Gesellschaft für
Reaktorsicherheit (GRS) mbH

GRS-Bericht

Sicherheitstechnischer Vergleich eines festverdrahteten dynamischen Reaktorschutzsystems mit einem Rechnerschutzsystem

Teil 2

W.-E. Büttner

GRS-9 (März 1978)

Gesellschaft für Reaktorsicherheit (GRS) mbH

GRS-Bericht

Sicherheitstechnischer Vergleich eines festverdrahteten dynamischen Reaktorschutzsystems mit einem Rechnerschutzsystem

Teil 2

Wolf-Ewald Büttner

GRS-9 (März 1978)

Glockengasse 2 · 5000 Köln 1 · Telefon (02 21) 20 68–1 · Telex 8 881 807 grs d

Dieser Bericht ist der 2. Teil des Vergleichs zweier verschiedener Reaktorschutzkonzepte. Der 1. Teil erschien unter dem Titel: W.-E. Büttner, Sicherheitstechnischer Vergleich eines festverdrahteten dynamischen Reaktorschutzsystems mit einem Rechnerschutzsystem (Teil 1), MRR 161, Juli 1976

KURZFASSUNG

In der vorgelegten Untersuchung wird ein konventionelles festverdrahtetes dynamisches Reaktorschutzsystem einem Rechnerschutzsystem gegenübergestellt. Während im Teil 1 /1/ unter Berücksichtigung der eindeutig sicherheitsgerichteten Schutzaktionen für beide Systeme die mittlere Nichtverfügbarkeit bestimmt wurde, befaßt sich dieser zweite Teil mit den nicht eindeutig sicherheitsgerichteten Schutzaktionen. Für beide Systeme wird die Fehlauslösungswahrscheinlichkeit, das ist die Wahrscheinlichkeit der fälschlichen Auslösung einer oder mehrerer Schutzaktionen infolge von Fehlern, bestimmt. Beim Rechnerschutzsystem werden auch einige nicht eindeutig sicherheitsgerichtete Schutzaktionen über Arbeitsstrom-Anregungen ausgelöst. Da diese bei einem Ausfall des Schutzsystems im Falle einer Anforderung blokkiert sind, wird für sie die mittlere Nichtverfügbarkeit ermittelt. In einer Gegenüberstellung sind die Vor- und Nachteile der beiden Systeme aufgezeigt.

ABSTRACT

The investigation presented here compares a conventional hard-wired dynamic reactor protection system with a computerized alternative. Whereas in part 1 /1/ the mean unavailability in case of a demand is determined for distinctly safety-oriented protection actions, part 2 takes into consideration protection actions which are not distinctly safety-oriented. For both systems the spurious trip probability is determined, i.e. the probability of a false release of one or more protection actions due to failures. The mean unavailability is also determined for those not distinctly safety-oriented protection actions of the computerized protection system which are released via the open circuit current principle. This is because system breakdowns prevent the release of those protection actions in case of demand. The advantages and disadvantages of either type of system are viewed against each other.

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

FORMELABKÜRZUNGSVERZEICHNIS

a_i	Wurzeln des quadratischen bzw. kubischen Polynoms des Nenners
b_i	Wurzeln des quadratischen bzw. kubischen Polynoms des Nenners
ε	Fehlererkennungsrate
λ	Ausfallrate
μ	Reparaturrate
MTBF	Mittlere Zeit bis zum Ausfall
MTTR	Mittlere Zeit für die Instandsetzung
$\overline{\text{MTTR}}$	Mittlere Länge des Anteils der MTTR für einen Kanal bis zum Ausfall eines zweiten Kanals
n	Anzahl der Kanalgruppen
P_i	Wahrscheinlichkeit des Systemzustands i
p	Fehlauslösungswahrscheinlichkeit, Versagenswahrscheinlichkeit
R	Zuverlässigkeit
s	Variablenbezeichnung im Laplace-Raum
t	Zeit
τ	Mittlere Zeit für die Instandsetzung
$\bar{u}$	Mittlere Nichtverfügbarkeit
2v3	2v3-Wertungsschaltung bzw. 2v3-System

Berichtigung für MRR 161

An dieser Stelle sei noch die Berichtigung eines Schreibfehlers der Gleichung (13) im Teil 1 angebracht. (Die ermittelten Ergebnisse werden davon nicht berührt.) Es heißt dort

$$0 \leq p \leq \frac{(m+1)\,a}{(m+1)\,a+n-m}$$

mit $a = \nu_{p\%}^{(2m+2,2n-m)}$. Letzter Ausdruck muß richtig lauten

$$a = \nu_{p\%}^{(2m+2,2n-2m)}.$$

1. EINLEITUNG

Der Vergleich erfolgt wieder, wie bereits in Teil 1 /1/, anhand des festverdrahteten dynamischen Reaktorschutzsystems mit Simatic-Bausteinen, wie es z.B. im Kernkraftwerk Isar eingesetzt ist, und des Reaktorschutzsystems mit Prozeßrechnern AEG 60-10, wie es versuchsweise in Brunsbüttel parallel zu einem konventionellen Schutzsystem ohne Eingriffsmöglichkeit in den Reaktorschutz (open loop) eingesetzt ist.

Während der erste Teil dieses Berichtes /1/ sich nur mit eindeutig sicherheitsgerichteten Schutzaktionen befaßte, sollen in diesem zweiten Teil die nicht eindeutig sicherheitsgerichteten Schutzaktionen berücksichtigt werden. Es wird vorwiegend der Fall behandelt, daß infolge eines Fehlers eine Schutzaktion fehlausgelöst wird. Fehler, die eine Schutzaktion im Anforderungsfall blockieren, wurden mit Ausnahme der Arbeitsstromschutzanregungen (siehe dazu Kap. 3.3, 3.4 und 3.5) bereits im Teil 1 betrachtet. Die dort ermittelten mittleren Nichtverfügbarkeiten gelten, mit Ausnahme bei Arbeitsstrom-Schutzanregungen, auch für die nicht eindeutig sicherheitsgerichteten Schutzaktionen.

In den Vergleich werden wiederum nur die Teile des Schutzsystems einbezogen, die sich bei beiden Systemen wesentlich voneinander unterscheiden, d.h. der Teil der Meßwertverarbeitung und der Logikteil einschließlich der Abschlußglieder (siehe auch /1,2/). Die anderen Teile des Schutzsystems sind für die beiden verglichenen Konzepte prinzipiell gleich und tragen deshalb auch bei beiden in gleichem Maße zur mittleren Nichtverfügbarkeit, wie sie im Teil 1 bestimmt wurde, und zur Wahrscheinlichkeit einer Fehlauslösung des Schutzsystems, wie sie in diesem Teil ermittelt wird, bei. Der angestrebte Vergleich würde also dadurch nur weniger transparent.

Bei den durchgeführten Betrachtungen werden wieder systematische Fehler oder Fehler gemeinsamer Ursache bei der Hardware ausgeschlossen. Während man bei der mittleren Nichtverfügbarkeit davon ausgehen muß, daß diese Fehler einen sehr starken

Einfluß haben /1/ bzw. sogar dominieren, zeigten die Untersuchungen, daß deren Vernachlässigung bei der Fehlauslösungswahrscheinlichkeit keinen so wesentlichen Einfluß auf die ermittelten Ergebnisse haben werden. Am stärksten würden sich die Fehler gemeinsamer Ursache beim festverdrahteten Schutzsystem durch das zu unterstellende Fehljustieren der Grenzwertmelder infolge menschlichen Versagens bemerkbar machen.

Bei der Software für das Rechnerschutzsystem ist die Unterscheidung nach eindeutig und nicht eindeutig sicherheitsgerichteten Schutzaktionen bei dem untersuchten System praktisch nicht realisierbar. Die mit der Fehlerfreiheit der Software zusammenhängenden Aspekte wurden bereits im Teil 1 beschrieben. In diesem Teil 2 wird nur insoweit darauf eingegangen, als auf Grund weiterer Untersuchungen und durchgeführter Testläufe die Ergebnisse von Teil 1 weiter präzisiert werden konnten bzw. zu überarbeiten waren.

Da durch die Unterscheidung beim Rechnerschutzsystem, ob eine Schutzaktion über Ruhestrom- oder Arbeitsstromanregung ausgelöst wird, eine übersichtliche Darstellung erschwert wird, soll Tabelle 1 das Auffinden der jeweils interessierenden Sicherheitskenngrößen erleichtern.

	eindeutig sicherheitsgerichtete Schutzaktionen	nicht eindeutig sicherheitsgerichtete Schutzaktionen
Ruhestrom-Anregungen	mittlere Nichtverfügbarkeit: Teil 1,Kap.6.5 Fehlauslösungswahrscheinlichkeit: Teil 2, Kap. 3.3.1	mittlere Nichtverfügbarkeit: Teil 1,Kap. 6.5 Fehlauslösungswahrscheinlichkeit: Teil 2, Kap. 3.3.1
Arbeitsstrom-Anregungen	existieren nicht	mittlere Nichtverfügbarkeit: Teil 2, Kap. 3.3.2 Teil 1, Kap. 6.5

Tab. 1: Übersicht der Sicherheitskenngrößen beim Rechnerschutzsystem für Ruhestrom- und Arbeitsstromschutzanregungen

2. BEMERKUNGEN ZU NICHT EINDEUTIG SICHERHEITSGERICHTETEN SCHUTZAKTIONEN

Nicht eindeutig sicherheitsgerichtete Schutzaktionen können bei Fehlauslösung unter Umständen die Auslösung anderer Schutzaktionen verhindern, die bei Eintreten eines Störfalles zu dessen Beherrschung erforderlich sind. Z.B. wird bei einem Druckwasserreaktor durch das Notkühl-Niederdruckeinspeisesignal das Hochdruckeinspeisesignal verriegelt.

Der Begriff soll aber hier noch globaler gefaßt sein und sämtliche Schutzmaßnahmen einschließen, die nicht den eindeutig sicherheitsgerichteten zuzurechnen sind. Dies kann als gerechtfertigt angesehen werden, da bei diesen Schutzaktionen von vornherein kaum bestimmt werden kann, wie sich ihre Fehlanregung bei einem noch unbekannten Anlagenzustand auswirken wird. Darunter fallen also auch Schutzmaßnahmen, deren Fehlauslösung selbst zu einem Störfall führen kann; ebenso alle diejenigen, bei deren Fehlauslösung eventuell eintretende Störfälle schwerer beherrschbar werden, d.h. die die Anlage durch ihre Fehlauslösung nicht in einen sicheren Zustand überführen. Der hier verwendete Begriff weicht demnach von /3/ ab, wo eine engere Definition für die nicht eindeutig sicherheitsgerichteten Schutzaktionen gewählt wurde.

