeit hin überprüft. Und es hat sich die Erfahrung ergeben, daß bedeutende Gelehrte begabte junge Wissenschaftler auch dann unterstützt und gefördert haben, wenn diese ganz andere Ansichten hatten. Gegenüber abweichenden, politischen oder weltanschaulichen Positionen ist ein echter Forscher fast immer tolerant und er zollt auch dem Gegner Respekt, wenn dieser auf hohem Niveau argumentiert.

Der Gegensatz zwischen „etablierter" und „kritischer" Wissenschaft ist eine Fiktion; die Wissenschaft ist eine Einheit und es ist sinnvoll, demjenigen, der es in der wissenschaft-

lichen Welt zu hohem internationalen Ansehen gebracht hat, einen Vertrauensvorschuß einzuräumen. Dieses grundsätzliche Vertrauen gegenüber dem angesehenen Gelehrten darf allerdings nicht in blinden Autoritätsglauben ausarten; der Laie muß noch andere Glaubwürdigkeitskriterien heranziehen, die in den fünf weiteren Ratschlägen versucht wurde, zu konkretisieren.

Zweiter Ratschlag: *„Prüfe, ob die Aussage eines Wissenschaftlers das Fachgebiet betrifft, auf dem er Kompetenz besitzt."*

Man macht dem Forscher oft den Vorwurf, er ziehe sich in den Elfenbeinturm seiner Wissenschaft zurück und kümmere sich nicht um den politischen Mißbrauch seiner Forschungsergebnisse. Im Zeitalter der Atombombe wird dieser Vorwurf von vielen Gelehrten sehr ernst genommen und wir beobachten heute eher das Gegenteil: Der Forscher fühlt sich politisch verantwortlich und engagiert sich leidenschaftlich auch für Angelegenheiten, die außerhalb des Bereichs seiner eigenen wissenschaftlichen Kompetenz liegen. Diesen Wandel im Verhalten vieler Wissenschaftler sollte man positiv bewerten, so lange damit kein Autoritätsmißbrauch verbunden ist. In Fragen von weitreichender Bedeutung, wie der Nutzung der Kernenergie oder der Anwendung der Gentechnologie hat jeder Staatsbürger, wenn nicht die Verpflichtung, so doch gewiß das Recht, sich zu engagieren und seine Meinung kund zu tun. Aber auch der berühmteste Gelehrte ist außerhalb seines Fachgebiets eben nur ein Staatsbürger und kein Experte, dessen Aussagen eine höhere Autorität beanspruchen können.

Der Laie sollte deshalb die Aussagen von Biologen und Chemikern zur Kernenergie oder von Physikern zur Gentechnologie nicht allzu ernst nehmen. Aber auch innerhalb eines Fachgebietes gibt es eine abgestufte Kompetenz. Ein Astro- oder Elementarteilchenphysiker ist bei der Beurteilung der Sicherheit kerntechnischer Anlagen kein Experte und bezieht seine Kenntnisse nicht aus eigener Erfahrung. Es erhöht daher die Glaubwürdigkeit der Aussage eines Wissenschaftlers ungemein, wenn dieser selbst die Grenzen seiner Kompetenz deutlich herausstellt. Carl-Friedrich von Weizsäcker ist sicherlich unter den heute lebenden Gelehrten einer der vielseitigsten und die von ihm zuerst aufgestellte sogenannte Bethe-Weizsäckerformel ist die physikalische Grundlage der Nutzung der Kernenergie, sowohl durch Kernspaltung als auch durch Kernfusion. Trotzdem hat C.F. von Weizsäcker in seinem schon erwähnten Aufsatz zu Beginn deutlich hervorgehoben, was die Basis seiner Aussagen ist: „Ich bin ausgebildeter theoretischer Kernphysiker, habe zwar seit 1945 nicht mehr selbst über Reaktortheorie gearbeitet, habe aber seit etwa vier Jahren systematisch zahlreiche Gespräche mit Fachleuten geführt und verdanke meiner Ausbildung wenigstens das Vokabular, in dem ich meine Gesprächspartner befragen – wie man im Umgangston sagt: „löchern" – konnte. Jede positive Behauptung, die ich im heutigen Vortrag ansprechen werde, habe ich zuvor der Kritik mehrerer Fachleute unterbreitet. Aber ich bekenne offen und mit Absicht, daß ich in fast keiner dieser Behauptungen hinreichenden eigenen speziellen Sachverstand besitze, um sie rein sachlich zu verteidigen. Ich bin überall bei meiner Meinungsbildung nicht nur auf mein Urteil über Sachen, sondern auch wesentlich auf mein Urteil über Menschen angewiesen. Ich muß mir bei jedem meiner Gesprächspartner selbst eine Meinung darüber bilden, welches sein Kenntnisstand, sein Partikularinteresse, seine Leidenschaft, und der Grad seiner Intelligenz, seiner Selbstkritik und seiner Redlichkeit ist."

Wer in diesem Sinne die eigene Kompetenz relativiert, besitzt größere Glaubwürdigkeit als derjenige, der den Eindruck zu erwecken versucht, die eigene Position sei unfehlbar. Dem letzteren geht es nämlich zumeist nicht um die Aufklärung eines Sachverhalts, sondern um die Durchsetzung der eigenen Auffassung und Zielsetzung. Das leitet über zu meinem dritten Ratschlag.

Dritter Ratschlag: *„Mißtraue jedem Experten, der – statt Fakten leidenschaftslos zu analysieren – versucht, Dich mit rhetorischem Einsatz zu einer bestimmten Überzeugung zu verleiten."*

Heinz Maier-Leibnitz hat in einem Aufsatz in der FAZ vom 12. Oktober 1982 unter dem Titel „Vorschlag einer Glaubwürdigkeitsprüfung" ausgeführt: „Wer beim Argumentieren energisch ein vorgegebenes Ziel verfolgt, kann nicht auf rhetorische Mittel verzichten, um den gewünschten Eindruck zu hinterlassen. Dafür gibt es zahllose Wege, vom Weglassen bis hin zur Verfälschung von Aussagen. Rhetorik aber hat nichts mit Fachwissenschaft zu tun."

Es ist sicher für den Politiker nicht leicht, die Fähigkeit, durch rhetorischen Glanz zu überzeugen, bei einem Experten nicht als Tugend, sondern als Untugend zu werten. Denn für den Politiker selbst kommt es ja in allererster Linie darauf an, den Wähler auf seine Seite zu ziehen und ihn von der Richtigkeit der eigenen Position zu überzeugen. Die Aufgabe des Experten in der Politikberatung aber ist eine völlig andere: Er soll nicht die eigene politische Überzeugung durchzusetzen versuchen, sondern er soll über Sachverhalte zutreffende Aussagen machen. „Es handelt sich um technische Aussagen, die richtig oder falsch sind, ganz unabhängig davon, ob ihnen eine Mehrheit folgt oder nicht." (H. Maier-Leibnitz). Man kann für oder gegen die Einführung der zivilen Nutzung der Kernenergie sein, aber die Aussage über die Strahlungsemission eines Reaktors oder einer Wiederaufarbeitungsanlage ist eine Aussage über eine objektiv meßbare Größe, die nur richtig oder falsch sein kann. Ob eine solche Aussage die eigene Position als Befürworter oder Gegner der Kernenergie stärkt oder schwächt, darf keine Rolle spielen; der Experte muß, wenn er für den Politiker und dessen Entscheidung brauchbar sein soll, die objektiv richtige Aussage machen. Dazu bedarf es keiner Rhetorik und der Politiker ist gut beraten, wenn er Rhetorik bei einer Expertenaussage als Zeichen der Voreingenommenheit wertet und der Aussage mißtraut.

Vierter Ratschlag: *„Versuche durch Stichproben festzustellen, ob der Experte mit Fakten redlich umgegangen ist oder versucht hat, die Fakten im Interesse der Durchsetzung einer bestimmten Position zu manipulieren."*

Dieser Ratschlag verlangt von dem Laien eine größere Bemühung und mehr Arbeitsaufwand als die vorherigen. Die Expertise muß sorgfältig gelesen und mit anderen Publikationen verglichen werden. Es ist sicher nicht einfach, als fachlich unvorgebildeter Laie Manipulationen zu entlarven. Ich glaube aber, daß es in vielen Fällen möglich ist und möchte dazu eine Passage aus dem schon erwähnten Aufsatz von H. Maier-Leibnitz zitieren: „Wenn zum Beispiel jemand leugnet, eine Arbeit als Beleg für eine bestimmte Behauptung zitiert zu haben, das Zitat sich aber doch findet; oder wenn er aus einer anderen Arbeit einen hohen Wert, den der Autor willkürlich zu Rechenzwecken angenommen hat, als real in seine Argumentation aufnimmt; oder wenn er eine thermische Energie als mechanische Energie bezeichnet und so sehr hohe mechanische Belastungen des Reakors angibt; alles das kann jedermann beurteilen." Die Manipulation von Fakten kann auch derjenige erkennen, der die Richtigkeit der Fakten selbst nicht beurteilen kann. Wenn eine Manipulation nachweisbar ist, dann sollte das Anlaß genug sein, größtes Mißtrauen zu hegen. Allerdings sollte der Aufweis einer vereinzelten Unrichtigkeit noch nicht hinreichen, um eine Expertise gnadenlos zu verwerfen. Jeder macht einmal Fehler und unglaubwürdig wird ein Wissenschaftler erst, wenn sich die Fehler häufen und eine bestimmte Tendenz erkennen lassen. Denn dann ist der Verdacht erhärtet, daß der Autor im Interesse einer vorgefaßten Meinung Fakten manipuliert.

Fünfter Ratschlag: *„Nimm nur Expertisen ernst, die die Sicherheit der eigenen Aussagen kritisch analysieren und begründete Fehlergrenzen angeben."*

In den Naturwissenschaften und der Technik wird dem Studenten schon in den ersten Semestern beigebracht, daß ein Meßwert ohne Angabe der Fehlergrenzen wertlos ist. Er wird mit dem Fehlerfortpflanzungsgesetz und den Methoden der Fehlerrechnung vertraut gemacht. Außerdem hält man ihn dazu an, die systematischen Fehler eines Experiments zu bedenken und so gut wie nur irgend möglich zu analysieren und bei der Diskussion der Ergebnisse zu berücksichtigen. Das, was man von jedem Anfänger verlangt, muß na-

türlich erst recht von einer Expertise gefordert werden. Seriöse Untersuchungen, unter denen ich die Deutsche Risikostudie Kernkraftwerke beispielhaft hervorheben möchte, entsprechen dieser Forderung selbstverständlich in vollem Maße. Da es bisher gottlob keine schweren Reaktorunfälle gegeben hat und man auch einschlägige Versuche nur in sehr eingeschränktem Umfang durchführen kann, hängt die Abschätzung der Unfallwahrscheinlichkeit unvermeidlich von Annahmen ab, die mit gewissen Unsicherheiten behaftet sind. Angaben über Sicherheitsrisiken sind deshalb abhängig von angenommenen Eingangsparametern und sie können sich ändern, wenn diese Eingangsdaten abgeändert werden. In einer seriösen Abschätzung des Sicherheitsrisikos wird man bei der Festlegung ungenau bekannter Eingangsparameter pessimistische Annahmen zugrunde legen. Das hat dann freilich zur Folge, daß Unfälle mit sehr schwerwiegenden Auswirkungen zwar höchst unwahrscheinlich, aber immerhin möglich wären. Es dürfte heute wohl allgemeine Auffassung bei den wirklichen Sachkennern sein, daß der in der Deutschen Risikostudie Kernkraftwerke ausgewiesene Schwerstunfall mit 14500 akuten Todesfällen, 104000 Toten infolge von Spätschäden, einer zu evakuierenden Fläche von 5680 km^2 und einer von der Evakuierung betroffenen Bevölkerung von 2,9 Millionen niemals eintreten wird. Andererseits waren diese Zahlen bei der Erstellung der Studie die Konsequenz, die sich unter extrem pessimistischen, aber nicht ganz und gar unrealistischen Annahmen, errechnete. Ich meine, daß es ein Verdienst dieser Studie war, solche Zahlen nicht verschwiegen zu haben, obwohl sie manchen Bürger veranlaßt haben mögen, sich gegen die Einführung einer Technologie zu wenden, bei der Auswirkungen dieser Größenordnung denkbar sind.

Vertrauen verdient eine Aussage, die alles offen auf den Tisch legt, die bequemen und die unbequemen Fakten aufführt und analysiert, die weder aufbauscht noch verharmlost, ohne Rücksicht auf taktische Überlegungen. Und damit bin ich bei meinem sechsten Ratschlag.

Sechster Ratschlag: *„Vertraue am ehesten demjenigen Experten, der niemandem nach dem Munde redet, in dessen Gutachten sich sowohl Aussagen finden, die Dir, wie solche, die Deinem Kontrahenten unbequem sind."*

Die Beherzigung dieses letzten Ratschlags setzt eine beträchtliche Uneigennützigkeit voraus, die sich aber doch lohnt. Gerade der Politiker ist oft – nicht zuletzt bei der Entscheidung für oder gegen eine bestimmte Technologie – gezwungen, neben technischen Gesichtspunkten auch politische Gegebenheiten zu berücksichtigen. Regionale oder konjunkturelle Aspekte oder die Rücksichtnahme auf die eigene Wählerschaft und vieles andere mehr können für ihn größte Bedeutung haben, während der wissenschaftlich-technische Politikberater keine in diese Richtung gehenden Überlegungen anstellen kann und soll. Auch der um eine sachgerechte Entscheidung bemühte Politiker wird darum häufig gezwungen sein, von den Empfehlungen der Experten abzuweichen. Ein gefügiger Experte, der sich die Entscheidung des Politikers zu eigen macht, ist bequem aber gefährlich. Denn er gaukelt dem Politiker eine falsche Sicherheit vor, während der unabhängige Experte dem Politiker klar aufzeigt, wo er sich auf das wissenschaftliche Votum stützen kann und wo er die Verantwortung allein zu tragen hat. Dies wird den klugen Politiker zur Vorsicht mahnen und ihn oft veranlassen, sich nicht allzu weit aus dem Fenster zu hängen und sich eine Hintertür offen zu halten. Er ist dann nicht völlig desavouiert, wenn die künftige Entwicklung zeigt, daß er auf das falsche Pferd gesetzt hat.

Ich bin damit am Ende meiner Ratschläge für den Laien und insbesondere für den zu Entscheidungen verpflichteten Politiker angelangt. Wahrscheinlich kann man diesem noch weitere Entscheidungshilfen an die Hand geben; mir sind allerdings keine anderen brauchbaren Kriterien mehr eingefallen, mit deren Hilfe die Glaubwürdigkeit von Expertenaussagen getestet werden könnte.

Die ganze Mühsal der Glaubwürdigkeitsprüfung wäre freilich unnötig, wenn wir von dem Streit der Experten und Gegenexperten und den damit verbundenen Gefahren für eine

wissenschaftlich-technische Politikberatung wieder loskommen könnten. Das sollte möglich sein, wenn sowohl Politiker als auch Wissenschaftler Selbstdisziplin üben und sich an bestimmte Verhaltensregeln binden würden.

Politiker und in fast noch stärkerem Maße die meinungsbildenden Medien müßten von der Mode gewordenen Konfrontationsstrategie abrücken. Wie in einschlägigen Untersuchungen nachgewiesen, führt diese Konfrontationsstrategie nicht nur zur Verunsicherung der Wähler bzw. des Publikums, sondern provoziert auch extreme Einstellungen. Die sachbezogene Darstellung des Für und Wider durch um Objektivität bemühte Fachleute baut dagegen Polarisierungen ab und fördert tragfähige und sachdienliche Kompromisse. Den Weg, der die wissenschaftlich-technische Politikberatung auf die schiefe Bahn gebracht hat, hat H. Maier-Leibnitz am Beispiel der Enquete Kommission „Zukünftige Kernenergie-Politik" klar beschrieben: „Die Gutachter sollen durch ihre fachlichen Leistungen ausgewiesen sein. Aber die Enquete Kommission hat beschlossen, daß außer den „klassischen" Experten auch erklärte Atomgegner Gutachten erstellen sollen. Da es hier nicht genügend Fachleute gibt, hat anscheinend das Bundesministerium für Forschung und Technologie, das diese Gutachten finanziert, festgelegt, daß auch die Ausgewiesenheit in anderen Fächern genügen soll. Die Kommission hat es ausdrücklich nicht als ihre Aufgabe betrachtet, die fachliche Ausgewiesenheit zu prüfen: Schon die Frage, ob die Gutachter akademische Grade erworben haben, wurde zwar gestellt, aber ihre Beantwortung wurde verhindert." Mit solchen Verfahrensweisen kommt man nicht zu einer brauchbaren Politikberatung, sondern man provoziert Parteilichkeit und Polarisation. Daher fordert Maier-Leibnitz mit vollem Recht: „So kann es nicht bleiben. Das erste ist wohl, daß man wieder auf der Kompetenz der Gutachter besteht, etwa indem man frühere Arbeiten der Gutachter in die Diskussion einbezieht. Natürlich ist es für eine Kommission wichtig, alle auch von der Norm abweichenden Meinungen zu kennen. Aber dazu ist es nicht nötig, Personen, die sich selbst als voreingenommen bezeichnen, als Gutachter einzusetzen, die gleichberechtigt neben den anderen zu Wort kommen."

Aber nicht nur die Politiker, sondern erst recht auch die Wissenschaftler müssen ihr Verhalten ändern. Wo der Wissenschaftler als Wissenschaftler gefordert ist, muß er sich an das Ethos der Wissenschaft binden und alle anderen Rücksichten und Bindungen demgegenüber zurückstellen. Wenn ein Wissenschaftler befürchtet, daß eine Sachaussage politische Wirkungen haben kann, die er nicht wünscht oder die er sogar für verderblich oder moralisch inakzeptabel hält, dann kann er die Aussage verweigern, aber er darf objektiv unstreitige Sachverhalte nicht verfälschen oder manipulieren. Denn das Ethos der Wissenschaft fordert, daß das Bekenntnis zur Wahrheit allen, aber auch wirklich allen anderen Rücksichten überzuordnen ist. Man kann, um ein Beispiel zu nennen, gentechnologische Eingriffe in die Keimbahn des Menschen aus religiösen, humanen oder sonstigen Erwägungen heraus radikal ablehnen, aber man darf trotzdem die Frage, ob durch solche Eingriffe Erbkrankheiten geheilt werden können, nicht verneinen, wenn man weiß, daß es sich umgekehrt verhält.

Die ethische Verpflichtung zum Bekennen des als wahr Erkannten wird, wie schon eingangs erwähnt, mit dem Hinweis relativiert, daß es eine vom Eigeninteresse unabhängige, objektiv gültige Erkenntnis der Wahrheit nicht gäbe. Ob dieser Einwand stichhaltig ist, sei dahingestellt. Ich weiß recht gut, daß sich selbst Naturgesetze nicht zwingend beweisen lassen, daß sie vielmehr vorläufige, bisher bewährte Versuche sind, die Phänomene der Natur zu ordnen und für den Menschen nutzbar zu machen. Wenn man aber bei Benutzung solcher Gesetze eine Raumsonde senden kann, die dort weich landet und uns Informationen übermittelt, dann wäre es unvernünftig, anzunehmen, daß die von uns verwendeten Naturgesetze keinerlei objektive Gültigkeit besitzen. Bei aller historisch bedingten Einkleidung muß in den Naturgesetzen ein unbestreitbarer Wahrheitskern enthalten sein. Die Verpflichtung auf das Bekenntnis zur Wahrheit und auf das Bemühen um Unvoreingenommenheit ist deshalb sinnvoll und gerechtfertigt. Wir erreichen zwar die

volle Objektivität niemals, aber wir können uns darum bemühen und wir können ihr nahe kommen.

Ich meine, daß wir Wissenschaftler uns auf diese ethische Grundlage unseres Handelns wieder stärker besinnen sollten. Man fordert heute mit Recht eine Ethik der Technik, die uns die Grenzen aufzeigt, die dem Machbaren gezogen sind. Nicht alles, was getan werden kann, läßt sich auch verantworten. Wir müssen die Lebenschancen künftiger Generationen im Auge haben und wir dürfen nicht um unseres eigenen Vorteils willen Entwicklungen einleiten, die diese Lebenschancen ernsthaft beeinträchtigen könnten. Das bedingt unter anderem, daß wir sorgfältig die Konsequenzen der Hypotheken prüfen, die wir unseren Nachkommen mit der Produktion langlebiger Radionuklide, aber auch mit der Vermehrung des Kohlendioxidgehalts der Atmosphäre und vielem anderem mehr, aufbürden. Ich meine aber, daß wir schwerlich eine Ethik verantwortlichen Handelns entwickeln können, wenn wir uns nicht auf die Wahrheit verpflichten und wenn wir der Forderung wissenschaftlicher Redlichkeit zuwiderhandeln. Der Zweck hat noch nie die Mittel geheiligt und das Mittel der Verschleierung der Wahrheit am allerwenigsten. Bemühen wir uns also um Sachlichkeit, Aufrichtigkeit, Redlichkeit und prüfen wir selbstkritisch, ob unsere Aussagen wirklich durch Fakten fundiert sind und nicht aus Vorurteilen entspringen. Wenn wir so handeln, dann wird es zwar noch immer richtige und falsche wissenschaftliche Aussagen geben, aber das Problem, das uns heute abend beschäftigt hat, die Beeinträchtigung der Glaubwürdigkeit durch eine willentliche Verschleierung, Verstümmelung oder gar Verfälschung der Wahrheit, dieses Problem, das heute die Atmosphäre vergiftet und das Ansehen der Wissenschaft zu ruinieren droht, wird seine Brisanz einbüßen und vielleicht sogar gänzlich verschwinden.

Einführung

Von A. Birkhofer[1])

Die Vorträge des diesjährigen GRS-Fachgesprächs befassen sich mit Entwicklungen zur Leittechnik in Kernkraftwerken.

Ich bin überzeugt, daß die Möglichkeiten und die Bedeutung der Leittechnik in den kommenden Jahren noch zunehmen werden. Das hat verschiedene Gründe.

Der Erfahrungsumfang mit Kernkraftwerken beträgt derzeit weltweit rund 4 000 Betriebsjahre. In den nächsten 10 bis 15 Jahren wird sich diese Zahl voraussichtlich auf etwa 10 000 erhöhen. Zugleich nimmt der Anteil der Kernenergie an der Stromerzeugung laufend zu, wenn auch in einzelnen Ländern in stark unterschiedlichem Ausmaß. In der Bundesrepublik wird heute bereits jede dritte Kilowattstunde aus Kernenergie gewonnen. Wenn die Anlagen, die zur Zeit gebaut werden, in Betrieb sind, dürfte der Anteil auf fast 40 % steigen.

Die zunehmende Bedeutung der Kernkraftwerke für die Energieversorgung ist Grund genug, alle Möglichkeiten zu nutzen, die Betriebssicherheit weiter zu erhöhen.

Hinzu kommt, daß wir in zehn Jahren etwa 130 Anlagen haben werden, die mehr als 20 Jahre in Betrieb sind. Die Zahl der Altanlagen nimmt dann mit einer Steigerungsrate von etwa 10 % laufend zu. Es ist dafür zu sorgen, daß auch bei Altanlagen der notwendige Sicherheitsgrad garantiert wird. Das ist nur durch angemessene Überwachungsprogramme möglich. Überwachung im technischen Sinn bedeutet ganz besonders auch den Einsatz moderner Diagnoseverfahren zur Betriebsüberwachung, ein Hauptthema des heutigen Fachgesprächs.

Dr. Bochmann, der die Abteilung Reaktorsicherheit beim Bundesministerium des Innern leitet, hat in seinem Referat anläßlich der 29. General-Konferenz der IAEA zur Reaktorsicherheit im September dieses Jahres unter anderem darauf hingewiesen, wie bedeutend der Einsatz von verbesserten und umfassenden Informationssystemen zur Gewährleistung der Betriebssicherheit ist. In diesem Zusammenhang verwies er besonders auf die Bedeutung einer Informationsverdichtung für den Operateur. Einer der heutigen Vorträge wird sich mit neuen Entwicklungen auf diesem Gebiet befassen. Übrigens hat auch der Chef der sowjetischen Genehmigungsbehörde, Kulov, bei der IAEA-Konferenz darauf hingewiesen, daß ein wesentlich verstärkter Einsatz von Diagnosehilfen notwendig sein wird.

Die Bundesrepublik hatte, wie eine Reihe anderer Länder, in den letzten 20 Jahren einen erheblichen Zubau von Kernkraftwerken. Die Zuwachsraten werden sich zwar verlangsamen; trotzdem nimmt die Zahl der in Betrieb befindlichen Kernkraftwerke laufend zu. Zugleich haben die Auslegungskonzepte einen hohen Reifegrad erreicht, so daß keine umwälzenden Neuerungen zu erwarten sind, zumindest was den Einsatz der Kernenergie zur Stromerzeugung angeht. Dies bedeutet, daß sich unsere Aktivitäten von Auslegungsfragen hin zu sicherheitstechnisch relevanten Betriebsfragen zu entwickeln haben.

Hier kommt der Leittechnik als Instrument zur Steuerung und Beobachtung der in einem Kernkraftwerk ablaufenden Prozesse zentrale Bedeutung zu. Deutsche Kernkraftwerke sind bereits jetzt in hohem Grad automatisiert, hier sind keine gravierenden Änderungen zu erwarten. Wichtiger erscheint es mir, den Informationsteil fortzuentwickeln. Dabei ist weniger daran zu denken, die ohnehin recht umfangreiche Meßtechnik, das heißt die Anzahl der Meßfühler zu erweitern. Es geht vielmehr darum, die bereits vorhandenen umfangreichen Primärinformationen intensiver und „intelligenter" weiterzuverarbeiten.

---

[1]) Professor Dr.Dr.-Ing. E.h. Adolf Birkhofer ist Geschäftsführer der Gesellschaft für Reaktorsicherheit (GRS) mbH.

Dabei ergeben sich zwei Hauptzielrichtungen:

1. Die Information muß in der Warte geeignet kondensiert werden. Dazu ist die heutige moderne Bildschirmtechnik hervorragend geeignet.
2. Die Betriebsdaten sind so aufzubereiten, daß Diagnosen über die Betriebssicherheit von Komponenten und Systemen möglich werden. Dazu bietet sich der Einsatz der heute hoch entwickelten Prozeßrechnertechnik an.

Der Realisierung dieser Ziele kommt der sich immer schneller vollziehende Technologiewandel in der Leittechnik entgegen. Dieser Wandel ist geprägt durch den extensiven Einsatz von Mikroprozessoren, neuen Datenübertragungssystemen und einer neuen Bildschirmtechnik. Dementsprechend sind verstärkte Bemühungen der Reaktorhersteller zu registrieren, die Vorteile der neuen Technologien für die Reaktortechnik nutzbar zu machen.

In Einzelanwendungen haben sich rechnergestützte Leittechniksysteme bereits bewährt, zum Beispiel der Kernschutzrechner in Grafenrheinfeld oder die Steuerstabfahrrechner für Siedewasserreaktoren. Der Trend geht jedoch eindeutig zu zentralen Lösungen.

In diesem Zusammenhang seien erwähnt: die von der Electricité de France für die Druckwasserreaktoren der 1400-MWKlasse entwickelten neuen Informationssysteme, die fortschrittliche Wartentechnik der Japaner und nicht zuletzt das KWU-System PRINS, das auf einer hierarchischen Rechnerstruktur beruht und die kompakten Darstellungsmöglichkeiten von Farbbildschirmen nutzt.

Wenn wir also von neuen Technologien in der Leittechnik sprechen, so hat die Zukunft bereits begonnen – bei uns in der Bundesrepublik mit den Konvoi-Anlagen –. Die Aufgabe der GRS ist es, auch auf diesem Gebiet die weitere Entwicklung der Sicherheitstechnik zu verfolgen. Dazu sollen Methoden und Verfahren erarbeitet werden,

- deren Einsatz dem Betriebspersonal, insbesondere in außergewöhnlichen Betriebszuständen, die nötige Unterstützung gewährleistet,
- und die eine ausgewogene Bewertung der neuen Sicherheitstechnik ermöglichen.

Entsprechend dieser doppelten Zielsetzung werden wir in den nächsten fünf Jahren Entwicklungen durchführen, die es ermöglichen,

- unsere bewährten Diagnoseverfahren auf die Überwachung aktiver Sicherheitskomponenten auszudehnen,
- durch rechnergestützte Informationssysteme die sicherheitsrelevante Information für den Operateur noch transparenter zu gestalten,
- eine geschlossene Qualifizierung der Sicherheitstechnik zu erreichen, die auf den erwähnten neuen Technologien basiert,
- eine geeignete Validierung von Informationen in den Warten zu gewährleisten.

Unser diesjähriges Fachgespräch soll einerseits die Entwicklungen der GRS auf dem Gebiet der sicherheitsrelevanten Leittechnik vorstellen; andererseits soll es aber vor allem dazu beitragen, den Blick für die Möglichkeiten der neuen Leittechnik zur Hebung der Sicherheit zu öffnen. Ich hoffe, daß beides dazu beiträgt, die Entwicklung von effizienten Qualifizierungsverfahren voranzutreiben, damit die Möglichkeiten der Leittechnik uneingeschränkt in der Praxis genutzt werden können.

Beurteilung und Qualifizierung neuer Leittechnik mit Sicherheitsverantwortung

Von S. Goßner und D. Wach [1])

Kurzfassung

Die Mikroelektronik und Rechnertechnik verdrängen in allen technischen Bereichen seit Jahren die konventionelle Elektronik. Festverdrahtete Schaltungen, logische Netzwerke und aufwendige Rechenbaugruppen werden in zunehmendem Maße durch hochintegrierte Bausteine bzw. rechnergestützte Systeme ersetzt. Mikrochips auf Siliciumbasis verändern die technische Welt.

Dieser Technologiewandel wird vor der Leittechnik von Kernkraftwerken nicht haltmachen. Neue leittechnische Systeme werden nicht nur betriebliche Funktionen, sondern auch Aufgaben mit Sicherheitsverantwortung übernehmen. Dies ist aus sicherheitstechnischer Sicht wegen der zahlreichen Vorteile der neuen Leittechnik auch erstrebenswert; aufgrund der Notwendigkeit, dem Stand der Technik zu folgen, wird ihr Einsatz langfristig sogar unumgänglich sein. Eine Verwendung für Sicherheitsaufgaben setzt voraus, daß die Eignung der neuen Technik im Rahmen atomrechtlicher Genehmigungsverfahren nachgewiesen werden kann.

Der Beitrag diskutiert die bei der Beurteilung und Qualifizierung neuer Leittechnik sich ergebenden Fragestellungen. Er ruft die Aufgaben der Leittechnik in Kernkraftwerken und die Leistungsmerkmale neuzeitlicher leittechnischer Systeme in Erinnerung. Probleme beim Einsatz neuer Leittechnik sowie die Situation im In- und Ausland werden angesprochen. Anhand wesentlicher Unterschiede zwischen konventioneller und neuer Leittechnik wird bewertet, ob und auf welche Weise existierende sicherheitstechnische Grundanforderungen erfüllt werden können und welche Anforderungen neu formuliert werden müssen. Es ist ein Gesamtkonzept zu entwickeln, innerhalb dessen für neue leittechnische Einrichtungen abgestufte Anforderungsprofile zur Auslegung und Qualifizierung zu definieren sind. Zugehörige Qualifizierungsmethoden und -werkzeuge sind anzupassen, neue zu entwickeln und aufeinander abzustimmen.

Abstract

Since several years micro electronics and computer technologies are replacing conventional electronics in all technical areas. Increasingly hardwired circuits, logical net works and sophisticated computation devices are substituted by highintegrated components or computer-based systems. Silicon micro chips are changing the technical world.

This change in technology will certainly also impact the instrumentation and control (I&C) systems of nuclear power plants. New I&C systems will be available for operational functions. Due to the numerous benefits of the new I&Cs it will be worthwhile to expend its applications also towards safety tasks. Because of the proceeding state of the art its further implementation will become even unavoidable. For safety relevant applications the new techniques have to be qualifiable according to the basic principles of proven licensing procedures.

The paper will discuss the questions related to the assessment and qualification of new I&C-systems. The tasks of nuclear power plant I&Cs as well as the efficiency of the new techniques are reflected.

---

[1]) Dipl.-Ing. Stefan Goßner und Dr.-Ing. Dieter Wach, Gesellschaft für Reaktorsicherheit (GRS) mbH, Garching

Problems with application of new I&Cs and the state of application in Germany and abroad are addressed. Starting from the essential differencies between conventional and new I&C-systems it is evaluated, if and in which way existing safety requirements can be met and to what extent new requirements need to be formulated. An overall concept has to be developed comprising the definition of graded requirement profiles for design and qualification. Associated qualification procedures and tools have to be adapted, developed and tuned upon each other.

Einführung

Die Mikroelektronik verdrängt seit Jahren in allen technischen Bereichen die konventionelle Elektronik. Die Ursache für diese zum Teil lawinenhaft verlaufende Entwicklung liegt sowohl in dem äußerst günstigen Preisniveau wie in der universellen und ständig verbesserten Leistungsfähigkeit der Mikroprozessoren. Hohe Leistungsfähigkeit, geringe Herstellungskosten sowie geringer Raum- und Energiebedarf ergeben für die Mikroelektronik zunehmend ein derart günstiges Kosten-Nutzen-Verhältnis, daß der konventionellen Elektronik langfristig nur Sonderanwendungsgebiete vorbehalten bleiben werden. Es ist zu erwarten, daß die geschilderte Entwicklung in absehbarer Zeit auf Kernkraftwerke übergreifen wird.

Mikroprozessoren werden nicht die einzigen neuen Komponenten in der Leittechnik von Kernkraftwerken sein. In ihrer Folge werden zahlreiche weitere neue Einrichtungen, Verfahren und Strukturen zum Einsatz kommen. Dies bedeutet eine neue Leittechnik in Kernkraftwerken.

Da diese neue Leittechnik neben rein betrieblichen Funktionen auch Aufgaben mit sicherheitstechnischer Bedeutung übernehmen wird, müssen die neuen Einrichtungen und Verfahren aus sicherheitstechnischer Sicht bewertet und für den kerntechnischen Einsatz qualifiziert werden. Dies kann sicherlich nicht losgelöst von den bisher gültigen Maßstäben erfolgen. Die neue Leittechnik wird nur dann für sicherheitstechnische Aufgaben im Kernkraftwerk eingesetzt werden können, wenn sie jenen Grundanforderungen gerecht wird, die in der Vergangenheit im Zusammenhang mit konventionellen leittechnischen Einrichtungen gewachsen sind und deren anerkannten Sicherheitsstandard begründeten (siehe zum Beispiel [1]).

Die folgenden Ausführungen werden sich mit den Fragestellungen auseinandersetzen, die sich bei der Beurteilung und Qualifizierung neuer Leittechnik ergeben. Zuvor sollen die von der Leittechnik in Kernkraftwerken wahrgenommenen Aufgaben, die bisher eingesetzten leittechnischen Systeme, ihre sicherheitstechnische Bedeutung und einige typische Auslegungsmerkmale in Erinnerung gerufen werden. Anschließend werden charakteristische Eigenschaften und besondere Leistungsmerkmale neuzeitlicher leittechnischer Systeme und dadurch bedingte Unterschiede zur konventionellen Leittechnik aufgezeigt. Anhand wesentlicher Unterschiede wird beispielhaft bewertet, ob und auf welche Weise existierende sicherheitstechnische Grundanforderungen erfüllt werden können, welche Anforderungen neu formuliert werden müssen und welche Anpassungen und Ergänzungen von Qualifizierungsmethoden und Qualifizierungsprozeduren erforderlich sein werden.

Leittechnische Aufgaben und Systeme im Kernkraftwerk

Der sichere Betrieb eines Kernkraftwerkes wird durch eine Vielzahl leittechnischer Systeme mit gestaffelten und sich ergänzenden Aufgaben unterstützt und ermöglicht. Bild 1 vermittelt einen schematischen Überblick über die wichtigsten leittechnischen Aufgabenbereiche und Systeme im Kernkraftwerk.

Die Abbildung zeigt im oberen Teil die Prozeßinstrumentierung, mit deren Hilfe dezentral alle zur Prozeßsteuerung und Prozeßüberwachung erforderlichen analogen und binären

Prozeßvariablen erfaßt, in Meßumformern in elektrische Signale gewandelt und zur Weiterverarbeitung zur Verfügung gestellt werden.

Im linken Teil der Abbildung schließen sich leittechnische Systeme an, die steuernd in den Prozeß eingreifen. Es sind neben Einrichtungen zur manuellen Prozeßsteuerung und Sollwertvorgabe (in Warten und Leitständen) insbesondere jene Systeme, die Signale der Prozeßinstrumentierung automatisch zu Steuerungssignalen weiterverarbeiten. Diese automatisch wirkenden Systeme dienen zur

- Steuerung und Regelung des Prozesses im ungestörten Anlagenbetrieb,
- Begrenzung und Rückführung von Prozeßgrößen, die ihre betrieblichen Toleranzbereiche verlassen (Betriebs- und Zustandsbegrenzungen),
- Auslösung abgestufter Schutzaktionen (zum Beispiel Begrenzen, Reduzieren/Zurückführen, Abschalten) bei sicherheitstechnisch bedeutsamen Betriebsstörungen oder bei Störfällen (Schutzbegrenzungen, Reaktorschutzsystem).

Die genannten Steuerungs- und Schutzeinrichtungen wirken über Vorrangbaugruppen (soweit erforderlich) und Einzelantriebs-Steuereinrichtungen auf die Stellgeräte im Prozeß (im Bild unten) ein.

Wenden wir uns dem rechten Teil von Bild 1 zu, so finden sich dort Informationseinrichtungen (Anzeigeeinrichtungen, Gefahrenmeldeanlagen, Alarmeinrichtungen, Störfallinstrumentierung, Diagnosesysteme), die dem Anlagenpersonal im bestimmungsgemäßen Betrieb der Anlage, aber auch bei Störfällen alle zur Prozeßführung, zur Systemüberwachung sowie für manuelle Steuerungsmaßnahmen erforderlichen aktuellen Informationen und Daten (aus dem Prozeß, aber auch aus den leittechnischen Einrichtungen) zur Verfügung stellen. Über Dokumentationseinrichtungen (Schreiber, Drucker, Massenspeicher etc.) werden wichtige Daten für spätere Auswertungen registriert.

Die Einrichtungen zum betrieblichen Steuern und Regeln, ein oder mehrere gestaffelt wirksam werdende betriebliche Begrenzungssysteme, Schutzbegrenzungen und Reaktor-

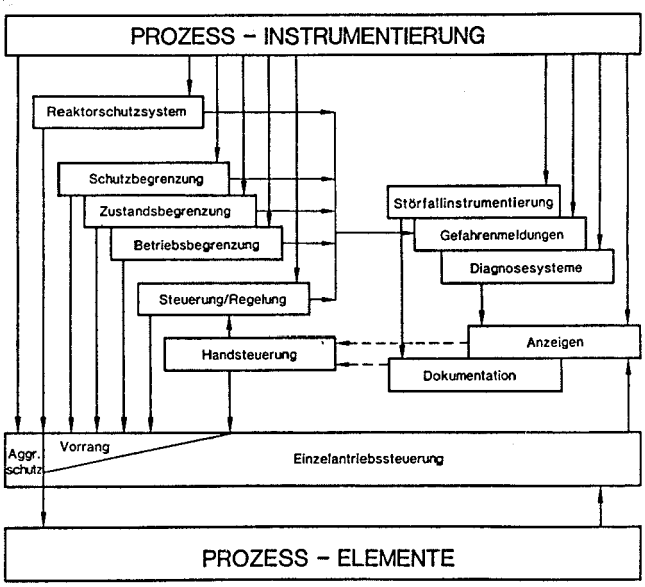


Bild 1: Leittechnik im Kernkraftwerk

schutzsystem bilden aufeinanderfolgende Barrieren gegen das Auftreten gefährlicher Zustände im Prozeß. Im Normalfall halten die betrieblichen Steuerungs- und Regelsysteme alle Prozeßvariablen innerhalb vorgegebener betrieblicher Toleranzbereiche. Versagen diese untersten leittechnischen Barrieren, so greifen als nächstes betriebliche Begrenzungssysteme ein (zum Beispiel Steuerstabausfahrsperre) und verhindern ein weiteres Anwachsen aufgetretener Abweichungen. Reichen auch diese Einrichtungen nicht aus, um eine aufgetretene Störung abzufangen, so kommen die leittechnischen Einrichtungen des Sicherheitssystems zum Tragen. Es sind dies zunächst die Schutzbegrenzungen, die mit noch relativ „weichen" Schutzaktionen (zum Beispiel Stabeinwurf) reagieren, und schließlich das Reaktorschutzsystem, das die letzte Barriere darstellt und mit entsprechend „harten" Schutzaktionen (zum Beispiel Reaktorschnellabschaltung) eingreift.

Das geschilderte Konzept mehrerer aufeinanderfolgender leittechnischer Barrieren ist charakteristisch für die in deutschen Kernkraftwerken realisierte Leittechnik. Es hat sich in der Vergangenheit bewährt und ist insbesondere unter der Bezeichnung „defense-in-depth" bekannt geworden (siehe Bild 2) [2].

Konventionelle leittechnische Geräte und Systeme besitzen folgende kennzeichnenden Merkmale, die für einen Vergleich mit neuen leittechnischen Einrichtungen bedeutsam sind:

- einfache, oder lediglich niedrig integrierte Bauelemente,
- zahlreiche Bauelemente pro Gerät (siehe Bild 3),
- wenige Funktionen pro Gerät,
- zahlreiche Geräte pro leittechnischer Teilaufgabe (zum Beispiel pro Meßkanal),
- getrennte Hardware für getrennte Aufgaben,
- Hardware-Umfang proportional zum Aufgaben-Umfang der Leittechnik.

Bei der sicherheitstechnischen Einstufung der verschiedenen Teile der Leittechnik gibt es einen Unterschied zwischen den globalen Vorgaben, wie sie in Regeln und Richtlinien festgeschrieben sind, und der Praxis von Genehmigungsverfahren: Kerntechnische Regeln und Richtlinien unterscheiden derzeit lediglich zwischen leittechnischen Einrichtungen des Sicherheitssystems und leittechnischen Einrichtungen des Betriebssystems. Diese Zweiteilung ist für eine Bewertung der sicherheitstechnischen Bedeutung der leittechnischen Systeme nicht ausreichend. In der kerntechnischen Praxis hat sich daher eine weitergehende Differenzierung herausgebildet.

Da geeignete quantitative Maßeinheiten für die sicherheitstechnische Bedeutung der Einrichtungen von Kernkraftwerken fehlen, werden diese in der genehmigungstechnischen Praxis üblicherweise drei Sicherheitsklassen zugeordnet.

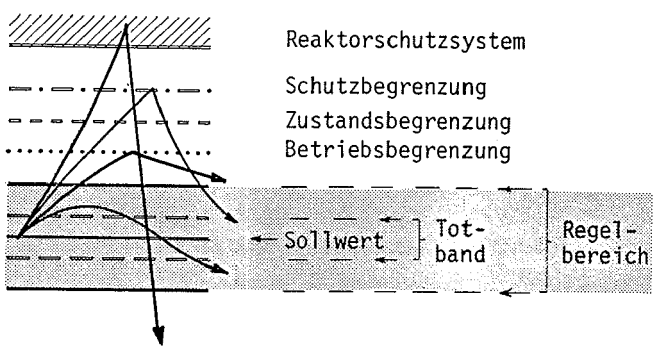


Bild 2: Leittechnikkonzept "defense-in-depth"

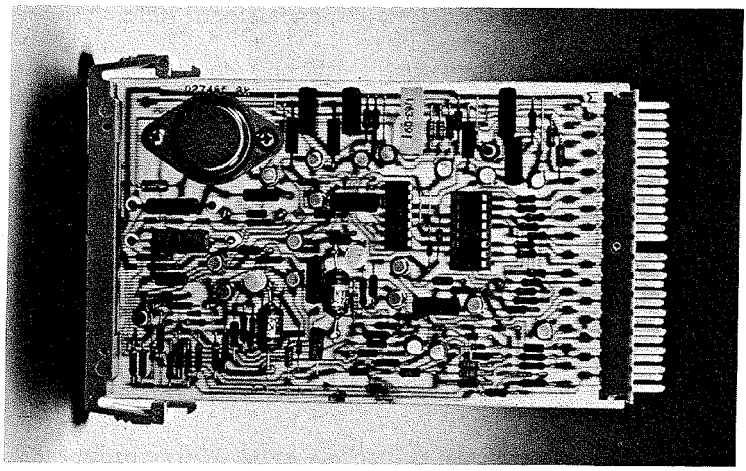


Bild 3: Konventionelle elektronische Baugruppe

Für leittechnische Einrichtungen haben sich dementsprechend folgende Bezeichnungen eingebürgert:

– sicherheitstechnisch wichtige Systeme:	Klasse 1; Klasse A; „schwarz",
– sicherheitstechnisch bedeutsame Systeme:	Klasse 2; Klasse B; „grau", sicherheitstechnisch relevant,
– Systeme ohne sicherheitstechnische Bedeutung	Klasse 3; Klasse C; „weiß", betrieblich

Zu den Einrichtungen ohne sicherheitstechnische Bedeutung (Klasse 3) werden alle Systeme gezählt, die ausschließlich zur Steuerung und Regelung im Normalbetrieb des Kernkraftwerkes dienen und denen keine zusätzlichen sicherheitstechnischen Aufgaben zugeordnet sind. Diese betrieblichen Systeme umfassen den größeren Teil der gesamten Leittechnik eines Kernkraftwerkes.

Zu den sicherheitstechnisch wichtigen leittechnischen Einrichtungen (Klasse 1) zählen die Systeme, die bei Störfällen kurzfristig automatische Schutzaktionen auslösen, um die Anlage innerhalb sicherer Grenzen zu halten oder sie in einen sicheren Zustand zu überführen. Es sind dies das Reaktorschutzsystem und die Schutzbegrenzungen.

In die mittlere Klasse der sicherheitstechnisch bedeutsamen Systeme (Klasse 2) werden zahlreiche und zum Teil recht unterschiedliche Einrichtungen eingeordnet. Im wesentlichen handelt es sich um Einrichtungen, die während des bestimmungsgemäßen Betriebes des Kernkraftwerkes, aber auch bei und nach Störfällen sicherheitstechnisch bedeutsame Informationen über Systemzustände und Prozeßabläufe erfassen und dem Anlagenpersonal zur Verfügung stellen (zum Beispiel Gefahrenmeldeanlage, Störfallinstrumentierung) sowie Einrichtungen, die zur manuellen Prozeßsteuerung bei sich langsam anbahnenden Störungen oder in der Mittel- und Langzeitphase nach Störfällen erforderlich sind.

Neue Leittechnik

Die im vorigen Abschnitt skizzierten leittechnischen Aufgaben werden auch bei Einführung neuer leittechnischer Einrichtungen weiterhin gelten. Im folgenden wird darüberhinaus unterstellt, daß für die zukünftige Leittechnik eine vergleichbare Aufgabenteilung und damit eine vergleichbare Grobstruktur gelten wird (betriebliche Steuerungen und Regelungen, Begrenzungen, Reaktorschutz, Informations- und Dokumentationssysteme).

Elemente, Eigenschaften und Vorteile neuer leittechnischer Einrichtungen

Wie bereits erwähnt, wird die zukünftige Leittechnik von Kernkraftwerken zahlreiche neuartige Bauteile, Komponenten, Verfahren und Strukturen enthalten. Wichtige Beispiele sind:

- Mikroprozessoren,
- Halbleiterspeicher (ROM, PROM, EPROM, RAM, etc.),
- Bus-Systeme,
- verteilte Rechnersysteme,
- Multiplexer und Demultiplexer,
- elektronische Datensichtgeräte und Grafikbildschirme,
- neuartige Bedienungseinrichtungen,
- Analog-Digital (AD)- und Digital-Analog (DA)-Wandler,
- Lichtwellenleiter.

Das bedeutsamste Element der neuen Leittechnik ist der Mikroprozessor (Bild 4). Dies ist ein Halbleiterbauelement, in dem einige zehn- bis hunderttausend logische Funktionselemente realisiert und zu einem vollständigen digitalen Rechnerbaustein zusammengefügt sind. Mit Hilfe geeigneter Programme (Software) sind Mikroprozessoren in der Lage, jede Aufgabe zu lösen, die sich vollständig auf arithmetische Grundfunktionen und logische Entscheidungen zurückführen läßt.

Im Gegensatz zu festverdrahteten, insbesondere analogen Schaltungen kann ein Mikroprozessor (ebenso wie jeder andere Digitalrechner) eine Aufgabe nicht kontinuierlich ausführen. Kontinuierlich auszuführende Aufgaben können daher nur durch zyklische Wiederholung des Programmes realisiert werden. Aufgrund der hohen Arbeitsgeschwindigkeit von Mikroprozessoren ist hierbei jedoch eine quasi-kontinuierliche Aufgabenausführung möglich.

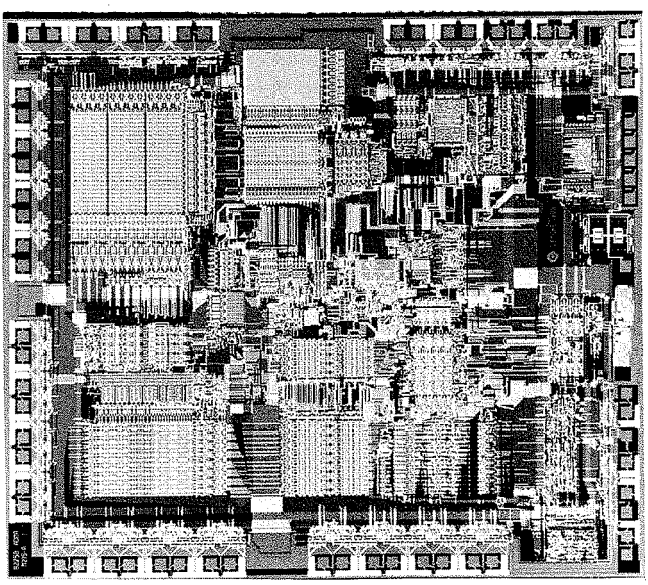


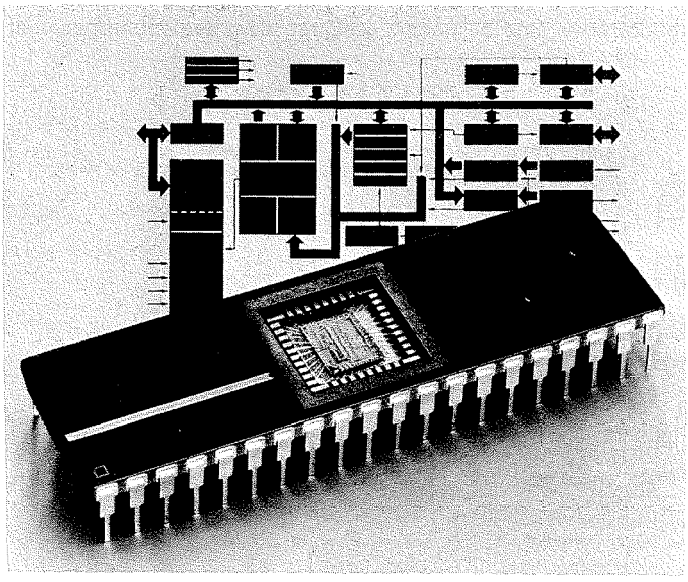
Bild 4: Mikroelektronisches Bauelement (Mikrochip)

Die hohe Arbeitsgeschwindigkeit und die sequentielle Arbeitsweise erlauben zusätzlich eine quasi-gleichzeitige Bearbeitung mehrerer unterschiedlicher Aufgaben durch eine einzige Hardware-Einrichtung. Von dieser Fähigkeit digitaler Rechner wird zum Beispiel bei Prozeßrechnern intensiv Gebrauch gemacht. Mit Rechnern läßt sich auf diese Weise eine sehr weitgehende Reduktion des Hardware-Bedarfes erzielen. Die Möglichkeit, mehrere Aufgaben von einer einzigen Hardware-Einrichtung quasi-gleichzeitig ausführen zu lassen, eröffnet auch völlig neue und sehr leistungsfähige Wege zur Selbstüberwachung der neuen Leittechnik; dies ist ein ganz wesentlicher Vorteil dieser Technik.

Die Funktion eines Rechners wird nicht durch die Hardware, sondern durch Programme (Software) bestimmt. In diesen aus standardisierten Einzelanweisungen aufgebauten Programmen wird festgelegt, welche Grundfunktionen von der Hardware sequentiell ausgeführt, welche Daten verwendet, wie diese Daten verknüpft und wohin sie übertragen werden sollen. Die Entwicklung von Programmen wird durch die Verwendung von Entwicklungssystemen und hochentwickelten Programmiersprachen so weit unterstützt, daß die Programmerstellung und Programmprüfung auch ohne Hardware-Kenntnisse möglich ist. Selbst der Rechner, auf dem das Programm eingesetzt werden soll, braucht für die Software-Entwicklung meist nicht zur Verfügung zu stehen.

Ein Mikroprozessor benötigt immer einen oder mehrere Speicherbausteine. In diesen Speicherbausteinen müssen einerseits das zu bearbeitende Programm und erforderliche feste Daten abgelegt und vorgegeben sein. Andererseits legt der Prozessor selbst in Speichern Eingangs- und Ausgangsdaten sowie Zwischenergebnisse ab und holt sie bei Bedarf von dort zurück.

Der Datenaustausch zwischen Mikroprozessoren, Speicherbausteinen, Ein-/Ausgabe-Ports etc. erfolgt über sogenannte Bus-Systeme. Ein Rechner benötigt mindestens einen Datenbus und einen Adressbus. Der Datenbus verbindet zum Beispiel die Datenausgänge des Prozessors mit den Dateneingängen aller vorhandenen Peripherie-Bausteine (Speicher, Eingabe- und Ausgabe-Ports). Ein vom Prozessor auf diesen Datenbus ausgegebenes Datum erreicht damit alle angeschlossenen Peripherie-Bausteine. Über den Adressbus teilt



der Prozessor anschließend allen angeschlossenen Bausteinen mit, in welche Adresse (zum Beispiel in welche Speicherstelle) das Datum übernommen werden soll. Der Datenbus wird vom Prozessor gleichermaßen für das Senden und Empfangen von Daten verwendet. Ob ein Datum abgerufen oder übergeben werden soll, teilt der Prozessor den peripheren Bauteilen zum Beispiel über eine zusätzliche Leitung mit. Die geschilderte prinzipielle Konfiguration erlaubt es zum Beispiel einem 16-Bit-Prozessor, über 16 Daten- und 20 Adressleitungen mit mehr als 1 Million 16-bit-tiefen Speichern Daten auszutauschen.

Über Bussysteme werden auch die Verbindungen zwischen Mikrocomputern und anderen Geräten, zum Beispiel externen Speichern, AD- und DA-Wandlern, zwischen mehreren Mikrocomputern bzw. zu anderen Rechnern hergestellt. Sind an ein Bussystem mehrere Teilnehmer mit aktiver Zugriffsmöglichkeit angeschlossen, so muß die Zugriffsberechtigung auf den gemeinsamen Systembus in geeigneter Weise geregelt und eine entsprechende Busverwaltung implementiert werden. Durch solche Buskopplungen können äußerst leistungsfähige Gesamtsysteme realisiert werden.

Bild 5 zeigt beispielhaft ein dezentral organisiertes Automatisierungssystem, in dem die einzelnen Teilautomatisierungseinrichtungen untereinander und mit zentralen Bedien- und Beobachtungseinrichtungen über einen Systembus verbunden sind. Jede Teilautomatisierungseinrichtung kann hierbei selbst wieder aus einer Vielzahl von Einzelrechnern bestehen.

Von Ausnahmen abgesehen muß ein für leittechnische Aufgaben eingesetzter Mikrocomputer mehr externe Signale verarbeiten als ihm Eingänge und Ausgänge zur Verfügung stehen. Es ist daher erforderlich, zwischen Mikrocomputer und zu überwachendem oder zu steuerndem Prozeß Multiplexer bzw. Demultiplexer einzufügen. Multiplexer und Demultiplexer stellen dann – zum Beispiel gesteuert durch den Mikrocomputer selbst – sequentiell die erforderlichen Verbindungen her. Da ein Rechner die verschiedenen Signale ohnedies nur sequentiell einlesen bzw. ausgeben kann, stellen Multiplexer und Demultiplexer optimale Verbindungselemente zum Prozeß dar.

Mikroprozessorgestützte Informations- und Automatisierungseinrichtungen schließen in der Regel neuartige Anzeige- und Bedieneinrichtungen ein. Elektronische Datensichtgeräte und insbesondere Grafikbildschirme sind besonders geeignet, dem Bedienungspersonal

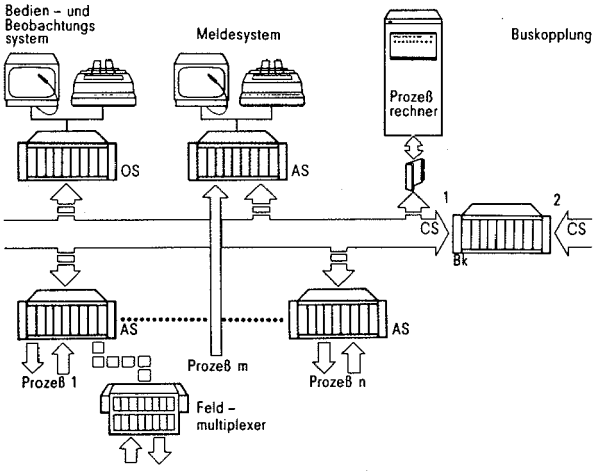


Bild 5: Dezentrales mikrocomputergestütztes Automatisierungssystem ([3])

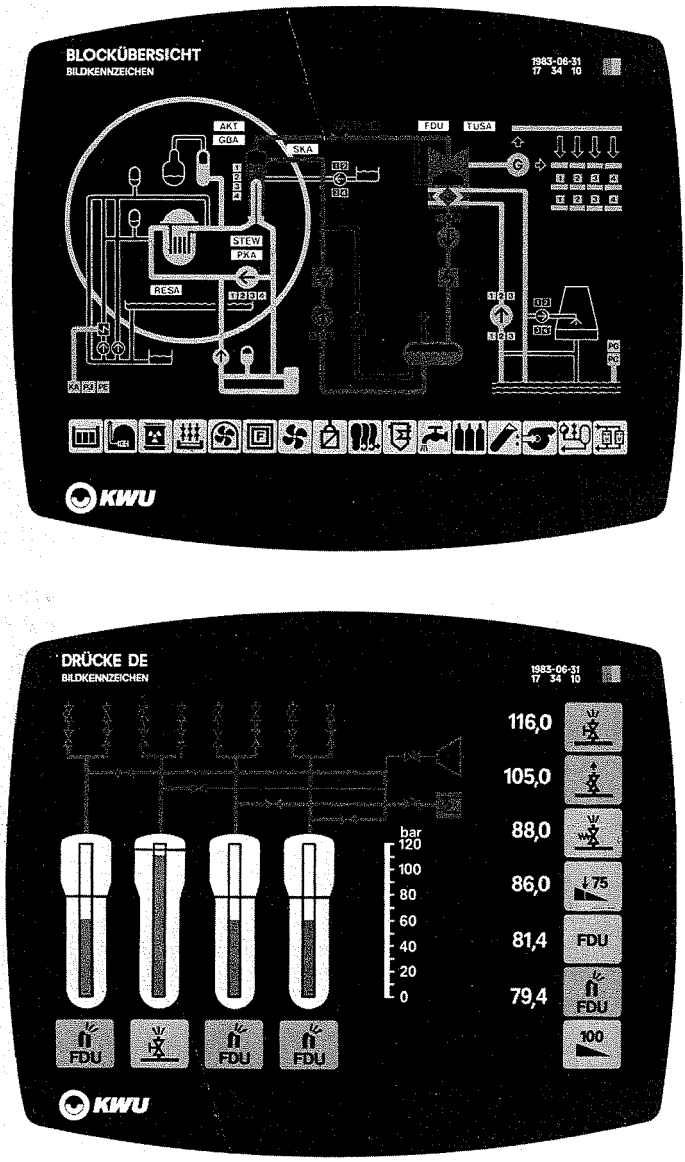


Bild 6: Informationsdarstellung auf dem Bildschirm

Informationen in leicht verständlicher Form (zum Beispiel unter Verwendung von Anlagenübersichtsbildern, Diagrammen, Trendanzeigen) zur Verfügung zu stellen (Bild 6).

Durch Informationsverdichtung über rechnerische Anlagen und Systemmodelle können viele schwer zu überblickende Einzelinformationen zusammengefaßt und damit die derzeitige Informationsflut in den Warten von Kernkraftwerken wirksam abgebaut werden. Die Bedienung der Bildschirmgeräte kann äußerst einfach gestaltet werden. Verbreitet sind

Lichtgriffel, mit denen auf dem Bildschirm dargestellte Bedienfunktionen durch einfaches Abtasten aufgerufen werden können, aber auch „mouse" und „roller ball". Durch solch einfache Bedienmaßnahmen kann zwischen Übersichts- und Detaildarstellungen, zwischen Moment- und Trendanzeigen usw. gewählt werden.

Bei heute verfügbaren mikroprozessorgestützten Automatisierungseinrichtungen sind nicht nur die Bedienung von Anzeige- und Beobachtungsstationen, sondern auch manuelle Steuerungseingriffe in den Prozeß über Bildschirme und zum Beispiel Lichtgriffel oder über „touch sensitive screens" möglich.

Als letztes soll ein neuartiges Element leittechnischer Systeme angesprochen werden, das nicht unmittelbar mit der Einführung mikroprozessorgestützter Systeme verknüpft ist, der Lichtwellenleiter. In heutigen Kernkraftwerken verbinden große Mengen von Leittechnikkabeln mehrere räumlich weit voneinander entfernte „Leittechnikinseln", zum Beispiel das Notspeisegebäude mit dem Schaltanlagengebäude. Es sind sehr umfangreiche technische Maßnahmen erforderlich, um bei den bisher verwendeten Kupferkabeln Störungen wegen Unterschieden in den Bezugspotentialen der einzelnen Leittechnikinseln oder Störungen aufgrund induzierter Störspannungen (zum Beispiel bei Blitz) zu vermeiden. Als Schutzmaßnahmen sind derzeit Entkopplungsschaltungen an beiden Enden jeder Leitung und aufwendige Abschirm- und Potentialausgleichsmaßnahmen üblich. Die genannten Probleme ließen sich auf einfachste Weise eliminieren, wenn für die Signalübertragung Lichtwellenleiter anstelle der Kupferleitungen eingesetzt würden.

Dem Einsatz von Lichtwellenleitern stehen bisher hauptsächlich zwei Gründe entgegen: der hohe Preis und die fehlende Eignung der Lichtwellenleiter zur Übertragung analoger Signale. Beide Gründe könnten jedoch beim Einsatz mikroprozessorgestützter leittechnischer Einrichtungen bedeutungslos werden. Analoge Signale müssen vor der Verarbeitung in Mikrocomputern ohnedies digitalisiert werden. Digitale Signale können problemlos über Lichtwellenleiter übertragen werden. Da der Einsatz von Mikroprozessoren zwangsweise den Einsatz von Multiplexern und Demultiplexern mit sich bringt, lassen sich auch die Zahl der erforderlichen Lichtleiterkabel und damit deren Gesamtkosten erheblich reduzieren.

Probleme beim Einsatz neuer Leittechnik

Bisher wurden nur Vorteile der neuen Leittechnik genannt. Diesen Vorteilen stehen jedoch einige Probleme gegenüber, die sich ergeben, wenn die neue Leittechnik für Aufgaben mit Sicherheitsbedeutung eingesetzt werden soll. Die aus sicherheitstechnischer Sicht wesentlichsten sollen hier aufgezeigt werden.

Das gravierendste Problem mikroelektronischer Systeme – insbesondere mikroelektronischer Rechnersysteme – liegt darin, daß die Prüfung einer fehlerfreien Auslegung und die Erkennung im Einsatz auftretender Ausfälle erheblich erschwert sind. Dieses Problem und Möglichkeiten zu seiner Lösung sollen im Zusammenhang mit der Frage der Qualifizierbarkeit der neuen Leittechnik im nächsten Abschnitt detaillierter diskutiert werden.

Mikroprozessorgestützte Systeme sind unter anderem deshalb so leistungsfähig, weil sie Daten sequentiell bearbeiten und Hardwareeinrichtungen in zeitlicher Folge für ganz unterschiedliche bzw. unabhängige Aufgaben nutzen können. Wird von dieser Fähigkeit Gebrauch gemacht, so führt dies zwangsläufig dazu, daß im Grunde unabhängige Aufgaben bei einem einzelnen Hardwareausfall gleichzeitig betroffen werden. Bei konventionellen leittechnischen Systemen waren für unabhängige Aufgaben technisch bedingt von selbst weitgehend unabhängige Hardware-Einrichtungen vorhanden. Das genannte Problem läßt sich dadurch lösen, daß zum Beispiel innerhalb einer Redundanzgruppe nur solche Funktionen einer gemeinsamen Hardware zugeordnet werden, deren gleichzeitiger Ausfall aus sicherheitstechnischer Sicht unbedenklich ist. Sicherheitsuntersuchungen auf

Systemebene werden daher bei der Beurteilung realisierter Anlagen eine wesentliche Rolle erhalten.

