

**KERNFORSCHUNGSZENTRUM  
KARLSRUHE**

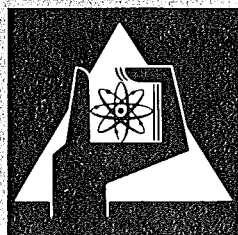
Februar 1973

KFK 1735

Labor für Elektronik und Meßtechnik

**Schutzsysteme für Schnelle Natriumgekühlte Reaktoren**

S. Jacobi, H. Lenhardt, R. Schneider



**GESELLSCHAFT  
FÜR  
KERNFORSCHUNG M.B.H.**

**KARLSRUHE**

Als Manuskript vervielfältigt

Für diesen Bericht behalten wir uns alle Rechte vor

GESELLSCHAFT FÜR KERNFORSCHUNG M. B. H.  
KARLSRUHE

KERNFORSCHUNGSZENTRUM KARLSRUHE

KFK 1735

Labor für Elektronik und Meßtechnik

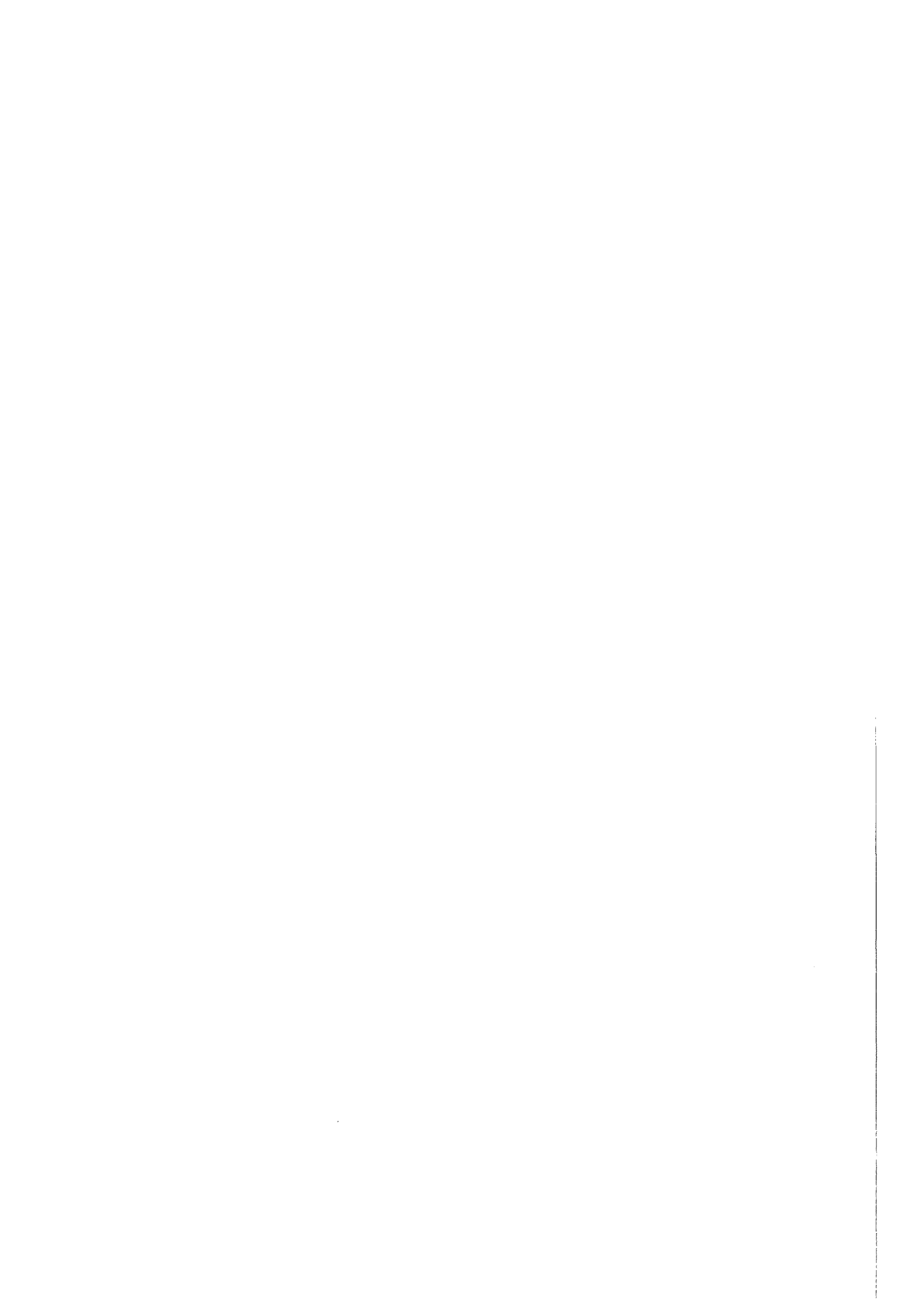
Schutzsysteme für Schnelle Natriumgekühlte Reaktoren

S. Jacobi

H. Lenhardt

R. Schneider

GESELLSCHAFT FÜR KERNFORSCHUNG M.B.H., KARLSRUHE



## Zusammenfassung

Der vorliegende Bericht zeigt Realisationsmöglichkeiten für ein Multi-Input-Schutzsystem MISS mit Rechnern zur lokalen Brennelement-Überwachung Schneller Natriumgekühlter Reaktoren (SNR). Eine ausgewogene Beziehung zwischen Sicherheit und Verfügbarkeit wird berücksichtigt.

In der Aufgabenstellung werden die wesentlichen Forderungen an das Schutzsystem begründet. Dabei wird beispielsweise eine lokale Core-Instrumentierung für 151 Brennelemente und 48 Brutelemente mit 4 x 199 Thermoelementen und 3 x 151 Durchsatzsignalen berücksichtigt.

In Verbindung mit dem konventionellen Schutzsystem kann gezeigt werden, daß durch Anwendung der diversitären Systemredundanz unter Verwendung optoelektronischer Koppellemente höchste Sicherheitsanforderungen realisierbar sind.

Aufgrund z. Z. verfügbarer Ausfalldaten von Systemkomponenten zeigt der Bericht, daß ein MTBF-Wert von ca. 10 Jahren für ein 2von3-System erreichbar ist. Dieses Ergebnis basiert auf einem angenommenen MTBF- und MTTR-Wert von 1000 h bzw. 2 h für die Grundausrüstung eines nichtredundanten Rechnersystems. Voraussetzung ist ferner, daß die Verfügbarkeit der Brennelementinstrumentierung groß ist im Vergleich zur Verfügbarkeit eines solchen nichtredundanten Systems.

Die Zeit von 1,5 s wird als "Reaktionszeit" festgelegt. Sie berücksichtigt die zeitlichen Anforderungen an den elektronischen Teil des Reaktorschutzsystems. Ebenso wird ein Schaltungsvorschlag angegeben, der das Synchronisierproblem eines 2von3-Rechersystems behandelt. Für alle vorgeschlagenen Systeme wird eine Synchronisierung als vorteilhaft betrachtet. Insbesondere läßt sich dadurch die Reaktionszeit verkürzen.

Für ein 2von3-System wird eine kontaktlose Abschlußschaltung mit einer umfassenden dynamischen Systemprüfung bei einer Prüffrequenz für gefährliche Fehler von  $f \geq \frac{1}{1,5s}$  vorgeschlagen.

Aufgrund der flexiblen Programmierung werden 3 Variationen von Abschaltbedingungen behandelt. Neue Sicherheitspostulate und neue Erkenntnisse in der Fühlerverfügbarkeit können durch weitere Variationen berücksichtigt werden. Für die Rechner wird eine Programmübersicht mit einer Speicherplatzabschätzung von min. 12 kWorte gegeben.

Für den Fall, daß ein MTBF-Wert von 10 Jahren nicht ausreicht, werden weitere redundante Schutzsysteme mit Rechnern untersucht. Dabei wird ersichtlich, daß polymorphe Systeme wegen ihrer umfangreichen Verkopplung als vorerst problematisch zu betrachten sind, ihre Struktur ist aber für eine Verfügbarkeitserhöhung interessant.

## Abstract

This report describes several possibilities of implementing by a balanced relationship between safety and availability, a Multi-Input-Protection System (MISS), using computers for the monitoring of each fuel element in a fast sodium-cooled reactor (SNR).

A clearly defined set of problems outlines the reasons for the essential requirements to the protection system and the application of computers.

For example an individual instrumentation for 151 fuel elements and 48 blanket elements with 4 x 199 thermocouples and 3 x 151 flow-meters is taken into account. In combination with the coexisting conventional protection system the use of diverse system redundancy can be shown to meet the most stringent safety requirements.

Referring to presently available failure-rates of system components, using an approximation this report shows that an MTBF-value of about 10 years can be attained for a 2 out of 3-system. This result is based on a MTBF-value of 1000 h and a MTTR-value of 2 h for a single basic computer system. Furthermore it is supposed, that the availability of the fuel element instrumentation is great compared with the availability of the basic computer system.

A basic solide state shut-down circuit including a coincidence logic with an all-over dynamic system check is proposed for a 2 out of 3-system which operates at a checking frequency of  $f \geq \frac{1}{1,5s}$  for failures in the unsafe direction. Another unit is proposed which deals with the problem of synchronizing a 2 out of 3-computer system, because a synchronized protection system is considered to minimize the reaction time.

On the basis of flexible programming, three variations of input data combinations resulting in shut-down signals are discussed. Other additional safety requirements as well as sensor availability can be taken into account through additional variations. A program review is given leading to an estimated minimal core memory capacity of 12 k-words.

Additional redundant protection systems with computers have been studied to overcome difficulties arising from MTBF's of detectors in the same range as estimated for the electronic system or a desired longer MTTR. Polymorphous structures may overcome some availability problems coming from the detectors as well as from the computer system itself.



## Inhaltsverzeichnis

1. Einleitung
2. Aufgabenstellung
  - 2.1. MISS-SNR-Eingangsdaten
  - 2.2. Grenzwerte und Grenzwertführung
  - 2.3. Abschaltbedingungen
  - 2.4. Systemforderungen
  - 2.5. Zeitliche Forderungen
  - 2.6. Sicherheit durch Prüfbarkeit des MISS und Diversität des Gesamtsystems
  - 2.7. Verfügbarkeit
3. Reaktorschutzsysteme mit Prozeßrechnern
  - 3.1. 2von3-System
    - 3.1.1. Systemaufbau
    - 3.1.2. Synchronisation
    - 3.1.3. Prüfbarkeit
      - 3.1.3.1. Periphere Fehler
      - 3.1.3.2. Interne Fehler
    - 3.1.4. Programme
    - 3.1.5. Abschlußschaltung
    - 3.1.6. Verfügbarkeit
      - 3.1.6.1. Verfügbarkeit des 2von3-Systems
      - 3.1.6.2. Einfluß der Abschlußschaltung auf die Verfügbarkeit
  - 3.2. 2von3-System mit aktiver Redundanz durch 4. MPX/ADC
  - 3.3. Polymorphes 2von3-System
  - 3.4. Polymorphes 2von3-System mit vier MPX/ADC
  - 3.5. 3von4-System
4. Diskussion der Lösungsvorschläge
5. Literatur
6. Verzeichnis der Abbildungen

## 1. Einleitung

Bei vielen technischen Einrichtungen ist infolge ihrer inneren Struktur bei Betriebsstörungen grundsätzlich eine Selbstzerstörung der Einrichtung möglich. Die Gefährdung der Umgebung kann in solchen Fällen selten ausgeschlossen werden. Chemische Anlagen, Flugzeuge oder Schiffe gehören zu derartigen Einrichtungen, Kernkraftwerke sind ein weiteres Beispiel und haben vom Prinzip her keine Sonderstellung. Diese Prozesse der Umformung oder des Transports von Materie oder Energie erfordern für den eigentlichen Betriebsablauf Systeme zur Prozeßregelung, oft Betriebssysteme bezeichnet, sie werden im folgenden nicht näher betrachtet. Zur Vermeidung gefährlicher Betriebszustände werden zusätzliche Systeme zur Prozeßüberwachung verwendet. Sie führen nach vorgegebenem Schema Sicherheitsoperationen aus und werden daher Sicherheits- bzw. Schutzsysteme genannt. Bei Kernreaktoren ist eine Tendenz der völligen Entkopplung zwischen Betriebs- und Schutzsystem festzustellen.

Das Betriebsverhalten der bisherigen Kernreaktoren einschließlich der theoretischen und hypothetischen Störungen wird bzw. wurde bis vor kurzem als ausreichend bekannt vorausgesetzt. Damit waren auch die Aufgaben für das Schutzsystem fest abgegrenzt [1, 2]. Das Konzept des Schnellen Natriumgekühlten Reaktors brachte einen neuen Aspekt: Durch Kühlmittelverlust infolge Natriumsieden oder durch Änderung der Kerngeometrie infolge Niederschmelzen des Kernes sind nach Smidt sowie Gast und Schlechtendahl Reaktivitätsstörungen möglich, die eine nukleare Exkursion prinzipiell nicht ausschließen [3, 4]. Bei den Schnellen Reaktoren der ersten Generation wurde die Sicherheitsphilosophie in erster Linie von der Annahme beeinflusst, daß insbesondere das Abschalt-system völlig versagt. Als notwendige Konsequenz dieser Betrachtungsweise ergab sich, daß auch alle Folgen der zwar hypothetischen, aber schweren Unfälle sicher beherrscht werden. Notwendigerweise werden dadurch Genehmigungsverfahren, Bau und Betrieb der Reaktoren erschwert. In den vergangenen Jahren erfolgte eine Verbesserung der

---

eingegangen am 5. Januar 1973

Detailkenntnisse. Von Judd [5] wurde die Schadenspropagation durch Kühlungsstörungen von Pin zu Pin und in der Folge von Brennelement zu Brennelement ausführlich behandelt. Derzeit besteht die Auffassung, daß die Schadenspropagation der wahrscheinlichste Beginn schwerer Unfälle ist. Eine frühzeitige Unterbrechung dieses Störablaufes ist die neue Zielsetzung. Zwei wichtige Voraussetzungen sind dafür zu erfüllen: Einerseits müssen Meßverfahren untersucht bzw. entwickelt werden, um den Beginn eines Propagationsunfalles zu detektieren. Die dazu notwendigen Untersuchungen über den Störablauf, ihre Bedeutung für die Reaktorsicherheit und ein Meßverfahren wurden von Gast behandelt [6]. Andererseits sollen verbesserte Methoden und Technologien bei der Durchführung dieser Meßverfahren ein allen Anforderungen genügendes Maß an Zuverlässigkeit unter Beweis stellen. In der vorliegenden Arbeit wird dieser Punkt ausführlich behandelt. Die Möglichkeit der Realisierung der genannten Forderungen führte zu einer modifizierten Sicherheitsphilosophie, bei der dem Schutzsystem eine wesentlich erhöhte Bedeutung zukommt: Rechtzeitige Unterbrechung eines Schadensablaufes zwecks Verhinderung schwerwiegender Unfallfolgen.

Bedingt durch eine auch bei sehr großem Aufwand nur begrenzt erreichbare Zuverlässigkeit technischer Einrichtungen - so auch bei der Prozeßüberwachung - entstand nach Smidt die Forderung nach einem zweiten Abschaltssystem [3]. Wesentliche Vorteile, von Birkhofer u. a. [7] auch für Notkühlssysteme wassergekühlter Reaktoren genannt, können damit auch für die Schutzsysteme Schneller Reaktoren angewendet werden: Redundanz und Diversität. Systemredundanz bedeutet, daß für den gleichzeitigen Ausfall der beiden unabhängigen Schutzsysteme die Gesamtwahrscheinlichkeit gleich dem Produkt der Einzelausfallwahrscheinlichkeiten ist, ein Betrag, der auch den höchsten Sicherheitsforderungen entspricht.

Vorteile durch Diversität lassen sich im voraus kaum quantitativ ausdrücken, sie ist jedoch anerkanntes Prinzip gegen systematische Fehler und im vorliegenden Fall realisierbar.

## 2. Aufgabenstellung

Nach dem gegenwärtigen Stand des Wissens sind die von Judd [5], Gast [6] u. a. behandelten Propagationsunfällen an Schnellen Reaktoren nicht auszuschließen. Theoretische und experimentelle Arbeiten zu diesem Thema lassen erst in den nächsten Jahren neue Erkenntnisse erwarten. Daraus erklärt sich, daß die globale Aufgabe für ein Schutzsystem sich zwar angeben läßt, Details derzeit aber nur in Form vorläufiger Annahmen verarbeitet werden können. Hieraus wiederum resultiert, daß eine Lösung mit einer maximalen Flexibilität für Detailvariationen anzugeben ist. Als Aufgabe ergibt sich folglich:

- I. Es ist ein Reaktorschutzsystem zur Vermeidung eines Propagationsunfalles zu konzipieren, logische Verknüpfungen verschiedener Meßsignale sind vorläufig und nur Annahmen, ihre Variation muß ohne grundlegende Systemänderung möglich sein.

Soll ein Propagationsunfall bereits während des Schadensablaufes detektiert werden, so müssen sich die dazu notwendigen Meßfühler am Kernrand, vorzugsweise am Brennelementaustritt befinden. Der wünschenswerte Einbau in den Kern stößt auf extrem große konstruktive Schwierigkeiten. In Tabelle 1 sind die möglichen Detektoren, ihr Meßsignal und die angezeigten Störungen angegeben.

Tabelle 1: Mögliche Kerninstrumentierung des SNR

Nr.	Meßfühler	Meßgröße	Angezeigte Störung
1	Durchsatz- messer	Durchsatz  Durchsatz schwankung	verminderter Durchsatz  Siedeblasen  große Gasblasen
2	Ionisations- kammer	Neutronenfluß und Neutronenfluß- schwankungen	Reaktivitätsände- rungen z. B. durch Sieden
3	Schallaufnehmer	Schall	Sieden
4	Thermoelement	Temperatur  Temperatur- schwankungen	Temperaturerhöhung durch partielle Verblockung  Durchsatzstörung
5	Zyklon	Temperatur	Gasblasen

Vorläufig ausgewählt wurden die Meßfühler Nr. 1 und 4. Als Aufgabenformulierung ergibt sich:

II. Es ist ein Reaktorschutzsystem zu konzipieren, welches Meßsignale von Durchsatzmessern und Thermoelementen verarbeitet. Wechsel in der Art der Meßfühler müssen ohne grundlegende Systemänderungen möglich sein.

Zur rechtzeitigen Unterbrechung eines Propagationsunfalles müssen sämtliche Brennelemente einzeln überwacht werden. Aus konstruktiven Gründen kann je Brennelement nur ein Durchsatzmesser verwendet werden. Wegen der bisher beobachteten relativ großen Ausfallrate der Thermoelemente werden drei Stück je Brennelement verwendet. Zur Weiterverarbeitung der Meßsignale aus den Brennelementen sollen bis zu zwanzig Signale der Prozeßüberwachung - integrale Signale genannt - zusätzlich verwendet werden. Als Aufgabenformulierung ergibt sich:

III. Es ist ein Schutzsystem zu konzipieren, welches zwanzig integrale Signale und von jedem Brennelement vier Meßsignale, d. h. ca.  $3 \times 1000$  Meßsignale verarbeitet.

Wegen dieser großen Anzahl der Signale werden die hier zu beschreibenden Systeme Multi-Input-Schutzsysteme = MISS genannt.

Jedes Schutzsystem soll vor Erreichen gefährlicher Betriebszustände aus den Eingangssignalen Abschaltsignale generieren. Die große Zahl der Eingangssignale, die vielen Möglichkeiten ihrer logischen Verknüpfungen und der derzeitige Wissensstand lassen noch keine endgültige Entscheidung über die Erzeugung der Abschaltsignale zu, es muß mit vorläufigen Annahmen gearbeitet werden. Als Aufgabenformulierung ergibt sich:

- IV. Es ist ein Schutzsystem zu konzipieren, welches Änderungen in der Erzeugung der Abschalt-signale ohne grundlegende Systemänderungen gestattet.

Aus den derzeitigen Kenntnissen über die Zeitdauer zwischen dem Auftreten einer Störung und dem Bereitstellen eines Abschalt-signales ergibt sich als Aufgabenformulierung:

- V. Es ist ein Schutzsystem zu konzipieren, welches spätestens etwa 3 Sekunden nach Beginn der Störung ein Scramsignal bereitstellt.

Die aus Tabelle 1 ausgewählten Meßfühler liefern neben ihren Signalen für das Schutzsystem auch Informationen über das Verhalten des Kerns vor Eintreten von Störungen. Für das Sammeln von Betriebserfahrungen und das Erkennen von Störabläufen ist ein Auskoppeln der Meßsignale erforderlich, gegebenenfalls auf den Prozeßrechner. Als Aufgabenformulierung ergibt sich:

- VI. Es ist ein Schutzsystem zu konzipieren, welches die rückwirkungsfreie Übergabe von Primärdaten an andere, nicht zum MISS gehörende datenverarbeitende Anlagenteile ermöglicht.

Wegen der endlichen Zuverlässigkeit des wie an jedem anderen Reaktor vorhandenen Schutzsystems für die integralen Daten, hier Schutzsystem Nr. 1 oder konventionelles Schutzsystem genannt, können gefährliche Fehler nicht ausgeschlossen werden. Da das MISS ohnehin ca. 20 wesentliche integrale Meßwerte als Eingangsdaten erhält, ergibt sich zwecks zusätzlicher Risikoabdeckung als Aufgabenformulierung:

- VII. Es ist ein Schutzsystem zu konzipieren, welches die gleichen Abschaltkriterien erfüllt wie das Schutzsystem Nr. 1.

## 2.1. MISS-SNR-Eingangsdaten

Bei der Konzepterstellung wird davon ausgegangen, daß nachstehend angeführte Instrumentierung<sup>\*)</sup> gegeben ist. Es wird zwischen integraler und lokaler Instrumentierung unterschieden: Integrale Daten sind beispielsweise Neutronenfluß am Corerand, Kühlmitteltemperaturen am Ein- und Austritt des Reaktors und Natriumdurchsatz durch Hauptkühlmittelleitungen. Lokale Daten sind Meßwerte, die am Kühlmittelaustritt der Brennelemente erfaßt werden, Fig. 1. Das MISS verwendet die lokalen und zusätzlich die integralen Daten.