Anders als bei den eindeutig sicherheitsgerichteten Schutzaktionen sind also auch die Fehler und Ausfälle bei einer sicherheitstechnischen Betrachtung zu berücksichtigen, die zu einer Fehlauslösung von Schutzaktionen führen.

Im Teil 1 des Berichtes wurden alle auslösehemmenden Fehler (siehe Abb. 1b in /1/) zur Ermittlung der mittleren Nichtverfügbarkeit bei Anforderung des Schutzsystems herangezogen. Diese mittlere Nichtverfügbarkeit gilt auch für die nicht eindeutig sicherheitsgerichteten Schutzaktionen. Auch diese können durch auslösehemmende Fehler blockiert werden, so daß sie bei Anforderung nicht mehr ausgelöst werden können. Daneben ist hier aber noch die Wahrscheinlichkeit für eine Fehlauslösung,

im weiteren Fehlauslösungswahrscheinlichkeit genannt, des Schutzsystems zu bestimmen. Dazu sind alle auslösegerichteten Fehler zu betrachten.

Um zu einer weiterführenden Beurteilung der Wahrscheinlichkeit einer Gefährdung für die Anlage oder deren Umgebung bei Fehlauslösung einer oder mehrerer nicht eindeutig sicherheitsgerichteter Schutzaktionen zu kommen, müßte die Ausfallwahrscheinlichkeit für die entsprechenden Schutzaktionen mit der Eintrittswahrscheinlichkeit von den Störfällen innerhalb der Zeit bis zur Instandsetzung der ausgefallenen Kanalgruppe multipliziert werden, bei denen zu deren Beherrschung angeforderte notwendige Schutzaktionen fälschlicherweise blockiert sind oder durch andere fehlangeregte Schutzaktionen in ihrer Wirkung beeinträchtigt werden. Da für einen Vergleich eine derartige Beurteilung nicht ohne größeren Aufwand möglich ist und andererseits durch die in Arbeit befindliche deutsche Risikostudie geleistet werden kann, wurde hier darauf verzichtet.

Einer besonderen Betrachtung bedürfen noch die Fehlauslösungen des Schutzsystems, die unter Umständen selbst zu Störfällen führen können. Durch geeignete Maßnahmen innerhalb der Steuerungs- und Verriegelungsebene ist dafür Sorge zu tragen, daß auch solche Fehlauslösungen beherrscht werden (siehe auch Kap. 3.4).

Ein weiterer Aspekt muß hier noch berücksichtigt werden. Beim Rechnerschutzsystem werden einige Schutzmaßnahmen durch Ruhestrom-Digital-Ausgaben und einige durch Arbeitsstrom-Digital-Ausgaben angeregt (siehe auch Kap. 3.3). Bei den Ruhestromausgaben führen Fehler in zwei redundanten Kanälen zu einer Fehlauslösung, bei den Arbeitsstromausgaben verbleibt das System in seinem vorherigen Zustand, eine notwendig werdende Anregung ist jedoch blockiert. Die in diesem Teil ermittelte Ausfallwahrscheinlichkeit gilt somit nur für Ruhestromanregungen, für Arbeitsstromanregungen ist in Analogie eine mittlere Nichtverfügbarkeit mit den Gl. (8) und (3) bzw. (11) in Teil 1 zu ermitteln.

3. FEHLAUSLÖSUNGSWAHRSCHEINLICHKEIT DER BEIDEN REAKTORSCHUTZ-SYSTEME

3.1 Mathematischer Zusammenhang

Es sei nochmals darauf verwiesen, daß unter Fehlauslösungswahrscheinlichkeit des Schutzsystems hier die Wahrscheinlichkeit verstanden wird, daß das Schutzsystem infolge von Fehlern eine oder mehrere Schutzaktionen fälschlich auslöst. Der Fall einer Verhinderung einer Schutzaktion im Anforderungsfall infolge eines auslösehemmenden Fehlers wurde bereits im Teil 1 betrachtet.

Eine 2v3- bzw. 2v4-Auswahlschaltung löst dann eine (oder mehrere) Schutzaktion fälschlich aus, wenn nach auslösegerichteten Fehlern in einem der drei bzw. vier redundanten Kanäle einer Kanalgruppe in mindestens einem weiteren Kanal auslösegerichtete Fehler auftreten, ehe der erste Kanal durch Reparatur wieder instand gesetzt wurde. Bei einem 1v2-System führt bereits ein auslösegerichteter Fehler in einem Kanal zur Fehlauslösung.

Die Fehlauslösungswahrscheinlichkeit wurde mit Hilfe der Markovschen Prozesse ermittelt. Aussagen, was nach der Fehlauslösung geschieht, d.h. darüber, wie lange es dauert, bis durch Instandsetzung eines oder beider ausgefallener Kanäle die Fehlauslösung aufgehoben wird oder mit welcher Wahrscheinlichkeit mit dem Ausfall weiterer Kanäle gerechnet werden muß, wurden nicht gemacht. Die Fehlauslösungswahrscheinlichkeit des Schutzsystems innerhalb der Zeit t kann durch die Lösung der Differentialgleichungssysteme für ein 2v3-System bzw. ein 2v4-System ermittelt werden. Ein gleichzeitiger Ausfall innerhalb eines Überwachungszyklus von zwei Kanälen wird dabei wegen der sehr kleinen Eintrittswahrscheinlichkeit nicht berücksichtigt. Eine ausführliche Ableitung der genannten Gleichungen findet sich im Anhang. Eine Erklärung der verwendeten Formelzeichen ist im Formelabkürzungsverzeichnis zu finden.

Das Differentialgleichungssystem für das 2v3-System lautet (siehe auch Abb. 1a):

$$
\begin{aligned}
\dot{P}_1 &= -3\lambda P_1 + \mu P_2 & P_1(t=0) &= 1 \\
\dot{P}_2 &= 3\lambda P_1 - (2\lambda+\mu) P_2 & P_2(t=0) &= 0 \qquad (1) \\
\dot{P}_3 &= 2\lambda P_2 & P_3(t=0) &= 0
\end{aligned}
$$

und für das 2v4-System (siehe auch Abb.1b)

$$
\begin{aligned}
\dot{P}_1 &= -4\lambda P_1 + \mu P_2 & P_1(t=0) &= 1 \\
\dot{P}_2 &= 4\lambda P_1 - (3\lambda+\mu) P_2 & P_2(t=0) &= 0 \qquad (2) \\
\dot{P}_3 &= 3\lambda P_2 & P_3(t=0) &= 0
\end{aligned}
$$

wobei die mittlere Ausfallrate λ hier nur auslösegerichtete Fehler berücksichtigt und μ die mittlere Reparaturrate bezeichnet. Die P_i (i=1,2,3) bezeichnen dabei die Wahrscheinlichkeit folgender Systemzustände:

P_1: Alle redundanten Kanäle sind intakt.

P_2: Einer der redundanten Kanäle ist ausgefallen.

P_3: Zwei der redundanten Kanäle sind ausgefallen.

Die Wahrscheinlichkeit einer Fehlauslösung (Fehlauslösungswahrscheinlichkeit) ist dann

$$p = 1 - (P_1 + P_2) \qquad (3)$$

Somit erhält man die Fehlauslösungswahrscheinlichkeit für ein 2v3- bzw. 2v4-System als Lösung der Differentialgleichungssysteme zu

$$p_{2v3} = p_{2v4} = 1 - \frac{b_1 e^{b_2 t} - b_2 e^{b_1 t}}{b_1 - b_2} \qquad (4)$$

mit

$$b_1 = \frac{1}{2}\left[-(5\lambda+\mu) + \sqrt{\lambda^2+10\lambda\mu+\mu^2}\right]$$

$$b_2 = \frac{1}{2}\left[-(5\lambda+\mu) - \sqrt{\lambda^2+10\lambda\mu+\mu^2}\right] \qquad \text{für ein 2v3-System}$$

und

$$b_1 = \frac{1}{2}\left[-(7\lambda+\mu)+\sqrt{\lambda^2+14\lambda\mu+\mu^2}\right]$$

$$b_2 = \frac{1}{2}\left[-(7\lambda+\mu)-\sqrt{\lambda^2+14\lambda\mu+\mu^2}\right] \qquad \text{für ein 2v4-System.}$$

Einige wenige Schutzaktionen werden über 1v2-Verknüpfungen der Anregekriterien ausgelöst. Deshalb sei der Vollständigkeit halber auch die Fehlauslösungswahrscheinlichkeit eines 1v2-Systems angegeben (siehe auch Abb.1c)

$$p_{1v2} = 1 - e^{-2\lambda t} \tag{5}$$

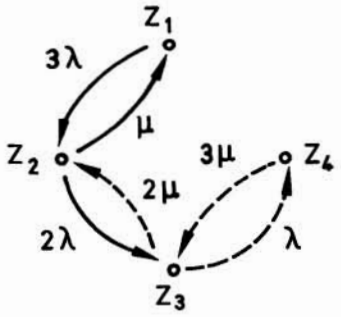
Bei einem festverdrahteten Reaktorschutzsystem schließt die Fehlauslösung einer Schutzaktion (bzw. Schutzteilaktion) durch den Ausfall einer Kanalgruppe, d.h. mindestens zweier Kanäle für ein Anregekriterium, nicht die Fehlauslösung weiterer Schutzaktionen aus. Um die Wahrscheinlichkeit dafür zu erhalten, daß innerhalb eines Betrachtungszeitraumes mindestens eine der Schutzaktionen eines 2v3-Systems fehlausgelöst wird, kann man näherungsweise die Anregekanäle vernachlässigen, die über eine UND-Bedingung verknüpft sind und weiter annehmen, daß alle n übrigen Kanalgruppen gleichartig aufgebaut sind und daher die Fehlauslösung über jedes Anregekriterium gleich wahrscheinlich ist. Somit ist dann die Wahrscheinlichkeit für die Fehlauslösung mindestens einer Schutzaktion

$$p = 1-(1-p_{2v3})^n = \sum_{j=1}^{n} (-1)^{j+1} \binom{n}{j} p_{2v3}{}^j \tag{6}$$

Von besonderem Interesse ist weiterhin die mittlere Zeit bis zum Ausfall (MTBF), d.h. hier bis zur Fehlauslösung des Schutzsystems. Die MTBF läßt sich nach folgender Gleichung ermitteln (Ableitung siehe z.B. /4/):

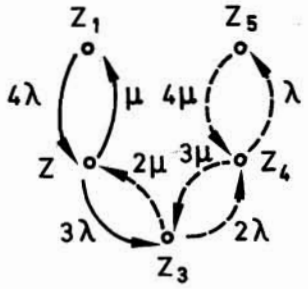
$$MTBF = \int_0^\infty R(t)dt \tag{7}$$

wobei $R(t) = 1-p_{nvm}$ die Zuverlässigkeit des Schutzsystems bezeichnet.