Mikroprozessorgestützte Systeme erlauben an vielen Stellen exaktere Problemlösungen als konventionelle elektronische Geräte (zum Beispiel Berechnung des DNB-Verhältnisses). Diese Fähigkeit der neuen Leittechnik kann dazu genutzt werden, um bei (den seltenen) Betriebsstörungen anlagenschonendere Gegenmaßnahmen zu ermöglichen. Bei Einsatz neuer leittechnischer Einrichtungen wird es jedoch auch möglich, im Dauerbetrieb des Kernkraftwerkes näher an sicherheitsrelevante Grenzen heranzugehen (zum Beispiel Betrieb mit höheren Leistungsdichten im Reaktorkern). Wegen der hiermit verbundenen wirtschaftlichen Vorteile wird dies sicherlich auch angestrebt werden. Die Konsequenz könnte ein Betrieb mit höheren Beanspruchungen verfahrenstechnischer Komponenten und mit geringeren Sicherheitsabständen sein. Auch dieses Problem ist lösbar, indem im Rahmen der Auslegung und Begutachtung auf die Einhaltung ausreichender Sicherheitsabstände geachtet wird.

Die neue Leittechnik bietet ausgezeichnete Voraussetzungen für eine dringend erforderliche Reduktion der heute in Leitständen und Warten konzentrierten Menge von Detailinformationen für das Anlagenpersonal sowie für eine ergonomisch optimale Informationsdarstellung zum Beispiel auf Grafikbildschirmen. Die Möglichkeiten, die Gesamtzuverlässigkeit des Mensch-Maschine-Systems zu steigern, stoßen jedoch auf Grenzen. Werden Prozeßinformationssystemen, Diagnosesystemen etc. sehr komplizierte Anlagen- und Systemmodelle zugrundegelegt oder wird die Informationsreduktion zu weit getrieben, so sinkt in gleichem Maße die Fähigkeit des Anlagenpersonals, die angebotene Gesamtinformation zum Beispiel mit Hilfe von Plausibilitätsbetrachtungen auf Korrektheit zu prüfen. Soll die Gesamtzuverlässigkeit der Mensch-Maschine-Kommunikation bei zukünftigen Informationssystemen gegenüber konventionellen Meldeanlagen mindestens gleich bleiben, so muß zum Beispiel sichergestellt werden, daß entweder das Personal auch auf die dem Prozeß entnommene Primärinformation zurückgreifen kann, oder daß zusätzliche Maßnahmen die Fehlerfreiheit der Primärinformation zuverlässig überwachen.

Existierende und in Regeln und Richtlinien niedergelegte kerntechnische Anforderungen sind zwar von der Zielsetzung her technologieneutral. Häufig orientieren sich diese Anforderungen dennoch so stark an bekannten und in der Kerntechnik bereits eingesetzten Leittechniksystemen, daß sie für die neue Leittechnik nicht anwendbar sind. Dabei geht es meist nicht darum, daß eine Anforderung von der Zielsetzung her nicht erfüllt werden könnte. Das Problem liegt vielmehr darin, daß auf neue leittechnische Einrichtungen nicht unmittelbar anwendbare Auslegungs- und Qualifizierungsanforderungen formuliert, die eigentlichen Anforderungsziele jedoch ungenannt sind.

So stellt zum Beispiel die kerntechnische Regel KTA 3501 an Geräte des Reaktorschutzsystems und von Schutzbegrenzungen folgende Forderung: „Das Schaltungskonzept muß einfach, übersichtlich und zweckentsprechend sein". Die Forderung ist so formuliert, daß sie keine Ausnahmen zuläßt. Im Hinblick auf das angesprochene „Schaltungskonzept" ist davon auszugehen, daß dieses bei speicherprogrammierbaren Einrichtungen nicht nur die Hardware, sondern auch die Software einschließt. Schwieriger ist die Frage, wann ein Schaltungskonzept „einfach" und „übersichtlich" ist. Beide Eigenschaften sind nicht absolut meßbar oder quantifizierbar; eine Bewertung hängt vollständig davon ab, wie gut der Beurteilende mit der betrachteten Technik vertraut ist und welche Vergleichsmaßstäbe er anlegt. Unabhängig von solchen Interpretationsspielräumen muß festgestellt werden, daß die zitierten Anforderungen nach „Einfachheit" und „Übersichtlichkeit" mit neuen leittechnischen Einrichtungen, insbesondere mit mikroelektronischen Einrichtungen, nur schwer, ohne Verzicht auf funktionell besonders leistungsfähige Strukturen eventuell überhaupt nicht wörtlich erfüllbar ist. Berücksichtigt man jedoch, daß die Anforderungen dazu dienen sollen,

– Auslegungsfehler vermeidbar und auffindbar zu machen,

- Qualifizierungsprüfungen zu erleichtern oder zu ermöglichen,
- Fehler bei Bedienung, Instandhaltung und Programmpflege im Betrieb vermeidbar zu machen,

so eröffnen sich durchaus Möglichkeiten, diese Anforderungen von ihrer Zielsetzung her zu erfüllen.

Ein weiteres Beispiel für existierende, aber auf mikroelektronische Einrichtungen nicht unmittelbar anwendbare Anforderungen betrifft die „Ausfalleffektanalyse". Mit ihrer Hilfe sollen zum Beispiel bei Geräten die Auswirkungen aller technisch möglichen Bauelementausfälle auf die Gerätefunktion ermittelt werden. Diese Analyse ist bei mikroelektronischen Bauelementen nicht durchführbar. Nun ist die Angabe der Ausfalleffekte im kerntechnischen Regelwerk (KTA 3503) eine Soll-Anforderung, von der in begründeten Ausnahmefällen abgewichen werden darf. Die fehlende Durchführbarkeit einer Prüfung kann für sich alleine jedoch kein hinreichender Grund für den Verzicht auf die Erfüllung einer Anforderung sein.

Beleuchtet man die hinter der Ausfalleffektanalyse verborgenen Nachweisziele, so ist festzustellen, daß die Kenntnis der Ausfalleffekte dazu dient, um auf der Ebene leittechnischer Systeme beurteilen zu können,

- ob Geräteausfälle gefährlich wirken können,
- durch welche Maßnahmen eine vollständige Ausfallerkennung erreichbar ist.

Da gerade Fragen dieser Art bei komplexen Systemen besonders schwer beurteilt werden können, wäre die Ausfalleffektanalyse an mikroelektronischen Einrichtungen im Grunde wichtiger als bei konventionellen Geräten. Ein ersatzloser Verzicht auf die Ausfalleffektanalyse erscheint daher beim Einsatz neuer leittechnischer Einrichtungen für sicherheitstechnische Aufgaben im Kernkraftwerk nicht zulässig. Es ist vielmehr notwendig, die Anforderungen ihrem Sinngehalt nach zu erfüllen. Angesichts der fehlenden Kenntnis der Ausfalleffekte erfordert dies einen größeren Umfang von Maßnahmen zur Ausfalltolerierung und zur Ausfallerkennung.

Die oben genannten Beispiele zeigen, daß die Einführung der neuen Leittechnik neben erheblichen Vorteilen auch einige neue Fragestellungen mit sich bringt. Mit Hilfe geeigneter Problemanalysen lassen sich diese Fragestellungen erkennen und Lösungswege auffinden. Bisher bereits durchgeführte Problemanalysen zeigen, daß sicherheitstechnische Grundanforderungen der Kerntechnik auch mit neuen leittechnischen Einrichtungen erfüllt werden können.

Bewertung des Einsatzes neuer leittechnischer Einrichtungen für sicherheitstechnische Aufgaben

Nach dieser Darstellung von besonderen Leistungsmerkmalen und Problemen neuer leittechnischer Einrichtungen stellt sich die Frage, ob ein Einsatz dieser Einrichtungen für sicherheitstechnische Aufgaben anzustreben ist. Dabei ist zu untersuchen, welche Einsatzbereiche in Frage kommen und welche Gründe den Einsatz zweckmäßig erscheinen lassen.

Bewertet man, an welchen Stellen im Kernkraftwerk ein Einsatz neuer leittechnischer Einrichtungen aus sicherheitstechnischer Sicht Vorteile verspricht, so läßt sich feststellen:

- Durch die Möglichkeit komplexerer und exakterer Modelle und Algorithmen lassen sich wesentlich feinfühliger reagierende Begrenzungseinrichtungen realisieren. Damit kann das oben genannte Defense-in-Depth-Konzept wesentlich leistungsfähiger gemacht werden.
- Die Möglichkeit komplexerer und exakterer Modelle und Algorithmen erlaubt die Erstellung leistungsfähiger Diagnose- und Expertensysteme, mit deren Hilfe sich zum Bei-

spiel Störungsanalysen, Schadensfrüherkennung und Maßnahmen zum Accident-Management realisieren lassen.

- Die funktionale Leistungsfähigkeit neuer Einrichtungen erlaubt in Verbindung mit elektronischen Grafikbildschirmen eine ergonomisch optimierte Bereitstellung von Informationen für das Kraftwerkspersonal. Neben der Bereitstellung von Informationen in leicht verständlicher Form ist durch Informationsauswahl und -verdichtung insbesondere auch eine Eliminierung der Informationsflut in Warten und Leitständen realisierbar.

Die innerhalb des Reaktorschutzsystems zu realisierenden Funktionen sind grundsätzlich von geringer Komplexität. Der Einsatz neuer leittechnischer Einrichtungen wird daher Vorteile im Hinblick auf exaktere und leistungsfähigere Problemlösungen nur an einzelnen Stellen mit sich bringen. Beispiele möglicher Verbesserungen sind

- exaktere Füllstandskorrekturrechnungen,
- exaktere Reaktorleistungsberechnungen,
- optimalere gleitende bzw. situationsbedingte Grenzwerte,
- verbesserte Selbstüberwachung.

Bereits Überlegungen, die unter dem Aspekt des erreichbaren sicherheitstechnischen Gewinnes durchgeführt wurden, führen somit zu der Feststellung, daß ein Einsatz neuer leittechnischer Einrichtungen in weiten Bereichen der Leittechnik von Kernkraftwerken zweckmäßig ist. In Verbindung mit dem gegenwärtig sich vollziehenden Technologiewandel gibt es darüberhinaus jedoch auch Gründe, daß die Einführung der neuen Leittechnik langfristig sogar unvermeidbar ist. Dies ergibt sich zum Beispiel aus der Tatsache, daß derzeit bzw. in der Vergangenheit eingesetzte leittechnische Einrichtungen zukünftig von der Industrie nicht mehr hergestellt werden und damit nicht mehr verfügbar sein werden (auch nicht als Ersatzteile für Altanlagen). Bereits Engpässe bei der Verfügbarkeit von Ersatzteilen und qualifiziertem Personal für „veraltete" Technik könnten eine nicht akzeptable Minderung der Sicherheit mit sich bringen.

Derzeitige Einsatzpraxis in Kernkraftwerken

Gegenwärtig existieren in Deutschland noch wenige Anwendungen mit neuer Leittechnik für sicherheitsrelevante Aufgaben in Kernkraftwerken. Gescheitert ist der Einsatz eines Schutzrechner-Systems für die Anlagen Brunsbüttel und Philippsburg 1. Realisiert wurden unter anderem folgende Systeme: Steuerstabfahrrechner in SWR, Kernschutzrechner in Grafenrheinfeld, DNB-Rechner in Mülheim-Kärlich, Siedeabstandsrechner für die Störfallübersichtsanzeige in Grohnde und Philippsburg 2.

Die derzeit in der deutschen Kernenergie erkennbaren Entwicklungstendenzen bestätigen zumindest zum Teil die im vorigen Abschnitt genannten Einsatzbereiche. Der Schwerpunkt der Entwicklung lag in den letzten Jahren auf dem Gebiet der intelligenten Informations- und Diagnosesysteme (zum Beispiel STAR-Generis; PRINS; SÜS/KÜS; Kernüberwachung). Es ist bekannt, daß für die nächste Generation von Kernkraftwerken Bestrebungen bestehen, zusätzlich neue leittechnische Einrichtungen im Bereich betrieblicher Automatisierung, insbesondere aber auch im Bereich der Begrenzungssysteme einzusetzen.

Bisher ist in Deutschland nur eine sehr zögernde Entwicklung beim Einsatz neuer Einrichtungen für Reaktorschutzsysteme zu erkennen. Die Gründe hierfür liegen auf der Hand: Angesichts des Mangels genehmigungsspezifischer einheitlicher Vorgaben (vorhandene Regeln und Richtlinien sind an der konventionellen Technik orientiert und derzeit fallweise zu interpretieren) sowie der Schwierigkeiten, die sich beim Sicherheitsvergleich zweier unterschiedlicher Technologien zwangsläufig ergeben (die neue Technik darf keine Sicherheitseinbußen verursachen, der Nachweis muß qualifiziert erfolgen), scheuen die Betreiber und Hersteller derzeit — wie bisherige Erfahrungen zeigen: zu recht — das hohe

Genehmigungsrisiko. Hier ist sicherlich die Genehmigungsseite, das heißt die öffentliche Hand, aufgerufen, durch Schaffung geeigneter Rahmenbedingungen dafür Sorge zu tragen, daß nicht das Genehmigungsverfahren selbst sicherheitstechnisch wünschenswerte, durch neue Technik machbar gewordene, Systemlösungen verhindert oder langfristig sogar Sicherheitsprobleme erzeugt.

Die Situation wird noch verschärft, da das schrittweise Einführen neuer Leittechnik, das die Kostenrisiken der Genehmigung reduzieren könnte, wegen besonderer Schwierigkeiten bei der Kommunikation verschiedener Leittechnik-Arten und somit zusätzlicher Sicherheitsprobleme nicht zweckmäßig ist und letztlich – innerhalb kommunizierender Teilsysteme – nur ganzheitliche Lösungen sinnvoll sind. Es ist unmittelbar einsichtig, daß ein Nebeneinander von „1-Signal/ 1-Draht"-Technik mit „Bus-System"-Technik solche Probleme schaffen würde.

Betrachtet man die Entwicklung der Leittechnik von Kernkraftwerken im Ausland, so sind zwei Gruppen von Ländern mit jeweils entsprechender Grundeinstellung und Genehmigungssituation zu unterscheiden. Bei den einen besteht offensichtlich deutlich weniger Zurückhaltung im Hinblick auf den Einsatz mikroprozessorgestützter bzw. rechnergestützter Systeme für sicherheitstechnische Aufgaben. Beispiele für rechnergestützte Reaktorschutzsysteme sind

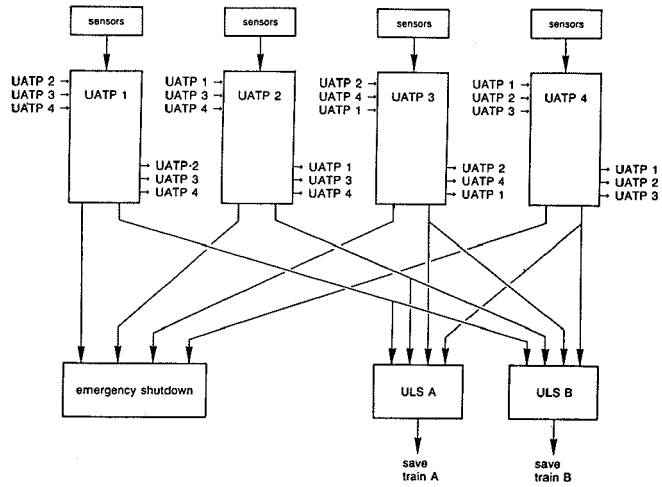
- das in französischen Kernkraftwerken der 13-MW-DWR-Baulinie eingesetzte rechnergestützte Reaktorschutzsystem SPIN (Bild 7),
- ein für kanadische Reaktoren (CANDU-Reaktoren) im Kernkraftwerk Darlington vorgesehenes Rechner-Schutzsystem,
- ein von Westinghouse entwickeltes Rechner-Schutzsystem EAGLE (das jedoch offensichtlich nur bei Exportaufträgen Chancen hat, eingesetzt zu werden).

Andere Länder haben eine vergleichbare Situation wie Deutschland. In USA zum Beispiel ist zwar ein von Combustion Engineering entwickelter Kernschutz-Rechner im Einsatz (der im wesentlichen DNB-Verteilungen berechnet) und hat Westinghouse das rechnergestützte Schutzsystem EAGLE entwickelt. Aufgrund der festgeschriebenen Sicherheitsstandards und hochentwickelten, allerdings auf konventionelle Technik ausgerichteten, Regeln und Richtlinien existieren jedoch Innovationshemmnisse, die ohne Schaffung neuer Rahmenbedingungen nicht überwunden werden können. NRC hat die Notwendigkeit, sich mit dieser Problematik intensiv zu befassen, erkannt und die Betreiber und Industrie aufgerufen, zusammen mit ihr die Probleme anzugehen. Im November letzten Jahres fand in Washington ein Symposium über neue Leittechnik statt [8], das auf Anregung von NRC gegenüber EPRI zustandegekommen war und das den Start intensiver gemeinsamer Bemühungen darstellen sollte. Es dürfe nicht sein, daß ein „High-Tech"-Land wie USA in ihren Kernkraftwerken nur konventionelle unflexible Technik einsetzt, während Entwicklungsländer die Vorteile der modernen Technik ohne Einschränkungen nutzen können, beschrieb der vor kurzem für die Intensivierung der Leittechnikaktivitäten beauftragte EPRI-Programmanager die Haltung verantwortlicher Stellen in seinem Lande. Auf dem Gebiet der Leittechnik seien gewaltige Fortschritte und echte Innovationen möglich geworden, die Leittechnik berge daher auch das größte Entwicklungspotential für weitere Verbesserungen der Reaktorsicherheit und Verfügbarkeit.

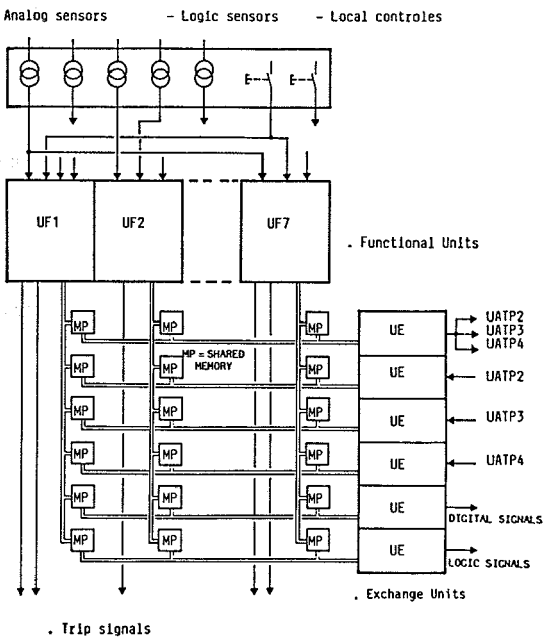
Die Häufung von einschlägigen Meetings und internationalen Symposien in USA (zum Beispiel [4] bis [7]) sowie der rege Zuspruch, den diese Veranstaltungen verzeichneten, zeigen, welche Bedeutung neuen leittechnischen Systemen für Kernkraftwerken in diesem Land beigemessen wird.

Bild 7a zeigt das aus vier gleichen mikroprozessorgestützten Meßwerterfassungs- und Signalverarbeitungssystemen (UATP) bestehende Reaktorschutzsystem SPIN, das zur Auslösung von Reaktorschnellabschaltung und anderen Schutzaktionen dient.

Bild 7b verdeutlicht die innere Struktur eines UATP.



a)



b)

Bild 7: Französisches μP-gestütztes Reaktorschutzsystem SPIN ([8])

Qualifizierung neuer leittechnischer Einrichtungen

Wie zuletzt dargestellt, gibt es viele und gute Gründe, die neue Leittechnik in Kernkraftwerken einzusetzen. Mit neuen leittechnischen Einrichtungen erreichbare Vorteile sind hier zu nennen, aber auch die Notwendigkeit, dem Stand der Technik zu folgen. Eine Verwendung für sicherheitstechnische Aufgaben setzt zusätzlich voraus, daß die Eignung der neuen Leittechnik im Rahmen atomrechtlicher Genehmigungsverfahren nachgewiesen werden kann.

Im folgenden soll untersucht werden, ob die für konventionelle leittechnische Einrichtungen üblichen Qualifizierungsmethoden und Qualifizierungsprozeduren auch für neue leittechnische Einrichtungen geeignet sind, welche neuen Qualifizierungsmethoden zur Verfügung stehen, und an welchen Stellen Weiterentwicklungen erforderlich sind.

Derzeitiger Stand der Qualifizierbarkeit

Die meisten bei neuen leittechnischen Einrichtungen auftretenden Qualifizierungsfragen lassen sich auf den Problemkreis „Erkennbarkeit von Fehlern und Ausfällen" zurückführen. Aus diesem Grunde soll dieser Problemkomplex den folgenden Betrachtungen zugrunde gelegt werden.

Die Erkennbarkeit von Fehlern und Ausfällen nimmt im Rahmen der Qualifizierung leittechnischer Einrichtungen in drei Phasen eine entscheidende Rolle ein.

- Zunächst müssen geeignete Verfahren verfügbar sein zum Nachweis, daß eine zu qualifizierende Einrichtung keine Auslegungsfehler, das heißt keine Entwurfs- und Konstruktionsfehler beinhaltet. Dieser Nachweis ist von übergeordneter Bedeutung, da Auslegungsfehler systematisch alle gleichartigen Komponenten, Geräte und Systeme betreffen und eine der wichtigsten zuverlässigkeitserhöhenden Maßnahmen im Sicherheitssystem von Kernkraftwerken, die Redundanz, von vorneherein unwirksam machen.
- Weiterhin müssen ausreichende Fehler- und Ausfallerkennungsmethoden verfügbar sein, um Fertigungs- und Herstellungsfehler feststellen und fehlerhafte Teile aussondern zu können.
- Schließlich muß bereits im Rahmen der Qualifizierung eine ausreichende Erkennbarkeit von Ausfällen während des Einsatzes im Kernkraftwerk nachweisbar sein. Ohne eine ausreichend vollständige Erkennbarkeit von Ausfällen im Einsatz läßt sich die erforderliche Zuverlässigkeit der Sicherheitssysteme nicht über die gesamte Betriebszeit eines Kernkraftwerkes erhalten.

Bei konventionellen leittechnischen Geräten erfolgt der Nachweis der fehlerfreien Funktions-Auslegung im Rahmen von Typprüfungen mit Hilfe von Funktionsprüfungen[2]). Bei diesen Funktionsprüfungen werden an den Geräteeingängen alle relevanten Eingangssignale, Eingangssignalverläufe und Eingangssignalkombinationen aufgeprägt und die Gerätefunktionen durch Messung der korrespondierenden Signale an den Geräteausgängen ermittelt. Die hierfür erforderlichen Prüfprogramme orientieren sich bei konventionellen Geräten kaum an der geräteinternen Schaltung, sondern fast ausschließlich an den in Anforderungsspezifikationen, Datenblättern und sonstigen Geräteunterlagen ausgewiesenen Sollfunktionen.

Die Erkennung von Fertigungs- und Herstellungsfehlern im Rahmen von Werksprüfungen stützt sich ebenfalls wesentlich auf Funktionsprüfungen an fertigen Geräten.

Für die Ausfallerkennung im kerntechnischen Einsatz kommen bei der konventionellen Leittechnik recht einfache und dennoch sehr wirksame Verfahren zum Einsatz. So werden zur Ausfallerkennung Überwachungseinrichtungen in leittechnische Systeme eingebaut, die zum Beispiel auf der Basis eines einfachen Vergleichs der Ausgangssignale redundanter Geräte und Signalkanäle arbeiten oder die andere einfach meßbare Systemzustände (zum Beispiel Versorgungsspannung, dynamische Signalwechsel) auf Abwei-

---

[2]) Bei sogenannten Fail-Safe-Schaltungen sind zusätzlich Ausfalleffektanalysen zum Nachweis des spezifikationsgemäßen Ausfallverhaltens durchzuführen. Da Fail-Safe-Schaltungen kaum mit mikroelektronischen Schaltungen realisiert werden, wird hierauf an dieser Stelle nicht weiter eingegangen.

chungen von Sollzuständen überwachen. Diese Selbstüberwachungsverfahren werden zum Teil durch gezielte Auslegungsmaßnahmen erleichtert bzw. ermöglicht, zum Beispiel durch die analoge Erfassung von Prozeßvariablen oder die Verwendung dynamisierter logischer Signale. Ergänzt werden diese Maßnahmen zur Selbstüberwachung durch administrativ geregelte wiederkehrende Prüfungen aller sicherheitstechnisch wichtigen Systeme während des Kernkraftwerksbetriebs. Diese wiederkehrenden Prüfungen werden grundsätzlich in Form von Funktionsprüfungen auf Systemebene durchgeführt. In der Regel werden keine besonderen Geräteeigenschaften, sondern nur die Systemfunktion bei simulierten Anforderungsbedingungen (das heißt zum Beispiel mit simulierten Anregesignalen) geprüft. Von den genannten und weitgehend standardisierten Überwachungs- und Prüfmaßnahmen wird nur in begründeten Ausnahmefällen abgewichen, zum Beispiel aufgrund der Ergebnisse von Ausfalleffektanalysen an Geräten.

Die genannten Nachweise und Ausfallerkennungsmaßnahmen sind für konventionelle leittechnische Einrichtungen allgemein akzeptiert und werden als ausreichend betrachtet für den Nachweis der fehlerfreien Funktionsauslegung und einer ausreichenden Erkennbarkeit von Ausfällen im Betrieb.

Die skizzierten Nachweis- und Überwachungsmethoden sind (mit Ausnahme der Ausfalleffektanalyse) auf neue leittechnische Einrichtungen zwar uneingeschränkt anwendbar; sie können jedoch, insbesondere für mikroelektronische und speicherprogrammierte Geräte und Systeme, nicht als ausreichend gelten. Mit den nachfolgenden Betrachtungen läßt sich begründen, warum bisher ausreichende Qualifizierungsprüfungen bei neuen leittechnischen Einrichtungen nur eingeschränkte Aussagekraft besitzen.

Die Schaltung konventioneller leittechnischer Geräte besitzt sehr geringen Umfang und läßt sich vollständig auf die vorgesehenen Sollfunktionen der Geräte zurückführen. Eine vollständige Funktionsprüfung stellt damit eine weitgehend vollständige Prüfung der Schaltung dar. Hinzu kommt, daß konventionelle leittechnische Geräte überwiegend Schaltnetzeigenschaften aufweisen. Ein reines Schaltnetz enthält keine Speicherschaltungen, so daß sich alle Ausgangssignale unmittelbar aus den augenblicklichen Eingangssignalen ergeben und kein Einfluß früherer Signale existiert. Hierdurch ergibt sich ein relativ geringer Prüfumfang für einen vollständigen Funktionstest. Sofern konventionelle Geräte einzelne Speicherschaltungen enthalten, so ist dies darauf zurückzuführen, daß die Geräte-Sollfunktionen Speicherfunktionen einschließen. Auch in diesen Fällen stellt ein vollständiger Test der Geräte-Sollfunktionen einen weitgehend vollständigen Test der Schaltung dar.

Hieraus ergibt sich, daß eine vollständige Funktionsprüfung im Rahmen von Typ- oder Werksprüfungen bei konventionellen Geräten grundsätzlich zum Nachweis der Fehlerfreiheit ausreicht. Anhand der Ergebnisse von Ausfalleffektanalysen sind die möglichen Fehlfunktionen der eingesetzten Geräte bekannt, so daß sich die Wirksamkeit der für den kerntechnischen Einsatz vorgesehenen Überwachungsmaßnahmen und Prüfungen eindeutig beurteilen und die Notwendigkeit zusätzlicher Ausfallerkennungsmaßnahmen einfach feststellen läßt.

Völlig anders liegen die Verhältnisse beim Einsatz mikroprozessorgestützter Geräte. Der Nachweis der fehlerfreien Funktionsauslegung muß bei solchen Geräten die universell einsetzbare Hardware und die jeweilige Arbeitssoftware abdecken. Es versteht sich von selbst, daß mit einem Test der durch eine bestimmte Software festgelegten Anwenderfunktionen eines Gerätes ein vollständiger und universell gültiger Hardwaretest nicht realisierbar ist. Mikroprozessoren besitzen eine so hohe Schaltungsdichte und Komplexität, daß eine Prüfung der Fehlerfreiheit dieser Bauelemente nur während der Herstellung in großer Tiefe möglich ist (aber bereits hier nicht mehr vollständig). Für Prüfungen (zum Beispiel Wareneingangsprüfungen) bei anderen Unternehmen sind zwar umfangreiche Prüfautomaten verfügbar und auch im Einsatz; in der Regel ist dem Prüfer jedoch unbekannt, was und mit welcher Vollständigkeit der Automat prüft.

Auf einen universellen und vollständigen Hardware-Test könnte verzichtet werden, wenn sich Hardware und Software wenigstens im Hinblick auf die im Einzelfall vorgesehenen Geräte-Sollfunktionen vollständig testen ließen. Wegen der extrem ausgeprägten Schaltwerkseigenschaften der Mikroprozessoren besteht jedoch kein unmittelbarer und eindeutiger Zusammenhang zwischen augenblicklichen Eingangs- und Ausgangssignalen. Die Ausgangssignale sind vielmehr abhängig von prozessor- oder geräteintern gespeicherten Daten. Ein mikroprozessorgestütztes Gerät kann daher ein bestimmtes Ausgangssignal abgeben, obwohl sich die hierfür erforderlichen Eingangssignale längst wieder geändert haben. Wegen dieser immer anzunehmenden Abhängigkeit der Ausgangssignale von früheren Signalen läßt sich kein endlicher Prüfumfang für einen vollständigen Funktionstest rechnergestützter Geräte angeben.

Komplexität und Unzugänglichkeit mikroelektronischer Bauelemente machen eine Ausfalleffektanalyse unmöglich. Das mögliche Ausfallverhalten der neuen Leittechnik und die Wirksamkeit von Überwachungsmaßnahmen und Funktionsprüfungen lassen sich daher nicht detailliert vorhersagen.

Diese eingeschränkte Aussagefähigkeit von Funktionsprüfungen und Überwachungsmaßnahmen an mikroelektronischen, insbesondere mikroprozessorgestützten Geräten muß durch Anwendung zusätzlicher Nachweismethoden kompensiert werden. Hierbei können auch Methoden zum Nachweis der Fehlerfreiheit eingesetzt werden, die nicht unmittelbar auf Fehler- und Ausfallerkennung beruhen. Folgende Möglichkeiten stehen zum Beispiel zur Verfügung:

1. Zum Nachweis einer fehlerfreien bzw. fehlerarmen Auslegung und Herstellung:
   - Nachweis der Betriebsbewährung der eingesetzten mikroelektronischen Bauelemente,
   - Nachweis der Betriebsbewährung der eingesetzten Betriebs-Software (Compiler; Betriebssysteme),
   - Verifikation und Validierung der Anwendungs-Software,
   - deterministische und statistische Funktionsprüfungen,
   - bei Herstellern mikroelektronischer Bauelemente durchgeführte Qualitätsprüfungen,
   - Überprüfung der Qualitätssicherungssysteme von Bauelemente-, Geräte-, Software- und System-Hersteller.
2. Zur Tolerierung nicht vollständig auszuschließender Auslegungsfehler:
   - Hardware-Diversität,
   - Software-Diversität.
3. Zur Ausfallerkennung im kerntechnischen Einsatz:
   - Selbstprüfprogramme für CPU, ROM, RAM, I/O etc.,
   - Programmlaufüberwachung,
   - fehlererkennende Codes,
   - Ergebnisvergleich.

Alle genannten Methoden sind prinzipiell bekannt; zum Teil wurden sie bereits bei konventionellen leittechnischen Geräten angewandt. Im Hinblick auf mikroelektronische Einrichtungen ist jedoch keine der genannten Methoden für sich allein ausreichend zum Nachweis einer fehlerfreien Auslegung und Herstellung bzw. für eine vollständige Fehler- und Ausfallerkennung im Einsatz. So erschwert zum Beispiel die Komplexität und fehlende Zugänglichkeit der internen Strukturen von mikroelektronischen Bauelementen die Erstellung von Selbstprüfprogrammen und eine Überprüfung von deren Wirksamkeit.

Es ist daher erforderlich, stets eine Kombination mehrerer sich ergänzender und überlappender Maßnahmen zur Eliminierung oder Erkennung von Fehlern und Ausfällen einzusetzen. Mit Hilfe solcher geeigneter Kombinationen von Qualifizierungsmaßnahmen lassen

sich zuverlässige Aussagen über die Fehlerfreiheit der Auslegung und ein hohes Maß an Erkennbarkeit von Fehlern und Ausfällen im Einsatz erreichen. Durch eine Kombination mehrerer bekannter Qualifizierungsmaßnahmen können neue leittechnische Einrichtungen innerhalb bestimmter Grenzen von Komplexität und Umfang heute bereits qualifiziert werden.

Die einzelnen verfügbaren und auf neue leittechnische Einrichtungen anwendbaren Methoden sind jedoch derzeit nicht optimal aufeinander und auf kerntechnische Anforderungen abgestimmt. Dies führt dazu, daß sich wegen der begrenzten Wirksamkeit der Qualifizierungsmethoden ein relativ hoher Qualifizierungsaufwand und bei etwas umfangreicheren oder komplexeren Anwendungsfällen ein zu hohes verbleibendes Genehmigungsrisiko ergibt.

Notwendige Weiterentwicklungen und vorhandene Ansätze zur Verbesserung der Qualifizierbarkeit

Zur Verbesserung der Qualifizierbarkeit der neuen Leittechnik ist es erforderlich, in den kommenden Jahren folgende Probleme einer Lösung zuzuführen:

- Festlegung von auf die neue Leittechnik anwendbaren Auslegungsanforderungen, Qualifizierungsmaßstäben und Qualifizierungskriterien,
- Quantifizierung der Wirksamkeit einzelner Qualifizierungsmaßnahmen,
- Ermittlung optimaler Kombinationen von Qualifizierungsmaßnahmen,
- Festlegung von Kriterien für Prüfumfang und Prüftiefe,
- Erarbeitung von Regeln für die Erstellung leicht qualifizierbarer Hardware-Strukturen (ähnlich den in der Vergangenheit erstellten Programmierrichtlinien),
- Neu- oder Weiterentwicklung von Qualifizierungsmethoden und Qualifizierungswerkzeugen.

Es ist davon auszugehen, daß sich diese Probleme nicht unabhängig voneinander, sondern nur im Gesamtzusammenhang lösen lassen. So erscheint es nicht zweckmäßig, einzelne Qualifizierungsmethoden weiter oder gar neu zu entwickeln, ohne gleichzeitig die zu erfüllenden Auslegungsanforderungen und daraus abgeleitete Qualifizierungskriterien an die neue Leittechnik anzupassen. Umgekehrt sollten Qualifizierungsanforderungen nicht ohne Rücksicht auf vorhandene oder realisierbare Nachweismethoden formuliert werden.

Es ist zusätzlich zu berücksichtigen, daß sich mit der Einführung neuer Leittechnik Fragestellungen in Bereichen ergeben, denen bisher bei der Qualifizierung keine oder nur sehr untergeordnete Bedeutung zukam. So nimmt zum Beispiel die Qualifizierung elektronischer Bauelemente in bisherigen Genehmigungsverfahren eine ungleich geringere Bedeutung ein als die Qualifizierung von Geräten und Baugruppen. Bei mikroelektronischen Geräten ist eine erhebliche Verschiebung funktionsbestimmender Merkmale und Schaltungsstrukturen in die Bauelemente hinein zu verzeichnen. Es ist daher zum Beispiel zu prüfen, ob der Bauelementequalifikation zukünftig nicht wesentlich größere Bedeutung innerhalb von Genehmigungsverfahren zuzumessen ist.

An diesem Beispiel ist erkennbar, daß die Einführung der neuen Leittechnik nicht nur eine Anpassung von Qualifizierungsmethoden an einzelnen isolierten Stellen erforderlich macht (zum Beispiel verbesserte Methoden der Funktionsprüfungen an Geräten). Es ist vielmehr erforderlich, das bisher zugrundeliegende Gesamtkonzept von Auslegungs- und Qualifizierungsanforderungen auf seine Eignung für die neue Leittechnik zu prüfen und in die Anpassung an die neue Leittechnik einzubeziehen. Die nachvollziehbare Qualifizierung mikroelektronischer Einrichtungen ist prinzipiell schwieriger als die Qualifizierung konventioneller Leittechnik. Aus diesem Grunde ist es erforderlich, noch stärker als bisher zwischen notwendigen und entbehrlichen Anforderungen und Nachweisen zu unterscheiden. Nur durch Verzicht auf unnötige Anforderungen lassen sich die Ausle-

gungs- und Qualifizierungsmaßnahmen auf die tatsächlich wichtigen Sicherheitsfragen konzentrieren.

Die neue Leittechnik erfordert daher eine wesentlich stärkere Differenzierung von Auslegungs- und Qualifizierungsanforderungen in Abhängigkeit von der sicherheitstechnischen Bedeutung der gestellten leittechnischen Aufgabe. Erst mit der Schaffung eines neuen ganzheitlichen Systems aufeinander abgestimmter Auslegungs- und Qualifizierungsanforderungen und -maßnahmen wird ein Einsatz neuer leittechnischer Einrichtungen ohne unnötige Preisgabe von ihrer besonderen Leistungsfähigkeit und ohne Zwang zur Anwendung überzogener Anforderungen möglich sein.

Ansätze zur Schaffung solcher neuer Gesamtkonzepte existieren durchaus. Bereits in den Jahren 1978/79 erstellten die Firmen BBC, KWU, Siemens und GRS im Rahmen eines BMFT-Förderungsvorhabens ein „Rahmenpflichtenheft zur Leittechnik in Kernkraftwerken" [9]. In diesem Rahmenpflichtenheft wurden Rahmenbedingungen für die Entwicklung und die Qualifizierung mikroprozessorgestützter leittechnischer Einrichtungen von Kernkraftwerken zusammengestellt. In seinen konzeptionellen Aussagen ist das Rahmenpflichtenheft auch heute noch gültig. Ein damals neuer Ansatz bestand zum Beispiel darin, die Leittechnik sieben abgestuften Anforderungsklassen zuzuordnen (Tafel 1.) Jeder Anforderungsstufe wurden einige übergeordnete Ausiegungs- und Qualifizierungsanforderungen sowie eine Zuverlässigkeits-Zielgröße zugeordnet. Die Zahl von sieben Klassen wurde und wird allgemein als zu hoch empfunden. Auch die definierten Klassen sind zum Teil umstritten. Ansonsten gilt jedoch nach wie vor die dem Rahmenpflichtenheft zugrundeliegende Überlegung, daß ein umfangreicher und optimaler Einsatz mikroprozessorgestützter Einrichtungen für sicherheitstechnische Aufgaben nur auf der Basis einer differenzierten Bewertung der sicherheitstechnischen Bedeutung der einzelnen leittechnischen Einrichtungen möglich sein wird.

Als weiterer Ansatz in Richtung auf ein Gesamtkonzept für Auslegung und Qualifizierung neuer leittechnischer Einrichtungen ist das Ergebnis des ebenfalls vom BMFT außerhalb der Kerntechnik geförderten, von TÜV-Rheinland und TÜV-Bayern unter Mitarbeit der GRS durchgeführten und im Jahre 1984 abgeschlossenen Forschungs- und Entwicklungsvorhabens „Mikrocomputer in der Sicherheitstechnik" zu nennen. In dem als Handbuch bezeichneten Ergebnisbericht [10] zu diesem Vorhaben sind differenzierte Vorgaben für Auslegung und Qualifizierung von Mikrocomputern für sicherheitstechnische Aufgaben enthalten. Der konzeptionelle Rahmen dieser Vorgaben ist in Bild 8 dargestellt. Er beruht darauf, daß jede sicherheitstechnische Anwendung von Mikrocomputern einer von fünf Sicherheitsklassen zugeordnet werden soll. Die Sicherheitsklasse dient hierbei der Kennzeichnung eines bestimmten erforderlichen Sicherheitsniveaus. Jeder Sicherheitsklasse sind alternativ anwendbare Kombinationen verschiedener Auslegungs- und Qualifizierungsmaßnahmen zugeordnet. Mit Hilfe jedes einzelnen einer Sicherheitsklasse zugeordneten Maßnahmenbündels soll das durch die Sicherheitsklasse definierte Sicherheitsniveau erreicht werden können.

Das skizzierte Konzept hat leider noch einige Schwächen:

- Das Handbuch enthält keine Definition oder sinnvollen Zuordnungskriterien für die verwendeten fünf Sicherheitsklassen.
- Das Handbuch quantifiziert das einer Sicherheitsklasse entsprechende Sicherheitsniveau nicht.
- Die einzelnen Sicherheitsklassen zugeordneten verschiedenen Maßnahmenbündel sind häufig nicht gleichwertig.
- Die in Maßnahmenbündeln vorgesehenen (1-kanaligen und 2-kanaligen) Systemstrukturen decken nur einen Teil kerntechnischer Anforderungen ab.
- Das Handbuch schließt die Kerntechnik selbst aus seinem Anwendungsbereich aus.

Tafel 1: Anforderungsstufen des Rahmenpflichtenheftes zur Leittechnik ([8])

Anforderungsstufe	Richtwert der Unverfügbarkeit	funktionelle Anforderungen	Abgrenzung der Systeme	typische Merkmale	Beispiele Anwendung	Beispiele Einrichtung
I	$<10^{-5}$	Höchste Anforderungen der Reaktorsicherheit	Systeme, die zum Schutz gegen Gefährdung von Mensch und Umwelt automatisch Aktionen auslösen	Direkterfassung einfache Kriterien (keine Modelle) Eignungsprüfung (worst-case) redundant und diversitär oder höherwertig redundant hohe Sicherheit gegen Fehlauslösung	Große und mittlere KM-Verluststörfälle Speisewasser- und Frischdampfleitungsbrüche Anlagen-Teilzerstörung beherrschen	Schnellabschalt- und Teile des Abkühlsystems
II	10^{-4}	Hohe Anforderungen der Reaktorsicherheit	Systeme, die zum Schutz gegen Gefährdung von Mensch und Umwelt — überwachte Sicherheitsvariable im anormalen Betrieb automatisch entsprechend festgelegten Werten führen — Handeingriffe zwingend veranlassen	sichere Erfassung und Verarbeitung (evtl. Modelle) Eignungsprüfung (worst case) redundant diversitär oder höherwertig redundant	Schnellabkühlen Leistungsdichte begrenzen Abschaltreaktivität sichern Gebäudeabschluß	Schutzbegrenzung Sicherheitsverriegelung Sicherheitsgefahrmeldung Störfallfolgeinstrumentierung Strahlenschutz
III	10^{-3}	Normal Anforderungen der Reaktorsicherheit	Systeme — die Prozeßvariable auf Ausgangswerte begrenzen — die Abschaltungen vermeiden — die Störungen in Systemen der Stufe I bis III oder unzulässige Umgebungsbedingungen signalisieren	redundant (wenn erforderlich) nicht diversitär Eignungsprüfung (normal case)	Energieinhalte begrenzen DNB-Zustand sichern wichtige Prozeßvariable begrenzen Abschaltungen vermeiden	Zustandsbegrenzungen Reaktorsicherheitstechnische Informationen z.B. Gefahrmeldungen Klasse I Warten-Sichtgeräte Strahlenschutz Überwachungsrechner Störungsanalyserechner Rechnergestütztes Betriebshandbuch
IV	10^{-4}	Hohe Anforderungen der Anlagensicherheit	Systeme — die zum Schutz gegen Gefährdung von Menschen innerhalb der Kraftwerksanlage automatisch Aktionen auslösen — die dem Schutz wichtiger Anlagenteile und großer Aggregate dienen	redundant oder eventuell diversitär Funktionsprüfung (worst-case)	Groß-Aggregateschutz Groß-Komponentenschutz	Brandschutz Rohrbruchsicherung Turbinenschutz Generatorschutz
V	10^{-3}	Hohe Anforderungen der Anlagenverfügbarkeit und Lebensdauererhöhung	Systeme — die der Erhöhung der Anlagenverfügbarkeit dienen — die dem Schutz von Anlagenteilen und Aggregaten dienen	teilredundant Einzelfehler führt nicht zur Einschränkung Funktionsprüfung (normal case)	Unnötige Abschaltungen vermeiden Aggregateschutz, wenn Handeingriffe des Operators zu langsam Informations- und Aktionsmöglichkeiten bei wichtigen Anlagenteilen	Betriebsbegrenzung FD-Max-Druck-Regelung Umschaltfunktion für Speisepumpen Kondensatpumpenschutz Turbine: Freibetragsbildung Grenzdrehzahlregelung
VI	10^{-2}	Systemtechnische Ausführung mit hoher funktioneller Anforderung	Systeme, — die einem optimalen Betrieb der Anlagen dienen (Kriterien: Wirkungsgrad, Anlagenschonung, Manövrierbarkeit)	großes Funktionsspektrum große Flexibilität (bei Auslegung) Änderungsfreundlich (im Betrieb) Funktionsprüfung (normal case)	Betriebssysteme	Turbinenregeleinrichtungen Reaktorregeleinrichtungen Schutzverriegelungen / Aggregateschutz Funktionsgruppensteuerung Anlagenüberwachungssysteme Betriebsbegrenzungen Störablaufdokumentation Informations- und Aktionsmöglichkeiten
VII	10^{-2} bis 10^{-3}	komponentengebundene Leittechnik und / oder Einfachtechnik	Systeme — die einfachen Anforderungen genügen	Einfachausführung (black box) Umgebungsbedingungen entsprechend Einbauort .	Wasseraufbereitungsanlage	

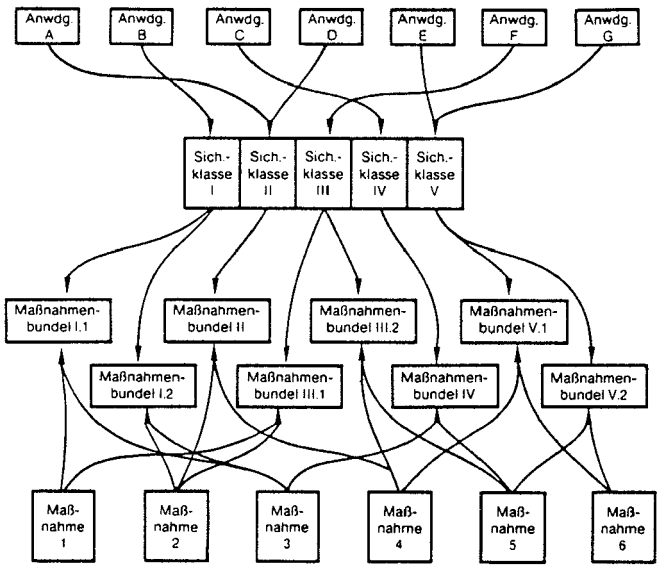


Bild 8: Zuordnung von Sicherheitsklassen und Maßnahmenbündel bei sicherheitsrelevantem Einsatz von Mikrocomputern ([10] und [11])

Die soeben skizzierten Ergebnisse von BMFT-Vorhaben zeigen, daß ein geeignetes Schema ausreichend abgestufter Sicherheitsklassen in der deutschen Kerntechnik derzeit noch fehlt. Selbst das in Kapitel „Leittechnische Aufgaben und Systeme im Kernkraftwerk" dargestellte System aus drei Sicherheitsklassen existiert nur außerhalb kerntechnischer Regeln. Als Konsequenz ist festzustellen, daß die kerntechnischen Regeln zu wenig nach der abgestuften sicherheitstechnischen Bedeutung verschiedener leittechnischer Einrichtungen differenzieren und damit an Systeme mit begrenzter sicherheitstechnischer Bedeutung zum Teil unnötig restriktive Anforderungen stellen. Ein derartiges Beispiel sind die Schutzbegrenzungen. Nach KTA 3501 darf bei diesen Systemen unter gewissen Voraussetzungen auf die Verwendung diversitärer Anregegrößen verzichtet werden. Ansonsten gelten jedoch exakt dieselben Auslegungs- und Qualifizierungsanforderungen wie für den „schwärzesten" Reaktorschutz. Wegen der de facto geringeren sicherheitstechnischen Bedeutung der Schutzbegrenzungen wären hier jedoch weniger restriktive Anforderungen gerechtfertigt (in der bisherigen Praxis kommen auch durchaus bereits stark abgestufte Anforderungen, zum Beispiel im Hinblick auf die zulässige Komplexität der Systeme, zur Anwendung).

Im folgenden soll versucht werden, Ansätze für eine differenziertere Betrachtung der sicherheitstechnischen Bedeutung leittechnischer Einrichtungen aufzuzeigen.

Generell gilt, daß die sicherheitstechnische Bedeutung einer technischen Einrichtung

- aus der sicherheitstechnischen Aufgabenstellung und
- aus den Konsequenzen des Fehlens oder Versagens der Einrichtung

abgeleitet werden kann.

Bild 9 zeigt ein System mit insgesamt sechs Sicherheits- bzw. Anforderungsstufen, das auf den genannten Kriterien aufbaut.

Es wird zunächst unterschieden zwischen Einrichtungen, deren Aufgaben ausschließlich während des bestimmungsgemäßen Betriebes von Bedeutung sind, und Einrichtungen, die

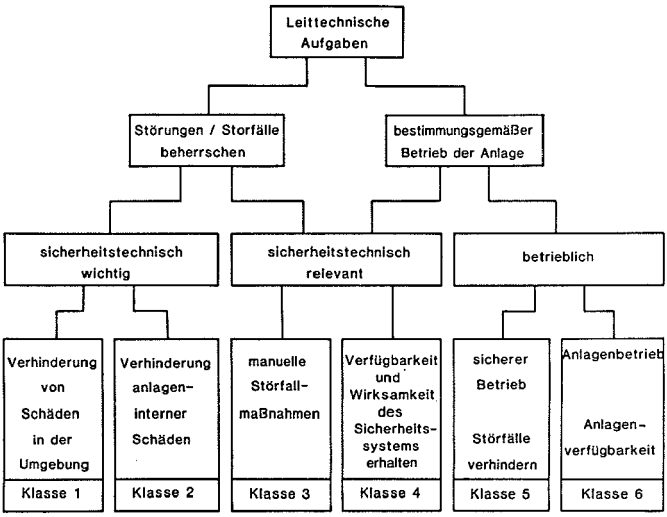


Bild 9: Vorschlag einer neuen zielorientierten sicherheitstechnischen Klassifizierung der Leittechnik

zur Störfallbeherrschung vorgesehen sind. Bei den zuerst genannten betrieblich benötigten Systemen können jene Einrichtungen in eine unterste Anforderungsstufe (Anforderungsstufe 6) eingeordnet werden, die keinerlei sicherheitstechnische Aufgaben zu erfüllen haben und deren Versagen aus sicherheitstechnischer Sicht keine Konsequenzen nach sich zieht. Die Leittechnik der Wasseraufbereitungsanlage ist ein Beispiel für solche Einrichtungen.

Die nächste Stufe (Anforderungsstufe 5) wird gebildet von betrieblichen Einrichtungen, denen zwar keine sicherheitstechnischen Aufgaben zugeordnet sind, bei deren Versagen jedoch aus sicherheitstechnischer Sicht in das Geschehen eingegriffen werden muß. Zum Beispiel sind die Einrichtungen zur Reaktorregelung, deren Versagen zu Reaktivitätsstörfällen führen kann, hier einzuordnen.

Die Anforderungsstufe 4 umfaßt jene Einrichtungen, die während des bestimmungsgemäßen Betriebes erforderlich sind, um die Einrichtungen des Sicherheitssystems ordnungsgemäß instandhalten zu können. Es sind dies zum Beispiel die leittechnischen Einrichtungen zur Überwachung und zu wiederkehrenden Prüfungen an Systemen der Anforderungsstufen 1 bis 3. Entscheidend für die Einstufung ist neben der sicherheitstechnischen Aufgabe im bestimmungsgemäßen Betrieb, daß beim Versagen einer solchen Einrichtung keine unmittelbaren sicherheitstechnischen Konsequenzen auftreten und ausreichend Zeit zur Ausfallerkennung und zur Reparatur existiert.

Die verbleibenden drei Anforderungsstufen umfassen Einrichtungen zur Beherrschung von schwerwiegenden Betriebsstörungen oder von Störfällen.

Zur Anforderungsstufe 1 zählen leittechnische Einrichtungen des Sicherheitssystems, die bei Störfällen in der Anlage automatisch Schutzaktionen auslösen müssen und bei deren Versagen Schäden für die Umgebung des Kernkraftwerkes unmittelbar unterstellt werden müssen. Hier ist der Teil des Reaktorschutzsystems einzustufen, der zum Beispiel bei Kühlmittelverluststörfällen oder plötzlichem Ausfall der Wärmeabfuhr die sofortige Reaktorabschaltung und Kernnotkühlung einleiten muß.

Zur Anforderungsstufe 2 zählen leittechnische Einrichtungen des Sicherheitssystems, die bei Störfällen oder schwerwiegenden Betriebsstörungen automatisch Schutzaktionen auslösen müssen, bei deren Versagen jedoch nur anlageninterne Schäden zu erwarten sind oder bei deren Versagen Schäden für die Umgebung des Kernkraftwerkes bei einer höheren, aber noch zulässigen Grenze durch Einrichtungen der Anforderungsstufe 1 verhindert werden. In die Anforderungsstufe 2 sind zum Beispiel Schutzbegrenzungen, aber auch Teile des Reaktorschutzsystems einzugruppieren.

Die verbleibende Anforderungsstufe 3 umfaßt jene leittechnischen Einrichtungen, die zur Auslösung manueller Maßnahmen zur Störfallbeherrschung erforderlich sind. Es sind dies zum Beispiel Einrichtungen der Störfallübersichtsanzeige sowie Bediensteuerstellen in Warte und Notsteuerstelle, die für Handmaßnahmen in der Mittel- und Langzeitphase von Störfällen erforderlich sind. Entscheidendes Einstufungskriterium ist neben der sicherheitstechnischen Aufgabenstellung bei und nach Störfällen, daß im Falle eines Versagens der Einrichtungen Zeit und Möglichkeiten für Reparatur oder Ersatzmaßnahmen zur Verfügung stehen.

Ein dem vorgestellten Konzept sehr ähnliches System von Anforderungsstufen für leittechnische Einrichtungen wird derzeit im VdTÜV-Facharbeitskreis „Leittechnik und Elektrotechnik" diskutiert. Das Konzept dieses Facharbeitskreises faßt die hier den Anforderungsstufen 3 und 4 zugeordneten Einrichtungen in einer einzigen Klasse zusammen, so daß insgesamt nur fünf Klassen definiert werden.

Als wichtigstes Merkmal aller genannten und die Kerntechnik betreffenden Klassifizierungssysteme erscheint die Tatsache, daß der bei drei Klassen gebildete Block „sicherheitstechnisch wichtiger Systeme" jeweils zweigeteilt wird. Dies erlaubt eine bessere Differenzierung der tatsächlichen sicherheitstechnischen Bedeutung der hierzu zählenden leittechnischen Einrichtungen und kann die für neue leittechnische Systeme erforderliche Definition angemessener Auslegungs- und Qualifizierungsanforderungen erheblich erleichtern.

Zusammenfassung

Neue leittechnische Einrichtungen können an vielen Stellen innerhalb eines Kernkraftwerkes zu einer weiteren Erhöhung der Sicherheit beitragen. Längerfristig wird ihr Einsatz sogar unumgänglich sein. Der Einsatz der neuen Leittechnik bedeutet jedoch derzeit einen Übergang von einer vertrauten zu einer weniger vertrauten und mit bisherigen Bewertungs- und Qualifizierungsmaßstäben zum Teil nur schwer erfaßbaren neuen Technologie.

Die Qualifizierung neuer leittechnischer Einrichtungen für sicherheitstechnische Aufgaben in Kernkraftwerken ist heute zwar innerhalb gewisser Grenzen und mit zum Teil großem Aufwand möglich. Ein wünschenswerter und zukünftig voraussichtlich umfassender oder gar ausschließlicher Einsatz neuer leittechnischer Einrichtungen erfordert jedoch noch eine wesentliche Verbesserung der Qualifizierbarkeit.

Für dieses Ziel sind grundsätzliche Untersuchungen und Entwicklungsarbeiten durchzuführen. Es ist ein Gesamtkonzept zu entwickeln, innerhalb dessen folgende Problemfelder zu bearbeiten und aufeinander abzustimmen sind:

- Auslegungsanforderungen,
- Qualifizierungsanforderungen,
- Qualifizierungsprozeduren,
- Qualifizierungsmethoden,
- Qualifizierungswerkzeuge.

Auf der Basis dieses Gesamtkonzepts kann in den kerntechnischen Regeln und Richtlinien eine Anpassung der Auslegungs- und Qualifizierungsanforderungen erfolgen, so daß den

Genehmigungsbehörden nachvollziehbare und einheitliche Beurteilungsmaßstäbe an die Hand gegeben werden können.

Eine Erledigung der oben genannten Aufgaben ist im Rahmen von einzelnen Genehmigungsverfahren nicht möglich. Nach unserer Meinung ist es erforderlich, die notwendigen Arbeiten parallel zur industriellen Entwicklung neuer Leittechnikkonzepte durchzuführen. Eine ausreichende Unabhängigkeit von der beteiligten Industrie ist dabei sicherzustellen. Die öffentliche Hand ist daher aufgerufen, durch Initiierung entsprechender Arbeiten die erforderlichen Rahmenbedingungen zu schaffen. Die notwendigen Arbeiten müssen baldmöglichst begonnen werden, damit neue leittechnische Einrichtungen

- in absehbarer Zeit,
- mit wirtschaftlich vertretbarem Aufwand,
- auf der Basis überschaubarer und anwendbarer Anforderungen,
- ohne Sicherheitsverlust, sondern möglichst mit Sicherheitsgewinn
- ohne unnötige Preisgabe besonderer Leistungsmerkmale,

für den Einsatz in Kernkraftwerken qualifiziert werden können.

Schrifttum

[1] Goßner, S.:Qualitätssicherung der Leittechnik von Kernkraftwerken (Statusbericht mit Verbesserungsvorschlägen für kerntechnische Regeln). Schriftenreihe Reaktorsicherheit und Strahlenschutz BMI-1985-078.
[2] Aleite, W.: Defense-in-Septh by Leittechnique Systems with Graded Intelligence. Proceedings of the International Symposium on Nuclear Power Plant Control and Instrumentation, Munich, Oct. 1982, IAEA-SM-265/14, Wien 1983.
[3] Teleperm M - Das Prozeßleitsystem. Siemens AG (A19100-E815-AZ-V1).
[4] New Technology in Nuclear Power Plant Instrumentation and Control NRC/EPRI-Symposium, Washington D.C., Nov. 28-30, 1984, ISBN: 0-87664-868-5, ISA 1985.
[5] Nuclear Power Plant Safety Control Technology. EPRI-Seminar, Palo Alto, Febr. 4-6, 1985.
[6] Power Plant Digital Control and Fault-Tolerant Microcomputers; EPRI-Seminar, Scottsdale Arizona, April 9-12, 1985.
[7] Computer Application for Nuclear Power Plant Operation and Control ANS/ENS Int. Topical Meeting 1985, Pasco, Washington Sept. 8-12, 1985.
[8] Dalle, H.: Functional Requirements leading to the Use of Digital Computing. Devices in the 1300 MWe Plant Protection System. IAEA Specialists' Meeting, "Use of Digital Computing Devices in Systems important to Safety" Saclay, Nov. 1984.
[9] Rahmenpflichtenheft zur Leittechnik in Kernkraftwerken. BMFT 1980.
[10] Hölscher, H. und J. Rader: Mikrocomputer in der Sicherheitstechnik. Verlag TÜV-Rheinland. ISBN-3-55585-180-6.
[11] Jansen, H.: Mikrorechner in sicherheitsrelevanten Anlagen. Vortrag bei der Tagung „Mikroelektronik" am 8.2.1984 in Düsseldorf.

Diskussion

W. Fischer (KKW Biblis):

Ohne mich gegen den technischen Fortschritt zu stellen, möchte ich als Betreiber der Leittechnik vor einer sogenannten Erhöhung der Leistungsfähigkeit warnen: sie kann – da sie die Möglichkeit bietet, mehr verfahrenstechnische Funktionen auf gleichem oder kleinerem Raum unterzubringen – zu einer unüberschaubaren Komplexität und Vernetzung der Einzelfunktionen führen. Die Schaltungen sind derzeit an der Grenze der Überschaubarkeit und sollten nicht weiter verkompliziert, vor allem aber nicht weiter vernetzt werden. Ausgenommen von diesem Einwand ist die Verbesserung der Informationsdarstellung in der Warte durch Bildschirmsysteme.

S. Goßner (GRS):

Herr Fischer, ich kann Ihre Ausführungen nur unterstützen. Wenn ich im Rahmen dieses Vortrages davon gesprochen habe, daß wir die Qualifizierung der neuen Leittechnik nur im Rahmen einer geeigneten Gesamtkonzeption schaffen werden, dann war damit natürlich gemeint, daß dieses Konzept auch über die Grenzen der Leittechnik hinausschaut. Es wird darauf zu achten sein, daß sicherheitstechnisch relevante leittechnische Einrichtungen nicht deshalb zusätzlich verkompliziert oder mit zusätzlicher sicherheitstechnischer Verantwortung belastet werden, weil zum Beispiel im Rahmen einer reinen Kostenminimierung verfahrenstechnische bzw. maschinenbauliche Systeme vereinfacht oder im Umfang reduziert und dafür mit entsprechend komplizierten Steuerungssystemen ausgestattet werden. Unter diesen Randbedingungen sehe ich keine prinzipiellen und unüberwindbaren Hindernisse für den Einsatz der neuen Leittechnik auch innerhalb eines Reaktorschutzsystems. Ich sehe dort einfachere Strukturen als in anderen Leittechnikbereichen.

W. Aleite (KWU):

Die von Herrn Fischer geäußerte und sicherlich berechtigte Furcht der Betreiber läßt sich mildern. Die Leittechnik ist zwar komplexer geworden und wird es noch mehr werden. Sie gestattet es nun aber auch, viele Dinge besser darzustellen. Die Technik, die wir heute noch einbauen, brauchen wir nicht zu verstecken, und auch in Zukunft nicht. Die im Vortrag nämlich als „alt" bezeichnete Anlage in Obrigheim hat eine bessere Leittechnik als die meisten – auch noch in Bau befindlichen – amerikanischen Anlagen sie aufweisen können, wenn auch dort – ebenfalls wie in Japan – die Entwicklungen inzwischen vorangetrieben werden. Die gestern von Herrn Innenminister Dr. Zimmermann geäußerte Meinung, daß die Auslegung der Reaktorsysteme uns weit vorausgeeilt sei und die Leittechnik nun langsam hinterherkommt, kann ich nicht teilen! Ich glaube, daß wir der Auslegung der maschinenbaulichen Systeme immer voraus waren. Viele Dinge, die die Systemtechniker erst bei der übernächsten Anlage überlegten, hatten wir vorher schon in die nächste eingebaut, weil wir bei Inbetriebnahmen schon früh die Probleme kommen sahen.

Durch den Einsatz einer Vielzahl von Rechnern – die Hardware wird ja immer billiger für solche Systeme – und die frühe gute Zusammenarbeit der Entwickler sind viele Ansätze zu Problemlösungen gegeben.

Daß Sie in Ihrem Vortrag einen Unterschied zwischen Schutzsystem und Schutzbegrenzung machen, stimmt nicht mit der KTA 3501 überein. Sie besagt ausdrücklich, daß Schutzbegrenzung und ein Teil der Funktionsgruppensteuerung Teil des Schutzsystems sind. Wir müssen aber immer wieder auf die Forderung nach Einfachheit zurückkommen. Die wesentlichen Prozesse müssen überschaubar gebaut werden. Dazu müssen wir – wie richtig gesagt wurde – die Gesamtheit des Systems sehen. Das, was wir an Komplexität von Funktionen einbauen müssen, muß durch die Art der Darstellung wieder einfach verständlich gemacht werden.

W. Bastl (GRS):

Der Reaktorschutz wird noch lange in der herkömmlichen Technik ausgeführt werden, er ist ja auch hinreichend gut. Auf der anderen Seite, wenn wir die Schutzbegrenzungen mit „mehr Intelligenz" ausstatten, das heißt mit Rechnern, werden sicherlich andere Beurteilungskriterien notwendig sein als für den konventionellen Reaktorschutz, weil wir die Regeln einfach nicht mehr anwenden können.

S. Goßner (GRS):

Herr Aleite, Ihren Worten ist nichts entgegenzuhalten. Erlauben Sie mir jedoch einige Worte zu Ihrem Vorwurf bezüglich der Differenzierung zwischen Reaktorschutzsystem und Schutzbegrenzungen in meinem Vortrag. Mir ist und war bewußt, daß ich mit meiner Terminologie gegen die Fassung 6/85 der KTA 3501 verstoße. Ich habe dies jedoch bewußt getan, um den aus meiner Sicht existierenden, zum Teil erheblichen Unterschied der sicherheitstechnischen Bedeutung von Schutzbegrenzungen einerseits und anderen Teilen des Reaktorschutzsystems andererseits charakterisieren zu können.

H. Nickel (KFA):

Eingangs Ihres Referates sprachen Sie von einer revolutionären Änderung der Leittechnik bei sämtlichen Kernkraftwerken. Welche Bedeutung hat diese Äußerung in bezug auf ein „backfitting" bei den sogenannten Altanlagen?