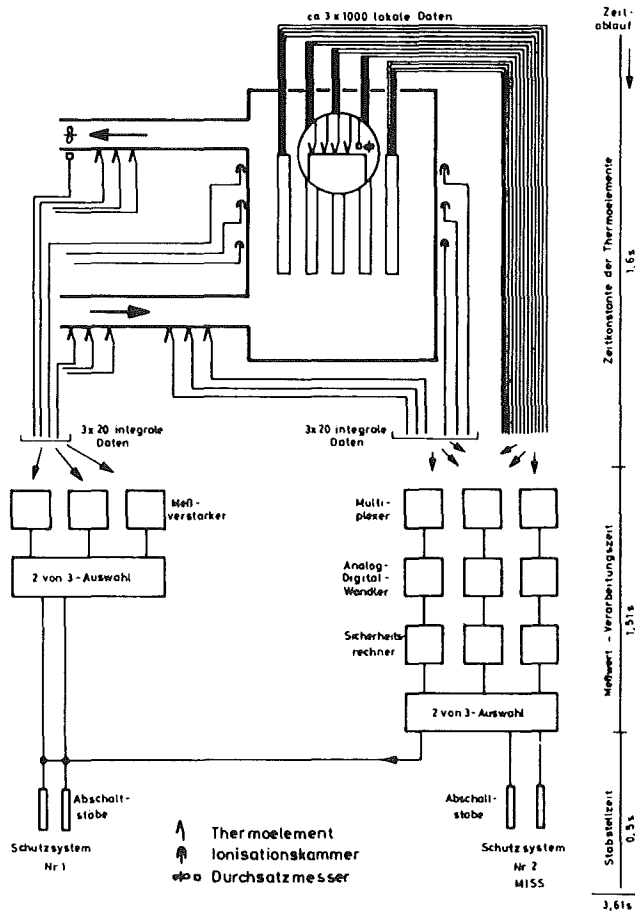






Fig. 1 Integrale und lokale Daten im MISS-SNR

<sup>\*)</sup> private Mitteilung der Fa. INTERATOM, Bensberg



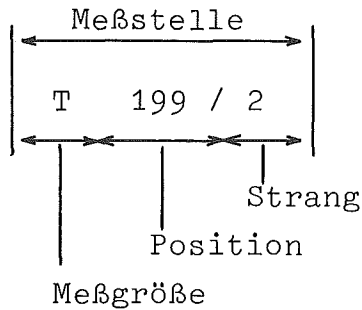
Alle 151 Brennelemente der Spaltzone werden mit 4 Thermoelementen (davon 1 Reserve) und 1 Durchsatzmesser mit 3 galvanisch getrennten Ausgängen und Selbstüberwachung ausgerüstet. Der Durchsatzmesser übernimmt noch zusätzlich die Siedeblasendetektion (Noise). Die restlichen 48 Brutelemente werden dagegen voraussichtlich nur mit 4 Thermoelementen bestückt. Nachstehende Tabelle 2 gibt eine Übersicht über die lokale Instrumentierung.

Tabelle 2: Lokale Instrumentierung

Meßgröße Symbol	Art des Fühlers und Schalt- zeichen	Zahl der Fühler	Zeitkon- stante $\tau$ (66 %)	Genauig- keit	Meßsignal
Tempera- tur [T]	NiCr-Ni- Thermo- element 	3x199 1x199 Reserve	1,6 s	nach DIN 43710 bis 500 °C + 3 °C darüber ± 0,75 %	Thermo- spannung
Durch- satz [Q]	Indukti- ves Prinzip 	151 bei 3x151 galv. ge- trennten Ausgängen	ca. 1 ms	bestens 5 % Ände- rung er- faßbar	0-20 mA
Siede- blasen (Durch- satz noise) [QN]	wird aus Durchsatz abgelei- tet 	151 bei 3x151 galv. ge- trennten Ausgängen	Vielfa- ches von $\frac{1}{2,5}$ Hz max. Fak- tor 4	-	0,20 mA
Durch- satz- messer- störung [QS]		3x151	ca. 1 ms	-	binär

Die lokale Instrumentierung ist in einer Meßpflaume über jedem Brennelement untergebracht. Zur Kennzeichnung einer Meßstelle wird in diesem Bericht folgende Schreibweise verwendet:

Z. B.



Das MISS erfaßt Meßgrößen von 199 lokalen und ca. 20 integralen Positionen. Entsprechend den Meßgrößen liegen mehrere Kanäle, z. B. Temperaturkanal, vor. Jeder Kanal besteht aus 3 Strängen. Nachstehende Übersicht erläutert den organisatorischen Aufbau der Fühler am Eingang des MISS, Fig. 2.

Unter integralen Eingangsdaten werden diejenigen Daten verstanden, die primär für die Instrumentierung des konventionellen Schutzsystems erforderlich sind. Für das MISS-Konzept werden diese Daten (ca. 20) zur Erzeugung gestaffelter Grenzwerte und zur Grenzwertführung ebenfalls benötigt. Die integralen Eingangsdaten sind daher für 2 Schutzsysteme zur Verfügung zu stellen, vorzugsweise durch eine entsprechende Anzahl von Fühlern mit Meßumformern und nicht durch Trennverstärker.

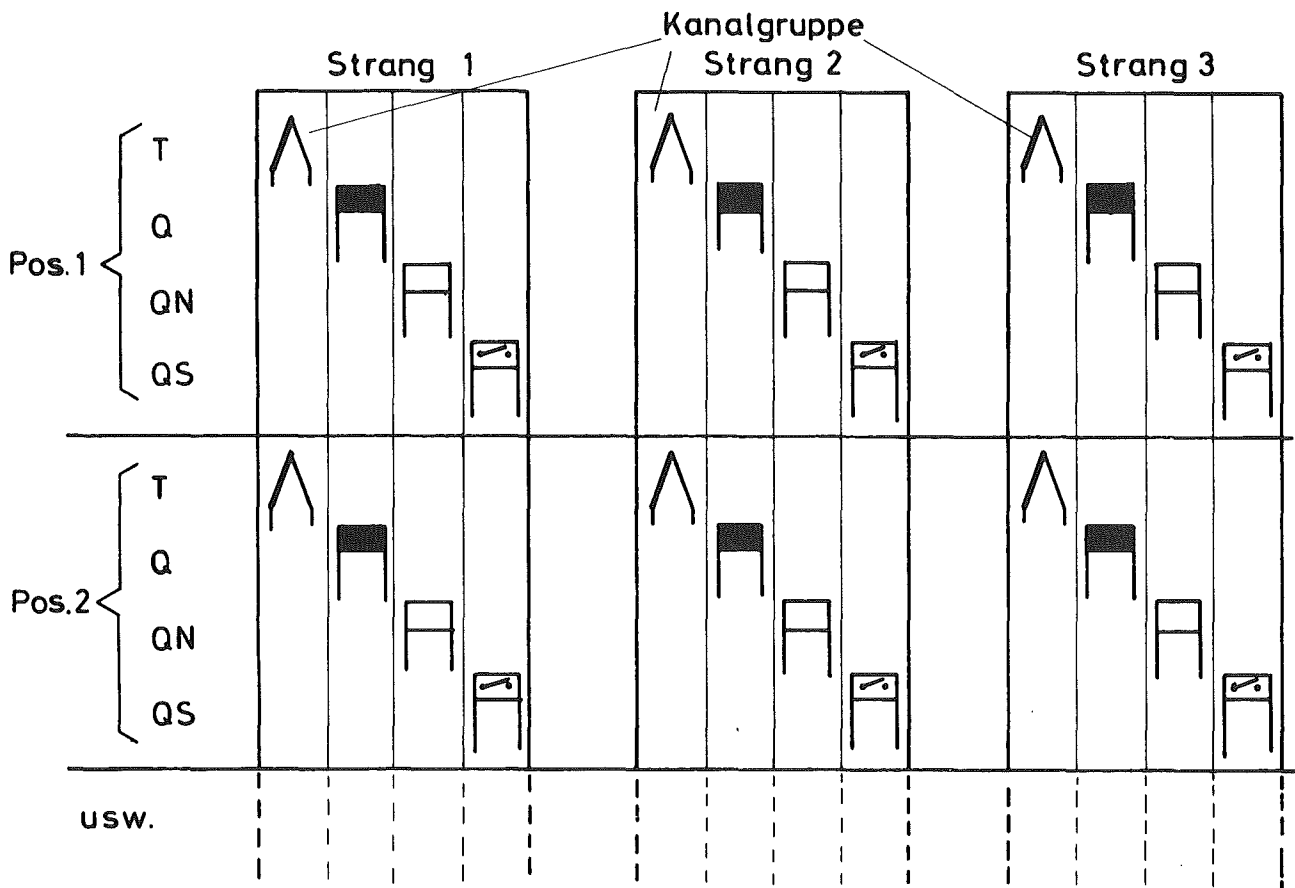


Fig. 2 Organisatorischer Aufbau der Fühler

## 2.2. Grenzwerte und Grenzwertführung

Das SNR-Konzept sieht u. a. eine variable Leistungsabgabe im Bereich von 30 - 100 % vor. Trotz einer Temperaturregelung des Kühlmittels am Kernaustritt mit Hilfe der Stellgröße Kühlmitteldurchsatz in Abhängigkeit der Reaktorleistung ist mit Temperaturschwankungen von ca. 40 °C zu rechnen, da eine endliche Ungenauigkeit in der Proportionalität zwischen thermischer Leistung und Gesamtdurchsatz besteht. Zusätzlich ist der quasistatische Einfluß des Abbrandes auf die Kühlmittelaustrittstemperatur nicht vernachlässigbar.

Es ist Aufgabe der Grenzwertführung, diese Temperaturänderungen derart zu berücksichtigen, daß bei Kühlmittelstörungen mit zeitlichem Vorteil gegenüber einem konstanten Temperaturgrenzwert abgeschaltet werden kann. Der konstante Temperaturgrenzwert bleibt daher einer unkontrollierten Leistungserhöhung vorbehalten und ist dem gleitenden Grenzwert übergeordnet.

Die Grenzwerte der integralen Größen werden ebenso wie die Grenzwerte des Durchsatznoise als Konstanten vorgegeben. Eine dynamische Grenzwertführung im Leistungsbereich von 30 % bis 100 % und eine quasistatische Grenzwertführung in Abhängigkeit des Abbrandes sind sowohl für die Temperatur als auch für den Durchsatz des Kühlmittels der einzelnen Brennelemente (BE) vorteilhaft.

Der Grenzwert der Temperatur des i-ten BE's läßt sich wie folgt bestimmen<sup>\*)</sup>:

$$T_{GWi} = T_E + \frac{K_i}{1000} (T_K - T_E) \pm \Delta T \quad (1)$$

dabei sind:

$T_{GWi}$  = Grenzwert der Austrittstemperatur des Kühlmittels des i-ten BE's

$T_E$  = Eintrittstemperatur des Kühlmittels in den Kern

$T_K$  = Austrittstemperatur des Kühlmittels aus dem Kern

$\pm \Delta T$  = Zulässige Temperaturabweichung vom Sollwert

$K_i$  = Kenngröße des i-ten BE's

<sup>\*)</sup> private Mitteilung der Fa. INTERATOM, Bensberg

Die Kenngröße  $K_i$  wird aus 2 Faktoren gebildet, wovon der eine Faktor  $\delta_i$  von der Drosselstellung des Brennelements abhängt und der andere Faktor  $\alpha_i$  vom Abbrand. Dieser Faktor wird aufgrund von Ergebnissen des Prozeßrechners bestimmt und in größeren Zeitabständen über ein Eingabegerät vom Operator in das MISS eingegeben.

Es gibt nun verschiedene Möglichkeiten, die Werte  $T_E$  und  $T_K$  zu erhalten. Die Werte können als Konstanten fest vorgegeben werden. Der Index  $e$  in der folgenden Gleichung soll sagen, daß es sich um eingegebene Werte für  $T_E$  handelt. Die Gleichung lautet:

$$T_{GWei} = T_{Ee} + \frac{K_i}{1000} (T_{Ke} - T_{Ee}) + \Delta T \quad (2)$$

Eine weitere Möglichkeit ist, die Werte für  $T_E$  und  $T_K$  zu messen und den Grenzwert aus den gemessenen Werten zu errechnen. Der Index  $g$  zeigt an, daß es sich um gemessene Werte handelt:

$$T_{GWgi} = T_{Eg} + \frac{K_i}{1000} (T_{Kg} - T_{Eg}) + \Delta T \quad (3)$$

Die Kernaustrittstemperatur  $T_K$  kann integral am Austritt des Kerns gemessen werden. Dabei ist zu beachten, daß das Kühlmittel über 3 getrennte Leitungen aus dem Kern geführt wird. Die Kernaustrittstemperatur  $T_{Kg}$  ist dann der Mittelwert der 3 Temperaturmeßwerte der 3 Teilströme. Die Gefahr der Strahlenbildung und die dadurch möglichen Fehlmessungen veranlaßt, diesem Verfahren ein anderes entgegenzustellen: die Mittelwertbildung über die Austrittstemperaturen des Kühlmittels aller Brennelemente

$$T_{Kg} = \frac{1}{199} \sum_{i=1}^{199} T_{Ki} \quad (4)$$

Die Grenzwertbildung aus gemessenen Werten nach Gleichung (3) kann im Fall eines ungewollten Temperaturanstiegs im ganzen Kern eine ungewollte GW-Drift zur Folge haben. Da dieser Fall eintreten kann, ist eine Berücksichtigung der Vergangenheit



Ähnliche Betrachtungen wie über die Führung der Temperaturgrenzwerte gelten für Grenzwerte des Durchsatzes. Der Durchsatzgrenzwert wird aber zweckmäßigerweise aus dem Gesamtdurchfluß gebildet, da die Durchsatzmesser der Brennelemente mit voraussichtlich größeren Fehlern behaftet sind. Der Gesamtdurchsatz ist die Summe der 3 Teildurchsätze  $Q_{K1}$ ,  $Q_{K2}$  und  $Q_{K3}$ :

$$Q_K = Q_{K1} + Q_{K2} + Q_{K3} \quad (6)$$

Die Gleichung, nach welcher der Grenzwert  $q_i$  des Durchsatzes des  $i$ -ten Brennelements festgelegt wird, lautet:

$$q_i = P_i \frac{Q_K}{199} - \Delta Q \quad (7)$$

Die Kenngröße  $P_i$  wird aus 2 Faktoren gebildet, wovon der eine Faktor  $\beta_i$  von der Drosselstellung des Brennelements abhängt und der andere Faktor  $\lambda_i$  vom Abbrand. Dieser Faktor wird aufgrund von Ergebnissen des Prozeßrechners zur quasistatistischen Grenzwertführung in das MISS eingegeben.

Die Leistungsabhängigkeit soll anhand der Fig. 4 gezeigt werden.

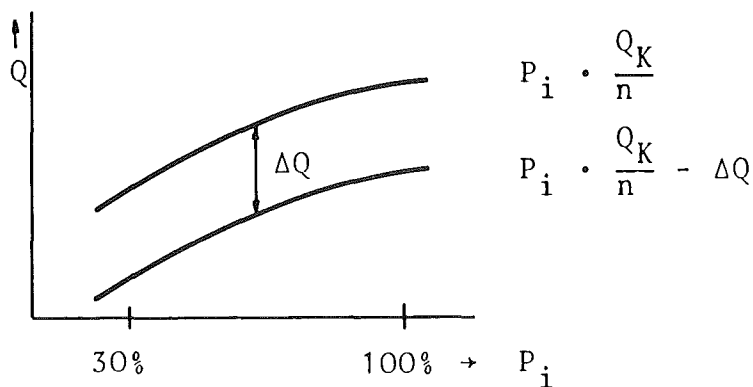


Fig. 4: Durchsatzgrenzwerte in Abhängigkeit der Brennelementleistung

### 2.3. Abschaltbedingungen

Die Brennelemente der Brutzone und der Spaltzone haben unterschiedliche Bestückung in der Art der Meßfühler und müssen daher im Hinblick auf ihre Abschaltbedingungen verschieden behandelt werden. Es gibt nun eine Reihe von Möglichkeiten, die Abschaltbedingungen zu formulieren.

Im Folgenden werden 3 Varianten der Abschaltbedingungen zur Diskussion gestellt, bei denen den verschiedenen Meßgrößen unterschiedliches Gewicht gegeben wird.

Die Variante 1 wird in Fig. 5 dargestellt. Sobald der Meßwert eines Fühlers den vorgegebenen Grenzwert überschritten hat, wird ein Abschaltsignal erzeugt. Liegt in 2 von 3 Strängen ein Abschaltsignal vor, so ist die Abschaltbedingung erfüllt. Einem Brennelement der Spaltzone sind bei dieser Variante 1 drei Abschaltbedingungen zugeordnet, während einem Brennelement der Brutzone nur eine Abschaltbedingung zugeordnet ist. Demnach sind in einem Abfragezyklus  $3 \times 151$  und  $1 \times 48$ , also insgesamt 501 Abschaltbedingungen zu prüfen. Der Nachteil, den diese Formulierung hat, ist schwerwiegend. Fällt z. B. in einem Strang ein Thermoelement aus, so arbeitet ab diesem Zeitpunkt das System bereits als 1 von 2-System. Daher sollen die beiden nachfolgenden Varianten die Verfügbarkeit des Systems erhöhen.

Die Variante 2, dargestellt in Fig. 6, gibt besonders dem Durchsatznoise großes Gewicht. Die Überschreitung des Grenzwertes des Durchsatznoise genügt für die Abschaltung. Das Durchsatznoise ist ein primäres und damit ein schnelles Signal für einige<sup>\*)</sup> Brennelementdefekte, denn für eine merkbare Temperatur- und Durchsatzänderung muß minimal eine 30 %ige Verstopfung vorliegen. Somit machen sich Temperatur- und Durchsatzänderungen erst wesentlich später bemerkbar [6]. Die Grenzwertüberschreitung der Temperatur reicht allein nicht aus, ein Abschaltsignal in einem Strang zu erzeugen. Nur wenn die Temperatur und der Durchsatz gemeinsam die Grenzwerte überschreiten, wird ein Abschaltsignal in den Strängen erzeugt. Diese Abschaltbedingungen für die Brennelemente der Brutzone sind gegenüber der Variante 1 abgeschwächt. Hier genügt die Überschreitung des

---

\*) z. B. Spaltgasfreisetzung, partielle Verstopfung



Grenzwertes der Temperatur des betrachteten Brennelements nicht, sondern es muß mindestens noch bei einem Nachbarelement eine Temperaturgrenzwertüberschreitung vorliegen. Bei der Variante 2 ergeben sich für lokale Größen insgesamt 199 Abschaltbedingungen.

Bei der Variante 3 der Abschaltbedingungen, dargestellt in Fig. 7, sind gegenüber der Variante 2 nur die Abschaltbedingungen der Brennelemente der Spaltzone geändert. Ein Abschaltsignal wird in einem Strang erzeugt, wenn der Grenzwert der Temperatur überschritten wird und der Grenzwert des Durchsatzes oder der Grenzwert des Durchsatznoise überschritten wird oder der Durchsatzmesser defekt ist. Bei der Variante 3 ergeben sich für lokale Größen insgesamt 199 Abschaltbedingungen.

Die behandelten Varianten sollen nur wenige der vielen kombinatorischen Möglichkeiten aufzeigen, die mit einem programmierbaren Rechner-Schutzsystem realisierbar sind. Die endgültige Festlegung der Abschaltbedingungen kann erst erfolgen, wenn die Ergebnisse aus einer SNR-Störfallanalyse und die Ergebnisse einer Instrumentierungs-Verfügbarkeitsanalyse zur Verfügung stehen.

#### 2.4. Systemforderungen

Da außer dem MISS noch ein konventionelles Reaktorschutzsystem zur integralen Überwachung vorhanden ist und für jedes der beiden Schutzsysteme eine eigene Abschlußschaltung und Abschalt Einrichtung vorgesehen wird, ergibt sich aus dieser Koexistenz die prinzipielle Möglichkeit der diversitären Systemredundanz.

Da Schutzsysteme sowohl mit probabilistischen als auch mit deterministischen Fehlern behaftet sein können, sollte die diversitäre Systemredundanz konsequent verfolgt und möglichst an vielen Systemkomponenten gleicher Aufgabenteilung realisiert werden. Diese Systemredundanz ist durch ein Prozeßrechnersystem beispielsweise

gegenüber SIMATIC oder LOGIPULS gegeben. Aus prinzipiellen Gründen läßt sich die Sicherheit eines Systems u. a. durch diversitäre Systemredundanz erhöhen; eine Steigerung der Verfügbarkeit dagegen erreicht man bereits schon durch Geräteredundanz.

Wegen der Forderung nach Diversität sind die integralen Daten auf das MISS aufgeschaltet. Das unterschiedliche Zeitverhalten der Meßfühler ist dabei zu berücksichtigen. Dies kann dadurch geschehen, daß die Multiplexer nach dem Abtasttheorem von SHANNON [8] zu programmieren sind. Damit wird aber ein wahlfreier Zugriff zu den Eingangsdaten erforderlich. Beispielsweise wird dadurch der Neutronenfluß durch eine höhere Abtastfrequenz zeitlich bevorzugt.

Ferner ist bei der Konzipierung des MISS ähnlich wie beim konventionellen Schutzsystem die Bildung von 2 Grenzwerten pro Meßgröße vorzusehen, welche wie folgt zu staffeln sind:

Tabelle 3: Grenzwerte

GW für integrale Daten

$GW_{int} \text{ I}$

$GW_{int} \text{ II}$

$GW_{int} \text{ I} < GW_{int} \text{ II}$

GW für lokale Daten

$GW_{lok} \text{ I}$

$GW_{lok} \text{ II}$

$GW_{lok} \text{ I} < GW_{lok} \text{ II}$

Damit ist u. a. die Möglichkeit eines Setback oder einer 2. Abschaltung eingeräumt.

Weiter ist eine dynamische Grenzwertführung im Leistungsbereich von 30 - 100 % und eine quasistatische Grenzwertführung in Abhängigkeit des Abbrandes zu berücksichtigen.

## 2.5. Zeitliche Forderungen

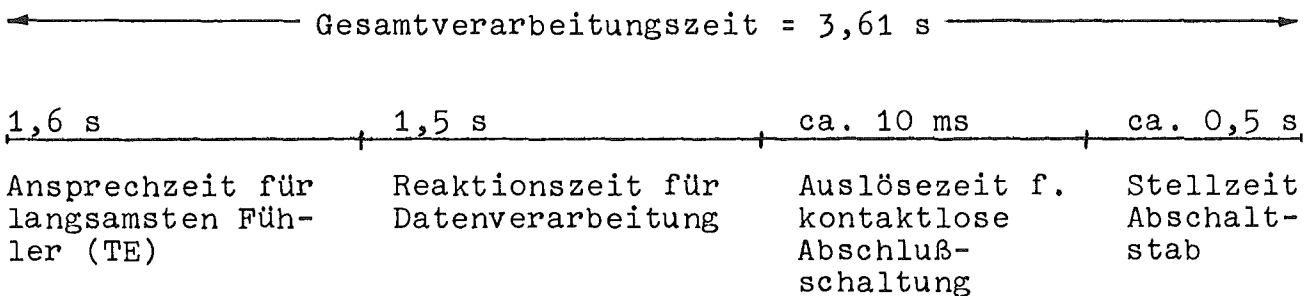
Das MISS hat die primäre Aufgabe, lokale Kühlungsstörungen im Kernbereich zu detektieren und daraus gleichzeitig ausreichende Maßnahmen zum Schutze des Reaktors abzuleiten. Die zeitlichen Forderungen an das MISS orientieren sich an der Größe und an der Dynamik dieser Störungen.