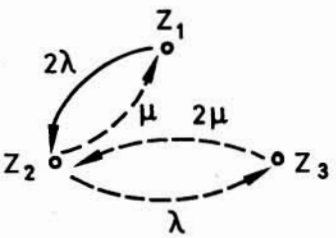
Zustand Z_1: alle drei Kanäle intakt
Zustand Z_2: ein Kanal ausgefallen
Zustand Z_3: zwei Kanäle ausgefallen und damit Systemausfall
Zustand Z_4: drei Kanäle ausgefallen

Abb. 1a: Zustandsdiagramm für ein 2v3-Schutzsystem



Zustand Z_1: alle vier Kanäle intakt
Zustand Z_2: ein Kanal ausgefallen
Zustand Z_3: zwei Kanäle ausgefallen und damit Systemausfall
Zustand Z_4: drei Kanäle ausgefallen
Zustand Z_5: vier Kanäle ausgefallen

Abb. 1b: Zustandsdiagramm für ein 2v4-Schutzsystem



Zustand Z_1: beide Kanäle intakt
Zustand Z_2: ein Kanal ausgefallen und damit Systemausfall
Zustand Z_3: beide Kanäle ausgefallen

Abb. 1c: Zustandsdiagramm für ein 1v2-Schutzsystem

Abb. 1a-c: Zustandsdiagramm für ein 2v3-, 2v4- und 1v2-Schutzsystem für auslösegerichtete Fehler

Für ein 1v2-, 2v3- bzw. 2v4-Schutzsystem ergeben sich demnach folgende MTBF (Ableitung siehe Anhang):

$$MTBF_{1v2} = \frac{1}{2\lambda} \tag{8}$$

$$MTBF_{2v3} = \frac{5\lambda+\mu}{6\lambda^2} \tag{9}$$

$$MTBF_{2v4} = \frac{7\lambda+\mu}{12\lambda^2} \tag{10}$$

Beim festverdrahteten dynamischen Schutzsystem gelten diese Gleichungen jeweils nur für eine bestimmte, durch die auslösegerichteten Fehler betroffene Schutzaktion, während beim Rechnerschutzsystem alle Ruhestrom-Schutzanregungen fehlausgelöst und alle Arbeitsstrom-Schutzanregungen blockiert werden (siehe Kap. 3.3, 3.4 und 3.5).

Um die in Kap. 2 angesprochene weiterführende Beurteilung einer Gefährdungswahrscheinlichkeit durchführen zu können, ist noch ein weiterer Aspekt zu berücksichtigen. Fällt ein zweiter Kanal für ein Anregekriterium aus, so wird mit Ausnahme des Zusammentreffens dieses Ausfalls mit dem Ausfall des ersten Kanals bereits mit der Instandsetzung dieses ersten Kanals begonnen worden sein. Das System kann also vor Ablauf der ganzen MTTR wieder in Betrieb gehen. Es sei hier nach der mittleren Länge $\overline{MTTR}$ des Anteils der MTTR für den ersten ausgefallenen Kanal bis zum zweiten Systemausfall gefragt unter der Voraussetzung, daß der zweite Systemausfall innerhalb der MTTR mit gleicher Wahrscheinlichkeit für jedes Teilintervall der Länge MTTR/n auftritt. Diese mittlere Länge $\overline{MTTR}$ läßt sich über den Erwartungswert des Ausfalles bestimmen und es ist

$$\overline{MTTR} = \lim_{n\to\infty} \sum_{i=1}^{n} \frac{MTTR}{n} (i-1)\frac{1}{n} =$$

$$= \lim_{n\to\infty} \left(\frac{MTTR}{2} - \frac{MTTR}{2n}\right) = \frac{MTTR}{2} \tag{11}$$

(Der Faktor i-1 rührt daher, daß im Falle des zweiten Systemausfalls innerhalb des Teilintervalls MTTR/n der Systemausfall schon zu Beginn des betreffenden Teilintervalls angenommen wurde,

d.h.,man nähert sich dem Grenzwert von unten. Selbstverständlich kommt man zum gleichen Ergebnis bei einer Annäherung an den Grenzwert von oben.) Somit ist zu erwarten, daß im Mittel ein 2v3-System bereits nach der halben mittleren Instandsetzungszeit für einen Kanal wieder in Betrieb gehen kann, wenn es durch den Ausfall zweier Kanäle ausgefallen ist und wenn man den Ausfall auch noch des dritten Kanals vor Instandsetzung des ersten vernachlässigt.

3.2 Fehlauslösungswahrscheinlichkeit des festverdrahteten dynamischen Schutzsystems

Tritt in einem Baustein eines der drei redundanten Kanäle für ein Anregekriterium ein auslösegerichteter Fehler auf, so geht das 2v3-System bis zur Wiederinstandsetzung des ausgefallenen Kanals in ein 1v2-System über. Ein weiterer auslösegerichteter Fehler noch vor Beendigung der Reparaturen des ersten Fehlers in einem anderen Kanal für das gleiche Anregekriterium führt dann zu einer Fehlanregung der betreffenden Schutzaktion. Wie im Kap. 2 ausgeführt, kann bei einer nicht eindeutig sicherheitsgerichteten Schutzaktion dadurch eine andere Schutzaktion blockiert werden, die zur Beherrschung eines eventuell eintretenden Störfalls aber notwendig ist oder dessen Beherrschung unnötig erschweren bzw. eventuell sogar selbst zu einem Störfall führen.

Die folgenden Ausfallraten für auslösegerichtete Fehler wurden den Quellen /5,6,7/ entnommen. Gegenüber den dort genannten Ausfallraten wurde hier noch ein Belastungsfaktor von 0,3 berücksichtigt, da die Bauelemente der einzelnen Baugruppen nur etwa 30 % der zulässigen thermischen und elektrischen Belastung unterworfen sind.

Liste der Ausfallraten für auslösegerichtete Fehler:

Strom/Spannungs-Wandler	$2 \cdot 10^{-6}$ 1/h
Spannungs/Spannungs-Wandler	$2 \cdot 10^{-6}$ 1/h

Rechenschaltung	$1 \cdot 10^{-6}$ 1/h
Grenzwertgeber	$4,5 \cdot 10^{-6}$ 1/h
2v3-Kettenglied	$1 \cdot 10^{-6}$ 1/h
Abschlußglied	$3,2 \cdot 10^{-6}$ 1/h
Taktgeber	$4,7 \cdot 10^{-6}$ 1/h

Für die mittlere Zeit bis zur Instandsetzung (MTTR) werden, wie im Teil 1, 24 h angenommen, da es fraglich ist, ob an Wochenenden, Feiertagen und während der Nachtschicht Reparaturen durchgeführt werden, gleichwohl ist diese Annahme als sehr konservativ anzusehen. Die Fehlererkennungszeit kann bei den hier betrachteten auslösegerichteten Fehlern gegenüber der Reparaturzeit vernachlässigt werden, da diese Fehler alle selbstmeldend sind. Die Reparaturrate μ ist 1/MTTR (siehe Gl. 7 in Teil 1 oder Ableitung in /4/).

Die im folgenden ermittelten Fehlauslösungswahrscheinlichkeiten beziehen sich alle auf den Betrachtungszeitraum von 1 Jahr.

Mit den angeführten Ausfall- und Reparaturraten und Gl.(4) erhält man dann die Fehlauslösungswahrscheinlichkeit für ein bestimmtes einfaches Anregekriterium in 2v3-Wertung zu

$$p_{2v3} \simeq 1,9 \cdot 10^{-4}.$$

Für ein Anregekriterium, das über eine Rechenschaltung mit drei Eingangsparametern gebildet wird, ist die entsprechende Fehlauslösungswahrscheinlichkeit

$$p_{2v3} \simeq 4,8 \cdot 10^{-4}.$$

Um eine Abschätzung über die Wahrscheinlichkeit zu erhalten, daß mindestens eine der nicht eindeutig sicherheitsgerichteten Schutzaktionen fälschlich angeregt wird, kann man die vereinfachende Näherung treffen, daß alle Schutzaktionen jeweils nur über ein einfaches Anregekriterium in 2v3-Wertung ausgelöst werden. (Tatsächlich treten auch 1v2- und 2v4-Wertungen auf und sind einige Anregekriterien über UND- bzw. ODER-Bedingungen

miteinander verknüpft, trotzdem erscheint die getroffene Näherung erlaubt, da es sich hierbei nur um eine grobe Abschätzung handeln soll.) Bei ca. 70 Kanalgruppen zur Anregung nicht eindeutig sicherheitsgerichteter Schutzaktionen ergibt sich dann nach Gl. 6

$$p \simeq 1{,}3 \cdot 10^{-2}.$$

3.3 Fehlauslösungswahrscheinlichkeit bzw. mittlere Nichtverfügbarkeit des Rechnerschutzsystems

Auch hier geht nach Ausfall eines Rechners das 2v3-System für alle Ruhestromanregungen in ein 1v2-System über und löst nach Ausfall eines zweiten Rechners noch vor Instandsetzung des ersten alle Ruhestrom-Digital-Ausgaben fälschlich aus.

Bei Ruhestrom-Digital-Ausgaben fallen die den Taktüberwachungseinheiten nachgeschalteten Relais bei Ausbleiben der vom Rechner kommenden Impulskette ab und lösen bei Ausfall von mindestens zwei Rechnern dadurch die entsprechenden Schutzaktionen aus (siehe Kap. 3.2, Teil 1). Alle eindeutig sicherheitsgerichteten, aber auch einige nicht eindeutig sicherheitsgerichtete Schutzaktionen sind nach diesem Ruhestromprinzip verwirklicht.

Alle anderen nicht eindeutig sicherheitsgerichteten Schutzaktionen und eine Reihe von Meldungen werden über Arbeitsstrom-Digital-Anregungen ausgelöst. Diese Ausgabestufen werden am Ende des Überwachungszyklus (ca. 80 µs), falls vom Überwachungsprogramm her gefordert, in ihrer Lage verändert (gesetzt bzw. rückgesetzt). Die Digitalausgabe besitzt als Abschlußglied ein bistabiles Relais mit einer Setz- und Rücksetzwicklung. Das Relais verharrt in der entsprechenden Richtung, auch wenn kein Auslöseimpuls mehr ansteht. Bei einem Ausfall des Schutzsystems werden somit die Arbeitsstrom-Digital-Ausgaben nicht angeregt, sondern verbleiben in ihrem vorherigen Zustand. Die entsprechenden Schutzmaßnahmen können aber auch nicht mehr bei Überschreiten der entsprechenden Grenzwerte ausgelöst werden. Bei einem

Ausfall eines Kanals des Schutzsystems geht für diese Anregungen das 2v3-System in ein 2v2-System über.