S. Goßner (GRS):

Herr Professor Nickel, ich glaube, so weitreichend wie Sie dies zitieren, war meine Prognose zum Einzug der neuen Leittechnik in unsere Kernkraftwerke nicht. Ich habe zwar gesagt, daß die konventionelle Leittechnik langsam vom Markt verschwinden wird, was hinsichtlich der Instandhaltung für existierende Anlagen Probleme mit sich bringt. Es kann langfristig – in etwa zehn Jahren oder mehr – auch dazu führen, daß in einer älteren Anlage die Leittechnik komplett ersetzt werden muß. Ich weiß jedoch nicht, ob das in meinem Vortrag genannte Kraftwerk Obrigheim ein Backfitting in dieser Richtung nötig haben wird.

A. Birkhofer (GRS):

Dazu kann ich als Betreiber eines kleinen Forschungsreaktors (SUR) an der Hochschule beitragen, daß das Problem für Forschungsreaktoren bereits existiert. Der Reaktor, der eine Siemens-Instrumentierung hat, liegt derzeit still, weil es unmöglich ist, Ersatzteile zu bekommen. Wir müßten eine ganz neue Leittechnik beschaffen, aber dazu fehlt uns das Geld. Der Reaktor ist etwa 1960 gebaut worden. Dieses Problem, das bisher nur für Forschungsreaktoren existiert, wird später auch bei Großanlagen auftreten, denn die Hersteller werden nicht mehr in der Lage sein, passende Ersatzteile zu liefern.

Zuverlässigkeit der Hard- und Software von Rechnern

Von M. Kersken und H. Schüller[1])

Kurzfassung

Heutige Rechner zeichnen sich durch ständig billiger werdende Hardware und flexible, für komplexere Überwachungs- und Steuerungsaufgaben geeignete Software aus. Die Komplexität erschwert allerdings den Zuverlässigkeits- und Sicherheitsnachweis. In der Praxis wurden durch Beachtung besonderer Erstellungsrichtlinien und intensiver Tests bereits Systeme von sehr beachtlicher Zuverlässigkeit entwickelt.

Für die Hardware wird der zentrale Einfluß der Fehlererkennung auf die Zuverlässigkeitskenngrößen dargelegt. Vor allem auf dem Gebiet der Fehlererkennung durch Selbstüberwachungsprogramme hat die GRS in der Vergangenheit erfolgreiche Lösungswege aufgezeigt. Für die Software wurden in praktischen Anwendungen auf Steuerstabfahrrechner, Schutzbegrenzungs- und Schutzrechner Softwareanalysemethoden erarbeitet und erprobt. Das von der GRS entwickelte automatische Analysewerkzeug für PEARL-Programme wird zur Anwendung auf Fortran- und Assemblerprogramme fortentwickelt. Damit wird dazu beigetragen, bestehende Lücken beim Softwaresicherheitsnachweis zu füllen.

Abstract

Trends within modern computing are marked by the steadily decreasing hardware costs and a flexible software which is suitable for complex monitoring and control purposes. Complexity on the other hand complicates the verification of safety and reliability. In practice systems of remarkable reliability have been established by using special rules (guidelines) within system design and by intensive testing.

Concerning hardware, the important influence of fault detection on reliability parameters is outlined in this contribution. Mainly in the area of fault detection via self-monitoring software GRS has demonstrated successful solutions already some time ago. Methods for analyzing software have been developed and applied to computer programs used in the areas of absorber rod control, protection and power limitation. The development of an analysis tool (for PEARL programs) and its extension towards FORTRAN and assembler programs contributes to closing the gaps still existing within verification of software.

Einleitung

In der modernen Leittechnik wird der Fortschritt im wesentlichen durch die rasante Entwicklung auf dem Gebiet der integrierten Schaltkreise geprägt. Die Anzahl der realisierbaren Transienten-(oder Gatter)-Funktionen pro Bauteil (Chip) ist mittlerweile auf einige Millionen angewachsen. Damit lassen sich (nahezu beliebig komplizierte logische Funktionen ausführen und zwar sowohl anwendungsabhängig – also kundenspezifisch – als auch anwendungsunabhängig, zum Beispiel als Mikrorechner. Ein 32-bit-Mikrorechner wie etwa die VAX II von DEC macht heute die Kapazität früherer sehr teurer Großrechenanlagen relativ billig für leittechnische Aufgaben verfügbar.

Der Vorteil der Verbilligung gilt allerdings nur für die Hardware. Die eigentlichen leittechnischen Funktionen werden über die Software realisiert. Diese hat gegenüber festverdrahteten Systemen den Vorteil, daß sie flexibel gehandhabt und an nahezu beliebig komplexe Überwachungs- und Steuerungsaufgaben angepaßt werden kann.

[1]) Dipl.-Ing. Manfred Kersken und Dr.rer.nat. Herbert Schüller, Gesellschaft für Reaktorsicherheit (GRS) mbH, Garching

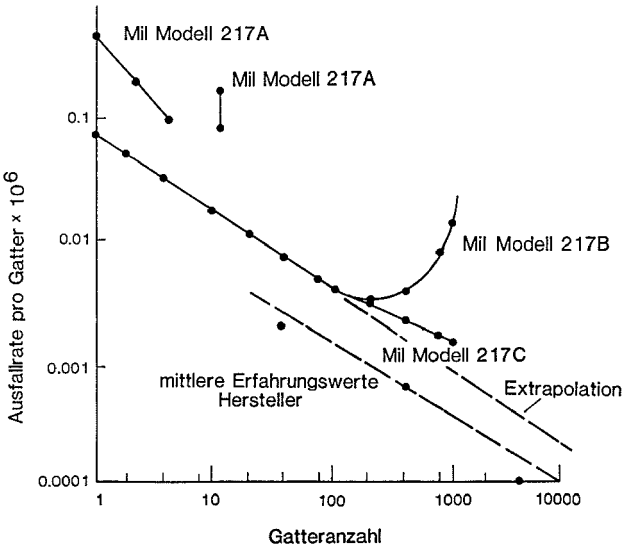


Bild 1: Ausfallrate (pro Gatter) für integrierte Schaltkreise. Voraussagen nach Modellen des MIl-Handbuches 217 sowie mittlere Erfahrungswerte von Herstellern [1]

Obwohl die Komplexität der Hard- und Software den für einige Anwendungsgebiete unverzichtbaren Nachweis der ausreichenden Sicherheit erschwert, werden auf lange Sicht diese neuen hoch integrierten frei programmierbaren Komponenten auch die Leittechnik von Kernkraftwerken erobern. Im folgenden soll vor diesem Hintergrund aufgezeigt werden, welchen Zuverlässigkeitsstand Rechnersysteme heute bereits erreichen können.

Zuverlässigkeit der Hardware

Ausfallraten

Bei Beobachtung der Ausfälle der Hardware stellt man fest, daß die Ausfallraten nach einiger Zeit (Frühausfälle) über viele Jahre konstant bleiben. Durch Rückmeldungen aus den meist gegebenen hohen ausgelieferten Stückzahlen sowie durch praktische Versuche bei erhöhter Temperatur und Rückschluß auf normale Betriebstemperaturen lassen sich die Ausfallraten bestimmen. Daneben wurden Modelle zur Prädiktion entwickelt, die allerdings ständig an die verbesserten Produktionsmethoden angepaßt werden müssen. Bild 1 zeigt die Entwicklung der Modelle gemäß MIL Handbuch 217 A-C. Bild 2 zeigt die Verringerung der Ausfallrate eines speziellen Mikroprozessors in Abhängigkeit des Herstellungsjahres.

Eine Gegenüberstellung der über MIL-Modelle ermittelten Ausfallraten gegenüber den in der Praxis verifizierten Werten für SSI (*S*mall *S*cale *I*ntegration) und MSI(*M*edium *S*cale Integration)-Schaltkreise zeigen Bild 3a und 3b. Man sieht, daß die berechneten Ausfallraten meist größer sind als die in der Praxis festgestellten. Dies liegt daran, daß die Verbesserungen der Produktionsmethoden stets mit Verspätung in den Modellen Aufnahme finden. Die Ausnahmen zeigen aber auch die möglichen Verschlechterungen durch „Montagsschichten" bei der Produktion. Bei einer Größenordnung der Ausfallrate von 10^{-6} pro Stunde erscheint eine Abweichung der Vorhersage um eine Zehnerpotenz, die außerdem zur sicheren Seite geht, tolerabel, das heißt die Modelle sind brauchbar.

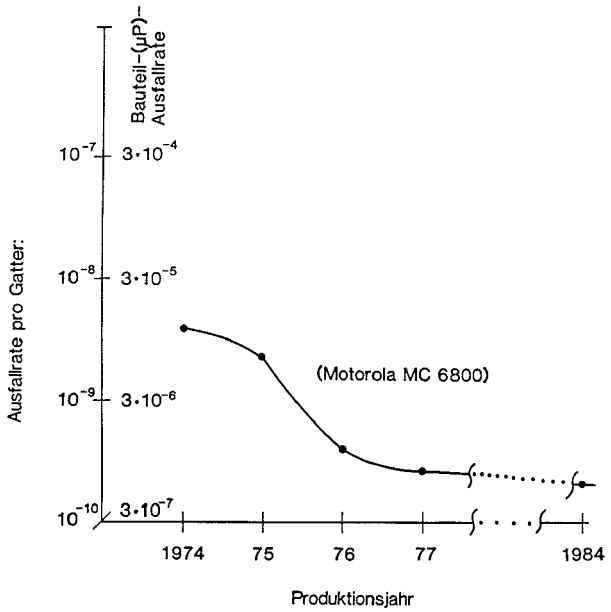


Bild 2: Ausfallrate eines Mikroprozessors in Abhängigkeit vom Produktionsjahr

Einfluß der Fehlererkennung auf Zuverlässigkeitskenngrößen

Die Komponentenausfallraten sind allerdings nicht die einzigen Kenngrößen, die für eine Zuverlässigkeits- bzw. Sicherheitsbewertung wichtig sind. Weitere Kenngrößen sind in Tafel 1 aufgelistet. Zwischen ihnen bestehen mathematische Beziehungen, die hier nicht näher erläutert werden. Sie können in allen gängigen Büchern über Zuverlässigkeitstheorie nachgelesen werden.

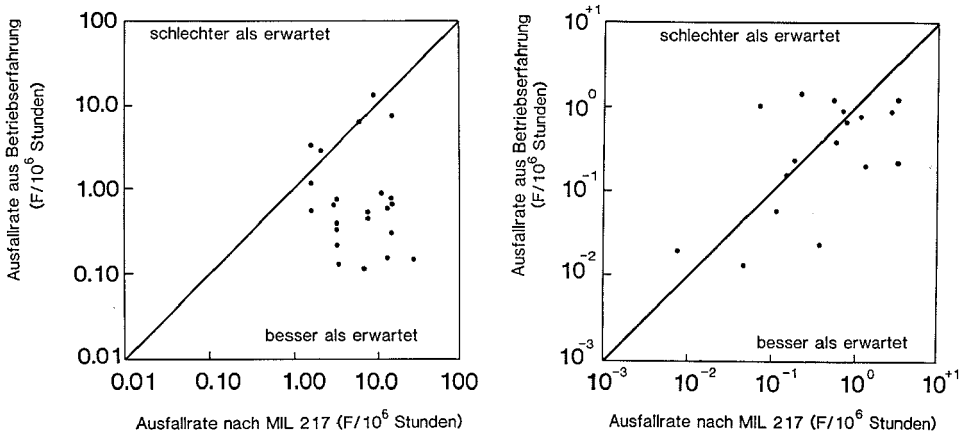


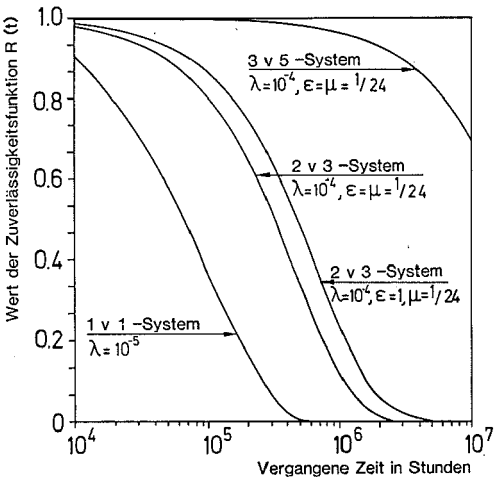
Bild 3: Gegenüberstellung von betrachteten Fehlerraten zu nach MIL 217 berechneten Fehlerraten [1]

Tafel 1: Beispiele für wichtige Kenngrößen zur Zuverlässigkeits- bzw. Sicherheitsbewertung

Ausfallrate
(Mittlere) Zeit bis zum ersten Ausfall
Mittlere Reparaturzeit
Mittlere Fehlererkennungszeit
Anteil nicht erkennbarer Fehler
Zuverlässigkeitsfunktion (System-Überlebenswahrscheinlichkeit)
Sicherheitsfunktion (Komplement der Wahrscheinlichkeit für gefährlichen Systemausfall)
Verfügbarkeit

In Bild 4 sind einige Berechnungsbeispiele dargestellt. Diese Beispiele machen deutlich, daß die Systemstruktur und die Reparatur bei redundanten Systemen einen besonders gewichtigen Einfluß auf die Zuverlässigkeitsfunktion haben. Da eine Reparatur eine Fehlererkennung voraussetzt, sind deren Geschwindigkeit und Vollständigkeit oft die bestimmenden, das heißt den Wert der Zuverlässigkeitsfunktion begrenzenden Einflußfaktoren. Bild 5 zeigt diesen Einfluß an einem Berechnungsbeispiel für ein 2v3-System.

Rechner haben den besonderen Vorteil, daß sie sich selbst prüfen können. Dies gilt sogar für die Zentraleinheit, wobei dann jedoch bei Einprozessorsystemen als Fehlerreaktion jeweils nur der Rechnerstillstand möglich ist. Solche Selbstüberwachungs- oder besser Fehlererkennungsprogramme können ohne spezielle Kenntnis der Hardware von Programmierern als Black-Box-Tests oder mit genauer Kenntnis der Hardware und damit bauteilspezifisch erstellt werden. Letztere können normalerweise eine wesentlich vollständigere Fehlerentdeckung gewährleisten als ein Black-Box-Test. Wenn es allerdings möglich ist, alle für die spezielle Anwendung benötigten Funktionen mit allen in der



λ = Ausfallrate des Einzelsystems
ε = Fehlererkennungsrate (Kehrwert der mittleren Fehlererkennungszeit)
μ = Reparaturrate (Kehrwert der mittleren Reparaturzeit)

Bild 4: Zeitlicher Verlauf der Zuverlässigkeitsfunktionen für spezielle Parameter [2].

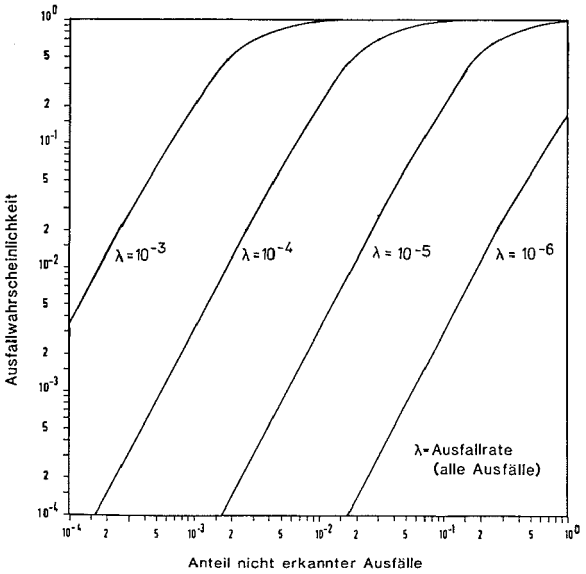


Bild 5: Ausfallwahrscheinlichkeit eines 2v3-Systems innerhalb der Kraftwerkslebensdauer (40 Jahre) durch unerkannte Fehler

Praxis vorkommenden Ein-/Ausgangswerten zu prüfen, werden auch von einem Black-Box-Test alle für die Anwendung relevanten Fehler erfaßt. Ein Beispiel dafür ist der Test eines A/D-Wandlers, bei dem der gesamte Wertebereich der Kennlinie mit kleinstmöglichem Increment durchfahren und jeweils das Ergebnis mit dem Sollwert verglichen wird. Ein solcher Test kann auch von einem Nicht-(Rechner-)Spezialisten im Rahmen der Begutachtung überprüft werden. Die Beurteilung der Wirksamkeit bauteilspezifisch erstellter Selbsttestprogramme erfordert dagegen genauso intime Kenntnisse der Hardwarestruktur wie sie zu deren Erstellung notwendig sind. Das macht eine Begutachtung natürlich teurer, wenn bei der Gutachterinstitution hier noch keine ausreichenden Erfahrungen vorliegen.

Praktische Erfahrungen mit Selbstüberwachungsprogrammen

Welche Qualität der Fehlererkennung ist in der Praxis mit der Methode der Selbstüberwachung von Rechnerzentraleinheiten überhaupt erreichbar? Da in der GRS für einen Prozeßrechner der 3. Generation (SSI bis MSI-Technik) ein solches Selbsttestprogramm erstellt und durch praktischen Fehlereinbau ausgetestet wurde, können wir daraus einige Zahlen ableiten, die auch für heutige Mini- und Mikrorechner Gültigkeit haben. Der Fehlereinbau erfolgte durch Festhalten der Gatterausgänge (Zugriffsmöglichkeit ist bei Rechnern der 3. Generation gegeben) auf 0 V bzw. +5 V, womit sogenannte Stuck-At-0- bzw. Stuck-At-1-Fehler simuliert wurden. Das Hardwaretestprogramm war in guter Kenntnis der Rechner-Hardwarestruktur erstellt worden (es ist, nebenbei bemerkt, bis heute in den Steuerstabfahrrechnern der Siedewasserreaktorlinie im Einsatz). Der allererste Test nach Fertigstellung des Selbstüberwachungsprogramms erbrachte einen Anteil von 99,5 % erkannter Fehler bei etwa 2000 für den Rechnerbetrieb relevanten Signalverfälschungen. Die nicht erkannten Fehler hatten — wie zu erwarten — nur in sehr spezifischen Situationen Auswirkungen, die zudem keine sicherheitstechnische Bedeutung gehabt hätten. Dennoch wurde das Selbstüberwachungsprogramm so ertüchtigt, daß auch

diese Fehler erkennbar wurden. Die Fehlererkennungszeit betrug für 97,5 % der Fehler weniger als 200 ms, für den Rest weniger als 1 min. Ein weiteres wichtiges Ergebnis des praktischen Tests, das allerdings noch besser abgesichert werden müßte, lautet: Das Vorhandensein eines nicht erkannten Erstfehlers hat auf die Erkennbarkeit eines weiteren hinzukommenden normalerweise keinen Einfluß.

Was bedeuten diese Zahlen in der Projektion auf den Einsatz in einem Kernkraftwerk? Wenn man ein 1v2- oder 2v3-System aus jeweils einzelnen Mikrorechnern mit einer Ausfallrate von 10^{-5} (h^{-1}) zugrundelegt sowie eine Fehlererkennung von 99 % erreicht hat, muß man innerhalb der Kraftwerkslebensdauer von 40 Jahren bei 1 von etwa 1000 eingesetzten Mikrorechnersystemen damit rechnen, daß in zwei Systemkomponenten gleichzeitig ein unerkannter Fehler vorliegt. Ohne Fehlererkennung wäre in jedem System im Mittel alle 9,5 Jahre ein solcher, ohne weitere Maßnahmen als gefährlich einzustufender Doppelfehler zu erwarten.

Ein großes offenes Problem liegt allerdings noch darin, diese probabilistischen Betrachtungsweisen in notwendige Regeln für eine deterministische Begutachtung umzusetzen.

Bedeutung systematischer Fehler

Nach diesen Ausführungen zum Einfluß von Ausfällen und deren Erkennung auf die Zuverlässigkeit soll nun die Frage der möglicherweise von Anfang an vorhandenen Auslegungs- und Herstellungsfehler beleuchtet werden. Gegen solche Fehler hilft bekanntlich der Einsatz von Redundanz auf Systemebene nicht weiter. Es steht außer Frage, daß bei Komponenten, die in großen Stückzahlen ausgeliefert werden, solche Fehler sehr selten vorkommen, da der Hersteller in diesen Fällen durch äußerst sorgfältige und zahlreiche Tests sein Markt-Akzeptanzrisiko zu minimieren versucht. Es hilft jedoch nicht weiter, wenn man versucht, die Möglichkeit, daß VLSI (*V*ery *L*arge *S*cale *I*ntegrated) und vor allem ULSI (*U*ltra *L*arge *S*cale *I*ntegrated) Schaltungen noch Auslegungsfehler haben können, wegzudiskutieren. Jeder Hersteller von solchen höchstintegrierten Schaltkreisen hat durch Kundenrückmeldungen aus den vielfältigen Anwendungen praktische Zahlen für diese Bausteine gesammelt. Zum Teil werden solche Fehler sogar in Fachzeitschriften veröffentlicht, so daß die Kunden ihre Anwendung gegebenenfalls vor diesen bekannten fehlerhaften Eigenschaften schützen können. Das ist normalerweise möglich, da diese Fehler naturgemäß nur für ganz spezielle Eingangszustände bzw. Eingangszustandsfolgen auftreten (nur so konnten sie den umfangreichen Prüfungen entgehen). Wenn diese bekannt sind, lassen sie sich meist in der Anwendung vermeiden.

Diese Tatsache läßt sich unter Umständen auch dazu verwenden, im Design eines sicherheitsrelevanten Systems zu verhindern, daß diese systematischen Bauteilfehler zu sogenannten Common-Mode-Fehlern werden. So ist es zweifellos unwahrscheinlich, daß sich ein solcher Fehler bei unterschiedlicher Software völlig gleichartig auswirkt. Damit wird er aber detektierbar. Um Common-Mode-Fehler quantifizierbar und mit von Anfang an überschaubarem angemessenem Aufwand allgemeingültig beurteilbar zu machen, sind allerdings noch detaillierte Untersuchungen anzustellen. Diese müssen sich auch auf die Erkennung bzw. Vermeidung von Herstellungsfehlern beziehen. Natürlich kann man der Problematik auch mit dem klassischen Mittel gegen Common-Mode-Fehler, nämlich dem Einsatz von Diversität zu Leibe rücken. Welches Vorgehen unter Einbeziehung der Kosten für den Sicherheitsnachweis am günstigsten ist, muß heute noch im Einzelfall entschieden werden, weil noch keine allgemeingültigen Untersuchungsergebnisse vorliegen.

Unabhängig von der schwierigen Nachweisbarkeit der Freiheit von Auslegungsfehlern von hochintegrierten Schaltkreisen kann festgestellt werden, daß es mit den heute angewendeten Entwurfs- und Testmethoden in der Praxis tatsächlich gelingt, Auslegungsfehler der Hardware vor der Großserienfertigung weitestgehend auszumerzen. Eine wesentliche Rolle spielt dabei, daß dem Entwickler zahlreiche rechnergestützte Entwurfshilfsmittel zur Verfügung stehen. Außerdem werden die Schaltfunktionen vor der eigentlichen

Fertigung komplett softwaremäßig simuliert und bereits in der Simulation ausgetestet. Alle diese Methoden sind zwangsläufig sehr teuer, was sich aber wegen der hohen Stückzahlen auf das einzelne Bauteil nicht zu stark auswirkt. Es müssen Methoden und Verfahren gefunden werden, dieses Entwicklerwissen und die Ergebnisse der Herstellertests für Sicherheitsnachweise verfügbar zu machen.

Damit ist indirekt auch der Beweis erbracht, daß Software ausreichend fehlerfrei erstellt werden kann. Das Hardwareprodukt, das aufgrund vorhergehender vollständiger Softwaresimulation gefertigt wurde, kann ja nur dann auslegungsfehlerarm geworden sein, wenn auch die Simulationssoftware nahezu fehlerfrei war.

Damit kommen wir zum Problem der Zuverlässigkeit der Software.

Softwaresicherheit

Allgemeines

Das Verhältnis des Kostenaufwands zwischen Hardware und Software eines Rechnersystems hat sich im Laufe der Jahre beträchtlich verschoben (Bild 6). Lag im Jahr 1955 der Software-Anteil noch unter 20 %, so erreichte er 1965 fast die 50-%-Marke und heute, im Jahr 1985, werden Größenordnungen von 80 bis 95 % genannt. Im Bild 6 ist die Voraussage für den Kostenanteil der Software etwa 90 % für 1985 und trifft somit sehr gut die heutigen Verhältnisse; das Bild selbst stammt aus einem Aufsatz, der im Jahr 1973 erschienen ist [3].

Eine typische Verteilung des Aufwands bei der Erstellung von Software aus einem veröffentlichten Beispiel zeigt Bild 7 [4].

Die Spezifikation, also die detaillierte Festlegung dessen, was die Software leisten soll, umfaßt etwa 12 % und Grob- und Feinentwurf machen zusammen etwa 34 % aus. Die Codierung, das heißt die Umsetzung in eine Programmiersprache, zusammen mit einer ersten Behebung von Fehlern ist mit 20 % angegeben, und die folgenden Testphasen mit etwa 34 %. Betrachtet man die Tests als die Maßnahmen, die am ehesten zur Steigerung der Softwarezuverlässigkeit dienen, so beträgt der anteilige Aufwand hier etwa 45 % bei einem kommerziellen Projekt. Für Software, die in sicherheitsrelevanten Bereichen, wie in

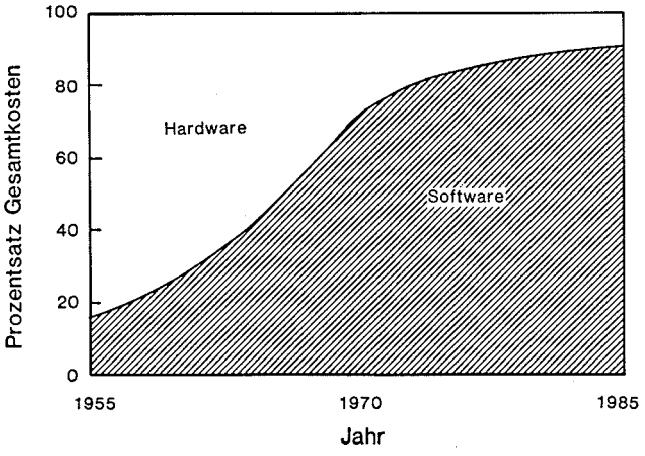


Bild 6: Aufteilung der Systemkosten (aus [3])

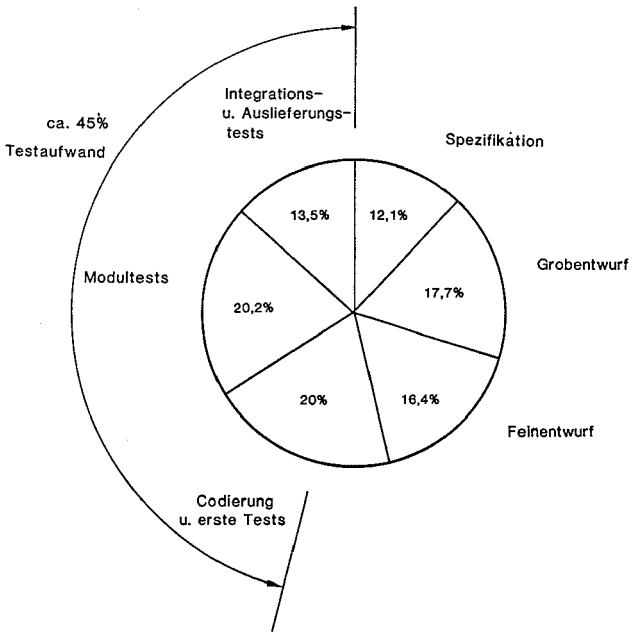


Bild 7: Verteilung des Aufwands zur Erstellung von Software

den Schutz- und Schutzbegrenzungssystemen von Kernkraftwerken eingesetzt werden soll, muß ein erheblich höherer Aufwand zur Gewährleistung ihrer Zuverlässigkeit aufgewendet werden. Insbesondere müssen auch während der Spezifikations- und Entwurfsphasen Maßnahmen zur Steigerung der Zuverlässigkeit ergriffen werden. Glücklicherweise wird diese Forderung durch eine weitere von ökonomischer Bedeutung gestützt: Fehler, die in frühen Stadien der Softwareentwicklung gemacht werden, sollen auch möglichst bald entdeckt werden, da ihre späte Beseitigung unverhältnismäßig hohe Kosten verursacht.

Ein typischer Software-Lebenszyklus ist in Bild 8 dargestellt. Er beginnt mit der Spezifikation, die aus den Systemanforderungen abgeleitet ist. Wie bereits erwähnt, ist hier festgelegt, was die Software leisten soll. Die Spezifikation kann in Form von natürlicher Sprache, Diagrammen, Entscheidungstabellen, u.a. vorliegen; es existieren auch formale Spezifikationssprachen.

Im Grob- und Feinentwurf wird in immer detaillierteren Stufen festgelegt, wie die Funktionen, die die Software ausführen soll, implementiert werden. Anschließend folgt die Codierungsphase, in der die letzte Stufe des Feinentwurfs in eine Programmiersprache umgesetzt wird. Diese Umsetzung kann ebenfalls mehrstufig erfolgen, indem zum Beispiel aus einer höheren – dem Programmierer gut verständlichen – Sprachebene mit einfach zu überprüfenden automatischen Hilfsmitteln (Codegenerator) in eine niedrigere Ebene, die der Rechner verarbeiten kann, übertragen wird.

Die Maßnahmen zur Steigerung der Softwarezuverlässigkeit lassen sich unterteilen in einen bezogen auf den Software Lebenszyklus

- vorwärtsgerichteten Anteil von konstruktiven Maßnahmen zur Vermeidung von Fehlern, und einen

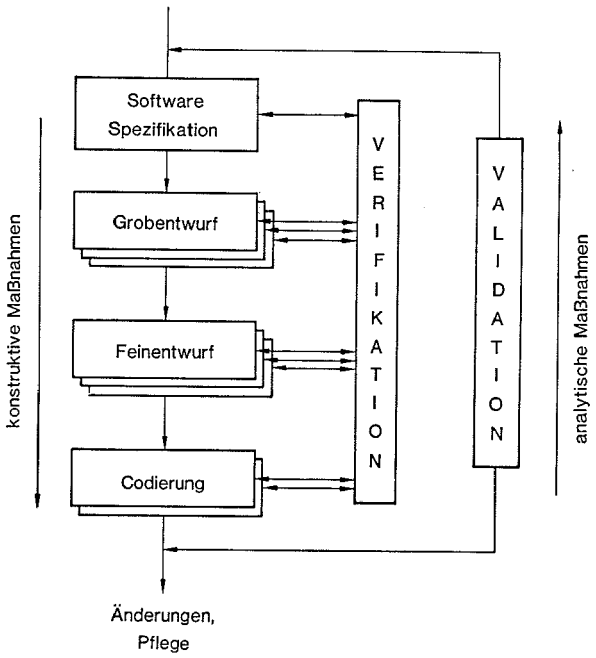


Bild 8: Software-Lebenszyklus

– rückwärtsgerichteten Anteil von analytischen Maßnahmen, der nach Abschluß der einzelnen Produktstadien zur Aufdeckung und Verbesserung von Fehlern und Schwachstellen und zum Nachweis der spezifikationsgerechten Funktionsweise des Produkts dient.

Die analytischen Maßnahmen werden mit Verifikation und Validation (V&V) bezeichnet. Dabei versteht man unter Verifikation die Überprüfung der richtigen und vollständigen Übertragung aller Funktionen von einer Ebene auf die nächste (Bild 8) und unter Validation die mehr umfassendere Prüfung, ob eine Systemlösung (hier das ablauffähige Programm) die Systemanforderungen (hier die Softwarespezifikation) erfüllt.

Konstruktive Maßnahmen zur Steigerung der Softwarezuverlässigkeit

Der gesamte Software-Lebenszyklus sollte lückenlos von konstruktiven Maßnahmen zur Steigerung der Softwarezuverlässigkeit begleitet sein. Diese Maßnahmen beginnen bereits auf Managementebene, wo die Zusammensetzung des Teams mit der eindeutigen Zuordnung von Aufgaben und Verantwortlichkeiten sowie die Methoden und Hilfsmittel (Hardware und Software) zur Herstellung des Endprodukts (ablauffähiges Programm) und seiner Zwischenstufen gemäß Bild 8 festgelegt werden.

Für den gesamten Softwareentwurf gilt, daß er von oben nach unten (Top-Down) erfolgen sollte, um Unverträglichkeiten zu vermeiden, die zwangsläufig entstehen, wenn ein System aus seinen Komponenten von unten nach oben (Bottom-Up) entwickelt wird. Der Detaillierungsgrad zwischen den aufeinander folgenden Entwurfsebenen sollte möglichst nicht zu groß sein, da die Wahrscheinlichkeit steigt, bei größeren Abstraktionssprüngen Fehler zu erzeugen. Jede der Entwurfsebenen sollte das Softwaresystem voll-

ständig – nur in unterschiedlicher Detaillierung – enthalten, um die im nächsten Kapitel beschriebenen V&V-Aktivitäten zu ermöglichen.

Auf der Codierungsebene spielt natürlich die Auswahl der Programmiersprache eine nicht zu vernachlässigende Rolle [5]. Sprachen, die für spezielle Anwendungsgebiete geschaffen wurden, helfen dem Programmierer Fehler zu vermeiden; andererseits sind solche Sprachen nicht weit verbreitet und ihre Verwendung stößt bei Gutachtern und Genehmigungsbehörden auf Skepsis, da die zugehörigen Übersetzer und sonstige Hilfsmittel durch ihre geringe Verbreitung und der daraus resultierenden geringen Anwenderreaktion auf Fehler nicht so stark in der Praxis ausgetestet sind, wie die entsprechenden Systeme der verbreiteten Programmiersprachen. Ein ähnliches Argument spielt bei der Entscheidung zwischen Assemblersprachen und höheren Programmiersprachen eine Rolle. Höhere Sprachen reduzieren durch ihre „Anwendernähe" die Fehlerwahrscheinlichkeit beim Programmieren, der Nachweis der Fehlerfreiheit der zugehörigen Übersetzer (Compiler) ist jedoch kaum möglich. Bei der Verwendung von Assemblersprachen werden durch die „Maschinennähe" der Sprache mehr Fehler beim Programmieren begangen, jedoch ist der Nachweis der richtigen Arbeitsweise ihrer Übersetzer leichter möglich. Für die in der Vergangenheit eingesetzten Prozeßrechner und für Mikrorechner sind häufig keine höheren Programmiersprachen vorhanden, so daß ohnehin nur die Assemblerprogrammierung angewendet wird. Für zeitkritische Echtzeitanwendungen, bei denen ein Rechnersystem innerhalb kurzer Zeit auf Signale, die zu beliebigen Zeitpunkten vom Kraftwerksprozeß kommen können, antworten muß, sind ebenfalls Assemblerprogramme, die schneller ablaufen können als Programme in höheren Sprachen, geeigneter. In beiden Fällen – Assembler und höhere Sprache – wird man für sicherheitsrelevante Anwendungen Einschränkungen im Sprachumfang, in der Verwendung bestimmter Befehle, in der Bezeichnung und Verwendung von Daten, in der Behandlung von Unterprogrammen und Prozeduren, u.a. machen. Einzelheiten hierzu finden sich in [6, 5].

Zur Unterstützung des gesamten Prozesses der Herstellung von Software gibt es rechnergestützte Hilfsmittel (Tools, Werkzeuge). Diese Werkzeuge automatisieren im Idealfall die Erzeugung einer Verfeinerungsstufe (Bild 8) aus der vorherigen, oder sie erzeugen zumindest eine Rahmenkonfiguration einer Verfeinerungsstufe, die der Softwareentwerfer noch ausfüllen muß. Diese Werkzeuge müssen natürlich nach mehr oder weniger formalisierten Verfahren arbeiten und erzwingen durch diese Arbeitsweise die Erfüllung von Forderungen an sicherheitsrelevante Software wie zum Beispiel Vollständigkeit der Systemfunktionen auf jeder Verfeinerungsebene, Konsistenz mit der vorhergehenden Ebene, Dokumentation jeder Verfeinerungsebene, u.a. Desgleichen vermindert sie durch die (weitgehende) Automatisierung des Vorgangs die Wahrscheinlichkeit des Fehlermachens bei der Übertragung der Systemfunktion von einer Ebene auf die nächste – vorausgesetzt sie arbeiten selbst korrekt. Leider gibt es noch kein Bündel von Werkzeugen, das eine Software-Produktionsumgebung der Art schafft, daß alle Stufen der Softwareerstellung von der Spezifikation bis zum ablauffähigen Code gleichmäßig gut unterstützt werden [7], [8], [9]. Hier wird jedoch für die Zukunft ein beträchtliches Potential zur effizienten Verbesserung der Softwarezuverlässigkeit erwartet.

Analytische Maßnahmen zur Steigerung der Softwarezuverlässigkeit

Da durch konstruktive Maßnahmen allein die Erstellung fehlerfreier Software nicht gewährleistet und insbesondere nicht nachgewiesen werden kann, muß der Software-Lebenszyklus ebenfalls ständig von analytischen Maßnahmen zur Erkennung und Beseitigung von Fehlern und Schwachstellen begleitet sein. Hier wird unterschieden zwischen statischen und dynamischen Analysen, wobei unter letzteren im wesentlichen Programmtests verstanden werden, die zu ihrer Ausführung ein ablauffähiges codiertes Programm benötigen; erstere können von allen möglichen Programmaufschreibungen (zum Beispiel Quellcode, Pseudocode, Speicherabzug) ausgehen.

Schreibtischprüfungen (Desk Checks) sind Verfahren, bei denen mittels vorgegebener Prüflisten von Hand überprüft wird, ob vorgegebene Kriterien in der jeweils vorliegenden Programmaufschreibung erfüllt sind. Die Prüflisten sind auf die jeweils dokumentierte Phase des Lebenszyklus abgestimmt [10].

Revisionstreffen (Reviews, Inspections) sind Zusammenkünfte eines vor Projektbeginn festgelegten Kreises von bestimmten am Projekt beteiligten und eventuell auch externen Personen. Reviews finden am Ende vorher definierter Projektphasen statt und laufen nach einem vorgegebenen Schema ab (Structured Walkthrough). Revisionstreffen haben sich als sehr geeignete Methode zur Aufdeckung von Fehlern vor allem in frühen Stadien des Software Lebenszyklus erwiesen.

Die erwähnten Methoden der Schreibtischprüfung und Revisionstreffen gehören zu den statischen Analysen. Von diesen sind jedoch diejenigen am weitesten verbreitet, die vom codierten Programm ausgehen. Der Zweck dieser statischen Analysen ist es, Kenntnisse über interne Struktur und Zusammenhänge im Programm zu gewinnen, dadurch Fehler aufzudecken und gleichzeitig Vorbereitung für die folgende dynamische Analyse zu sein. Dazu wird die Kontrollflußstruktur eines Programms ermittelt, das heißt alle möglichen Sequenzen von Anweisungen, die aufgrund der im Programm enthaltenen Verzweigungs- und Sprungbefehle ausgeführt werden.

Eine Sequenz von Anweisungen, die vom Programmanfang zum Ende führt, ist ein Pfad. Die Datenbewegungen, die nun aufgrund des Durchlaufens eines Pfades ausgeführt werden, bilden eine Teilfunktion des Programms. Könnte man alle Pfade eines Programms und alle Datenbewegungen, die entlang dieser Pfade stattfinden, ermitteln, so wäre das Programmverhalten vollständig bekannt. Leider ist schon die Zahl der möglichen Pfade durch ein Programm ebenso wie die Zahl der möglichen Datenbewegungen in der Praxis quasi unendlich. Mit dieser Methode können deshalb nur sehr kleine Programme, die zudem sehr einfach aufgebaut sein müssen, vollständig analysiert werden. Im allgemeinen liegt der Wert der statischen Analyse in ihrer Vorbereitungsfunktion für folgende Tests.

Die GRS hat bezogen auf die Programmiersprache PEARL in der Vergangenheit ein leistungsfähiges Analyseprogramm erstellt [11]. Es wird derzeit für andere Anwendungen angepaßt. Eine dieser Anpassungen betrifft Assemblersprachen, da die bisher in der Leittechnik von Kernkraftwerken eingesetzten Rechner zu einem großen Teil in Assemblersprache programmiert sind. In Zusammenarbeit mit dem TÜV-Norddeutschland und dem Institutt for Energiteknikk in Norwegen wird das von der GRS entwickelte Analyseprogramm in ein System eingebunden, das es erlaubt, Assemblerprogramme einer automatischen statischen Analyse zu unterziehen. An einer Erweiterung des Analysators zur Bearbeitung von FORTRAN-Programmen wird ebenfalls gearbeitet.

Bisher erfolgte die statische Analyse von Assemblerprogrammen manuell mit einem speziell für sicherheitsrelevante Anwendungen bei der GRS entwickelten Verfahren [12], das aus einer grafischen Umsetzung des Assemblercodes den Kontroll- und Datenfluß ermittelt, und die Angabe von Testfällen für spätere dynamische Analysen ermöglicht. Dieses Verfahren wurde bisher u.a. für die Programmanalyse der Schutzrechner der Kraftwerke Brunsbüttel und Philippsburg, der Schutzbegrenzungsrechner in Grafenrheinfeld [13] und der Steuerstabfahrrechner für KWU Siedewasserreaktoren [14] angewandt.

Die dynamischen Analysen oder Tests lassen sich grob in Funktions- und Strukturtests unterteilen. Funktionstests werden weitgehend ohne Kenntnisse der Programmstruktur ausgeführt. Es wird die – möglichst vollständige – Summe der Teilfunktionen getestet, die ein Programm ausführen soll. Die Eingabedaten, die dazu dem Programm angeboten werden müssen,und die Ausgabedaten, die bei korrekter Funktion vom Programm geliefert werden müssen, werden aus der Spezifikation ermittelt. Strukturtests bauen auf einer vorangegangenen statischen Analyse auf. Kriterien für solche Tests sind zum Beispiel

- alle Befehle müssen mindestens einmal ausgeführt werden (sogenannte C1-Überdeckung),
- alle Äste von Verzweigungen müssen mindestens einmal durchlaufen werden (sogenannte C1-Überdeckung),
- alle Pfade müssen mindestens einmal durchlaufen werden.

Das letztgenannte Kriterium ist in der Praxis ohne Aufteilung in Teilpfade kaum erfüllbar, da die Anzahl der Pfade sehr groß sein kann.

Es gibt noch weitere Teststrategien (symbolische Exekution, Mutationstest, Feldgrenzentests), über deren Anwendung von Fall zu Fall, abhängig von den Aufgaben, die ein Programm zu lösen hat, entschieden werden muß. Die von der GRS in der Vergangenheit durchgeführten Tests von Schutzrechnerprogrammen unter Einsatz eines Hybridrechners umfaßten etwa 450 000 Testfälle. Sie erbrachten ausnahmslos die erwünschte sicherheitstechnisch richtige Reaktion der Schutzrechner. Zusammen mit der ebenfalls inzwischen abgeschlossenen Auswertung einer mehrjährigen Einsatzerfahrung [15] kann daher heute behauptet werden, daß einer Genehmigung der Schutzrechner keine unüberwindlichen Hindernisse entgegengestanden hätten.

Bezüglich der Programme der Schutzbegrenzungsrechner wurden Testfälle für einen Modultest ermittel, die aus der schon erwähnten manuellen statischen Analyse der Module gewonnen wurden und die Module vollständig testen. In einer Definitions- und Durchführbarkeitsstudie für eine Lichtwellenleiter-Übertragungsstrecke, die Mikrorechner enthält, wurden ebenfalls spezielle Testfälle hinsichtlich ausreichender Aufdeckung aller möglichen Programmeigenschaften untersucht.

Fehlertoleranz

Ausgehend von der Tatsache, daß in Softwaresystemen trotz großem konstruktiven und analytischen Aufwand weiterhin Fehler enthalten sein können, sind Methoden entwickelt worden, die es erlauben, unentdeckt gebliebene Fehler im Betrieb zu tolerieren.

Eine der Systemlösungen hier ist der Recovery Block [16], wie er in Bild 9 dargestellt ist. Nachdem der Hauptmodul gerechnet hat, werden seine Ergebnisse einem Akzeptanztest unterworfen, nach dessen Bestehen der normale Rechenablauf weitergeführt wird; bei

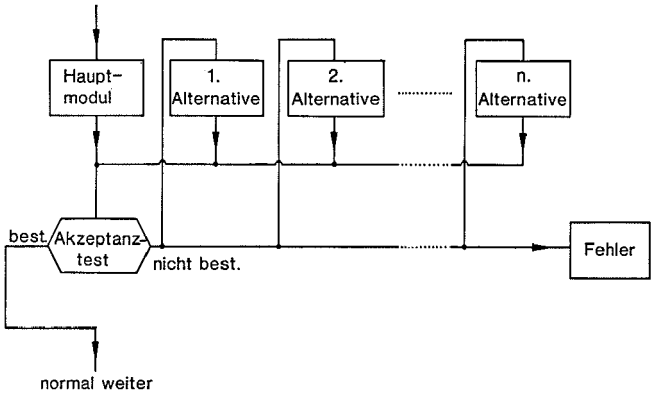


Bild 9: Recovery Block

nicht bestandenem Akzeptanztest wird die erste Alternative aktiviert, die die gleiche Aufgabe auf grundsätzlich andere Weise als der Hauptmodul löst (diversitäre Programmierung), usw. Sind alle Alternativen ohne Bestehen des Tests abgelaufen, so wird eine Fehlermeldung (oder eine Reaktion zur sicheren Seite) initiiert.

Andere im Prinzip nur wenig unterschiedliche Lösungen sind das N-Version Programming [17] und der Consensus Recovery Block [18], auf die hier nicht weiter eingegangen werden soll.

Softwarezuverlässigkeitsmodelle

All die erwähnten Maßnahmen zur Steigerung der Softwarezuverlässigkeit lassen per se noch keinen Schluß auf meßbare und quantifizierbare Kenngrößen zu, ausgenommen unter Umständen die Tests, wo man mit sehr großen Testanzahlen Versagensraten angeben kann.

Eine Methode zur Ermittlung von Kenngrößen zur Softwarezuverlässigkeit, deren theoretische Entwicklung Ende der sechziger Jahre begann und in den letzten Jahren zu einigen Anwendungen geführt hat, ist in der Modellierung des Vorgangs des Fehleraufdeckens und -korrigierens begründet. Zur Beschreibung der Methode soll ein sehr frühes, einfaches und in seinen Ergebnissen entsprechend ungenaues Modell [19] dienen.

Während des Testvorgangs werden zu bestimmten Zeiten Ausfälle des Programms beobachtet, die aufgrund von Fehlern in der Software auftreten. Diese Zeiten werden registriert und aus der Verteilung der Ausfallzeiten wird auf Kenngrößen geschlossen, wie zum Beispiel Anzahl der unerkannt verbliebenen Fehler nach Beendigung des Tests, mittleres Zeitintervall bis zum nächsten Ausfall, u.a.

Im Modell wird angenommen, daß

– die Ausfallrate zu jeder Zeit proportional zum jeweiligen Fehlergehalt des Programms ist (Proportionalitätsfaktor ϕ),

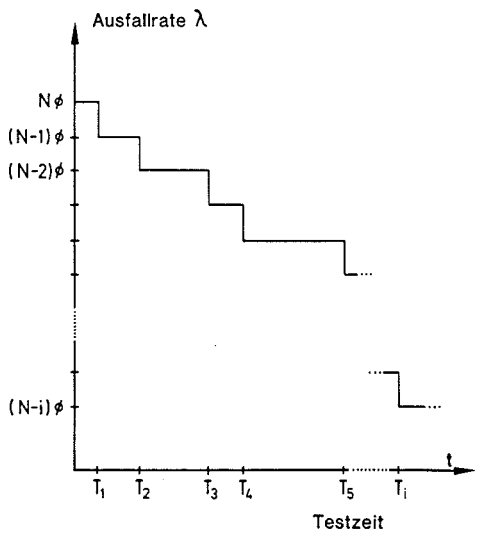


Bild 10: Ausfallratenverlauf für das Software-Zuverlässigkeitsmodell nach [19]

– zu jedem Zeitpunkt eines Ausfalls der Fehler (in unendlich kurzer Zeit) korrigiert und dabei kein neuer Fehler erzeugt wird.

Mit diesen Annahmen erhält man die in Bild 10 dargestellte Treppenfunktion für die Ausfallrate, in der die Stufenhöhe immer gleich ist und durch ϕ bestimmt wird. Die Schwächen des Modells sind schon in den beiden Annahmen erkennbar:

– In realen Programmen werden die Fehler mit sehr unterschiedlichem Gewicht zur Ausfallrate beitragen. Fehler in häufig durchlaufenen Programmteilen werden früher entdeckt, als solche in selten durchlaufenen.

– Die Korrekturzeit ist nicht unendlich kurz.

– Bei der Korrektur von Fehlern werden häufig neue eingeführt.

Neue Modelle sind in ihren Annahmen weniger restriktiv und liefern genauere Kenngrößen. Es kann jedoch allgemein gesagt werden, daß die Genauigkeit der Schätzwerte, die von den Modellen geliefert wird, derzeit noch nicht ausreicht, um Zuverlässigkeitskenngrößen für sicherheitsrelevante Programme zu ermitteln.

Schlußbetrachtung

Rechner werden heute bereits in Kernkraftwerken in größerer Zahl jeweils für spezielle Aufgaben eingesetzt. Dies wird in Zukunft verstärkt der Fall sein und es werden zunehmend sicherheitstechnisch relevante Anwendungen zum Zuge kommen. Die Rechner werden auf diesem Weg mitverantwortlich für die Vermeidung bzw. Minderung von Risiken bei Ausfällen von Komponenten und bei Störfällen. Damit müssen sie natürlich mindestens genauso sicher gemacht werden wie die bisher dafür eingesetzten Systeme. Beim Sicherheitsnachweis für Systeme mit Rechnern ist es allerdings nicht in gleicher Weise wie bei festverdrahteten Systemen möglich, rein deterministisch vorzugehen. Die in den vorhergehenden Kapiteln angewandten probabilistischen Betrachtungsweisen zeigen einen möglichen Ersatz. In diesem Zusammenhang ist es zweckmäßig, Sicherheitsklassen zu bilden. Dabei kommt es sowohl auf die Eintrittswahrscheinlichkeit des in seinen Auswirkungen zu beherrschenden unerwünschten Ereignisses an, als auch auf die zu erwartende Schadenshöhe, falls dies mißlingt.

Auch für Sicherheitssysteme stehen keine unbegrenzten Finanzmittel zur Verfügung. Wenn diese Mittel verantwortungsbewußt eingesetzt werden sollen, müssen sie optimal eingesetzt werden. Dann muß man aber die Fälle, bei denen möglicherweise Menschenleben direkt gefährdet werden können, noch zuverlässiger verhindern als solche, bei denen es zum Beispiel nur zu hohen Sachschäden kommen kann. Und es müssen Fälle mit gleichen möglichen Auswirkungen, die eine größere Eintrittswahrscheinlichkeit haben, auch mit größerer Wahrscheinlichkeit beherrscht werden als solche, mit deren Auftreten deutlich weniger zu rechnen ist.

Hier kommt auch den betrieblichen Belangen eine große Bedeutung zu. Es bringt oft den gleichen Sicherheitsgewinn, wenn eine betriebliche Verbesserung dazu führt, daß Schutz- oder Begrenzungssysteme seltener eingreifen müssen, wie der weitere, oft nur mehr mit großem Aufwand durchführbare Ausbau von zusätzlichen Sicherheitsmaßnahmen. Von besonderer Wichtigkeit ist es daher, daß für eine bundeseinheitliche Bewertung ein geschlossenes Qualifizierungskonzept entwickelt wird. Die GRS wird sich in den nächsten Jahren verstärkt diesen Problemen widmen.

Schrifttum

[1] Siewiorek, D., and R. Swarz: The Theory and Practice of Reliable System Design. Digital Press 1982.
[2] Schüller, H.: Methoden zum Erreichen und zum Nachweis der nötigen Hardwarezuverlässigkeit beim Einsatz von Prozeßrechnern. Dissertation, Technische Universität München, 1978.
[3] Boehm, B.W.: Software and its Impact: A Quantitative Assessment. Datamation, Mai 1973, pp. 48 - 59 .
[4] Wolverton, R.W.: The Cost of Developing Large-Scale Software. TRW Report, 1975.
[5] Ehrenberger, W.: Softwarezuverlässigkeit und Programmiersprache. Regelungstechnische Praxis, 25. Jg., 1983, Heft 1, S. 25 - 29.
[6] Ehrenberger, W., and J.R. Taylor: Recommendations for the Design and Construction of Safety Related User Programs. Regelungstechnik, Heft 2, 1977.
[7] Hausen, H.-L.; M. Müllerburg und H.M. Sneed: Software-Produktionsumgebungen. Verlagsgesellschaft Rudolf Müller, Köln, 1985.
[8] Baur, P., and R. Lauber: Design Verification for (Safety-Related) Software Systems. Proc. of the IFAC Workshop on Safety of Computer Control Systems. SAFECOMP 85, Como, Italy, Oct. 1985, pp. 31 - 37.
[9] Biewald, J.; P Göhner, R. Lauber and H. Schelling: EPOS-A Specification and Design Technique for Computer Controlled Real-Time Automation Systems. Proc. of the 4th Int. Conf. on Software Engineering, München, Sept. 1979, pp. 245 - 250.
[10] Wilburn, N.P.: Guidelines-Software Verification. Hanford Engineering Development Laboratory HEDL-TC-2425, Aug. 1983.
[11] Puhr-Westerheide, P.: Die statische Analyse von PEARL-Moduln mit dem PEARL-Analysator. PEARL-Rundschau, Heft 6, Band 2, Dezember 1981.
[12] Ehrenberger, W.: Manuelle Analyse von Programmen. PDV-Berichte KfK-PDV 179, Kernforschungszentrum Karlsruhe, Dezember 1979.
[13] Kersken, M.; L. Rietzsch and U. Mertens: Qualification of a Computer System for the Limitation of Power Density in a Reactor Core. Proc. IEEE Computer Software & Application Conference, COMPSAC 84, Chicago, Nov. 1984.
[14] Ehrenberger, W.; G. Glöe, J. Märtz, F.-U. Mainka, O. Nordland, G. Rauch und U. Schmeil: Sicherheitsanalyse der Programme der Steuerstabfahrrechner, Abschlußbericht BMI-Vorhaben SR 293, Dezember 1984.
[15] Zott, H.; H. Schüller, F. Kießler und H. Ueberall: Auswertung der Reaktorschutzrechner-Einsatzerfahrung in den Kernkraftwerken Brunsbüttel und Philippsburg, GRS-A-917, 1984.
[16] Horning, J.J.; H.C. Lauer, P.M. Melliar-Smith and B. Randell: Structure for Error Detection and Recovery. Proc. Conf. on Operating Systems, IRIA, April 1974, pp. 172 - 187.
[17] Avizienis, A.; and L. Chen: On the Implementation of N-Version Programming for Software Fault-Tolerance During Program Execution. Proc. COMPSAC 1977, pp. 149 - 155.
[18] Scott, R.K.; J.W. Gault, D.F. McAllister and J. Wiggs: Experimental Validation of Six Fault-Tolerant Software Reliability Models. 14th Int. Conf. on Fault-Tolerant Computing, Digest of Papers, 1984.
[19] Moranda, P.B.; and Z. Jelinski: Software Reliability Predictions. McDonell Douglas Astronautics Company, MDAC Paper WD 2482, Aug. 1975.

Diskussion

W. Aleite (KWU):

Wir müssen vermeiden, Furcht vor diesen neuen Systemen zu verbreiten. Wir werden versuchen, sie durch Struktur und Einsatz möglichst universeller Geräte überschaubar zu halten. Durch den Einsatz diversitärer Systeme müssen wir ja nicht mehr wie bisher auf Unverfügbarkeiten im Anforderungsfall in der Größenordnung von 10^{-6} zielen, sondern auf $10^{-3} \cdot 10^{-3}$ oder $10^{-2} \cdot 10^{-4}$ oder zum Beispiel $10^{-2} \cdot 10^{-2} \cdot 10^{-2}$. Die Anwendung der neuen Technik wird auch keine Rechnerspezialisten erfordern. Mit den neuen Systemen können dagegen Werte wesentlich besser sortiert und punktuell ausgewertet werden. Jedes notwendige Signal können wir berechnen, das heißt wir müssen nicht mehr soviel messen. Daß dies wieder geprüft werden muß, ist Sache der Validierung. Wir können somit „analytische Redundanz" schaffen.

Die neue Technik wird an die bestehende anschließen. Wir werden viele Funktionen, die es jetzt schon im Kraftwerk gibt, 1:1 übersetzen. Es werden aber die Stellen neu aufgegriffen werden, bei denen die neuen Möglichkeiten deutliche Vorteile bringen.

Ich bin nicht damit einverstanden, wenn gesagt wird, daß Rechner im Schutzsystem nicht verwendet werden können. Das klassische Schutzsystem wird soweit abgemagert werden, daß wir nur dort, wo ja in Deutschland diversitäre Anregekanäle gefordert werden, gerätetechnisch einfach bleiben wollen. Im verbleibenden größeren Bereich können wir dann mit der neuen Technik „intelligenter" und früher wirken.

Diese Techniken sind zwar sehr kompliziert, jedoch kann man schon während des Herstellungsprozesses immer wieder verifizieren, wodurch bereits viele Fehler vermieden werden. Daß man die Werkzeuge (Tools), um die Software zu behandeln, diesmal schon vor Erstellung der Hardware in Hand hat, ist ein bis dahin noch nie dagewesener Vorgang. Insofern sollten wir alles tun, um die Furcht vor solchen Systemen abzubauen.

W. Bastl (GRS):

Es war nicht unsere Absicht, Furcht zu verbreiten. Es sollte lediglich aufgezeigt werden, daß in diesen neuen Technologien ein Umdenken in Hinsicht auf Qualifizierungsmethoden und -maßnahmen notwendig sein wird und die bisherigen Methoden und Maßnahmen anzupassen sind.

H. Schüller (GRS):

Natürlich ist der Nachweis für ein System, dessen Ausfallwahrscheinlichkeit in der Größenordnung von 10^{-6} $[h^{-1}]$ liegt, ohne Einsatz von Diversität schwer zu führen. Die Verwirklichung der Diversität ist jedoch nicht nur im klassischen Schutzsystem, sondern auch innerhalb der gesamten Leittechnik möglich, das heißt, eine betriebliche oder zumindest eine Schutz-Begrenzungseinrichtung ist, wenn sie entsprechend aufgebaut ist, durchaus als Diversität zu werten.

Leitsysteme für den Airbus — Aufbau und Betriebserfahrung

Von P. H. Heldt[1])

Kurzfassung

Das Cockpit eines modernen Verkehrsflugzeuges ist eine Leitwarte besonderer Art. Sie bewegt sich fast mit Schallgeschwindigkeit, bei Tag und Nacht, bei jedem Wetter, durch Zeit- und Klimazonen. Sie ist eng, die Möglichkeit zur Unterbringung von Bedien- und Anzeigeelementen ist begrenzt. Sie läßt sich im Fluge nicht reparieren. Eine Schnellabschaltung des Gesamtsystems in der Luft hätte katastrophale Folgen. In einem Verkehrsflugzeug gibt es jedoch eine Reihe von Leitsystemen, deren Bedeutung und Interaktionen für Betreiber bodengebundener Anlagen interessant sein können. Zum Verständnis der heute üblichen Cockpitauslegungen sollen einige Grundregeln der Gestaltung genannt werden. Einige wichtige Leitsysteme werden vorgestellt. Soweit möglich, wird auf die inzwischen gemachten Betriebserfahrungen eingegangen. Das Gesamtsystem Cockpit kann nur richtig verstanden werden, wenn die Besatzung als integraler Bestandteil gesehen wird; daher ist sie in diese Betrachtung einzubeziehen. In einem Flugzeugcockpit haben die Piloten zwei unterschiedliche Aufgabenstellungen. Sie müssen fliegen und sie müssen sich in ihrer Leitwarte mit der Technik des Flugzeuges auseinandersetzen. Es soll nicht nur gezeigt werden, wie der Mensch in die Gesamtkonzeption der Cockpit-Auslegung einbezogen wird, sondern auch welche Fähigkeiten die Piloten für ihre Aufgaben mitbringen müssen.

Abstract

The cockpit of a modern passenger plane represents a special kind of control room, as it moves along with almost the speed of sound, night and day, under any weather situation, through various time and climatic zones. Due to its narrowness, it leaves only limited space for placing control and display elements. There is no chance of repair in flight. Moreover, a scram of the total system up in the air would lead to catastrophic consequences. In a passenger plane, however, there is a series of control systems, the importance and interactions of which could be of interest to the operators of grounded installations, too. For the understanding of actual cockpit layouts, a couple of basic principles for the design work shall be disclosed. A variety of important control systems is described. As far as possible, the operational experience with them is considered. The system "Cockpit" as such can only be understood if the crew is perceived as an integrated constituent of it; therefore, it is to be included into this consideration. In the cockpit of a plane, the pilots are confronted with two different tasks. On one hand, they have to fly the plane, on the other, they are required to deal with the plane's technology within their "control room". It shall be demonstrated not only, how to integrate the human being into the total conception of the cockpit design, but even which sort of capabilities the pilots are expected to offer with regard to mastering their tasks.

Entwurfsgrundsätze

Die Auslegung der Cockpits moderner Verkehrsflugzeuge (Bild 1) folgt international anerkannten Grundregeln (Bild 2). Sie sind in Bauvorschriften für Hersteller und Betreiber festgelegt. Darüber hinaus gehen in jeden neuen Entwurf, neben technischen Neuerungen, die ständig wachsenden Erfahrungen der Hersteller und nicht zuletzt der Luftverkehrsgesell-

---

[1]) Flugkapitän Peter H. Heldt, Technischer Pilot bei der Deutschen Lufthansa AG.

Bild 1: Airbus A 310

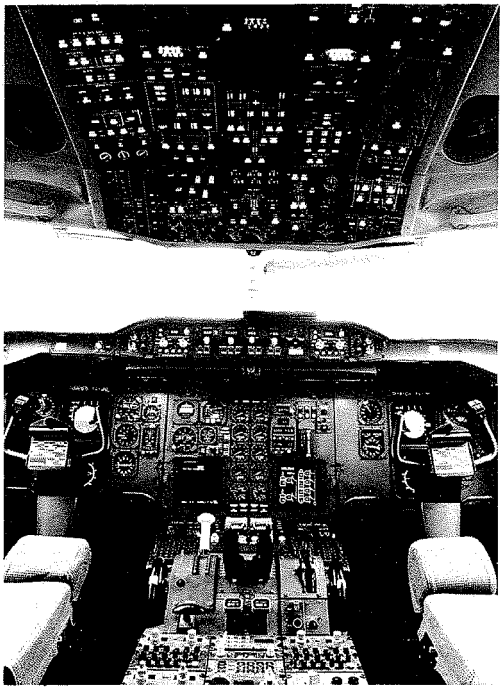


Bild 2: Cockpit im A 310

schaften ein. Für den Arbeitsplatz Cockpit hat die Lufthansa besondere Regeln aufgestellt:

- Redundanz der Flugbesatzung:
  Das Flugzeug muß auch bei Ausfall eines Besatzungsmitgliedes durch den (oder die) Verbleibenden voll beherrschbar sein. Deshalb müssen alle für die sichere Durchführung des Fluges wichtigen Bedienelemente und Anzeigen für mindestens zwei Besatzungsmitglieder erreichbar bzw. einsehbar sein.
- Redundanz der Systemelemente:
  Alle wichtigen Systemelemente, die nicht mit an Sicherheit grenzender Wahrscheinlichkeit ausfallsicher sind, müssen mindestens zweifach vorhanden sein. Bei Ausfall eines Elementes kann dessen Funktion durch das entsprechende zweite voll wahrgenommen werden.
- Kein unmittelbares Eingreifen durch die Flugbesatzung beim Auftreten des ersten Fehlers:
  Beim Auftreten des ersten technischen Fehlers darf kein sofortiges Eingreifen durch die Besatzung notwendig werden. Vielmehr muß ein korrigierendes Handeln in bestimmten Zeitgrenzen verschiebbar oder sogar gänzlich überflüssig gemacht werden, damit dem Flugzeugführer Dispositionsfreiheit innerhalb des Handlungsablaufes bleibt.
- Transparenz der technischen Systeme:
  Bei aller Automation, die zur Erfüllung dieser Ziele erforderlich ist, muß es dem Flugzeugführer mit Hilfe geeigneter Anzeige- und Warneinrichtungen in jeder Situation ohne großen Aufwand möglich sein, sich ein umfassendes Bild vom technischen Zustand des Flugzeuges zu verschaffen.
- Die Technik muß dem Menschen angepaßt werden, nicht umgekehrt:
  Sie muß insbesondere gegenüber Fehlbedienungen tolerant sein, Bedienungsfehler dürfen nicht sofort gravierende nachteilige Folgen haben.

Das Cockpit der A 310

Architektur

Das Cockpit der A 310 (Bild 3) hat die heute übliche Architektur. Es gibt keinen seitlichen Arbeitsplatz mehr. In der Mitte hinter den beiden Sitzen der Piloten ist ein Sitz für den gelegentlich mitfliegenden Ausbilder oder Prüfer vorgesehen.