Die Festlegung der zeitlichen Forderungen wird unter folgenden Voraussetzungen getroffen:

- eine totale und plötzliche Verstopfung wird ausgeschlossen
- die Siedetemperatur des Natriums (knapp unter  $900^{\circ}\text{C}$ ) wird bei einer angenommenen plötzlichen Verstopfung von 30 % in ca. 5 s erreicht. Nach weiteren ca. 5 s beginnt der Brennstoff zu schmelzen.

Legt man dieses Übergangsverhalten zugrunde, so ist eine Gesamtverarbeitungszeit des MISS von max. 4 s noch zulässig.

Unter Berücksichtigung des Zeitverhaltens der einzelnen Systemkomponenten ergibt sich damit für das MISS folgende zeitliche Aufteilung:



Das Zeitverhalten der Fühler muß als gegeben betrachtet werden. Das gleiche gilt für die Abschaltstäbe der Abschaltseinrichtung. Für die Auslösezeit der Abschlußschaltung dürfte die Induktivität der Haltespule maßgebend sind. Genaue Werte liegen noch nicht vor, jedoch ist dieser Zeitanteil relativ klein.

Damit verbleiben 1,5 s für die Reaktionszeit des MISS. In dieser Zeit müssen 199 lokale Positionen und - falls man Systemredundanz berücksichtigt - noch zusätzlich ca. 20 integrale Positionen verarbeitet werden. Damit steht pro Position eine Reaktionszeit von ca. 6 bis 7 ms zur Verfügung.

Die Gesamtverarbeitungszeit beträgt demnach 3,61 s. Sie kann aber auch im günstigsten Falle, je nach Phasenlage zwischen Auftreten der Störung und Meßwertabfrage, nur ca.  $3,61 \text{ s} - 1,5 \text{ s} = 2,11 \text{ s}$  betragen, sofern an die Meßdatenabfrage einer Position (Brennelement) anschließend die Prüfung der Abschaltbedingungen folgt. Werden dagegen zuerst die Meßdaten aller Positionen eingelesen, so kann sich bei ungünstiger Phasenlage die Gesamtverarbeitungszeit auf ca.  $3,61 \text{ s} + 1,5 \text{ s} = 5,11 \text{ s}$  erhöhen.

## 2.6. Sicherheit durch Prüfbarkeit des MISS und Diversität des Gesamtsystems

Definitionsgemäß wird von einem sicheren Schutzsystem verlangt, daß gefährliche Fehler extrem unwahrscheinlich auftreten. Da sich gefährliche Fehler prinzipiell nicht vermeiden lassen, verfolgt das MISS eine umfassende dynamische System-Prüfung mit Ausnahme der Mechanik der Abschaltseinrichtung. Hierdurch wird mit einer Frequenz  $f_s = \frac{1}{\text{Reaktionszeit}} = \frac{1}{1,5\text{s}}$  das MISS von den Fühlern bis einschließlich einer kurzzeitigen Unterbrechung der Halteströme für die Abschaltstäbe geprüft. Fehlt der Abschaltimpuls an einer oder an mehreren der vorgesehenen Haltespulen wird zwangsläufig daraus sofort ein "Scramsignal" abgeleitet.

Durch diese Maßnahme werden gefährliche Fehler innerhalb der Systemreaktionszeit von 1,5 s in einen ungefährlichen Fehler überführt, der allerdings eine Abschaltung des Reaktors zur Folge hat. Damit wird ein gefährlicher Zustand des Reaktors ausgeschlossen. Interne Fehler werden nach Abschnitt 3.1.3. mit einer Frequenz von ca.  $f_i = 1$  kHz geprüft.

Liegt nur in einem Strang ein gefährlicher Fehler vor - falls man ein 2von3-System voraussetzt - so wird dieser ebenfalls in einen ungefährlichen Fehler überführt, jedoch folgt hierbei lediglich eine Alarmmeldung.

Einen weiteren Beitrag zur Sicherheit liefert die diversitäre Systemredundanz nach Abschnitt 3. Impliziert man als "worst-case" den Fall, daß trotz dynamischer Prüfung des MISS ein gefährlicher Fehler unentdeckt bleibt, so darf aufgrund unterschiedlicher Funktions- und Konstruktionsprinzipien diversitärer Systeme es als unwahrscheinlich angenommen werden, daß die Fehlerverteilungskurven für gefährliche Fehler beider Systeme deckungsleich sind. Damit ist aber eine Koinzidenz von gefährlichen Fehlern im MISS und dem konventionellen Schutzsystem als äußerst unwahrscheinlich zu betrachten.

Ein Reaktorunfall wäre daher nur über eine Triple-Koinzidenz denkbar:

gefährlicher Fehler im konventionellen Schutzsystem und  
gefährliche Fehler im MISS und  
gefährlicher Zustand des SNR.

## 2.7. Verfügbarkeit

Die MTBF- und MTTR-Werte<sup>\*)</sup> eines Systems sind Kenngrößen für seine Verfügbarkeit. Eine rechnerische Abschätzung wird im Abschnitt 3 jeweils im Anschluß an die entsprechenden Systemvariationen vorgenommen.

Problematisch bei der Projektierung eines Schutzsystems ist die Ausgewogenheit zwischen Sicherheit und Verfügbarkeit, da beide Größen gegenläufig sind. Ein Verfügbarkeitsvergleich zwischen einem konventionellen Schutzsystem und dem MISS ist nur auf der Basis von angenommenen Ausfalldaten durchzuführen, da Hersteller und Betreiber von konventionellen Schutzsystemen mit der Veröffentlichung eigener Daten zurückhalten. Ein realistischer Vergleich wird daher in diesem Rahmen für nicht möglich gehalten.

Es stehen ausreichende Mittel bzw. Methoden zur Verfügung, um für einen Kraftwerksbetreiber akzeptable Verfügbarkeitswerte zu erhalten. Deshalb werden für das MISS folgende Möglichkeiten vorgesehen:

- Ausreichende Dimensionierung der Geräteredundanz, entsprechend der zu erwartenden Ausfallwahrscheinlichkeit der Systemkomponenten,
- Fehlerdiagnose als Bestandteil des Prüfprogrammes, mit dem Ziel, die Reparaturzeit zu verkürzen und dadurch Fehlerkoinzidenzen herabzusetzen,
- Plausibilitätsprüfung der Meßwerte durch geeignete logische Verknüpfungen.

---

<sup>\*)</sup> MTBF = Mean Time Between Failure  
MTTR = Mean Time To Repair

### 3. Reaktorschutzsysteme mit Prozeßrechnern

Die umfangreiche Aufgabenstellung nach Abschnitt 2 und die weitgehenden Systemforderungen nach Abschnitt 2.4. zwingen zu einer Lösung mittels Prozeßrechner, d. h. neben dem Einsatz eines Prozeßrechners zur Dokumentation, Störungsmeldungen, Abbrandberechnungen u. ä. sollen zusätzlich Prozeßrechner den Reaktorschutz übernehmen.

Diese neue Einsatzart von Prozeßrechnern resultiert nicht allein aus den spezifischen Forderungen Schneller Natriumgekühlter Reaktoren. Sie stellt vielmehr einen konsequenten Schritt dar, nachdem bereits Prozeßrechner, vor allem in ausländischen Kernkraftwerken steuer- und regeltechnische Aufgaben übernommen haben [9]. Das MISS ist demnach ein Reaktorschutzsystem mit Rechnern, das aufgrund seiner zahlreichen Eingangsdaten auf zeitmultiplexer Basis arbeitet.

Bei der Konzipierung des MISS genügt es nicht, sich auf seine SNR-spezifischen Aufgaben (Erfassen und Verarbeiten der lokalen Eingangsdaten) zu beschränken. Es muß zusätzlich die Peripherie berücksichtigt werden, mit der das MISS in Verbindung zu stehen hat.

Die wesentlichen peripheren Systeme sind:

1. das konventionelle Schutzsystem
2. zwei unabhängige Abschalteinrichtungen
3. der Prozeßrechner zur Datenerfassung

Dieser Zusammenhang und der prinzipielle Aufbau des MISS werden in Fig. 8 dargestellt. Das darin vorgestellte Konzept dient als Basissystem für weitere Systemvariationen. Es erhebt nicht den Anspruch, daß die im Basissystem gewählte partielle Redundanz

(2von3) die optimale Lösung darstellt. Die Parameterstudien in den Abschnitten 3.1. - 3.5. sollen hierfür eine Entscheidungshilfe geben.

Da bereits schon ein konventionelles Schutzsystem existiert, ergibt sich für ein zweites, hinzukommendes Schutzsystem (MISS) die prinzipielle Forderung nach diversitärer Systemredundanz, welche die höchste Wertigkeit einer Redundanz darstellt. Dies bedeutet in dem vorliegenden Fall, daß die einzelnen, in den beiden Systemen sich entsprechenden Komponenten diverse Funktionsprinzipien aufweisen müssen. Nachstehende Übersicht läßt die Erfüllung dieser Forderung bei den wichtigsten Komponenten erkennen (SS = Schutzsystem):

Tabelle 4: Diversitäre Systemredundanz

System-Komponente	Funktionsprinzip im	
	konvention. SS	MISS
Grenzwertmelder	analoger Differenzverstärker für Subtraktion: Grenzwert-Meßwert	binäre Subtraktion: Grenzwert-Meßwert
2von3-Verknüpfung	Summieren von Impulströmen an einem Magnetkern mit rechteckförmiger Magnetisierungsschleife	DT- oder TT-Logik
Abschlußschaltung	Relaistechnik	Verstärkertechnik (kontaktlos)

Der konsequente diversitäre systemredundante Aufbau ist entscheidend für eine hohe Wertigkeit des Gesamtschutzsystems. Diese Wertigkeit kann mit Geräteredundanz allein nicht erreicht werden, allein schon deshalb nicht, weil die deterministischen Fehler im Gegensatz zu



den probabilistischen Fehlern nur durch diversitäre Systemredundanz wirksam abzubauen ist. Die Berücksichtigung dieser Forderung ist eines der wesentlichen Merkmale des MISS.

Wie aus Fig. 8 zu erkennen ist, wird dieser Weg durch Aufschaltung der integralen Eingangsdaten auf das MISS konsequent weiterverfolgt. Nach den Systemforderungen im Abschnitt 2.4. werden sowohl für das konventionelle Schutzsystem als auch für das MISS gestaffelte Grenzwerte gefordert.

Da das MISS die integralen Eingangsdaten zur Führung der lokalen Grenzwerte benötigt, werden aus Gründen der Diversität im MISS auch die gestaffelten Grenzwerte  $GW_{int}$  II gebildet und daraus resultierende Abschaltensignale zur MISS-Abschlußschaltung geführt. Umgekehrt werden die Abschaltensignale, die aus dem Vergleich mit den lokalen Grenzwerten  $GW_{lok}$  II resultieren, rückwirkungsfrei an die Abschlußschaltung des konventionellen Schutzsystems geführt.

Somit ergeben sich folgende Zuordnungen:

Tabelle 5: Grenzwertverarbeitung

<u>GW</u>	<u>wird gebildet in</u>	<u>und verwendet in Abschlußschaltung des</u>
$GW_{lok}$ I	MISS	MISS
$GW_{lok}$ II	MISS	konv. SS
$GW_{int}$ I	konv. SS	konv. SS
$GW_{int}$ II	MISS	MISS

Damit wird gewährleistet, daß bei Versagen des konventionellen Schutzsystems mit Ausnahme der Fühler und der Abschaltein-

richtung<sup>\*)</sup> über die exkursive Rückkopplung des Reaktors von der Bildung der Grenzwerte  $GW_{int}$  II bis einschließlich der Abschlußschaltung ein zweites diversitäres konventionelles System für eine zweite Abschaltung zur Verfügung steht. Für das MISS wird dadurch Diversität bezüglich der Abschlußschaltung erreicht.

Die Diversität wird in dem vorliegenden Konzept durch Verkopplung des konventionellen Schutzsystems mit dem MISS erreicht. Mittels konventioneller Koppellemente wäre solch eine Verkopplung nicht zulässig. Nachdem jedoch opto-elektronische Isolatoren mit einer Mindestdurchbruchspannung von 2,5 KV zur Verfügung stehen, kann eine rückwirkungsfreie Verkopplung gewährleistet werden. Dieser Nachweis dürfte auch gegenüber den Sicherheitsbehörden zu erbringen sein.

Ferner sieht das MISS vor, daß es den Prozeß-Rechner sowohl mit integralen als auch mit lokalen Eingangsdaten versorgen kann, was sich ohne zusätzlichen Aufwand durch die Aufschaltung der integralen Eingangsdaten auf das MISS ergibt. Die Übergabe der Daten an den Prozeßrechner erfolgt redundant, rückwirkungsfrei mittels Opto-Elektronik und unidirektional. Eine Daten-Versorgung des Prozeß-Rechners durch Reservefühler wird als ungünstig angesehen, da dieselben vom MISS selbst benötigt werden und damit eine zufriedenstellende Datenversorgung des Prozeß-Rechners nicht möglich wäre.

Ein weiterer Vorteil der vorgesehenen MISS-Konzeption liegt darin, daß für zukünftige Schutzsysteme von Reaktoren bei Bewährung des MISS das konventionelle Schutzsystem unter Verzicht der Systemredundanz wegfallen könnte, da die Aufgaben des konventionellen Schutzsystems bereits vom MISS übernommen werden.

---

<sup>\*)</sup> diese ist geräteredundant vorgesehen

### 3.1. 2von3-System

Die vergleichenden vorläufigen Berechnungen der Verfügbarkeit verschiedener ausfallsicherer Systeme in folgenden Abschnitten ergaben, daß die Verfügbarkeit eines 2von3-Systems mit konventionellen Rechnerkomponenten und Prozeßgeräten als Reaktorschutzsystem ausreicht. Nicht zuletzt aufgrund dieser Tatsache, aber auch aus der bereits vorgegebenen Meßfühlerbestückung wird anhand des 2von3-Systems die Aufgabenstellung untersucht und eine Lösung vorgeschlagen, die sich auf andere Systeme projizieren läßt.

In einem 2von3-System sollen drei Stränge möglichst folgende Forderungen erfüllen können:

- die drei Stränge sollen möglichst unabhängig voneinander sein. Eine gänzlich asynchrone Arbeitsweise ist aber bei der vorgegebenen Aufgabenstellung nicht möglich. Die Synchronisierung soll möglichst einfach erfolgen und eine starke Rechner-Rechnerkopplung z. B. zum Austausch großer Datenmengen soll möglichst vermieden werden.
- das System soll prüfbar sein und zwar in Abständen, die dem Zyklus der Prüfung der Abschaltbedingungen entspricht, d. h. alle 1,5 s. Die Prüfung soll die Abschlußschaltung und die Unterbrechung des Haltestromes mit einschließen.
- das Programm soll in Verbindung mit der Hardware "fail-safe"-Verhalten haben.
- das System sollte aus auf dem Markt erhältlichen Komponenten bestehen.

### 3.1.1. Systemaufbau

Das MISS ist aus drei Strängen und fünfzehn Abschlußschaltungen zur Betätigung der Abschaltvorrichtung, bestehend aus 15 Stäben, aufgebaut. Die 15 Stäbe setzen sich zusammen aus:

- 3 Abschaltstäben, vom MISS ansteuerbar und
- 12 Trimm-Abschaltstäben, vom MISS und vom konventionellen Schutzsystem ansteuerbar.

Das Blockschaltbild in Fig. 9 gibt einen Überblick über die Komponenten des Schutzsystems. Jeder der drei Stränge hat die gleiche Aufgabe. Die zentrale Komponente eines jeden Stranges ist der Rechner. Die Flexibilität eines Stranges und somit des gesamten Schutzsystems ist hauptsächlich auf die freie Programmierung zurückzuführen. Sollten sich die anfangs erwähnten Abschaltbedingungen als ungünstig erweisen, können neue Postulate durch Programmänderungen leichter berücksichtigt werden als die konventionellen festverdrahteten Schutzsysteme. An die Rechner sind eine Reihe von peripheren Geräten angeschlossen, von denen nur die wichtigsten im Blockschaltbild, dargestellt in Fig. 9, eingezeichnet sind. Die lokalen Meßgrößen, wie die Temperatur, der Durchsatz und das Durchsatznoise werden über Meßfühler in elektrische Größen wie Spannungen und Ströme umgewandelt und über Multiplexer MPX auf Analog-Digital-Konverter ADC geschaltet. Im Analog-Digital-Konverter werden die elektrischen Größen in digitale Informationen umgewandelt, die im Rechner gespeichert und verarbeitet werden. Das Meßwert Erfassungsprogramm in den einzelnen Strängen sorgt für die zeitlich richtige Abfrage der Meßwerte. Nach der Erfassung der Meßwerte werden synchron in allen drei Strängen die Abschaltbedingungen geprüft. Für die synchrone Verarbeitung sorgt eine Synchronisierereinrichtung. Wird in einem Strang die Abschaltbedingung als erfüllt anerkannt, dann werden über eine Digitalausgabe an jede Abschlußschaltung

eines Stabes zwei Abschaltssignale gegeben. Die Abschlußschaltung ist nämlich aus Gründen der Verfügbarkeit als 2von2-System aufgebaut. Auf die Abschlußschaltung wird in einem späteren Abschnitt näher eingegangen. Ist in mindestens 2von3 Strängen die gleiche Abschaltbedingung erfüllt, so werden von diesen Strängen Abschaltssignale an die 15 Abschlußschaltungen gegeben. Jede Abschlußschaltung generiert dann in einer 2von3-Entscheidung ein Scramsignal. Die Scramsignale sind identisch mit der Unterbrechung der Haltestrome und Haltemagnete in den dem MISS zugeordneten Abschaltstäben, Fig. 9.

Eingangs wurde besonders die Prüfbarkeit des Schutzsystem erwähnt; insbesondere soll die Prüfung die Unterbrechung des Haltestromes einschließen. Dazu ist aber zunächst das Verständnis des Funktionsablaufes in den einzelnen Strängen erforderlich.

Zur Ausgabe eines Abschaltssignals stehen pro Abschaltbedingung nur 6 ms zur Verfügung, wie noch später erläutert wird. Diese Zeit reicht wahrscheinlich nicht aus, um die Abschaltvorrichtung ansprechen zu lassen. Länger kann aber die Zeit nicht gewählt werden, so daß eine Selbsthaltung vorgesehen werden muß. Diese Selbsthaltung kann in der Abschlußschaltung sein, sie kann aber auch durch Rückführung der Haltestromunterbrechungsimpulse und mit Hilfe des Programms gemacht werden. Der Haltestrom der Haltespule wird höchstens so lange unterbrochen, daß der Stab noch nicht fällt bzw. mindestens so lange unterbrochen, daß das rückgeführte Signal eindeutig erkannt werden kann. Das Programm sorgt nun dafür, daß das Abschaltssignal gehalten wird. Wird nun in 2von3 Strängen das Abschaltssignal gehalten, kann die Abschaltvorrichtung ausgelöst werden.

Zur Prüfung des Systems besteht nun die Möglichkeit, eine simulierte Abschaltung einzuleiten. Dabei wird durch das Programm die Selbsthaltung verhindert. Um mögliche Fehlläufe des Pro-

gramms ohne Einfluß auf das "fail-safe"-Verhalten der Anlage zuzulassen, wird die Digitalausgabe mit einer programmgesteuerten Selbsthaltung versehen. Im Programm werden in zeitlichen Abständen Befehle eingebaut, die ein wiedertriggerbares Zeitglied in der Digitalausgabe ansteuern und nur so die Digitalausgabe in dem gewünschten Zustand hält. Fehlen diese Impulse, dann gibt die Digitalausgabe ein Abschaltsignal aus.

Die Fig. 10 zeigt den zeitlichen Funktionsablauf. Alle drei Stränge werden synchron von der Synchronisiereinrichtung alle 1,5 s gestartet. Ebenfalls sendet die Synchronisiereinrichtung alle 6 ms an alle 3 Rechner einen Impuls.

Das Programm hat folgende Aufgaben zu erfüllen:

- Erfassen der Meßwerte
- Prüfen der Abschaltbedingungen
- Prüfen der peripheren Geräte auf Fehler, wie Thermoelementisulationsverlust oder -bruch, Analog-Digital-Konverterdefekte, Abschlußschaltung defekt
- Prüfen auf interne Fehler des Rechners, wie Programmfehler
- Prüfen simulierter Abschaltbedingungen
- Ausgabe von Alarmmeldungen
- Ausgabe von Abschaltsignalen
- Grenzwertführung

Die Meßwerte können auf zweierlei Art erfaßt werden, entweder durch ein gesondertes Meßwerverfassungsprogramm, das gleich nach dem Start alle Meßwerte abfragt und speichert oder durch Abfrage der Meßwerte durch das Hauptprogramm und zwar zu dem Zeitpunkt, wenn die Meßwerte benötigt werden (random access).

In diesem Bericht werden beispielsweise beide Methoden angewandt, da die gewählte Art der Prüfung der TE-Isolation eine nochmalige Abfrage der TE-Spannung erfordert. Am Anfang eines 1,5 s-Zyklus werden alle Meßwerte abgefragt, Bei einer Erfassungszeit eines analogen Meßwertes von 100  $\mu$ s werden für 530 analoge Meßwerte 53 ms benötigt. Das sind 9 Zyklen á 6 ms. Um eine Reserve für

eventuell neu hinzukommende Meßwerte zu haben, werden für die Erfassung der Meßwerte 10 Zyklen á 6 ms vorgesehen. Der Einfluß von Störspannungen, insbesondere der Netzspannung und stochastischer Störungen kann reduziert werden, indem die Abfrage in den 3 Strängen 5 ms zeitversetzt vorgenommen wird, z. B.: Abfrage von T5/1, 5 ms später T5/2 und weitere 5 ms später T5/3. Für diese Zeitverzögerungen müssen 10 ms berücksichtigt werden. Wegen der Taktzeit werden dafür 2 Zyklen á 6 ms verwendet.