Bei dem Rechnerschutzsystem in Brunsbüttel ist aber nur ein Teil des gesamten Reaktorschutzes auf die Schutzrechner geführt /1,2/. Bei dieser Konfiguration würde selbst die Unterdrückung der Schutzmaßnahmen über Arbeitsstrom-Digital-Ausgaben zu keinen gefährlichen Zuständen in der Anlage führen /8/.

Die Ausfallrate für einen Schutzrechner zusammen mit seinem Verkehrsverteiler ist wieder /9/ mit $\lambda = 479{,}5 \cdot 10^{-6}$ 1/h zu entnehmen. Die auslösegerichteten Fehler der Trennverstärker können wiederum wie in Kap. 6.51 Teil 1 bei der Ermittlung der mittleren Nichtverfügbarkeit gegenüber denen des Rechners und Verkehrsverteilers vernachlässigt werden. Die Ausfallrate für auslösegerichtete Fehler der Taktüberwachungseinheiten ist $10{,}6 \cdot 10^{-6}$ 1/h /10/. Allerdings löst der Ausfall zweier zusammengehörender Taktüberwachungseinheiten nicht sämtliche, sondern nur eine Schutzaktion fälschlich aus.

3.3.1 Fehlauslösungswahrscheinlichkeit bei Ruhestrom-Digital-Ausgaben

Die Fehlauslösungswahrscheinlichkeit, bezogen auf ein Jahr bei einer mittleren Instandsetzungszeit von 24 h, ist dann nach Gl.(4)

$$p_{2v3} \simeq 0{,}24.$$

In Abb. 2 ist die Fehlauslösungswahrscheinlichkeit für die MTBF eines Einzelrechners von 2000 h, 4000 h und 8000 h in Abhängigkeit der mittleren Instandsetzungszeit aufgetragen.

Nach Gl. (9) ist bei einer mittleren Instandsetzungszeit von 24 h die MTBF für die Fehlauslösung für das 2v3-Schutzsystem

$$MTBF_{2v3} \simeq 31200 \text{ h}.$$

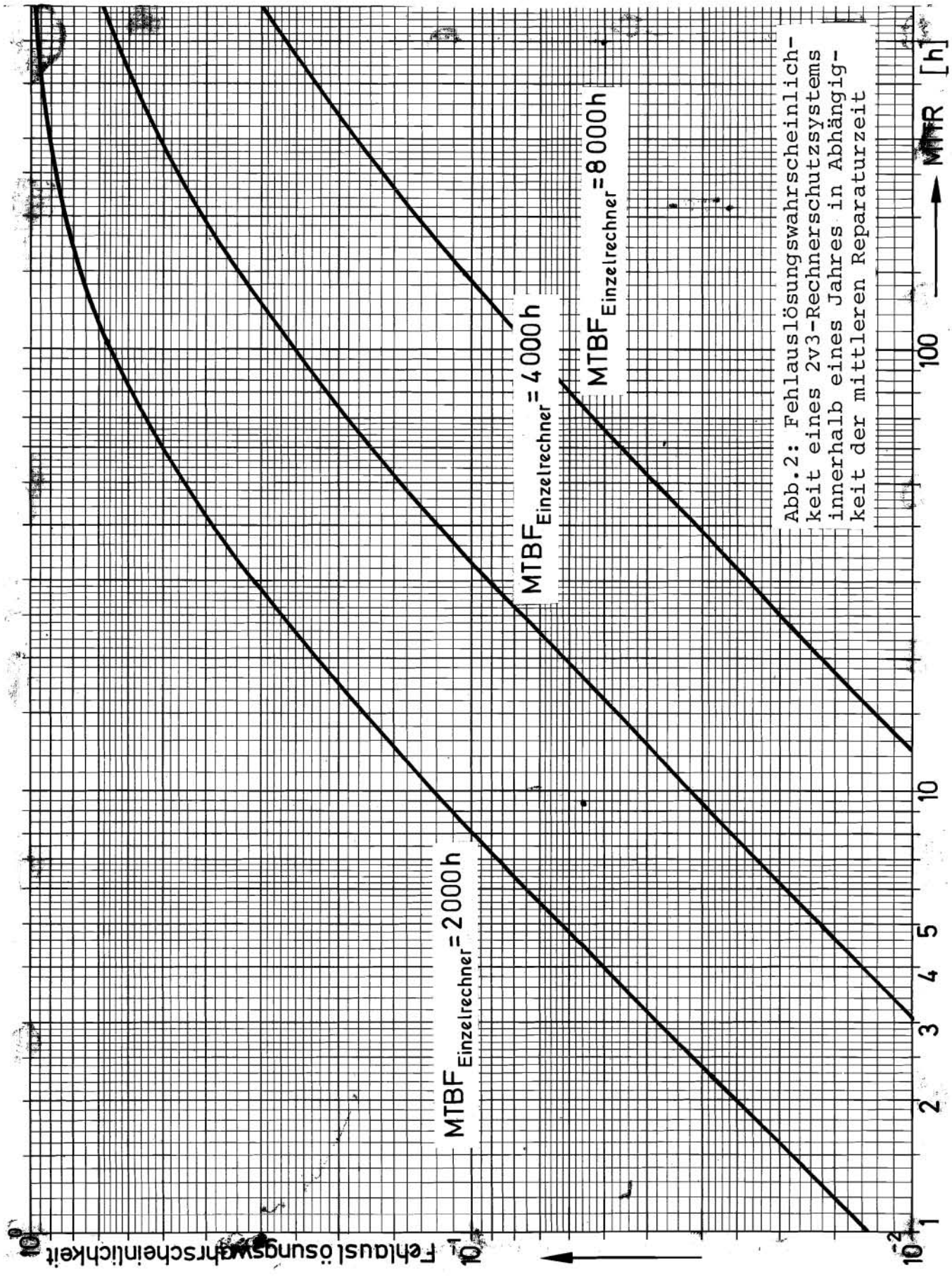


Abb.2: Fehlauslösungswahrscheinlichkeit eines 2v3-Rechnerschutzsystems innerhalb eines Jahres in Abhängigkeit der mittleren Reparaturzeit

Abb. 3 zeigt die MTBF des 2v3-Schutzsystems in Abhängigkeit der mittleren Instandsetzungszeit mit der MTBF 2000 h, 4000 h und 8000 h des Einzelrechners als Parameter.

Die diesen ermittelten Ergebnissen zugrunde liegenden Daten können als konservativ gelten (siehe auch Kap. 3.4), denn sicher lassen sich auch kürzere Reparaturzeiten verwirklichen und wurden im Einsatz erheblich bessere MTBF's als 2000 h erzielt.

3.3.2 Mittlere Nichtverfügbarkeit bei Arbeitsstrom-Digital-Ausgaben

Für die Schutzmaßnahmen über Arbeitsstrom-Digital-Ausgaben ist nicht die Fehlauslösungswahrscheinlichkeit, sondern die mittlere Nichtverfügbarkeit zu bestimmen, da bei Ausfall des Schutzsystems dasselbe nicht in der Lage ist, bei Anforderung einer Schutzaktion diese auszulösen, solange das System nicht durch Reparatur wieder instand gesetzt wurde. Hier sind somit alle Ausfälle wie gefährliche selbstmeldende Fehler zu behandeln. Selbstmeldend sind die Ausfälle deshalb, weil über einen entsprechenden Rechnerausgang sämtliche durch die Rechnerselbstüberwachung erkannten Fehler gemeldet werden und zur Abschaltung des Rechners führen. Die Frage nach der Vollständigkeit der Entdeckung aller Fehler durch die Rechnerselbstüberwachung wurde in Kap. 6.52 Teil 1 des Berichtes behandelt.

Die mittlere Nichtverfügbarkeit für die Arbeitsstromanregungen, die bei Ausfall des Rechnersystems blockiert werden, läßt sich nach Gl.(8) aus Teil 1 für einen Rechner und analog Gl.(3) aus Teil 1 für das 2v3-System berechnen und ergibt sich zu

$$\bar{u}_{2v3} \simeq 3(\lambda\tau)^2 \qquad \text{mit } \tau = \text{MTTR} = \frac{1}{\mu}$$

$$\simeq 4 \cdot 10^{-4}$$

bei Annahme des gleichen λ und μ wie oben. (Das gleiche Ergebnis erhält man auch mit Gl.(11) aus Teil 1, wenn man bedenkt,

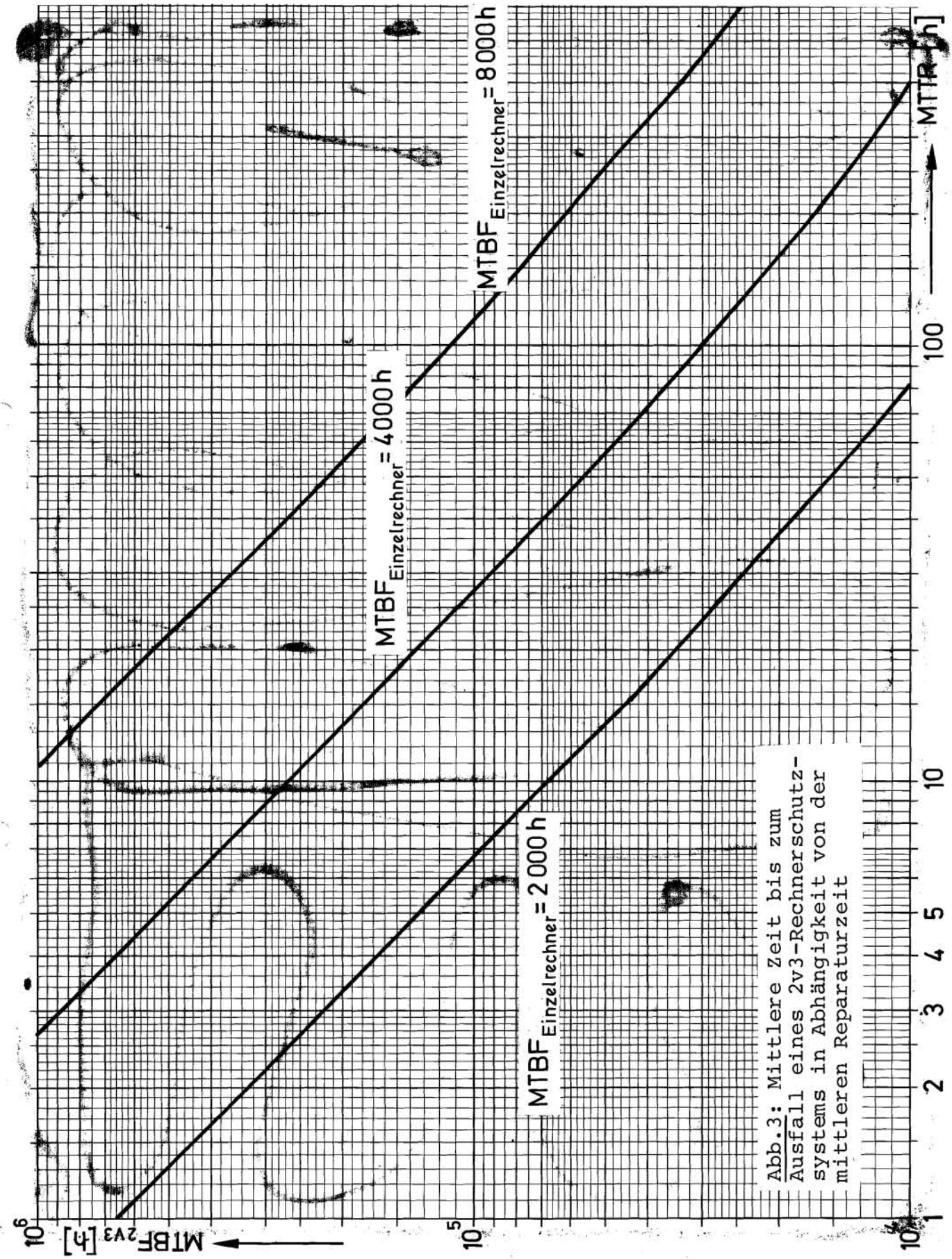


Abb.3: Mittlere Zeit bis zum Ausfall eines 2v3-Rechnerschutzsystems in Abhängigkeit von der mittleren Reparaturzeit