Das vordere Hauptinstrumentenbrett, Overhead Panel, Konsole und Glareshield (ein als Blendschutz dienendes Armaturenbrett über den Hauptinstrumenten) folgen den Anordnungskriterien: einsehbar und erreichbar.

Gut einsehbar sind die Hauptinstrumentenbretter links und rechts. Sie sind nahezu identisch bestückt und erlauben, die Maschine von jeder Seite zu fliegen. Gut erreichbar ist das Overhead Panel. Sowohl gut einsehbar als auch gut erreichbar ist das Glareshield. Hinter dieser Architektur verbirgt sich ein weiteres wichtiges Kriterium: "Head down Monitoring". Nachdem es gelungen ist, das seitliche Instrumentenbrett zur Bedienung der Systeme vollständig in das Overhead Panel zu integrieren, soll sich daraus nicht ein Zwang zum ständigen Überwachen des Overhead Panels ergeben. Die Systeme sollen auf dem Hauptinstrumentenbrett überwacht werden.

Die Anordnung der Instrumente in den genannten drei Anzeigebereichen ist im einzelnen in Bild 3 beschrieben.

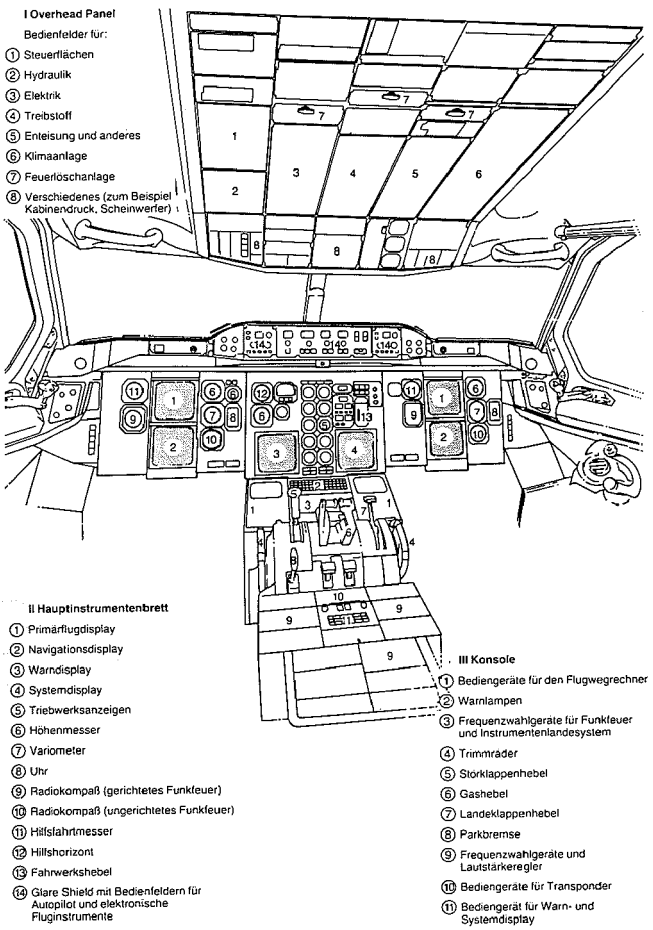


Bild 3: Bedienelemente im Cockpit des Airbus

Leitsysteme

Die Leitsysteme lassen sich zwei Aufgaben zuordnen. Zweifach ist auch die Aufgabe des Flugzeugführers: Fliegen und dabei die Technik des Flugzeuges überwachen und im Griff behalten.

Zur Flugführung gehören:

FCC Flight Control Computer
Automatisches Flugregelungssystem (Autopilot)

ATS Auto Thrust System
Automatischer Vortriebsregler

IRS Inertial Reference System
Trägheits-Navigationsgerät ("Laser-Kreisel") zur Bestimmung der geographischen Position

Bild 4: Autopilot und Vortriebsregler

FMS Flight Management System
Flugwegrechner

EFIS Electronic Flight Instrument System
Elektronisches Fluginstrumentensystem

Der technischen Überwachung dient:

ECAM Electronic Centralised Aircraft Monitor
Zentrales elektronisches Informations- und Überwachungssystem.

Flugführung

Autopilot und Vortriebsregler

Autopilot und Vortriebsregler bilden ein integriertes System (Bild 4). In der Grundbetriebsart Control Wheel Steering (CWS) wird das Flugzeug wie beim manuellen Flug über die Steuersäule geflogen, jedoch unterstützt der Autopilot die Eingaben nach der Art der Servolenkung eines Autos. Zur Lösung taktischer Aufgaben werden dem Autopiloten über das Bediengerät im Glareshield Daten wie Fahrt/Machzahl (Speed/Mach), barometrische Höhe (Altitude), Kompaßkurs (Heading) und auch Vertikalgeschwindigkeit (Vertical Speed) vorgegeben. Zusammen mit dem Vortriebsregler sorgt der Autopilot dann dafür, daß das Flugzeug das so vorgegebene Flugprofil exakt nachfliegt. Außerdem kann der Flugwegrechner direkt mit dem Autopiloten kommunizieren und ihm Vorgaben für das Abfliegen eines optimalen strategischen Flugpfades machen.

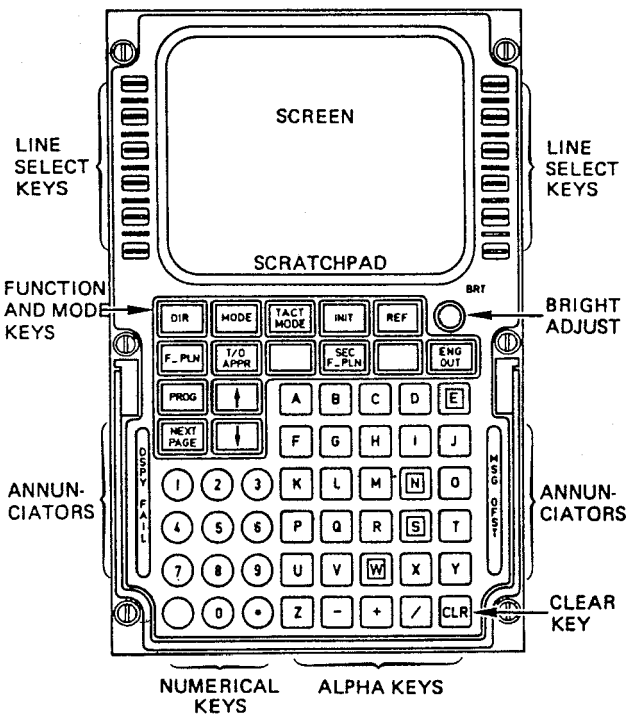


Bild 5: Der Flugwegrechner (FMS)

Flugwegrechner

Der Flugwegrechner (FMS) ist der aufwendigste Rechner an Bord (Bild 5). Er ist zweifach vorhanden, wie übrigens der Autopilot auch. Sein Speicher faßt 385 000 Worte zu je 16 bit. Er ist in der Lage, 700 000 Rechenoperationen pro Sekunde durchzuführen. Im FMS sind nicht nur die Flugleistungsdaten der A 310 gespeichert, sondern auch der Karteninhalt für das gesamte Einsatzgebiet (Europa, Nordafrika, Naher Osten). Dazu gehören alle Informationen über Flughäfen, An- und Abflugverfahren, Luftstraßen, Wegpunkte, Radionavigationshilfen und vieles mehr. Insgesamt sind es über 1 600 Einzelposten, von denen sich jeden Tag einige ändern. Sie werden alle 28 Tage revidiert und zum Stichtag eingelesen.

Trägheitsnavigation

Um auch navigieren zu können, muß der Flugwegrechner erst einmal selbst wissen, wo er ist. Seine Informationen holt er sich vom Laser-Kreisel, einem Trägheitsnavigationsgerät. Die von diesem Gerät errechnete Position kann innerhalb der Empfangsreichweite von Radionavigationsanlagen noch zusätzlich korrigiert werden. Der Flugwegrechner weiß in jeder Gegend, welche Stationen dazu am besten geeignet sind. Er rastet die entsprechenden Frequenzen automatisch.

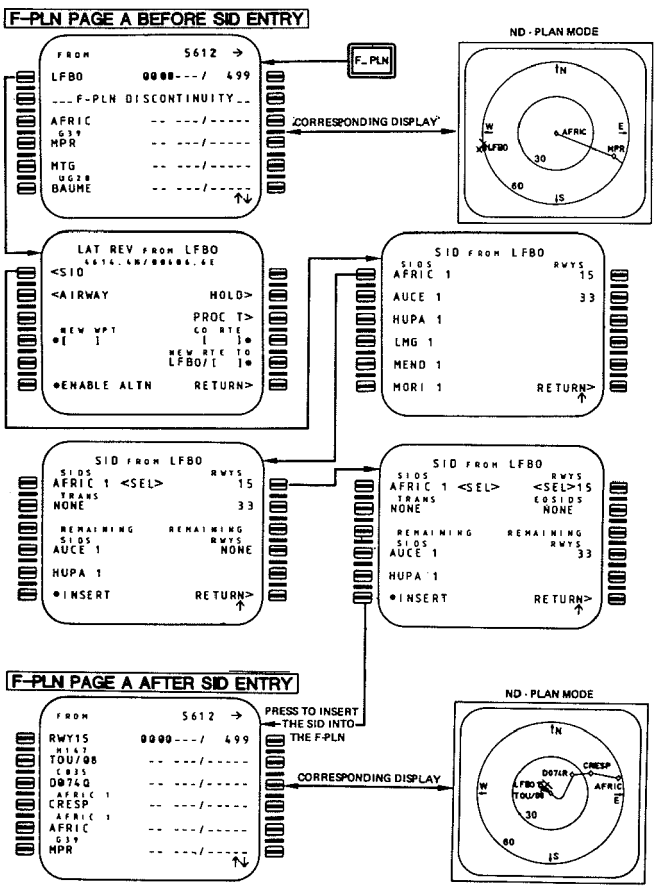


Bild 6: Streckenflugplandetail auf dem FMS

Benutzerführung

Die Tastatur des Flight Management Computers (FMS) hat mit seinen Verwandten, die man auf Schreibtischen findet, wenig Ähnlichkeiten; seine vorbildliche Benutzerführung noch weniger. Am Eingabebeispiel eines Streckenflugplanes kann man den Bedienungskomfort erkennen, der durch Menüführung in Verbindung mit den Zeilenwahlschaltern möglich wird. Der Rest ist einer guten Software-Gestaltung zu verdanken (Bild 6).

Lagebild

Das umfangreiche Informationsangebot des Flugwegrechners wird zu einem Lagebild verarbeitet und auf dem farbigen Navigationsdisplay graphisch dargestellt. Das Navigationsdisplay ist das untere der beiden übereinanderliegenden Bildröhren auf den Hauptinstrumentenbrettern. Das Bild dieser Anzeigegeräte ist gestochen scharf und flimmerfrei (Bild 7).

Redundanz

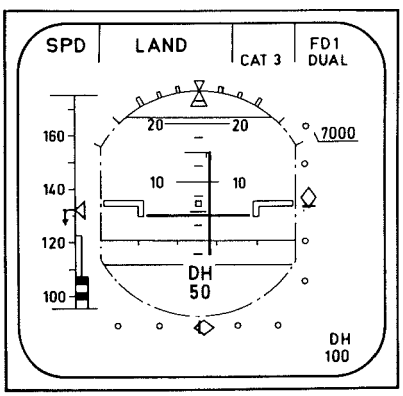
Von den fünf Symbolgeneratoren, unten im Computerraum des Flugzeuges, sind drei für die elektronischen Fluginstrumente zuständig. Alles, was darzustellen ist, läuft bei den Symbolgeneratoren auf, wird zu Satz, Layout und Graphik umgeformt und als fertige Seite an die Displays weitergegeben. Zwei reichen bereits, um jeweils ein Instrumentenpaar zu versorgen. Der dritte ist Reserve. Wenn ein Bildschirm selbst ausfallen sollte, kann sein Nachbar das Bild übernehmen.

Die restlichen zwei Symbolgeneratoren versorgen das elektronische Informations- und Überwachungssystem (ECAM). Auf diese Weise ist eine hohe Redundanz in allen wichtigen Leitsystemen vorhanden.

Systemüberwachung

Datenzentrale

Was FMS für die Flugführung bedeutet, ist ECAM für die Technik des Flugzeuges. ECAM, das elektronische Informations- und Überwachungssystem, sammelt alle Informationen und hält sie nach dem Prinzip "Head down Monitoring" im Blickfeld der Piloten bereit. ECAM streckt seine Fühler bis in die entlegensten Ecken der A 310 aus und spürt Unregelmäßigkeiten auf, wie eine Spinne im Netz. Solange alles normal verläuft, dient das



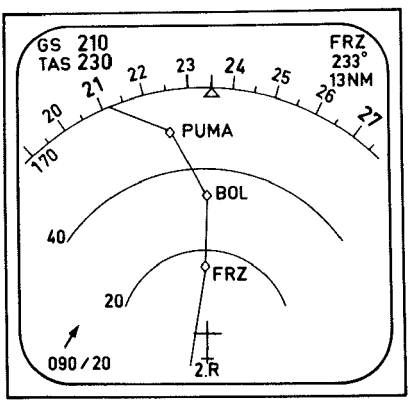
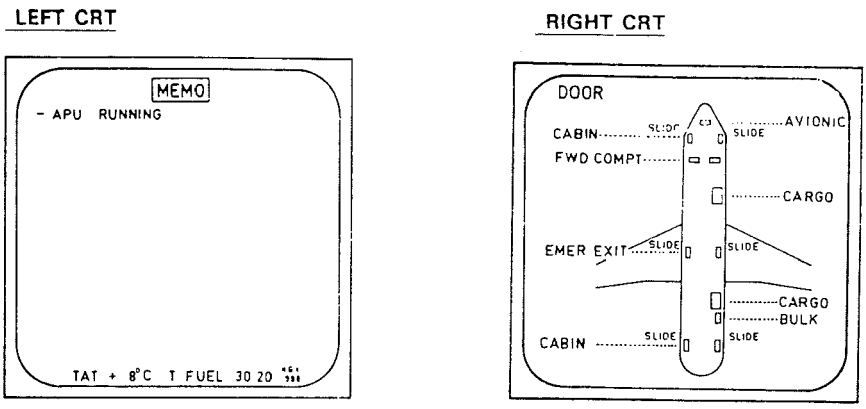


Bild 7: Primärfluginstrument (PFD) und Navigationsdisplay (ND)



The left CRT displays warning messages, STATUS and MEMO information.

The right CRT displays system synoptics.

Bild 8: Zentrales Überwachungs- und Informationssystem (ECAM)

linke Display als Merkzettel ("Memo") für die Besatzung und liefert in englischer Sprache Informationen über zeitweise zugeschaltete Anlagen (zum Beispiel Triebwerksenteisung: "icing conditions . . engine anti ice: ON"). Das rechte Display zeigt graphische Systembilder zum Beispiel über das Hydrauliksystem oder die Kabinendruckregelanlage. Welche Seite gerade aufgeschlagen wird, hängt im Normalbetrieb von der augenblicklichen Flugphase ab (Bild 8).

Im Störfall meldet sich selbsttätig das betroffene System. Auf dem rechten Bildschirm wird der aktuelle Zustand visualisiert. Was das linke Display dazu liefert, könnte einmal als Keimzelle für spätere Expertensysteme im Cockpit angesehen werden. Es erscheint eine checklistenartige Abhandlung der Probleme anhand vorab bewerteter Entscheidungskriterien (Bild 9).

Fehlerabhandlung

Der Fehlerabhandlung liegt eine dreistufige Hierarchie zugrunde.

- Fehler, die wegen der Folgenschwere manuell abgehandelt werden müssen; zum Beispiel das Abstellen eines Triebwerkes bei Triebwerksfeuer.
- Fehler mittelschwerer Bedeutung: dem Flugzeugführer wird die gesamte Abfolge des Fehlermanagements auf dem Bildschirm vorgeschlagen. Er initiiert mit einem Knopfdruck ihren automatischen Ablauf: zum Beispiel das Abschalten eines Hydrauliksystems mit den entsprechenden Folgerungen.
- Fehler leichter Bedeutung: der Fehler wird automatisch abgehandelt und der Flugzeugführer wird lediglich über den Status des Flugzeuges nach Abhandlung des Fehlers informiert: zum Beispiel das Umschalten einer Stromschiene nach Ausfall eines Generators.

Checklisten

Ungeachtet der Fähigkeiten des zentralen Informations- und Überwachungssystems sind die inzwischen klassischen Cockpit-Arbeitsmittel wie Checklisten nicht verschwunden. Sie sind aber erheblich kürzer geworden. Im Normalbetrieb beschränken sie sich auf einige wenige sicherheitsrelevante Punkte. Es gibt Prüfpunkte, für die sich vermutlich auch in

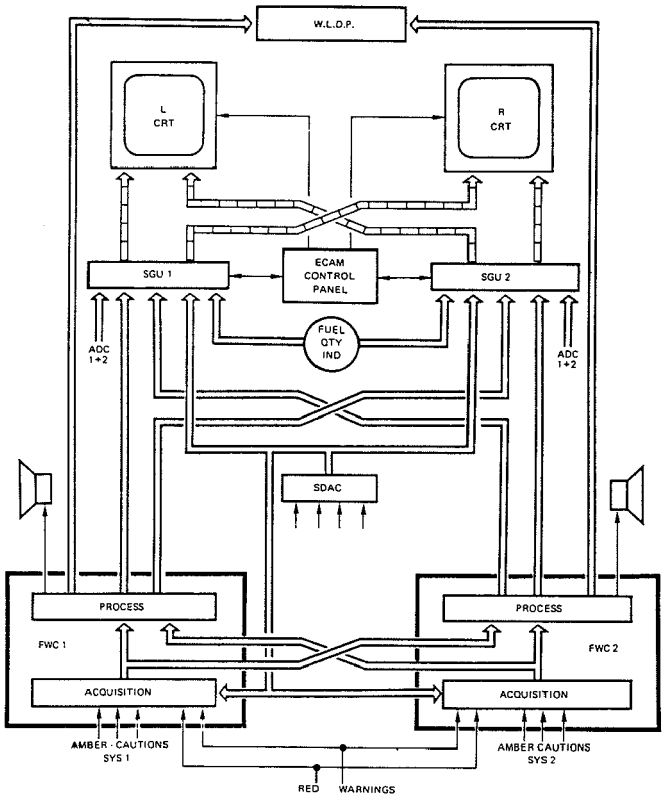


Bild 9: ECAM-Systemverknüpfung

Zukunft keine befriedigende Mechanisierung finden wird. Die Überprüfung der barometrischen Höhenmessereinstellung wird zum Beispiel nach einer Checkliste vorgenommen.

Generell kann man sagen: Bei der Abhandlung von Störfällen finden die elektronischen Überwachungssysteme dort ihre Grenzen, wo das verursachende Problem in dem Bereich der Stromversorgung liegt, die das ECAM System versorgt. Hier muß noch mit Papierlisten gearbeitet werden.

Piloten

Erfahrung

In der Luftfahrt werden Unfälle und kritische Ereignisse weltweit erfaßt und ausgewertet. Flugschreiber und Tonband sind im Cockpit gesetzlich vorgeschrieben. Anonyme Auswertungen von Flugberichten tragen zum internationalen Informationsaustausch bei. Gerade im Bereich der "Human Factors" gibt es gesicherte Erkenntnisse aus dem Unfallgeschehen.

Wo stehen wir heute?

Das Jahr 1985 liegt trotz hoher Unfallzahlen noch im langjährigen Trend. Seit Einführung der Jetflugzeuge im Jahre 1959 bis Ende 1984 wurden in der Zivilluftfahrt der westli-

chen Welt 390 Totalverluste registriert. Bei diesen Unfällen kamen mehr als 18 000 Menschen ums Leben. Bezüglich der Relation Totalverluste zu geflogenen Stunden und Starts wird das Fliegen immer sicherer. Jährlich werden heute über 15 Mio. Flugstunden geflogen. Man rechnet mit 20 Totalverlusten im Jahr. In den vergangenen 20 Jahren haben sich die Menschenverluste pro 100 Mio. Passagierkilometern von 0,48 auf 0,08 reduziert.

Bei der Ursachenforschung kommt man zu folgenden Ergebnissen:

Menschliches Versagen	62,4 %.
Flugzeug/Technik	12,9 %,
Sabotage	11,8 %,
Wetter	5,4 %,
Wartung	5,4 %,
Kollosionen	2,1 %.

Der stetigen Verringerung der Rate von Menschenverlusten pro geflogenen Passagierkilometern steht der hohe Prozentsatz von über 60 % für menschliches Versagen gegenüber. Diese Zahl bedeutet aber nicht, daß in der Statistik der Anteil Unfallursache „Mensch" übermäßig gewachsen ist. Die Entwicklung erlaubt uns festzustellen, daß es dem Menschen gelungen ist, die übrigen Unfallursachen Technik, Wetter und Umgebungsbedingungen in den Griff zu bekommen.

Pilotenauswahl

Die im Laufe der Jahre gewonnenen Kriterien zur Personalauswahl sind nach unseren Erkenntnissen auch im Hinblick auf neuere Cockpit-Technologie gültig. Die Auswahl findet nach wie vor nach folgenden Kriterien statt:

1. Begabungseigenschaften:
   - Schlußfolgendes kombinatorisches Denken,
   - Kurzzeitmerkfähigkeit,
   - Aufnahmefähigkeit für akustische Informationen,
   - Räumliche Orientierung und Erfassung von Richtungsbeziehungen
   - Wahrnehmungs- und Beobachtungstempo,
   - Steuerung der Aufmerksamkeit,
   - Sensomotorische Feinkoordination.
2. Persönlichkeitseigenschaften:
   - Motivation,
   - Kontrolliertheit des Verhaltens,
   - Belastbarkeit,
   - Flexibilität,
   - Selbstbehauptung,
   - Zuverlässigkeit.

Während die Feststellung der Begabung kein Problem darstellt, trifft dies für die Persönlichkeitseigenschaften nicht immer zu. Es ist schwierig, die Belastbarkeit eines Menschen über den langen Zeitraum seines zu erwartenden beruflichen Einsatzes vorherzusagen.

Ausbildung

Die Ausbildung besteht bei der Lufthansa aus zwei Teilen, der Grundausbildung und der Linienausbildung. Die etwa zweijährige Grundausbildung findet in Bremen sowie in Phönix/USA statt und schließt mit dem Verkehrsflugzeugführerschein ab. Darauf folgt der Erwerb der Musterberechtigung für die Eingangsmuster B 727 oder B 737 mit anschließender Linieneinweisung. Bei der Musterberechtigung geht es zunächst um Vermittlung des technischen Grundwissens und um die Beherrschung der Betriebsverfahren des

entsprechenden Musters. Die praktische Einweisung findet überwiegend in Simulatoren statt. Inzwischen haben Simulatoren einen hohen Entwicklungsstand erreicht und werden auch ausgiebig genutzt.

Alle Besatzungsmitglieder müssen ihre Qualifikation in regelmäßigen Überprüfungen erneuern. Das Auffrischungstraining trägt der Erkenntnis Rechnung, daß zur Beherrschung von kritischen Situationen und Störfällen andere, meist größere Fähigkeiten gefordert sind als zur Abwicklung des routinemäßigen Normalbetriebs. Die Trainings-Strategie ist darum auf Störfälle ausgelegt. Es gilt, vorhersehbare Probleme so gut in den Griff zu bekommen, daß für unvermeidbare Überraschungen noch genügend Kapazitäten freibleiben. Unser Lernziel heißt: Fehler vermeiden, das heißt Entstehung von Fehlern antizipieren; unvorhergesehene Fehler erkennen und richtig und rechtzeitig korrigieren.

Inhaber einer Lizenz kann natürlich nur ein Individuum sein. Jeder einzelne muß sein Können unter Beweis stellen. Im praktischen Training wird aber zugleich großer Wert auf Teamarbeit gelegt. Schwerpunkte sind Crew-Koordination und Crew-Kooperation. Eine Besatzung, in der jeder einzelne für sich zwar über das notwendige Wissen und Können verfügt, die aber trotz dieser Qualitäten zur Koordination und Kooperation nicht in der Lage ist, kann gemeinsam durch die Prüfung fallen.

Betriebserfahrung

Crew-Konzept

Die A 310 ist inzwischen über zwei Jahre im Linieneinsatz. Der bisherige Erfolg kann sich sehen lassen. Die technische Pünktlichkeitsrate beträgt 97 %. Es wurden bisher 37 850 Starts und Landungen durchgeführt und dabei 45 000 Flugstunden geflogen.

Bei unseren Betriebserfahrungen gibt es gerade in bezug auf Punkte, die bei der Indienststellung der A 310 besonders umstritten waren, gute Ergebnisse. Das Zweimanncockpit hat sich erneut bewährt. Es war dies keine technische Frage, die es erstmalig zu lösen galt.

Bildschirme

Die Bildschirmanzeigegeräte sind sehr zuverlässig und bieten eine wesentlich besser auf die jeweilige Aufgabe abgestimmte Informationsdarstellung.

Wie verhält es sich mit dem Nebeneinander von Bildschirmen und konventionellen Anzeigen? Ergeben sich zum Beispiel Schwierigkeiten aus einem Parallelbetrieb? Wie schon erwähnt, sind im A 310 die Triebwerksinstrumente noch mechanisch. Dies wird in zukünftigen Flugzeugen nicht so sein. Bildschirme haben den Vorteil, daß man durch Vorverarbeitung, Filterung und Strukturierung näher an den für den Benutzer optimalen Informationsgehalt kommt, und diesen vor allem noch der jeweiligen Flugphase anpassen kann. Sobald wegen mangelnder Redundanz auf konventionelle Instrumente umgeschaltet werden muß, läßt sich feststellen, daß dies sehr trainingsaufwendig ist. Der Grund ist einfach: Es ist nachteilig, wenn der Pilot gerade bei der Abhandlung von Störfällen, die erfahrungsgemäß mit Zeitstreß verbunden sind, abrupte Wechsel der Informationsweise verkraften muß.

Schulung

Verursachte die neue Technologie Schulungsprobleme? Natürlich ist bei jeder Schulungsmaßnahme die vorhandene Erfahrung maßgebend. In Einzelfällen kann eine Umschulung auf A 310 einen großen Schritt bedeuten. Das müssen wir verkraften. Diese Sprünge entstehen, weil wir unsere Flotten nicht fortlaufend modifizieren können, um sie der technischen Entwicklung anzupassen. Unsere Flugzeuge sind durchschnittlich 10 bis 15 Jahre im Einsatz. Zur Zeit sind markante Entwicklungsschübe in der Cockpitgestaltung zu verzeichnen. So kann die Umschulung auf den A 310 für den einzelnen Flugzeugführer durchaus zu einem deutlichen Schritt werden. Wir sind uns dessen bewußt und gestalten

unser Training entsprechend. Wir tun dies lieber, als daß wir uns durch zu starke Beachtung der Kommunalität den technischen Fortschritt entgehen ließen.

Automatisierungsgrad

Wie verhält es sich mit dem Automatisierungsgrad? Die in unseren Grundregeln geforderte Transparenz wird durch die neuen Leitsysteme wie ECAM, FMS, EFIS bedeutend gesteigert. Das FMS zeichnet sich zum Beispiel durch ausgeprägte Toleranz gegenüber Bedienfehlern aus. Der Autopilot befreit von lästiger Routine im Reiseflug. Er ermöglicht uns heute Anflüge bei nur 200 m Horizontalsicht. Weitere Reduzierung erwarten wir in Kürze.

Bei der Frage, wieviel von Hand, wieviel automatisch zu fliegen ist, ist die Handlungsfreiheit des Piloten voll erhalten geblieben. Situationsabhängig hat er die Möglichkeit, entweder ganz von Hand (und das sollte er zur Übung gelegentlich tun) oder fast vollautomatisch zu fliegen. Das automatische Flugführungssystem ist mit seinen unterschiedlichen Betriebsfunktionen baukastenartig konzipiert. Die verschiedenen Funktionsblöcke lassen sich situationsgerecht einsetzen. Die Übergänge sind komfortabel.

Lernkurve

Die positiven Kommentare sollen allerdings keine heile Welt vorgaukeln. Natürlich hat es auch Probleme gegeben, wir arbeiten daran. Einige Systeme liefern noch nicht die gewünschte Betriebszuverlässigkeit. Andere können noch nicht in ihrer vollen Ausbaustufe betrieben werden; das gerade lobend erwähnte FMS gehört dazu.

Während der Einführung hatten unsere Techniker ebenfalls einen Lernprozeß durchzumachen. Man darf aber feststellen, daß die unvermeidlichen Probleme, die mit der Indienststellung eines jeden neuen Fluggerätes einhergehen, vergleichsweise gering waren und den Gesamterfolg nicht schmälern konnten.

Zukünftige Entwicklung

Das nächste Produkt aus dem Hause Airbus Industrie wird die A 320 sein. Sie wird bei Lufthansa ab 1989 eingesetzt werden (Bild 10).

Bild 10: Cockpit im A 320

Dieses Flugzeug wird auf den ersten Blick recht konventionell aussehen, aber einige bedeutende technische Neuerungen aufweisen. Konsequenzen in bezug auf die Cockpitgestaltung fordert die Steuerungsanlage.

Die A 320 wird das erste Verkehrsflugzeug mit einer voll elektrischen Steuerung sein (FBW: fly by wire). Wegen der elektrischen Signalübertragung entfallen konstruktive Zwänge zum herkömmlichen Steuerhorn. Die A 320 wird einen Seitensteuergriff haben.

Ohne dieses Traditionsbauteil läßt sich im Verein mit weiterer Systemintegration die Einsehbarkeit und Erreichbarkeit der Instrumentierung und der Bedienelemente nochmals verbessern.

Die heute vorliegende Erfahrung wird zur konsequenten Weiterentwicklung aller Systeme genutzt. Das Primärflugdisplay wird zum Beispiel alle Fluglageinformationen beinhalten. Dies wird die Redundanz der Cockpitinstrumentierung nochmals deutlich steigern.

Die Rolle des Piloten

Eine elektrische Flugsteuerung wird das Fliegen leichter und sicherer machen.

Man spricht heute viel von der sich ändernden Rolle des Piloten, vom Manipulator zum Manager, oder Systemoperator. Beide Bilder sind unscharf und geben die Entwicklung nicht richtig wieder. Die wesentliche Aufgabe des Piloten ist und bleibt zu fliegen und richtige Entscheidungen zu treffen.

In dem Maße, wie es gelingt, die Technik besser in den Griff zu bekommen, kann das Fliegerische in den Vordergrund treten. Die fliegerische Erfahrung wird auch zukünftig vor Ort verlangt. Eine stärkere bodenseitige automatisierte Einflußnahme auf den Flugverlauf würde den unvermeidlichen Anteil von menschlichem Fehlverhalten nicht schmälern, sondern nur in einen Bereich verlagern, der so weit weg vom Geschehen ist, daß die nötige Betroffenheit ausbleibt.

Schrifttum

[1] Cockpit-Layout - Cockpit Crew Complement aus der Sicht der Deutschen Lufthansa AG, DLH-interne Veröffentlichung, 7.12.1979, Frankfurt.
[2] Hach, J.-P.; und P.H. Heldt: Das Cockpit des Airbus A 310, Spektrum der Wissenschaft, März 1984, Heidelberg.
[3] Das Crew-Coordination-Concept, Cockpit Report No. 19, 30.01.85, Vereinigung Cockpit e.V.
[4] Woodburn, P.: Flying The Lean Machine Boeing 757. Aerospace, London, Vol. 11, Jul - Aug 84.
[5] Hach, J.-P.: Die Technik im Cockpit eines modernen Verkehrsflugzeuges. „Ortung und Navigation, 3/84.
[6] Heldt, P.H.: Der Mensch im Cockpit eines modernen Verkehrsflugzeuges. Ortung und Navigation, 3/84.
[7] "Airline Guide to Human Factors", IATA 1981.
[8] "Pilot Error", Ronald & Leslie Hurst, Granada London/New York.
[9] Steininger, K.: Eignung und Tauglichkeit zum Flugzeugführer. DFVLR, 1976.

Diskussion

R. Polzenberg (AVR):

Werden manuelle Eingaben durch den Co-Piloten bestätigt? Sind die Quittiertasten so weit auseinander, daß diese nicht von einer Person alleine betätigt werden können?

P.H. Heldt (Deutsche Lufthansa):

Sie sind so gelagert, daß beide sie sowohl erreichen als auch einsehen können. Bei ad hoc zugewiesenen Höhenänderungen kann man das maschinell nicht in den Griff bekommen. Hier ist die von mir angesprochene Thematik der Crew-Koordination und Crew-Kooperation, die mit einer großen Portion Disziplin gekoppelt sein muß, von großer Bedeutung. Sind diese Komponenten nicht vorhanden, kommt es zu dem genannten menschlichen Versagen.

H. Pleger (GRS):

Sie gehen weltweit von 20 Totalausfällen pro Jahr aus. Ist es möglich – und sind Ihre Bemühungen darauf gerichtet – diese Zahl zu reduzieren?

P.H. Heldt (Deutsche Lufthansa):

Die genannten Zahlen stammen aus einer IATA-Statistik, in der die Unfälle der westlichen Welt erfaßt sind. Die Industrie bemüht sich natürlich, das Verhältnis zu verbessern. Hätte ich Ihnen ein Schaubild über diese Zusammenhänge gezeigt, hätten Sie erkannt, daß wir schon im asymptotischen Bereich der Sicherheitskurve liegen. Es wird sehr schwierig werden, bessere Ergebnisse zu erreichen. Überwältigende Steigerungen werden nicht mehr möglich sein. Wir müssen auch einbeziehen, wie stark der Luftverkehr zugenommen hat. Das heißt aber nicht, daß man sich mit dem Erreichten schon zufrieden geben sollte. Die Experten sind sich aber einig, daß es nicht möglich sein wird, in den nächsten zehn Jahren die Zahlen in dem gleichen Maße zu steigern, wie es uns in den letzten 20 Jahren gelungen ist.

W. Bastl (GRS):

Ihre Statistik weist einen beträchtlichen Anteil von Fehlern aufgrund menschlichen Versagens aus. Ist beabsichtigt, diesen Anteil durch Trainingsmaßnahmen oder verbesserte Leittechnik zu reduzieren? Oder handelt es sich hier um Wartungsfehler?

P.H. Heldt (Deutsche Lufthansa):

Der Anteil von Fehlern bei Wartungsmaßnahmen ist ja relativ gering. Wir glauben, daß man sich dieser Problematik in der gesamten Bandbreite nähern muß. Darum wurde bei meinem Vortrag über Leitsysteme im Cockpit ganz bewußt der Mensch mit einbezogen. Wir bemühen uns bei der Auslegung darum und versuchen, die vorhandene Erfahrung in bezug auf Schnittstellenprobleme und Betriebsverfahren einzubringen. Die Thematik „Mensch" spielt eine ganz große Rolle in der Ausbildung, bei dem gesamten Überprüfungswesen usw. Wir schämen uns auch nicht, diese Zahlen zu nennen; denn wo immer Menschen tätig sind, werden die für Menschen typischen Fehler auftreten. Im Luftverkehr werden wegen des bestehenden Meldesystems diese Probleme durch das umfangreiche Datenmaterial sehr gut beziffert. Wir sind froh darüber, denn das erlaubt uns, unsere Bemühungen zu konzentrieren.

K. Becker (DIN/NKe):

Sehen Sie in der Sicherheitstechnik im Luftverkehr einen sich vergrößernden Abstand zwischen den hochtechnisierten Industrieländern und den Ländern der Dritten Welt?

P.H. Heldt (Deutsche Lufthansa):

Vom rein technischen Standpunkt kann sich der Abstand nicht vergrößern, da die wichtigsten Flugzeughersteller in der westlichen Welt angesiedelt sind. Dritte-Welt-Länder können sich mit genügend Geld hochwertiges Fluggerät kaufen. Inwieweit es gelingt, damit umzugehen, ist allerdings eine andere Frage, die aber durch Fremdtraining, wie es auch bei uns durchgeführt wird, weitgehend lösbar ist.

Es gibt in diesem Zusammenhang aber eine sehr überraschende Entwicklung. Es zeigt sich, daß die Europäer hinsichtlich der Cockpit-Auslegung im Vergleich zu amerikanischen Gesellschaften wesentlich anspruchsvoller sind. Die Deregulation in den Vereinigten Staaten hat offenbar zur Reduzierung wichtiger Aktivitäten geführt. Eine Dienststelle „Technischer Pilot", wie wir sie uns leisten, finden Sie bei vielen amerikanischen Gesellschaften gar nicht. In den internationalen Gremien, in denen die Fluggesellschaften jenseits jeglichen Konkurrenzdenkens auf technischem Gebiet im Gespräch mit den Herstellern sehr eng zusammenarbeiten, zeigen sich immer wieder große Unterschiede zu beiden Seiten des Atlantiks. Daß die Europäer heutzutage anspruchsvoller sind, hängt mit der Deregulation zusammen und mir scheint es sehr bedenklich, daß derartige wirtschaftliche Strömungen auf den Sicherheitsbereich einwirken können.

W. Aleite (KWU):

1. Wie groß ist die Zahl der Störfälle, die Sie schulen?
2. Auf wieviele Sichtgeräte wollen Sie übergehen, wieviele Parallelinformationen wollen Sie geben?
3. Wieviele Formate von Informationen beabsichtigen Sie, dem Flugzeugführer zu zeigen?

P.H. Heldt (Deutsche Lufthansa):

Zur ersten Frage: Das ist nicht genau zu sagen, denn die Fehlerbehandlung hat eine Baumstruktur mit erheblichen Verästelungen. Die wichtigsten Störfälle sind Triebwerkausfall, Probleme in der Elektrik, Hydraulik etc. Die Überprüfungen für eine Besatzung dauern vier Stunden, die kaum ausreichen, um das behördlich vorgeschriebene Programm abzuwickeln. Es sind Überlegungen im Gange, ob man im Rahmen einer programmgesteuerten Unterweisung Zyklen herausarbeiten und genehmigen lassen kann, etwa einen Prüfflug A, B, C . . . , den man innerhalb von 24 Monaten abzuwickeln hat. Damit käme man aus diesem Zeitstreß heraus.

Zu den anderen Fragen folgendes: Zukünftig sind es acht Bildschirme: je zwei für die Piloten, davon einer für die Fluglagedarstellung, in dem das erwähnte „Basic T" zu finden ist, darunter oder daneben ein Navigationsdisplay, wo alles zum Thema Navigation zusammengefaßt ist. Komplementär dazu je ein Management-Computer. In der Mitte zwei Bildschirmgeräte für Triebwerke und Systeme. Dabei ist es in der Regel so, daß das obere Display für die Triebwerkanzeigen benutzt wird, aber auch hier schon flugphasengesteuerte Informationen, um die Dichte zu reduzieren. Dieses Prinzip wenden wir schon recht lange an. Manche Warnungen werden in gewissen Phasen unterdrückt, damit man nicht irritiert wird. Darunter befindet sich das Display für Systeminformationen und checklistenartige Führung. Die Bildschirmgeräte sind bis auf das FMS baugleich und somit austauschbar.

H. Trauboth (KfK):

1. Wie ist die Akzeptanz der Piloten von modernen bildschirmgesteuerten Cockpits? Die Pilotenvereinigung warnt vor zu viel einprogrammierter Flugplanung durch Personal am Boden, die dem Piloten (vor allem bei unvorhergesehenen Situationen) die Entscheidung nehmen. Dadurch würde die Sicherheit (durch verstärkte Computertechnik) reduziert statt erhöht werden.
2. Je mehr Elektronik Eingang beim Flugzeug findet, wird es nicht anfälliger durch elektromagnetische Einstreuungen wie Blitz? Werden die leittechnischen Systeme solchen Einflüssen beim Test unterworfen?

P.H. Heldt (Deutsche Lufthansa):

Zur ersten Frage: Es ist richtig, daß es gewisse Vorbehalte gegeben hat. Manche Experten haben möglicherweise vorab zu offene und zu kritische Betrachtungen veröffentlicht. Aber mit der steigenden Erfahrung mit den neuen Systemen wächst auch das Vertrauen.

Zur zweiten Frage: Der Blitzeinschlag ist ein großes Problem. Unter dem Strich kann man sagen, daß die Digitaltechnik nicht ganz so anfällig ist. Dagegen gewinnt die Thematik mit der Einführung von „Fly-by-Wire" – das heißt, vollelektrisch gesteuerte Flugzeuge – größere Bedeutung. Es gibt bestimmte Problemzonen, in die der Blitz bevorzugt einzuschlagen geneigt ist. Das ist in Verbindung mit „Fly-by-Wire" und verstärkter Kunststoffbauweise ein großes Thema, an dem intensiv gearbeitet wird. Wir alle zusammen hoffen, dieses Thema im Griff zu behalten.

R.O. Schneider (KfK):

Welche Fehlertoleranzen hat das INS? Müssen die Ergebnisse dieses Systems über lokale Funkfeuer korrigiert werden?

P.H. Heldt (Deutsche Lufthansa):

Bei den Langstreckenflugzeugen ist das INS dreifach ausgelegt. Es wird ein Voting-System angewendet, wobei sich die Systeme gegenseitig überprüfen. Man kann also im großen und ganzen ein „Weglaufen" des Rechners ausschließen. Es verlangt eine hohe Disziplin, die Daten korrekt in ein INS einzutippen. Diese Aufgabe ist mit dem hier gezeigten Flight-Management-Computer wesentlich einfacher zu lösen, zumal er über Land durch Update mit Radionavigations-Funkfeuern – es ist nämlich eine leichte Drift in dem System vorhanden – immer wieder korrigiert wird. Zukünftig, etwa in drei bis vier Jahren, erwarten wir, daß auf den Überwasserstrecken durch Einsatz von Navigationssatelliten zusätzliches Update möglich sein wird.

STAR-GENERIS — Ein Softwarepaket zur Informationsaufbereitung — Konzept und Anwendung —

Von L. Felkel[1])

Kurzfassung

Die Mensch-Maschine-Kommunikation in elektrizitätserzeugenden Kraftwerken nützt immer mehr die Möglichkeiten moderner Prozeßrechner aus. Im Gegensatz jedoch zum meist üblichen Darstellen von „roher" Prozeßinformation ist eine komplexere Verknüpfung von Prozeßdaten nötig, um Operateure durch Verbesserung der Informationsqualität zu unterstützen. Unter fortgeschrittenen Operateur-Hilfsmitteln für Kernkraftwerke versteht man zum Beispiel Programme zur Reduktion der Meldedichte, Störungsanalyse- und Expertensysteme, sowie bildhaft darstellende Informationssysteme.

Diese Operateur-Hilfsmittel basieren auf komplexen Verknüpfungen von Prozeßdaten. Die Verknüpfungen müssen in formaler und kompakter Art und Weise beschrieben werden können.

Die Realisierung rechnergestützter Informationssysteme dieser Art erfordert außergewöhnliche Softwareansätze und umfangreiche Systemanalysen. Das STAR-GENERIS[2])-Software-Konzept, das in diesem Artikel beschrieben wird, reduziert den Softwareaufwand auf ein Minimum durch Bereitstellung eines umfangreichen Programmpakets, mit Hilfe dessen die Projektierung und Implementierung von Ingenieurwissen (aus den Systemanalysen) zur Benutzung in fortschrittlichen operateurunterstützenden Systemen ermöglicht wird.

Abstract

Man-machine-communication in electrical power plants is increasingly based on the capabilities of minicomputers. Rather than just displaying raw process data more complex processing is done to aid operators by improving information quality. Advanced operator aids for nuclear power plants are, e.g. programs for alarm reduction, disturbance analysis and expert systems, as well as integral information display systems.

Operator aids use complex combinations and computations of plant signals, which have to be described in a formal and homogenous way. The design of such computer-based information systems requires extensive software and engineering efforts. The STAR software concept described in this paper, however, reduces the software effort to a minimum by proving an advanced program package which facilitates specification and implementation of engineering know-how necessary for sophisticated operator aids.

Historischer Überblick

In den frühen 60er Jahren wurde von dem englischen Betreiber CEGB (Central Electricity Generating Board) der Versuch unternommen, die schon zum damaligen Zeitpunkt während einer Störung auftretende umfangreiche Menge von Alarmen zu reduzieren [1]. Als Methode wurden sogenannte Alarmbäume zugrundegelegt, die es erlaubten, Alarmsequenzen sowie Relationen zwischen Alarmen zunächst grafisch darzustellen. Das hierdurch erworbene Wissen über Zusammenhänge von Alarmen sollte dann ein Compu-

[1]) Dipl.-Informatiker Lothar Felkel, Gesellschaft für Reaktorsicherheit (GRS)

[2]) STAR: Störungsanalyserechner; GENERIS: Generisches Rechnergestütztes Informationssystem

ter, gekoppelt an die Anlageninstrumentierung, benützen, um eine Ausgabe der folgenden Art auf einem Displaybildschirm zu erzeugen:

- Letzter aktiver Alarm,
- Fehlermeldungen zum letzten aktiven Alarm,
- nicht unterdrückte Alarme,
- Fehlermeldungen zu nicht unterdrückten Alarmen,
- höchstwertiger aktiver Alarm,
- Fehlermeldungen zum höchstwertigen aktiven Alarm,
- synthetisierter (hergeleiteter) Alarm,
- Fehlermeldungen zu hergeleiteten Alarmen.

Die gewählten Darstellungen unterscheiden sich nur unwesentlich von den heute in modernen Expertensystemen verwendeten sogenannten Wissensbasen. Leider wurde dem System nicht der erwartete Erfolg zuteil. Der Grund dafür lag damals vorwiegend in der Tatsache, daß die damalige Hardware nicht die nötige Leistungsfähigkeit haben konnte, sowie im Fehlen von komfortablen Hilfsmitteln zur Erstellung, Modifikation, Dokumentation und Archivierung der oben genannten Alarmrelationen (Wissensbasis).

Parallel zu diesen Aktivitäten wurden in den 60er Jahren auch Methoden zur Zuverlässigkeitsbestimmung komplexer industrieller Anlagen auf der Basis von Fehlerbäumen entwickelt. Dies geschah auf dem Gebiet der Flugzeugentwicklung durch Boeing, in der chemischen Industrie durch Arbeiten von Professor Powers von der Carnegie-Mellon-University sowie im nuklearen Bereich durch die amerikanische Risikostudie WASH 1400 von Norman Rasmussen. Im Risö National Laboratorium wurden von D.S. Nielsen die sogenannten Ursachen-Folgen-Diagramme entwickelt. Auch diese Methode hatte das Ziel, Aussagen über die Gesamtsystemzuverlässigkeit herzuleiten. Ursachen-Folgen-Diagramme haben eine enge Verwandtschaft mit Fehlerbäumen (DIN 25424) und sogenannten Ereignis-Ablauf-Diagrammen (DIN 25419).

Seit etwa 1974 beschäftigt sich das Laboratorium für Reaktorregelung und Anlagensicherung (LRA), aus dem 1977 zusammen mit dem Kölner Institut für Reaktorsicherheit die GRS gegründet wurde, ebenfalls mit Ursachen-Folgen-Diagrammen. Auf der Basis der englischen Erfahrungen sollten die Ursachen-Folgen-Diagramme als Repräsentation kausaler und zeitlicher Zusammenhänge von Prozeßereignissen fungieren, mit dem Ziel, eine Analyse von gestörten Anlagenzuständen rechnergestützt durchzuführen. Auf der Basis von erheblich verbesserten Hardwareeinrichtungen sowie einem zusätzlichen Konzept zur Erstellung, Modifikation, Dokumentation und Archivierung von Ursachen-Folgen-Diagrammen sollten die negativen Erfahrungen der englischen Pioniere vermieden werden.

Im Rahmen eines PDV-Projektes wurde von 1974 bis 1976 eine Prototypentwicklung für ein Störungsanalysesystem durchgeführt. Diese Entwicklung, die schließlich einem experimentellen Test am Halden Boiling Water Reactor unterzogen wurde, ließ die Möglichkeiten ahnen, die mit einem solchen System in bezug auf Sicherheit und Verfügbarkeit von Kernkraftwerken offenstanden.

Von 1977 bis 1982 wurde im Rahmen eines vom BMFT und der Kernkraftindustrie finanzierten Projekts die ursprünglichen Ideen weiterverfolgt mit dem Ziel einer Anwendung in einem Standard-1300-MW-Kernkraftwerk. Als Kernkraftwerk wurde Grafenrheinfeld ausgewählt, da dessen Fertigstellung für etwa 1980 geplant war (zum Zeitpunkt der mutmaßlichen Fertigstellung des Störungsanalysesystems). Die Experimente liefen über eine Zeitdauer von zwei Jahren und sind in [2] dokumentiert. Die Methodik der Ursachen-Folgen-Diagramme erwies sich als geeignet zur Beschreibung von

Störungsabläufen und Signalverknüpfungen. Allerdings zeigte sich die ursprüngliche Absicht, auf kontinuierliche dynamische Beschreibungsmöglichkeiten zu verzichten, als nicht realistisch, da dies zu nicht ausreichender Darstellung dynamischer Vorgänge in den Prozeßmodellen (zum Beispiel Trendinformationen, Rückkopplungseffekte, arithmetische Verknüpfungen) führt. Im wesentlichen fehlte es an der Menge der zur Verfügung gestellten Analogwerte. Auf jeden Fall zeigte sich, daß das dem STAR-System (Störungsanalyserechner) zugrundeliegende Softwarekonzept (das STAR-Konzept) es erlaubte, ein breites (zunächst nicht beabsichtigtes) Anwendungsspektrum zu erreichen. Es zeigte sich nämlich, daß die mit dem STAR-System verfolgte Funktion in Abhängigkeit der zugrundegelegten Beschreibung variiert werden konnte. Es ist daher möglich, die folgenden Funktionen, die in Diskussionen mit Herstellern, Betreibern und Instituten als wünschenswert zur Verbesserung der Information in der Kernkraftwerkswarte identifiziert wurden, zu realisieren:

1. Überwachung der Parameter des Sicherheitssystems,
2. rechnergestützte Nutzung von Teilen des Betriebshandbuchs,
3. Statusüberwachung von Komponenten und Anlagensystemen,
4. Reduktion der Meldedichte,
5. Versorgung von komplexeren Bilddarstellungen mit Parametern,
6. Überwachung des auslegungsgemäßen Anlagenverhaltens nach Störungen (Post-Mortem-Analyse),
7. integrierte Störungsanalyse,
8. Signalvalidation.

Parallel zu dieser Entwicklung wurde in den Vereinigten Staaten zunächst bei EPRI an einem Disturbance Analysis System (DAS), nach dem TMI-Störfall, verstärkt durch EPRI und DOE, an Möglichkeiten für ein Disturbance Analysis and Surveillance System (DASS) gearbeitet [3]. Was die Reduktion der Meldedichte betrifft, wurden Experimentalsysteme [4] entwickelt, jedoch nicht im industriellen Umfang eingesetzt.

Ein weiteres Projekt, das in Zusammenarbeit mit RWE und KWU unter Förderung des BMFT und der Industrie durchgeführt wird, zielt auf die Realisierung der Funktionen 5 bis 7 der oben genannten Liste ab. Das System wird Ende dieses Jahres im Kernkraftwerk Biblis, Block B, installiert.

Des weiteren ist derzeit das STAR-GENERIS-Softwarepaket in ausschließlicher Industrieförderung zur industriellen Anwendungsreife gebracht worden. Eingesetzt wird das Paket im Kernkraftwerk Philippsburg II, wobei die Funktionen 3, 4 und 6 realisiert werden.

Wie bereits eingangs erwähnt, wurden bisher fast ausschließlich binäre Informationen genutzt. Unter Einbeziehung auch analoger Information, die auch zur deterministischen Beschreibung von Teilprozessen (Modellen) genutzt werden kann, kann die „Wissensbasis" nennenswert erweitert werden. Das diese Modelle interpretierende On-line-Prozeßrechnerprogramm kann dann als ein sogenannter Inferenzmechanismus [5] betrachtet werden. In diesem Sinne hat das vorliegende STAR-GENERIS-Softwarepaket bereits viele Eigenschaften eines modernen Expertensystems. Der Schwerpunkt wird deshalb in den nächsten Jahren auf dem vollständigen Ausbau des STAR-GENERIS-Konzepts zu einem Expertensystemkonzept sein. Insbesondere wird dabei versucht werden, bisher notwendiges, vollständiges, deterministisches Vordenken möglicher Störungsverläufe bis ins kleinste Detail um heuristische Verfahren zu erweitern, um auch für nicht vorhergedachte Störfallsituationen noch sinnvolle Information an das zuständige Personal geben oder durch Interaktion mit diesem erzeugen zu können.

Funktionen

Wie bereits im ersten Kapitel erwähnt, ist es möglich, mit dem STAR-GENERIS-Konzept eine Reihe verschiedenartiger Informationsziele für das Personal in Kernkraftwerken zu erreichen. Die wichtigsten sollen im folgenden kurz beschrieben werden.

Rechnergestütztes Betriebshandbuch

Es gibt viele Situationen während des Betriebs eines Kernkraftwerks, für die die Anweisungen im Betriebshandbuch darin bestehen, die Werte bestimmter Anlagenparameter zu überprüfen, sie in logischer Weise miteinander zu verknüpfen und die im Betriebshandbuch beschriebene Handlungsanweisung auszuführen, wenn die spezielle Situation identi-

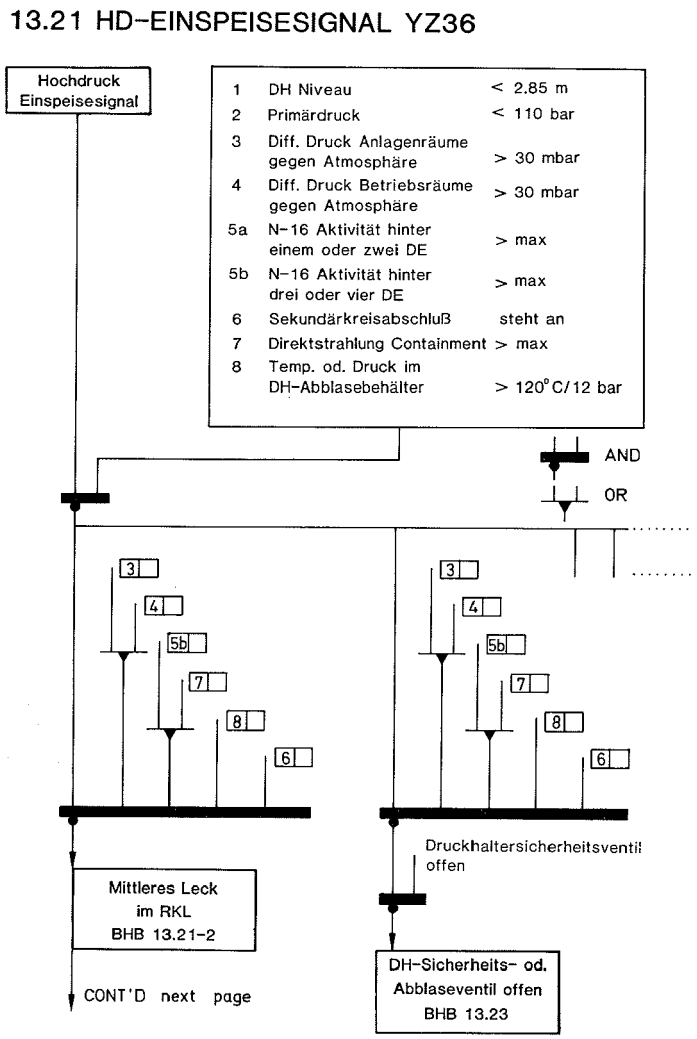


Bild 1: Sogenannte Logikfahne im Betriebshandbuch eines 1300-MW-Druckwasserreaktors

fiziert wurde. Im folgenden wird ein Beispiel solcher Anweisungen des Betriebshandbuchs ausgeführt. Es bezieht sich auf die Identifizierung eines mittleren Lecks in einem Druckwasserreaktor der KWU-1300-MW-Klasse.

Um den Grund für ein mittleres Leck feststellen zu können, ist zunächst ein Auslöseereignis zu finden. Im Fall eines mittleren Lecks kann das das Hochdruckeinspeisesignal sein. Das Vorhandensein eines Hochdruckeinspeisesignals erfordert, daß der Operateur eine Überprüfungsprozedur ausführt, um den Grund für das Anstehen des Hochdruckeinspeisesignals festzustellen und dann die im Betriebshandbuch eventuell festgelegte Handlungsanweisung realisiert. Während die Handlungsanweisung aus den verschiedensten Aktivitäten bestehen kann, ist die Überprüfungsprozedur ausschließlich auf Grund von Signalen der Instrumentierung durchzuführen. Diese Daten können deshalb auch einem Computer zur Verfügung gestellt werden, in dem natürlich die Überprüfungsprozedur entsprechend repräsentiert sein muß. Diese Repräsentation erfordert nur die logischen Operatoren „und", „oder", „nicht", „m von n" und arithmetische Relationen, um numerische Werte in logische zu verwandeln (zum Beispiel $a < b$, $a \neq b$, etc). Dieser kleine Umfang von primitiven Funktionen reicht aus, um Überprüfungsprozeduren des Betriebshandbuchs zu automatisieren. Als Resultat würde der Rechner die Situation identifizieren, die notwendige Handlungsanweisung bestimmen und den Operateur über die Anweisung informieren oder wenigstens darüber, wo die Beschreibung der Handlungsanweisung gefunden werden kann.

Es kann erwartet werden, daß in vielen Fällen so eine schnellere Bestimmung der Problemsituation und eine Reduktion des möglichen menschlichen Fehlers einhergeht.

In Bild 1 ist ein Teil der Originalprozedur des Betriebshandbuchs dargestellt. Der Operateur muß alle Parameter (1 bis 8) überprüfen und sie anhand der angegebenen Kriterien klassifizieren. Auf diese Klassifizierung wird weiter unten im Diagramm zurückgegriffen, um den vom Operateur zu beschreitenden logischen Weg zu steuern. Das Diagramm teilt sich in mehrere mögliche Kombinationen auf, die sich jedoch gegenseitig ausschließen. Deshalb wird er immer nur zu einem der auf Bild 1 unten sichtbaren Kästen kommen. Dieser Kasten enthält dann die Aktivitäten, die in bezug auf die identifizierte Situation unternommen werden müssen.

Zusammenfassend ist zu sagen, daß alle Prozedurschritte durch ein logisches Diagramm beschrieben werden können. Wenn darüberhinaus alle Signale auf dem Anlagenrechner zur Verfügung stehen, kann diese Logik automatisch ausgewertet werden und als Ergebnis den in den Resultatkästen angegebenen Kapiteln und Aktionen zugeordnet werden. Damit kann bei Auftreten des Auslöseereignisses automatisch und unmittelbar dem Operateur ein Hinweis gegeben werden, wo die notwendigen Betriebsprozeduren im Betriebshandbuch zu finden sind, ein Hinweis, der bei einem Umfang von etwa 15 Teilbänden mit je etwa 150 Seiten eine sehr hilfreiche Sache sein kann, oder er kann bei der Durchführung der Anweisungen unterstützt werden.

Bild 2 zeigt ein logisches Netzwerk, das die Information, die in Bild 1 gegeben ist, automatisch verarbeiten kann. Die Anzahl der verwendeten Logikgatter könnte weiter reduziert werden, um die Rechenzeit zu optimieren. Andererseits zeigt schon die nichtoptimierte Version eine im Gegensatz zu Bild 1 nicht mehr günstige Lesbarkeit für den Betrachter.

Reduktion der Meldedichte

Gerade bei mittleren, komplexen Ereignisabläufen im Kernkraftwerksbetrieb kommt es in der Warte zu einer ungewöhnlich großen Anzahl von Meldungen. Dies können bereits in den ersten fünf Sekunden nach einer Störung 500 Alarme und mehr sein. Auf der anderen Seite tragen die meisten dieser Alarme wenig oder sogar keine neue Information (zum Beispiel niedriger Öldruck an nicht arbeitenden oder nicht benötigten Pumpen). Auch

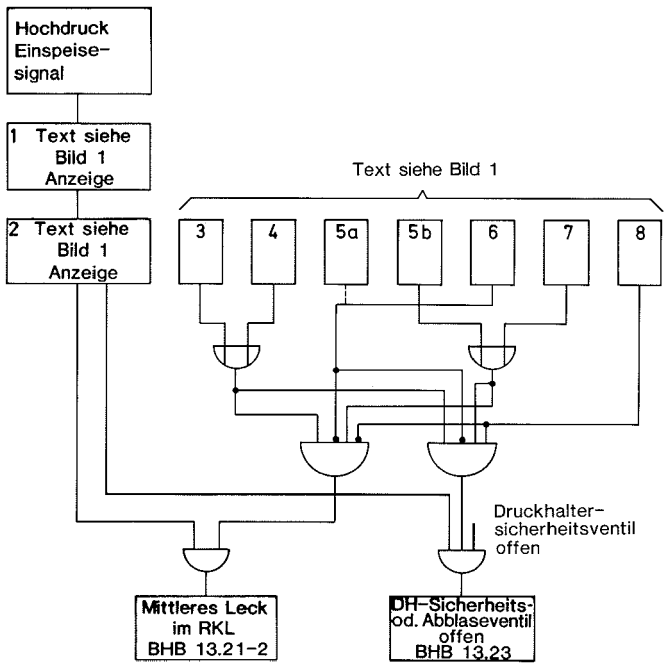


Bild 2: Rechnerrepräsentation der Logik aus Bild 1

sind viele dieser Alarme eine direkte Folge von anderen Alarmen oder sie implizieren einen vorangegangenen Alarm (Temperatur $> 50\ ^{\circ}C$ Temperatur > 60 %). Dies bedeutet jedoch, daß man entscheiden sollte, ob ein Alarm ausgegeben wird oder nicht. Dazu muß jedoch die jeweilige Anlagensituation analysiert werden. Manchmal kann dazu einfache Logik verwendet werden, um Alarme zu unterdrücken. Um jedoch eine wesentliche Alarmreduktion zu erreichen (Ziel muß sein, die Anzahl der Meldungen um den Faktor 20 bis 50 zu reduzieren, denn 150 von ursprünglich 300 ändern an der Problemsituation nichts), müssen jedoch auch schwierigere Fälle behandelt werden können. Bild 3 zeigt eine solche Situation. Das Beispiel bezieht sich auf die Bilanzierung von Zu- und Abflüssen zum Beispiel des Speisewassertanks. Die Zu- und Abflüsse werden summiert und deren Differenz gebildet. Manche Zuflüsse werden durch Regelventile gesteuert und sollen den Wert 0 haben, wenn die Regelventile geschlossen sind. Dies geschieht über sogenannte Analogschalter (oben im Bild 3). Nach Differenz oder Verhältnisbildung können die resultierenden Werte auf Überschreitung von Grenzwerten geprüft werden. Die dabei entstehenden logischen Werte können mit weiteren Binärsignalen verknüpft werden. Darüber hinaus soll eine Sperrung erst nach Ablauf von 30 s erfolgen. Diese Situation ist mit Logik und Arithmetik allein nicht zu erfassen, sie erfordert auch eine zeitliche Überwachung der in Frage stehenden Signale. Durch Einbau von zeitlichen Verzögerungen (zum Beispiel Ansprechverzögerung) können solche Fälle adäquat beschrieben werden (im Bild 3 unten).

Grundsätzlich enthält Bild 3 mehr Information, als daß die Meldungen von Untersystemen unterdrückt werden, wenn die Situation dies wirklich erfordert. Die Darstellung erlaubt nämlich auch eine Identifikation der Alarmursache. Dies bedeutet jedoch, daß trotz der Tatsache, daß viele Situationen durch einfache Logik abgehandelt werden

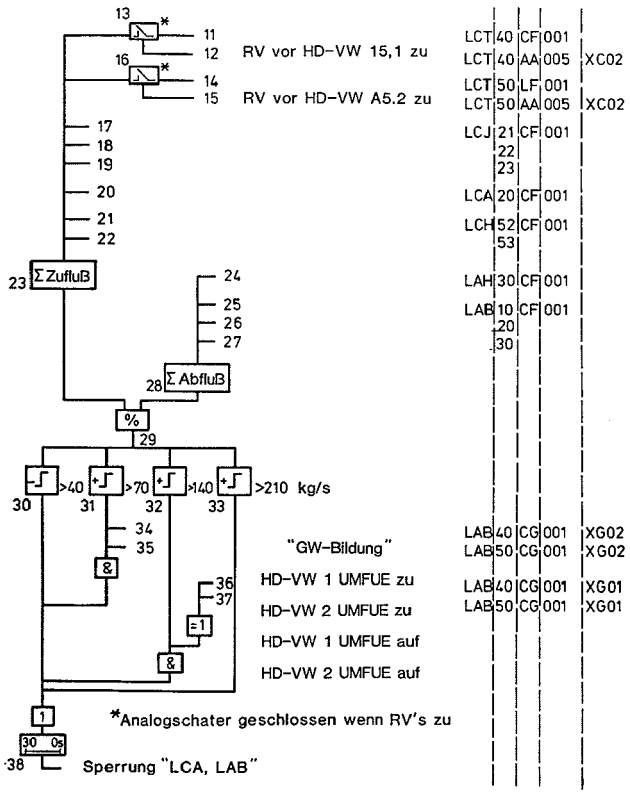


Bild 3: Komplexes Sperrkriterium für Meldereduktion

können, schon für einfache Alarmreduktionen eine Art Störungsanalyse durchgeführt werden muß.