Nach der Meßwertabfrage werden die Abschaltbedingungen geprüft. Die Taktzeit von 6 ms wurde gewählt, weil mit folgenden Annahmen gerechnet wurde:

- 199 Abschaltbedingungen aus lokalen Größen
- 20 Abschaltbedingungen aus integralen Größen
- 6 Abschaltbedingungen aus simulierten Größen und
- 13 Abschaltbedingungen zur Reserve

Im 13. 6 ms-Zyklus wird die erste Abschaltbedingung geprüft. Die gleiche Abschaltbedingung muß synchron in allen 3 Strängen bearbeitet werden bzw. das gleiche Abschaltsignal muß synchron in mindestens 2 von 3 Strängen erzeugt werden, wenn eine Abschaltung erfolgen soll.

### 3.1.2. Synchronisation

In konventionellen Schutzsystemen erübrigt sich wegen der gleichzeitigen Aufschaltung aller Meßgrößen eine Synchronisation der 3 Stränge. Da im MISS die Meßgrößen seriell aufgeschaltet werden, muß zwangsläufig eine Synchronisation der 3 Stränge erfolgen.

Diese Synchronisation ließe sich umgehen, sofern man die analogen Meßsignale auf alle MPX/ADC verzweigt (analoge Verzweigung) bzw. eine polymorphe Struktur nach Abschnitt 3.3. wählt, in welcher jedem Rechner alle Eingangsdaten zugeführt werden (digitale Ver-

zweigung). Speichert nun jeder Strang sein Scramsignal, so ist ein nichtsynchronisierter Lauf der 3 Stränge denkbar. Der entscheidende Nachteil besteht jedoch darin, daß sich damit die Majoritätsentscheidung nicht mehr auf die Fühler eines Brennelementes bezieht sondern daß diese Entscheidung durch beliebige Kombinationen irgendwelcher Brennelemente herbeigeführt werden kann. Besonders bei einem MISS mit ca. 200 Brennelementpositionen wird dadurch die Verfügbarkeit nicht tolerierbar verschlechtert. Daher wird für alle hier zu behandelnden Systeme - auch im Falle polymorpher Verzweigungen - eine Synchronisation vorausgesetzt.

Infolge der Reaktionszeit von 1,5 s müssen innerhalb dieser Zeit alle Abschaltbedingungen geprüft werden. Daraus ergibt sich nach Abschnitt 3.1.1., daß jeder Abschaltbedingung in jedem Strang das gleiche 6 ms-Intervall zugeordnet ist.

Das unterschiedliche Ansprechverhalten der 3 Thermoelemente eines Brennelementes - auf Grund von Fertigungstoleranzen - ist bei einer Momentanwertabfrage nicht mehr vernachlässigbar. Daraus resultieren Phasenverschiebungen zwischen den 3 Thermoelementspannungen, die sich natürlich nicht synchronisieren lassen. Unter Berücksichtigung dieser Phasenverschiebung und einer ungünstigen Phasenlage zwischen physikalischer Störung und Meßwertabfrage mit einer anschließenden 2von3-Majoritätsentscheidung, kann die Störung erst nach einem zweiten Abfragezyklus erfaßt werden. Werden diese asynchronen Thermoelementspannungen berücksichtigt, so muß die vorgenannte Reaktionszeit von 1,5 s reduziert werden.

Die Synchronisierung kann mit einer externen Synchronisierschaltung oder mit Hilfe der Software und der internen Uhren der Rechner realisiert werden. Beim letzten Vorschlag müssen die Rechner untereinander verkoppelt werden, eine Eigenschaft, die der externen Synchronisation den Vorzug geben sollte. Das Problem der Verkopplung ist zwar in die Synchronisierschaltung verlagert,



ist aber hier im Störfall leichter zu überblicken. Die Fig. 11 zeigt einen Schaltungsvorschlag für eine Synchronisierschaltung. Das Gatter G wird, solange der Umschalter in HALT-Stellung ist, gesperrt. Die Impulse des Oszillators können nicht auf den Zähler gelangen. Mit dem START-Impuls wird in allen 3 Strängen über das Monoflop MF1 ein 1,5 s-Impuls simuliert. Die Impulse werden in der 2von3-Auswahlschaltung ausgewertet und ein Rücksetzimpuls für die Zähler abgeleitet. Für die gleiche Zeit wird auch Gatter G gesperrt. Erst wenn 2von3 der 1,5 s-Impulse nicht mehr anstehen, werden die Impulse des Oszillators vom Zähler gezählt.

### 3.1.3. Prüfbarkeit

Die Sicherheit und die Verfügbarkeit eines Sicherheitssystems hängt in hohem Maße von seiner Prüfbarkeit ab. Durch die Prüfung des Schutzsystems bzw. seiner Komponenten können gefährliche Fehler in ungefährliche Fehler umgewandelt werden.<sup>\*)</sup> Zweck der Prüfung ist es, solche Fehler zu finden und zu lokalisieren. Zur Erhöhung der Verfügbarkeit eines Systems ist es ratsam, der Prüfung eine Diagnose folgen zu lassen, um die Reparatur möglichst schnell durchführen zu können. Das Diagnoseprogramm teilt über einen Störprotokollblattschreiber möglichst detailliert die Fehlerursache mit. Fehler können nach verschiedenen Merkmalen klassifiziert werden. Klassifiziert man sie in Bezug des Ortes, wo sie auftreten, unterscheidet man periphere Fehler und interne Fehler.

---

<sup>\*)</sup> Gefährliche Fehler: Der Reaktor hat einen derartigen Betriebszustand erreicht, daß eine Abschaltung durch das Schutzsystem ausgelöst werden soll. Ein Fehler im Schutzsystem verhindert diese notwendige Abschaltung.

Ungefährliche Fehler: Der Betriebszustand des Reaktors ist normal, ein Fehler im Schutzsystem löst eine Abschaltung aus.

### 3.1.3.1. Periphere Fehler

Periphere Fehler sollen solche Fehler sein, die in den peripheren Geräten des Rechners und in den Meßumformern auftreten. Es gibt zwei Arten von peripheren Fehlern: solche, die in Geräten auftreten, deren Ausfall nicht unbedingt ein Abschalten der Anlage erfordert (z. B. Ausfall eines Störprotokolldruckers) und solche Fehler, die in Geräten auftreten, deren Ausfall die Sicherheit der Anlage in Frage stellt und deshalb ein Abschalten des betreffenden Stranges erfordert (z.B. Ausfall eines Analog-Digital-Konverters).

In dem folgenden sollen nur die Prüfungen der letztgenannten Fehler behandelt werden.

Die Thermoelemente können auf zweierlei Art defekt werden: Ein Thermoelement kann brechen oder es ist ein Isolationsverlust möglich. Ein Thermoelementbruch wäre ohne Prüfung ein gefährlicher Fehler, da ein gebrochenes Thermoelement keine Temperaturüberschreitung anzeigt. Thermoelementbruch kann mit der Plausibilitätsprüfung detektiert werden: Es ist plausibel, daß ein intaktes Thermoelement bei einer bestimmten Reaktorleistung eine bestimmte Mindesttemperatur anzeigen muß. Wird dieser untere Grenzwert unterschritten, dann liegt mit großer Wahrscheinlichkeit ein Thermoelementbruch vor, oder aber der Multiplexerschalter ist defekt. Das Diagnoseprogramm gibt auf einem Störprotokollblattschreiber die mögliche Fehlerursache und den Fehlerort aus.

Die Thermoelementisolation kann verloren gehen, wenn Natrium in die Meßpflaume und in die Mantelthermoelemente eindringt. Das Natrium kann die Meßstelle in einen wesentlich über dem Brennelementaustritt liegenden Bereich verlagern. Dort ist es bereits von vielen Brennelementen durchmischt. Temperaturerhö-

hungen des einzelnen, dem Thermoelement zugeordneten Brennelement können nicht angezeigt werden. Somit läge ein gefährlicher Fehler vor. Durch Prüfung der Thermoelementisolation kann dieser gefährliche Fehler eliminiert werden. Die Fig. 12 zeigt die Meßmethode. Über den Hilfsmultiplexer wird eine Hilfsspannung  $U$  an einen Schenkel des Thermoelements gelegt, und zwar über die Dauer eines 6 ms-Zyklus. Über dem Leitungswiderstand  $R_L$  und dem Thermoelement-schenkelwiderstand  $R_{TES}$  bildet sich eine Spannung, deren Verlauf in der Fig. 12 dargestellt ist. Diese Spannung überlagert sich der Thermoelementspannung. Die Summe beider wird am Ende des 6 ms-Zyklus gemessen. Weicht der Meßwert in vorzugebenden Grenzen von dem Meßwert ohne Hilfsspannung ab, so ist der Isolationswiderstand zu klein.\*)

Jede Temperaturmeßstelle wird im 1,5 s-Zyklus überprüft. Diese Überprüfung kann aber auch in größeren Zeitabständen erfolgen.

Der Durchsatzmesser hat einen speziellen Ausgang, der bei Defekt ein digitales Signal liefert. Außer dieser Möglichkeit kann aber zusätzlich der Meßwert des Durchsatzes auf seine Plausibilität hin untersucht werden.

Die Prüfung der Abschlußschaltungen wird mit simulierten Abschaltbedingungen durchgeführt. Hiermit werden nicht nur die Abschlußschaltungen, sondern auch das Programm und alle wichtigen Geräte eines Stranges getestet. In mehreren Prüfzyklen wird jeweils von 2 von 3 Rechnern ein Abschaltsignal an die Abschlußschaltung gegeben. Damit ist die Scrambedingung erfüllt und der Haltestrom in der Abschaltvorrichtung wird unterbrochen. Über eine Rückführung können die Rechner feststellen, ob der Haltestrom von allen Abschlußschaltungen unterbrochen wurde und können gleichzeitig den Haltestrom wieder einschalten. Die Unterbrechung des Haltestroms darf höchstens so lang sein, daß die Abschaltvorrichtung noch nicht angesprochen hat und die Stäbe nicht abfallen. Die Abschluß-

---

\*) Es kann eine Folgeoperation ausgelöst werden.

schaltung ist als 2von2-System aufgebaut. Aus dem Impulsplan Fig. 10 geht die Prüffolge der Abschlußschaltung hervor. Im 245. 6 ms-Zyklus werden nur vom ersten Strang Rechner-Abschaltsignale an die Abschlußschaltungen gegeben. In diesem Fall darf keine Haltestromunterbrechung erfolgen. Wird diese trotzdem angezeigt, so liegt ein Fehler in der Auswahl-schaltung vor. Das gleiche gilt für den 246. und 247. 6 ms-Zyklus.

In den drei darauffolgenden Zyklen werden von jeweils zwei Rechnern Abschalt-signale an die Abschalt-einrichtung gegeben. Dabei muß von allen Abschlußschaltungen eine Rückmeldung der Haltestromunterbrechung erfolgen. Bei diesen insgesamt 6 Prüfzyklen für simulierte Abschaltbedingungen muß der Haltestrom nach wenigen Millisekunden wieder eingeschaltet werden, während bei den üblichen Prüfzyklen für echte Abschaltbedingungen eine programmierte Selbsthaltung stattfindet.

Pro 1,5 ms-Zyklus müssen von jedem Strang je 3 simulierte Haltestromunterbrechungen rückgemeldet werden. Werden nur 2 Unterbrechungen rückgemeldet, so wurde ein gefährlicher Fehler entdeckt und das System arbeitet nur noch als 1von2-System.

### 3.1.3.2. Interne Fehler

Unter internen Fehlern sollten solche verstanden werden, die in der Zentraleinheit des Rechners auftreten und falsche Programm-abläufe zur Folge haben. Derartige Fehler lassen sich leichter detektieren, wenn man zusätzlich die Hardware benutzt. Die Digitalausgabegeräte, die die Abschalt-signale ausgeben, können mit einer zusätzlichen Selbsthaltung versehen werden. An bestimmten Programmstellen wird in bestimmten Zeitabständen von ca. 1 ms an die Digitalausgabegeräte ein Impuls gegeben, der die Digitalausgabe in der Lage hält, daß kein Abschalt-signal ausgegeben wird. Beim Fehlen dieser Impulse steht ein Dauersignal als Abschalt-signal an.

#### 3.1.4. Programme

Das Betriebssystem oder Organisationsprogramm koordiniert den Ablauf aller im System vorhandenen Programme unter Verwendung einer vom Systementwickler vorgegebenen Prioritätstabelle und führt Buch über die Zustände, in denen sich die Programme gerade befinden. Die einzelnen Programme können zu vorgegebenen Zeiten durch andere Programme gestartet werden. Ferner ist eine Initialisierung über externe Geräte, wie z. B. die Eingabe von Parametern, die infolge des Abbrandes geändert werden müssen, möglich.

Die Programme, die unter der Kontrolle des Betriebssystems laufen, sind im einzelnen:

- Programm zur Erfassung der Meßgrößen
- Programm zur Prüfung der echten und simulierten Abschaltbedingungen sowie der Alarmbedingungen, die eine Vorwarnung eines Scrams darstellen.
- Programme zur Prüfung der peripheren Geräte und Fühler und zur Diagnose
- Programme zur Berechnung der Grenzwerte der Temperatur und des Durchsatzes, die sowohl von der Leistung als auch vom Abbrand abhängig sind
- Programm zur Eingabe von Faktoren zur Berücksichtigung des Abbrandes bei der Neufestsetzung der Grenzwerte
- Programm zur Erfassung von Meßgrößen, um nach einem Scram einen Störablauf auszudrücken.
- Programm zur Übergabe der Meßwerte an den Prozeßrechner.

Bereits in Abschnitt 3.1.1. wurde auf einige Eigenschaften der Programme hingewiesen, sofern sie zum Verständnis des Systems nötig waren.

Das Meßwernerfassungsprogramm erfaßt sowohl analoge als auch digitale Meßwerte. Analoge Meßwerte sind 199 Temperaturmeß-

werte, 151 Durchsatzmeßwerte und 151 Durchsatznoisemeßwerte. Die 151 Störungssignale des Durchsatzmessers sind digitale Signale. Die analogen Meßwerte werden über einen Multiplexer auf einen Analog-Digital-Wandler geschaltet und dort digitalisiert. Das Ergebnis kann sowohl dual als auch binär-codiert-dezimal vorliegen. Bezogen auf den Speicherplatzbedarf, ist die duale Codierung günstiger. Einige Multiplexer-Eingänge sind mit Prüfspannungen oder Pseudomeßwerten für eine simulierte Grenzwertüberschreitung belegt. Pro analogem Meßwert kann mit einer Gesamtverarbeitungszeit von 100  $\mu$ s gerechnet werden. Die digitalen Meßwerte werden über eine Digitaleingabe abgefragt.

Die Gesamtlaufzeit des Meßwernerfassungsprogramms beträgt ca. 60 ms. Die Meßwernerfassung wird der Prüfung der Abschaltbedingungen vorausgestellt. Eine Abfrage der Meßwerte jeweils kurz vor der entsprechenden Prüfung der Abschaltbedingung (random access) ist aus zeitlichen Gründen nur sinnvoll, wenn die Meßwerte der Nachbarschaftselemente nicht berücksichtigt werden. Gleiche Meßstellen würden sonst mehrmals abgefragt werden.

Nach der Erfassung der Meßwerte kann die eigentliche Meßwertverarbeitung erfolgen, nämlich die Prüfung der Abschaltbedingungen sowie der Alarmbedingungen. Letztere ist identisch mit einer Prüfung einer Überschreitung eines Vorwarnpegels. Diese Prüfung der Alarmbedingung führt zu einer Alarmausgabe, die den Operator in Kenntnis setzen soll, daß mit einem Abschalt-signal zu rechnen ist. Die Abschaltbedingungen sind in Abschnitt 2.3. erläutert. Das Programm ist für alle Abschaltbedingungen dasselbe und wird in Abhängigkeit von der Nummer der Abschaltbedingung durchlaufen. Für einen Durchlauf stehen 6 ms zur Verfügung.

Das Programm zur Berechnung der Grenzwerte von Temperatur und Durchsatz löst die im Abschnitt 2.2. angegebenen Gleichungen und läuft simultan zu dem vorher angeführten Programm ab.

Die Eingabe der Korrekturfaktoren zur Berücksichtigung des Abbrandes erfolgt über ein Bedienungspult. Die Korrekturfaktoren brauchen nur in größeren Zeitabständen geändert zu werden. Die Fig. 13.1. und 13.2. gibt eine Zusammenstellung aller Programme und eine vorläufige minimale Kernspeicherabschätzung von 12 kWorten.

Organisationsprogramm a) Interrupt-Verwaltung b) Scheduler c) Überwachung der Ein- und Ausgabe d) Koordinierung	2 k
Meßwerterfassungsprogramm	0,5 k
Speicherplatz für 199 Temperatur-Momentan-Meßwerte 151 Durchsatz-Meßwerte 151 Durchsatznoise-Meßwerte 151 Störungssignale des Durchsatzmessers	1 k
Grenzwertbildungsprogramm z. B. über Mittelwertbildung von Temperatur, Durchsatz und Durchsatznoise	1 k
Speicherplatz für 199 Temperatur-Grenzwerte 151 Durchsatz-Grenzwerte 151 Durchsatznoise-Grenzwerte	0,5 k
Hauptprogramm Prüfen der Abschaltbedingungen und Funktionsüberwachung der Anlage (Ausgabe von Testsignalen)	2 k

Fig. 13.1.: Speicherplatzabschätzung für das MISS-SNR

Prüfen der Alarmbedingungen und Ausgabe von Alarmmeldungen (in Klartext)	2 k
Zusatzprogramm zur schnellen Datenausgabe. Start erfolgt nach dem Scram durch Rückmeldung von der Abschalt- einrichtung	1 k
Prüfprogramme  Prüfung der Thermoelemente auf Bruch und Isolation sowie Prüfung des Durchsatzes auf Plausibilität	1 k
Eingabeprogramme zur Berücksichtigung des Abbrandes bei der Neufestsetzung der Grenzwerte	0,5 k
Beladungsplan	0,5 k
Tabelle der Nachbarschaftselemente	1 k
	<u>12 k</u>
	Σ 12 k (minimale Abschätzung)

Fig. 13.2.: Speicherplatzabschätzung für das MISS-SNR

### 3.1.5. Abschlußschaltung

Die Abschlußschaltung liefert die Halteströme für die 15 Haltespulen der 15 Abschaltstäbe. Fig. 14 gibt einen Überblick über die Abschlußschaltung. Die Abschlußschaltung ist als 2von2-Schal-



tung aufgebaut. Die zwei Stränge bestehen aus den Auswahl-  
schaltungen und den Halteverstärkern für 15 Stäbe. Jeder Rechner gibt  
über eine Digitalausgabe 2 x 15 Abschalt-signale. Die Abschalt-  
signale können gleichzeitig oder auch einzeln gesendet werden,  
z. B. um die Funktionstüchtigkeit der beiden Stränge einzeln zu  
überprüfen. Die Auswahl-schaltung ist über opto-elektronische Koppel-  
elemente an die Digitalausgabe angeschlossen. Die Auswahl-schaltung  
eines Stranges gibt ein Unterbrechungssignal an den Halteverstärker,  
wenn 2 von 3 Rechner ein Abschalt-signal an die Auswahl-schaltung  
liefern. Das gleiche gilt für die Auswahl-schaltung des zweiten  
Stranges. Wenn 2 von 2 Halteverstärker keinen Strom mehr an  
die Haltespule liefern, wird die Abschalt-einrichtung betätigt.  
In den Stromkreisen der Haltespulen sind Übertrager. Eine Halte-  
stromunterbrechung kann dadurch von den 3 Rechnern erfaßt werden.  
Wird bei der Prüfung einer echten Abschaltbedingung eine Halte-  
stromunterbrechung festgestellt, so geht das Programm in Selbst-  
haltung und der Haltestrom bleibt über die Zeit von 6 ms hinaus  
unterbrochen. Bei der simulierten Abschaltung darf der Halte-  
strom nur so kurzzeitig unterbrochen werden, daß die Abschalt-ein-  
richtung noch nicht anspricht. Genauere Werte über die Zeiten, wie  
lange der Haltestrom abgeschaltet sein darf, ohne daß die Abschalt-  
einrichtung anspricht und wie lange der Haltestrom mindestens ab-  
geschaltet sein muß, damit die Abschalt-einrichtung sicher an-  
spricht, liegen noch nicht vor. Es ist jedoch anzunehmen, daß  
6 ms sicher nicht ausreichen, um die Abschalt-einrichtung an-  
sprechen zu lassen.

Durch die gewählte 15-fache Unterteilung der Digitalausgabe ist  
die Möglichkeit gegeben, die simulierte Abschaltung der Halte-  
ströme zeitlich auch seriell vorzunehmen.

Im Gegensatz zu einer anderen bereits in der Anwendung [10] befind-  
lichen Schaltung enthält die hier vorgeschlagene Abschluß-schaltung  
eine festverdrahtete 2 von 3-Logik. Als weiterer wesentlicher Unter-  
schied ist festzustellen, daß die Prüfung der Abschluß-schaltung

auf der Basis einer programmierten Selbsthaltung in die Gesamtprüfung eines Stranges (s. 3.1.3.) integriert ist, d. h. die Prüfimpulse für die Abschlußschaltung sind mit den simulierten Meßwerten an den Analogeingängen der MPX/ADC identisch.

### 3.1.6. Verfügbarkeit

Die Verfügbarkeit bzw. Nichtverfügbarkeit eines Reaktorschutzsystems läßt sich anschaulich durch seinen MTBF- und seinen MTTRwert ausdrücken. Diese Werte sind abhängig vom Systemaufbau und von den MTBF-Werten bzw. den MTTR-Werten der Systemkomponenten.

In den folgenden Betrachtungen wird dieser Zusammenhang auf binominaler Basis abschätzend untersucht, wobei die Reparaturzeit als Parameter eingeführt wird. Da es derzeit nicht möglich ist, von Komponentenherstellern verbindliche Verfügbarkeitsdaten zu erhalten und zum Einsatzzeitpunkt des MISS möglicherweise günstigere Verfügbarkeitsdaten als zurzeit gelten, wurde der MTBF-Wert der Systemkomponenten variabel gehalten.

Die nachfolgenden Betrachtungen sollen aufgrund probabilistischer Komponentenfehler und einer konstanten Ausfallrate (Poisson-Verteilung) die zeitlich mittleren Ausfallabstände verschiedener Systemvariationen miteinander vergleichen. Für die Rechnungen wurden ausfallsichere Voterschaltungen angenommen. Sie unterscheiden nicht zwischen gefährlichen und ungefährlichen Fehlern.