daß die hier betrachteten Fehler zu einem Ausfall des Rechners führen und damit selbstmeldend sind.) Abb.4 zeigt die mittlere Nichtverfügbarkeit des Schutzsystems in Abhängigkeit von der mittleren Reparaturzeit unter der Annahme, daß alle Fehler selbstmeldend sind.

3.4 Beurteilung der Fehlauslösungswahrscheinlichkeiten

Das Rechnerschutzsystem schneidet bei der Betrachtung der nicht eindeutig sicherheitsgerichteten Schutzaktionen gegenüber dem festverdrahteten dynamischen System erheblich schlechter ab. Allerdings wurde bei der vorliegenden Untersuchung von konservativen Voraussetzungen ausgegangen. So ist die mittlere Instandsetzungszeit sicherlich durch administrative Maßnahmen auf ein erheblich kleineres Maß zu drücken, was sich entsprechend auf die Fehlauslösungswahrscheinlichkeit auswirken würde; ebenso ist die Annahme einer MTBF von 2000 h für den Einzelrechner sicherlich zu pessimistisch (siehe Abb.2 und 3). So fielen z.B. weder einer der drei Schutzrechner in Brunsbüttel noch der gleiche Rechner bei der GRS in Garching innerhalb der letzten zwei Jahre auch nur einmal aus. Aber auch bei Annahme günstigerer Parameter ist es fraglich, ob bei Aufnahme sämtlicher Schutzaktionen in das Rechnerschutzsystem die durch den stark zentralistischen Ausbau bedingte, relativ hohe Fehlauslösungswahrscheinlichkeit hingenommen werden kann. Allerdings führt jeder Schutzsystemausfall zur Abschaltung des Reaktors, beeinträchtigt dadurch aber auch die Verfügbarkeit.

Dagegen ist anzunehmen, daß durch Konzepte, die eine starke Dezentralisierung des Rechnersystems vorsehen, oder die nur einzelne Aufgaben aus dem gesamten Reaktorschutz den Schutzrechnern (z.B. Mikroprozessoren) übertragen, Lösungen gefunden werden können, die den hohen sicherheitstechnischen Anforderungen gerecht werden können, die an ein Reaktorschutzsystem gestellt werden müssen.

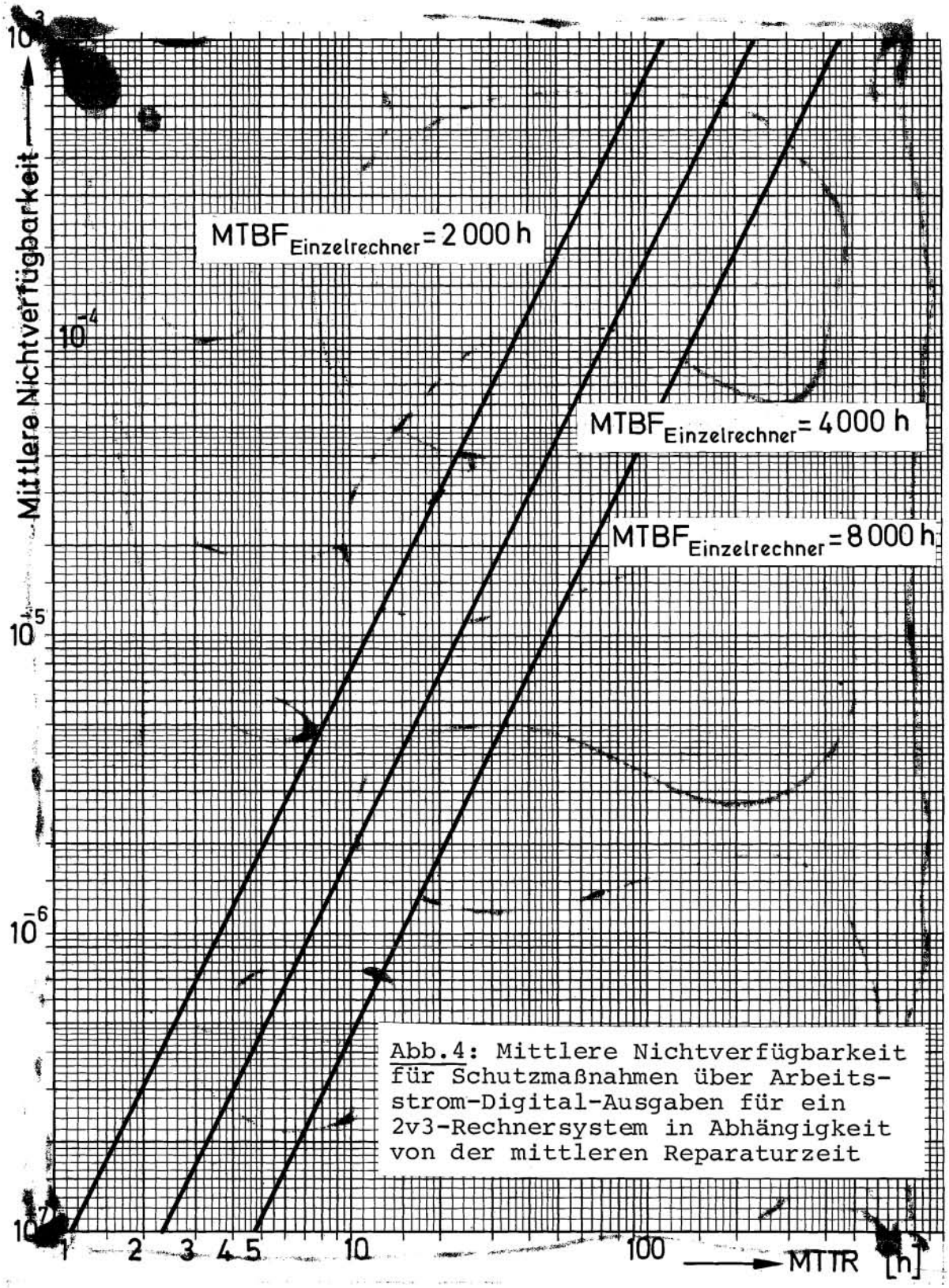


Abb.4: Mittlere Nichtverfügbarkeit für Schutzmaßnahmen über Arbeitsstrom-Digital-Ausgaben für ein 2v3-Rechnersystem in Abhängigkeit von der mittleren Reparaturzeit

Wie bereits in Kap. 2 erwähnt, sind für die nicht eindeutig sicherheitsgerichteten Schutzaktionen sowohl die mittlere Nichtverfügbarkeit als auch die Fehlauslösungswahrscheinlichkeit relevant. Allerdings ist die Fehlauslösungswahrscheinlichkeit allein noch kein Maß für die Sicherheit; wesentlich sind hier auch die Dauer der Fehlauslösung (siehe Kap. 3.1) und die Eintrittswahrscheinlichkeit von entsprechenden Störfällen.

Auf einen besonderen Fall soll hier noch eigens eingegangen werden, der für beide Schutzsysteme gilt, aber für das Rechnersystem infolge der höheren Fehlauslösungswahrscheinlichkeit besonders relevant ist. Es wurde bereits mehrfach erwähnt, daß die Fehlauslösung von Schutzaktionen u.U. selbst zu einem Störfall führen könnte (siehe Abb.1b Teil 1). Dies wäre z.B. durch eine Fehlauslösung der Schutzmaßnahmen "Öffnen der Entlastungsventile" gegeben. Diese Ventile könnten in diesem Fall nämlich nach einer Absenkung des Reaktordruckes um 5 bar unter den Ansprechdruck nicht mehr wie vorgesehen geschlossen werden. Vielmehr würden sie ständig weiter Dampf abblasen und könnten somit selbst einen Störfall verursachen. Deshalb wird die Öffnungszeit dieser Ventilgruppen, die über Ruhestrom-Digitalausgänge angeregt werden, innerhalb der Steuerungsebene begrenzt. Nach einer Zeit, die sicher größer als die normal benötigte Zeit zur Druckabsenkung unter 5 bar des Ansprechdruckes ist, gibt eine Zeitstufe ein entsprechendes Schließsignal. Die Ausfallrate dieser Zeitstufe beträgt ca. $2{,}4 \cdot 10^{-6}$ 1/h /5/. Es müssen also hardwaremäßige Lösungen gefunden werden, um die Auswirkungen bestimmter Fehlauslösungen von Schutzmaßnahmen zu begrenzen. Bei der weiterführenden Beurteilung der Wahrscheinlichkeit einer Gefährdung der Anlage sind diese Bausteine mit einzubeziehen.