Post-Mortem-Analyse

Eine der wichtigsten Aufgaben des Operateurs, vor allem aber des Schichtleiters bzw. Anlageningenieurs zum Beispiel nach einer Reaktorschnellabschaltung oder einem Turbinenschnellschluß ist es, festzustellen, ob alle Signale innerhalb eines Zeitraums vollständig und in der richtigen Zeitfolge aufgetreten sind. In solchen Fällen kann – unter der Voraussetzung einer zeitlichen Signalauflösung von ungefähr 10 ms – dabei schon ein Ergebnisausdruck von einigen Metern Länge die Folge sein. Normalerweise sind die Meldungen auf dem Ausdruck ausschließlich chronologisch geordnet. Das bedeutet jedoch, daß voneinander logisch bzw. verfahrenstechnisch abhängige Meldungen durch andere Meldungen voneinander getrennt werden. Man kann sich unschwer vorstellen, daß es eine zeitaufwendige und fehlerträchtige Aufgabe ist, erstens festzustellen, ob sich die Signale in der korrekten zeitlichen Reihenfolge befinden und zweitens, ob überhaupt alle Signale vollständig vorhanden sind. Eine Reduzierung der Zeit, die man für diese Aufgabe bis jetzt benötigt, kann sicherlich die Anlagenverfügbarkeit erhöhen, da man unter Umständen wieder schneller anfahren kann (das Anfahren ist ja erst wieder möglich, wenn eine ausreichende Bestätigung über das auslegungsgemäße Anlagenverhalten sowie der Ursache für das aufgetretene Problem vorliegt).

ZEIT-Kontrolle : Datum : 23.10.1985 =>> 14:46:33.6 <<=

Auslegungsgemaesses Anlagen-Verhalten BIBLIS-B Nummer 94

Anregung: Datum: 13.10.1985 Uhrzeit von: 21:20:00.0
bis: 21:21:00.0 Turbinenschnellabschaltung (TUSA)
Ueberwachungs-Zeitspanne: 60 sec

Anrege-Signal(e):

C0094	R124 U094XU00	Ausl.Signal fuer Abl.-Protokoll: 94	
B1756	YZ72 U001XU03	*TUSA SIGNAL	
B1757	YZ72 U002XU03	*TUSA SIGNAL	
B1758	YZ72 U003XU03	*TUSA SIGNAL	
B0626	SC14 K001XG01	*SS-EINRICHTUNG 1 (TUSA)	
B0627	SC14 K002XG01	*SS-EINRICHTUNG 2 (TUSA)	
B0628	SC14 P011XG52	*DR.SS-OEL (SS AUSGELOEST)	
B0627	SC14 K002XG01	*SS-EINRICHTUNG 2 (TUSA)	

Ablauf-Protokoll: Nummer 94 Fortsetzung auf Blatt 2

Ablaufkontrolle

Zeit	Bf/An Nr.	A K Z	Text	Soll	Ist (Ausgabe nur bei Abweichung vom Soll-Wert)	Bemerkungen
>> 2 s<<	* * *	* * * * * * *	* * * * * * * * * * * * * * * * * *	* * * *		
21:20:01.1	B0626	SC14 K001XG01	*SS-EINRICHTUNG 1 (TUSA)	AUSLOESG		
21:20:01.2	B0627	SC14 K002XG01	*SS-EINRICHTUNG 2 (TUSA)	AUSLOESG		
21:20:01.2	B0628	SC14 P011XG52	*DR.SS-OEL (SS AUSGELOEST)	ZU TIEF		
21:20:01.2	B0629	SC14 P012XG52	*DR.SS-OEL (SS AUSGELOEST)	ZU TIEF		
21:20:01.1	B0611	SC00 U101XU01	*ZUSUE ANREGUNG 1 LSR/SS	ANGESPR.		
21:20:01.1	B0612	SC00 U101XU02	*ZUSUE ANREGUNG 2 LSR/SS	ANGESPR.		
21:20:01.1	B0613	SC00 U101XU03	*ZUSUE ANREGUNG 3 LSR/SS	ANGESPR.		
21:20:01.3	B0589	SA11 S001XG02	HD-SS-V1	ZU		
21:20:01.4	B0590	SA11 S002XG02	HD-SS-V2	ZU		
21:20:01.4	B0591	SA11 S003XG02	HD-SS-V3	ZU		
21:20:01.4	* *	* * *	*	*		
21:20:01.4	* *	* * *	*	*	*NI.ZU *	
21:20:01.4	* *	* * *	*	*		
21:20:01.5	* *	* * *	*	*	*NI.ZU *	
21:20:01.5	* *	* * *	*	*		
21:20:01.5	* *	* * *	*	*	*NI.ZU *	
21:20:01.5	* *	* * *	*	*		
21:20:01.6	* *	* * *	*	*	*NI.ZU *	
21:20:01.6	B0592	SA11 S004XG02	HD-SS-V4	ZU		
21:20:01.6	B0598	SA11 S011XG02	FD-STELLVENTIL 1	ZU		
21:20:01.7	B0600	SA11 S012XG02	FD-STELLVENTIL 2	ZU		
21:20:01.7	B0602	SA11 S013XG02	FD-STELLVENTIL 3	ZU		

Ablauf-Protokoll: Nummer 94 Fortsetzung auf Blatt 3

Ablaufkontrolle

Ablauf-Protokoll: Nummer 94 13.10.1985 21:20:00.0 Blatt 3 von 4

Zeit	Bl/An Nr.	A K Z	Text	Soll	Ist (Ausgabe nur bei Abweichung vom Soll-Wert)	Bemerkungen
21:20:01.7	B0604	SA11 S014XG02	FD-STELLVENTIL 4	ZU		
21:20:01.6	B0597	SA11 S011XG01	FD-STELLVENTIL 1	N1.AUF		
21:20:01.6	B0599	SA11 S012XG01	FD-STELLVENTIL 2	N1.AUF		
21:20:01.7	B0601	SA11 S013XG01	FD-STELLVENTIL 3	N1.AUF		
21:20:01.7	B0603	SA11 S014XG01	FD-STELLVENTIL 4	N1.AUF		
21:20:01.8	B0648	SF11 S001XG02	UMLEITSCHNELLSCHLUSSVENTIL 1	N1.ZU		
21:20:01.8	B0649	SF11 S011XG02	FD-UMLEITSTELLVENTIL 1	N1.ZU		
21:20:01.8	B0650	SF12 S001XG02	UMLEITSCHNELLSCHLUSSVENTIL 2	N1.ZU		
21:20:01.8	B0651	SF12 S011XG02	FD-UMLEITSTELLVENTIL 2	N1.ZU		
21:20:01.8	B0652	SF13 S001XG02	UMLEITSCHNELLSCHLUSSVENTIL 3	N1.ZU		
21:20:01.9	B0653	SF13 S011XG02	FD-UMLEITSTELLVENTIL 3	N1.ZU		
21:20:01.2	B0638	SE10 C010XH05	*TURB.OEFFNUNGSREGL.1 AUSSER EINGRI	JA		
21:20:01.3	B0639	SE10 C010XH15	TURB.OEFFNUNGSREGL.2 AUSSER EINGR.	JA		
>> 3 s<<	* * *	* * * * * * * *	* * * * * * * * * * * * * * * * * * *	* * * *		
21:20:02.8	B0640	SE10 C010XH36	LEISTUNGSREGLER	AUS		
>> 2 s<<	* * *	* * * * * * * *	* * * * * * * * * * * * * * * * * * *	* * * *		
21:20:01.0	E0071	RI28 U094XU01	L-Sch.Block B und Erregung "aus"	ERFUELLT		
21:20:02.9	B0661	SP10 K018XN03	*RUECKLEISTUNG KURZZEIT	AUSLOESG		AUSLOESG
21:20:00.8	B0013	AP03 H001XB01	*L-SCH.BLOCK B (27KV)	AUS		EIN
21:20:24.0	B0654	SP10 C010XB01	ERREGUNG	AUS		EIN
>> 1 s<<	* * *	* * * * * * *	* * * * * * * * * * * * * * * * * * *	* * * *		
21:20:01.0	E0072	RI28 U094XU02	STAW-LAW bei Reakt.Leist. > 55 %	ERFUELLT	ERFUELLT	um 0.020 sec zu spaet

Ablauf-Protokoll: Nummer 94 Fortsetzung auf Blatt 4

Ablaufkontrolle

Ablauf-Protokoll: Nummer 94 13.10.1985 21:20:00.0 Blatt 4 von 4

Zeit	Bl/An Nr.	A K Z	Text	Soll	Ist (Ausgabe nur bei Abweichung vom Soll-Wert)	Bemerkungen
21:19:59.2	A0042	YZ05 U985	KORR.THERMISCHE REAKTORLEISTUNG	<analog>	72.5600 (PROZENT)	
21:20:00.9	B1582	YR43 C100XR61	*STEW-LAW	ANGESPR.	ANGESPR.	

Ende des Protokolls der Ablaufueberwachung Nummer: 94

Bild 4: Komplementäres Störablaufprotokoll mit „post-mortem"-Analyse für „Turbinenschnellabschaltung"

Das folgende Beispiel soll illustrieren, welche Anforderungen an die Aufgabe gestellt werden.

Die Situation „Turbinenschnellabschaltung" kann durch drei verschiedene Signalklassen ausgelöst werden:

— (zusätzliche) Maßnahmen gegen Überdrehzahl,

— Turbinenschnellschlußauslösung,

— Hydrauliköldruck der Turbine zu niedrig.

Ein Signal dieser Klassen ist immer der „Auslöser", die beiden anderen müssen jedoch nach spätestens einer Sekunde auch aufgetreten sein. Die weitere chronologische Folge sieht dann so aus:

Der Überwachungszeitraum für die Situation im Beispiel „Turbinenschnellabschaltung" ist auf 60 s festgelegt. Nach Ablauf dieser Zeitspanne wird das in Bild 4 gezeigte Protokoll ausgegeben.

Das Beispiel zeigt, daß hier extensiv nicht nur Signalzustände, sondern auch das Verhalten der Signale innerhalb bestimmter definierter Überwachungszeiträume untersucht werden muß. Hauptzielsetzung dabei ist es nun, nicht das Auftreten von Signalen auszugeben (was meist ein sehr umfangreiches Protokoll ist), sondern diejenigen Meldungen zu protokollieren (bzw. zu markieren, wie es das Beispiel in der Spalte „Ist" und „Bemerkungen" zeigt), die nicht oder nicht in der zeitlich korrekten Reihenfolge aufgetreten sind. Darüber hinaus werden Aussagen gemacht, die zunächst nicht als Einzelsignale im Prozeß vorhanden sind und deshalb synthetisiert werden müssen, zum Beispiel

„Vier Minuten nach Auftreten des Auslöseereignisses darf sich höchstens einer von vier bestimmten Analogwerten um mehr als einen bestimmten Betrag geändert haben."

Dies bedingt, daß, selbst wenn die letzte Aussage auf einen ja/nein-Zustand zurückgeführt werden kann, zur Herleitung dieser Aussage unter anderem umfangreiche arithmetische Verknüpfungen (zum Beispiel Gradientenbildung etc.) und natürlich logische Verknüpfungen durchgeführt werden müssen.

Von der Komplexität her werden hier schon Funktionen gefordert, die auch extensiv bei der integrierten Störungsanalyse angewendet werden.

Integrierte Störungsanalyse

Die Hauptzielsetzung der integrierten Störungsanalyse ist: Eine gestörte Situation möglichst früh zu entdecken, Primärursachen zu identifizieren sowie wichtige Information über die möglichen Folgen der Störung zusammenzustellen. Darüber hinaus soll versucht werden, mögliche Gegenmaßnahmen sowie Erfolgspfade zu bestimmen.

Um dies zu erreichen, sind die verfahrenstechnischen Aufgaben der einzelnen Prozesse einer funktionsorientierten Klassifizierung unterworfen worden, das heißt der Prozeß wird in seine funktionellen Einheiten zerlegt. Die einzelnen Funktionen können allgemein durch (normalerweise einige wenige) physikalische Prozeßvariablen beschrieben werden.

Um Störungen entdecken zu können, werden die relevanten Prozeßvariablen auf Abweichungen von ihren Nominalwerten hin untersucht. Diese Nominalwerte sind normalerweise keine Konstanten, es kann sich hierbei sogar um komplizierte charakteristische Funktionen (Kennlinien) handeln. Eine Wichtung und Auswertung der Abweichungen wird auf der Basis einer prozeßabhängigen Varianz, dem Absolutwert der Abweichung, als auch dem Gradienten der Abweichung durchgeführt. Einige der Prozeßgrößen erlauformation zu verwenden oder als einen Ersatzwert für nicht gemessene oder nicht meßbare Größen heranzuziehen. Diese Modelle eignen sich auch zur Vorabschätzung der prozeßabhängigen Varianzen.

Die integrierte Störungsanalyse, wie sie zum Beispiel in der Anwendung in Kernkraftwerk Biblis B eingesetzt wird, fußt noch immer auf den Erfahrungen der Störungsanalysefunktionen der STAR-Anwendung in Grafenrheinfeld. Anders als dort, wo die Analyse vornehmlich auf Binärsignalen und Binärlogik aufgebaut war, das heißt im wesentlichen auf Grenzwertüberschreitungen, werden bei der Anwendung in Biblis wesentlich mehr analoge Variablen zur Analyse herangezogen. Dies ist umso wertvoller, als die Analyse bereits zu Zeitpunkten durchgeführt werden kann, zu denen noch keine (festgelegten) Grenzwerte verletzt worden sind. Natürlich erfordert dies die Verwendung von Filtertechniken, um nicht Störungen zu identifizieren, die nicht vorhanden sind. Die Logik wird jetzt im wesentlichen dazu verwendet, dem Operateur geeignete Information weiterzugeben, nachdem Störungen entdeckt worden sind und darüberhinaus Informationen in speziell entworfene Bilddarstellungen auf Farbsichtgeräten dynamisch einzuspielen.

Neben Boolescher Logik werden für die Störungsanalyse deshalb eine Reihe von generischen Funktionen verwendet: STATUS, TREND, FILTER, EVALUATE, LIMIT, TIMER, und einige mehr. Dieser Satz von generischen Funktionen kann auch leicht neuen Erfordernissen aus der Systemanalyse angepaßt werden.

Generische Funktionen

Die Statusfunktion, die eine Prozeßvariable X zum Argument hat, bildet diesen Wert X sowohl wie ihre Ableitung auf mehrere Klassen ab: Normal (innerhalb des Toleranzbands einer sich beruhigenden Störung), außerhalb des Toleranzbands einer solchen Störung, außerhalb des Toleranzbands mit progressivem Verhalten. Ziel ist es, zum Beispiel Darstellungen auf einem Farbsichtgerät zu steuern oder Meldungen zu erzeugen mit den Attributen wie zum Beispiel keine lokale, regionale oder globale Störung.

Eine andere Funktion ist TREND; sie arbeitet auf dem Gradienten einer einzelnen Prozeßvariablen. TREND wird benutzt, um die Änderungsrate von Variablen zu klassifizieren (dies gilt auch für synthetisierte Variable, die ja Störungen präsentieren). Außerdem generiert TREND Attribute, wie „Trend nach oben", „Trend nach unten" sowie verstärkter bzw. verminderter Gradient der Prozeßvariablen.

Im Normalfall werden die Prozeßmeßgrößen verrauscht sein. Deshalb ist eine Glättung der Prozeßvariablen notwendig. Um dies zu erreichen, gibt es die FILTER-Funktion, die die letzten 5 Abtastungen (Fixed-Point-Memory-Filter), die Ableitung der geglätteten Größe y^* zum Zeitpunkt t_i sowie den geglätteten Gradienten y^* zum Zeitpunkt t_i benutzt. Die Filterfunktion gibt auch einen aktuellen Schätzwert für den Wert von y an sowie eine Vorhersage des erwarteten Werts von y zum Zeitpunkt t_{i+1}.

Bei der Funktion EVALUATE handelt es sich eigentlich um einen „kleinen Simulator" für bestimmte ausgewählte Prozeßvariablen x, und sie repräsentiert damit eine analytische Redundanz: $\hat{x}(t_i) = F(y(t_i))$, was natürlich bedeutet, daß es eine funktionale Relation zwischen x und y gibt. Dies bedeutet eine Validation von x durch die Funktion $F(y)$.

Die sehr einfache Funktion LIMIT überprüft Prozeßvariablen dahingehend, ob fest eingestellte Grenzwerte im Intervall zweier Abtastzeitpunkte verletzt worden sind.

Ein Problem bereitet die nicht synchrone Abtastung bzw. Aufdatierung der Prozeßvariablen (die Aufdatierung erfolgt erst bei einer Signaländerung um einen bestimmten Deltawert), was insbesondere die Berechnung der Gradienten erschwert. Es mußte deshalb eine TIMER-Funktion geschaffen werden, die die verstrichene Zeit zwischen zwei Meßzeitpunkten berechnen kann und somit in der Lage ist, aus einer asynchronen Prozeßgrößenerfassung eine solche mit scheinbar fest vorgegebenem Zeitintervall zu machen.

Störungsanalyse

Wenn immer eine oder mehrere Variablen ihre Werte ändern (dies ist üblicherweise nicht häufiger als 1 s oder 5 s für Analogwerte und 10 ms für Binärsignale), wird eine Analyse gestartet. Zunächst muß der Anlagenbetriebsmodus festgestellt werden. Dieser ist repräsentiert durch die Variable MODE. Gegenwärtig werden für die Störungsanalyse zwei Betriebsarten unterschieden (produktive bzw. nicht-produktive Betriebsweise). MODE wird definiert als eine Boolesche Oder-Verknüpfung auf einem relativ kleinen Satz von Binärsignalen. MODE liefert ebenfalls einen binären Wert, der, falls er 0 ist, die nichtproduktive Fahrweise repräsentiert (zum Beispiel Reaktorschnellabschaltung, Turbinenschnellschluß oder auch Reaktorleistung < 25 % etc.).

Wenn MODE den Wert 1 hat, so werden wichtige Untersysteme des Hauptkondensat- bzw. Speisewassersystems (zum Beispiel Pumpen, Speisewasserbehälter, Nieder- bzw. Hochdruckvorwärmer etc.) einer detaillierten Überwachung und Störungsanalyse unterzogen. Als Ergebnis wird eine Prioritätenreihenfolge bestimmt, ob und gegebenenfalls

welche Anlagenkomponenten den stärksten Einfluß auf die Hauptwärmesenke haben. Auf der Basis dieser Information kann der Operateur dann entscheiden, welche Gegenmaßnahmen die beste Wirkung zeitigen werden. Darüber hinaus kann nach deren Einleitung ihre Effektivität überwacht werden.

Solange die MODE-Variable auf 0 gesetzt ist, wird die detaillierte Überwachung übersprungen und der Zustand des Wärmeübergangs vom Primär- zum Sekundärsystem wird vor allem durch die Prioritätenzuweisung dargestellt.

Die hier kurz dargestellte Methode zur integrierten Störungsanalyse erlaubt es, Störungen zu identifizieren, bevor die sogenannten konventionellen Alarme eintreten. Nachdem ein Problem auf diese Weise identifiziert worden ist, besteht die Möglichkeit, die Komponenten zu klassifizieren, die den größten Einfluß zur Wiederherstellung des ursprünglichen oder zwischenzeitlich neu definierten Betriebsziels haben.

Das Star-Generis-Softwarekonzept

Zunächst mögen die im letzten Kapitel dargestellten Funktionen und Informationsziele relativ inhomogen erscheinen. Als die Arbeiten etwa 1974 begannen, war die Hauptzielsetzung ausschließlich die rechnergestützte Störungsanalyse. Man mußte sich deshalb keine Gedanken über mögliche Abstraktions- und Homogenisierungsanforderungen machen. Bereits während der ersten Phase der Systemanalyse zur Grafenrheinfeld STAR-Anwendung zeigte sich jedoch, daß ein vernünftiges Softwarekonzept nicht auf der Basis solch inhomogener Anforderungen gemacht werden konnte. Es stellten sich hauptsächlich zwei Probleme:

- Das Problem der Projektierung, das heißt der Repräsentation von Ergebnissen der sogenannten Systemanalyse,
- das Problem der Interpretation, das heißt der On-line-Verarbeitung von Prozeßgrößen in Abhängigkeit der von der Systemanalyse erstellten Verhaltensmodelle.

Wenig später kam auch noch die Einsicht hinzu, daß funktionelle Modifikationen bzw. Erweiterungen am Gesamtsystem wohl ständig vorgenommen werden würden. Ohne ein homogenes Konzept wäre die Weiterarbeit zum Scheitern verurteilt gewesen, da man sich die hohen Softwarekosten, die mit den Änderungen bzw. Erweiterungen einhergehen, nicht hätte leisten können. Es mußte deshalb versucht werden, die wesentlichen Elemente, die zum Beispiel allen den eingangs genannten Informationsanforderungen und Funktionen gemeinsam sind, herauszulösen und zu abstrahieren. Das gemeinsame und immer wiederkehrende Schema bei diesen Funktionen ist die Ereignis-Bedingung-Aktion-Sequenz.

Welche Funktionen auch immer durch ein Prozeßüberwachungs- und Diagnosesystem ausgeführt wird, sie wird angesteuert durch ein Ereignis, zum Beispiel ein Prozeßereignis oder auch durch synthetische, das heißt aus vielen Prozeßereignissen über logische bzw. arithmetische Relationen hergestellte Ereignisse. Zum Zeitpunkt der Ansteuerung, bzw. in einem definierten Zeitraum für eine Analyse oder Überwachung, herrschen bestimmte Bedingungen. Aufgrund der Ansteuerung und der vorherrschenden Bedingungen kann und muß entschieden werden, welche Aktionen ausgeführt werden. Diese Aktion kann die Generierung von Aktionen für den Operateur, die Steuerung von Bilddarstellung zum Beispiel auf Farbsichtgeräten oder auch, wenn man in die ferne Zukunft blickt, die direkte digitale Prozeßsteuerung sein.

Ausgehend von diesem Grundkonzept werden nun die einzelnen Funktionen bzw. Informationsziele durch eine geeignete Verknüpfung und Zusammenstellung sogenannter Ereignis-Bedingungs-Aktions-Sequenzen oder zusammengehörige Ströme von Ereignis-Bedingungs-Aktions-Sequenzen realisiert. Nachfolgend einige Beispiele bezogen auf die Funktionen, die im vorigen Kapitel beschrieben sind:

- Rechnergestütztes Betriebshandbuch

  Ereignis: Anstehen des Auslösesignals,

  Bedingung: Der Zustand der Prozeßvariablen bzw. die durch Logik aus diesen entstandenen, synthetischen Bedingungen

  Aktion: Ausgabe des zu konsultierenden Teils des Betriebshandbuchs

- Reduktion der Meldedichte

  Ereignis: Eine eventuell zu unterdrückende Meldung

  Bedingung: Ein ja/nein-Sperrkriterium

  Aktion: Unterdrückung bzw. Nichtunterdrückung des Ereignisses (der ursprünglichen Meldung)

- Post-Mortem-Analyse

  Ereignis: Auslöseereignis

  Bedingung: Überwachungszeitraum sowie Soll-Signal-Zustandbeschreibungen

  Aktion: Erzeugung und Ausgabe eines Protokolls der Ereignisse, die nach Beendigung des Überwachungszeitraums nicht auslegungsgemäß aufgetreten sind.

- Integrierte Störungsanalyse

  Ereignis: Änderung irgendeiner im Prozeßmodell verwendeten Prozeßvariablen (analog oder binär)

  Bedingung: Komplizierte synthetisierte Bedingungen, die den jeweiligen Anlagenzustand beschreiben bzw. mögliche Abweichungen davon

  Aktion: Generierung und Steuerung entsprechender Farbsichtgeräteinformation und/oder Meldungen auf entsprechenden Protokollen.

Diese Zusammenstellung von Ereignis-Bedingung-Aktions-Sequenzen muß letztlich ein Rechenprogramm verstehen und interpretieren können.

Repräsentationskonzept

Die Aufgabe war nun, ein Konzept zur Repräsentation der von den Verfahrenstechnikern gelieferten Ergebnisse zu erstellen, das es einerseits erlaubt, die Ergebnisse unmittelbar, wenn möglich automatisch, in eine vom Rechner interpretierbare Form zu bringen, andererseits den Verfahrenstechnikern nicht grundlegende Informatikkenntnisse abzunötigen.

Zunächst muß das von den Verfahrenstechnikern zu beschreibende Gebiet in Umfang und Bedeutung festgelegt werden. Dazu gehört zum Beispiel: Was ist als Ereignis zu betrachten? Welche Bedingungen müssen beschreibbar sein? Welches sind die primitiven (Bedeutungs-)Elemente (semantic primitives)? Dieser Satz von primitiven Elementen bestimmt die Möglichkeit dessen, was mit dem Gesamtsystem insgesamt bewirkt werden kann. Diese primitiven Elemente werden als Knoten eines Graphen aufgefaßt. Dieser logische bzw. chronologische Zusammenhang wird durch verbundene Kanten dargestellt. Primitive Elemente sind zum Beispiel ADD, MULT, AND, OR etc. Hinzu kommen aber auch noch die schon bei der integrierten Störungsanalyse erwähnten generischen Funktionen TREND, FILTER etc. Die primitiven Elemente (Funktionen) müssen durch Argumente versorgt werden, was, graphisch dargestellt, die Vorgänger des Funktionsknotens sind. Es gibt Anfangs- und Endknoten (solche ohne Vorgänger bzw. ohne Nachfolger). Die Ersteren müssen durch Elementarereignisse (Prozeßsignale) ausgewertet werden, die letzteren bewirken eine Ausgabe (Aktion).

Aufgabe der Systemanalyse ist es nun, die so identifizierten primitiven Elemente in einer Weise zusammenzufassen, daß die gewünschte Funktion realisiert wird:

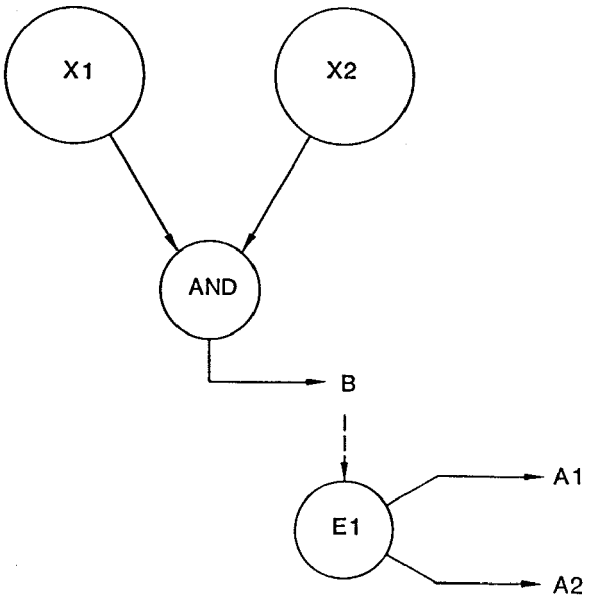


Bild 5: Graphische Darstellung der Ereignis-Bedingungs-Aktions-Sequenz

Beispiel Meldereduktion: Elementarereignisse X1 und X2 werden mit AND verknüpft, um die Bedingung B zu bilden. Falls E1 auftritt, werden, je nach dem, ob B=ja oder B=nein ist, die Aktionen 1 bzw. 2 ausgelöst (Bild 5).

Die schon erwähnten Funktionen TREND, FILTER etc. könnten auch mit primitiven AND, OR, ADD, MULT etc. realisiert werden. Dies würde jedoch den Schreibaufwand erhöhen, weshalb sie, da sie häufig verwendet werden, als eigene „primitive" eingebracht werden.

Die semantischen Primitiven bestimmen, was wirklich durchgeführt werden muß: AND (a, b) besagt zum Beispiel, daß die Argumente a und b, die zum Beispiel Prozeßsignale sein können, zu einem neuen Element durch eine logische Und-Verknüpfung vereinigt werden. Durch Schachtelung und Parallelanwendung, da die Argumente selbst wieder solche primitiven Funktionen sein können, können beliebige funktionelle Geflechte aufgebaut werden. Letztlich werden die Funktionen auf Standardfunktionen moderner Programmiersprachen abgebildet, wo sie dann vom Rechner effektiv ausgeführt werden können. Es muß jedoch betont werden, daß diese funktionellen Geflechte als Daten zu betrachten sind und nicht als Programme. Dies ist einer der wichtigen Punkte, da die von den Verfahrenstechnikern erarbeiteten Prozeßzusammenhänge in eine Datenbasis, das sogenannte Datenmodell (oder auch Wissensbasis in moderner Terminologie) eingebracht werden, so daß diese Daten dann in einem invarianten Programm in Abhängigkeit der aktuellen Prozeßdaten interpretiert werden können und die im Datenmodell spezifizierten Aktionen ausgelöst werden können.

Spezifikation, Projektierung und Implementierung des Datenmodells

Es wurde bereits erwähnt, daß die Verfahrenstechniker und Systemanalytiker keine Rechnerspezialisten sein müssen. Weiterhin wurden aus den von den Verfahrenstechnikern gelieferten Analysen die semantischen Primitiven identifiziert und abstrahiert. Was nun

noch fehlt, ist das „syntaktische Kleid" für die semantischen Primitiven. Sowohl die Erarbeitung der semantischen Primitiven, wie auch die syntaktische Repräsentation obliegt einer Person, die sowohl die Informatikseite, als auch die wesentlichen Punkte der Verfahrenstechnik beherrscht (in moderner Terminologie wäre dies der „Knowledge-Engineer"). Die syntaktische Repräsentation erfolgt durch eine formale Grammatik. Formale Grammatiken sind strukturelle Hilfsmittel, um (künstliche) Sprachen zu definieren und einen Algorithmus (parsing algorithm) bereitzustellen, der in der Lage ist, festzustellen, ob ein vorgelegter Satz aus der definierten Sprache stammt oder nicht, und der es erlaubt, die syntaktische Struktur des Satzes auf die identifizierten semantischen Primitiven abzubilden. Diesen Vorgang nennt man Übersetzung. Die Vorteile dieser Vorgehensweise sind:

- Der Systemanalytiker ist in der Lage, sich in seiner Terminologie auszudrücken.
- Der Übersetzungsvorgang kann automatisch erfolgen.
- Erweiterungen und Modifikationen der Sprachstruktur sind durch Werkzeuge aus der Informatik (Parser-Generatoren etc.) relativ leicht durchführbar.
- Aus der formalen Syntax der definierten Sprache kann automatisch ein syntaxgesteuerter Editor (STEP) erzeugt werden.

Bild 6 zeigt die Vorgehensweise für die Herstellung der Wissensbasis. Die bereits erwähnten semantischen Primitiven werden als Regeln einer formalen Grammatik syntaktisch dargestellt (eine solche Grammatik ist im Anhang gezeigt). Diese Regeln können nun, soweit syntaktisch erlaubt, in beliebiger Weise zusammengesetzt werden. Ein solcher Satz bildet zum Beispiel die Beschreibung eines Sperrkriteriums und des zugehörigen zu unterdrückenden Meldeereignisses. Diese Beschreibung kann, da sie formal erstellt ist, von einem Rechnerprogramm, dem sogenannten Modellgenerator (MOGEN) automatisch bearbeitet werden. Sie wird benutzt, um die Eingabe des Systemanalytikers auf die assoziierten semantischen Aktionen zu bilden. Diese semantischen Aktionen werden dann vom sogenannten Datenbasisinterpreter ausgeführt (sie übernächstes Kapitel „On-line-Interpretationssysteme"). Auf diese Weise haben die Verfahrenstechniker und Ingenieure volle Kontrolle darüber, was das Informationssystem als Ausgabe für den Operateur

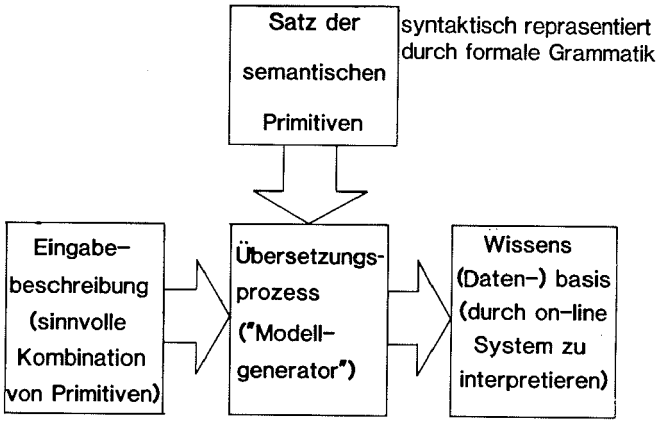


Bild 6: Formale Vorgehensweise

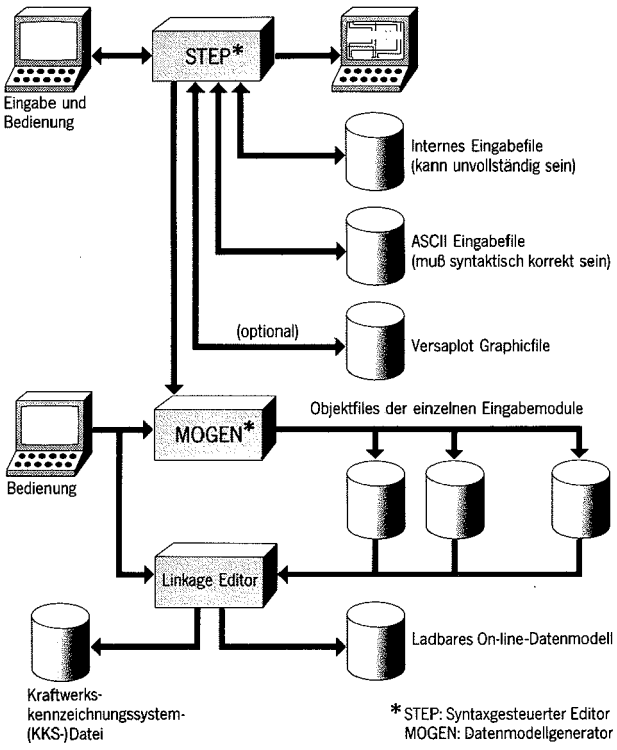


Bild 7: Implementierung des Datenmodells (Wissensbasis)

produzieren soll, sind auf der anderen Seite aber nicht genötigt, im Detail zu wissen, wie der Rechner diese Aufgabe durchführt.

Üblicherweise sind die aus der Systemanalyse stammenden Prozeßbeschreibungen umfangreich und komplex, so daß sie in kleinere Teile aufgeteilt werden müssen. Dies bedingt jedoch, daß sie, bevor sie on-line benutzt werden können zu einem gesamten Datenmodell zusammengebunden werden müssen. Die Vorgehensweise bei der Implementierung des gesamten Informationssystems wird unterstützt durch die bereits erwähnten Module

- syntaxgesteuerter Editor (STEP),
- Modellgenerator (MOGEN),
- Linkage-Editor (Bindeprogramm),
- Hilfsmittel zur grafischen Dokumentation.

All diese Werkzeuge garantieren, daß syntaktische Fehler unmöglich sind (es kann nichts syntaktisch Falsches eingegeben werden) und semantische Fehler (zum Beispiel der Versuch, ein Binärsignal und einen Analogwert zu addieren) weitestgehend entdeckt werden können. Auf dem Weg bis zur Erzeugung des sogenannten On-line-Datenmodells werden verschiedene Dateien erstellt, unter anderem für Archivierung und Dokumentation. Die Vorgehensweise bei der Implementierung der Datenbasis ist in Bild 7 dargestellt.

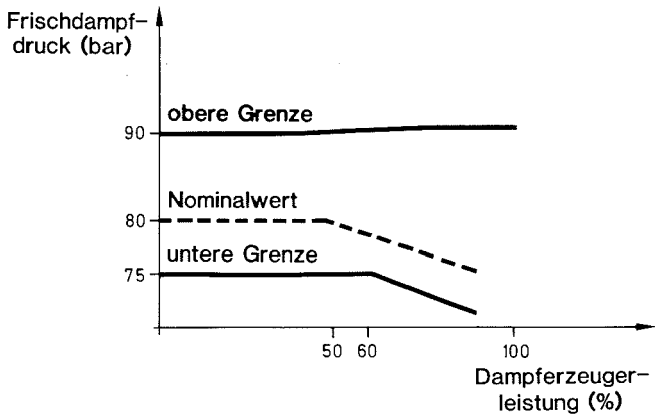


Bild 8: Kennlinien

Beispiel für die Eingabe einer Kennlinie

In Bild 8 ist die grafische Repräsentation von variablen Grenzwerten (Kennlinien) gezeigt. Üblicherweise werden die Werte zweier physikalischer Prozeßvariablen gemessen und stellen somit einen Punkt in der zweidimensionalen Ebene dar. Das Informationssystem muß nun den Punkt in dieser Ebene lokalisieren und feststellen, ob er innerhalb der spezifizierten Grenzen liegt. Im einfachen Fall wird das Ergebnis eine binäre Aussage sein (ja: liegt innerhalb des Kennlinienfeldes, nein: liegt nicht innerhalb dieses Bereichs). Dieses binäre Ergebnis kann im bereits beschriebenen Sinne wieder mit anderen logischen Signalen kombiniert werden, wie es in Bild 9 gezeigt ist. Die Verfahrenstechniker brauchen nicht zu wissen, wie das Ergebnis letztlich im Rechner hergestellt wird. Sie müssen aber alle notwendige Information liefern, so daß ihre Zielsetzungen erfüllt werden können (zum Beispiel müssen die Systemanalytiker die Grenzlinien angeben, den Anlagencode der physikalischen Variablen usw.). Wenn diese Information vorliegt, muß es dem Informationssystem mitgeteilt werden.

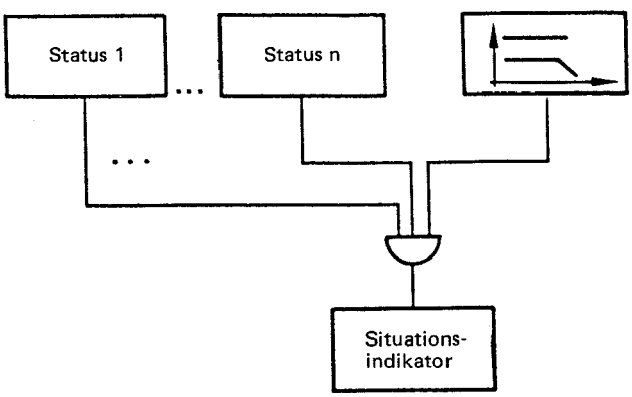


Bild 9: Synthetische Variable

Die von den Systemanalytikern gelieferte Spezifikation muß nun natürlich der bereits erwähnten (einfachen) formalen Sprache entsprechen. Das in Bild 8 gezeigte Kennlinienfeld würde in dieser Sprache wie folgt aussehen:

```
CHAR-CURVE (x,y)
*
      HYSTERRESIS: 0,5 %
      UPPER-BOUND: (0,90), (100, 90)
      LOWER-BOUND:(0,75), (60, 75), (100, 70)
      SCALE-Y:  0,5
*
```

Dieses Beispiel zeigt, wie wenig Eingabeinformation notwendig ist, um eine relativ komplexe Kennlinie zum Testen des Arbeitspunktes zweier Prozeßvariablen zu beschreiben. Diese Eingabe kann direkt von dem syntaxgesteuerten Editor STEP (bzw. dem Modellgenerator MOGEN) gelesen und in die benötigte Zieldatenstruktur übersetzt werden. Bemerkenswert in diesem Zusammenhang ist auch, daß einige Information zu fehlen scheint: Der Skalierungsfaktor auf der X-Achse. Dies ist eine weitere Vereinfachung des Eingabeaufwands, denn für häufig wiederkehrende Eingaben werden sogenannte Default-Werte eingesetzt. Aufgrund des verwendeten Konzepts der formalen Grammatik kann, obwohl keine Eingabe erfolgt ist, dennoch erkannt werden, an welchen Stellen solche absichtlich ausgelassenen Angaben entsprechend einzusetzen sind. In unserem Fall wäre der Default-Wert für den Skalierungsfaktor 1.0. Es sollte ebenso offensichtlich sein, daß die Beschreibung in Klartext erfolgt ist und damit eine leichte Überprüfbarkeit sowie Dokumentation der Eingabe gewährleistet ist.

On-line-Interpretationssystem

Die Informationssynthese bzw. die Erzeugung von Aktionen wird von den aus dem Prozeß kommenden Signalen in Abhängigkeit der abgespeicherten Modelle (Wissensbasis) durchgeführt. Wie bereits erwähnt, sind diese Aktivitäten nicht in Programmiersprachen wie zum Beispiel FORTRAN, PL/1, PASCAL, ADA, etc. geschrieben, sondern als Datentabellen abgespeichert worden. Dies ist notwendig, um einen programmäßig invarianten On-line-Datenbasisinterpreter anwenden zu können. Prüfbarkeit und Zuverlässigkeit der verfahrenstechnischen Modelle wären wesentlich eingeschränkt, wenn diese direkt in einer konventionellen Programmiersprache (was grundsätzlich möglich ist) geschrieben wären. Darüber hinaus würde es erfordern, daß die Systemanalytiker und Verfahrenstechniker Rechnerspezialisten (Programmierer) sind, und zur Folge haben, daß die erstellten Modelle die Zielsetzungen des rechnergestützten Informationssystems nicht mehr unmittelbar widerspiegeln würden. Weiterhin wäre die Programmgröße von der Größe des Datenmodells abhängig, was eine Reihe weiterer Probleme mit sich brächte. Zum Schluß wäre die Programmgeschwindigkeit, das heißt die Reaktion auf Prozeßereignisse weniger effektiv.

Bild 10 zeigt die wesentlichen Elemente des sogenannten On-line-Systems. Die On-line-Datenbasis enthält alle Information darüber, wie die Eingangssignale zu behandeln sind. Ein (meist prozeßabhängiges) Datenakquisitionssystem liefert diese Prozeßsignale in den sogenannten Ringspeicher 1. Wegen der Abhängigkeit des Datenakquisitionssystems der einzelnen Prozesse wurde mit dem Ringspeicher 1 eine generelle Schnittstelle geschaffen, die sich sehr leicht an alle möglichen Prozesse und Datenakquisitionssysteme anpassen läßt. Normalerweise wird davon ausgegangen, daß die Signalaufdatierung spontan erfolgt und im Bereich einer zeitlichen Auflösung von 2 bis 10 ms für binäre Signale und zwischen 1 und 60 s für Analogwerte auf einer zyklischen Basis liegt. Bild 10 zeigt auch, daß neben dem Auftreten von Signalen aus dem Prozeß auch eine Aufdatierung aus der sogenannten internen Ereigniswarteschlange (IEQ) möglich ist. Diese internen Ereignisse sind notwendig für die verzögerte Behandlung von Prozeßereignissen. Sie sind in der

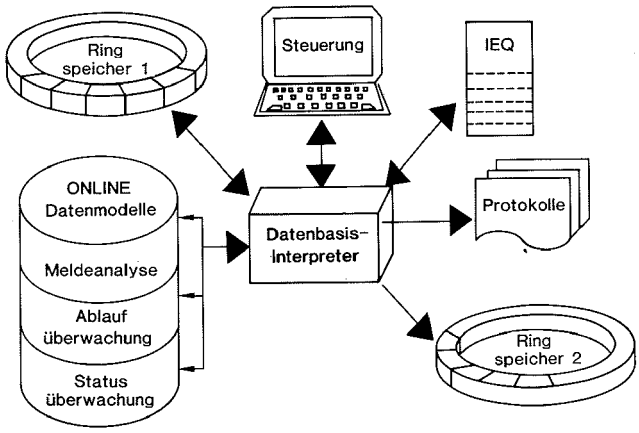


Bild 10: On-line-Interpretersystem

IEQ zusammen mit ihrer neuen Auftretenszeit abgespeichert und werden dann chronologisch in die aus dem Ringspeicher 1 auftretenden Prozeßsignale eingeschleust.

Jedes Ereignis aus dem Prozeß sowie aus der IEQ trägt die Zeit seines Auftretens und alle zeitabhängigen Berechnungen beziehen sich auf diese Prozeßzeit; dies im Gegensatz zur internen Rechnerzeit. Der Vorteil dieser Vorgehensweise ist, daß Inkonsistenzen aufgrund von starker Rechnerlast nicht mehr auftreten können und daß einmal abgelaufene Folgen wieder eingespielt werden können und exakt dieselben Ergebnisse zeitigen werden. Es gehen, auch bei starker Anforderung, vom Prozeß her gesehen keine Daten verloren oder werden geändert, einzig die Ausgabe kann in diesem Fall geringfügig verzögert erscheinen.

Der Datenbasis-Interpreter produziert entweder direkt lesbare Ausgabe (Protokolle) oder liefert synthetisierte Information in einem sogenannten Ringspeicher 2 ab, von wo aus eine spezielle Behandlung dieser Daten erfolgen kann (zum Beispiel Darstellung der Information auf einem Farbsichtgerät etc.).

Zusammenfassung

Das sogenannte STAR-GENERIS-Konzept umfaßt einen Satz von semantischen Primitiven, die notwendig sind, um komplexe Beschreibungen von Prozeß- und Datenverhaltensmodellen zu erstellen und zu interpretieren. Interessanterweise ist dieser Satz jedoch relativ klein. Für die Systemanalyse bedeutet dies, daß die Zielsetzungen ohne großes Verstehen des Computers realisiert werden können (im Gegensatz dazu muß der Prozeß jedoch genau verstanden werden).

Die Verfahrenstechniker, Systemanalytiker und Operateure werden damit in die Lage versetzt, ihr Wissen über Situationszusammenhänge oder Anlagenzustände in ein computerisiertes Informationssystem einzubringen und später, wenn die Situationen eintreten bzw. die Zustände vorherrschen, dieses Wissen zu nutzen. Einzig diese Vorgehensweise ermöglicht es, aus rohen Daten Information herzustellen. Darüber hinaus werden formale Werkzeuge (STEP, MOGEN, etc.) zur Verfügung gestellt, um das systemanalytische Wissen in komplizierte, vom Rechner interpretierbare Wissensbasen umzusetzen mit dem gleichzeitigen Vorteil einfacher Anpassungs- und Erweiterungsmöglichkeiten.

Das Softwarekonzept ist so ausgelegt, daß es auf den verschiedensten Rechnersystemen ohne großen Aufwand implementiert werden kann. Derzeit ist es auf den Rechnern

Norsk Data ND-500, Gould SEL 3227/3287 und, mit Einschränkung, der Amdahl 470 implementiert.

Um vernünftige Weiterentwicklungen von reinen Signalzustandsinformationssystemen über Informationsverarbeitungssysteme zu wissensverarbeitenden Systemen zu erhalten, erscheint eine zentrale Erfassung der Leistungsfähigkeit der bisherigen Wartungsinformation zusammen mit der Leistungsfähigkeit der automatischen Überwachungs-, Begrenzungs- und Abschaltsysteme unbedingt erforderlich. In der Bundesrepublik Deutschland gilt die Regel, daß bei allen Störfallabläufen Automatiken des Reaktorschutzsystems eingreifen müssen, wenn für die Einleitung einer Gegenmaßnahme weniger als 30 Minuten Zeit bleibt. Auch in der konventionellen Leittechnik sind zahlreiche Beispiele für die Realisierung komplexer Signalverknüpfungen zu finden. Diese könnten mit großer Wahrscheinlichkeit in zukünftiger NPgestützter Leittechnik billiger, gezielter eingesetzt und für den Operateur in ihrer aktuellen Wirkung transparenter dargestellt werden. Natürlich bedeutet der Einsatz der neuen Leittechnik ein hohes Maß an Umdenken für den Anwender. Bisherige Versuche mit zusätzlichen, für den Betrieb nicht unbedingt erforderlichen Anwendungen für Operateure, die in konventioneller Technik geschult wurden, brachten zwangsläufig stets mehr oder weniger große Akzeptanzprobleme mit sich. Die bisherige Anwendung ausschließlich der „neuen Leittechnik" in der chemischen Industrie zeigen allerdings, daß diese Akzeptanzprobleme aufgrund der Tatsache, daß die Operateure jünger sind und ausschließlich auf moderner Ausrüstung ausgebildet werden, nicht auftreten.

Anhang I

EDITED GRAMMAR

```
 1   COMP-UNIT ::= LOGIC _|
 2                 | OUTPUT-DESCRIPTOR _|_
 3   LOGIC ::= HEAD DESCRIPTOR
 4   HEAD ::= MODULNAME VERS DATE USER DBASE
 5   MODULNAME ::= MODUL : TEXT
 6   VERS ::= VERSION : UNSINT . UNSINT
 7   DATE ::= DATUM : DAY . MONTH . YEAR
 8   DAY ::= UNSINT
 9   MONTH ::= UNSINT
10   YEAR ::= UNSINT
11   USER ::= BEARBEITER : TEXT ABT ; TEXT
12   DBASE ::= DATEI : TEXT
13   DESCRIPTOR ::= ELEMENTS
14   ELEMENTS ::= ELEMENTS ELEMENT
15              | ELEMENT
16   ELEMENT ::= FUNCTION-GROUP ;
17             | INPUT-GROUP ;
18   INPUT-GROUP ::= INPUT-GROUP INPUT
19                 | INPUT
20   INPUT ::= NUM-ID <== ID
21   FUNCTION-GROUP ::= NUM-ID <== FUNCTION TRANSFER.
22   TRANSFER ::= ==>
23              |
24   FUNCTION ::= A-FUNCTION
25              | B-FUNCTION
26   A-FUNCTION ::= ADD ( A-ARGS , A-ARG )
27                | SUB ( A-ARG , A-ARG )
28                | MULT ( A-ARGS , A-ARG )
29                | DIV ( A-ARG , A-ARG )
30                | MAX ( A-ARGS , A-ARG )
31                | MIN ( A-ARGS , A-ARG )
32                | SWITCH ( A-ARG , B-ARG )
33                | ADELAY ( A-ARG ) D-DESCRIPTION
34                | ASTORE ( B-ARG , A-ARG )
35                | TIME ( T-ARG )
```

```
36   B-FUNCTION ::= NOT ( B-ARGS )
37                | AND ( B-ARGS , B-ARG )
38                | OR ( B-ARGS , B-ARG )
39                | CHAR-CURVE ( A-ARG , A-ARG ) C-DESCRIPTION
40                | LIM ( A-ARG ) L-DESCRIPTION
41                | EQ ( A-ARG , A-ARG )
42                | NE ( A-ARG , A-ARG )
43                | GE ( A-ARG , A-ARG )
44                | LE ( A-ARG , A-ARG )
45                | GT ( A-ARG , A-ARG )
46                | LT ( A-ARG , A-ARG )
47                | BDELAY ( B-ARG ) D-DESCRIPTION
48                | BSTORE ( B-ARG , B-ARG )

49   A-ARGS ::= A-ARGS , A-ARG
50            | A-ARG

51   B-ARGS ::= B-ARGS , B-ARG
52            | B-ARG

53   A-ARG ::= NUM-ID
54           | REAL
55           | A-FUNCTION

56   B-ARG ::= NUM-ID
57           | 0
58           | 1
59           | B-FUNCTION

60   T-ARG ::= NUM-ID
61           | ABS-TIME
62           | ID

63   C-DESCRIPTION ::= * HYST UB LB SCALE *

64   HYST ::= HYSTERESIS : REAL %

65   UB ::= UPPER-BOUND : COORDS

66   LB ::= LOWER-BOUND : COORDS

67   COORDS ::= COORDS , COORD
68            | COORD

69   COORD ::= ( REAL : REAL )

70   SCALE ::= SCALE-X : REAL SCALE-Y : REAL
71           | SCALE-X : REAL
72           | SCALE-Y : REAL
73           |

74   D-DESCRIPTION ::= * DTYPE *

75   DTYPE ::= REAL =>
76           | => REAL
77           | => REAL , REAL =>
78           | => REAL =>

79   L-DESCRIPTION ::= < REAL
80                   | > REAL
81                   | REAL <> REAL

82   ID ::= TEXT

83   NUM-ID ::= # UNSINT

84   SIGN ::= +

85           | -
86           |

87   INTEGER ::= SIGN UNSINT

88   UNSINT ::= DIGIT
89            | DIGIT DIGIT
90            | DIGIT DIGIT DIGIT
91            | DIGIT DIGIT DIGIT DIGIT
92            | DIGIT DIGIT DIGIT DIGIT DIGIT

93   REAL ::= INTEGER
94          | INTEGER . UNSINT
95          | INTEGER EXPONENT
96          | INTEGER . UNSINT EXPONENT

97   EXPONENT ::= E SIGN DIGIT
98              | E SIGN DIGIT DIGIT

99   TEXT ::= ' SYMBSEQ '

100  SYMBSEQ ::= SYMBSEQ SYMB
101            | SYMB

102  SYMB ::= LETTER
103         | DIGIT
104         | SPECCHAR

105  LETTER ::= A
106           | B
107           | C
108           | D
109           | E
110           | F
111           | G
112           | H
113           | I
114           | J
```

```
115                 | K
116                 | L
117                 | M
118                 | N
119                 | O
120                 | P
121                 | Q
122                 | R
123                 | S
124                 | T
125                 | U
126                 | V
127                 | W
128                 | X
129                 | Y
130                 | Z

131   DIGIT ::= 1
132           | 2
133           | 3
134           | 4
135           | 5
136           | 6
137           | 7
138           | 8
139           | 9
140           | 0

141   SPECCHAR ::= %
142              | #
143              | $
144              | &
145              | ?
146              | :
147              | ;
148              | _
```


Schrifttum

[1] Kay, P.C.M.; P.W. Heywood: Alarm Analysis and Indication at Oldbury Nuclear Power Station. IEE Conf. Publ. 16, Part I (1966).

[2] Felkel, L.; et al.: STAR - Ein rechnergestütztes System zur Online Störungsanalyse. GRS-A-483, Vol. 1-8 (1983).

[3] Meijer, C.H.; B. Frogner: On-line Power Plant Alarm and Disturbance Analysis System. EPRI-Report NP-1379, Palo Alto (1980),

[4] Øwre, F.; et al.: A Software Structure for Handling of Alarms Using Logic (HALO). Halden Work Report HWR 45, Halden, Norway (1982).

[5] Barr, A.; E.A. Feigenbaum: The Handbook of Artificial Intelligence, Vol. II Stanford CA, (1982)

[6] Long, A.B.: Technical Assessment of Disturbance Analysis Systems. Nuclear Safety Journal 21 (1980) 1

[7] Bastl, W.; L. Felkel: Disturbance Analysis Systems. In: Human Detection and Diagnosis of System Failures. J. Rasmussen, W.B. Rouse (Eds.) pp. 451 - 471, Plenum Publ. Corp. (1981). J. Rasmussen, W.B. Rouse, Eds., pp. 451 - 471, Plenum Publ. Corp., (1981).

[8] Grumbach, R.; H. Hoermann: Plant Disturbance Analysis by Process Computers. IAEA/NPPCI-Meeting, Neuherberg/München (1976).

Diskussion

P.H. Heldt (Deutsche Lufthansa):

Zum Stichwort „Schaue ins Betriebshandbuch" möchte ich meine Anregung geben, denn wir führen im Flugzeug ja auch eine Menge Betriebshandbücher mit. Da im Laufe der Jahre zu erwarten ist, daß auch Betriebshandbücher nicht mehr ohne Computer erstellt werden können, halten wir es für sinnvoll, uns hier des „Werkzeugs" eines modernen Datenbankmanagements zu bedienen. Das bedeutet, daß man per Bildschirm mit der „Datenbank Betriebshandbuch" komfortabel direkt weiterarbeiten kann. Im Flugzeug können wir uns das eines Tages vorstellen, und es scheint uns aus Benutzersicht auch recht attraktiv zu sein.

W. Bastl (GRS):

Das ist ein typisches Beispiel für einen transienten Zustand der Nutzungsmöglichkeiten des Computers. Diese Fahnen, die Abhaklisten, die mit unserem System computerisiert werden und schließlich angeben, wo man im Betriebshandbuch nachschauen muß, sind derzeit tatsächlich in Form von Diagrammen und Matrizen im Benutzerhandbuch vorhanden. Genau diesen Teil wollte man dem Computer überlassen, aber noch nicht den Textteil. Es liegt aber auf der Hand, daß es überhaupt kein Problem ist, den Text auch auszugeben.

L. Felkel (GRS):

Noch eine kurze Bemerkung zum Betriebshandbuch: Es wird in bezug auf die „Wissensbasis" oft danach gefragt, wer das, was darin steht, eigentlich verifiziert. Dort ist ja sehr viel Wissen gespeichert, das nicht unmittelbar nachvollziehbar ist. Auch das Betriebshandbuch ist eine Wissensbasis, und es muß auch dort eine Verifikation stattgefunden haben. Die Problematik ist an sich dieselbe, nur nicht mehr ganz so sichtbar für den rechnertechnischen Laien. Man kann bei im Rechner gespeicherten „Wissensbasen" aber sichtbar und plausibel machen, was damit newirkt wird oder von welchen Annahmen Aussagen abgeleitet werden. Dies ist für das Betriebshandbuch in die Operateurausbildung bzw. Training verlagert und nicht unbedingt vor Ort nachvollziehbar.

Überwachungs- und Diagnosesysteme zur Schadenfrüherkennung

Von R. Sunder und D. Wach[1])

Kurzfassung

Schädigungen und Anomalien in Kernkraftwerken bereits frühzeitig während des Normalbetriebs erkennen und diagnostizieren zu können, war die Zielsetzung von Methodenentwicklungen zur Schwingungs-, Schall- und Rauschsignalanalyse, die im letzten Jahrzehnt von GRS im Rahmen bundesgeförderter F&E-Vorhaben zusammen mit der Industrie durchgeführt wurden. Inzwischen sind entsprechende Systeme in allen deutschen Kernkraftwerken installiert. Zur Überwachung der Integrität des Primärkühlkreislaufs, speziell des Reaktordruckbehälters und seiner Einbauten, finden die dynamischen Signalanteile von Schwingweg-, Druck-, Neutronenfluß- und Beschleunigungsaufnehmern Verwendung. Da der wesentliche Unterschied zur vorhandenen Kraftwerksinstrumentierung in der stochastischen Natur der Signale liegt, ist der Einsatz statistischer Kennwerte und Funktionen erforderlich. Das Überwachungs- und Diagnoseprinzip basiert auf dem Vergleich aktueller Signaturen mit Referenzmustern. Die Interpretation dieser Musterfunktionen wird durch theoretische Modelle und Korrelationsanalysen der Meßsignale erreicht. Bei der Schwingungsüberwachung erfolgt die Analyse bevorzugt im Frequenzbereich, bei der Schallüberwachung liegt der Schwerpunkt bei Darstellungen im Zeitbereich. Der Nutzen der Diagnosesysteme konnte zwischenzeitlich durch die Betriebserfahrungen in mehreren Kraftwerksanlagen unter Beweis gestellt werden. Schädigungen wurden prognostiziert und konnten durch nachfolgende Inspektionen während Anlagenabschaltungen bestätigt werden. Beispiele derartiger Vorhersagen werden vorgestellt.

Abstract

Vibration, acoustic and noise analysis methods have been developed by GRS within R&D programs of the federal ministries and in cooperation with industry in the last decennium with the aim of incipient failure and malfunction detection during normal steady-state operation of nuclear power reactors. Based on these methods, monitoring systems were developed and installed in German plants. In order to monitor the integrity of primary circuit components, especially of the reactor pressure vessel and the internals, the dynamic signals of displacement, pressure, neutron and accelerometer sensors are used. The basic difference to normal plant instrumentation systems lies in the stochastic nature of the information sources used; therefore statistical quantities and functions have to be applied. The monitoring and diagnostic principle is based on the comparison of actual signatures with reference signatures. The interpretation of these signatures is done by means of theoretical models and correlation analysis of measured signals. In vibration monitoring emphasis is laid on frequency domain analysis, in acoustic monitoring on time domain analysis. Meanwhile operational experience in several plants has proved the usefulness of the diagnosis systems. Failures could be predicted and were confirmed by inspections in the subsequent shutdown periods. Examples of such predictions are given.

Einleitung

Die Vielfalt der neuen technischen Möglichkeiten, die aufgrund der Entwicklungen der modernen Elektronik und Rechnertechnik dem planenden und entwickelnden Ingenieur

---

[1]) Dipl.-Ing. Reinhold Sunder und Dr.-Ing. Dieter Wach, Gesellschaft für Reaktorsicherheit (GRS) mbH, Garching

heute zur Verfügung steht, ist in den bisherigen Beiträgen des GRS-Fachgespräches bereits deutlich geworden. Bei Kernkraftwerken lag der Schwerpunkt der in den letzten Jahren neu realisierten leittechnischen Einrichtungen eindeutig an der Schnittstelle zwischen Mensch und Maschine, das heißt bei den Informationssystemen. Mit ihnen können die Zustände des Prozesses und der Systeme dem Reaktoroperateur wesentlich besser, übersichtlicher und den menschlichen Fähigkeiten angepaßt vermittelt werden.

Eine Teilgruppe der neuen Informationssysteme, die sich jedoch durch die Natur der zugrundeliegenden Meßinformationen und die dafür erforderlichen Analysetechniken von den übrigen unterscheidet, sind die Überwachungs- und Diagnosesysteme zur Schadenfrüherkennung an Reaktorkomponenten. Bei ihnen wird – ähnlich wie bei ambulanten Diagnosetechniken des Arztes – aus Messungen von außen auf Unregelmäßigkeiten im Innern zurückgeschlossen. Zur Signalanalyse müssen allerdings wesentlich aufwendigere Verfahren eingesetzt werden: Die Berechnung von statistischen Kennwerten, der Einsatz von Korrelationsanalyseverfahren oder die Bereitstellung von vielkanaligen hochaufgelösten Signaldarstellungen erfordern spezielle Analysatoren oder rechnergestützte Systeme, mit denen die Daten so aufbereitet und reduziert werden, daß dem Reaktorfahrer oder dem Diagnosespezialisten rasch eine Beurteilung wichtiger Merkmale oder Signalmuster möglich ist. Man kann sogar sagen, daß erst durch die nun verfügbare neue Elektronik und Rechnertechnik der Einsatz dieser Verfahren in einem wirtschaftlich angemessenen Aufwand realisierbar geworden ist.

Bereits im GRS-Fachgespräch 1980 war über diese – damals neuen – Überwachungssysteme in Kernkraftwerken berichtet worden [1]. Inzwischen haben die Systeme allgemein Eingang in die kerntechnische Praxis gefunden ([2] bis [4]) und sind in Ergänzung zu den bisherigen qualitätssichernden Maßnahmen am Reaktorprimärkreis getreten (Bild 1). Der vorliegende Beitrag diskutiert die benutzten Meßprinzipien, die realisierten Systeme und den Stand der Einsatzpraxis. Beispiele erfolgreicher Diagnosen verdeutlichen den Nutzen, den die Systeme schon heute in der Praxis unter Beweis stellen konnten, indem sie abseits von spektakulären Störungen im Vorfeld größerer Beschädigungen rechtzeitig Hinweise gaben.

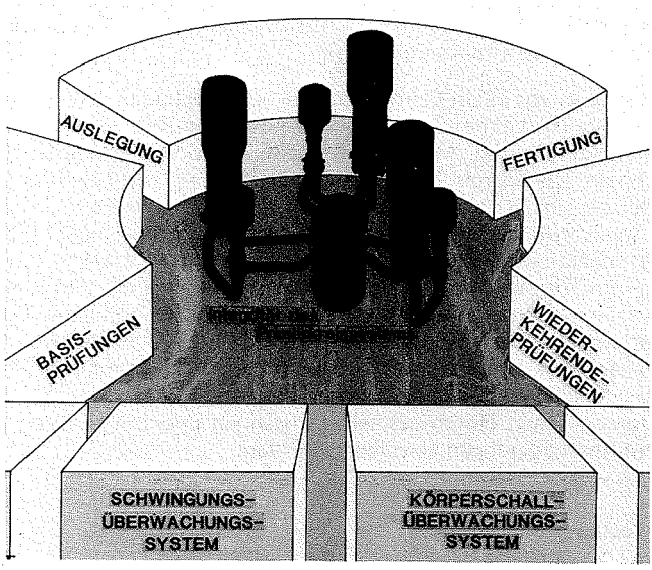


Bild 1: Einordnung der neuen Überwachungs- und Diagnosesysteme

Meßmethoden

Eine wichtige Randbedingung bei der Entwicklung von Meßmethoden zur Schadenfrüherkennung war die aus Betriebs- und Sicherheitsüberlegungen resultierende Forderung, nach Möglichkeit keine zusätzlichen Meßfühler innerhalb der druckführenden Komponenten anzubringen. In der Praxis bedeutete dies, daß zumindest für die Überwachung von Reaktoreinbauten indirekte Meßverfahren zum Einsatz kommen mußten, das heißt, daß auf Vorgänge im Innern aus Messungen an der Außenwand oder aus Sekundäreffekten der bereits vorhandenen Betriebsinstrumentierung geschlossen werden mußte. Ferner sollte die Überwachung möglichst global sein und alle Reaktoreinbauten und Primärkreiskomponenten einschließen, ohne den Aufwand bei der Instrumentierung zu hoch zu treiben. Die genannten Anforderungen und Zielsetzungen führten zu systemtechnischen Lösungen, bei denen eine Kombination von Schwingungs-, Rauschsignal- und Schallüberwachung zum Einsatz kommt. Die beiden ersteren sind in „Schwingungsüberwachungssystemen" zusammengefaßt, letztere wird durch „Körperschallüberwachungssysteme" realisiert [5].