Die Ergebnisse werden nur unter Berücksichtigung der probabilistischen Fehler erzielt. Deterministische Fehler wurden nicht betrachtet, da sie einer Rechnung praktisch nicht zugänglich sind. Daher stehen im folgenden vergleichende Betrachtungen im Vordergrund.

### 3.1.6.1. Verfügbarkeit des 2von3-Systems

Sind in einem Schutzsystem mehrere Stränge redundant so verschaltet, daß die gewünschte Funktion von  $i$  der vorhandenen  $k$  Stränge ausgeführt wird, und hat jeder Strang die gleiche Nichtverfügbarkeit  $Q_s$ , so ist die Nichtverfügbarkeit eines  $i$ von $k$ -Systems:

$$Q_{i\text{von}k} = \binom{k}{i} Q_s^i \quad Q_s \ll 1 \quad (8) \quad [1, 11]$$

Die Nichtverfügbarkeit  $Q_s$  errechnet sich aus der Ausfallwahrscheinlichkeit [12]

$$Q_s(t) = \frac{\lambda_s}{\lambda_s + \mu_s} \left\{ 1 - \exp [ - (\lambda_s + \mu_s) t ] \right\} \quad (9)$$

Es gelten folgende Symbole:

$m_s$  = mittlerer zeitlicher Ausfallabstand eines Stranges (MTBF)

$\lambda_s$  =  $\frac{1}{m_s}$  = Ausfallrate eines Stranges

$\mu_s$  =  $\frac{1}{t_r}$  = Reparaturrate eines Stranges

$t_r$  = mittlere Reparatur- und Diagnosezeit (MTTR) eines Stranges bzw. "down-time"

$t_{r,\text{syst}}$  = mittlere Reparatur- und Diagnosezeit (MTTR) des Systems

$t_r, t_{r,\text{syst}} \ll m_s$

Wird  $t \rightarrow \infty$  so erhält man die Nichtverfügbarkeit [13]

$$Q_s = \frac{\lambda_s}{\lambda_s + \mu_s} = \frac{t_r}{m_s + t_r} \cong \frac{t_r}{m_s} = \frac{t_{\text{down}}}{t_{\text{up}}} \quad (10)$$

Damit wird die Strang-Nichtverfügbarkeit als das Verhältnis von mittlerer "down-time" und mittlerer "up-time" formuliert. Für eine begrifflich mehr abgesicherte Rechenmethode ist auf die Momentenmethode [14] zu verweisen. Die Ergebnisse sind jedoch ähnlich.

Die Nichtverfügbarkeit  $Q_{2\text{von}3}$  für ein 2von3-System errechnet sich

$$Q_{2\text{von}3} = \binom{3}{2} Q_s^2 = 3 Q_s^2 \approx 3 \frac{t_r^2}{m^2} \quad (11)$$

Zur Errechnung des mittleren zeitlichen Ausfallabstandes  $m_{2\text{von}3}$  des 2von3-Systems wird angenommen, daß bei Ausfall eines Stranges sofort mit der Reparatur begonnen wird. Diese beansprucht die Zeit  $t_r$ .

Das System wird dann ausfallen, wenn während dieser Zeit  $t_r$  ein zweiter Strang ausfällt. Auch diese Reparatur wird sofort begonnen und benötigt ebenfalls die Zeit  $t_r$ . Das System ist aber bereits wieder funktionsbereit, wenn die Reparatur des ersten Stranges beendet ist.

Nimmt man eine gleichmäßige Verteilung der Ausfallereignisse an, so wird im Mittel der Ausfall des zweiten Stranges dann eintreten, wenn die Reparatur des ersten Stranges zur Hälfte beendet ist. Damit ist aber das System nur für die Zeit

$$t_{r,\text{syst.}} = \frac{1}{2} t_r \quad (12)$$

außer Betrieb.

Mit den Gleichungen (11) und (12) kann die Beziehung zur Errechnung des mittleren zeitlichen Systemausfallabstandes  $m_{2\text{von}3}$  formuliert werden:

$$3 \frac{t_r^2}{m^2} = \frac{t_{r,\text{syst.}}}{m_{2\text{von}3}} = \frac{1}{2} \frac{t_r}{m_{2\text{von}3}} \quad (13)$$

$$m_{2\text{von}3} = \frac{1}{6} \frac{m_s^2}{t_r} \quad (14)$$

Die graphische Auswertung dieser Gleichung ist u. a. im Diagramm in Fig. 15 enthalten. Hieraus ist beispielsweise unter Berücksichtigung der Reparaturzeit der erforderliche mittlere zeitliche Strang-Ausfallabstand  $m_s$  zu entnehmen, um einen für die Praxis akzeptablen System-Ausfallabstand zu erhalten.

Die vorerst relativ unsichere Größe bei der Benutzung des Diagramms ist  $m_s$ . Wie wichtig diese Größe ist, zeigt in Gl. 14 ihr potentieller Einfluß auf das Gesamtverfügbarkeits-Ergebnis  $m_{2\text{von}3}$ . Die Größe  $m_s$  hängt im wesentlichen von der Verfügbarkeit der Fühler (vor allem der Thermoelemente), des MPX/ADC, des Rechners und der Abschlußschaltung ab.

Es ist damit zu rechnen, daß die Thermoelemente eine ausreichende Verfügbarkeit haben werden. Andernfalls kann durch Bereitstellung von Reservethermoelementen und/oder Ersatz von defekten Thermoelementen durch Software - z. B. durch Nachbarschaftsabfrage oder Plausibilitätsprüfungen - die Verfügbarkeit zumindest indirekt weiter gesteigert werden. Ebenso wird im Abschnitt 3.1.6.2. abgeschätzt, daß die Abschlußschaltung weitgehend ausfallsicher aufgebaut werden kann.

Damit beschränken sich die nachfolgenden Abschätzungen auf die redundante und strukturelle Anordnung von MPX/ADC und Rechner als kritische Systemkomponenten, deren mittlerer zeitlicher Ausfallabstand zur Zeit je bei ca.  $m = 2000$  h liegen dürfte [9]. Mit diesem Wert ergibt sich dann beispielsweise - wegen der Serienschaltung von MPX/ADC und Rechner - ein mittlerer Strang-Ausfallabstand  $m_s = 0,5 m = 1000$  h. Setzt man dabei eine Reparaturzeit von  $t_r = 2$  h voraus, so ergibt sich nach Diagramm in Fig. 15 ein System-Ausfallabstand von  $m_{2\text{von}3} \approx 9,5$  Jahre.

Bei allen Verfügbarkeitsbetrachtungen wurden die Stromversorgung und die Klimaanlage, sofern letztere erforderlich ist, nicht betrachtet. Eine ausreichende Redundanz dieser Anlage-Komponenten wird vorausgesetzt.

### 3.1.6.2. Einfluß der Abschlußschaltung auf die Verfügbarkeit des Gesamtsystems

Konventionelle Schutzsysteme sind so aufgebaut, daß die Abschalt-signale der einzelnen Stränge in der Regel zwei oder mehrere Voter-elemente seriell durchlaufen. Fig. 16 zeigt beispielsweise vereinfacht den Zusammenhang an einem 2von3-System.

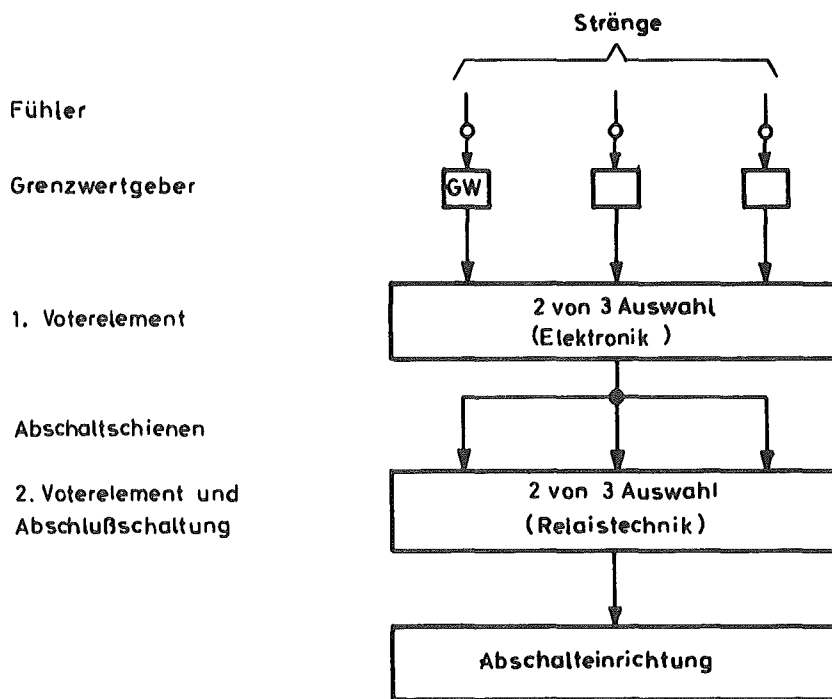


Fig.16 Serienschaltung von Voterelementen

Setzt man ausfallsichere Voterelemente voraus, so ist der Vorteil relevant: Liefert ein Strang durch Defekt ein Abschaltsignal, so werden durch das davorgeschaltete Voterelement die Abschaltsschienen von einem unerwünschten Abschaltsignal freigehalten. Unter Berücksichtigung einer nicht vernachlässigbaren Ausfallwahrscheinlichkeit der Abschlußschaltung erreicht man durch diese Maßnahme eine Verfügbarkeitserhöhung. Diese Maßnahme ist jedoch nur sinnvoll und notwendig, wenn das davorgeschaltete Voterelement selbst weitgehend ausfallsicher ist und die Abschlußschaltung eine ungenügende Verfügbarkeit hat.

Das in diesem Bericht vorgestellte Schutzsystem-Konzept verzichtet zugunsten der Prüfbarkeit der ODER-Funktionen in der Abschlußschaltung auf die Serienschaltung zweier Voterelemente. Wie die nachfolgende Abschätzung zeigt, ist diese Vereinfachung dadurch gerechtfertigt, daß eine Verfügbarkeitsminderung, bedingt durch den Wegfall eines 2. Voterelements, auf das Gesamtsystem vernachlässigbar ist. Zu einer vereinfachten Abschätzung wird angenommen, daß die am Ausfall beteiligten Komponenten A, A' ... H, H' (Fig. 17) alle die gleiche Nichtverfügbarkeit Q haben.

Nach den MIL-HDBK-217A-Spezifikationen [12] wird eine konstante Ausfallrate einer einzelnen Komponente  $\lambda = 40 \cdot 10^{-8}/h$  angenommen. Bei einer angenommenen "Downtime"  $t_r = 1 h$  ergibt sich damit die Nichtverfügbarkeit für eine Komponente zu

$$Q = t_r \cdot \lambda = 40 \cdot 10^{-8} \quad (15)$$

Zwischen der Nichtverfügbarkeit Q und der Verfügbarkeit R besteht die Beziehung

$$Q = 1 - R \quad (16)$$

Bei eingehender Betrachtung von Fig. 17 erkennt man, daß beispielsweise bei Vorhandensein der Abschaltssignale 1 - 15 und 1' - 15' von Rechner 1 28 verschiedene Ausfallkombinationen zweier defekter Bauelemente, z. B. A und A' oder B und B' eine unerwünschte Ab-

schaltung herbeiführen können. Defekte Bauelemente werden durch ein Negationszeichen über der Bezeichnung des Bauelementes gekennzeichnet. Für eine Kombination lautet die entsprechende Wahrscheinlichkeitsfunktion [12]:

$$P(\bar{A} \wedge \bar{A}' \wedge B \wedge B' \wedge C \wedge C' \wedge D \wedge D' \wedge E \wedge E' \wedge F \wedge F' \wedge G \wedge G' \wedge H \wedge H') = Q^2 R^{14} \quad (17)$$

Da alle 28 Ausfallkombinationen eintreten können, gilt für die resultierende Nichtverfügbarkeit

$$Q_{\text{res}} = 28 Q^2 R^{14} \quad (18)$$

Wird die Verfügbarkeit  $R = 1 - Q$  substituiert, so erhält man

$$\begin{aligned} Q_{\text{res}} &= 28 Q^2 (1 - Q)^{14} \\ &= 28 Q^2 (1 - 14 Q + \dots + Q^{14}) \end{aligned} \quad (19)$$

$$Q \ll 1 \quad Q_{\text{res}} \cong 28 Q^2$$

Berücksichtigt man, daß insgesamt 15 solche 2von2-Schaltungen parallel an die Abschaltschiene geschaltet sind, dann ergibt sich für die resultierende Nichtverfügbarkeit

$$Q_{\text{ges}} \cong 420 Q^2 \quad (20)$$

und mit  $Q = 40 \cdot 10^{-8}$

$$Q_{\text{ges}} \cong 6,7 \cdot 10^{-11} \quad (21)$$

Daraus errechnet sich die MTBF bei 1 h "Downtime":

$$MTBF \cong \frac{t_r}{Q_{\text{ges}}} = 1,5 \cdot 10^{10} \text{ h} \approx 1,5 \cdot 10^6 \text{ Jahre} \quad (22)$$



Dieser mittlere Ausfallabstand ist so groß, daß durch die Abschlußschaltung mit nur einer Voterebene keine wesentliche Verfügbarkeitsminderung für das gesamte MISS zu erwarten ist.

### 3.2. 2von3-System mit aktiver Redundanz durch 4. MPX/ADC

Prinzipiell ist der Systemaufbau in Fig. 18 dargestellt. Aufgrund seines "stand-by-Verhaltens" ist der 4. MPX/ADC als eine aktive Geräteredundanz gekennzeichnet. Tritt in 1von3 Strängen ein Fehler auf, so muß durch ein Fehleranalyseprogramm der Fehler nach Funktionseinheiten lokalisiert werden. Zeigt es sich, daß der Fehler "vor" dem Rechner liegt, so hat der betroffene Rechner programmgemäß Zugriff zu dem 4. MPX/ADC. Für einen weiteren Zugriff durch die beiden anderen Rechner wird solange eine Verriegelung gespeichert, bis die Reparatur behoben ist.

Eine derartige Lösung erscheint deshalb interessant, da durch die System-Erweiterung um einen 4. MPX/ADC das Reserve-Thermoelement im Bedarfsfalle automatisch aufgeschaltet werden kann. Eine manuelle Aufschaltung ist zeitaufwendig und bringt vor allem durch den Faktor Mensch gerade in einem-Schutzsystem ein zusätzliches Risiko.

Ferner bietet diese Systemvariante den Vorteil des automatischen und daher kurzfristigen "Austausches" eines MPX/ADC, der wie der Rechner als eines der relativ unsicheren Systemkomponenten betrachtet wird. Der automatische Austausch eines MPX/ADC gleicht einer extrem kurzen Reparaturzeit  $t_p$ , was sich nach Gl. 5, Abschn. 3.1.6.1., günstig auf das Gesamtverfügbarkeitsergebnis  $m_{2von3}$  auswirkt.

Diese vorangegangenen Betrachtungen verlangen allerdings einen weitgehend ausfallsicheren Umschalter. Ebenso kann die Umschaltung auf die Reservekomponente nur einmal pro Reparaturzeit  $t_p$  und einmal pro Strang vorgenommen werden. Unter diesen Einschränk-

kungen darf die nachfolgende Verfügbarkeitsabschätzung interpretiert werden.

Die Aufschaltung eines 4. Ersatz-MPX/ADC entspricht einer teilweisen Strangredundanz, wie in Fig. 18 dargestellt.

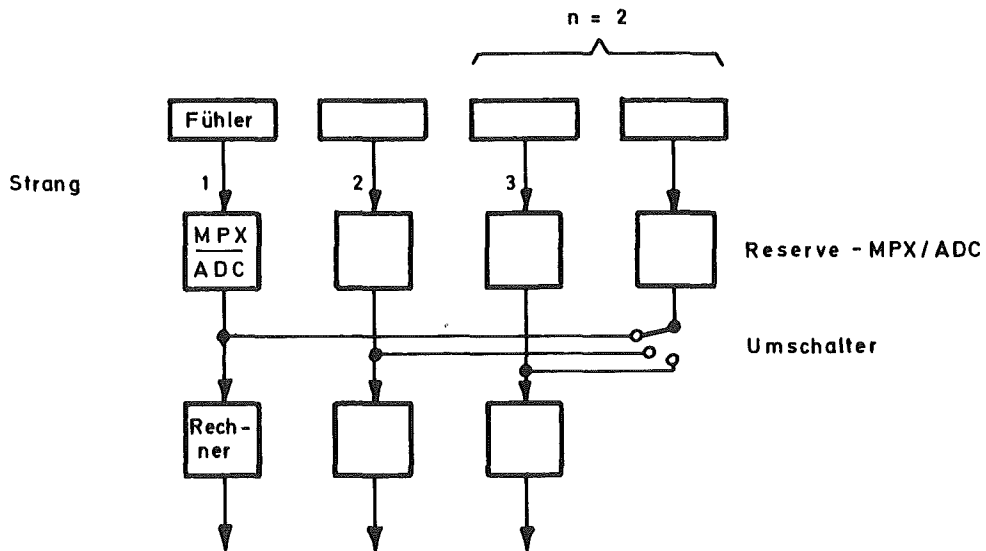


Fig.18 Teilweise, aktive Strangredundanz durch 4. MPX/ADC

Bei aktiver Redundanz gilt für den Ausfallabstand des MPX/ADC [12]

$$m_{\text{MPX/ADC, akt. Red.}} = \frac{1}{\lambda} \sum_{k=1}^n \frac{1}{k} \quad [h] \quad (23)$$

$n$  = Anzahl der parallelen Komponenten

$\lambda$  = Ausfallrate

Für  $n = 2$  ergibt mit Gl. 22

$$m_{\text{MPX/ADC, akt. Red.}} = 1,5 \frac{1}{\lambda_{\text{MPX/ADC}}} = 1,5 m_{\text{MPX/ADC}} \quad (24)$$

Für die Serienschaltung von Rechner und MPX/ADC gilt:

$$\frac{1}{m_{\text{s, akt. Red.}}} = \frac{1}{1,5 m_{\text{MPX/ADC}}} + \frac{1}{m_{\text{Rech}}} \quad (25)$$

Nimmt man wieder wie in Abschnitt 3.1.6.1. für MPX/ADC und Rechner die gleichen Ausfallabstände an ( $m_{\text{MPX/ADC}} = m_{\text{Rech}} = m$ ) so erhält man als Ergebnis den Strang-Ausfallabstand:

$$m_{\text{s, akt. Red.}} = 0,6 \cdot m \quad (26)$$

gegenüber

$$m_{\text{s}} = 0,5 \cdot m \quad (27)$$

bei einem einfach aufgebauten Strang. Wegen der quadratischen Abhängigkeit vom Strang-Ausfallabstand  $m_{\text{s}}$  nach Gl. 5, Abschnitt 3.1.6.1. ergibt sich für das aktiv redundante 2von3-System gegenüber dem einfachen 2von3-System bei gleicher Systemreparaturzeit ein Verbesserungsfaktor von

$$\frac{m_{2\text{von}3, \text{ akt. Red.}}}{m_{2\text{von}3}} = \frac{0,6^2}{0,5^2} = 1,44 \quad (28)$$

Mit diesem Faktor kann unter Benutzung des Diagramms in Fig. 15, Abschnitt 3.1.6.1. der mittlere zeitliche Ausfallabstand für ein 2von3-System mit aktiver Redundanz für MPX/ADC entnommen werden.

### 3.3. Polymorphes 2von3-System

Die bisher vorgestellten Systeme haben den Nachteil, daß aufgrund ihrer ungenügenden internen Flexibilität zwischen den Funktionseinheiten MPX/ADC und Rechnern bei einem Defekt keine optimale automatische Systemregeneration möglich ist. Solange man aber diese automatische Systemregeneration nicht in ein Schutzsystem mit Rechnern aufnimmt, nützt man die Möglichkeiten eines Rechners nur teilweise aus.

Eine technische Lösungsmöglichkeit zur Systemregeneration bietet die Polymorphie an. Polymorphie bedeutet in dem vorliegenden Fall, daß jeder Rechner zu jedem MPX/ADC und damit auch beispielsweise zu jedem Thermoelement eines Brennelementes Zugriff hat. Dieses System besitzt damit den Vorteil, daß seine Funktionstüchtigkeit auch bei 2 defekten Strängen erhalten bleibt, sofern der Defekt unterschiedliche Funktionseinheiten betrifft. Dies bedeutet, daß es aufgrund der polymorphen Struktur genügt, wenn beispielsweise 2von3 MPX/ADC und 2von3 Rechner funktionstüchtig sind. Mit diesen Definitionen läßt sich das Ersatzschaltbild in Fig. 19 aufbauen, d. h. die erforderlichen Verzweigungen zwischen MPX/ADC und Rechnern werden symbolisch zur analytischen Behandlung als eine 2von3-Majoritätsentscheidung (Voterebene) dargestellt.

Prinzipiell sollte eine solche Verzweigung nach den Funktionseinheiten eingeschaltet werden, von denen die meisten Fehler zu erwarten sind, sofern man nicht zwischen allen Funktionseinheiten diese Maßnahme ergreifen will. Die Verzweigung nach den MPX/ADC hat den technischen und finanziellen Vorteil, daß sie im Gegensatz zu einer Verzweigung nach den analogen Fühlern auf digitaler Ebene mit optoelektronischen Kopplungsmöglichkeiten stattfindet und eine wesentlich geringere Anzahl von Verbindungen hergestellt werden muß.