Die hier ermittelten Fehlauslösungswahrscheinlichkeiten beziehen sich nur auf auslösegerichtete Fehler. Auch bei den nicht eindeutig sicherheitsgerichteten Schutzaktionen können auslösehemmende Fehler eine Schutzauslösung im Anforderungsfall verhindern. Für die nicht eindeutig sicherheitsgerichteten Schutzaktionen sind also (anders als bei den eindeutig sicherheitsge-

richteten, bei denen nur auslösehemmende Fehler betrachtet wurden) beide Fehlerarten von Bedeutung (siehe auch Kap. 2). Die also hier ebenfalls interessierende mittlere Nichtverfügbarkeit wird genauso berechnet wie im Teil 1 die mittlere Nichtverfügbarkeit für eindeutig sicherheitsgerichtete Schutzaktionen. Da in der Erfassung und Verarbeitung der Meßgrößen für die einzelnen Anregekriterien zwischen beiden Schutzaktionen kein Unterschied besteht, gelten auch die gleichen in Teil 1 ermittelten Ergebnisse. Demnach ist die mittlere Nichtverfügbarkeit beim festverdrahteten dynamischen Schutzsystem für ein bestimmtes Anregekriterium $\bar{u}_{2v3} \simeq 4{,}9 \cdot 10^{-7}$ und bei Berücksichtigung eines zweiten Anregekriteriums zur Beherrschung eines Störfalles $\bar{u} \simeq 2{,}4 \cdot 10^{-13}$. Beim Rechnerschutzsystem wäre bei vollständiger Erfassung aller Fehler die mittlere Nichtverfügbarkeit $\bar{u} \simeq 5{,}3 \cdot 10^{-14}$ und bei unvollständiger Erfassung aller Fehler durch die Selbstüberwachungsprogramme $\bar{u} \leq 1{,}6 \cdot 10^{-6}$ für alle Ruhestromanregungen und Arbeitsstromanregungen, für auslösegerichtete Fehler bei Arbeitsstromanregungen siehe Kap. 3.3.2.

3.5 Vorschlag zur Konzeption von Ruhestrom- und Arbeitsstrom-Digitalausgaben

Bei den nicht eindeutig sicherheitsgerichteten Schutzaktionen wird bei dem untersuchten Rechnerschutzsystem eine Reihe über Ruhestrom- und andere über Arbeitsstrom-Digitalausgaben angeregt. Wenn eine solche Aufteilung bei den nur wenigen aufgelegten nicht eindeutig sicherheitsgerichteten Schutzaktionen auch vertretbar ist, sollten die nicht eindeutig sicherheitsgerichteten Schutzaktionen doch möglichst alle über Arbeitsstrom-Anregungen ausgelöst werden. Dabei könnte der Umstand ausgenutzt werden, daß der Ausfall eines Rechners über die Selbstüberwachungsprogramme erkannt wird. Der ausgefallene Rechner eines 2v3-Systems sollte damit für die Arbeitsstrom-Anregungen nicht mehr in die Mehrheitsentscheidung einbezogen werden, so daß für diese Anregungen das Schutzsystem nach Ausfall eines Rechners in ein 2v2- (oder falls erwünscht in ein

1v2-System) und nach Ausfall zweier Rechner in ein 1v1-System übergeht. Da es bei diesen Schutzmaßnahmen eben in bezug auf die eventuelle Fehlauslösung keinen "sicheren" Zustand gibt, sondern je nach Anlagenzustand bzw. vorliegendem Störfall entschieden werden muß, ob die entsprechende Schutzaktion notwendig ist oder andere notwendige vielleicht blockiert, erscheint es richtiger, einen als defekt erkannten Rechner aus der Mehrheitsentscheidung auszuschließen und nicht in Abhängigkeit davon die Schutzaktion einfach auszulösen. Ebenso kann man sich bei Ausfall eines Rechners einen Übergang auf eine doppelte 1v1-Wertung vorstellen, wobei der einzelne Rechner nicht nur durch das Selbstüberwachungsprogramm, sondern auch durch einen Ergebnisvergleich mit dem anderen Rechner auf seine Funktionsfähigkeit überwacht wird. Bei den nicht eindeutig sicherheitsgerichteten Schutzaktionen bedeutet eine Erhöhung der Verfügbarkeit auch eine Erhöhung der Sicherheit. Selbstverständlich wird aber die Reaktorschnellabschaltung bei Ausfall eines zweiten Rechners weiterhin ausgelöst. Der gleichzeitige Ausfall aller drei Rechner ist ziemlich unwahrscheinlich. Für $\lambda = 479{,}5 \cdot 10^{-6} \frac{1}{h}$ und $\mu = \frac{1}{24} \frac{1}{h}$ ist die Wahrscheinlichkeit innerhalb eines Jahres dafür

$$p \simeq 1{,}6 \cdot 10^{-3}$$

Nach Gl.(7) ist dafür die MTBF $\simeq 5{,}46 \cdot 10^{6}$ h Für $\lambda =$

Für $\lambda = 5 \cdot 10^{-4} \frac{1}{h}$ und $\mu = \frac{1}{12} \frac{1}{h}$ erhält man $p \simeq 4{,}6 \cdot 10^{-4}$

und für $\lambda = 2{,}5 \cdot 10^{-4} \frac{1}{h}$ und $\mu = \frac{1}{24} \frac{1}{h}$ wird $p \simeq 2{,}3 \cdot 10^{-4}$,

in allen Fällen ist der Betrachtungszeitraum wieder 1 Jahr. Abb. 5 zeigt die Wahrscheinlichkeit des gleichzeitigen Ausfalls aller drei Rechner in Abhängigkeit von der mittleren Reparaturzeit und der MTBF des Einzelrechners als Parameter. (Ableitungen der Gleichungen für den Ausfall aller drei Rechner siehe Anhang.)

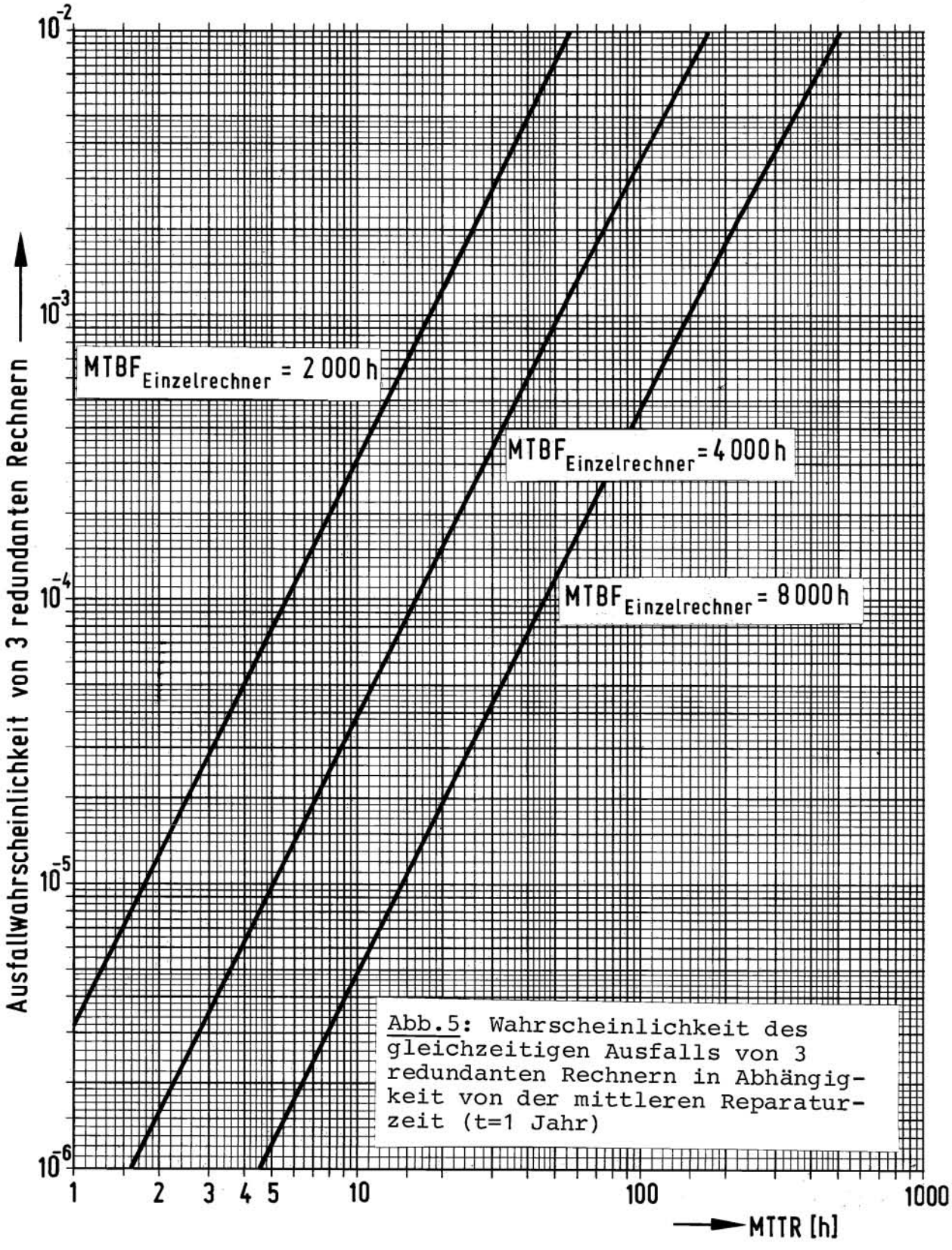


Abb.5: Wahrscheinlichkeit des gleichzeitigen Ausfalls von 3 redundanten Rechnern in Abhängigkeit von der mittleren Reparaturzeit (t=1 Jahr)

Die mittlere Nichtverfügbarkeit des Schutzsystems hinge im Falle des hier vorgeschlagenen Vorgehens ebenso wie bei den eindeutig sicherheitsgerichteten Schutzaktionen, neben der Ausfallrate und Reparaturzeit (bei den eindeutig sicherheitsgerichteten Schutzaktionen der Fehlererkennungszeit), nur noch von der Zuverlässigkeit der Rechnerselbstüberwachungsprogramme ab.

4. FEHLERFREIHEIT DER PROGRAMME

Die im Teil 1 gemachten Einschränkungen für die damals ermittelte Fehlerfreiheit der Programme müssen nicht länger aufrechterhalten werden. Mit /11/ wurde eine Untersuchung vorgelegt, die auch die verzögerten Schutzaktionen berücksichtigt, ebenso konnten die unterschiedlichen Reaktionen des Simulationsmodells und der Schutzrechnerprogramme bei den schnellen Reaktordruckänderungen erklärt werden.