Ziel der *Schwingungsüberwachung* ist es, im Bereich des Primärkreissystems von Kernkraftwerken sich anbahnende mechanische Schäden so rechtzeitig an einem geänderten Betriebs-Schwingungsverhalten zu erkennen, daß ein weiteres Anwachsen noch vor unmittelbaren Konsequenzen für den Betrieb bzw. noch vor Folgeschäden durch geeignete Maßnahmen verhindert werden kann. In der Praxis werden hierzu diskontinuierlich Messungen – meist drei pro Brennelementzyklus – durchgeführt. Für die Auswertung werden die Signale in den Frequenzbereich transformiert und statistische Kennfunktionen wie Leistungsdichten, Kohärenzen und Phasenbeziehungen der Signale untereinander berechnet. Sie werden daraufhin untersucht, ob sich Resonanzstellen (nachfolgend Peaks genannt), die mechanische Eigenfrequenzen der Struktur repräsentieren, in bezug auf Lage und Intensität geändert haben. Werden Änderungen im Schwingungsverhalten gefunden, so müssen das Bauteil und die Schadensmechanismen identifiziert werden, die für die Veränderungen verantwortlich sind. Werden mechanische Schäden, die das Schwingungsverhalten beeinflussen und sich meist langsam anbahnen, frühzeitig erkannt und Trends in der Schadenentwicklung durch gezielte und häufigere Schwingungsmessungen beobachtet, steht einem weiteren Betrieb der Anlage bis zur nächsten geplanten Revision meist nichts im Wege. Bis dahin können dann auch entsprechende Ersatzteile bzw. Reparaturgeräte, wie Manipulatoren, bereitgestellt werden.

Die *Schallüberwachung* ist vor allem dann gefordert, wenn Schäden prompt auftreten. Das Meßprinzip beruht darauf, die Betriebsgeräusche kontinuierlich auf Veränderungen hin zu überwachen. Schalldetektoren an der Außenseite der druckführenden Umschließung des Reaktors nehmen die durch die Kühlmittelströmung verursachten Hintergrundgeräusche auf. Werden im Kühlmittelstrom abgelöste oder lockere Teile bewegt, so schlagen diese an der Umschließung oder an Einbauten an. Diese metallischen Schlaggeräusche führen zu Schallimpulsen, die sich durch die Struktur bis hin zum Aufnehmer ausbreiten und sich im Körperschallsignal als mehr oder weniger das Hintergrundgeräusch übersteigende Kurzzeitereignisse (nachfolgend Bursts genannt) abbilden. Die Erkennung und Identifikation eines solchen Schadens sowie eine entsprechende Reaktion auf ihn müssen rasch erfolgen. Aus diesem Grunde werden Signalerfassung und Grenzwertüberwachung in Körperschallüberwachungssystemen kontinuierlich während des gesamten Reaktorbetriebs durchgeführt. Durch schnelles Erkennen und Lokalisieren kleiner Schäden können größere Beschädigungen vermieden werden.

Schwingungsüberwachung

Schwingungsüberwachungsverfahren sind in nichtnuklearen Bereichen der Technik vor allem von aktiven Systemen – meist rotierenden Maschinen – bekannt. Beim Primärkreis-

system von Kernkraftwerken handelt es sich hingegen mit Ausnahme der Hauptkühlmittelpumpen um passive Komponenten, bei denen sich Schwingungen im wesentlichen durch das Umwälzen des Hauptkühlmittels in Verbindung mit einer pendelnden Komponentenlagerung ausbilden. Ferner ergeben sich aufgrund der komplexen Beschaffenheit der Komponenten sowie aufgrund der Notwendigkeit zur indirekten Messung von Einbautenschwingungen andere Problemstellungen als bei rotierenden Maschinen: Die eindimensionale Meßtechnik, das heißt die Erfassung und Amplitudenüberwachung einzelner Meßsignale für sich allein, spielt nur bei gezielten Einzelfragestellungen, zum Beispiel Überwachung einer speziellen Komponentenschwingung, eine Rolle. Bei der hier erforderlichen multisensoriellen Meßtechnik tritt die simultane Verarbeitung der Signale und die Nutzung ihrer Verbundinformation in den Vordergrund.

Seit April 1984 ist die Forderung nach einer geeigneten Schwingungsüberwachung in der KTA-Regel 3204 „Reaktordruckbehälter-Einbauten" niedergelegt. Im folgenden sind die wesentlichen Forderungen zusammengestellt:

- Zur frühzeitigen Erkennung von Veränderungen im Schwingungsverhalten der RDB-Einbauten sind diese während des Betriebes zu überwachen.
- Die Schwingungsüberwachung muß jederzeit durchgeführt werden können. Sie darf diskontinuierlich erfolgen.
- Es sind mindestens drei Messungen je Brennelementzyklus bei stationärem Betrieb der Kraftwerksanlage erforderlich.
- Maßnahmen bei festgestellten Veränderungen im Schwingungsverhalten der RDB-Einbauten sind anlagenspezifisch festzulegen.

Nachdem der Prototyp eines Schwingungsüberwachungssystems (SÜS) 1975 am Reaktor des Gemeinschaftskernkraftwerkes Neckar (GKN) eingerichtet wurde und bereits in den ersten Betriebsjahren sehr gute Betriebserfahrungen lieferte, sind heute Schwingungsüberwachungssysteme an allen modernen deutschen Kernkraftwerken mit Druckwasserreaktor standardmäßig installiert (Bild 2).

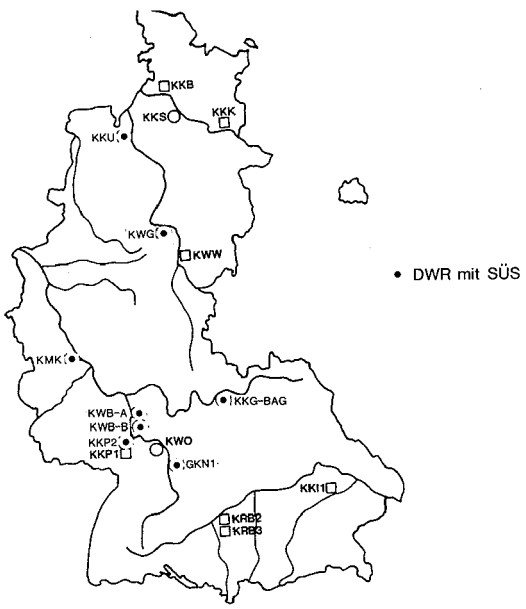


Bild 2: Einsatz von Schwingungsüberwachungssystemen in der Bundesrepublik Deutschland

Meß- und Analyseeinrichtungen

Die Meßeinrichtung eines modernen Schwingungsüberwachungssystems am Primärkreis eines Druckwasserreaktors besteht aus Meßwertaufnehmern im Containment und Datenaufbereitungs- und Analyseeinheiten im Wartennebenraum. Die dazwischen liegenden mehrere 100 m langen Signalleitungen müssen durch das Containment geführt und durch gezielte Abschirmmaßnahmen vor Störeinstreuungen geschützt werden. Als Meßgrößen finden sowohl die Signale von speziell für SÜS-Aufgaben installierten Schwingungs- und Drucksensoren, als auch die von Betriebsmeßstellen ausgekoppelten und nachverstärkten dynamischen Anteile der Neutronenflußsignale Verwendung.

Die SÜS-Standardinstrumentierung am Beispiel eines 4-Loop-Druckwasserreaktors umfaßt folgende Signalgeber:

- vier Absolutschwingwegaufnehmer am Reaktordruckbehälter (A1... A4),
- acht Relativschwingwegaufnehmer an den vier Hauptkühlmittelpumpen (R1R, R1D ... R4R, R4D),
- acht Relativschwingwegaufnehmer an den vier Austrittsleitungen (R1H, R1V ... R4H, R4V),
- fünf Druckaufnehmer in vier Eintrittsleitungen und einer Austrittsleitung (P1E ... P4E, P3A),
- acht Neutronenflußdetektoren der Außeninstrumentierung (X10, X1U ...X40, X4U).

Die Aufnehmerpositionen – und bei den Relativschwingwegaufnehmern auch ihre Meßrichtung – sind in Bild 3 in eine Primärkreissystem-Isometrie eingetragen. Die Aufgabenstellung bzw. die Charakteristik der einzelnen Sensorgruppen kann wie folgt umrissen werden:

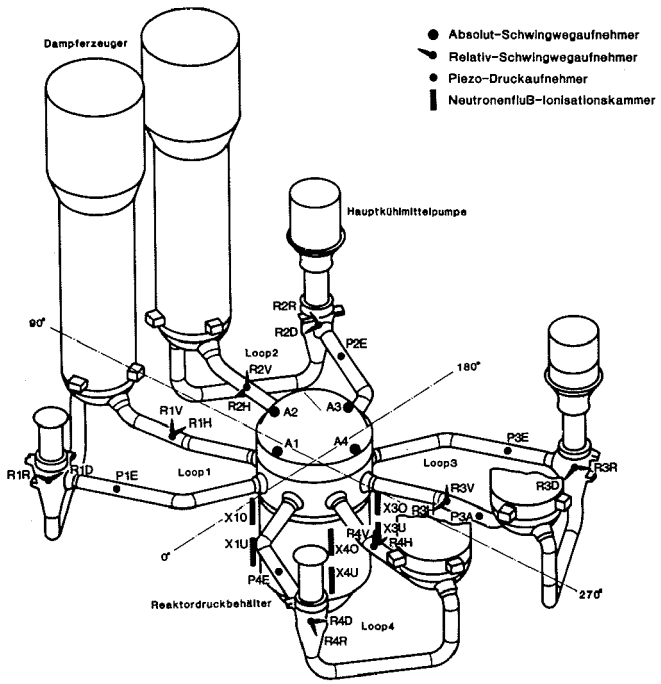


Bild 3: SÜS-Standardinstrumentierung an 4-Loop-Druckwasserreaktoren

Die mechanischen Schwingungen des Reaktordruckbehälters werden durch vier Schwingwegaufnehmer am Reaktordeckel gemessen. Die Sensoren sind jeweils 90° versetzt angeordnet; die Meßrichtung ist vertikal. Die Schwingwegaufnehmer, eine Spezialentwicklung der KWU sind tiefabgestimmte seismische Systeme mit einer Resonanzfrequenz von etwa 6 Hz, die ferngesteuert kalibriert und auf Null abgeglichen werden können. Ein elektrisches Entzerrernetzwerk ermöglicht eine amplitudenrichtige Wegmessung von 0,5 bis 200 Hz.

Die Schwingungen der Hautkühlmittelpumpen und Dampferzeuger werden an hierfür besonders geeigneten Positionen in den Loops erfaßt. Als Kompromiß zwischen optimaler Beobachtbarkeit von Schwingungsvorgängen und der eingeschränkten Zugänglichkeit zur Aufnehmeradaption haben sich Meßpositionen am Pumpenaggregat selbst und an der Austrittsleitung in Nähe des Dampferzeugers als praktikabel erwiesen. An der Hauptkühlmittelpumpe werden relativ zu einem Gebäudefestpunkt in zwei horizontalen, zueinander senkrecht stehenden Richtungen die Gehäuseschwingungen gemessen. Schwingungen von Dampferzeugern und Hauptkühlmittelleitungen werden mit den horizontal und vertikal orientierten Aufnehmern an der Austrittsleitung erfaßt. Als Sensoren werden Relativwegaufnehmer nach dem Tauchspulenprinzip eingesetzt. Sie arbeiten im Frequenzbereich von 0 bis 200 Hz.

Zur Messung der Druckfluktuationen in den Eintrittsleitungen bzw. der Austrittsleitung sind dynamische Piezo-Druckaufnehmer installiert. Impedanzwandler möglichst nahe am Aufnehmer machen aus den druckproportionalen Ladungsschwankungen der Geber ein Wechselspannungssignal, ein Tiefpaßfilter dient zur Ausblendung der akustischen Resonanzen der Gebereinbauvorrichtung. Die Signale sind im Bereich 1 Hz bis etwa 500 Hz verwendbar. Der dynamische Anteil der Betriebs-Drucksignale kann für Aufgaben der Schwingungsüberwachung nicht genutzt werden, da die Resonanzen der hierfür verwende-

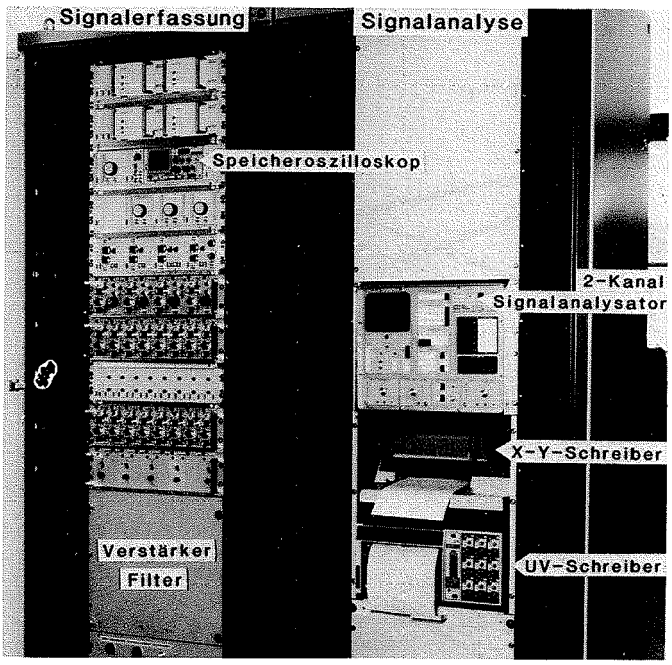


Bild 4: SÜS-Signalanalyseschränke zur Auswertung vor Ort (KWU-System)

ten Bartonzellen bei 18 bis 20 Hz und somit in dem für die zu beobachtenden Bauteilschwingungen interessanten Bereich liegen.

Die dynamischen Signalanteile der Excore-Neutronenflußsignale werden durch schnelle Trennverstärker und eine Hochpaßschaltung mit 0,2 Hz Eckfrequenz aus der Betriebsmessung ausgekoppelt. Bei der Analyse werden die Spektren auf den Gleichanteil des Flusses normiert – damit werden sie unabhängig von dem momentan gefahrenen Absolutwert der Reaktorleistung.

Ein vollständig ausgestattetes SÜS eines modernen Druckwasserreaktors umfaßt somit über 30 Meßsignale. Alle diese Signale liegen in einem Signalaufbereitungsschrank im Wartennebenraum auf. Der Schrank beinhaltet außerdem die Hochpaßfilter/Verstärkerkarten für die Excore-Neutronenflußsignale, die Trägerfrequenz- und Korrekturverstärker für die RDB-Absolutschwingwegaufnehmer, die Trägerfrequenzverstärker für die Relativschwingwegaufnehmer und die Verstärker, Kalibrier- und Filtereinheiten für die Drucksignale. Über eine Rangiereinheit lassen sich je zwei der SÜS-Signale in den benachbarten Analyseschrank (Bild 4) schalten, dessen wichtigste Komponenten ein Oszilloskop, ein Spektrum-Analysator sowie Speicher- und Registriergeräte sind. Mit den vorhandenen Geräten sind gezielte vor Ort-Analysen durchführbar. Auf der Rückseite der Rangiereinheit können alle SÜS-Signale parallel für Bandaufzeichnungen abgegriffen werden.

Wie bereits erwähnt, werden im Normalfall drei Messungen pro Brennelementzyklus durchgeführt. Um die große Zahl von Signalen zeitsynchron auf Band nehmen zu können, hat es sich bewährt, die Pulse-Code-Modulationstechnik (PCM) anzuwenden: Die analogen Zeitsignale werden digitalisiert und bis zu acht von ihnen gestaffelt in einen Zeitrahmen geschrieben (Multiplexbetrieb). Damit ist es möglich, acht Analogsignale digital auf eine Spur eines Analog-Magnetbandsystems exakt zeitrichtig und korrelierbar zu schreiben.

Bei den erfaßten Signalen handelt es sich um stochastische, das heißt regellose Signale, denen zum Teil deterministische Anteile überlagert sein können. Von derartigen Signalen

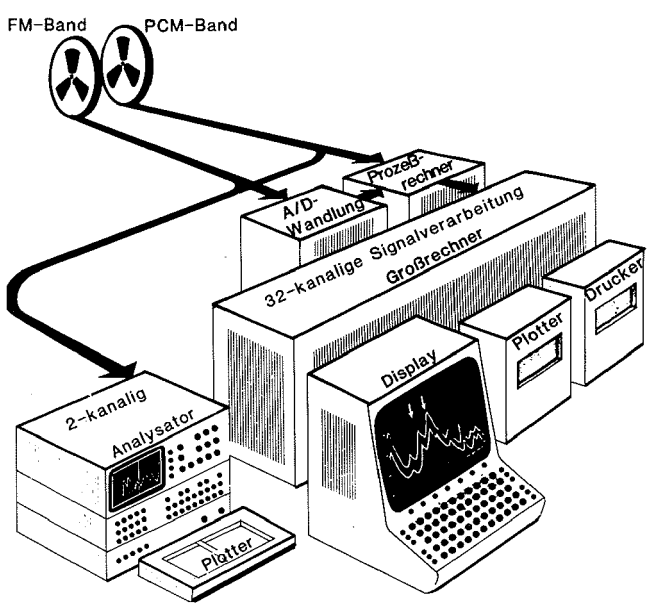


Bild 5: Rechner und Signalanalysatoren zur Off-line-Analyse im Labor (GRS-Systemkonfiguration)

lassen sich Kennwerte oder Musterfunktionen ermitteln. Den mathematischen Hintergrund, auf dessen Darstellung hier bewußt verzichtet wurde, liefert die Korrelationsanalyse, die im Zeit- oder Frequenzbereich durchgeführt werden kann. Die in der Praxis wichtigsten Musterfunktionen sind die Spektraldichtefunktionen (zum Beispiel Autoleistungsdichtespektren, ALDS), kurz Spektren genannt, die die Fouriertransformation der Korrelationsfunktionen darstellen. Andere Musterfunktionen, mit denen wechselseitige Abhängigkeiten festgestellt werden können, sind Kreuzspektraldichte-, Kohärenz-, Phasen- oder Übertragungsfunktionen. Diese Musterfunktionen sind von Messung zu Messung auf Veränderungen hin zu überwachen.

Die hierzu nötige Signalverarbeitung ist relativ zeitintensiv, da für jedes Spektrum mehrere Minuten des Originalsignals verarbeitet werden und eine sehr große Anzahl von Signalbeziehungen als Informationsbasis gefordert ist. Zur off-line-Auswertung wird deshalb bei GRS vorwiegend eine Analysesoftware eingesetzt, die eine synchrone Verarbeitung von 32 Meßsignalen in einem Rechenlauf gestattet, wobei anschließend eine Auswahl von gewünschten Korrelationsbeziehungen für Detailanalysen unmittelbar zur Verfügung steht. Zwei-Kanal-Analysatoren gelangen vorwiegend für transiente Vorgänge (Kaskadendarstellung, Histogramme) mit begrenzter Signalpalette zum Einsatz. Die GRS-Gerätekonfiguration zur SÜS-Signalanalyse ist in Bild 5 zusammengestellt.

Informationsgehalt und Interpretation der Signale

Entsprechend den unterschiedlichen Meßgrößen, Meßorten und Meßprinzipien erfassen die verschiedenen Signaltypen Einbauten- und Komponentenschwingungen in unterschiedlicher Weise und mit unterschiedlicher Intensität.

Um den Informationsgehalt der Signale zweifelsfrei zu separieren, ist eine abgestufte Vorgehensweise erforderlich, die sich in drei Arbeitsschritte einteilen läßt:

- Auswertung von Inbetriebnahmemessungen an sogenannten Prototyp-Anlagen mit einer temporär vorhandenen RDB-Inneninstrumentierung,
- Korrelationsanalysen der zur Verfügung stehenden SÜS-Signale zum Nachweis charakteristischer Schwingungsformen,
- Strukturmodelle zur Simulation der strukturmechanischen Vorgänge.

Inbetriebnahmemessungen wurden bei Druckwasserreaktoren mit Prototypcharakter (zum Beispiel erste 3-Loop-Anlage, erste 4-Loop-Anlage, erster RDB mit Siebtonne . . .) mit einer zum Teil sehr umfangreichen RDB-Einbauten-Instrumentierung durchgeführt. Der große Vorteil liegt darin, daß direkt an den Komponenten das Strukturverhalten in Form von Schwingwegen, Schwinggeschwindigkeiten oder Beschleunigungen erfaßt wird, und somit eine eindeutige Zuordnung von dominierenden Schwingungsmodes erreicht wird. Bild 6 zeigt eine Auswahl von Meßwertaufnehmern innerhalb des Reaktordruckbehälters bei der Inbetriebnahmemessung des Kernkraftwerks Biblis, Block A. Steht gleichzeitig mit der Inneninstrumentierung ein RDB-Deckelsignal zur Verfügung, kann beispielsweise der Nachweis von Einbautenschwingungen in dieser Außeninstrumentierung geführt werden (Bild 7): Bei Korrelation eines Aufnehmers am Kernschemel (R22) mit einem Schwingwegsignal am RDB-Deckel (A4) wird eine Reihe von Frequenzpeaks mit relativ hoher Kohärenz in beiden Signalen nachgewiesen. Diese relativ hohen Kohärenzwerte haben ihre Ursache in einer engen statistischen Abhängigkeit beider Signale. Als Ursache hierfür sind in erster Linie Eigenmoden von Strukturschwingungen des Reaktordruckbehälters oder des Schemels zu nennen, so zum Beispiel die Biegeschwingung des Kernschemels bei 36 Hz. Auf diese Weise wird der Nachweis erbracht, daß das Schemelschwingungsverhalten mit der RDB-Außeninstrumentierung überwacht werden kann.

Korrelationsanalysen der SÜS-Signale dienen darüber hinaus aber auch zum Nachweis von Schwingungsmodes, die aus dem Autoleistungsdichtespektrum allein nicht separierbar

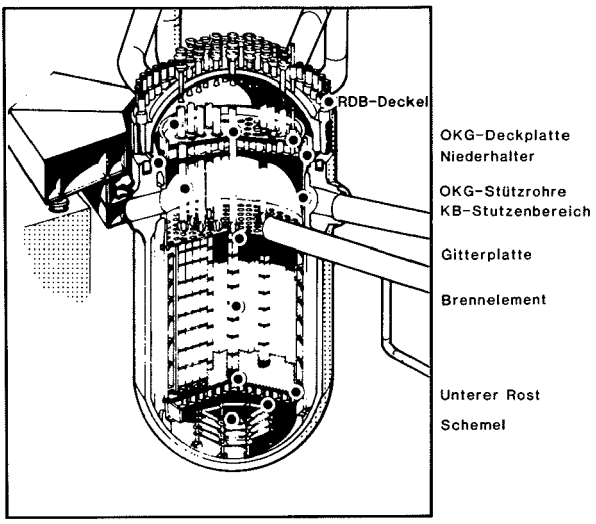


Bild 6: RDB-Inneninstrumentierung für Inbetriebnahmemessungen von Prototyp-Druckwasserreaktoren

sind. Dies gilt insbesondere für die Untersuchung von Neutronenflußsignalen und den darin enthaltenen Kernbehälter- und Brennelementschwingungseinflüssen: Die im biologischen Schild positionierten Detektoren messen Leckageneutronen, die den Kern verlassen und ein Maß für die Reaktorleistung sind. Beim Durchdringen der verschiedenen Wasserschichten und Behälterwände werden die Neutronen abgebremst. Führt nun eine Komponente Schwingungen aus, die einen Wasserspalt verändern, so wird der durchtretende Neutronenstrom durch unterschiedliche Abschwächungen moduliert, das heißt, der Schwingungsvorgang bildet sich im Neutronenrauschen ab. In Bild 8 ist die Verteilung des thermischen Neutronenflusses zwischen dem Reaktorkern und einem Detektor in radialer/azimutaler Abhängigkeit dargestellt.

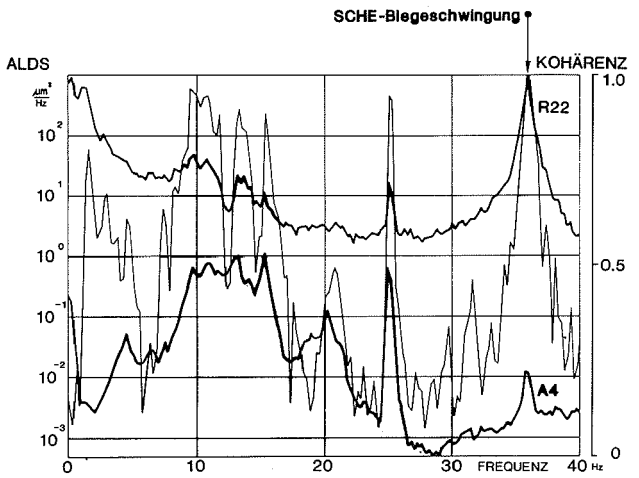


Bild 7: Nachweis von Einbauten-Resonanzen in der Außeninstrumentierung durch Korrelation mit der Inneninstrumentierung

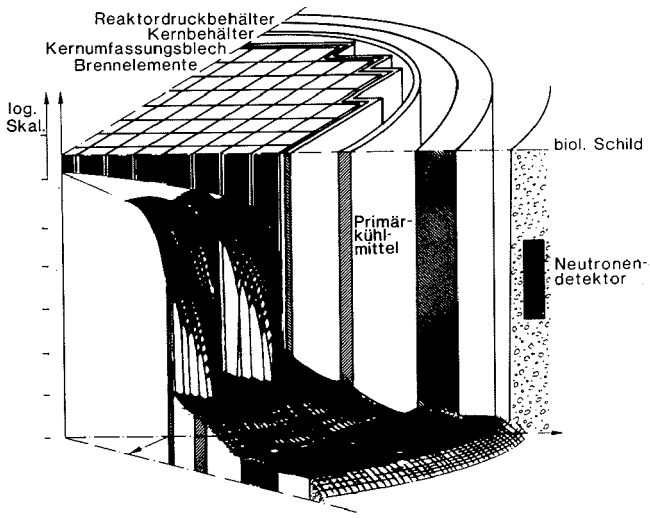


Bild 8: Radiale und azimutale Flußverteilung zwischen Reaktorkern und Detektor

Als wesentliches Kriterium zur Separierung zum Beispiel des Schalenmodes des Kernbehälters kann das Phasenverhalten der um 90° am RDB-Umfang versetzten Ionisationskammern gelten: Verformt sich der Kernbehälter zu einer Ovalisierungsschwingung, so wird zu diesem Zeitpunkt an zwei gegenüberliegenden Seiten der Wasserspalt RDB/KB vergrößert, 90° versetzt zu dieser Schwingungsebene verringert sich der Wasserspalt dementsprechend. Somit zeigen gegenüberliegende Neutronenflußsignale Gleichphasigkeit, 90° versetzt positionierte Signale sind jeweils gegenphasig. Bild 9 veranschaulicht diesen Sachverhalt am Beispiel des 3-Loop-Druckwasserreaktors GKN: Bei 23,5 bis 24,5

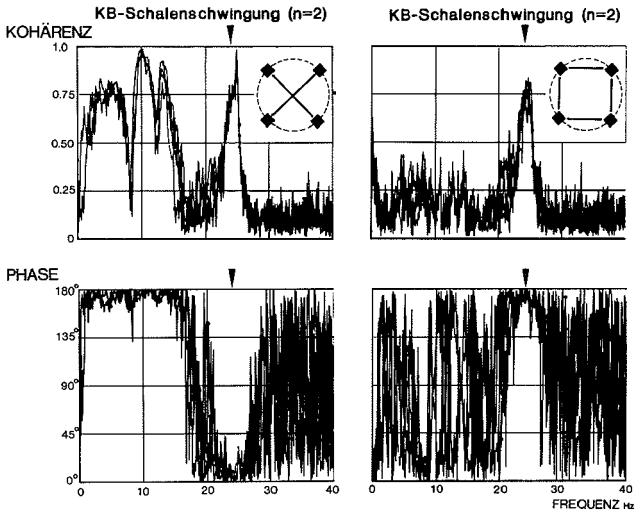


Bild 9: Kohärenz und Phasenspektren gegenüberliegender und benachbarter Excore-Neutronenflußsignale

Hz ist der Ovalisierungs-Schalenmode des Kernbehälters (n=2) in den Phasenbeziehungen der Außeninstrumentierung nach oben genannter Beziehung eindeutig erkennbar. Die Signalkombinationen sind jeweils den Einschüben in den Kohärenzspektren (rechts oben) zu entnehmen.

Strukturmodelle des Primärkreissystems werden entwickelt, um das globale und meßtechnisch erfaßbare Schwingungsverhalten der Bauteile hinreichend genau beschreiben, bzw. postulierte Schädigungen in ihren Auswirkungen auf das Schwingungsverhalten simulieren zu können.

Der massive Aufbau der wesentlichen Strukturkomponenten sowie der betrachtete Frequenzbereich erlauben für den Druckwasserreaktor eine Beschreibung als Balkenmodell mit Massenkonzentrationen in den Komponentenschwerpunkten. Infolge der relativ guten mechanischen Kopplung zwischen dem Reaktordruckbehälter und den Primärkreiskomponenten Dampferzeuger und Hauptkühlmittelpumpen über die Hauptkühlmittelleitungen wurde die Integration aller Komponenten in ein Primärkreismodell erforderlich. Das Strukturmodell für eine 4-Loop-DWR-Anlage (RDB mit Siebtonne und somit ohne Schemel) umfaßt folgende Komponenten (Bild 10):

- Reaktordruckbehälter,
- Kernbehälter,
- Oberes Kerngerüst,
- Kern,
- vier Dampferzeuger,
- vier Hauptkühlmittelpumpen.

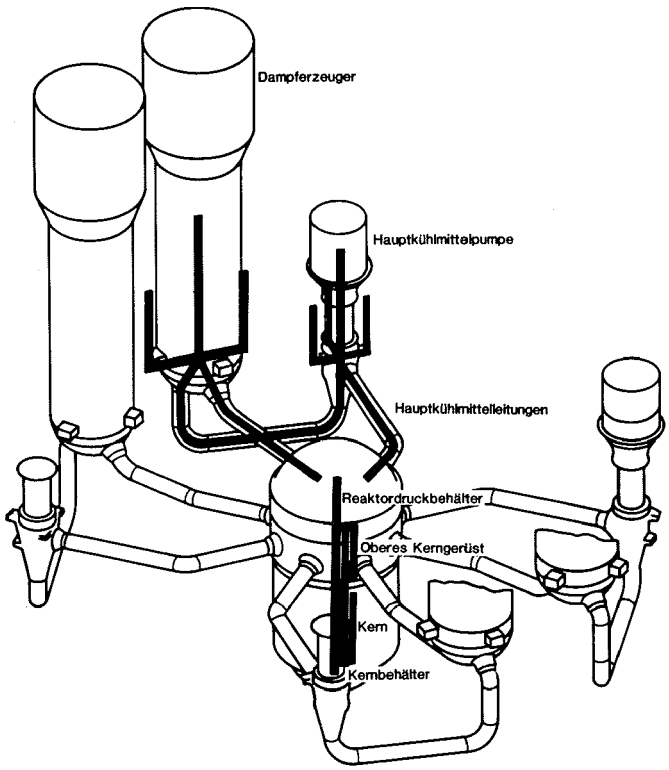


Bild 10: Strukturmodellentwicklung für DWR-Primärkreissystem

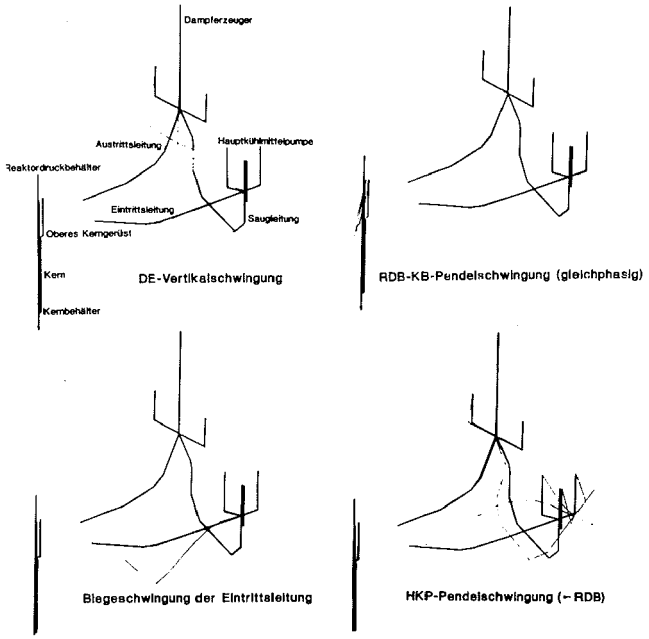


Bild 11: Beispiele für berechnete Schwingungsmodes

Jede dieser Massen hat mindestens drei Bewegungs-Freiheitsgrade: Pendelbewegungen um zwei horizontale Achsen und eine Vertikalbewegung. Bei den Dampferzeugern und Hauptkühlmittelpumpen wurden zusätzlich jeweils zwei horizontale Translationsbewegungen berücksichtigt. Die Steifigkeits- und Masseneinflüsse der Hauptkühlmittelleitungen wurden über Ersatzfedern bzw. Ersatzmassen berücksichtigt.

In Bild 11 sind für vier ausgewählte Strukturresonanzen die Schwingungsmodes des RDB-Einbautenverbands einschließlich eines Loops dargestellt. Grundlage für die Modellerstellung waren einerseits rechnerisch ermittelte bzw. vom Hersteller zur Verfügung gestellte Massen- und Steifigkeitsparameter, andererseits die experimentellen Ergebnisse von Shakertests und Unwuchterregungen der Komponenten in Form der modalen Parameter, die von KWU im Rahmen gemeinsamer F&E-Aktivitäten ermittelt worden sind [6].

Eine möglichst vollständige Interpretation der für eine Schwingungsüberwachung benutzten Signalmuster mit Hilfe der Inbetriebnahmemessungen, Korrelationsanalysen und Strukturmodelle bildet die Basis für treffsichere und belastbare Diagnosen. Nur bei zuverlässigen Prognosen findet das Überwachungsverfahren allseitige Akzeptanz und können die Vorteile tatsächlich genutzt werden.

Als Beispiel für vollständig interpretierte Spektren sind in den Bildern 12 bis 15 die ALDSs einiger Drucksignale, HKP-Schwingwege, RDB-Schwingwege und Excore-Neutronenflußsignale der DWR-Anlage in Neckarwestheim zusammengestellt.

Die Druckfluktuationen werden vor allem für die Identifikation und Überwachung der Schwingungserregung herangezogen. Die bei 6 Hz, 13 Hz und 40 Hz gefundenen breitbandigen akustischen Druckresonanzen in Rohrleitungssystemen des Primärkreises sind auch als Anregungen für Strukturschwingungen wirksam, was auch in den Bildern 13, 14 und 15 deutlich wird (mit *S* gekennzeichnet). Zudem sind ihre Resonanzfrequenzen, als

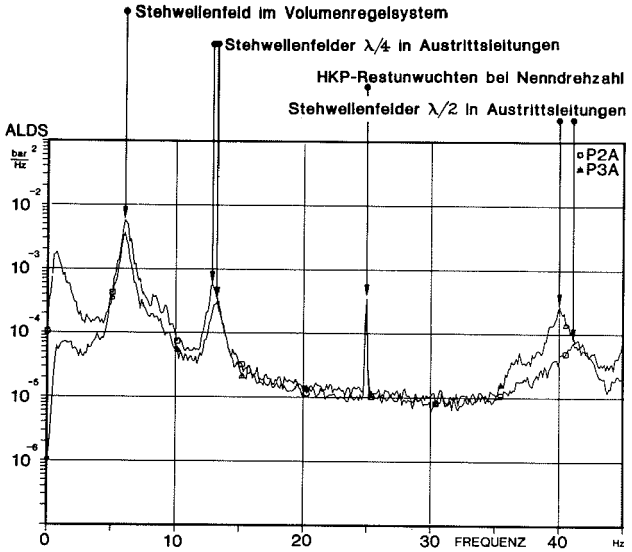


Bild 12: Interpretation von Druckspektren

Stehwellenfelder proportional zur Schallgeschwindigkeit, stark von Druck und Temperatur abhängig. Veränderte Betriebsbedingungen, wie der Streckbetrieb am Zyklusende, bedingen demnach schon als Folge einer geänderten Anregung Veränderungen in den Schwingungsspektren, die nicht als Frühwarnung sich anbahnender Schäden mißverstanden werden dürfen.

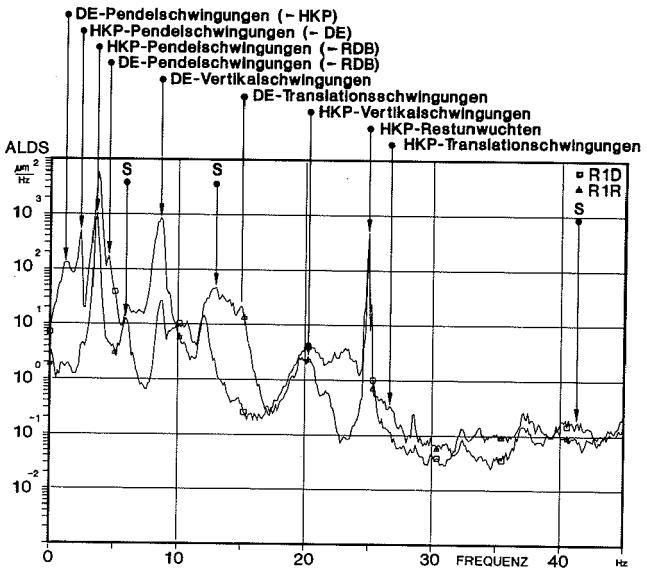


Bild 13: Interpretation von Schwingwegspektren der Hauptkühlmittelpumpen

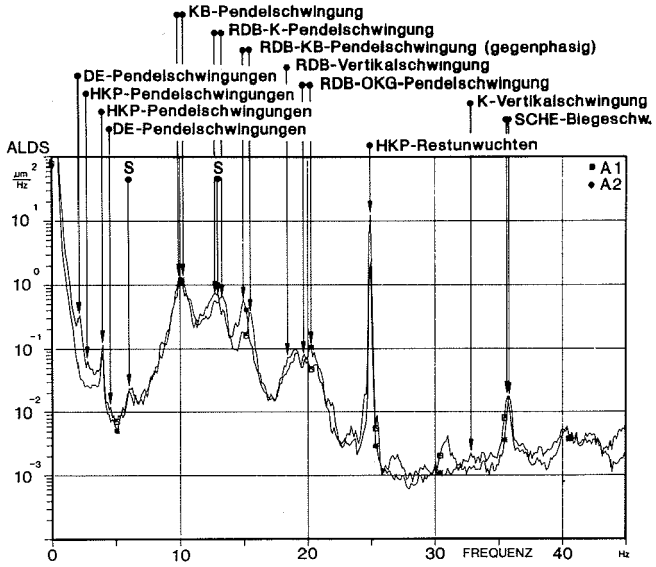


Bild 14: Interpretation von Schwingwegspektren des Reaktordruckbehälters

Die HKP-Schwingwegspektren enthalten primär die Starrkörperschwingungen des Pumpenaggregats (Pendel-, Vertikal- und Translationsschwingungen). Über die Saugleitung werden ferner Dampferzeugerschwingungen an die Pumpe angekoppelt, die ebenfalls in den HKP-Spektren identifiziert werden können. Aufgrund der beiden rechtwinkligen Meßrichtungen können bei Pendelschwingungen der Komponenten die Vorzugsschwingungsrichtungen angegeben werden (zum Beispiel → HKP, → RDB, → DE).

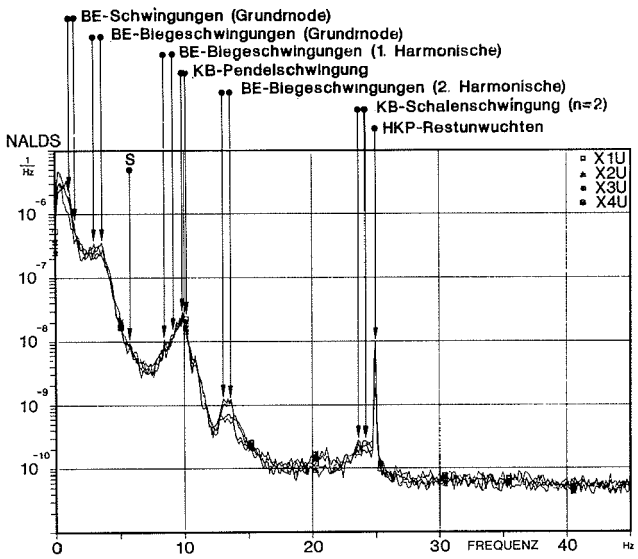


Bild 15: Interpretation von Excore-Neutronenflußspektren

Bei den RDB-Schwingwegspektren dominieren die Pendelschwingungsformen des Reaktordruckbehälters in Verbindung mit dem Kernbehälter, dem Kern, dem Oberen Kerngerüst und dem Kernschemel. Diese Strukturschwingungen weisen eine Richtungsabhängigkeit auf, das heißt, in Relation zur Aufnehmerposition am RDB-Deckel variieren die Eigenfrequenzen geringfügig. Entsprechendes trifft bei Vertikalschwingungen nicht zu, so daß hier auch keine Peak-Aufspaltung zu registrieren ist. Wie aus den Spektren ferner ersichtlich, ist der Einfluß von Stehwellenfeldern und Strukturresonanzen von Dampferzeugern und Hauptkühlmittelpumpen in den RDB-Schwingwegsignalen nicht unerheblich.

Beim Neutronenfluß dominieren die Brennelementbiegeschwingungen „einseitig fest" und „beidseitig gelenkig" mit höheren Harmonischen. Aufgrund der unterschiedlichen Standzeiten im Kern variieren die Brennelementresonanzen aufgrund bekannter Langzeittrends im jeweiligen Frequenzband um bis zu 10 %. Biege- und Schalenschwingungen des Kernbehälters sind ebenfalls sehr sensitiv mit der Neutronenflußaußeninstrumentierung nachweisbar.

Allen Spektren gemeinsam sind Einflüsse der durch Restunwuchten der Pumpenwelle bei Nenndrehzahl von 25 Hz erzwungen angeregten RDB-KB-Pendelbewegung, die sich infolge ihres deterministischen schmalbandigen Peaks und der im Zeitbereich als Schwebungsvorgang nachweisbaren Charakteristik deutlich von den Strukturresonanzen abhebt. Die interpretierten Spektren stellen den wesentlichen Teil des Musterkatalogs dar, auf den sich eine Schwingungsüberwachung abstützt.

Die Summe der auf diese Weise dokumentierten Informationen wird für jede Reaktoranlage nochmals in einem Interpretationsschema zusammengefaßt, wie dies in Tafel 1 geschehen ist: Die Resonanzfrequenzen sind loopspezifisch aufgelistet, da sich das Schwin-

Tafel 1: SÜS-Interpretationsschema für einen 3-Loop-Druckwasserreaktor

Resonanzfrequenzen			Erläuterung der Frequenzpeaks
Loop 1	Loop 2	Loop 3	
1,3	1.2	1.1	DE-Pendelschwingungen (⇌HKP)
	1.4. . . 1.8		BE-Schwingungen (Grundmode)
2.4	2.4	2.3	HKP-Pendelschwingungen (⇌DE)
3.9	4.0	4.0	HKP-Pendelschwingungen (⇌RDB)
4.4	4.6	4.2	DE-Pendelschwingungen (⇌RDB)
	4.3. . . 4.8		BE-Biegeschwingungen (Grundmode)
	6.2		Stehwellenfeld im Volumenregelsystem
	8.2. . . 9.2		BE-Biegeschwingungen (1. Harmonische)
8.5	9.1	8.3	DE-Vertikalschwingungen
	9.8. . . 10.4		RDB-KB-Pendelschwingung (gleichphasig)
	12.6. . . 13.1		RDB-K-Pendelschwingung
	12.8	13.2	Stehwellenfelder $\lambda/4$ in Austrittsleitungen
	12.9. . . 14.4		BE-Biegeschwingungen (2. Harmonische)
	15.0. . . 15.6		RDB-KB-Pendelschwingung (gegenphasig)
14.8	15.4	14.3	DE-Translationsschwingungen
	18.6		RDB-Vertikalschwingung
	19.7. . . 20.2		RDB-OKG-Pendelschwingung
20.2	20.3	21,0	HKP-Vertikalschwingungen
	23.5. . .24.5		KB-Schalenschwingung (n=2)
24.9	24.9	24.9	HKP-Restunwuchten bei Nenndrehzahl
26.4	29.5	29.1	HKP-Translationsschwingungen
	33		K-Vertikalschwingung
	35.6. . . 35.9		SCHE-Biegeschwingung
	37.8		Stehwellenfelder $\lambda/2$ in Eintrittsleitungen
	42.1	41.2	Stehwellenfelder $\lambda/2$ in Austrittsleitungen

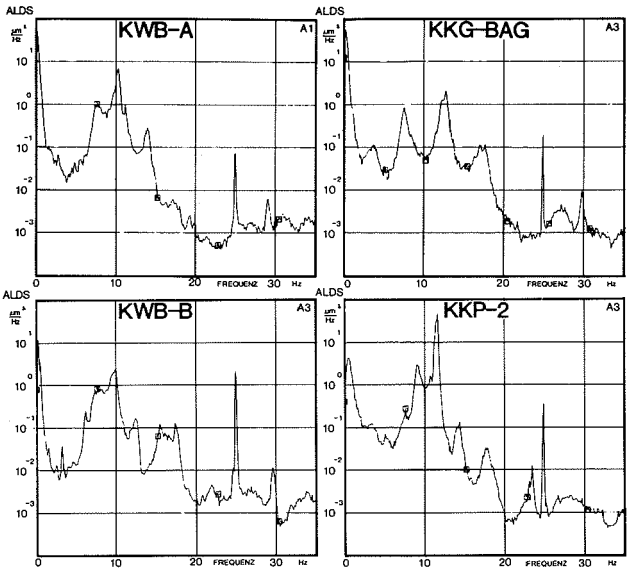


Bild 16: RDB-Schwingwegspektrenvergleich von 4-Loop-Druckwasserreaktoren

gungsverhalten der Pumpen und Dampferzeuger individuell geringfügig unterscheiden kann. Resonanzen, die den Reaktordruckbehälter mit Einbauten betreffen, wurden ebenfalls in die Spalte bei Loop 2 integriert. Der hier gezeigte Auszug umfaßt den Frequenzbereich 0 bis 45 Hz, die Originalinterpretationsliste beinhaltet den Frequenzbereich bis 100 Hz.

Ein anlagenübergreifender Vergleich von SÜS-Spektren offenbart zunächst relativ große Abweichungen – dies trifft auch zu, wenn nur Musterfunktionen von 4-Loop-Druckwasserreaktoren der Leistungsklassen 1200 bis 1350 MW zugrundegelegt werden. In Bild 16 sind vier RDB-Schwingwegspektren der Reaktoren Biblis - A, Biblis - B, Grafenrheinfeld und Philippsburg - 2 im Frequenzbereich 0 bis 35 Hz zusammengestellt. Mit Ausnahme der 25-Hz-Unwuchterregung sind korrespondierende Frequenzpeaks nicht unmittelbar erkenntlich. Die Ursachen im unterschiedlichen RDB-Schwingungsverhalten liegen in Modifikationen der Komponentenlagerung oder geringfügigen konstruktiven Änderungen der Kerneinbauten begründet. Darüber hinaus kann auch bei konstruktionsgleichen Anlagen die unterschiedliche Traglastverteilung der acht RDB-Tragpratzen bereits das resultierende RDB-Schwingungsverhalten beeinflussen! Somit ist für jedes Druckwasserreaktor-Primärkreissystem eine individuelle Basismessung einschließlich Basisinterpretation erforderlich, um den anlagenspezifischen Besonderheiten gerecht zu werden. Vergleichbar mit dem für GKN dokumentierten Interpretationsstand basiert auch bei den 4-Loop-Anlagen die Schwingungsüberwachung auf adäquaten Interpretationsschemata.

Beispiele erfolgreicher Schadensprognosen

Die bisher beim Einsatz von Schwingungsüberwachungsverfahren durch GRS gewonnenen praktischen Erfahrungen bestätigen sehr eindrucksvoll, daß strukturmechanische Schadensentwicklungen durch Überwachung der entsprechenden Musterfunktionen diagnostiziert werden können. Die Effektivität dieser Schadenfrüherkennungsmethoden konnte an einer Reihe von Ereignisabläufen nachgewiesen werden:

- Anlaufen einer Hauptkühlmittelpumpe an GAU–Abstützung,
- Welle/Gehäuse-Kontakt bei Auslauf einer Hauptkühlmittelpumpe,
- Anomale Brennstabbiegeschwingungen im Bereich eines Abstandshalters,
- Mangelhafte Schildkühlung einer Hauptkühlmittelpumpe,
- Integrale Relaxation von Brennelement-Abstandshaltern,
- Vorspannungsverlust der Kernbehältereinspannung,
- Anzugsmomentverlust an Schrauben der Schemelbefestigung.

An dieser Stelle sollen zwei Beispiele näher erläutert werden, die auf geradezu klassische Weise die Methodik der Frühdiagnose veranschaulichen:

Das erste Beispiel beschreibt eine Schadensentwicklung an Federelementen, deren Aufgabe es ist, eine definierte Verspannung der Kerneinbauten mit dem Reaktordruckbehälter sicherzustellen. Nachdem an einem Druckwasserreaktor bereits für die Dauer eines Brennelementzyklus Schwingungs- und Neutronenflußmessungen durchgeführt worden waren (und somit eine ausreichende Basis für Mustervergleiche vorlag), traten im Folgezyklus Musterveränderungen auf. Bild 17 zeigt die Abweichungen der aktuell gemessenen Musterfunktion (breite Liniendicke) vom „gesunden" Anlagenzustand (geringe Liniendicke) am Beispiel des Autoleistungsdichtespektrums eines Schwingwegsignals vom Reaktordruckbehälter. Auch bei den Neutronenflußsignalen der Außeninstrumentierung konnten Veränderungen beobachtet werden. Die stärksten Abweichungen konzentrierten sich auf den Bereich der Kernbehälterpendelschwingung bei 7,5 Hz. In Bild 18 kann die zeitliche Entwicklung dieser Frequenzverschiebung im Verlauf des Brennelement-Zyklus detailliert verfolgt werden: Nachdem bei der ersten Messung im Zyklus (September 1980) Musterveränderungen separiert werden konnten, wurde der Betreiber über die Diagnosebefunde unterrichtet: Als Ursache des veränderten Einbautenschwingungsverhaltens kam eine Abnahme der Einspannkräfte im Bereich der Flanscheinspannung von Kernbehälter/Oberem Kerngerüst zum Reaktordruckbehälter in Betracht. Diese Einspannung ist durch Niederhalter-Federpakete realisiert.

Aufgrund dieser Diagnose wurde für die nächste planmäßige Anlagenrevision eine Überprüfung bzw. der Austausch von Niederhaltern empfohlen. Zur Kontrolle des Einbauten-

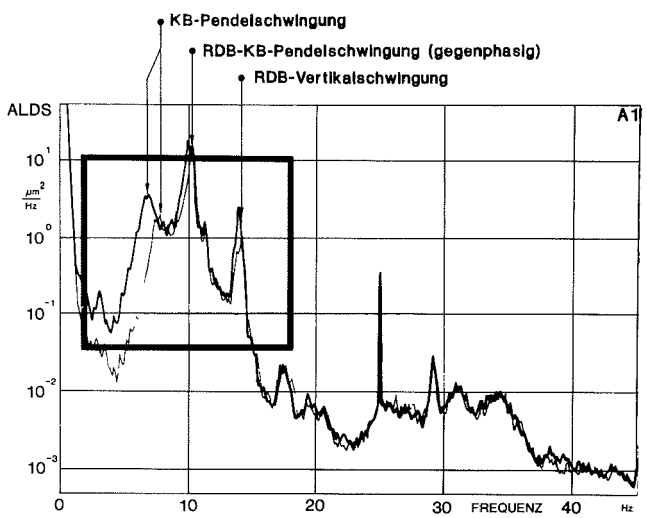


Bild 17: Abweichung bei RDB-Schwingwegspektren infolge veränderter Kernbehälter-Einspannung

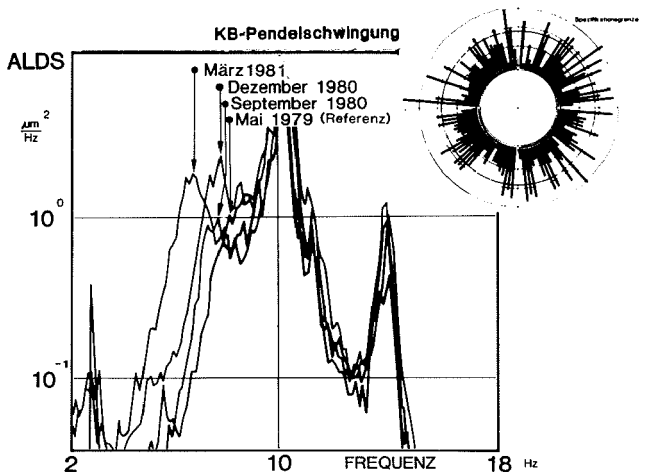


Bild 18: Entwicklung der Frequenzverschiebung im Verlauf eines Brennelementzyklus

Schwingungsverhaltens wurden während des weiteren Anlagenbetriebs wiederholt Messungen durchgeführt.

Wie aus Bild 18 ersichtlich ist, wurde bis Dezember 1980 keine weitere Frequenzdrift festgestellt, die Leistungsdichte und somit die Schwingungsamplitude erhöhte sich jedoch eindeutig. Bis zur Messung im März 1981 war die Kernbehälter-Pendelresonanz dann bereits auf 6,5 Hz abgesunken. Zwei Monate später und somit acht Monate nach den ersten Musterverschiebungen konnten die Niederhalter während der Revisionsphase der Anlage geprüft werden: Während eine erste optische Inspektion keine Veränderungen erkennen ließ, wurden bei der anschließenden Federkraftbestimmung, bei der unter Simulation der Einbaubedingungen die aktuellen Vorspannkräfte gemessen wurden, Abweichungen festgestellt: Das Ergebnis der Überprüfung ist in Bild 18 integriert: Die

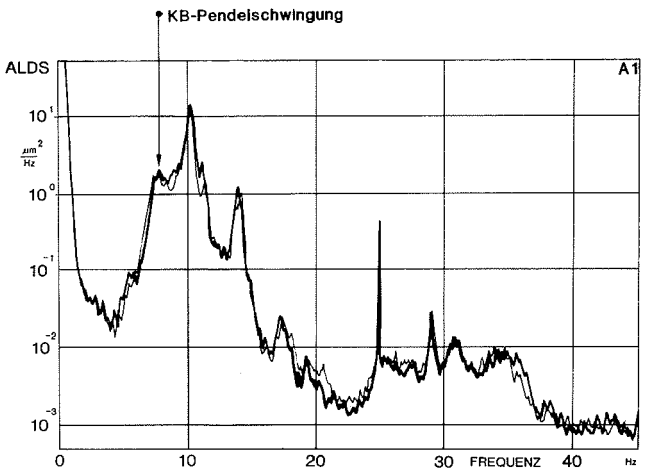


Bild 19: Spektrenvergleich nach Austausch defekter Niederhalter-Federpakete

gemessenen Federkräfte sind strahlenförmig am Umfang des Reaktordruckbehälters aufgetragen. 62 der 112 Federpakete, die unterhalb der Spezifikationsgrenze lagen, wurden ausgetauscht.

Nach dem Anfahren der Reaktoranlage zum folgenden Brennelementzyklus wurden erneut Messungen und vergleichende Analysen durchgeführt. Das Schwingungsspektrum in Bild 19 zeigt beim Quervergleich mit dem Referenzspektrum eindeutig, daß durch den Austausch der defekten Niederhalter die aufgetretenen Abweichungen vollständig eliminiert werden konnten.

Sind Frequenzverschiebungen diagnostiziert und eindeutig durch Inspektionsbefunde abgesichert, werden die daraus ableitbaren Erkenntnisse auf andere Reaktoranlagen übertragen, um zulässige bzw. unzulässige Frequenzverschiebungen gegeneinander abzugrenzen. Wichtig ist in diesem Zusammenhang das Langzeitverhalten der betreffenden Strukturresonanz, da nur nach Kenntnis der Vorgeschichte eine aktuelle Musterabweichung beurteilt werden kann. Dies soll am Beispiel der Kernbehälterresonanzen in GKN mit Bild 20 verdeutlicht werden: der 10-Hz-Biegemode des Kernbehälters ist über Jahre hin sehr stabil. Deutlich kann ein Frequenzunterschied zwischen der A1/A3- und der A2/A4-Meßrichtung festgestellt werden, der auf eine konstruktionsbedingte geometrische Asymmetrie der RDB-Lagerung zurückzuführen ist. Das Absinken der Kühlmitteltemperatur im Streckbetrieb bedingt eine geringfügige Änderung der Einspannbedingungen des KB und einen Anstieg der Dichte des Wassers im RDB. Daraus resultiert ein deutliches Absinken der KB-Biegeschwingung. Nach Übertragung der an der 4-Loop-Anlage beobachteten Frequenzverschiebung als Toleranzband in den Kernbehälter-Langzeittrend der 3-Loop-Anlage bleibt festzustellen, daß eine Relaxation der Niederhaltefedern mit 30 % Vorspannungsverlust eindeutig als Peakverschiebung registrierbar ist, auch während des Streckbetriebs der Anlage.

Das zweite Beispiel einer beginnenden Schadensentwicklung beinhaltet das Absinken der sogenannten Schemelbiegeschwingung: Dem Leistungsdichtepeak bei 29 Hz in Bild 21 kann eine Resonanz des Kernschemels zugeordnet werden, einem Bauteil, das aus acht

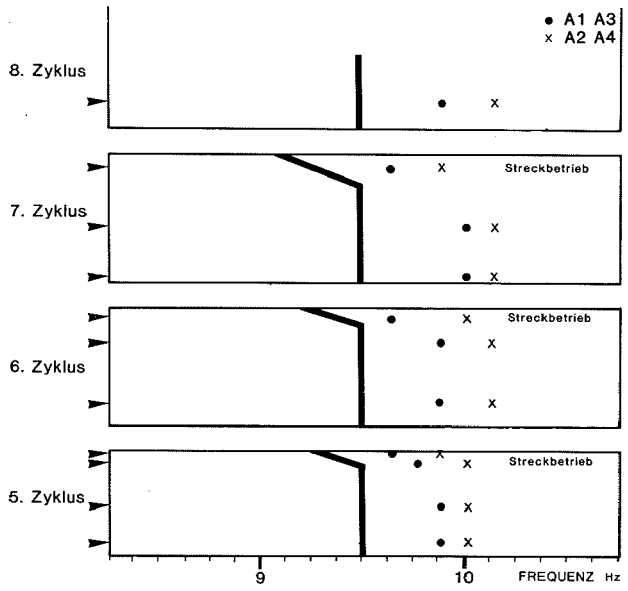


Bild 20: Langzeitverhalten der Kernbehälterresonanz mit Angabe des Toleranzbereichs

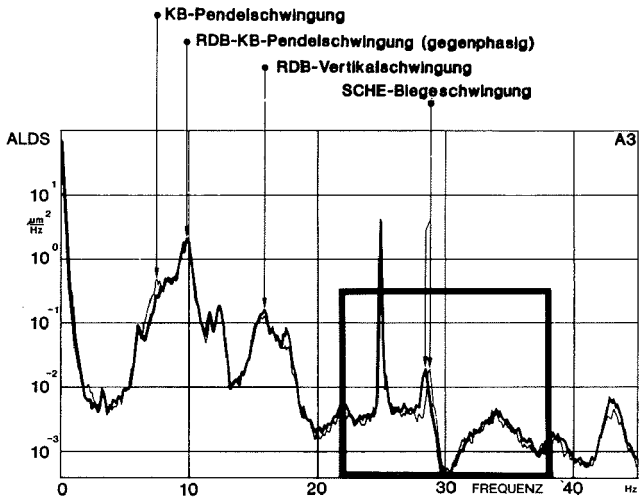


Bild 21: Abweichungen bei RDB-Schwingwegspektren infolge veränderter Schemelbefestigung

Standbeinen und Verbindungselementen besteht und an Konsolen mit der unteren Reaktordruckbehälter-Kalotte verschraubt ist. Der Kernschemel hat keine mechanische Verbindung mit dem Kernbehälter. Er wird durch die im Kalottenbereich wirkenden Strömungswirbel zu Biegeschwingungen angeregt.

Wie aus der Ausschnittsvergrößerung in Bild 22 erkennbar ist, betrug die Frequenzverschiebung im Juni 1984 im Vergleich zu einem Referenzzustand nur 0,1 Hz: Aus Langzeit-Trenduntersuchungen war bekannt, daß die normale Alterung des Schemels und seiner Befestigung eine Frequenzverringerung von maximal 0,1 Hz pro Jahr verursachen darf.

Im November 1984, also fünf Monate später, konnte bereits eine weitere Frequenzdrift von 0,3 Hz registriert werden. Aufgrund des beschleunigten Absinkens der Resonanz

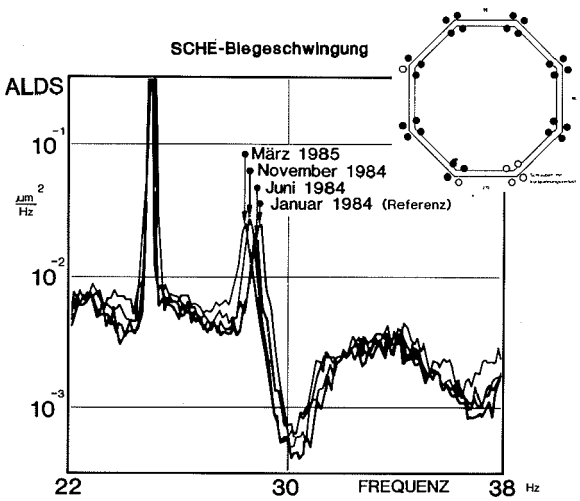


Bild 22: Entwicklung der Frequenzverschiebung im Verlauf eines Brennelementzyklus

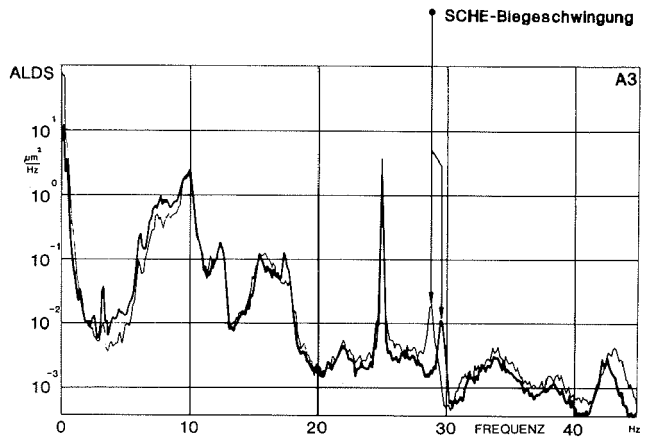


Bild 23: Spektrenvergleich nach Neuverspannung von Schemelschrauben

konnte eindeutig auf die beginnende Lockerung der Beine des Schemels geschlossen werden, die mit je vier Schrauben in der RDB-Bodenkalotte befestigt sind. Eine Untersuchung der Befestigungsschrauben wurde empfohlen. Einem weiteren Anlagenbetrieb bis zur planmäßigen Anlagenrevision stand nichts entgegen, da durch die begleitenden Messungen eine beschleunigte Schemellockerung erkennbar gewesen wäre. In der nachfolgenden Revision waren bei der visuellen Inspektion des Kernschemels zunächst keine Unregelmäßigkeiten erkennbar. Die Überprüfung der Anzugsdrehmomente der Schrauben an den Schemelbeinen ergab jedoch, daß sechs Schemelschrauben ohne Vorspannung waren.

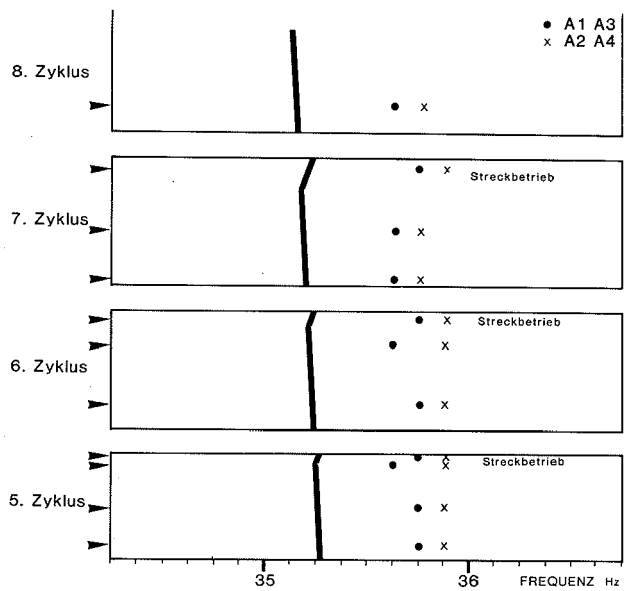


Bild 24: Langzeitverhalten der Schemelresonanz mit Angabe des Toleranzbereiches

Die Ergebnisse der Drehmomentuntersuchung mit einem Manipulator sind im Schemelaufriß (Bild 22, oben rechts) integriert. Nachdem alle Schemelschrauben mit einem erhöhten Anzugsdrehmoment erneut befestigt und verdrehgesichert worden waren, zeigte eine Folgemessung, daß die Schemelresonanz im Vergleich zur Referenzmessung nun oberhalb der Referenzfrequenz liegt (Bild 23). Somit sind nun auch alle Langzeitfrequenzdrifts der zurückliegenden Jahre durch die Neuverspannung eliminiert.