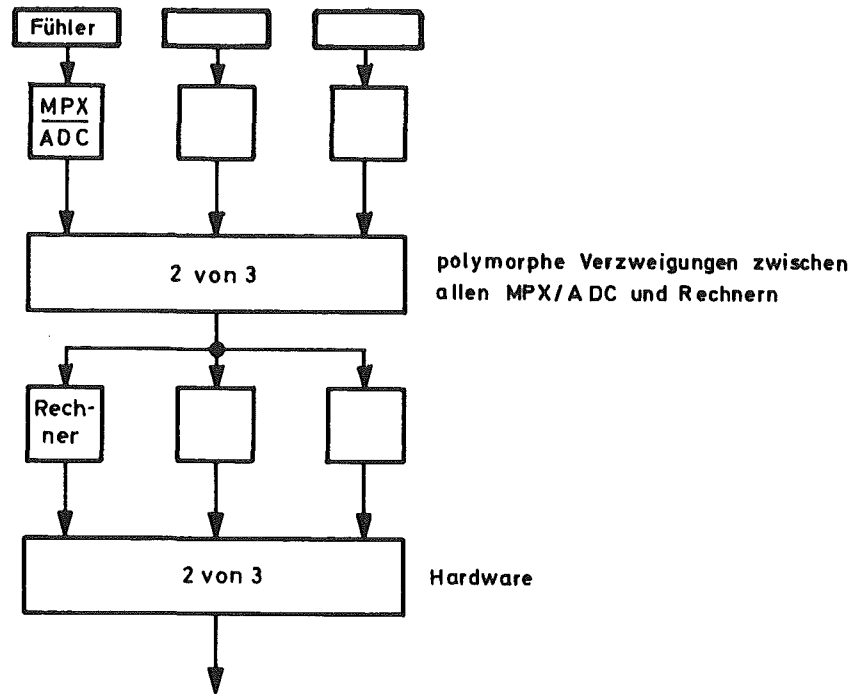


Fig.19 Prinzipielle Darstellung zur Polymorphie zwischen MPX / ADC und Rechner

Unter der Annahme von ausfallsicheren Koppelgliedern und  $Q_{\text{MPX/ADC}} = Q_{\text{Rech}} \ll 1$  gilt für die Nichtverfügbarkeit des polymorphen 2von3-Systems nach Fig. 19

$$Q_{2\text{von}3, \text{ polym.}} = Q_{2\text{von}3 \text{ MPX/ADC}} + Q_{2\text{von}3 \text{ Rech}} \quad (29)$$

Wird für MPX/ADC und Rechner

$$Q_{\text{MPX/ADC}} = Q_{\text{Rech}} = \frac{1}{2} Q \quad (30)$$

gesetzt, so erhält man unter Benutzung von Gl. 11, Abschnitt 3.1.6.1., als Ergebnis

$$Q_{2\text{von}3, \text{ polym.}} = \frac{3}{4} Q^2 + \frac{3}{4} Q^2 = \frac{3}{2} Q^2 \quad (31)$$

Den Verbesserungsfaktor gegenüber dem einfachen 2von3-System nach Abschnitt 3.1.6.1. erhält man bei gleicher Systemreparaturzeit

durch das Verhältnis

$$\frac{Q_{2\text{von}3}}{Q_{2\text{von}3, \text{ polym.}}} = \frac{m_{2\text{von}3, \text{ polym.}}}{m_{2\text{von}3}} = 2 \quad (32)$$

Inwieweit dieser Faktor durch den Mehraufwand an Koppelgliedern gerechtfertigt ist, bedarf einer weiteren Untersuchung. Die Annahme, daß die Nichtverfügbarkeit der für die Polymorphie erforderlichen Koppelglieder für das System vernachlässigbar ist, wurde in neuesten theoretischen Untersuchungen [15] bestätigt. Zu ähnlichen Ergebnissen kommt man durch Überlegungen nach Fig. 20. Darin sind auf der linken Seite die möglichen Kombinationen zwischen MPX/ADC und Rechnern in einem polymorphen 2von3-System dargestellt. Nimmt man an, daß die betreffenden Koppelglieder defekt werden, so lassen sich die auf der rechten Seite dargestellten "Ersatzkopplungen" aufbauen, die bei Polymorphie als Hardware ohnehin vorhanden sind. Damit läßt sich auf Software-Basis eine Koppelglied-Redundanz herstellen, die zumindest aus theoretischer Sicht wegen ihrer 2von2-Charakteristik eine hohe Verfügbarkeit der Koppelglieder für ein polymorphes System sicherstellt.

#### 3.4. Polymorphes 2von3-System mit 4 MPX/ADC

Erweitert man das polymorphe 2von3-System im vorhergehenden Abschnitt aufgrund der 4-fachen Thermoelementbestückung eines Brennelements von 3 auf 4 MPX/ADC, so ergibt sich daraus ein System wie in Fig. 21 dargestellt.

Durch die polymorphe Struktur hat jeder der 3 Rechner aufgrund eines Fehleranalysenprogramms Zugriff zu jedem der 4 MPX/ADC. Damit wird gegenüber den vorhergehenden Systemvarianten eine weitere Verfügbarkeitserhöhung erreicht, denn das System fällt nur aus, wenn 3von4 MPX/ADC und/oder 2von3 Rechner defekt sind.

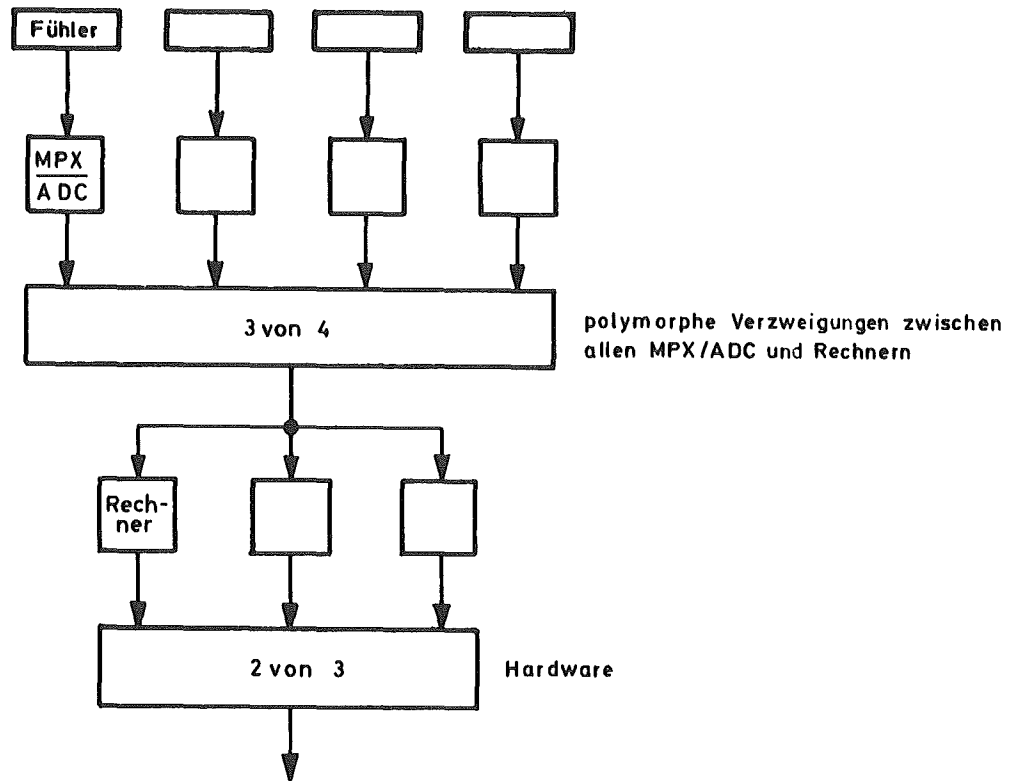


Fig. 21 Polymorphes 2 von 3-System mit 4 MPX / ADC

Unter den gleichen Voraussetzungen wie in Abschnitt 3.3.2. ergibt sich für die Nichtverfügbarkeit des polymorphen 2von3-Systems mit 4 MPX/ADC

$$Q_{2\text{von}3, \text{ polym.}, 4 \text{ MPX/ADC}} = Q_{3\text{von}4\text{-MPX/ADC}} + Q_{2\text{von}3\text{-Rech}} =$$

$$\frac{4}{8} Q^3 + \frac{3}{4} Q^2 = \frac{3}{4} Q^2 \quad (33)$$

Den Verbesserungsfaktor gegenüber dem einfachen 2von3-System nach Abschnitt 3.1.6.1. erhält man bei gleicher Systemreparaturzeit durch das Verhältnis

$$\frac{Q_{2\text{von}3}}{Q_{2\text{von}3, \text{ polym.}, 4 \text{ MPX/ADC}}} = \frac{m_{2\text{von}3, \text{ polym.}, 4 \text{ MPX/ADC}}}{m_{2\text{von}3}} = 4 \quad (34)$$

Mit diesem Faktor kann unter Benutzung des Diagramms in Fig. 15, Abschnitt 3.1.6.1. der mittlere zeitliche Ausfallabstand für ein polymorphes 2von3-System mit 4 MPX/ADC entnommen werden.

### 3.5. 3von4-System

Wenn bereits 4 Thermoelemente je Brennelement und 4 MPX/ADC vorhanden sind, ist die Verwendung eines vierten Rechners naheliegend. Damit ergibt sich aber ein 3von4-System, das wegen seiner hohen Verfügbarkeit auf eine polymorphe Struktur verzichten kann. Daher wird für die nachfolgende Verfügbarkeitsbetrachtung ein einfacher, unverkoppelter Systemaufbau zugrunde gelegt.

Die Nichtverfügbarkeit des 3von4-Systems errechnet sich nach den im Abschnitt 3.1.6.1. bereits angegebenen Gl. 8 und Gl. 10:

$$Q_{3\text{von}4} = 4 \frac{t_r^3}{m_s^3} \quad (35)$$

Werden wieder analoge Voraussetzungen hinsichtlich der Systemreparaturzeit  $t_{r, \text{ syst}}$  wie in Gleichung (12), Abschnitt 3.1.6.1. gemacht, so ergibt sich die Gleichung

$$4 \frac{t_r^3}{m_s^3} = \frac{t_{r, \text{ syst}}}{m_{3\text{von}4}} = \frac{1}{2} \frac{t_r}{m_{3\text{von}4}} \quad (36)$$

Daraus erhält man als Ergebnis den zeitlichen mittleren Ausfallabstand für ein 3von4-System

$$m_{3\text{von}4} = \frac{1}{8} \frac{m_s^3}{t_r^2} \quad (37)$$



Um eine für die Praxis interessierende Vergleichsmöglichkeit gegenüber dem 2von3-System zu haben, wurde vorstehende Gleichung in das Diagramm in Fig. 15 mit einem wesentlich höheren Parameterwert für die Reparaturzeit  $t_r$  übertragen. Durch diese Maßnahme läßt sich beispielsweise folgende praktische Frage beantworten:

Um wieviel größer darf die Reparaturzeit  $t_r$  eines 3von4-Systems gegenüber einem 2von3-System sein, wenn sich für beide Systeme ein gleichgroßer mittlerer zeitlicher Systemausfallabstand  $m_{2von3}$  bzw.  $m_{3von4}$  bei gleichem Strangausfallabstand  $m_s$  ergeben soll?

Diese Frage wird durch die Schnittpunkte in dem angegebenen Diagramm beantwortet. Beispielsweise erkennt man, daß die Reparaturzeit für ein 3von4-System um den Faktor 20 gegenüber einem 2von3-System größer sein darf, sofern ein Strang-Ausfallabstand  $m_s$  von ca. 1000 h vorausgesetzt wird.

Um auf der Basis gleicher Systemreparaturzeit wie in den vorhergehenden Abschnitten das 3von4-System mit dem 2von3-System zu vergleichen, wird wieder das Verhältnis gebildet:

$$\frac{m_{3von4}}{m_{2von3}} = \frac{3}{4} \frac{m_s}{t_r} = \frac{3}{4} \cdot \frac{1}{Q_s} \quad (38)$$

Hier ist der Verbesserungsfaktor nicht konstant. Er ist abhängig von der Strang-Nichtverfügbarkeit und relativ groß. Beispielsweise ist bei einer Reparaturzeit  $t_r = 2$  h und einem mittleren Ausfallabstand  $m_s = 1000$  h die Strang-Nichtverfügbarkeit

$$Q_s = \frac{t_r}{m_s} = \frac{2 \text{ h}}{1000 \text{ h}} = 2 \cdot 10^{-3} \quad (39)$$

Somit ist der Verbesserungsfaktor:

$$\frac{m_{3von4}}{m_{2von3}} = \frac{3}{4} \cdot \frac{1}{2 \cdot 10^{-3}} \approx 400 \quad (40)$$

#### 4. Diskussion der Lösungsvorschläge

Die aufgezeigten Systemvariationen unterscheiden sich durch erhebliche Vor- und Nachteile. Die folgende Tabelle vermittelt einen Überblick über die abgeschätzten, auf ein 2von3-System normierten zeitlichen Ausfallabstände.

Tabelle 6: Ausfallabstände verschiedener Systeme

System	Verbesserungsfaktor für den zeitlich mittleren Ausfallabstand $m_{2von3}$
2von3	$1 \cdot m_{2von3}$
2von3, akt. Redundanz durch 4. MPX/ADC	$1,44 \cdot m_{2von3}$
2von3, polymorph	$2 \cdot m_{2von3}$
2von3, polymorph mit 4 MPX/ADC	$4 \cdot m_{2von3}$
3von4	$\frac{3}{4} \cdot \frac{1}{Q_s} \cdot m_{2von3}$

Falls man den praktikablen Grundsatz "so einfach wie zulässig" verfolgt, dürfte das 2von3-System im Vordergrund des Interesses stehen. Für konventionelle Schutzsysteme hat es sich vielfach bewährt. Ob es sich auch für ein Schutzsystem mit Rechnern eignet, sollte man erst entscheiden, wenn zuverlässige MTBF-Daten der vorgesehenen Komponenten vorliegen und die Frage von sofort einsatzbereiten Ersatzkomponenten sowie die Organisation einer Reparatur innerhalb weniger Stunden geklärt ist.

Diese Faktoren bestimmen wesentlich den Systemausfallabstand. Sie sollten - falls sie von Industrieseite nicht vorliegen - durch eigene experimentelle Untersuchungen frühzeitig ermittelt werden, soweit der statistische Charakter der Ausfalldaten dies in der

zur Verfügung stehenden Zeitspanne zuläßt. Auf der Grundlage der derzeitigen Komponenten-Verfügbarkeitsdaten läßt sich vorhersagen, daß bei einem 2von3-System der zeitlich mittlere Ausfallabstand  $m_{2von3}$  ca. 9,5 Jahre beträgt (siehe Diagramm in Fig. 15, Abschnitt 3.1.6.1.). Dabei sind die deterministischen Fehler nicht berücksichtigt.

Der Vorteil des 2von3-Systems mit aktiver Redundanz durch einen 4. MPX/ADC liegt nicht so sehr in dem Verbesserungsfaktor 1,44. Er liegt viel mehr in einer schnellen automatischen Umschaltung eines Ersatzthermoelementes und/oder Ersatz-MPX/ADC im Falle eines Defektes. Bedenkt man bei der Vielzahl der Thermoelemente einen manuellen Eingriff während des Reaktorbetriebes in einen sicherlich umfangreichen Kreuzschienenverteiler eines Schutzsystems, so ist die Gefahr einer Fehlschaltung nicht zu unterschätzen. Bedeutungsvoll ist auch die kurze "Reparaturzeit" von ca. 1 bis 2 s bei einer automatischen Umschaltung gegenüber ca. 1 h bei einer manuellen Umschaltung. Bei dem heutigen Stand der Technik müßte es möglich sein, einen für diese Systemvariante rückwirkungsfreien und weitgehend ausfallsicheren Umschalter einzusetzen.

Die polymorphen Systemvarianten 2von3 bzw. 2von3 mit 4 MPX/ADC zeigen zumindest von der theoretischen Seite relativ gute Verbesserungsfaktoren. Allerdings ergibt sich die Frage, mit welchem Aufwand an Soft- und Hardware dieser Vorteil erkauft werden muß. Der Aufwand an rückwirkungsfreier polymorpher Koppel elektronik für eine Wortlänge von 12 bit bei ca. 1000 Adressen zwischen MPX/ADC und den Rechnern ist sicherlich beträchtlich. Ebenso darf die Belastung des Programms durch die Berücksichtigung der polymorphen Systemstruktur nicht unterschätzt werden.

Entwicklungstendenzen in Richtung Polymorphie sind nicht neu [16]; sie sind allerdings mehr auf einen modularen Aufbau innerhalb des Rechners ausgerichtet. Da es diese Rechner noch nicht gibt, verfolgt dieser Bericht mehr einen polymorphen Systemaufbau zwischen mehreren Rechnern und MPX/ADC's.

Um gegenüber einem einfachen 2von3-System zu einer höheren Verfügbarkeit zu kommen, zeigen beide Wege interessante Möglichkeiten, die man nicht außer acht lassen sollte. Jedoch kann für diese Systemvarianten eigentlich erst eine praktische Erprobung ein abschließendes Urteil bilden.

Vor den aufgezeigten Systemvariationen zeigt natürlich das 3von4-System die interessanteste Verfügbarkeitserhöhung gegenüber einem 2von3-System. Falls man wegen ungenügender Verfügbarkeit des 2von3-Systems zu einem höheren System übergehen sollte, bietet das 3von4-System erhebliche Vorteile:

- a) Setzt man aufgrund der vierfachen Thermoelementbestückung in einem Brennelement 4 MPX/ADC voraus, so wird zusätzlich nur noch ein Rechner benötigt. Dafür entfällt die relativ aufwendige Koppелеlektronik für Polymorphie bzw. Umschalter für den 4. MPX/ADC. Das System wird einfacher und übersichtlicher im Aufbau und somit reparaturfreundlicher.
- b) Gegenüber einem 2von3-System erreicht man bei gleicher Reparaturzeit eine Verlängerung des Systemausfallabstandes um zwei bis drei Größenordnungen oder bei gleichen Systemausfallabständen eine beispielsweise zwanzigfache höhere zulässige Reparaturzeit, was praktisch mehrere Tage bedeutet. In dieser Zeit könnte aber eine echte Reparatur vom Gerätehersteller ausgeführt werden, so daß man auf betriebsbereite Ersatzteile vom Umfange eines Stranges verzichten könnte. Damit würden sich gegenüber einem 2von3-System mit entsprechenden Ersatzteilen keine höheren Kosten ergeben. Ohnehin wäre noch die Frage zu klären, wie und wo die Ersatzteile während der Lagerzeit geprüft werden. Somit wäre das 3von4-System gerätemäßig auf ein 2von3-System zurückgeführt, bei welchem die Ersatzteile als 4. Strang mit in Betrieb sind. Man erspart sich bei gleichem Geräteaufwand die externe Prüfung der Ersatzteile und erzielt eine erhebliche Verfügbarkeitsverbesserung.

- c) Fallen gleichzeitig oder nacheinander zwei unterschiedliche Funktionsgruppen in zwei Strängen aus, so kann durch kurzfristigen manuellen Austausch ohne Reserve ein vollwertiges 2von3-System hergestellt werden. Dies stellt eine "manuell herstellbare Polymorphie" ohne Verkopplung dar<sup>\*)</sup>. Nachstehend ist ein Beispiel ausgeführt und in Fig. 22 dargestellt:

Zuerst wird der MPX/ADC in Strang 1 defekt. Er wird zur Reparatur herausgenommen. Es bleibt ein 2von3-System übrig. Die Reparatur ist noch nicht beendet und in Strang 2 wird der Rechner defekt. Er wird zur Reparatur herausgenommen. Es bleibt ein 1von2-System übrig. Nun kann sofort der Rechner von Strang 1 manuell in die Position des defekten Rechners in Strang 2 gebracht werden. Es ist wieder ein 2von3-System vorhanden.

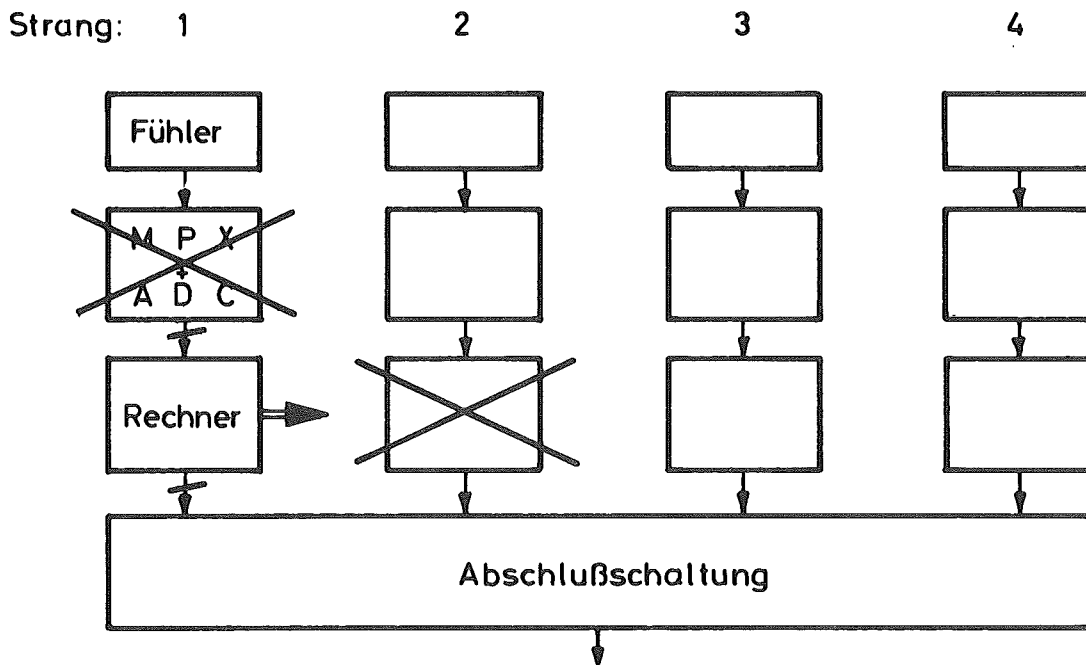


Fig.22    Manuelle Polymorphie in einem 3 v.4-System

<sup>\*)</sup> Bei einem 2von3-System ist wegen der vorgeschriebenen Systemreaktionszeit von 1,5 sec nur eine "automatisch herstellbare Polymorphie" möglich, die aber Strangverkopplungen zur Folge hat.

Als Nachteile des 3von4-Systems werden angeführt:

- erweiterte Verkopplungen für Synchronisation und für eventuellen Strangvergleich
- erweiterte Abschlußschaltung gegenüber 2von3-System, da doppelte Zahl an UND-Logikelementen
- Durchsatzmesser benötigen einen 4. galvanisch getrennten und rückwirkungsfreien Ausgang
- erhöhte Verkabelung

## 5. Literatur

- [1] Schrüfer, E.  
Vorschläge zur Auslegung von Reaktorschutzsystemen,  
atomwirtschaft 15 (1970) S. 185 - 188
  
- [2] Hanauer, S. H., et al.  
Design Principles of Reactor Protection Instrument Systems,  
ORNL-NSIC-51
  
- [3] Smidt, D.  
Reaktortechnik, Karlsruhe  
G. Braun, 1971, 534 S.
  