Mit den im Zuge der weiteren Untersuchungen gemachten Testläufen wurden bis jetzt für den in Teil 1 beschriebenen Hybridrechnertest (siehe Abb.6) insgesamt ca. 535 000 Testläufe an einer Programmversion durchgeführt. Sich ergebende Abweichungen zwischen Reaktionen des Simulationsmodells und der Schutzprogramme der AEG 60-10 wurden analysiert /11,12/. Bei einigen verzögerten Schutzaktionen wurden dabei Abweichungen um einen Überwachungszyklus (ca. 70 ms) gegenüber der Spezifikation festgestellt, was aber als unbedenklich akzeptiert werden kann und sich auch durch eine entsprechende Programmänderung leicht beheben ließe (was aber neue Tests erforderlich machen würde). Weiterhin traten einige Abweichungen in den Reaktionen der Schutzprogramme gegenüber dem Modell auf, die eindeutig auf den Testaufbau zurückzuführen sind. Es verblieben aber noch insgesamt 27 abweichende Reaktionen, für die keine eindeutige Ursache gefunden werden konnte. Für jede dieser Abweichungen wurde der Test nochmals mit den gleichen Testdaten wiederholt, ohne daß wieder eine abweichende Reaktion aufgetreten wäre. Ein vorliegender Softwarefehler (im Testobjekt oder im Modell)

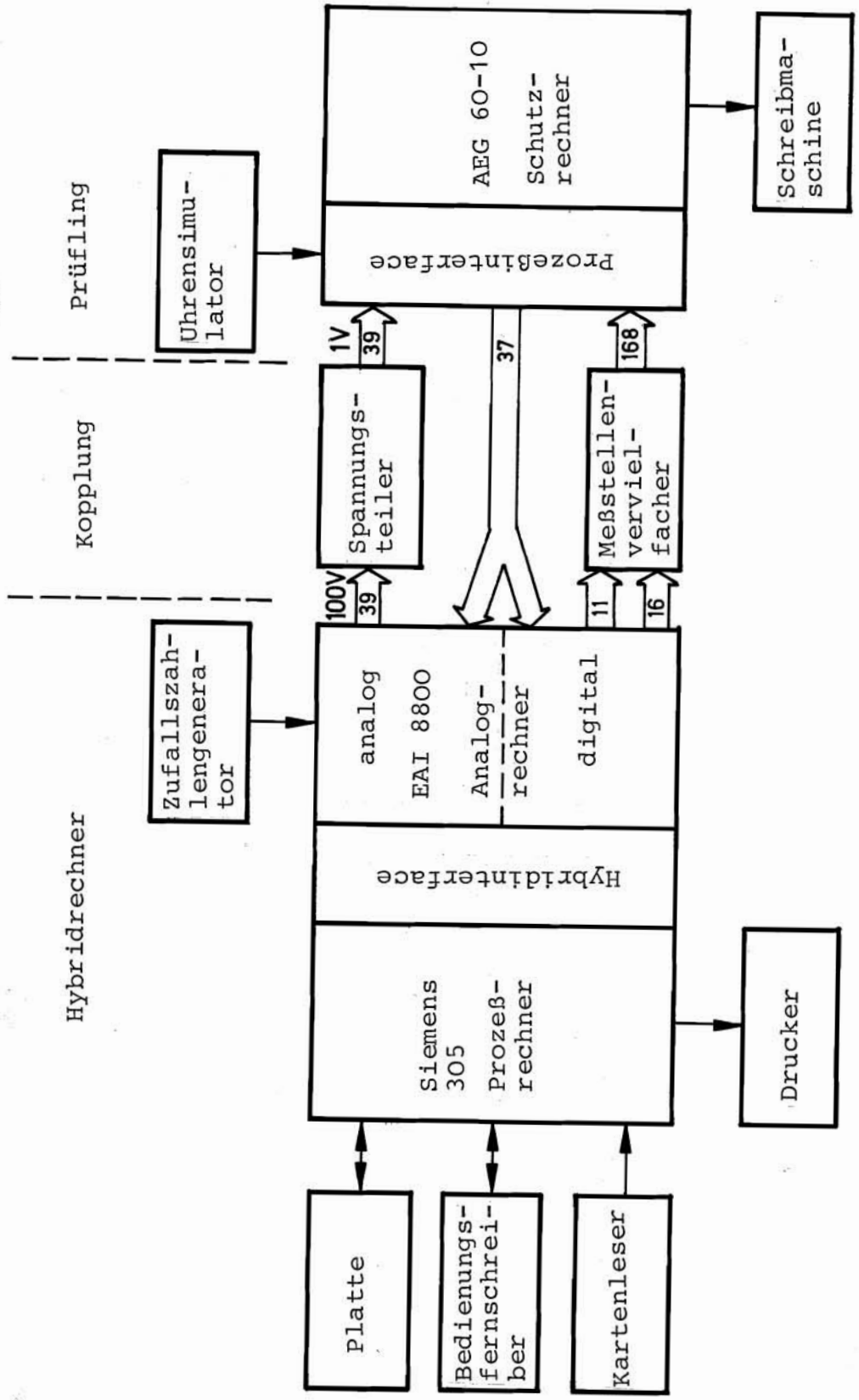


Abb. 6: Versuchsaufbau des Hybridrechnertests

hätte aber zur Folge haben müssen, daß die vorliegende Abweichung reproduzierbar gewesen und deshalb erneut aufgetreten wäre. Es muß sich dabei demnach um sporadische Hardwarefehler gehandelt haben, wobei nicht mehr feststellbar ist, ob diese Hardwarefehler im Prüfling oder im Testsystem auftraten. Da aber bisher aufgetauchte Fehler der AEG 60-10 durch die Selbstüberwachungsprogramme entdeckt und gemeldet wurden, ist die Vermutung naheliegend, daß die Fehler im Testsystem zu suchen sind. Diese Annahmen bestätigen auch Beobachtungen bei anderen Versuchen, bei denen sporadische Fehler im Hybridrechner in etwa der gleichen Größenordnung festzustellen waren.

Unter der Voraussetzung, daß diese unterschiedlichen Reaktionen alle auf Hardwarefehler zurückzuführen sind, ist Gl.(16) aus Teil 1 uneingeschränkt anwendbar und es ergibt sich mit einer Aussagesicherheit von 99 % die Versagenswahrscheinlichkeit der Schutzprogramme unter Annahme eines fehlerfreien Modells und unter Berücksichtigung aller bisher durchgeführten Testläufe zu

$$p \leq 8{,}6 \cdot 10^{-6}.$$

Berücksichtigt man auch hier wieder, daß auch gemeinsame gleichartige Fehler im Simulationsmodell und den zu testenden Schutzprogrammen auftreten können (siehe Kap.7 Teil 1), so ergibt sich nach Gl.(17) aus Teil 1 eine obere Schranke für die Versagenswahrscheinlichkeit der Arbeitsprogramme mit einer Aussagesicherheit von 99 % von

$$p < 1{,}72 \cdot 10^{-5}.$$

Mit dieser Versagenswahrscheinlichkeit wird noch keine Aussage über die Art eventueller Fehler der Software gemacht. Es kann sich dabei sowohl um auslösegerichtete als auch um auslösehemmende Fehler handeln. Es ist jedoch aufgrund der ganzen Selbstüberwachungsstrategie zu erwarten, daß die meisten der eventuell noch vorhandenen Fehler zu einer Fehlauslösung des Schutzsystems führen würden.

4.1 Beurteilung der erreichten Fehlerfreiheit

Trotz eines hohen geräte- und programmtechnischen Aufwandes, verbunden mit der Erfordernis einer manuellen Auswertung der Ergebnisprotokolle, konnte die Fehlerfreiheit der Software nur so weit nachgewiesen werden, daß die Wahrscheinlichkeit eventuell noch in ihr enthaltener Fehler gegenüber der mittleren Nichtverfügbarkeit bedingt durch die Hardware immer noch dominiert. Nachteilig ist auch, daß bei notwendig werdenden Programmänderungen (z.B. als Folge entdeckter Fehler) oder -ergänzungen eventuell die Prozedur des Nachweises der Fehlerfreiheit in erheblichem Umfang wiederholt werden muß. Durch die Entwicklung eines Verfahrens zur automatischen Analyse von Prozeßrechnerprogrammen /12/, wie es bei der GRS verfolgt wird (siehe Teil 1, Kap.7), dürften hier zukünftig noch bessere Ergebnisse zu erzielen sein. Im übrigen wurde bei den hier durchgeführten Untersuchungen von der konservativen Grundvoraussetzung ausgegangen, daß die Schutzprogramme je nach vorliegenden Eingangsdaten unendlich viele Pfade mit unendlich vielen Programmeigenschaften durchlaufen können. Die Anzahl der Programmeigenschaften ist jedoch endlich, und unter Berücksichtigung dieser Tatsache sind erheblich bessere Ergebnisse ohne weitere Tests zu erwarten. In Verbindung mit analytischen Nachweismethoden kann der Aufwand zum Nachweis der Fehlerfreiheit der Software sicher noch gegenüber dem bisher erforderlichen Aufwand erheblich reduziert werden.

Die Wahrscheinlichkeit einer Fehlauslösung von Reaktorschutzaktionen wird von der Software kaum berührt, ihr Einfluß kann gegenüber dem der Hardware praktisch vernachlässigt werden.

5. SCHLUSSBEMERKUNGEN

In den Teilen 1 und 2 der vorgelegten Untersuchung wurden die beiden Reaktorschutzsysteme hinsichtlich sicherheitstechnisch relevanter Gesichtspunkte verglichen. Ausgehend von den ermittelten Ergebnissen, kann man zu folgenden Beurteilungen der Systeme gelangen:

Für eindeutig sicherheitsgerichtete Schutzaktionen kann man davon ausgehen, daß beide Schutzsysteme für die betrachteten Teile (Meßwertverarbeitung, Logikteil und Abschlußglieder) den Anforderungen genügen, die an ein System mit solch hoher Sicherheitsverantwortung zu stellen sind. Die hier vorgenommenen Untersuchungen sollten noch durch weitere Untersuchungen hinsichtlich Common-mode-Fehler ergänzt werden; trotzdem kann aus den bisher vorliegenden entsprechenden Ergebnissen für Common-mode-Fehler geschlossen werden, daß die oben gemachte Aussage auch unter Einbezug derselben gültig bleiben wird (siehe dazu auch Teil 1, Kap.6).

Bei den nicht eindeutig sicherheitsgerichteten Schutzaktionen zeigen die Ergebnisse der Untersuchung für das festverdrahtete dynamische Schutzsystem, daß es die Sicherheitsanforderungen erfüllt. Für das Rechnerschutzsystem wirkt sich der weitgehend zentrale Aufbau allerdings sehr nachteilig aus, so daß unter der Annahme, daß sämtliche Schutzfunktionen von ihm übernommen werden sollten, es bei der vorliegenden Konfiguration fraglich ist, ob die relativ hohe Wahrscheinlichkeit von Fehlauslösungen (zwischen etwa 0,24 und $5 \cdot 10^{-3}$, je nach Wahl der noch als plausibel anzusehenden Parameter MTTR zwischen 24 h und 6 h und MTBF zwischen 2000 h und 8000 h) noch hingenommen werden kann. Man kann aber davon ausgehen, daß durch eine verbesserte Systemauslegung (z.B. dezentraler Aufbau) bzw. geeignete Aufteilung der Schutzfunktionen auf festverdrahtete Logik und Rechnermodule Lösungen für rechnergestützte Schutzsysteme zu finden sind, deren sicherheitstechnische Kenngrößen akzeptiert werden können. Ebenso könnte die in Kap. 3.5 vorgeschlagene Behandlung der nicht eindeutig sicherheitsgerichteten Schutzaktionen über Ar-

beitsstromanregungen unter Ausschluß defekter Rechner eine wesentliche Verbesserung bedeuten.