Die Übertragung dieser Schemellockerung auf eine andere Reaktoranlage muß ebenfalls unter Berücksichtigung des Langzeittrends erfolgen. Für die 3-Loop-Anlage in GKN heißt dies konkret (Bild 24):

Der Schemel schwingt – etwas richtungsabhängig – mit einer Eigenfrequenz von etwa 35,7 Hz. Seine Eigenfrequenz sinkt bedingt durch Setzvorgänge im Schraubgewinde mit weniger als 0,1 Hz pro Jahr ab. Der Streckbetrieb hat einen geringen Frequenzanstieg zur Folge.

Eine Lockerung der Schraubbefestigung an einem Schemelbein (mindestens vier Schrauben ohne Vorspannung) würde eine Frequenzverschiebung von mindestens 0,3 Hz bewirken: Das betreffende Toleranzband ist in den Langzeittrend integriert, eine Unterschreitung ist eindeutig nachweisbar.

Die beiden behandelten Beispiele zeigen, daß für eine erfolgreiche Schwingungsüberwachung mehrere Faktoren zusammenwirken müssen: Voraussetzung ist eine hoch entwickelte Meß- und Auswertetechnik, die in der Lage ist, die stets sehr kleinen Amplituden der Betriebsschwingungen bzw. die geringen Fluktuationen der Prozeßsignale mit genügender Dynamik zu erfassen und zu analysieren. Weiter müssen die richtigen und ausreichend abgesicherten Referenzmuster für den Systemzustand vorliegen, in dem eine Schwingungsüberwachung durchgeführt werden soll. Die Referenzmuster sollen vollständig interpretiert und verstanden sein, so daß aus etwaigen detektierten Veränderungen auch eine hilfreiche Diagnose abgeleitet werden kann. Schließlich müssen die „natürlichen" Langzeittrends bekannt sein, denen die Referenzmuster zwangsläufig unterliegen und die deshalb nicht als Fehlerfrühindikator mißverstanden werden dürfen.

Körperschallüberwachung

Das Prinzip der Körperschallüberwachung beruht auf der seit Beginn des Maschinenbaus bekannten Fehlererkennung durch Abhören der Betriebsgeräusche. Der vom erfahrenen Werkmeister bei kleinen Turbinen und Motoren verwendete Schraubendreher wird allerdings hier im nicht begehbaren Bereich von Kernkraftwerken durch entsprechende Instrumentierung ersetzt. Die Notwendigkeit zur Körperschallüberwachung ist in KTA 3204 festgelegt:

> „Zur frühzeitigen Erkennung von Schäden sind die RDB-Einbauten auf lose Teile mittels eines Körperschallüberwachungssystems nach DIN 25 475 zu überwachen."

Die technischen Spezifikationen und Details zur Durchführung der Überwachung sind in DIN 25 475 geregelt, Auszüge hiervon lauten:

> „Die Überwachung erfolgt kontinuierlich mit automatischer Meldung bei Grenzwertüberschreitung.
>
> Die Überwachung wird durch regelmäßiges Abhören der einzelnen Signale ergänzt.
>
> Nach längeren Betriebspausen, zum Beispiel zwecks Brennelementwechsel, sind Referenzaufzeichnungen durchzuführen."

In allen deutschen Leichtwasserreaktoren sind Körperschallüberwachungssysteme installiert und im Einsatz (Bild 25).

Die Körperschallaufnehmer sind in Bereichen der druckführenden Umschließung angebracht, die natürliche Sammelräume für abgelöste Teile darstellen (Eintrittsplenum in

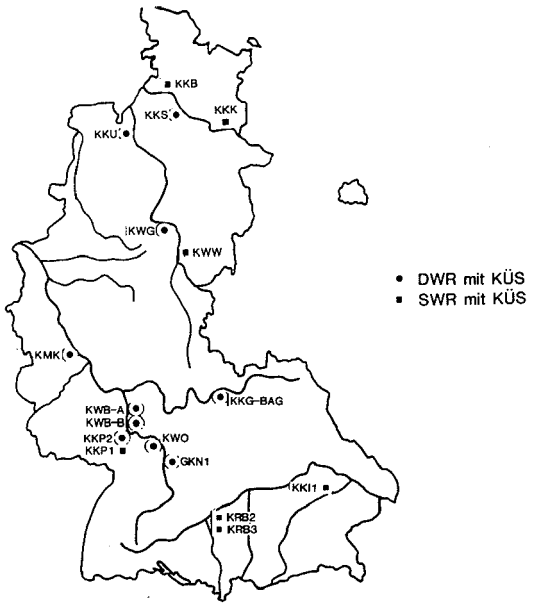


Bild 25: Einsatz von Körperschallüberwachungssystemen

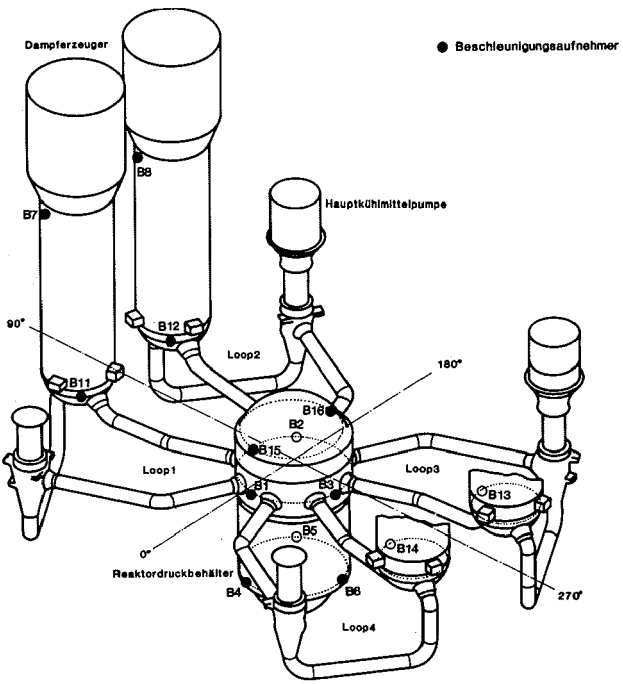


Bild 26: KÜS-Standardinstrumentierung an 4-Loop-Druckwasserreaktoren

RDB und DE) oder für die eine erhöhte Wahrscheinlichkeit lockerer Teile angenommen wird (RDB-Stutzenteil und DE-Dampfraum).

Meß- und Analyseeinrichtungen

Bild 26 beinhaltet die Standardinstrumentierung am Beispiel eines 4-Loop-Druckwasserreaktors. Die 16 Beschleunigungsaufnehmer verteilen sich wie folgt:

- drei Beschleunigungsaufnehmer im RDB-Stutzenbereich (B1. . .B3),
- drei Beschleunigungsaufnehmer an der RDB-Kalotte (B4. . .B6),
- vier Beschleunigungsaufnehmer am Dampferzeuger, oben (B7 . . .B10),
- vier Beschleunigungsaufnehmer am Dampferzeugerprimäreintritt (B11 . . .B14),
- zwei Beschleunigungsaufnehmer am RDB-Deckelflansch (B15, B 16).

Bei Siedewasserreaktoren gelangen bis zu zehn Beschleunigungsaufnehmer zum Einsatz:

- drei Beschleunigungsaufnehmer am Druckbehälterdeckel (B1 . . .B3),
- drei Beschleunigungsaufnehmer an der Bodenkalotte (B4. . .B 6),
- vier Beschleunigungsaufnehmer an der Ringraumabdeckung (B7 . . . B10).

Da bei Anzeigen in einzelnen Signalkanälen unter Umständen für den Betrieb sehr weitgehende Konsequenzen abgeleitet werden müssen, andererseits bei langen Schallwegen sich Unschärfen einstellen können, die eine eindeutige Identifikation der Schallursache erschweren, haben einige Reaktorbetreiber zusätzliche Meßstellen für Diagnosezwecke vorgesehen. Es kann sich hierbei durchaus um passive Kanäle handeln, das heißt solche ohne eigene Elektronik. Im Bedarfsfall werden diese Aufnehmer auf verfügbare, nicht benötigte Meßketten aufgeschaltet.

Als Aufnehmer werden temperatur- und strahlungsresistente Beschleunigungsaufnehmer auf Piezo-Basis verwendet, die im akustischen Frequenzbereich arbeiten. Sie werden bisher meist mit Magneten an den Oberflächen der überwachten Struktur adaptiert, in neueren Anlagen zum Beispiel Krümmel, Mülheim-Kärlich sind sie geschraubt. In Warten-

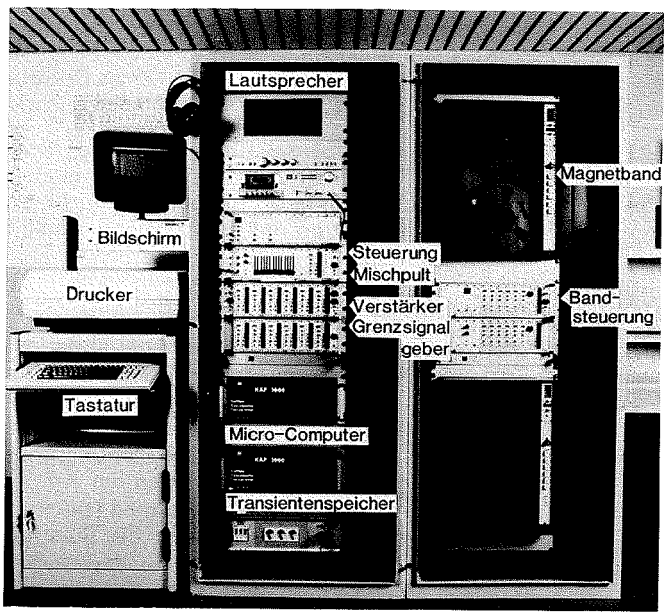


Bild 27: Signalanalyseeinheiten zur Körperschallüberwachung vor Ort (AZT-Systemkonfiguration)

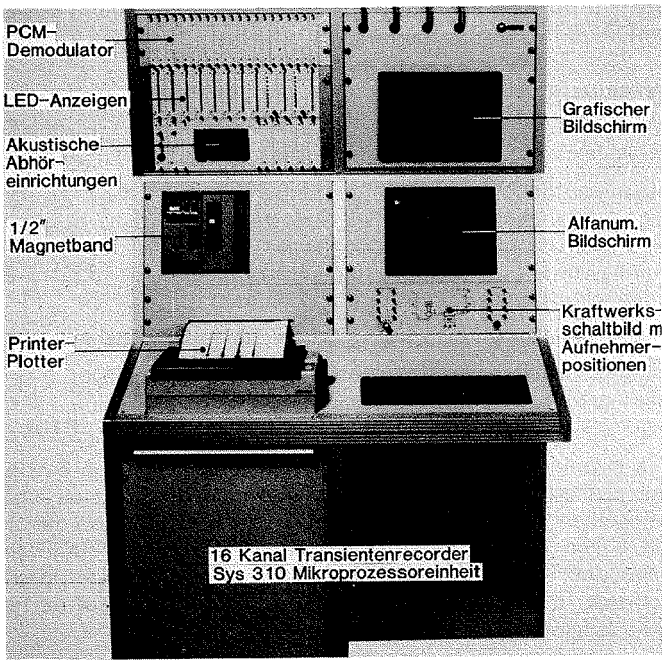


Bild 28: Signalanalyseeinheiten zur Körperschallüberwachung vor Ort (KWU-Systemkonfiguration)

nähe befinden sich Signalaufbereitungs- und Überwachungseinheiten sowie Lautsprecher und Dokumentationseinrichtungen.

Die meisten bisher installierten Körperschallüberwachungssysteme arbeiten mit Lichtschreibern zur Dokumentation. Der Schreiber wird bei Überschreiten eines Grenzwertes automatisch gestartet. Parallel dazu können die Signale auf Magnetband aufgezeichnet werden.

In den Bildern 27 und 28 sind Körperschallüberwachungssysteme der neuesten Generation, wie sie vom Allianz Zentrum für Technik (AZT) und KWU angeboten werden, gezeigt: Burstspeicherung, -darstellung und -analyse bis hin zur Schallortung werden durch Mikroprozessoren gesteuert. Die Kommunikation mit dem Bedienpersonal ist im Dialogverkehr möglich [7].

Schallausbreitung und Schallortung

Die durch das Anschlagen loser oder lockerer Teile in das Material der druckführenden Umschließung eingeleitete Energie breitet sich bevorzugt als Plattenwelle mit symmetrischen (s) und asymmetrischen (a) Moden in der Struktur aus. Die unterschiedlichen, von der Frequenz abhängigen Ausbreitungsgeschwindigkeiten dieser Wellenmoden führen dazu, daß der ursprünglich sehr kurze, scharf einsetzende Spannungsimpuls auf seinem Weg durch die Struktur zerfließt (Dispersion). In den Signalen der Körperschallaufnehmer bildet er sich daher jeweils mit unterschiedlichen Signalformen (Bursts) ab. Die einem Schallereignis zuzuordnenden Signalverläufe bezeichnet man als Burstmuster. Bild 29 zeigt ein durch einen Testanschlag an der Behälterwand eines Siedewasserreaktors erzeugtes Burstmuster, bei dem der Schall einen Weg von 0,5, 5, 9, 13 und 15 m durchlaufen hat. Neben dem Zerfließen des ursprünglichen Impulses ist in diesem Bild auch deutlich der Zeitverzug der (nachverstärkten) Signale 2 bis 5 gegenüber 1 zu erkennen. Aus der

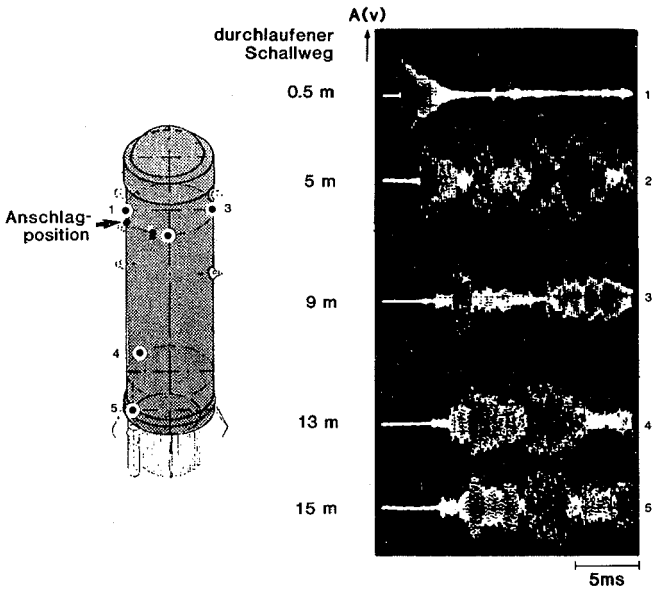


Bild 29: Burstmuster eines Testschlages an einem Siedewasserreaktor

Erscheinungsform der Burstsignale und aus dem relativen zeitlichen Versatz der Signale zueinander kann auf Ursache und Einleitungsort des Schallereignisses geschlossen werden [8].

Die GRS hat bereits seit 1980 ein auf Transientenrekordern und Tischrechnern basierendes System für Off-line-Analysen im Labor zur Verfügung (Bild 30). Die Signale werden

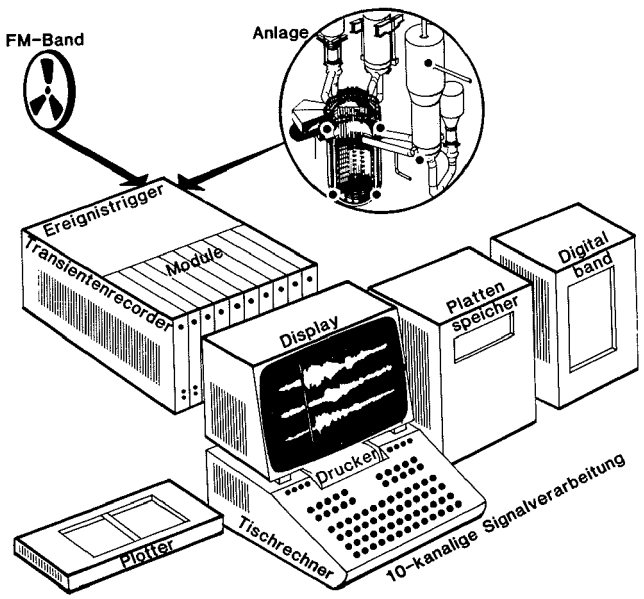


Bild 30: Rechner und Transientenrecorder zur Off-line-Analyse im Labor (GRS-Systemkonfiguration)

auf Magnetband gespeichert angeliefert; gegebenenfalls könnte das System auch vor Ort gebracht werden. Das System hat sich bei der Analyse von ungeklärten Anzeigen und von Routinemessungen, die GRS in mehreren Anlagen wiederkehrend durchführt, bestens bewährt. Daneben wird das System zur Weiterentwicklung von Auswertealgorithmen und zum Aufbau einer zentralen Datenbank für betriebliche und schadensbedingte Burstmuster eingesetzt.

Antworten auf folgende Fragen werden bei der Auswertung von Burstmustern erwartet:

- Bleibt der Schallentstehungsort für alle Ereignisse derselbe (lockeres Teil) oder wechselt er stetig (loses Teil)?
- Gibt es Gruppen gleichartiger Muster (gleiche Schallursache an unterschiedlichen Positionen, zum Beispiel Kondensationsschläge)?
- Wo liegt der Ort bzw. liegen die Orte der Schallentstehung?
- Wie ist die zeitliche Verteilung der Ereignisse?
- Wie ist die Verteilung des Energieinhalts der Ereignisse?
- Wenn tatsächlich metallische Anschläge vorliegen, wie groß ist die Masse der lockeren bzw. losen Teile, wie groß sind die Anschlagenergien?

Zur Beantwortung dieser Fragen, die aus der Bewertung der Burstformen, -laufzeiten, -intervallverteilungen und -häufigkeiten in oder zwischen den verfügbaren Signalen zu erfolgen hat, sind insbesondere Kenntnisse über die vorliegenden Schallausbreitungsbedingungen von Bedeutung.

Die Ausbreitung von Körperschall ist wesentlich vom Verhältnis Wellenlänge λ zur Wandstärke d bestimmt. Es wird zwischen den Bereichen $\lambda < d$ und $\lambda > d$ unterschieden. Bei „dicken" Bauteilen ($\lambda < d$) breitet sich der Körperschall in vergleichsweise einfacher Form als Longitudinal-, Transversal- und Oberflächenwellen mit von der Frequenz unabhängigen Ausbreitungsgeschwindigkeiten aus. Bei „dünnen" Bauteilen sind die Ausbreitungsverhältnisse wesentlich komplizierter, die auftretenden Wellentypen können Plattenwellen gleichgesetzt werden.

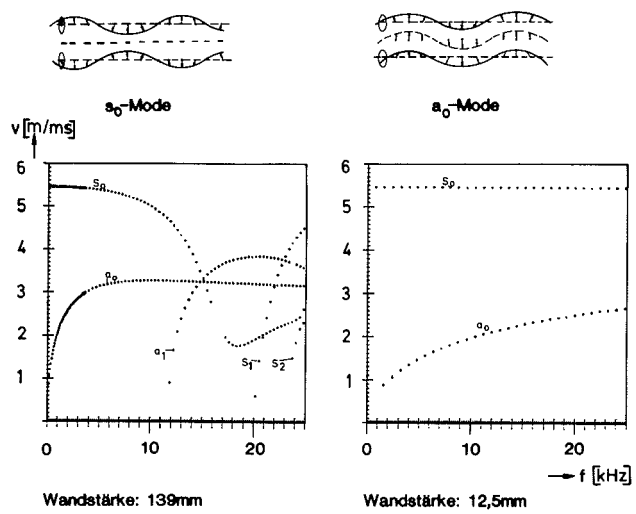


Bild 31: Frequenzabhängigkeit der Ausbreitungsgeschwindigkeiten von Plattenwellen, berechnet für zwei unterschiedliche Wanddicken

Am Primärsystem von Leichtwasserreaktoren ist die Wellenlänge größer als die Wandstärke, somit ist bei der Körperschallausbreitung grundsätzlich von Plattenwellen auszugehen.

Bei den Plattenwellen lassen sich zwei verschiedene Grundtypen unterscheiden (Bild 31):

- Die Dehnwelle oder symmetrische Welle (s_0-Mode): Bei diesem Wellentyp schwingen die Strukturelemente symmetrisch zur Mittelzone und in dieser rein longitudinal.
- Die Biegewelle oder asymmetrische Welle (a_0-Mode): Hier schwingen die Strukturelemente mit einer zur Mittelzone asymmetrischen Auslenkung. In der neutralen Faser erfolgt rein transversale Auslenkung.

Zu diesen beiden Grundwellentypen gibt es beliebig viele Oberwellen.

Plattenwellen sind nicht dispersionsfrei wie Longitudinal- oder Transversalwellen. Das bedeutet, wie bereits erwähnt, daß ihre Ausbreitungsgeschwindigkeiten von der Frequenz ahängig sind. Teilimpulse verbreiten sich aus diesem Grund, „zerfließen" entsprechend der Länge des durchlaufenen Schallwegs, und zwar unterschiedlich stark, je nachdem, wie groß die Dispersion der zugehörigen Moden ist. Die Ausbreitungsgeschwindigkeit ist außerdem abhängig von der Wandstärke der Struktur. Die Ergebnisse der Berechnungen der Körperschall-Gruppengeschwindigkeiten für die Wandstärke des RDB-Zylinders (139 mm) bzw. einer SWR-Speisewasserleitung (12,5 mm) sind in Bild 31 als Funktion der Frequenz dargestellt.

Das bekannteste Verfahren zur Feststellung des Schallentstehungsortes ist die Triangulation mit Hilfe des Hyperbelschnittverfahrens (Bild 32). Aus den Zeitdifferenzen der Burstsignale eines Ereignisses, gemessen an drei verschiedenen Positionen, wird nach der Beziehung

$$r_1 - r_2 = v_G \cdot \Delta t_{1,2}$$

der Quellort ermittelt. Die Genauigkeit dieser Methode ist vor allem davon abhängig, wie exakt der Burstanfang definiert werden kann. Dabei ist auch auf die Unterscheidung der verschiedenen Wellenmoden zu achten. Macht vor allem bei geringen Anschlagenergien

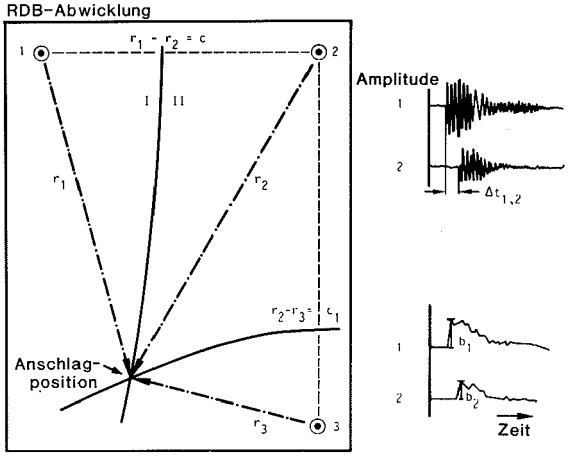


Bild 32: Lokalisierung des Anschlagortes durch Hyperbelschnittverfahren (Amplitudenverhältnisse bzw. Laufzeitunterschiede)

die Laufzeitbestimmung Schwierigkeiten, kann noch die Dämpfung der Schallereignisse zur Ortsbestimmung herangezogen werden. Ausgewertet wird dann das Verhältnis der an zumindest drei unterschiedlichen Orten gemessenen Peakamplituden:

$$r_2 - r_1 = \frac{\ln\hat{b}_1 - \ln\hat{b}_2}{\lambda}$$

In der Praxis zeigt sich, daß der s_o-Mode die höhere Ausbreitungsgeschwindigkeit besitzt, jedoch stark gedämpft wird und somit meistens im Hintergrundrauschen des Aufnehmers verdeckt ist. Der eigentliche Burstanfang wird daher in den meisten Fällen erst durch den langsameren a_o-Mode bestimmt.

Magnetisch adaptierte Körperschallaufnehmer haben im allgemeinen zwei bis drei, manchmal noch mehr Resonanzfrequenzen. Hat ein Aufnehmer zwei in den Frequenzen deutlich getrennte Resonanzen, zum Beispiel eine aufnehmerspezifische bei etwa 20 bis 30 kHz und eine Halterungsspezifische im Bereich 5 bis 10 kHz, so kann mit Hilfe der für beide Frequenzbereiche unterschiedlichen Schallausbreitungsgeschwindigkeiten v_{f1} und v_{f2} des a_o-Modes (Bild 31) zur Ermittlung des durchlaufenen Schallweges auch der Dispersionseffekt genutzt werden:

$$\text{Abstand } r \text{ des Sensors vom Quellort} = \frac{\Delta t_{f1,f2} \cdot v_{f1} \cdot v_{f2}}{v_{f1} - v_{f2}}$$

Bei eindimensionalen Strukturen, zum Beispiel Rohrleitungen, kann so mit einem einzigen Aufnehmer eine Lokalisierung durchgeführt werden.

Zur Bestimmung von Masse und Geschwindigkeit eines losen Teils bzw. der Energie der Anschläge muß die Ortung der Anschlagstelle bereits erfolgt sein. Die Energie läßt sich dann aus den Signalformen der Bursts, insbesondere den Burstamplituden abschätzen, wobei wegen der meist komplizierten Schallausbreitungsbedingungen empirische Erfahrungswerte, das heißt Testanschläge mit bekannten Anschlagenergien, die bei Stillstand der Anlage durchgeführt werden, sowie Untersuchungen über die speziellen Schallabschwächungsbedingungen herangezogen werden. Aus den so ermittelten Energien kann schließlich die Masse des schlagenden Teils mit der Annahme abgeschätzt werden, daß sich ein loses Teil meist etwas langsamer als das Kühlmittel bewegt, in dessen Strömung es mitgerissen wird.

Eine weitere Möglichkeit zur Abschätzung der Masse eines losen Teils ergibt sich aus dem Frequenzinhalt eines Bursts. Die Kontaktzeit eines Stoßes zweier metallischer Körper hängt nämlich neben der Geometrie und Materialeigenschaften im wesentlichen von der Masse und Geschwindigkeit ab. Sind also Kontaktzeit und Geschwindigkeit in etwa bekannt, so kann auf die Masse des losen Teils geschlossen werden. Ein Maß für die Kontaktzeit kann aus dem Frequenzspektrum der Burst abgeleitet werden. Kleine Teile erzeugen aufgrund kurzer Kontaktzeiten (Größenordnung 25 μs) sehr breitbandige, das heißt auch hochfrequente Bursts. Schwere Teile mit langen Kontaktzeiten (Größenordnung 200 μs) erzeugen keine hochfrequenten Signalanteile.

Beispiele erfolgreicher Schadensprognosen

Bei einer Reihe von Vorkommnissen, die als Beispiele für die Leistungsfähigkeit der Überwachungsmethode herangezogen werden können, war GRS zur Signalanalyse zugezogen [9]. Bei Siedewasserreaktoren handelt es sich um folgende Ereignisse:

- Bruch eines Verbindungsstegs im Dampf-Wasser-Separator,
- Einseitiger Bruch eines Pumpenabdeckbügels,
- Ausgeschlagene Lagerbuchse eines Speisewasserventils.

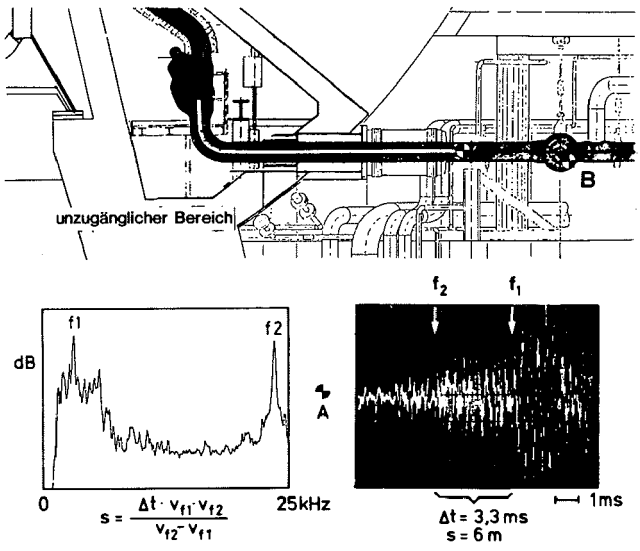


Bild 33: Lokalisierung eines Rückschlagventils als Geräuschquelle in einer Speisewasserleitung eines Siedewasserreaktors

Bei Druckwasserreaktoren traten unter anderem auf:

- Spindel/Gehäuse-Kontakte bei Speisewasserventilen,
- Rohr/Hänger-Anschläge im Not- und Nachkühlsystem,
- Fremdkörper in der Eintrittskammer eines Dampferzeugers.

Die jeweils letzten aufgeführten Beispiele bei SWR und DWR sollen kurz erläutert werden.

Das erste Beispiel einer erfolgreichen Diagnose mit Hilfe der Körperschallmeßtechnik ist in Bild 33 gezeigt: Starke Geräusche aus einem unzugänglichen Bereich, nämlich dem Containment eines Siedewasserreaktors, wurden mit Hilfe der Körperschallanalysentechnik identifiziert. In diesem Fall wurden im zugänglichen Bereich an einer Speisewasserleitung nachträglich Körperschallaufnehmer angebracht. Die Diagnose erfolgte unter Verwendung einer neuen Feinstrukturanalysentechnik, wobei ausgenutzt wurde, daß das Übertragungsverhalten des Aufnehmers A im wesentlichen durch zwei Resonanzlinien charakterisiert ist. Im Spektrum der Hintergrundgeräusche (Bild 33, unten links) ist die Resonanz der Aufnehmerhalterung mit f_1 und die Aufnehmerresonanz selbst mit f_2 gekennzeichnet. Durch Detailanalyse der beobachteten Körperschallbursts (Bild 33, unten rechts) und Verwendung der Ausbreitungsgeschwindigkeit des a_0-Wellenmodes im Bereich der beiden hauptsächlichen Frequenzen f_1 und f_2 konnte mit Hilfe der im Kapitel „Schallausbreitung und Schallortung" erläuterten Beziehung die Schallentstehungsstelle bis auf einen halben Meter genau, und zwar auf den Bereich des Rückschlagventils C innerhalb des unzugänglichen Bereiches, lokalisiert werden. Zusammen mit Detailanalysen von Körperschallsignalen eines bauähnlichen, aber zugänglichen Ventils B, das ebenfalls geringe, in der Struktur ähnliche Anschlaggeräusche emittierte, konnte darüber hinaus auch der Erzeugungsmechanismus geklärt werden. Die gestellte Schadensprognose, nämlich Lagerschaden an einem Rückschlagventil, wurde bei der nachfolgenden Inspektion voll bestätigt: Die ausgeschlagene Lagerschale wies ein gegenüber den Auslegungswerten 10fach vergrößertes Radialspiel auf.

Im zweiten Beispiel (Bild 34) sind einzelne Burstformen gezeigt. Nachgeschaltete Detailanalysen hatten zum Ergebnis, daß ein loses Teil im Dampferzeuger eines Druckwasserreaktors in guter Übereinstimmung mit dem späteren Befund prognostiziert werden konnte. Das nach der Abschaltung gefundene Teil, eine nach Revisionsarbeiten vergessene Reibahle von 43 g, stimmte gut mit der Voraussage überein: ein Teil von 50 bis 100 g in der Dampferzeugereintrittskammer. Auch ein derartig kleines Teil ist nicht unkritisch, da durch ständiges Behämmern des Rohrbodens die Dichtschweißung der im Boden steckenden Heizrohre beschädigt werden kann, so daß zwischen Primär- und Sekundärsystem Leckagen auftreten könnten. Beschädigungen der Plattierungen können zumindest einen langen Stillstand des Kraftwerks verursachen; in Frankreich zum Beispiel erforderten entsprechende Reparaturarbeiten acht Monate. Im vorliegenden Fall betrug der Zeitraum zwischen Abfahren vom Leistungsbetrieb mit nachfolgendem Abfahren von Temperatur, Absenken des Wasserstands im Dampferzeuger bis zur Bergung des lokalisierten Teils nur vier Tage.

Zusammenfassung und Ausblick

Die vorgestellten Systeme zur Schadenfrüherkennung, die auf Methoden zur Schwingungs- und Körperschallüberwachung basieren, ergänzen sich gegenseitig in der Aufgabe, belastbare Informationen aus unzugänglichen Bereichen von Kernkraftwerken zu liefern. Damit wird die sicherheitstechnische Zielsetzung, nämlich Frühindikatoren für die mechanische Integrität der Primärkreiskomponenten und Kerneinbauten zur Verfügung zu haben, mit einem technisch/wirtschaftlich vertretbaren Aufwand erreicht.

Die Integrität wurde bislang im wesentlichen durch umfangreiche Inspektionen, Prüf- und Wartungsarbeiten in vorgegebenen, regelmäßigen Zeitintervallen sichergestellt. Durch eine frühzeitige Erkennung von Schadensentwicklungen mit Hilfe der neuen Überwachungs-/Diagnoseeinrichtungen noch während des Reaktorbetriebs werden neben der

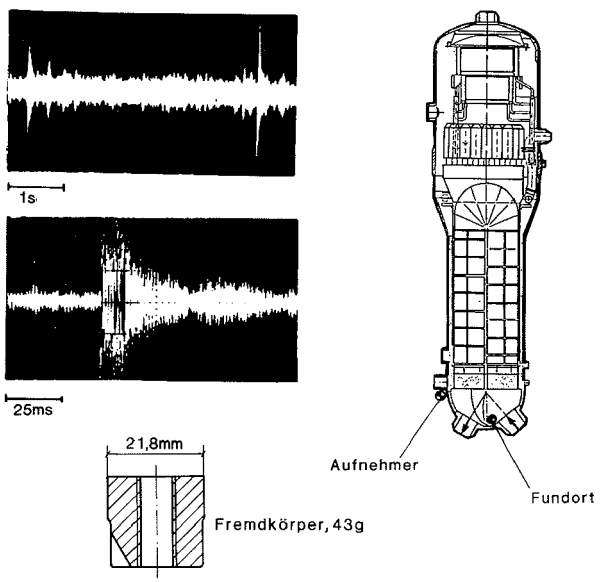


Bild 34: Identifizierung eines losen Teils in der Dampferzeuger-Eintrittskammer eines Druckwasserreaktors

Vermeidung von Folgeschäden eine Reihe weiterer Nutzeffekte erreicht: Gezielte Inspektionen helfen den Prüfumfang zu reduzieren, präventive Wartung vermeidet nicht geplante Abschaltungen, optimal vorbereitete Reparaturen wirken sich günstig auf Strahlenbelastung des Reparaturpersonals aus und erhöhen die Verfügbarkeit der Anlage.

Daneben sollte aber der allgemeine Informationsgewinn durch derartige Überwachungssysteme nicht übersehen werden, der beispielsweise nach außergewöhnlichen Systembelastungen, bei Problemen in Parallelanlagen oder bei nur vorläufig ausführbaren Reparaturmaßnahmen entscheidende Bedeutung erlangen kann. Hier können betriebsbegleitende Überwachungsmaßnahmen mit den Diagnosesystemen zur Unterstützung von Betriebsgenehmigungen dienen. Die Summe aller Nutzeffekte hat – bei Betreibern von Kernkraftwerksanlagen wie bei aufsichtführenden Stellen – in der Bundesrepublik Deutschland inzwischen zu einer breiten Akzeptanz der Schadenfrüherkennungsverfahren geführt.

GRS hat sich nach Abschluß der grundsätzlichen Methodenentwicklung intensiv mit dem Know-how-Aufbau bei anlagenspezifischen Signalmustern und betrieblichen Erfahrungen befaßt. Sie führt in einer Reihe von Anlagen sowohl bei der Schwingungs- wie bei der Körperschallüberwachung wiederkehrend Signalanalysen durch. GRS ist apparativ und personell in der Lage, kurzfristig belastbare Analyseresultate und Diagnosen zu liefern. Zahlreiche erfolgreiche Interpretationen von abweichenden Signalmustern und zutreffende Prognosen haben dies in den letzten Jahren bewiesen.

Die Entwicklung bei Schadenfrüherkennungsmethoden in Deutschland deckt sich mit der wichtiger Reaktorbetreiberländer. Zusammen mit Frankreich und Holland – aber auch verschiedenen Ostblockstaaten – nimmt Deutschland eine führende Stellung in der Anwendung dieser Techniken ein. Laufende Weiterentwicklungsarbeiten beziehen sich – wieder in Übereinstimmung mit dem Ausland – auf mehr Automatisierung durch Anwendung von Mustererkennungsverfahren und auf mehr Operateurentlastung durch Einbringung rechnergestützter Systeme, das heißt künstlicher Intelligenz. Der Einsatz moderner Überwachungs-/Diagnosesysteme zur Schadenfrüherkennung bei wichtigen Reaktorkomponenten wird sicherlich dazu beitragen, daß der im internationalen Vergleich hervorragende Rang der deutschen Reaktoranlagen hinsichtlich Sicherheit und Verfügbarkeit weiter gefestigt wird.

Schrifttum

[1] Wach, D.: Neue Überwachungssysteme in Kernkraftwerken. GRS-Fachgespräch 1980. Technische Mitteilungen, 74. Jg., Heft 1/2, Jan./Feb. 1981; GRS-20 (März 1981)

[2] Bastl, W.; R. Sunder; D. Wach: The Influence of Noise Diagnostic Techniques on the Safety and Availability of Nuclear Power Plants. Proceedings of the SMORN-IV Conference, Dijon, 1984.

[3] Wach, D.; R.Sunder; J. Weingarten: Überwachungssysteme und Diagnosetechniken zur Schadenfrüherkennung in Kernkraftwerken. VGB-Kraftwerkstechnik, 64. Jg., Heft 2, Februar 1984.

[4] Bauernfeind, V.; B. Olma; R. Sunder; D. Wach: Schwingungs- und Schallüberwachung an Primärkreiskomponenten von Kernkraftwerken. VDI-Tagung Schwingungsüberwachung von Maschinen, Hamburg, 7. - 8. November 1985.

[5] Jax, P.; K. Ruthrof; V. Streicher: Early Failure Monitoring Systems for LWR Operation. IAEA Symp. on Advances in Nuclear Power Plant Availability, Maintainability and Operation, Munich, May 20-23, 1985.

[6] Wehling, H.-J.; W. Schütz; D. Wiemerslage: Experimental Modal Analysis - An Auxiliary Means in Reactor Vibration Monitoring. Proceeding of the CSNI Specialists' Meeting on Continuous Monitoring for Assuring Coolant Circuit Integrity, London, August 12-14, 1985.

[7] Raible, B.; K. Komma; H.-G. Heuser; H. Pitzl; J. Poloczek: Das Körperschallüberwachungssystem KAP-80. Der Maschinenschaden 55, Heft 2, pp 122-128, 1982.

[8] Olma, B.: Source Location and Mass Estimation in Loose Parts Monitoring of LWRs. Proceedings of the SMORN-IV Conference, Dijon, 1984.

[9] Sunder, R.; D. Wach: Operational Experience with Vibration Monitoring and Loose Parts Detection in German LWRs. Proceedings of the CSNI Specialists' Meeting on Continuous Monitoring for Assuring Coolant Circuit Integrity, London, Aug. 12-14, 1985.

Diskussion

H. Pleger (GRS):

Die vorgetragenen Ergebnisse sind beeindruckend. Werden solche Überwachungssysteme auch im Ausland eingesetzt?

R. Sunder (GRS):

In der Tat gelangen in zahlreichen Ländern Schadenfrüherkennungsverfahren an Leistungsreaktoren zum Einsatz: Dies beweisen eine Reihe von einschlägigen internationalen Konferenzen, die dem Erfahrungsaustausch von Diagnosespezialisten dienen. Neben der Bundesrepublik Deutschland ist wohl in Frankreich und in den Vereinigten Staaten der Einsatz am weitesten vorangetrieben. Aber auch in den Staaten des Ostblocks wie Ungarn, der Tschechoslowakei oder der DDR werden diese Methoden angewendet. Im Gegensatz zu den bei uns etablierten getrennten Systemen zur Schwingungs- und Körperschallüberwachung werden häufig kombinierte Systeme betrieben, das heißt, die Beschleunigungssignale der Lose-Teile-Überwachung werden im niederfrequenten Bereich gemeinsam mit Neutronenflußsignalen zur Schwingungsüberwachung herangezogen. Nach unserer Meinung haben die bisher realisierten kombinierten Systeme aufgrund der reduzierten Instrumentierung Nachteile bezüglich der Aussagesicherheit bei Schwingungs-Prognosen. Ein weiterer Unterschied im Instrumentierungskonzept – zum Beispiel bei Druckwasserreaktoren vom russischen Typ – basiert auf konstruktiven Besonderheiten der Reaktor-Baulinien und entsprechend anders gelagerten Überwachungsaufgaben. Die international zu beobachtenden intensiven Entwicklungsarbeiten zur Schadenfrüherkennung lassen zweifelsfrei erkennen, daß derartige Informationssysteme auch im Ausland einen hohen Stellenwert besitzen.

R.O. Schneider (KfK):

Welche Chancen sehen Sie, die Schallemissionstechnik zur Detektion von Rißwachstum einzusetzen?

R. Sunder (GRS):

Die Schallemissionstechnik zur Rißdetektion nutzt das hochfrequente Übertragungsverhalten sogenannter Schallemissionssonden im Frequenzbereich 100 kHz bis 1 MHz. Für die Körperschallüberwachung hat sich dagegen der akustische Bereich, erweitert bis 25 kHz oder im Extremfall 30 kHz, bewährt. Dies nur zur Abgrenzung.

Die Schallemissionstechnik wird bereits heute – neben anderen Methoden wie zum Beispiel Ultraschallprüfverfahren – bei Wiederholungsprüfungen von Großkomponenten eingesetzt. Eine kontinuierliche Überwachung auf Rißausbreitungsgeräusche während des Leistungsbetriebs von Reaktoranlagen wird durch die vorhandenen Betriebsgeräusche erschwert. Deshalb ist von entscheidender Bedeutung, einen Frequenzbereich zu nutzen, in welchem ein starker Rückgang der Strömungsgeräusche in Relation zu den Rißgeräuschen existiert, zum Beispiel zwischen 400 und 500 kHz. In Anbetracht der Tatsache, daß nicht alle zu überwachenden Strukturen gleich „laut" sind, ist eine gezielte Schallemissionsüberwachung in Gebieten mit geringen Hintergrundgeräuschen durchaus denkbar. Die Arbeiten zur Erprobung eines derartigen Systems an Leistungsreaktoren sind zur Zeit jedoch noch nicht abgeschlossen.

W. Nef (KKW Beznau):

Zu Ihren Ausführungen bezüglich der Auslandsentwicklung möchte ich etwas ergänzen: Wir haben in Beznau seit mehreren Jahren eine Körperschallüberwachungsanlage in Betrieb – seit einem Jahr die zweite Generation. Beide Anlagen sind in Betrieb.

Rechnergestützte Kernüberwachung

Von D. Beraha[1])

Kurzfassung

Die Verfügbarkeit leistungsfähiger Prozeßrechner in der Kraftwerksanlage ermöglicht es, komplexe dreidimensionale Kernmodelle parallel zum Prozeß mitzurechnen. Auf solchen schnellen Kernsimulatoren baut das Konzept des in der GRS entwickelten Systems zur Kernüberwachung auf. Ziel der Kernüberwachung ist die Information des Wartenpersonals über den aktuellen Kernzustand. Darüber hinaus ist eine Leistungsverteilungsregelung auf Grundlage des Kernsimulators entwickelt worden, die vorgegebene lokale Grenzwerte berücksichtigen kann. Dadurch wird eine optimale Leistungsverteilungsregelung unter Einhaltung der Grenzwerte erreicht und der Kernzustand in einem sicheren Betriebsbereich gehalten. Ein interaktives Kommunikationssystem, das über Farbgrafik verfügt, ermöglicht die einfache Handhabung des Kernüberwachungssystems sowie die Darstellung des Kernzustands und wichtiger Kenngrößen.

Das System zur Kernüberwachung hat den Entwicklungsstand eines Prototypsystems erreicht, das im Kraftwerk erprobt werden kann. Die erzielten Ergebnisse lassen erwarten, daß mit der Kernüberwachung ein wesentlicher Beitrag zur Sicherheit, Verfügbarkeit und Wirtschaftlichkeit erzielt wird.

Abstract

The availability of powerful computers in nuclear power plants allows to run complex three-dimensional core models in parallel to the process. Such fast core simulators provide the basis for the core surveillance system developed at GRS. Aim of the core surveillance is to provide the operator with information on the actual core state. Furthermore, a power distribution control has been developed utilizing the core simulator which is able to observe given local constraints.Thus, the control keeps the core state in a safe operating region within the specified constraints. An interactive communication system with colour grafics provides for ease of handling the core surveillance system and for display of the core state and important characteristic values.

The core surveillance system has reached the state of a prototype system which can be tested in the power plant. The obtained simulation results indicate the potential of the core surveillance to significantly contribute to safety, availability and economy of plant operation.

Einleitung

Die Entwicklung von Rechenprogrammen zur Nachbildung der physikalischen Vorgänge im Reaktorkern war in den letzten Jahren gekennzeichnet durch immer kürzere Rechenzeiten bei gleichbleibender oder sogar höherer Genauigkeit der Ergebnisse. Dies ist zum einen auf den Einsatz verbesserter mathematischer Verfahren, zum anderen auf die Rechnerentwicklung zurückzuführen. Die Verfügbarkeit schneller Prozeßrechner hat den Gedanken nahegelegt, solche Rechenprogramme nicht nur zur Kernauslegung, sondern auch zur Betriebsverfolgung im Kernkraftwerk einzusetzen. Die Ankopplung der Rechenprogramme an Meßsignale der Kerninstrumentierung erlaubt, den Reaktorzustand mitzurechnen, wobei auch nicht direkt beobachtbare Größen wie die Spaltproduktverteilung bestimmt werden können. Erste Ziele, die mit parallel zum Prozeß (on-line) rechnenden Kernmodellen („Kernsimulatoren") erreicht worden sind, betreffen

[1]) Dipl.-Ing. David Beraha, Gesellschaft für Reaktorsicherheit (GRS) mbH, Garching

- Darstellung und verfeinerte Analyse des dreidimensionalen Kernzustands,
- Abspeichern der Leistungsgeschichte (lokale Brennstableistungen) zur Abbrandverfolgung und Brennelement-(BE)-Einsatzplanung.

Im off-line Betrieb sind Nach- und Vorausrechnungen möglich, die durchgeführt werden zur

- Analyse von betrieblichen Vorgängen und Störungen,
- Optiminierung der betrieblichen Fahrweise (zum Beispiel Anfahren am Zyklusende),
- Voroptimierung von BE-Einsatzplänen vor Ort.

Kernsimulatoren und dazugehörige Kommunikationssysteme, die zumeist mit grafischen Farbsichtgeräten ausgestattet sind, werden von Kraftwerks- und Brennelementherstellern sowie von betreibernahen Organisationen angeboten. In den USA sind solche Systeme in etwa der Hälfte aller SWR- und in einigen DWR-Anlagen, in Deutschland in den Kraftwerken Biblis B [1] und Krümmel [2] installiert.

Die bisherigen Einsatzbereiche von Kernsimulatoren zeigen deutlich das Ziel der Anbieter auf, der Physikmannschaft in der Anlage ein verfeinertes Hilfsmittel zur Betriebsverfolgung und -planung zur Verfügung zu stellen. Dementsprechend sind die Kernsimulatoren auf größtmögliche örtliche Auflösung und Genauigkeit ausgerichtet. Neuberechnungen des Kernzustands benötigen bei voller Auslastung des Prozeßrechners einige Minuten und werden in größeren, der Xenondynamik angepaßten Zeitabständen von etwa einer Stunde oder bei Überschreiten vorgegebener Auslöseschwellen (zum Beispiel Änderung des Lastzustands, Stabstellungsänderungen) angestoßen. Ein kontinuierlicher Betrieb des Kernsimulators mit kurzen Abtastschritten ist noch nicht möglich.

Die eigentliche Kernüberwachung im Sinne eines Beitrags zur Betriebssicherheit hat gegenüber den genannten vorwiegend wirtschaftlichen Aspekten eine weitergehende Zielsetzung, nämlich

- den Kernzustand in möglichst kurzen Abtastschritten laufend zu verfolgen und zu analysieren,
- das Wartenpersonal jederzeit über den Abstand zu betrieblichen Grenzwerten zu informieren und bei Überschreiten der Grenzwerte zu warnen,
- durch Vergleich von Meßsignalen und berechnetem Kernzustand Störungen (auch Meßfühlerausfälle) zu erkennen,
- rechnerische Ersatzwerte bei Meßfühlerausfall zu bilden.

Die Kernüberwachung bietet darüber hinaus die Handhabe, automatisch aktive Eingriffe zu veranlassen, das heißt die Leistungsverteilung derart zu regeln, daß ein die Kerneinbauten schonender Reaktorbetrieb erzielt wird, wobei alle für den sicheren Betrieb gültigen lokalen Grenzwerte eingehalten werden.

Ein System, das diesen Anforderungen gerecht wird, leistet einen wichtigen Beitrag zur Vorsorgesicherheit (defense-in-depth), indem einerseits das Wartenpersonal jederzeit über die Vorgänge im Kern detailliert unterrichtet wird, andererseits auf Regelungsebene lokale Begrenzungen unterhalb der Schutzgrenzwerte eingeführt werden, womit die Ansprechhäufigkeit von Reaktorschutz oder Schutzbegrenzungen verringert wird. Die GRS hat ein System zur Kernüberwachung, das diesen Anforderungen gerecht wird, im Rahmen eines vom BMFT geförderten Forschungsprojekts in Zusammenarbeit mit der Kraftwerk Union (KWU) für SWR und DWR entwickelt. Im folgenden wird ein Überblick über die Kernüberwachung und die erzielten Ergebnisse gegeben.

Prinzipien der GRS-Kernüberwachung

Das Prinzipschema in Bild 1 verdeutlicht den Aufbau des Systems zur Kernüberwachung. Das Schema gilt für DWR- und SWR-Kernüberwachung, die einzelnen Module sind aber je nach Reaktortyp unterschiedlich aufgebaut.

An zentraler Stelle steht ein schneller Kernsimulator. Der Kernsimulator wird an die Signale aus der Kerninstrumentierung angebunden, um die unvermeidlichen kleinen Abweichungen des rechnerisch ermittelten Kernzustands vom tatsächlichen Zustand, die sich im Lauf der Zeit akkumulieren können, laufend zu korrigieren. Der Kernsimulator wird off-line unterstützt durch sogenannte Basisprogramme, nämlich Kernauslegungsprogramme, die in größeren zeitlichen Abständen die im Kernsimulator verwendeten abbrandabhängigen Parameter auffrischen. Ferner können die Basisprogramme auch Brennstabversagensmodelle beinhalten, aus denen abbrandabhängige Grenzwerte der zulässigen lokalen Leistungsdichten zur größtmöglichen Brennstoffschonung bestimmt werden können. Die Off-line-Unterstützung entspricht etwa dem Funktionsumfang derzeit im KKW eingesetzter Kernrechenprogramme. Aus dem vom Kernsimulator ermittelten Kernzustand (Verteilung von Leistungsdichte, Temperaturen, Spaltprodukten, Kühlmitteldichte) werden in einem Analysemodul wichtige Kenngrößen (Heißstellenfaktoren, DNB-Verhältnisse, Abstand zur Siedelinie) berechnet. Kernzustand und Kenngrößen werden mit den zulässigen Werten verglichen, bei Überschreiten von Grenzwerten erfolgt eine Warnmeldung über das Kommunikationssystem.

Auf dem im Kernsimulator verwendeten Kernmodell baut die Leistungsverteilungs-(LV)-Regelung auf. Aufgabe der LV-Regelung ist es, die LV möglichst nahe an einer last- und abbrandabhängigen Sollverteilung zu halten und beim DWR die räumlichen Xenonschwingungen zu unterdrücken, wobei technische Randbedingungen (zum Beispiel maximale Stabfahrgeschwindigkeit) und sicherheitsbedingte Grenzwerte eingehalten werden müssen. Um den Anforderungen an eine LV-Regelung nach langen, an die Betriebsweise (zum Beispiel Lastzyklus) angepaßtem Regelungshorizont bei gleichzeitig kurzen Regelungsintervallen (s. auch Kapitel „Leistungsverteilungsregelung") zu genügen, ist die LV-Regelung in zwei Schichten mit unterschiedlichen Aufgaben angeordnet. Die

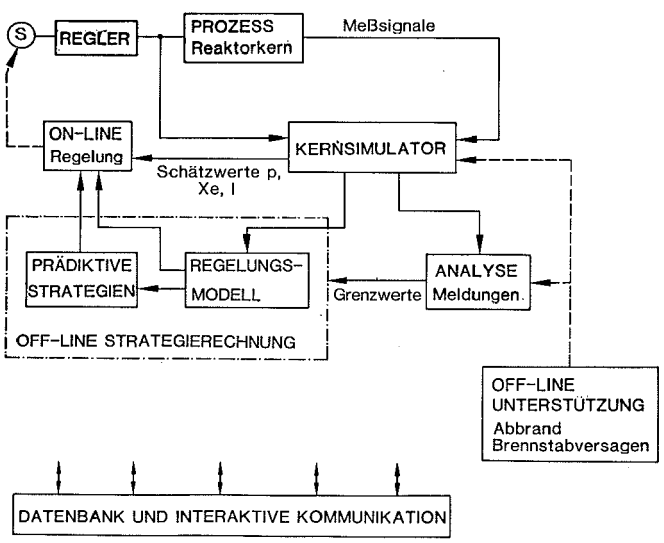


Bild 1: Prinzipschema der GRS-Kernüberwachung

übergeordnete Schicht, die in ihrer Funktion einem Leitrechner entspricht, prädiktiert off-line optimale Fahrstrategien über den gesamten Regelungshorizont. Die On-line-Regelung versucht diese Fahrstrategien unter Berücksichtigung des aktuellen Kernzustands, der im allgemeinen von der Off-line-Prädiktion abweichen wird, durchzusetzen.

Die von der LV-Regelung vorgeschlagenen Maßnahmen werden im Probebetrieb von Hand gefahren werden: Verläuft die Erprobung zufriedenstellend, kann in einem nächsten Schritt der Regelkreis geschlossen werden, indem die Stellgrößen der LV-Regelung als Sollwerte für Stabstellungsregler oder Steuerstabfahrrechner vorgegeben werden.

Die im Kernsimulator und der LV-Regelung berechneten Größen sind über das Kommunikationssystem abrufbar, das mit Drucker, Rechenterminal und grafischen Farbsichtgeräten ausgestattet ist. Ablaufsteuerung des Systems, Anwahl der Ergebnisdarstellung und Vorgabe von Sollwerten für die LV-Regelung erfolgen interaktiv. Anstelle des Kommunikationssystems kann, wenn die Kernüberwachung in die Reaktorleittechnik integriert wird, auch ein Warteninformationssystem treten.

Kernsimulatoren

Für den Kernsimulator und die LV-Regelung sind Modelle von DWR- und SWR-Kern entwickelt worden. Der Entwurf der Kernmodelle für beide Reaktortypen ist von zwei Gesichtspunkten nachhaltig beeinflußt, der Forderung nach hoher Rechengeschwindigkeit, um eine schnelle Abtastung des Prozesses zu ermöglichen, und der Anwendbarkeit des Kernmodells für den Regelungsentwurf. Um die geforderte Rechengeschwindigkeit zu erreichen, sind folgende vereinfachende Modellannahmen getroffen worden [3]:

- Transienten der Neutronenkinetik und Thermodynamik klingen im Vergleich zur Änderungsgeschwindigkeit der Stellgrößen sehr rasch ab und werden daher als quasistationäre Prozesse behandelt.
- Die Beschreibung der Neutronendichte wird durch die Zustandsgröße „Leistungsdichte" ersetzt (1 1/2-Gruppen-Formalismus).
- Ausgangspunkt für den Modellentwurf sind Daten des Basisprogramms. Die Kernparameter werden um einen vom Basisprogramm beschriebenen Startpunkt nach den Zustandsgrößen entwickelt.
- In einem Volumenelement können mehrere BE verschiedener Anreicherung zusammengefaßt werden. Die Kernparameter werden über das Volumenelement gemittelt (Homogenisierung und Rebalancing [4]). Die Homogenisierung ist zwar mit einer geringeren örtlichen Auflösung verbunden, führt aber zu einer erheblichen Steigerung der Rechengeschwindigkeit bei ausreichender Genauigkeit der Volumenmittelwerte.
- Die Beziehungen zwischen benachbarten Volumenelementen werden in Form von Kopplungskoeffizienten angegeben (Core Response Matrix Method, [5]).
- Der Reaktordruck beim SWR wird als konstant angenommen.
- die Spaltproduktverteilung wird in jedem Volumenelement durch zwei nichtlineare Differentialgleichungen (Xenon-Jod-Dynamik) beschrieben.

Besondere Anstrengungen sind unternommen worden, um die Thermohydraulik, die beim SWR den stärksten Einfluß auf die LV ausübt, sehr genau nachzubilden.

Die Forderung nach Anwendbarkeit zum LV-Regelungsentwurf bestimmt die Struktur der Modellgleichungen, indem Zustandsgrößen und Stellglieder in den Modellgleichungen explizit auftreten, im Gegensatz zur impliziten Berücksichtigung in den Wirkungsquerschnitten bei Kernauslegungsprogrammen.

Die aus diesen Annahmen resultierenden Modelle führen auf eine nichtlineare algebraische Matrixgleichung N-ter Ordnung (*N* bezeichnet die Anzahl von Volumenelementen) mit

einer dünn besetzten Systemmatrix zur Beschreibung der LV, und auf $2N$ nichtlineare gewöhnliche Differentialgleichungen für die Xe-I-Dynamik [6]. Die beiden Gleichungssysteme sind miteinander verkoppelt. Die Lösung des Gesamtsystems erfolgt iterativ mit einem schnellen Newton-Verfahren, wobei die sparse Belegung der Systemmatrix ausgenützt wird. Mit den vereinfachenden Modellannahmen und dem eingesetzten Lösungsverfahren werden zum Beispiel beim SWR-Modell bei einer Viertelkerneinteilung in 372 Volumenelemente (31 Kanäle mit je 12 axialen Nodes) typische Rechenzeiten von 1 s auf dem Großrechner AMDAHL 470/V8 erzielt; ein schneller Prozeßrechner würde etwa das Fünffache dieser Rechenzeit benötigen. Die Rechenzeit steigt ungefähr proportional zur Anzahl der Kanäle, quadratisch zur axialen Unterteilung an.

Die Verifikation des Kernmodells wurde im Vergleich mit Kernauslegungscodes durchgeführt. Dieses Verfahren ist einer direkten Verifikation anhand von Meßgrößen aus einem Kernkraftwerk vor allem deshalb vorzuziehen, weil die von Auslegungscodes berechneten Kernzustände in weit höherer räumlicher Auflösung vorliegen als die Signale der Kerninstrumentierung, und der Verifikationsaufwand deutlich geringer ist. Die Auslegungsprogramme selbst sind einer langjährigen Validierung unterworfen worden und gewährleisten eine gute Übereinstimmung mit dem Prozeß mit bekannten, geringen Fehlertoleranzen.

Die Zusammenfassung der Ergebnisse der durchgeführten Vergleichsrechnungen zeigt, daß die Maximalfehler in Zonen geringer Leistungsdichten auftreten, während die zur Berechnung der sicherheitsrelevanten Parameter verwendeten Werte der höchstbelasteten Bündel sehr gut beschrieben werden. Die Heißstelle wird immer richtig lokalisiert. Die nodalen Maximalfehler liegen bei 8 %, ausgenommen Volumenelemente in der Nähe der bewegten Regelstäbe, wo Fehler bis zu 14 % auftreten können.

Die Verifikation des SWR-Modells ist noch nicht abgeschlossen. Vergleichsrechnungen zeigen im allgemeinen mittlere Fehler (RMSE) von 3 % für axiale Schichten und Kanäle und 6 % für einzelne Volumenelemente (Maximalfehler $\approx$ 10 %). Diese Werte sind vergleichbar mit Ergebnissen von Codes der FLARE-Gruppe [7].

Leistungsverteilungsregelung

Um der in Kapitel „Prinzipien der GRS-Kernüberwachung" gerecht zu werden, Reaktorleistung und LV nahe an zeitabhängigen Sollwerten zu halten, beim DWR räumlich Xenonschwingungen zu unterdrücken und alle Beschränkungen des Betriebsbereichs zu berücksichtigen, benötigt die LV-Regelung ein ausreichend genaues Abbild der Regelstrecke. Die Kernmodelle wurden bereits in den ersten Entwurfsphasen an den von der LV-Regelung gestellten Anforderungen ausgerichtet, so daß sie ohne weitere Vereinfachungen als Grundlagen für die LV-Regelung verwendet werden konnten. Somit wird erreicht, daß die Modellgenauigkeit auch in der LV-Regelung vollständig erhalten bleibt.

Das Kernmodell beschreibt allerdings einen komplexen Prozeß, dessen dynamisches Verhalten von zeitlich sehr unterschiedlich sich auswirkenden Faktoren geprägt ist. Der Entwurf einer zentralisierten LV-Regelung mit gut bekannten Verfahren wäre zwar prinzipiell möglich, dessen Realisierung würde jedoch die heute verfügbare Rechenkapazität um Größenordnungen übersteigen. Es sind daher hierarchische Verfahren eingesetzt worden, um die dem Prozeß zugrundeliegenden Strukturen zu analysieren und die komplexe Regelungsaufgabe in einfachere dezentrale Teilaufgaben aufzutrennen [8].

Zur Analyse des Prozesses bietet sich eine Zerlegung nach der Zeit an, die auf eine Mehrschichtenstruktur gemäß Bild 2 führt. Die eigentliche LV-Regelung ist in zwei Schichten, der Optimierungs- und der On-line-Regelungsschicht, angeordnet. Der Entscheidungshorizont der Optimierungsschicht richtet sich an der mittelfristig wirksamen Xenon-Jod-Dynamik und an der Betriebsart des Kernkraftwerkes, vor allem an der Dauer von Lastzyklen, aus. Die Anforderungen an die LV-Regelung werden formal in einem Gütekriterium definiert. Aufgabe der Optimierungsschicht ist es, das Gütekriterium unter den

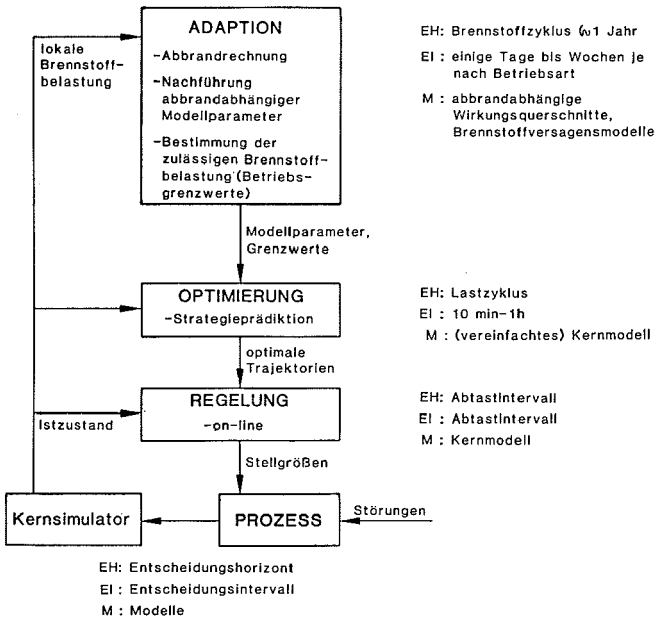
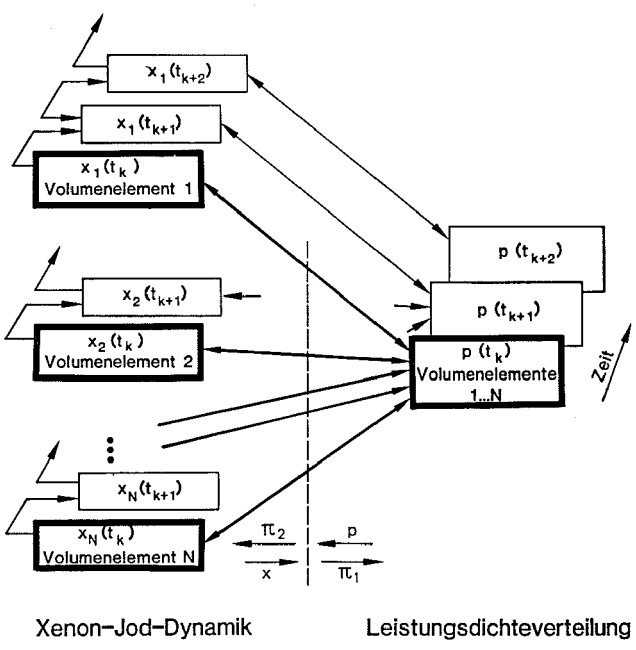


Bild 2: Zeitliche Schichtenstruktur des Prozesses



p Leistungsdichtevektor, x Xenon-Jod-Vektor

Bild 3: Verkopplung Leistungsdichte - Spaltproduktdynamik

Nebenbedingungen der nichtlinearen Kernmodellgleichungen und der ebenfalls nichtlinearen Beschränkungen von Stell- und Zustandsgrößen zu minimieren.