- [4] Gast, K. und Schlechtendahl, E. G.  
Schneller Natriumgekühlter Reaktor Na2,  
KFK 660, 1967
  
- [5] Judd, A. M.  
Boiling and Condensation of Sodium in Relation to Fast  
Reactor Safety,  
Intern. Conf. on the Safety of Fast Reactors, Aix-en-  
Provence, 1967
  
- [6] Gast, K.  
Die Ausbreitung örtlicher Störungen im Kern Schneller  
Natriumgekühlter Reaktoren und ihre Bedeutung für die  
Reaktorsicherheit  
KFK 1380, 1971
  
- [7] Birkhofer, A. et al.  
Reactor Safety in the Federal Republic of Germany,  
AED-Conf-71-100-006, Genf, 1971

- [8] Steinbuch, K.  
Taschenbuch der Nachrichtenverarbeitung,  
Springer Verlag, 1962, 1521 S.
- [9] Köhler, B.  
Anforderungen, die an Prozeßrechner in Kernenergie-  
anlagen zu stellen sind.  
Institut für Meß- und Regelungstechnik, Prof. Dr. Merz,  
München, MRR 84, Nov. 70
- [10] Hück, A.  
Größere Sicherheit bei Betriebsstörung - Elektronische Schaltung  
zur Stromversorgung für Haltemagnete der Abschaltstäbe eines  
Reaktors  
Hartmann & Braun-Meßwerte 2
- [11] Kaltenecker, H.  
Auswahlssysteme zur Erhöhung der Sicherheit von Signalen,  
Regelungstechnik, 6, 93 (1958)
- [12] Dombrowski, E.  
Einführung in die Zuverlässigkeit elektronischer Geräte  
und Systeme, AEG-Telefunken, 1970, 368 S.
- [13] Caldarola, L., Weber, G.  
General criteria to optimize the operation of a power-plant  
with special consideration to it's safety requirements  
KFK 640, EUR 3685a
- [14] Murchland, J. D., Weber, G. G.  
A Moment Method for the Calculation of a Confidence  
Intervall for the Failure Probability of a System  
(1972) Symposium on Reliability, San Francisco)



- [15] Schneeweis, W.  
Zuverlässigkeit von mehrfach intern verkoppelten Dreier-  
systemen, von denen zwei als Ersatz dienen  
AEÜ, Band 25 (1971)
- [16] Basten, R. G.  
Brosch 2294 - application of on-line computers to nuclear  
reactors  
Sandefjord, Norway, September 1968

## 6. Verzeichnis der Abbildungen

- Fig. 1        Integrale und lokale Daten im MISS-SNR
- Fig. 2        Organisatorischer Aufbau der Fühler
- Fig. 3        Temperaturgrenzwerte in Abhängigkeit der Brennelementleistung  $P_i$
- Fig. 4        Durchsatzgrenzwerte in Abhängigkeit der Brennelementleistung  $P_i$
- Fig. 5        Abschaltbedingungen - Variante 1
- Fig. 6        Abschaltbedingungen - Variante 2
- Fig. 7        Abschaltbedingungen - Variante 3
- Fig. 8        Prinzipieller MISS-SNR-Aufbau unter Berücksichtigung seiner Peripherie
- Fig. 9        MISS-SNR-Blockschaltbild der 2von3-Version
- Fig. 10       Zeitlicher Ablauf
- Fig. 11       Synchronisierschaltung
- Fig. 12       Thermoelement-Isolationsmessungen
- Fig. 13.1.    Speicherplatzabschätzung für das MISS-SNR
- Fig. 13.2.    Speicherplatzabschätzung für das MISS-SNR
- Fig. 14       Abschlußschaltung für das MISS-SNR

- Fig. 15      Zeitlich mittlere Systemausfallabstände  $m_{2\text{von}3}$  und  $m_{3\text{von}4}$  in Abhängigkeit des Strangausfallabstandes  $m_s$  unter Berücksichtigung verschiedener Reparaturzeiten  $t_r$
- Fig. 16      Serienschaltung von Voterelementen
- Fig. 17      Ausfallabschätzung der Abschlußschaltung bei nur einer Voterebene
- Fig. 18      Teilweise, aktive Strangredundanz durch 4. MPX/ADC
- Fig. 19      Prinzipielle Darstellung zur Polymorphie zwischen MPX/ADC und Rechner
- Fig. 20      Koppelglied-Redundanz durch Kombinatorik in einem polymorphen 2von3-System ohne Mehraufwand an Hardware
- Fig. 21      Polymorphes 2von3-System mit MPX/ADC
- Fig. 22      Manuelle Polymorphie in einem 3von4-System



Brennelement

Strang

GW (T) überschritten

TE defekt

GW (Q) unterschritten

Q-messer defekt

GW (QN) überschritten


Abschalt-signal

Scram-signal

Es gibt insgesamt 501 Abschalt-  
bedingungen für lokale Größen

m = Brennelement der Spaltzone

n = Brennelement der Brutzone

 = ODER

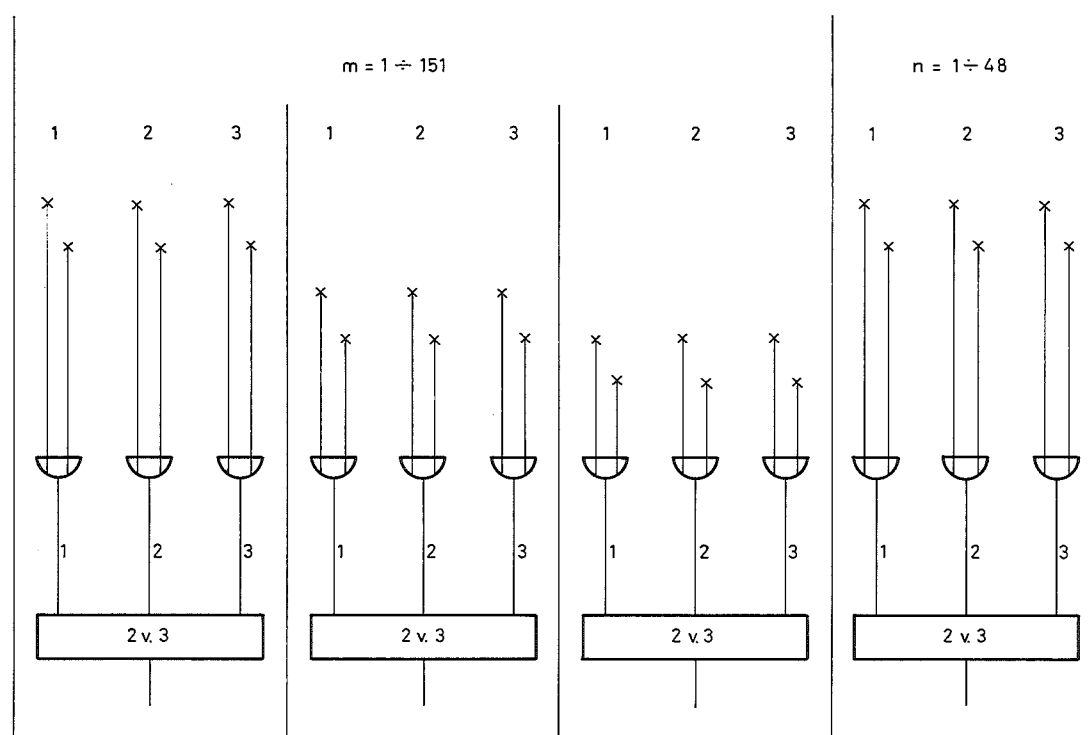


Fig. 5 Abschaltbedingungen -Variante 1



Brennelement

Strang

GW (T) überschritten

TE defekt

GW (T) des 1. Nachbarelementes  
überschritten oder TE defekt

GW (T) des 2. Nachbarelementes  
überschritten oder TE defekt

GW (T) des 6. Nachbarelementes  
überschritten oder TE defekt

GW (Q) unterschritten

Q-messer defekt

GW(QN) überschritten

Abschaltsignal

Scramsignal

m = Brennelement der Spaltzone  
n = Brennelement der Brutzone

 = ODER     = UND

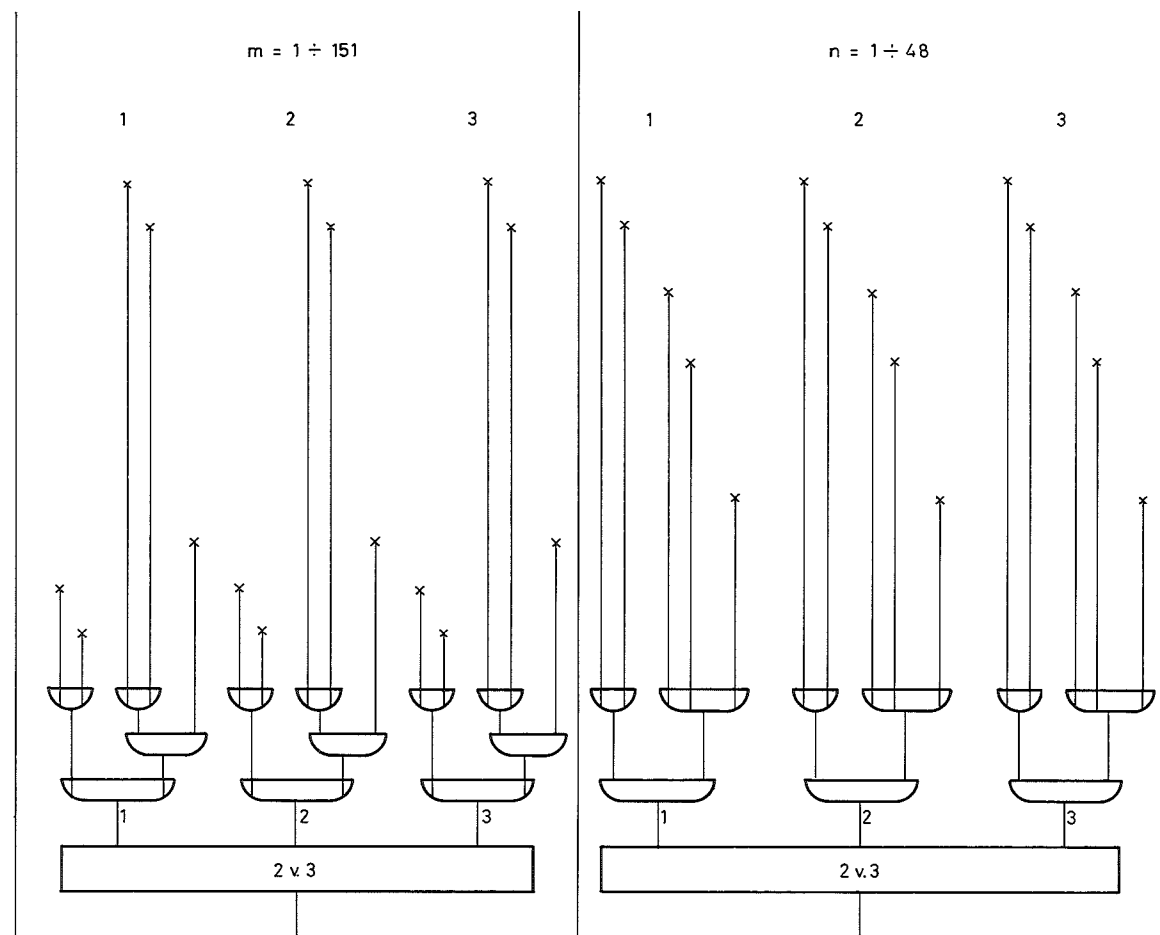


Fig.6                      Abschaltbedingungen - Variante 2

Brennelement

Strang

GW (T) überschritten

TE defekt

GW (T) des 1. Nachbarelementes  
überschritten oder TE defekt

GW (T) des 2. Nachbarelementes  
überschritten oder TE defekt

GW (T) des 3. Nachbarelementes  
überschritten oder TE defekt

GW (T) des 6. Nachbarelementes  
überschritten oder TE defekt

GW (Q) unterschritten

Q-messer defekt



GW (QN) überschritten

Abschaltsignal

Scramsignal

m = Brennelement der Spaltzone

n = Brennelement der Brutzone

 = ODER  = UND

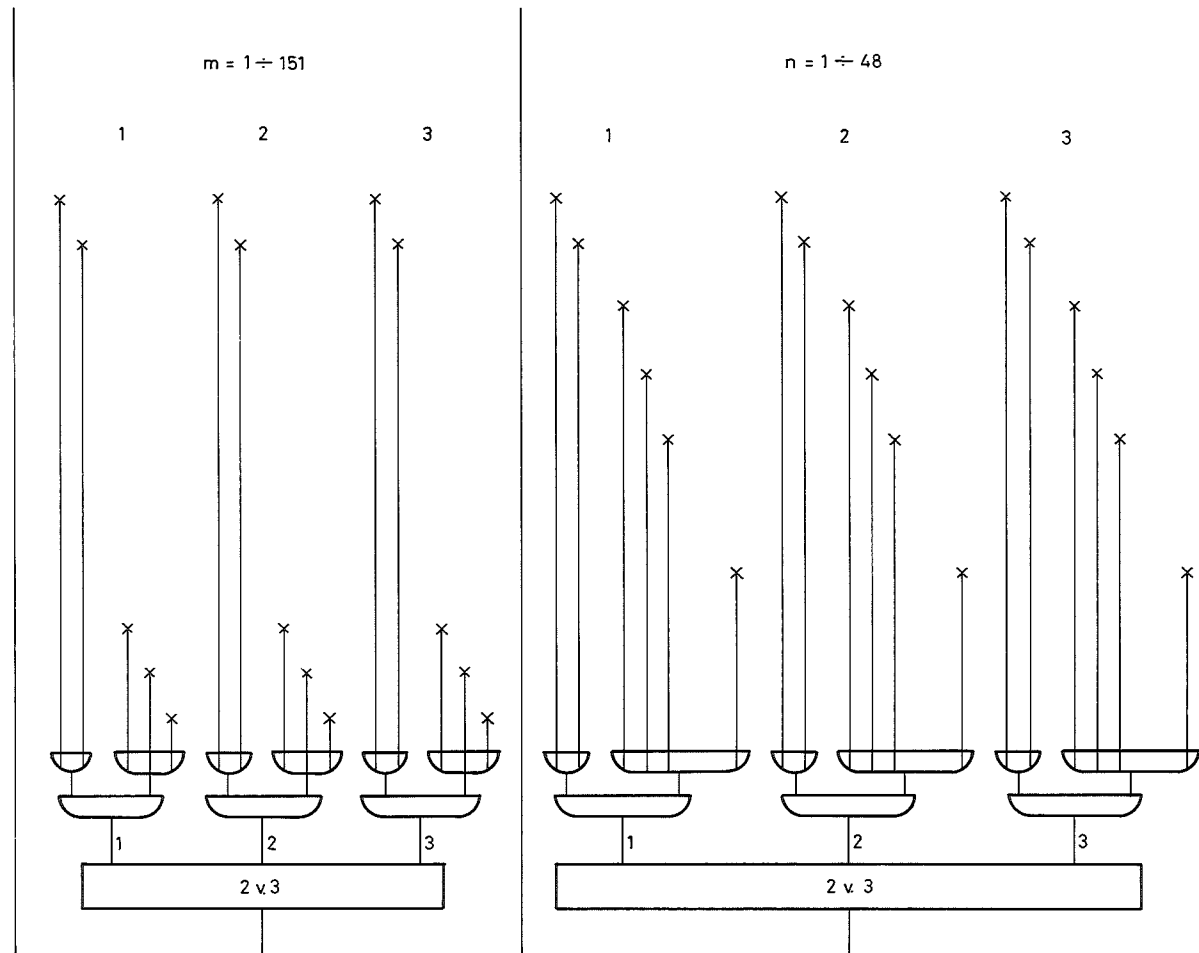


Fig. 7 Abschaltbedingungen - Variante 3



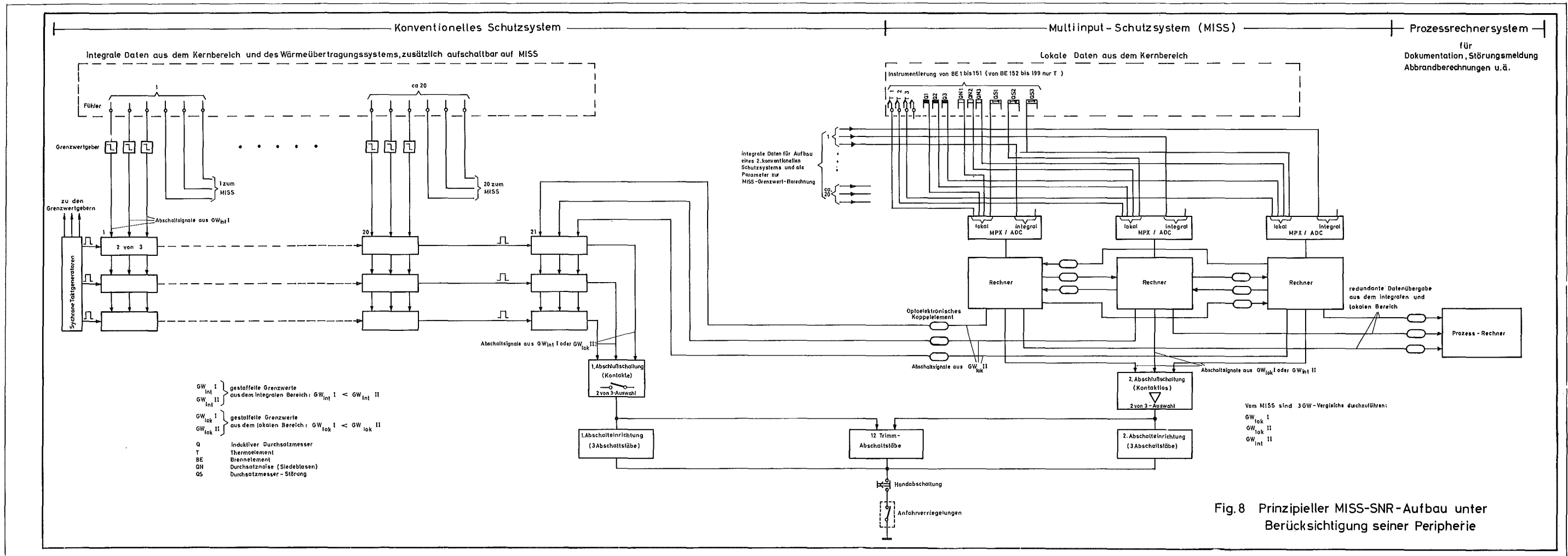


Fig. 8 Prinzipieller MISS-SNR-Aufbau unter Berücksichtigung seiner Peripherie



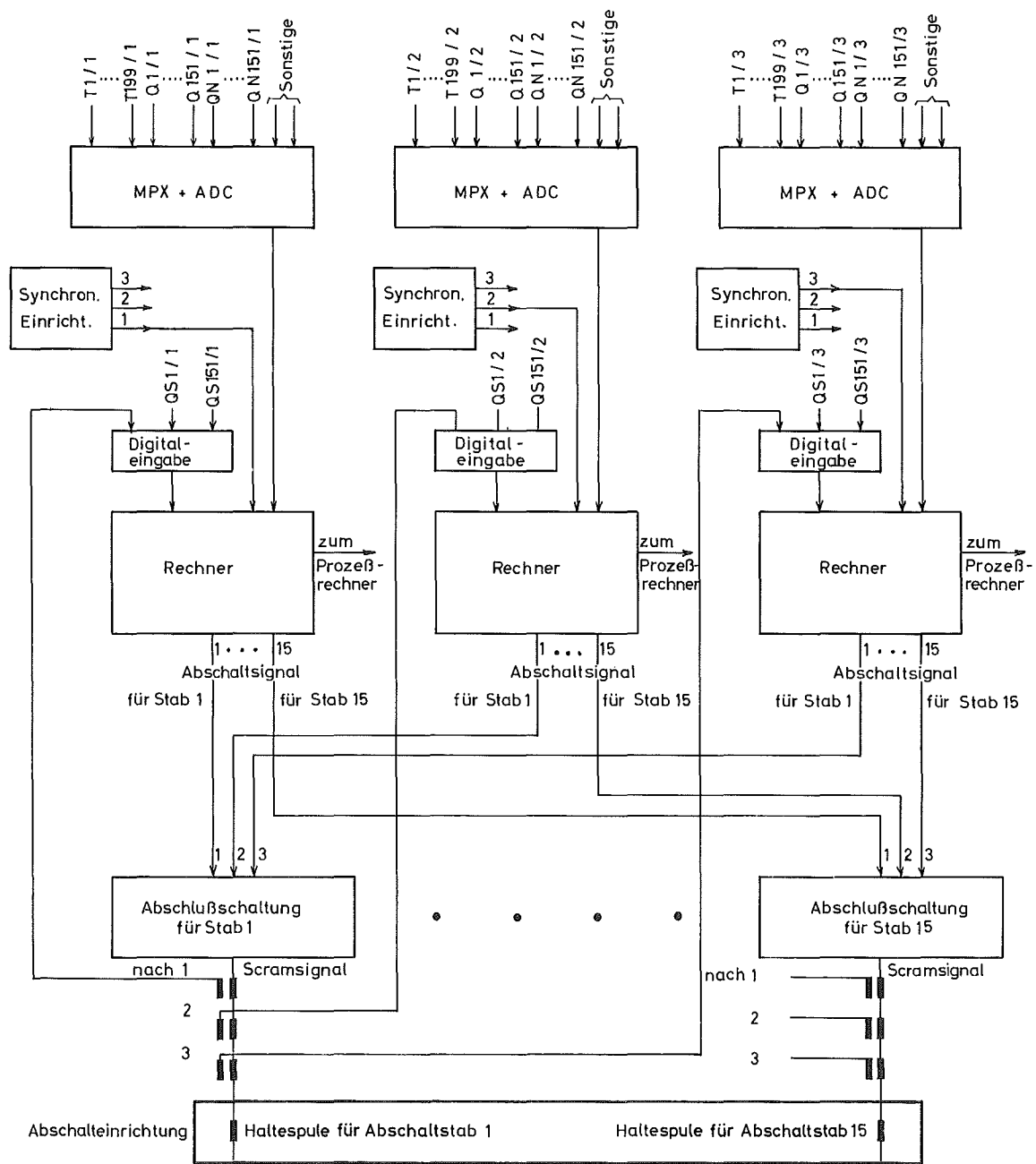


Fig.9 MISS - SNR-Blockschaltbild der 2 von 3-Version

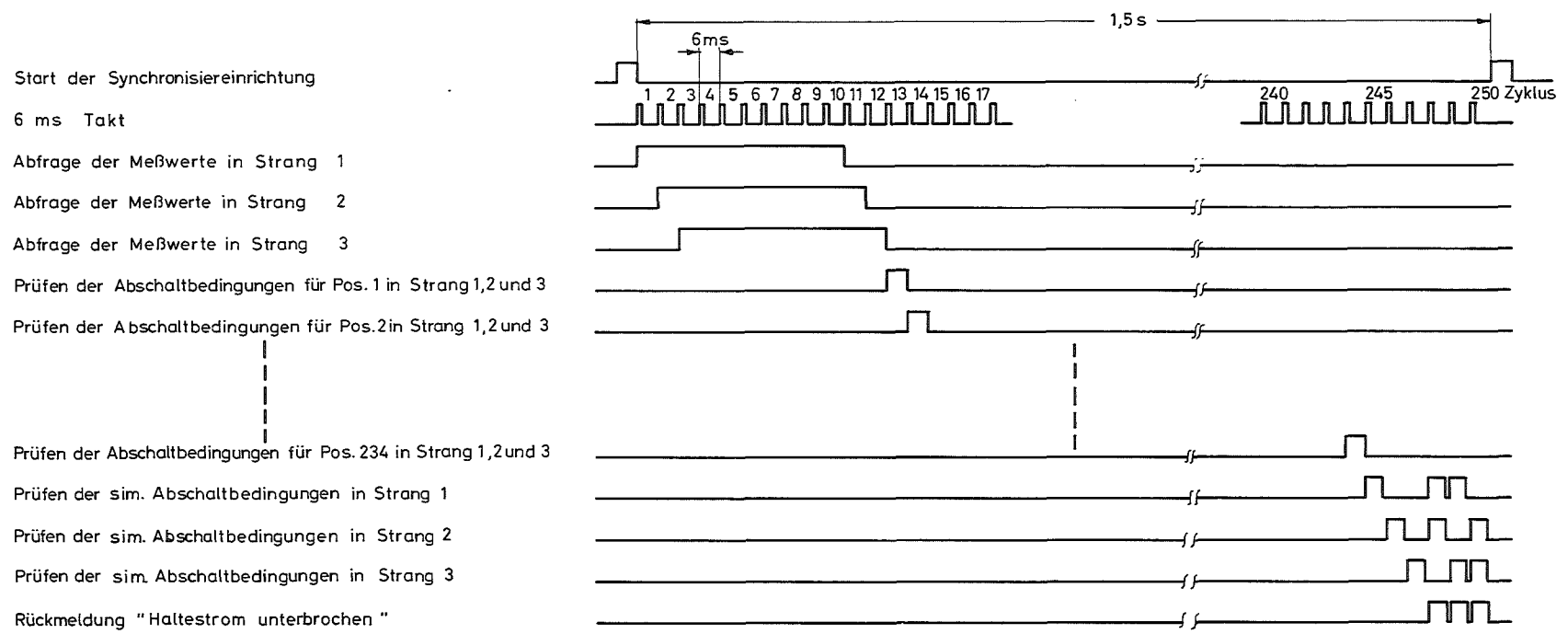


Fig. 10 Zeitlicher Ablauf



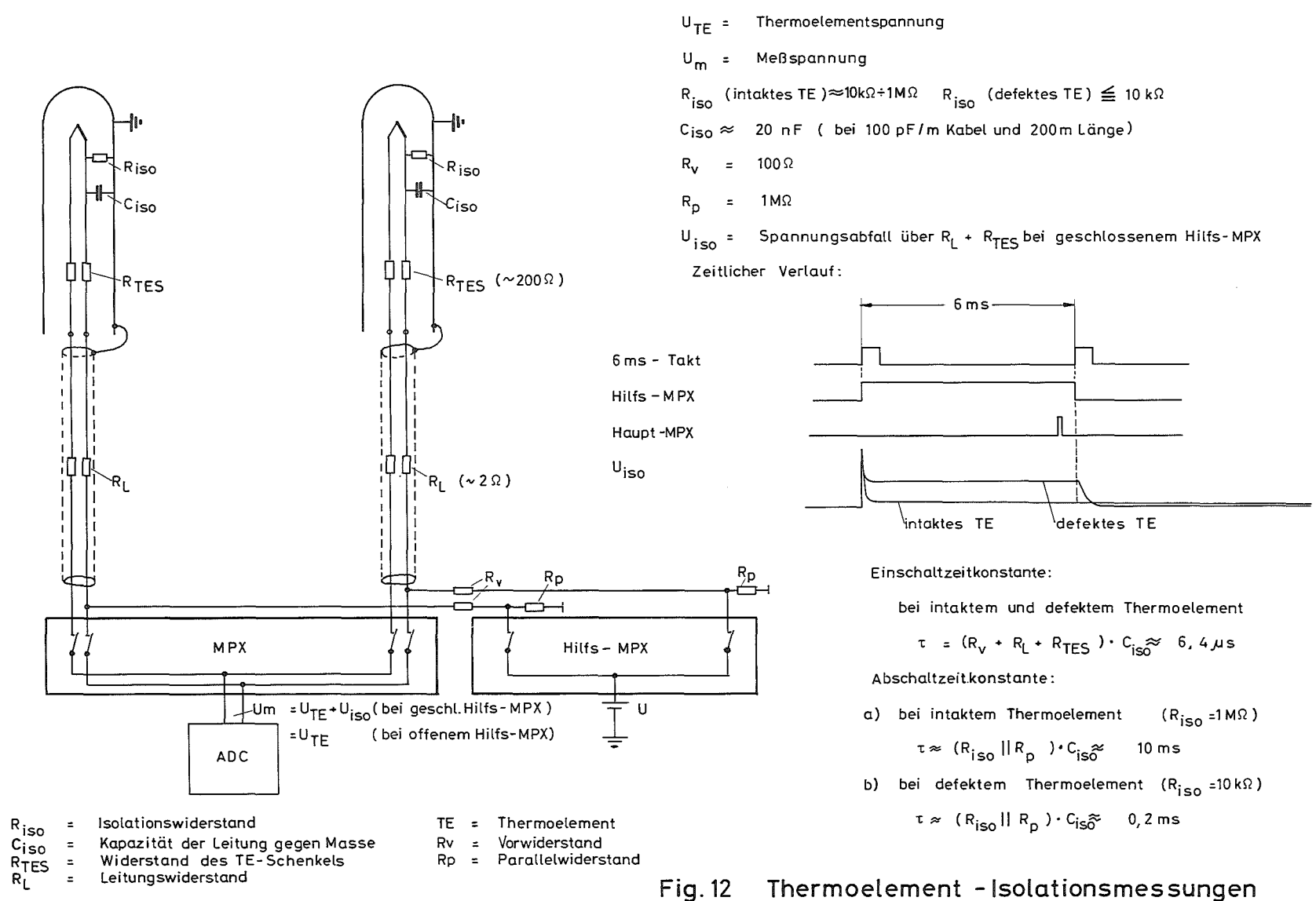


Fig. 12 Thermoelement - Isolationsmessungen

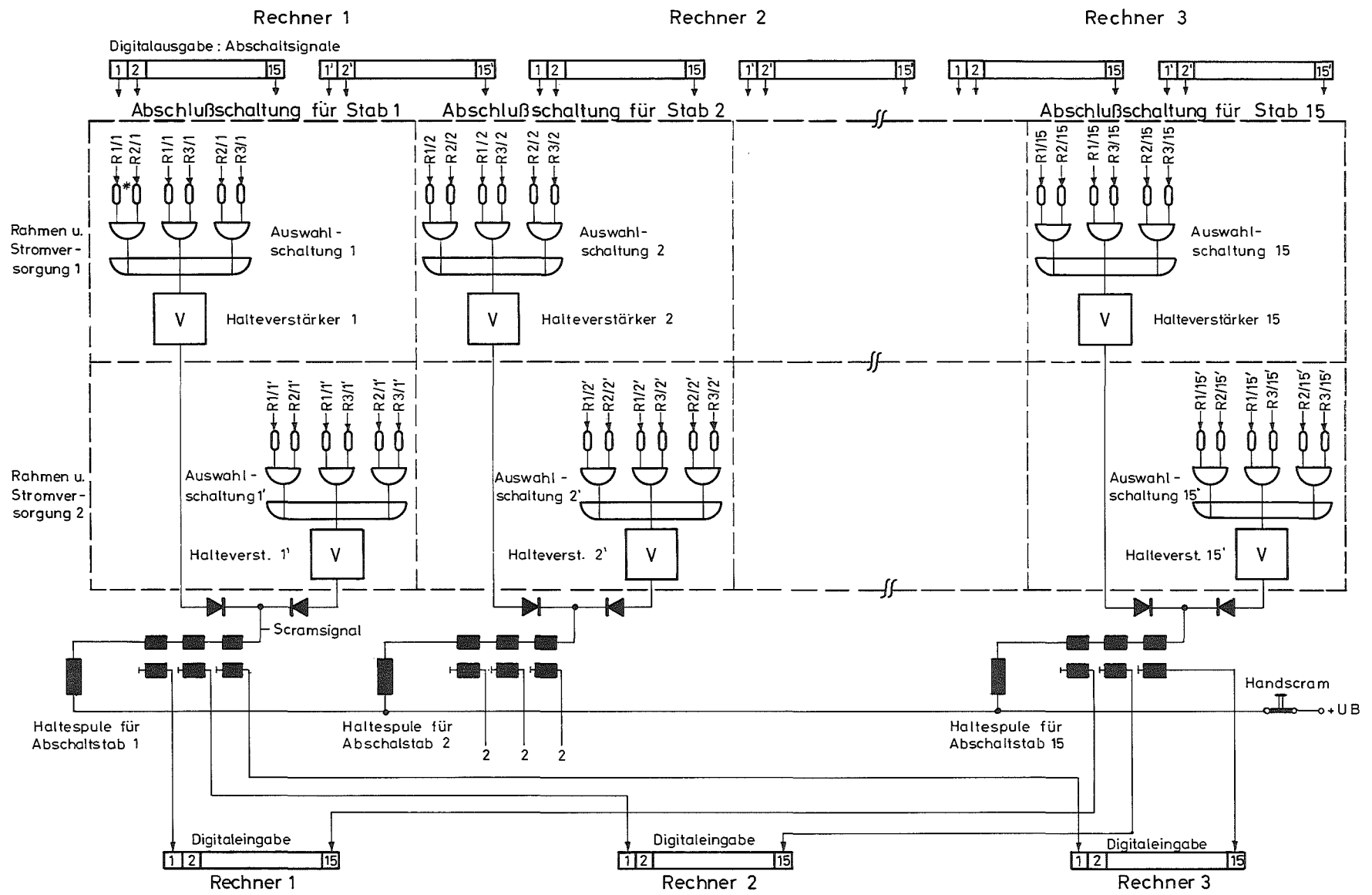


Fig.14 Abschlußschaltung für das MISS-SNR

\*) 0 = optoelektronische Koppellemente

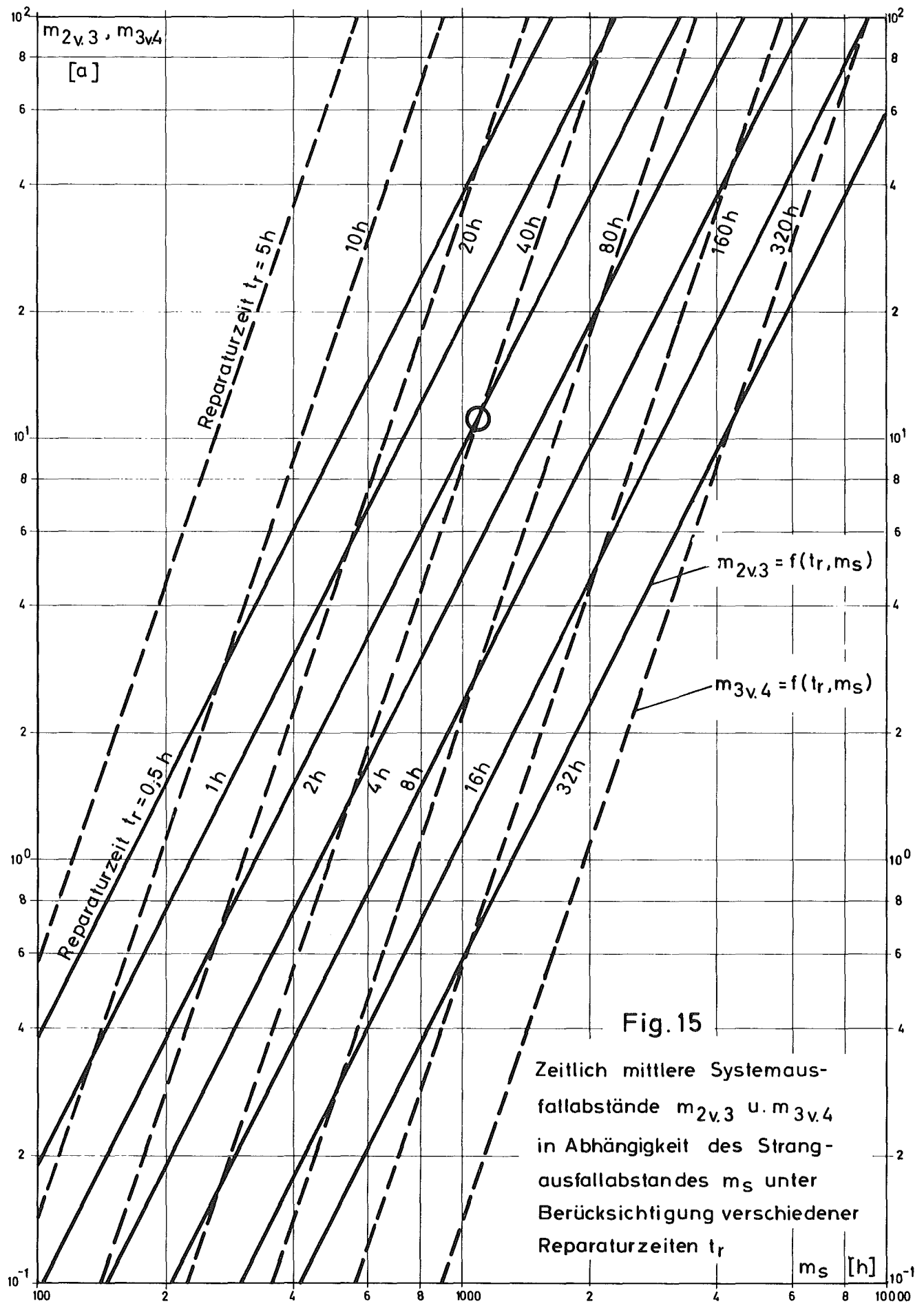


Fig. 15

Zeitlich mittlere Systemausfallabstände  $m_{2v,3}$  u.  $m_{3v,4}$  in Abhängigkeit des Strangausfallabstandes  $m_s$  unter Berücksichtigung verschiedener Reparaturzeiten  $t_r$

$m_s$  [h]



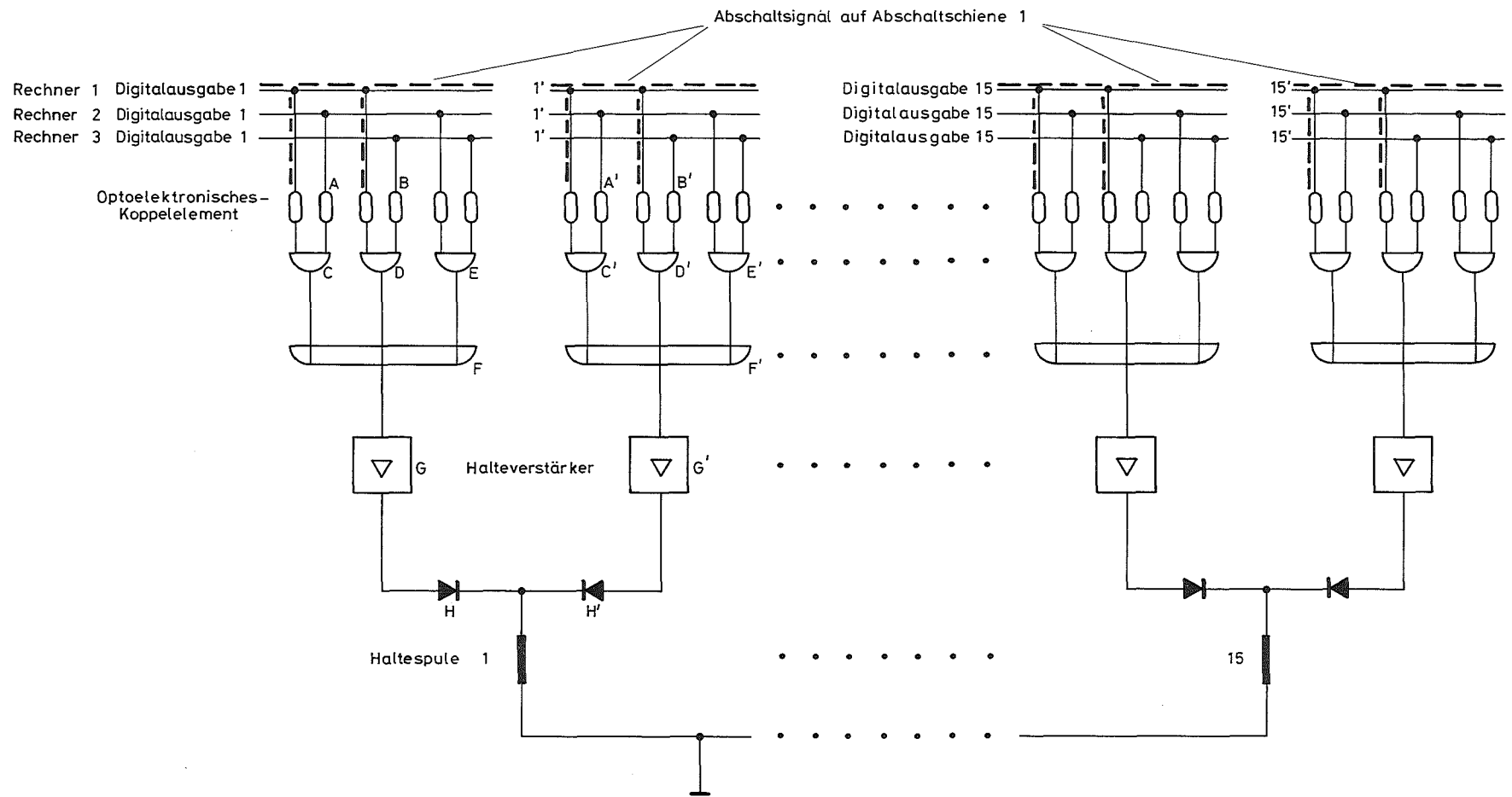


Fig. 17 Ausfallabschätzung der Abschlußschaltung bei nur einer Voterebene

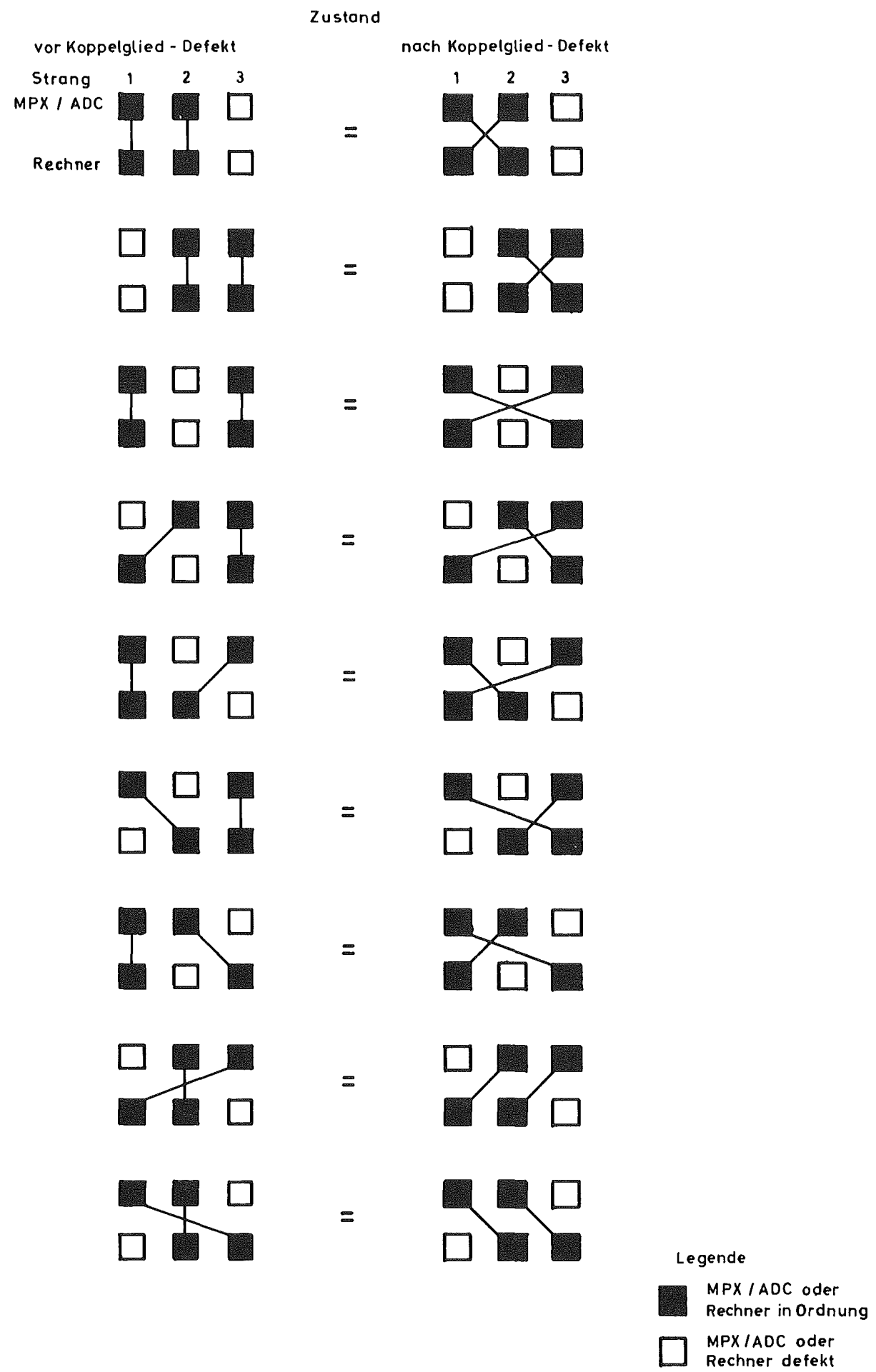


Fig. 20 Koppelglied-Redundanz durch Kombinatorik in einem polymorphen 2 von 3-System ohne Mehraufwand an Hardware.