Die Herleitung eines geschlossenen Regelgesetzes zur Lösung dieses komplexen Regelungsproblems ist nicht möglich, wohl aber die Voraussage einer optimalen Steuerfolge off-line. Aus Rechenzeitgründen besteht die Einschränkung, möglichst lange Entscheidungsintervalle anzusetzen, die sich an der Geschwindigkeit der Lasttransiente und an der Xenon-Jod-Dynamik ausrichten (10 min bis 1 h). Die On-line-Umsetzung der von der Optimierungsschicht vorausberechneten optimalen Steuerfolgen oder Fahrstrategien wird von einer unterlagerten Regelungsschicht übernommen. Die Regelungsschicht gleicht unvermeidliche, nicht voraussagbare diskrete und stochastische Störungen des Prozesses und Unsicherheiten im Kernmodell laufend aus. Sie besitzt gegenüber der Optimierungsschicht wesentlich kleinere Entscheidungsintervalle in der Größenordnung einer Minute.

Die Sollverteilung der Leistungsdichten, die Parameter des Kernmodells und die Betriebsgrenzen sind abbrandabhängig. Es ist daher erforderlich, die Sollwerte und das Kernmodell in größeren zeitlichen Abständen dem Abbrandzustand anzupassen. Diese Aufgabe wird von einer der Optimierung überlagerten Adaptionsschicht vorgenommen. Die Struktur, die sich aus der Zerlegung nach der Zeit ergibt, spiegelt sich im Prinzipschema (Bild 1) wider. Die Adaptionsschicht entspricht der Off-line-Unterstützung, die Optimierungsschicht der Strategierechnung, und die Regelungsschicht der On-line-Regelung.

Der Entwurf des Verfahrens zur Lösung der Aufgaben von Optimierungs- und Regelungsschicht geht aus von der Untersuchung der Verkopplung von Leistungsverteilung und Xenon-Jod-Dynamik, die in Bild 3 schematisch dargestellt ist. Der Zeitverlauf der Xenonkonzentration in einem Volumenelement wird nur durch dessen Leistungsdichte beeinflußt, nicht aber durch angrenzende Volumenelemente, während die Leistungsdichte zwar von allen benachbarten Volumenelementen abhängt, aber zeitlich nur durch die Xenon-Jod-Dynamik verkoppelt ist. Trennt man die Verkopplungen an der Mittellinie auf, so zerfällt das Gesamtsystem in eine Xenon-Jod- und ein LV-Untersystem. Das Xe-I-Untersystem selbst zerfällt in N örtlich entkoppelte Systeme, die jeweils durch zwei Differentialgleichungen erster Ordnung beschrieben werden, das LV-Teilsystem zerfällt in K (Anzahl der Entscheidungsintervalle) zeitlich entkoppelte Systeme, die durch eine algebraische Matrixgleichung beschrieben werden. Diese fast natürliche Dekomposition in

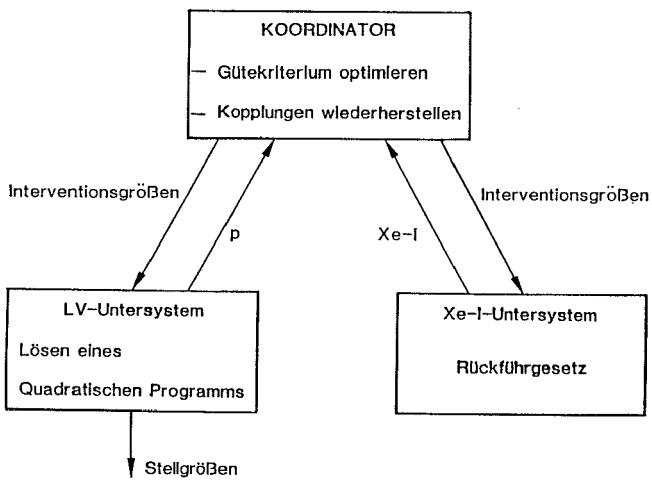


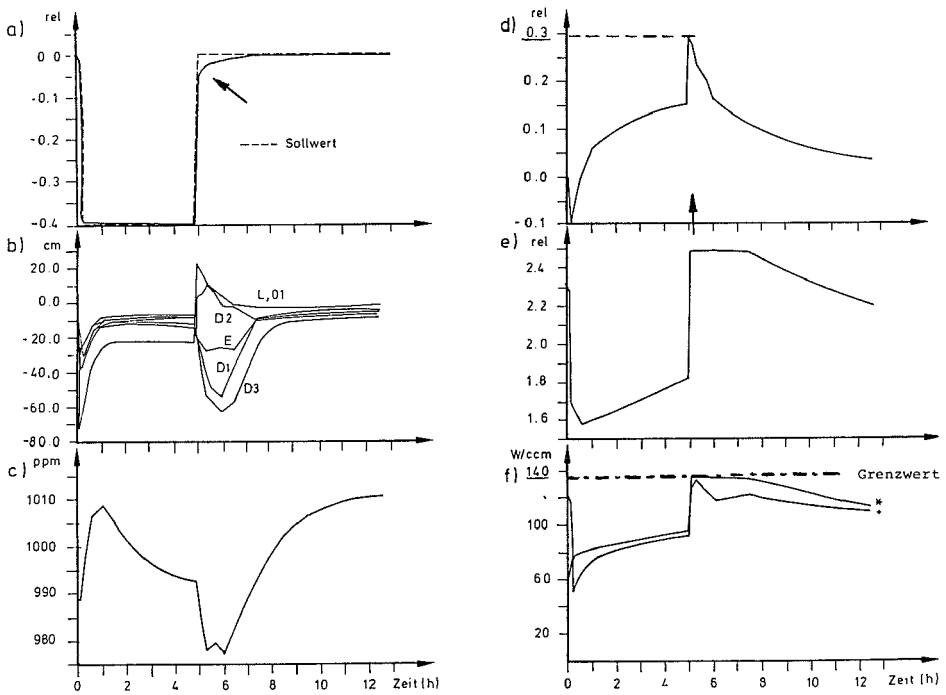
Bild 4: Hierarchischer Aufbau der LV-Regelung

Teilsysteme bietet sehr günstige Voraussetzungen für die Anwendung hierarchischer Mehrebenenverfahren.

Bild 4 zeigt schematisch den hierarchischen Aufbau der LV-Regelung. Die Teilsysteme lösen auf untergeordneter Ebene unabhängig voneinander die ihnen zugewiesene Regelungsaufgabe. Der Koordinator ruft die Untersysteme iterativ auf und modifiziert deren Aufgaben durch Vorgabe sogenannter Interventionsgrößen derart, daß einerseits das Gesamtziel, die Optimierung des Gütekriteriums, erreicht wird, andererseits die ursprünglichen Kopplungen zwischen den Untersystemen wiederhergestellt werden.

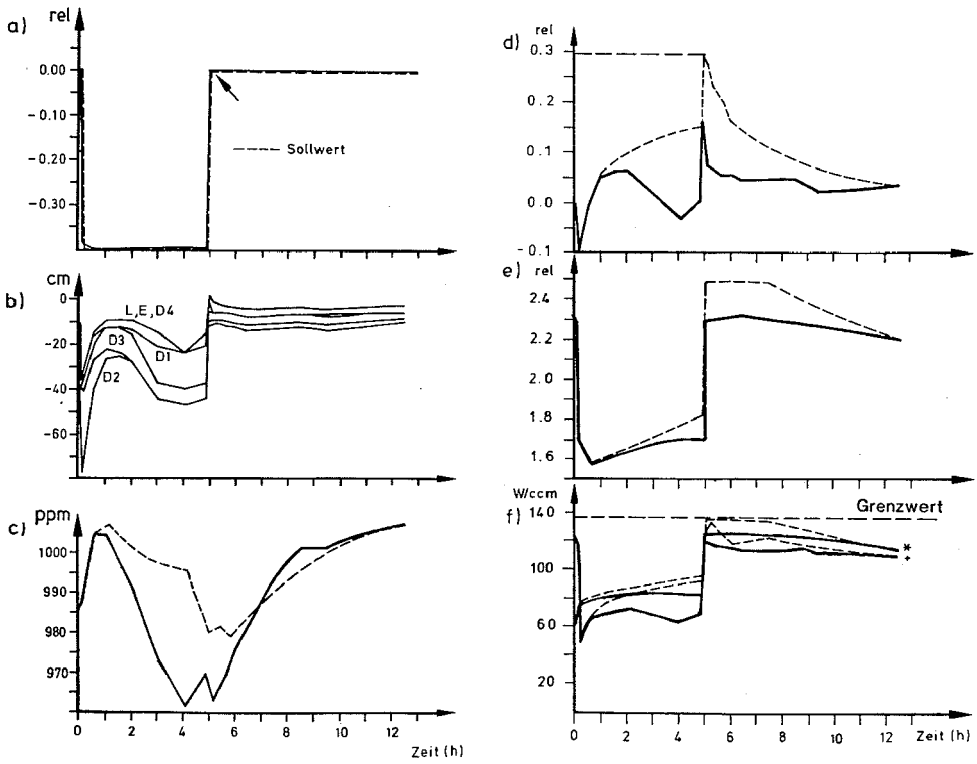
Sowohl Optimierungs- als auch Regelungsschicht besitzen diese Mehrebenenstruktur, wobei der Koordinator der Optimierungsschicht allerdings auf zwei Ebenen mit etwas umfangreicheren Aufgaben aufgeteilt ist. Da die Regelungsaufgaben der Teilsysteme wesentlich einfacher und schneller zu lösen sind als die Gesamtaufgabe, wird auch bei einer Kerneinteilung in eine große Zahl von Volumenelementen eine hohe Rechengeschwindigkeit erreicht. Es ergeben sich Rechenzeiten, die im allgemeinen nur geringfügig über der vom Kernsimulator benötigten Zeit liegen.

Die Bilder 5 und 6 zeigen Ergebnisse der Simulation von schnellen Lastwechseln (100 % auf 40 % Vollast in fünf Minuten, Wiederanfahren auf Vollast im Xenon-Maximum) beim DWR. Der LV-Regelung wird vorgegeben, dem Leistungssollwert so eng wie möglich zu folgen, wobei in keinem Volumenelement eine höhere Leistungsdichte als 135 W/cm^3 erreicht werden darf. Dieser Grenzwert ist schärfer als der im Betrieb zulässige Wert, um die Wirksamkeit der LV-Regelung besser herauszuarbeiten.



a) Reaktorleistung
b) Stabeintauchtiefe
c) Borkonzentration
d) Axiale Schieflast
e) Leistungsformfaktor
f) Lokale Leistungsdichten

Bild 5: Regelung mit lokalen Leistungsdichtebegrenzungen



a) Reaktorleistung
b) Stabeintauchtiefe
c) Borkonzentration
d) Axiale Schieflast
e) Leistungsformfaktor
f) Lokale Leistungsdichten

Bild 6: Optimale Fahrstrategie

Bild 5 entspricht einer On-line-Regelung ohne Vorgabe optimaler Fahrstrategien. Die Lastminderung wird erreicht, indem alle Stabgruppen in den Kern eingefahren werden. Die sich aufbauende Spaltproduktvergiftung bewirkt, daß über die Stellglieder Reaktivität eingebracht werden muß. Die geringere Xenonkonzentration in der oberen Kernhälfte bewirkt zum Zeitpunkt des Hochfahrens im Zusammenwirken mit dem Ziehen der Stäbe eine starke Leistungsüberhöhung, wodurch die Leistungsdichtegrenzwerte in einigen Volumenelementen erreicht werden.

Die Regelung wirkt einer Verletzung der Grenzwerte entgegen, indem die diesen Volumenelementen am nächsten liegenden Stabbänke (D1- und D3-Bank) in den Kern eintauchen. Gleichzeitig versucht die Regelung, den geforderten Leistungssollwert durch Ausfahren der übrigen Stabbänke einzustellen. Der Leistungssollwert wird wegen der Begrenzungen jedoch nicht erreicht, die Reaktorleistung kann nur bis auf 95 % der Nennleistung angehoben werden. Auch in den folgenden Zeitschritten sind die Begrenzungen aktiv, so daß die Reaktorleistung erst nach einer Stunde die Nennleistung erreicht. Die axiale Schieflast nimmt zum Zeitpunkt des Hochfahrens einen Wert von 29 % an, und wird erst anschließend ausgeregelt. Der Formfaktor erreicht den Maximalwert von 2,5.

Bild 6 enthält die optimierte Fahrstrategie. Nach der Leistungsreduktion antizipiert die Fahrstrategie das Hochfahren, indem die Leistungsüberhöhung durch Einfahren aller

Stabgruppen in die untere Kernhälfte geschoben wird. Um den Leistungssollwert zu halten, muß gleichzeitig die Borkonzentration stärker als in Bild 5 reduziert werden. Dadurch wird die Wirksamkeit der Stabgruppen beim Hochfahren erhöht, so daß der Leistungssollwert erreicht wird. Die Schieflast wird auf 15 %, der Formfaktor auf 2,38 begrenzt.

Die vorgestellten Simulationen zeigen, daß auch bei schnellen und großen Laständerungen die Regelung ohne Vorgabe von prädiktierten optimalen Strategien innerhalb der gegebenen Grenzwerte bleibt, daß aber der Spielraum für eine Verbesserung der Regelgüte groß ist.

Ankopplung des Kernmodells an den Prozeß

Im mitrechnenden Betrieb des Kernsimulators bauen sich, wenn keine Meßinformation aus dem Prozeß in das Kernmodell rückgekoppelt wird, Abweichungen zwischen Kernmodell und Prozeß auf. Es ist daher eine laufende Anpassung an den Prozeßzustand notwendig. Eine Methode zur Adaption des Modells, die auf einem Schätzfilter (Kalman-Filter) beruht, ist in der GRS entwickelt und an DWR-Simulatoren erprobt worden [9].

Ausgegangen wird von einer der LV-Regelung sehr ähnlichen Zerlegung des Modells in ein LV- und ein Xe-I-Untersystem. Die Meßsignale der Kerninstrumentierung werden mit den vom Koordinator aus der Schätzung der Leistungs- und Spaltproduktverteilung ermittelten Rechengrößen verglichen. Die Abweichungen zwischen Messung und Rechnung (der sogenannte Innovationsterm) werden in das LV-Untersystem rückgeführt und veranlassen das LV-Untersystem zur Berechnung einer verbesserten Schätzung der LV. Der Koordinator zieht über die Vorgabe von Interventionsgrößen das Xe-I-Untersystem nach. Der Vorgang wird wiederholt bis die ursprünglichen Kopplungsbedingungen der Untersysteme erfüllt sind. Ausgabe des mit einem Filter erweiterten Kernsimulators sind Schätzwerte für die nicht vollständig meßbare LV und die nicht beobachtbaren Xenon- und Jodverteilungen.

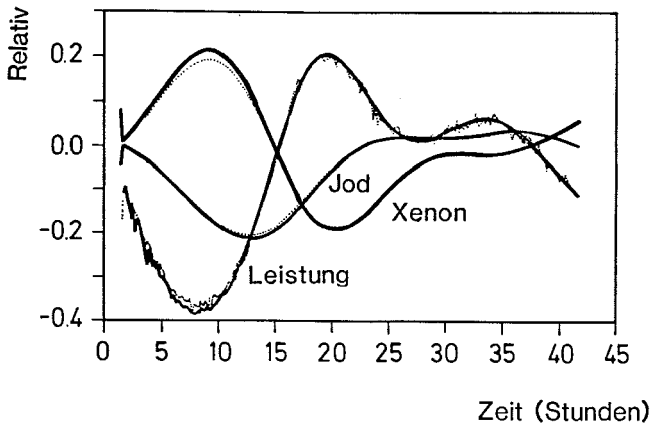
Im durchgeführten Test des Filters ist die Rolle des Prozesses, die Meßsignale zu liefern, vom Kernsimulator übernommen worden. Simulator und Meßsignale wurden mit kontinuierlichen Rauschquellen versehen. Die Parameter des im Filter verwendeten Kernmodells wurden gegenüber dem Kernsimulator verändert, um die im tatsächlichen Betrieb bestehende Unstimmigkeit zwischen Prozeß und Modell zu simulieren. Ein Testergebnis ist in Bild 7 dargestellt, das den Verlauf der Leistungs-, Xenon- und Joddichte für das Volumenelement mit dem größten anfänglichen Fehler zeigt.

Nach wenigen Abtastschritten wird die LV recht gut approximiert. Die Adaptionsgeschwindigkeit auf die Xe-I-Dynamik ist von deren Zeitkonstanten abhängig, so daß erst nach etwa 20 h eine gute Übereinstimmung mit dem Mittelwert der Meßgrößen erreicht wird.

Anstelle eines Schätzfilters können auch Modellparameter durch Messungen adaptiert werden. Das Schätzfilter bietet aber den Vorteil, daß der Innovationsterm zur Früherkennung von Störungen und Meßsignalfehlern herangezogen werden kann [10]. Die Auswertung des Innovationsterms zur Fehlererkennung ist derzeit noch Gegenstand von Forschungsarbeiten, mit Ergebnissen auf diesem Gebiet ist erst in Zukunft zu rechnen.

Kommunikationssystem

Das Kommunikationssystem soll die Funktion von Kernsimulator und LV-Regelung transparent machen, einen Überblick über den Kernzustand und die wichtigen Kenngrößen geben, und interaktive Eingriffe des Betriebspersonals ermöglichen. Der Grundgedanke beim Entwurf war, eine asynchrone Schnittstelle zwischen den im festen Zeittakt arbeitenden Systemen Kernsimulator und LV-Regelung und den Anforderungen seitens des Betriebspersonals zu schaffen. Als zentrale Schnittstelle ist eine Daten-



.....Referenz, ———— Schätzung

Bild 7: Gefilterte Leistungs-, Xenon- und Joddichten eines Volumenelements

bank eingesetzt worden, die für ein bestimmtes vorgebbares Zeitfenster alle relevanten Daten speichert. Der Abruf der Daten erfolgt über deren Kennung in der Datenbank, unabhängig von der Reihenfolge neu eintreffender Daten. Die variable Datenbankstruktur erlaubt eine sehr einfache Anpassung des Kommunikationssystems an verschiedene Kernsimulatoren. Die interaktiven Funktionen beziehen sich im wesentlichen auf die Vorgabe von Sollwerten für die LV-Regelung (soweit nicht durch eine Sollwertführung vorgegeben) und die Anwahl der von Kernsimulator und LV-Regelung erzeugten Informationen. Neben der Ausgabe am Drucker werden semi- und vollgrafische Farbsichtgeräte eingesetzt, die von zwei Softwarepaketen, dem SCORPIO-Grafikteil des OECD Halden Reactor Project und der GRS-Entwicklung INDIGO, getrieben werden. Die für die auf dem NORD 100/500-Prozeßrechnersystem ablaufende Laborversion realisierten Bildtypen umfassen

- Darstellungen von Kernquerschnitten mit Farbcodierung der Leistungs- und Temperaturverteilungen.
- Axiale LV entlang eines beliebig anwählbaren Kanals oder über alle Kanäle gemittelt.
- Trendkurven wichtiger Kernparameter. Ausgewählt werden können Sätze von Trendkurven, die im mitrechnenden Betrieb zu jedem neu errechneten Schritt aufgefrischt werden, oder stationäre Trendkurven zum Beispiel für den prädiktiven Betrieb.
- Balkendiagramme, die den Abstand von Grenzwerten der Regelung, der Leittechnik-Begrenzungseinrichtungen und des Schutzsystems angeben. Bei Überschreiten von Grenzwerten wird über Farbwechsel der Balken eine Warnung ausgeben.
- Teillastdiagramme mit vergangenen und aktuellen Betriebspunkten.

Zusammenfassung

Die GRS-Kernüberwachung zielt darauf ab, das Potential von Kernsimulatoren zu nutzen, um das Wartenpersonal laufend über den Kernzustand zu informieren und bei Erreichen von betrieblichen Grenzwerten zu warnen, und um die Leittechnik zu befähigen, die Leistungsverteilung im Kern zu regeln und die Grenzen des Betriebsbereichs einzuhalten.

Es sind schnelle Kernsimulatoren für DWR und SWR entwickelt worden, die eine gute Übereinstimmung mit Rechenprogrammen zur Kernauslegung zeigen. Auf Basis der Kernmodelle ist eine hierarchische, auf einem Prozeßrechner im Echtzeitbetrieb ablauffähige LV-Regelung realisiert worden, deren Leistungsfähigkeit an Fallstudien demonstriert worden ist.

Das System zur Kernüberwachung hat den Entwicklungsstand eines Prototypsystems erreicht. Für den Einsatz in einem Kernkraftwerk sind zunächst Kernsimulator und LV-Regelung an die Gegebenheiten des Kernkraftwerkes anzupassen. (Implementierung auf dem Kraftwerksrechner, Adaptieren von Modellparametern). In einer extensiven Offline-Testphase ist die Qualität des Kernüberwachungssystems sicherzustellen, ehe der Kreis LV-Regelung-Prozeß geschlossen werden kann. Die bisher erzielten Simulationsergebnisse lassen erwarten, daß mit der Kernüberwachung ein wesentlicher Beitrag zur Sicherheit, Verfügbarkeit und Wirtschaftlichkeit erzielt wird.

Schrifttum

[1] Bauer, F.; H. Heckermann, K. Siegel und U. Wolff: Fortschrittliches Kernüberwachungssystem für Biblis. Jahrestagung Kerntechnik, Berlin, Juni 1983.

[2] Lemke, H.D.; D. Pleuger und U. Schmidt: Fortschrittliche Nuklearrechnungen (FNR) für den SWR. Atomkernenergie Kerntechnik, Bd. 41 (1982)

[3] Höld, A., and O. Lupas: A nonlinear 3D real-time model for PWR nuclear power plants. Model description. GRS-A-751, Sept. 1982.

[4] Siewers, H.: An efficient coarse mesh rebalancing method for nodal cores. ATKE 28, 1976, pp. 175 - 178.

[5] Ancona, A.; M. Becker, M.D. Beg, D.R. Harris and A.D. Menezes: Nodal coupling by response matrix principles. Nuclear Science Eng. 64, 405, 1977.

[6] Beraha, D. and I. Karppinen: Power distribution control by hierarchical optimisation techniques. ANS/ENS Int. Meeting. Munich, Apr. 27 - 29, 1981.

[7] Gupta, N.K.: Nodal methods for three-dimensional simulators. Progress in Nuclear Energy, 7, 1981, pp. 127 - 149.

[8] Mesarovic, M.D., D. Macka and Y. Takahara: Theory of hierarchical, multilevel systems. Academic Press, 1970.

[9] Beraha, D.: Hierarchical control and estimation of the power distribution in PWR's. IFAC 9th World Congress, Budapest 1984.

[10] Chow, E.Y., and A.S. Willsky: Analytical Redundancy and the Design of Robust Failure Detection Systems.IEE Trans. Autom. Control, Vol. AC-29, No. 7, 1984.

Diskussion

W. Aleite (KWU):

Sie sagten, zwei dieser Teil-Simulatoren seien in Betrieb, ein Quadrex/NIS-Typ in Biblis und ein KWU-FNR in Krümmel. Außer diesen sind zwei weitere in Auftrag: 1 FNR für den SWR in Würgassen und ein zu entwickelnder für den SNR I in Kalkar.

Ich möchte hier etwas zu deren sinnvollem praktischen Einsatz sagen. Aus der GRS/KWU-Zusammenarbeit beim SWR wissen Sie, daß unter Einschaltung eines FNR eine Leistungsverteilungsregelung entwickelt wird. Ich würde dem Einsatz einer solchen Leistungsverteilungsregelung im SWR-Gebiet erst dann ohne Einschränkung zustimmen, wenn der SWR eine Leistungsdichtebegrenzung wie der DWR hat. Dann würde ich auch dem Operateur lieber erst diese Eingriffsmöglichkeiten geben, genau wie der einkanaligen Einrichtung, die über ein paar Rechner läuft. Wir haben das auch alles schon langfristig ins Auge gefaßt. Sobald wir beim DWR die neue, sehr viele potentere, rechnergestützte Generation der Leittechnik eingeführt haben, werden wir uns vermehrt mit dem SWR befassen, um auch dort eine Verteilungsregelung und eine Leistungsdichtebegrenzung für einen der Folgereaktoren zu entwickeln (oder gar einen laufenden damit aufzurüsten). Während beim SWR das Hauptinteresse immer dem Kern gilt, ist beim DWR die Dringlichkeit für die Entwicklung einer voll rechnergestützten Leistungsverteilungsregelung nicht gegeben. Wir haben hier eine (konventionelle) Leistungsverteilungsregelung, deren heutige Potenz von einer neuen Version ja erst wieder erreicht werden muß. Ich verspreche mir nicht sehr viele verfahrenstechnische Vorteile von deren Einsatz beim DWR.

Zu unserem PRINS-System sieht man immer einen Simulator dargestellt. Dieser Simulator steht noch nicht ganz fertig zur Verfügung, ist aber angebotsreif. Er kann und soll auch on-line laufen. Er simuliert nicht nur den Kern, sondern ebenfalls den Primärkreislauf und eine vereinfachte Sekundärseite. Vor allen Dingen enthält er die neue Leittechnik. Einen dieser Simulatoren haben wir angeboten. Leider kommt es z.Zt. aus bestimmten Gründen nicht zum Auftrag. Diese DWR-Teil-Simulatoren sind jedoch für uns mehrfach von großer Bedeutung. Ein Exemplar wird z.Zt. bei uns im Labor entwickelt und betrieben. Er dient dort zur Wartenentwicklung und Entwicklung der modernen rechnergestützten Leittechnik. Vor allem können diese Teil-Simulatoren aber zur Ergänzungs- und Spezialschulung benutzt werden. Die Schulung an den Voll-Simulatoren hat ja gezeigt, daß hauptsächlich der Teil des Gesamt-Simulators bei der Schulung am intensivsten genutzt wird, der mit diesen Teil-Simulatoren simuliert wird, das Verständnis der komplexen Leittechnik, die wir beim DWR schon haben, und deren Potenz wir in Zukunft auch auf den SWR übertragen wollen.

Mir gefällt nicht so ganz, daß man in die zur Zeit für den SWR in Entwicklung befindlichen Programme Regelungs- und Begrenzungsfunktionen implementiert. Ich werde dieser einkanaligen Ausführung nur mit großen Bedenken zustimmen. Ich halte eine Lösung, bei der die Begrenzungen mehrkanalig getrennt laufen, für die richtige, so daß die Regelung vor Erreichen von Begrenzungswerten optimal arbeiten kann. Vielleicht kann man einige milde Eingriffe der Begrenzungen innerhalb der Regelung vorsehen, diese dürfen aber nicht deren Zeitbedarf bestimmen.

W. Bastl (GRS):

Wenn wir hier von einem möglichen späteren Einsatz gesprochen haben, haben auch wir den SWR gesehen. Wir sind auch der Meinung, daß es dort wichtiger ist. Dies ist auch im Ausland so – nicht so sehr, was die Regelung angeht, sondern was Systeme zur Überwachung des Kernzustandes angeht – wo solche Systeme in immer größerem Maße eingesetzt werden. Auch viele Betreiber in Deutschland haben den Wunsch, solche Systeme

einzusetzen.Was die Applikationen angeht, die Herr Beraha nannte, so sind das keine Vorläufer des GRS-Systems, sondern Systeme anderer Firmen.

D. Beraha (GRS):

Ich glaube nicht, daß es Zufall ist, daß diese Begrenzungseinrichtungen, die sich beim DWR so bewährt haben, beim SWR nicht zur Verfügung stehen. Das ist sicherlich zum einen darauf zurückzuführen, daß die SWR-Linie einige Zeit nicht so intensiv verfolgt worden ist. Zum anderen sind die Verhältnisse nicht so einfach wie beim DWR. Dadurch muß man einerseits auf bessere Modelle zurückgreifen. Die Diskussion des Einsatzes von Modellen für Themen, die sicherheitsrelevant sind, geht hauptsächlich über Validierung und Verifikation der Software und Hardware. Wenn also beim DWR die Möglichkeit gegeben wird, zum Beispiel durch mehrere Rechner die Verfügbarkeit dieser Systeme sicherzustellen, dann ist hier vielleicht auch wieder eher eine Möglichkeit gegeben.

W. Aleite (KWU):

Ich möchte noch 2 Dinge ergänzen: Das noch größere Interesse des Auslands an einer DWR-Kernsimulation und einer rechnergestützten Regelung ist sicher damit zu begründen, daß dort (außer bei Babcock & Wilcox) keine Incore-Detektoren verwendet werden und damit keine echte Leistungsdichtebegrenzung zur Verfügung steht, wie wir sie haben. Für die KWU ist es insbesondere für den Schwerwasserreaktor Atucha II eine große Beruhigung, daß die Arbeiten zur rechnergestützten Leistungsverteilungsregelung gemacht worden sind, und wir diese Möglichkeiten haben, denn ich fürchte, daß für den Kern, von Atucha II, der durch die schrägen Stäbe eine besondere Problematik hat, einfache Regelungsmethoden nicht ausreichen werden.

Teilnehmerverzeichnis

A

Alder, Heinrich
Schweiz. National-Versicherungsgesellschaft
Postfach 85, CH–4003 Basel

Aleite, Werner, Dipl.-Ing.
KWU AG
Postfach 32 20, 8520 Erlangen

Anders, Uwe, Dipl.-Phys.
TÜV Norddeutschland e.V.,
Große Bahnstr. 31, 2000 Hamburg 54

Andritzky, Heinz, Dipl.-Ing.
Stadtwerke München
Postfach 20 22 22, 8000 München 2

Antoni, Robert, Dipl.-Ing.
GRS
Schwertnergasse 1, 5000 Köln 1

Aschhoff, Heinz-Gerhard, Dr.
Uhde GmbH
Friedrich-Uhde-Str. 15, 4600 Dortmund

Assmus, Reinhard, Dipl.-Ing.
Energiesysteme Nord GmbH
Walkerdamm 17, 2300 Kiel

Ay, Hans-W., Dipl.-Ing.
KWU AG
Postfach 9 62, 6050 Offenbach

B

Baier, Jürgen, Dr.-Ing.
Noell GmbH
Postfach 62 60, 8700 Würzburg

Bartsch, Hans, Obering.
Swedish State Power Board
S–16287 Vaellingby

Basse, Hermann, MR Dr.
Bayerisches Staatsministerium für Landesentwicklung und Umweltfragen
Rosenkavalierplatz 2, 8000 München 81

Bastl, Werner, Dr.-Ing.
GRS
Forschungsgelände, 8046 Garching

Beck, Jürgen, Dipl.-Ing.
Hartmann & Braun
Landsberger Str. 328, 8000 München 21

Becker, Karl Eugen, Dr.
TÜV Bayern e.V.
Westendstr. 199, 8000 München 21

Becker, Klaus, Prof. Dr.
DIN Normenausschuß Kerntechnik
Postfach 11 07, 1000 Berlin 30

Beckurts, Karl Heinz, Prof. Dr.
Siemens AG
Postfach 83 27 40, 8000 München 83

Bedrich, Manfred, Dipl.-Ing.
TÜV Baden e.V.
Dudenstr. 28, 6800 Mannheim

Beraha, David, Dipl.-Ing.
GRS
Forschungsgelände, 8046 Garching

Bernhardt, Siegfried, Dipl.-Ing.
GKN
Postfach, 7129 Neckarwestheim

Beuerle, Hans-Jürgen, Dipl.-Ing.
Oberbauleitung KKI 2
Postfach 11 42, 8307 Essenbach

Bilger, Hartmut, Dr.
Energie-Versorgung Schwaben AG
Postfach 1 58, 7000 Stuttgart 1

Birkhofer, Adolf, Prof. Dr. Dr.-Ing. E.h.
GRS
Forschungsgelände, 8046 Garching

Birkle, Michael, Dr.
Fraunhofer-Institut für Informations- und Datenverarbeitung
Sebastian-Kneipp-Str. 12, 7500 Karlsruhe 1

Bochmann, Hans-Peter, MinDir. Dr.
Bundesministerium des Innern
Postfach 17 02 90, 5300 Bonn

Borsch, Peter, Dr.
KFA
Postfach 19 13, 5170 Jülich 1

Bröcker, Bernhard, Dr.
Preussische Elektrizitäts AG
Postfach 48 49, 3000 Hannover 91

Bromkamp, Karl-Heinz, Dr.-Ing.
VEW AG
Postfach 9 41, 4600 Dortmund 1

Brosche, Dieter, Dr.-Ing.
Bayernwerk AG
Nymphenburger Str. 39, 8000 München 2

Büchler Heinz, MR Dr.
Bundesministerium des Innern
Postfach 17 02 90, 5300 Bonn 1

Buettner, Wolf-E., Dipl.-Ing.
GRS
Forschungsgelände, 8046 Garching

Burchardt, W.
TÜV Rheinland e.V.
Postfach 10 17 50, 5000 Köln 1

Burkart, Klaus, Dr.
KfK
Postfach 36 40, 7500 Karlsruhe 1

Burmeister, Werner, Ing.
KKW Krümmel
Elbuferstr. 82, 2054 Geesthacht

Butz, Heinz-P., Dr.
GRS
Schwertnergasse 1, 5000 Köln 1

C

Carls, Günther, Dipl.-Ing.
TÜV Norddeutschland e.V.
Große Bahnstr. 31, 2000 Hamburg 54

D

Deuster, Gerd, Dr.
FHG–IzfP
Universitätsgebäude 37, 6600 Saarbrücken

Dick, Gerhard, Dipl.-Ing.
Motor-Columbus AG
Parkstr. 27, CH–5410 Baden

Diem, Harald, Dipl.-Ing.
MPA
Pfaffenwaldring 32, 7000 Stuttgart 80

Dieterich, Lothar, Dipl.-Ing.
RWE AG
Kruppstr. 5, 4300 Essen 1

Dillmann, Jürgen
Energiewirtschaftliche Tagesfragen
Postfach 12 29, 8032 Gräfelfing

Dittmar, Herbert
KWG
Postfach 12 20, 3254 Emmerthal

Döring, Volker, Dipl.-Ing.
Ministerium für Wirtschaft, Mittelstand und Technologie
Haroldstr. 4, 4000 Düsseldorf 1

Dörler, Rudolf, Dipl.-Ing.
Fichtner – Beratende Ingenieure –
Sarweystr. 3, 7000 Stuttgart

Döttinger, Karl-Heinz, Dr.-Ing.
TÜV Stuttgart e.V.
Postfach 13 80, 7024 Filderstadt 1

Dressler, Erich, Dipl.-Phys.
KWU AG
Postfach 32 20, 8520 Erlangen

Dubbe, Rolf, Dipl.-Ing.
TÜV Norddeutschland e.V.
Große Bahnstr. 31, 2000 Hamburg 54

Dumsky, Georg, MR
Bayerisches Staatsministerium für Wirtschaft und Verkehr
Prinzregentenstr. 28, 8000 München 22

Dworzak, Franz, Dipl.-Ing.
Österr. Forschungszentrum Seibersdorf
A–2444 Seibersdorf

E

Eblenkamp, Bernhard, Dipl.-Ing.
KKS
Postfach 17 80, 2160 Stade

Edelhäuser, Hannes, RD
Bundesministerium des Innern
Postfach 17 02 90, 5300 Bonn 1

Eder, Erwin, Dr.-Ing.
Bayerisches Landesamt für Umweltschutz
Rosenkavalierplatz 3, 8000 München 81

Eibl, Josef, Prof. Dr.
Universität Karlsruhe (TH)
Institut für Massivbau und Baustofftechnologie
Postfach 63 80, 7500 Karlsruhe 1

Ellmer, Martin, Dipl.-Ing.
VAK
Postfach 6, 8756 Kahl

Engelhardt, Günther, Dr.
WAK, 7514 Eggenstein-Leopoldshafen

Erven, Ulrich, Dipl.-Ing.
GRS
Schwertnergasse 1, 5000 Köln 1

F

Faber
KWU AG
Postfach 9 62, 6050 Offenbach

Fabian, Hans-Ulrich, Dr.
Preussische Elektrizitäts AG
Postfach 48 49, 3000 Hannover 91

Felkel, Lothar, Dipl.-Inf.
GRS
Forschungsgelände, 8046 Garching

Fey, Dr.
Hartmann & Braun AG
Landsberger Str. 328, 8000 München 21

Fichtner, Norbert, Dipl.-Ing.
DIN Normenausschuß Kerntechnik
Postfach 11 07, 1000 Berlin 30

Fischbacher, Wolfgang, Dipl.-Ing.
Bayernwerk AG
Nymphenburger Str. 39, 8000 München 2

Fischer, Winfried
RWE AG
Postfach 11 40, 6843 Biblis

Floh, Werner
TÜV Bayern e.V.
Westendstr. 199, 8000 München 21

Frank, Hermann, MinDirig
Hessisches Ministerium für Wirtschaft und Technik
Kaiser-Friedrich-Ring 75, 6200 Wiesbaden 1

Franzen, L. Ferdinand, Dipl.-Phys.
IAEA
Postfach 2 00, A–1400 Wien

Freund, Jürgen, Dr.
GRS
Schwertnergasse 1, 5000 Köln 1

Freund Jürgen, Dipl.-Ing.
GRS
Schwertnergasse 1, 5000 Köln 1

Frisch, Willi, Dr.-Ing.
GRS
Forschungsgelände, 8046 Garching

Fröhlich, Hans-Joachim, Dipl.-Ing.
KWU AG
Postfach 9 62, 6050 Offenbach

Fuhs, Kurt, Dipl.-Ing.
KKP
Postfach 11 40, 7520 Philippsburg

G

Geppert, Uwe, Dipl.-Ing.
Ingenieurbüro Geppert
Hauptstr. 20, 7141 Beilstein

Geyer, Karl Heinz, Dipl.-Ing.
KWU AG
Postfach 3220, 8520 Erlangen 2

Gill, Ralph, Dipl.-Ing.
GRS
Forschungsgelände, 8046 Garching

Göing, Jochen, Dipl.-Ing.
Energiesysteme Nord GmbH
Walkerdamm 17, 2300 Kiel 1

Goßner, Stephan, Dipl.-Ing.
GRS
Forschungsgelände, 8046 Garching

Gremm, Otto, Dr.
KWU AG
Postfach 32 20, 8520 Erlangen 2

Guse, Klaus
Dornier System GmbH
Postfach 13 60, 7990 Friedrichshafen

H

Haase, Klaus-Dieter
DWK
Hamburger Allee 4
3000 Hannover 1

Hässler, Günther, Dr.-Ing.
Badenwerk AG
Badenwerkstr. 2, 7500 Karlsruhe 1

Hagen, Armin, RD
Bundesministerium des Innern
Postfach 17 02 90, 5300 Bonn 1

Hagen, Ekkehard, Dipl.-Ing.
KKP
Postfach 1140, 7522 Philippsburg

Hahn, Kurt, Dipl.-Ing.
Ministerium für Wirtschaft, Mittelstand und Technologie
Haroldstr. 4, 4000 Düsseldorf 1

Haug, Peter, Dr.
Deutsches Atomforum e.V.
Heussallee 10, 5300 Bonn

Hausner, Otto, Dr.
Isar-Amper-Werke AG
Postfach 37 02 20, 8000 München 37

Heinbuch, Dipl.-Ing.
Bayernwerk AG
Postfach 20 03 40, 8000 München 2

Heinsohn, Hartmuth, Dipl.-Ing.
GRS
Schwertnergasse 1, 5000 Köln 1

Heithoff, Johannes, Dr.
Isar-Amper-Werke AG
Postfach 37 02 20, 8000 München 37

Heldt, Peter H.
Deutsche Lufthansa AG
Flughafenbasis, 6000 Frankfurt 75

Hertlein, Fritz, MR Dr.
Bayerisches Staatsministerium für Landesentwicklung und Umweltfragen
Rosenkavalierplatz 2, 8000 München 81

Heusener, Gerhard, Dr.
KfK
Postfach 3640, 7500 Karlsruhe

Hicken, Enno, Prof. Dr.
GRS
Forschungsgelände, 8046 Garching

Himmel, Theodor, MR
Bundesministerium des Innern
Postfach 17 02 90, 5300 Bonn 1

Hoemke, Paul, Dipl.-Ing.
GRS
Schwertnergasse 1, 5000 Köln 1

Hoensch, Volker, Dipl.-Ing.
GKN
Postfach, 7129 Neckarwestheim

Hoermann, Heinz, Dr.-Ing.
GRS
Forschungsgelände, 8046 Garching

Hoffmann, Egon, MinDirig Dr.
Bayer. Staatsministerium für Wirtschaft und Verkehr
Prinzregentenstr. 28, 8000 München 22

Hoffmann, W.E., Dipl.-Ing.
Vereinigung der TÜV e.V.
Kurfürstenstr. 56–58, 4300 Essen 1

Hofmann, Hans, Dipl.-Ing.
SDK Ingenieurunternehmen GmbH
Postfach 22 27, 7850 Lörrach

Hofmann, Horst, Dipl.-Ing.
KWU AG
Postfach 32 20, 8520 Erlangen

Hohlefelder, Walter, Dr.
GRS
Schwertnergasse 1, 5000 Köln 1

Huismann, Jürgen
SBK
Postfach 12 20, 4192 Kalkar

I

Irlbeck, Dipl.-Ing.
Bayernwerk AG
Postfach 20 03 40, 8000 München 2

Ivens, Günter
AVR
Postfach 14 11, 4000 Düsseldorf 1

J

Jäger, Erich, MR
Ministerium für Umwelt und Gesundheit
Postfach 31 80, 6500 Mainz

Jaerschky, Rudolf
Isar-Amper-Werke
Postfach 37 02 20, 8000 München 37

Jaeschke, A., Dr.
KfK
Postfach 36 40, 7500 Karlsruhe 1

Jahns, Armin, Dipl.-Phys.
GRS
Schwertnergasse 1, 5000 Köln 1

Jaschek, Hilmar, Prof. Dr.-Ing.
Universität des Saarlandes Lehrstuhl für Systemtheorie der Elektrotechnik
Im Stadtwald, Bau 38, 6600 Saarbrücken 11

Jax, Peter, Dr.
KWU AG
Postfach 32 20, 8520 Erlangen

Jennewein, Norbert
KRB
Postfach 300, 8871 Gundremmingen

Jost, Ueli
KKW Mühleberg
CH–3203 Mühleberg

K

Kellermann, Michael
Siemens AG
Hofmannstr. 51, 8000 München 70

Kellermann, Otto, Dipl.-Ing.
GRS
Schwertnergasse 1, 5000 Köln 1

Kemmerling, Carl, Dipl.-Ing.
KFA
Postfach 19 13, 5170 Jülich 1

Kersken, Manfred, Dipl.-Ing.
GRS
Forschungsgelände, 8046 Garching

Kiessling, Rolf, Dipl.-Ing.
GRS
Forschungsgelände, 8046 Garching

Kirmse, Rudolf, Dr.-Ing.
GRS
Forschungsgelände, 8046 Garching

Knäulein, Heinz, Ing.
KRB
Postfach 300, 8872 Gundremmingen

Knoerzer, Gerhard, Dr.
Bayernwerk AG
Nymphenburger Str. 39, 8000 München 2

Koeberlein, Klaus, Dr.
GRS
Forschungsgelände, 8046 Garching

König, Gert, Prof. Dr.
Technische Hochschule Darmstadt
Institut für Massivbau
Alexanderstr. 5, 6100 Darmstadt

Kollath, Klaus, Dr.
GRS
Schwertnergasse 1, 5000 Köln 1

Koller, Martin
NOK AG
Kernkraftwerk Beznau
CH–5312 Döttingen

Korbach, W.
TÜV Rheinland e.V.
Postfach 10 17 50, 5000 Köln 1

Korn, Norbert, Dr.-Ing.
Hartmann & Braun AG
Gräfstr. 97, 6000 Frankfurt 90

Krause, Hans-Dieter, Dr.-Ing.
GRS
Forschungsgelände, 8046 Garching

Kraut, Alfred, Prof. Dr.
Atomkernenergie – Kerntechnik
Postfach 90 07 49
8000 München 90

Krewer, Karl-Heinz, MR
Bundesministerium für Forschung und Technologie
Postfach 20 07 06, 5300 Bonn 2

Kriks, Jakob, Dr.
GRS
Forschungsgelände, 8046 Garching

Krone, Stefan, Dipl.-Phys.
VEBA-Kraftwerke Ruhr AG
Postfach 10 01 25, 4650 Gelsenkirchen

Kroppenstedt, Franz, Staatssekretär
Bundesministerium des Innern
Postfach 17 02 90, 5300 Bonn 1

Krüger, Klaus, Dipl.-Phys.
AVR
Hambacher Forst, 5170 Jülich

Krugmann, Ulrich, Dr.
KWU AG
Postfach 32 20, 8520 Erlangen

Krzykacz, Bernard, Dipl.-Math.
GRS
Forschungsgelände, 8046 Garching

Kube, Bernd, Dr.
DWK
Postfach 14 07, 3000 Hannover 1

Kukla, Wilhelm, Dipl.-Phys.
KWO
Postfach 1 00, 6951 Obrigheim

L

Lehr, Günter, MinDir Dr.
Bundesministerium für Forschung und Technologie
Postfach 20 07 06, 5300 Bonn 2

Leiter, Edgar, Dipl.-Ing.
TÜV Bayern e.V.
Westendstr. 199, 8000 München 21

Liebholz, Wolf-M., Dipl.-Ing.
Redaktion „Atomwirtschaft Atomtechnik"
Kasernenstr. 67, 4000 Düsseldorf

Lindauer, Erwin, Dr.-Ing.
GRS
Schwertnergasse 1, 5000 Köln 1

Linhardt, Joachim, RD
Bayerisches Staatsministerium für Landesentwicklung und Umweltfragen
Rosenkavalierplatz 2, 8000 München 81

Linnemann, Herbert, Dipl.-Ing.
Hochtemperatur Kernkraftwerk GmbH
Siegenbeckstr. 10, 4700 Hamm 1

Linnenfelser K.
KKP
Postfach 11 40, 7520 Philippsburg 1

Löhle, Herbert, Senator E.h. Dipl.-Ing.
Neckarwerke
Elektrizitäts-Versorgungs-AG
Postfach 3 29, 7300 Esslingen

Loew, Heinz, Prof.
Isar-Amper-Werke AG
Postfach 37 02 20, 8000 München 37

Lummerzheim, Diethard, Dr.
GRS
Schwertnergasse 1, 5000 Köln 1

M

Märkl, Hans, Dr.
KWU AG
Postfach 32 20, 8520 Erlangen

Maertz, Josef, Dipl.-Math.
GRS
Forschungsgelände, 8046 Garching

Maier, Wolfgang
KWU AG
Postfach 9 62, 6050 Offenbach

Majer, Dieter, Bauoberrat
Hessisches Ministerium für Wirtschaft und Technik
Kaiser-Friedrich-Ring 75, 6200 Wiesbaden

Mansfeld, Gerhard, Dr.-Ing.
GRS
Forschungsgelände, 8046 Garching

Mauker, Rudolf, Ltd. MR Dipl.-Ing.
Bayerisches Staatsministerium für Landesentwicklung und Umweltfragen
Rosenkavalierplatz 2, 8000 München 81

May, Horst, Dipl.-Ing.
GRS
Schwertnergasse 1, 5000 Köln 1

Meier, Rudolf, Dipl.-Ing.
Motor Columbus AG
Parkstr. 27, CH–5401 Baden

Meier, Wolfhard, Dipl.-Ing.
Ministerium für Wirtschaft und Verkehr Rheinland-Pfalz
Postfach 32 69, 6500 Mainz

Meininghaus, Richard, Dipl.-Ing.
VEW AG
Rheinlanddamm 24, 4600 Dortmund 1

Metzger, Rolf, Dipl.-Ing.
BBC
Postfach 3 51, 6800 Mannheim 1

Meusel, Ernst-Joachim, Dr.
Max-Planck-Institut für Plasmaphysik
Forschungsgelände, 8046 Garching

Meyer, Fred, Dipl.-Ing.
RWE AG
Postfach 11 40, 6843 Biblis 1

Michael, Horst, Dipl.-Ing.
TÜV Baden e.V.
Dudenstr. 28, 6800 Mannheim

Mischke, Joachim, Dipl.-Ing.
DWK
Hamburger Allee 4, 3000 Hannover 71

Mohns, Günter, Dipl.-Ing.
TÜV Norddeutschland e.V.
Große Bahnstr. 31, 2000 Hamburg 54

Momm, Dieter, Dipl.-Ing.
Deutsche Kernreaktor-Versicherungsgemeinschaft
Sedanstr. 8, 5000 Köln 1

Morsten, Gerhard
BBC AG
CH–5401 Baden

Moschke, Hans-Jürgen, Dr.
BSM Gesellschaft für Betriebsberatung mbH
Schorlemer Str. 36, 4000 Düsseldorf 11

Mühlhölzl, Harald, Dipl.-Ing.
Oberbauleitung KKI 2
Postfach 11 42, 8307 Essenbach

Müller, J.
TÜV Rheinland e.V.
Postfach 10 17 50, 5000 Köln 1

Müller-Dietsche, Walter, Dipl.-Ing.
KfK
Postfach 36 40, 7500 Karlsruhe 1

Muck, Norbert
RWE AG
Kruppstr. 5, 4300 Essen 1

Mundt, J.
Uranit GmbH
Postfach 14 11, 5170 Jülich

N

Nef, Walter, Dipl.-Ing.
NOK Kernkraftwerk Beznau
CH–5312 Döttingen

Nickel, Hubertus, Prof. Dr.
KFA
Postfach 19 13, 5170 Jülich 1

O

Orth, Karlheinz, Dipl.-Ing.
KWU AG
Postfach 32 20, 8520 Erlangen 2

Osenroth, Klaus, Dipl.-Ing.
VGB
Klinkestr. 29/31, 4300 Essen 1

P

Pätzold, Herbert
Ministerium für Ernährung, Landwirtschaft, Umwelt und Forsten
Postfach 4 91, 7000 Stuttgart 1

Peeck, Jürgen, Ing.
GKSS
Postfach 11 60, 2054 Geesthacht

Peters, Werner, Dipl.-Ing.
GKSS
Postfach 11 60, 2054 Geesthacht

Petersen, Klaus, Dr.
RWE AG
Kruppstr. 5, 4300 Essen 1

Peuker, Rüdiger, Dipl.-Phys.
Berufsgenossenschaft der Feinmechanik und Elektrotechnik
Gustav-Heinemann-Ufer 130, 5000 Köln 51

Pfaffelhuber, Josef K., MinDirig.
Bundesministerium des Innern
Postfach 17 02 90, 5300 Bonn 1

Pfister, Dieter, Dipl.-Ing.
Bundesamt für Energiewirtschaft Hauptabteilung für die Sicherheit der Kernanlagen
CH–5303 Würenlingen

Pickel, L.
TÜV Rheinland e.V.
Postfach 10 17 50, 5000 Köln 1

Plank, Heinz, Dipl.-Ing.
Bayernwerk AG
Postfach 20 03 40, 8000 München 2

Pleger, Horst, Ing. (grad.)
GRS
Schwertnergasse 1, 5000 Köln 1

Pohl, Wolfgang, Dr.
Bayerisches Landesamt für Umweltschutz
Geschwister-Scholl-Str. 9, 8022 Grünwald

Polke, Heinz, Dipl.-Phys.
GRS
Forschungsgelände, 8046 Garching

Polzenberg, Rainer, Dipl.-Ing.
AVR
Hambacher Forst, 5170 Jülich

Prinz, Hubert M., Dipl.-Phys.
FIZ
7514 Eggenstein Leopoldshafen 2

Q

Quirrenbach, Franz-Josef, Dipl.-Ing.
Vereinigung der technischen Überwachungs-Vereine e.V.
Postfach 10 38 34, 4300 Essen 1

R

Rasche, Gerwin, Dipl.-Ing.
Interatom
Postfach, 5060 Bergisch Gladbach 1

Rau, Wolfgang
Dornier System GmbH
Postfach 13 60, 7990 Friedrichshafen

Reichart, Günther, Dipl.-Ing.
GRS
Forschungsgelände, 8046 Garching

Reik, Manfred, Dipl.-Ing.
TÜV Bayern e.V.
Westendstr. 199, 8000 München 21

Reinstein, Dieter
BBC
Postfach 3 51, 6800 Mannheim

Reuter, Burkhard, Dipl.-Ing.
Kernkraftwerk-Betriebsgesellschaft mbH
Postfach, 7514 Eggenstein-Leopoldshafen 2

Riebold, Willi, Dipl.-Ing.
Euratom
Casella Postale 1, I–21020 Ispra-Varese

Rieser, Rudolf, Dipl.-Ing.
Bayernwerk AG
Postfach 20 03 40, 8000 München 2

Ritter, Karl-Heinz, Dipl.-Ing.
VAK
Postfach 6, 8756 Kahl

Rittig, Dieter, Dipl.-Phys.
GRS
Schwertnergasse 1, 5000 Köln 1

Röthlein, Brigitte, Dr.
P.M.-Magazin
Postfach 80 07 44, 8000 München 80

Roghmanns, Helmut
Energieversorgung Schwaben AG
Kriegsbergstr. 32, 7000 Stuttgart 1

Rost, Klaus-Peter, MR
Bundesministerium des Innern
Postfach 17 02 90, 5300 Bonn 1

Ruckdeschel, Walter, MR Dr.
Bayerisches Staatsministerium für Landesentwicklung und Umweltfragen
Rosenkavalierplatz 2, 8000 München 81

Rüdiger, Bodo, Dipl.-Ing.
Battelle-Institut e.V.
Am Römerhof 35, 6000 Frankfurt 90

Rubbel, Frank Egbert, Dipl.-Ing.
Niedersächsisches Ministerium für Bundesangelegenheiten
Archivstr. 2, 3000 Hannover 1

S

Saglietti, Francesca, Dipl.-Math.
GRS
Forschungsgelände, 8046 Garching

Saedtler, Ernst, Dr.-Ing.
GRS
Forschungsgelände, 8046 Garching

Schaal, Matthias, Dr.
BTI Büro für technische Innovationsberatung
Rosenstr. 5, 8031 Eichenau

Schaefer, Helmut, Prof. Dr.-Ing.
Lehrstuhl für Energiewirtschaft und Kraftwerkstechnik TU München
Postfach 20 24 20, 8000 München 2

Schaller, Dipl.-Ing.
Bayernwerk AG
Postfach 20 03 40, 8000 München 2

Schallopp, Bernhard, Dipl.-Phys.
Büro Schallopp Berlin
Ringstr. 41/42, 1000 Berlin 45

Schallopp, Elisabeth
Büro Schallop Berlin
Ringstr. 41/42, 1000 Berlin 45

Schatz, Alfred, Prof. Dr.
Institut für Kernenergetik und Energiesysteme der Universität Stuttgart
Pfaffenwaldring 31, 7000 Stuttgart 80

Scheffel, Heinz, Dipl.-Ing.
Koblenzer Elektrizitätswerk und Verkehrs-AG
Schützenstr. 80–82, 5400 Koblenz

Schier, Helge, Dr.
Hessisches Ministerium für Wirtschaft und Technik
Kaiser-Friedrich-Ring 75, 6200 Wiesbaden

Schildheur, Reinhard, Dipl.-Ing.
TÜV Baden e.V.
Dudenstr. 28, 6800 Mannheim 1

Schimetschka, Edgar, Dipl.-Phys.
Battelle-Institut e.V.
Am Römerhof 35, 6000 Frankfurt 90

Schlenker
RWE AG
Kruppstr. 5, 4300 Essen 1

Schmid, Franz, Dipl.-Ing.
TÜV Bayern e.V.
Westendstr. 199, 8000 München 21

Schmidhuber, Paul M., Dipl.-Ing.
Stadtwerke München
Blumenstr. 28, 8000 München 2

Schmidt, Günther, Prof. Dr.-Ing.
Lehrstuhl für Steuerungs- und Regelungstechnik TU München
Postfach 20 24 20, 8000 München 2

Schmidt, Rainer, Dr.
TÜV Stuttgart e.V.
Gottlieb-Daimler-Str. 7, 7024 Filderstadt

Schmidt, Wolfgang, Dr.
Bundesbahn-Zentralamt Minden
Postfach 29 60, 4950 Minden

Schmitt-Thomas, Karlheinz G., Prof. Dr.
Lehrstuhl für Metallurgie und Metallkunde TU München
Postfach 20 24 20, 8000 München 2

Schneider, R.O., Dipl.-Ing.
KfK
Postfach 36 40, 7500 Karlsruhe

Scholz, Heinrich, Dipl.-Ing.
BEWAG
Stauffenbergstr. 26, 1000 Berlin 30

Schröder, Friedrich
IZE
Stresemannallee 23, 6000 Frankfurt 70

Schrüfer, Elmar, Prof. Dr.
Lehrstuhl und Laboratorium für elektrische Meßtechnik TU München
Postfach 20 24 20, 8000 München 2

Schüller, Herbert, Dr.
GRS
Forschungsgelände, 8046 Garching

Schützle, Rainer, Dr.-Ing.
MC-W Energie-Consult GmbH
Postfach 30 08 09, 7000 Stuttgart 30

Schulz, Helmut, Dipl.-Ing.
GRS
Schwertnergasse 1, 5000 Köln 1

Schumann, Lothar, Dipl.-Ing.
Ministerium für Wirtschaft, Mittelstand und Technologie NRW
Haroldstr. 4, 4000 Düsseldorf 1

Schur, Dieter, BauDir., Dipl.-Ing.
Bayerisches Staatsministerium für Landesentwicklung und Umweltfragen
Rosenkavalierplatz 2, 8000 München 81

Schwarzer, Wolfgang, Dipl.-Phys.
GRS
Schwertnergasse 1, 5000 Köln 1

Seidel, Ernst R., MR
Bayerisches Staatsministerium für Landesentwicklung und Umweltfragen
Rosenkavalierplatz 2, 8000 München 81

Sell, Joachim
Dornier System GmbH
Postfach 13 60, 7990 Friedrichshafen 1

Seubert, Winfried, Dipl.-Ing.
Stadtwerke München
Blumenstr. 28, 8000 München 2

Simon, Manfred, Dr.-Ing.
BBC
Postfach 3 51, 6800 Mannheim 1

Sonnenburg, Heinz-Günther, Dipl.-Ing.
GRS
Forschungsgelände, 8046 Garching

Spangenberg, K.H., Dipl.-Ing.
KWO
Postfach 1 00, 6951 Obrigheim

Stadie, Klaus B., Dipl.-Ing.
OECD–NEA
38, Boulevard Suchet, F–75016 Paris

Starke, Hans, Dipl.-Ing.
Bayerisches Landesamt für Umweltschutz
Rosenkavalierplatz 3, 8000 München 81

Steiger, Werner, Dipl.-Ing.
KfK
Postfach 36 40, 7500 Karlsruhe 1

Stern, Dipl.-Ing.
Bayernwerk AG
Postfach 20 03 40, 8000 München 2

Steuer, Jürgen, Dr.-Ing.
DIN Normenausschuß Kerntechnik
Postfach 11 07, 1000 Berlin 30

Stölben, Hans
KWU AG
Postfach 32 20, 8520 Erlangen

Stucken, Günther, Dr.
GRS
Schwertnergasse 1, 5000 Köln 1

Stute, Horst, Dipl.-Ing.
GRS
Schwertnergasse 1, 5000 Köln 1

Sütterlin, Lothar, Dr.
GRS
Schwertnergasse 1, 5000 Köln 1

Sunder, Reinhold, Dipl.-Ing.
GRS
Forschungsgelände, 8046 Garching

T

Thiemler, Frank, Dipl.-Ing.
Ministerium für Wirtschaft, Mittelstand und Technologie NRW
Haroldstr. 4, 4000 Düsseldorf 1

Thierfelder, Hans-Georg, Dipl.-Ing.
BBC
Postfach 3 51, 6800 Mannheim 1

Thoenes, Hans-Willi, Prof. Dr.
Rheinisch-Westfälischer TÜV e.V.
Postfach 10 32 61, 4300 Essen 1

Tietze, Alfons, Prof. Dr.
Universität Gesamthochschule Wuppertal
Fachbereich 14
Gauss Str. 20, 5600 Wuppertal 1

Timm, Manfred, Dr.-Ing.
Preussische Elektrizitäts AG
Postfach 48 49, 3000 Hannover 91

Tomas, Peter, Dr.
Institute „Ruder Boskovic"
P.O.B. 10 16, YU–41001 Zagreb

Trauboth, H., Prof. Dr.-Ing.
KfK
Postfach 36 40, 7500 Karlsruhe

U

Ullrich, Walter, Dipl.-Phys.
GRS
Schwertnergasse 1, 5000 Köln 1

V

Vetter, Heinz, Dr.
Spitzwegstr. 4, 6900 Heidelberg

Voges, Udo, Dipl.-Math.
KfK
Postfach 36 40, 7500 Karlsruhe 1

von Dobschütz, Peter, ORR Dr.
Bundesministerium des Innern
Postfach 17 02 90, 5300 Bonn

von Eyss, Josef, ORR Dr.
Bundesministerium des Innern
Postfach 17 02 90, 5300 Bonn

von Streitberg, Alexander
Allianz Versicherung AG
Königinstr. 28, 8000 München 44

W

Wach, Dieter, Dr.-Ing.
GRS
Forschungsgelände, 8046 Garching

Waessmann, Per-Olof, Dipl.-Ing.
Swedish State Power Board
S–16287 Vaellingby

Wagner, Heinz, Prof.
Lanzstr. 19, 6200 Wiesbaden

Weber, Alfred
Westdeutscher Rundfunk
Kommentare und Feature
Appellhofplatz 1, 5000 Köln 1

Weber, Matthias, BauDir. Dr.
Niedersächsisches Ministerium für Bundesangelegenheiten
Calenberger Str. 2, 3000 Hannover 1

Weidlich, Helmut, Dr.
GRS
Forschungsgelände, 8046 Garching

Weil, Leopold, RD Dr.
BMI
Postfach 18 02 90, 5700 Bonn

Weingarten, Jürgen
GKN
Postfach, 7129 Neckarwestheim

Wendler, Eberhard, Dr.
Gemeinsame Forschungsstelle der KEG
I–21020 Ispra (Varese)

Wendt, Manfred, Dipl.-Ing.
GRS
Schwertnergasse 1, 5000 Köln

Werner, Wolfgang, Dr.
GRS
Forschungsgelände, 8046 Garching

Wiesner, Siegfried, Dr.
Rheinisch-Westfälisches TÜV e.V.
Postfach 10 32 61, 4300 Essen 1

Wild, Eberhard, Dipl.-Ing.
KKW Grafenrheinfeld
Postfach 7, 8722 Grafenrheinfeld

Wild, Wolfgang, Prof. Dr.
Technische Universität München
Postfach 20 24 20, 8000 München 2

Witt, Werner, Dr.-Ing.
TÜV Norddeutschland e.V.
Große Bahnstr. 31, 2000 Hamburg 54

Wleklinski, Helmut, Dipl.-Ing.
KKW Mülheim-Kärlich
Postfach 1 25, 5403 Mülheim-Kärlich

Wolf, Dietrich, Dr.
GRS
Schwertnergasse 1, 5000 Köln 1

Wolff, Josef, Dr.
Athener Str. 46, 8000 München 90

Wolter, Wolfgang, MR Dr.
Sozialministerium des Landes Schleswig-Holstein
Brunswiker Str. 16/22, 2300 Kiel

Y

Young, Peter, Dr.
DBE
Postfach 11 69, 3150 Peine

Z

Zeck, Kurt, Dipl.-Ing.
TÜV Stuttgart e.V.
Gottlieb-Daimler-Str. 7, 7024 Filderstadt

Zehentbauer, Armin, Dipl.-Ing.
KKI-Betriebsleitung
Postfach 11 06, 8307 Essenbach

Ziermann, Egon, Ing. (grad.)
AVR
Hambacher Forst, 5170 Jülich

Zimmermann, Friedrich, Bundesinnenminister, Dr.
Bundesministerium des Innern
Postfach 17 20 90, 5300 Bonn 1

Zimmermann, Rainer, Dipl.-Ing.
KKP
Postfach 11 40, 7522 Philippsburg

Zimmermann, Volker, Dr.
Ministerium für Ernährung, Landwirtschaft, Umwelt und Forsten
Postfach 4 91, 7000 Stuttgart 1

Zinke, Hugo, Dipl.-Ing.
Technischer Überwachungsverein Wien
Krugerstr. 16, A—1015 Wien

Zitzelsberger, Werner Franz, Dr.-Ing.
TÜV Pfalz e.V.
Postfach 13 60, 6750 Kaiserslautern

Gesellschaft für Reaktorsicherheit (GRS) mbH

Schwertnergasse 1
5000 Köln 1

Forschungsgelände
8046 Garching

ISBN 3 - 923875 - 09 - 6