Ferner gibt es einige Gesichtspunkte, die die Einbeziehung freiprogrammierbarer Einheiten wünschenswert erscheinen ließen. Z.B. könnten dadurch neue Anregekriterien eingeführt werden, deren Realisierung durch festverdrahtete Rechenschaltungen nur sehr schwer möglich ist, da sie einen unangemessenen Hardwareaufwand erfordern würden, der sich auch sicherheitstechnisch wieder nachteilig auswirkt. Aus diesem Grunde seien am Ende dieses Berichtes die Vor- und Nachteile beider Systeme nochmals gegenübergestellt.

Festverdrahtetes dynamisches Schutzsystem

Vorteile:

- Dezentraler Aufbau
- Übersichtlichkeit durch Zuordnung bestimmter Funktionen an einzelne Bausteine
- Räumliche Trennung einzelner Redundanzgruppen
- Auftretende Fehler sind weitgehend selbstmeldend
- Langjährige Betriebserfahrung im Reaktorschutz
- Gute Möglichkeit der Fehlereingrenzung, Reparierbarkeit und Testbarkeit
- Aufbau des Systems, dem ingenieurmäßigen Denken des Betriebspersonals angepaßt.

Nachteile:

- Begrenzte Ausbaufähigkeit
- Hardwareaufwand steigt linear mit der Zahl der Anregekriterien
- Keine inhärente Dokumentation
- Drift oder Fehleinstellung der Sollgrößen von Grenzwerten möglich
- Rechenschaltungen nur schwierig vollständig austestbar.

Rechnerschutzsystem

Vorteile:

- Aufnahme neuer Anregekriterien möglich, deren Parameter eventuell direkt nicht erfaßbar sind
- Automatische Dokumentation von Fehlern, eingegebenen Grenzwerten usw.
- Durch die Selbstüberwachung sind auftretende Fehler weitgehend selbstmeldend
- Keine Drift der Sollgrößen von Grenzwerten
- Engere Staffelung von Grenzwerten möglich
- Hohe Systemgenauigkeit, die praktisch nur durch die Genauigkeit der Meßwertaufnehmer begrenzt ist
- Notwendig werdende Änderung von Grenzwerten (oder Neuaufnahme weiterer Anregekriterien) leicht möglich
- Eventuell geringerer Hardwareaufwand
- Gute Möglichkeit der Fehlereingrenzung und Reparierbarkeit bei der Hardware.

Nachteile:

- Weitgehende Zentralisierung
- Schlechte Übersichtlichkeit
- Zur Wartung eventuell eigens ausgebildetes Personal nötig (insbesondere für Software)
- Schwierige Fehlereingrenzung und Reparierbarkeit bei eventuell auftretenden Software-Fehlern
- Bisher noch hoher Aufwand für Nachweis der Software-Fehlerfreiheit
- Bisher noch wenig Betriebserfahrung im Reaktorschutz (dafür jedoch bei anderen Anwendungsgebieten).

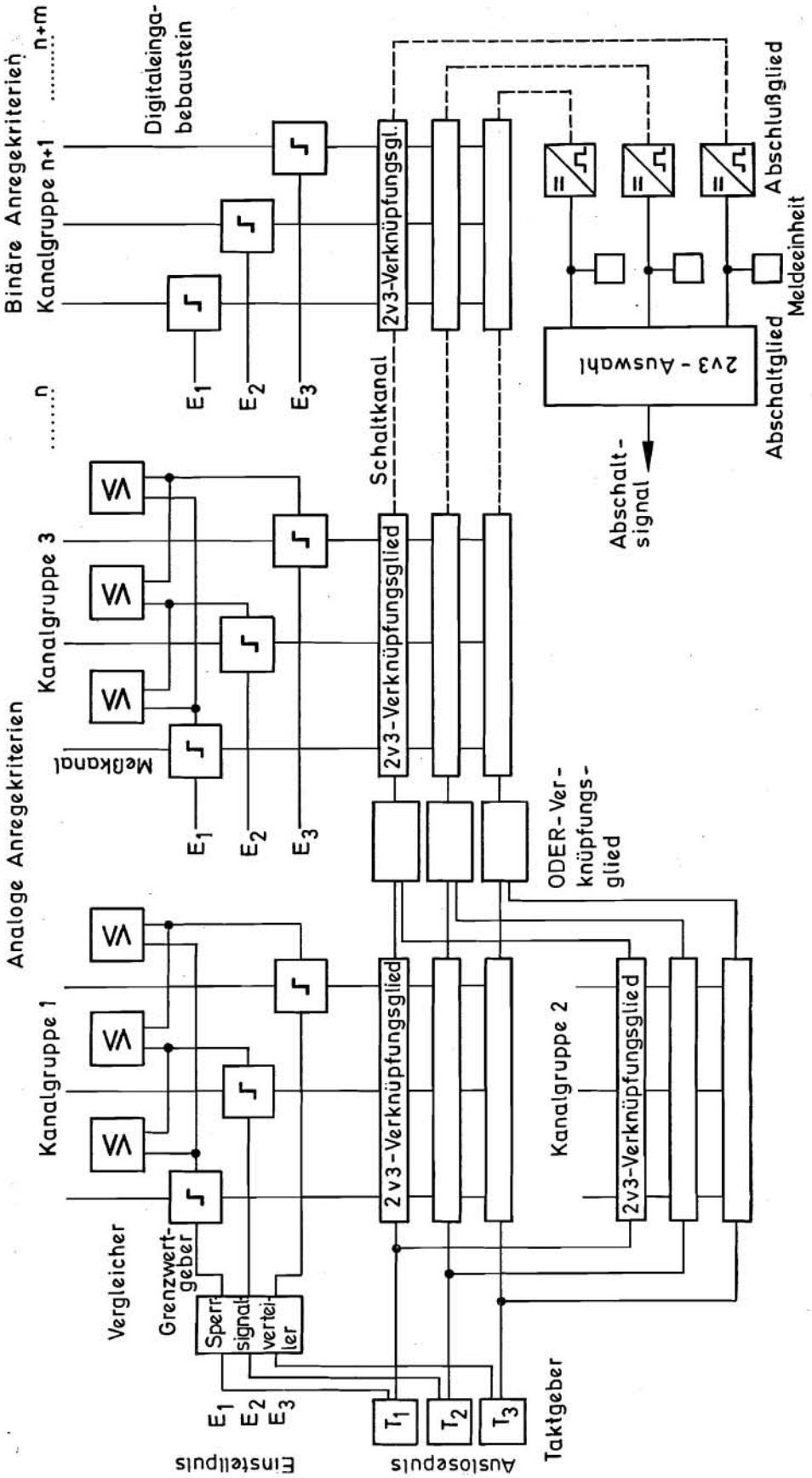


Abb. 7: Aufbau des festverdrahteten dynamischen Reaktorschutzsystems (aus Teil 1)

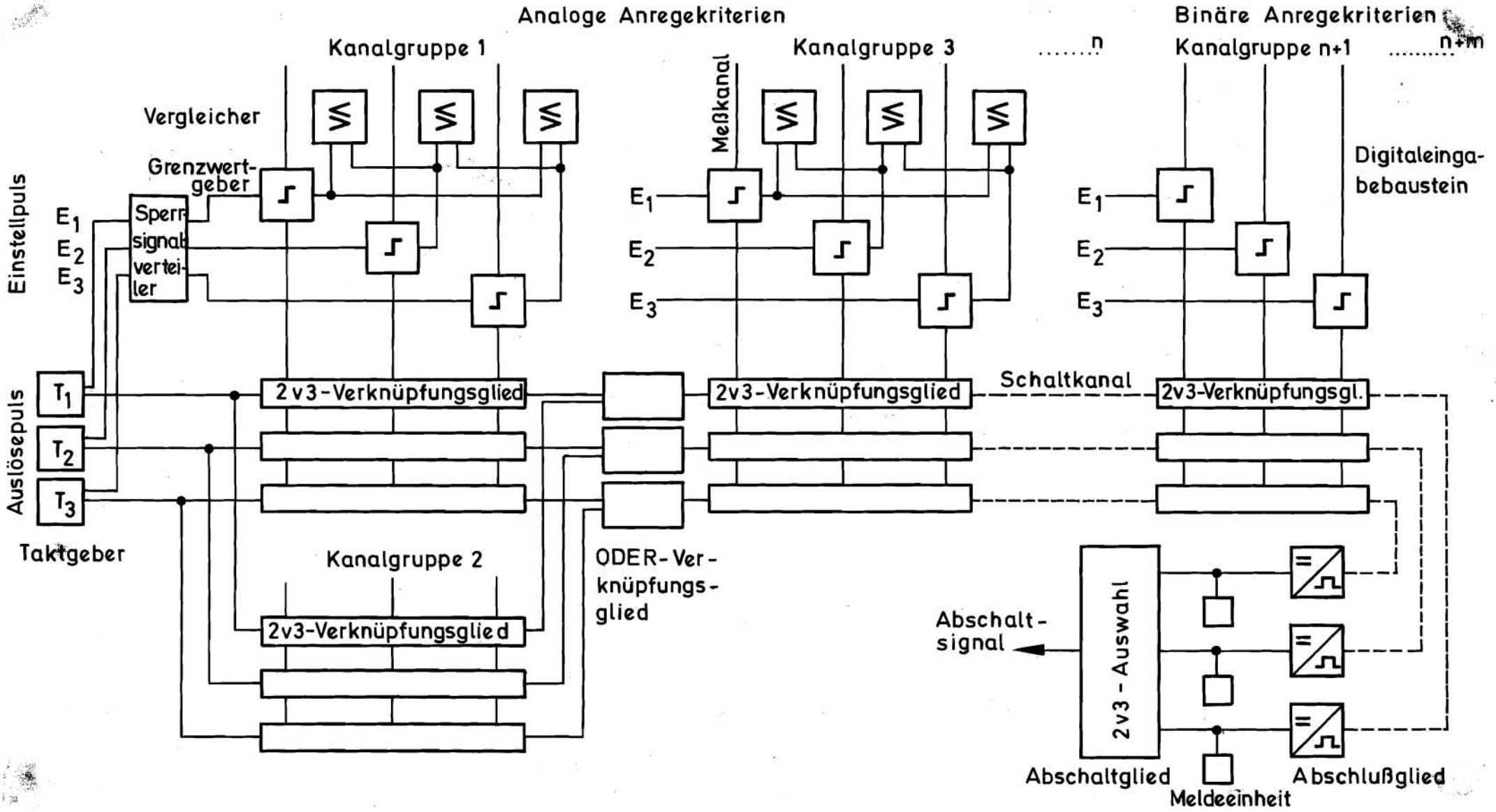


Abb. 7: Aufbau des festverdrahteten dynamischen Reaktorschutzsystems (aus Teil 1)

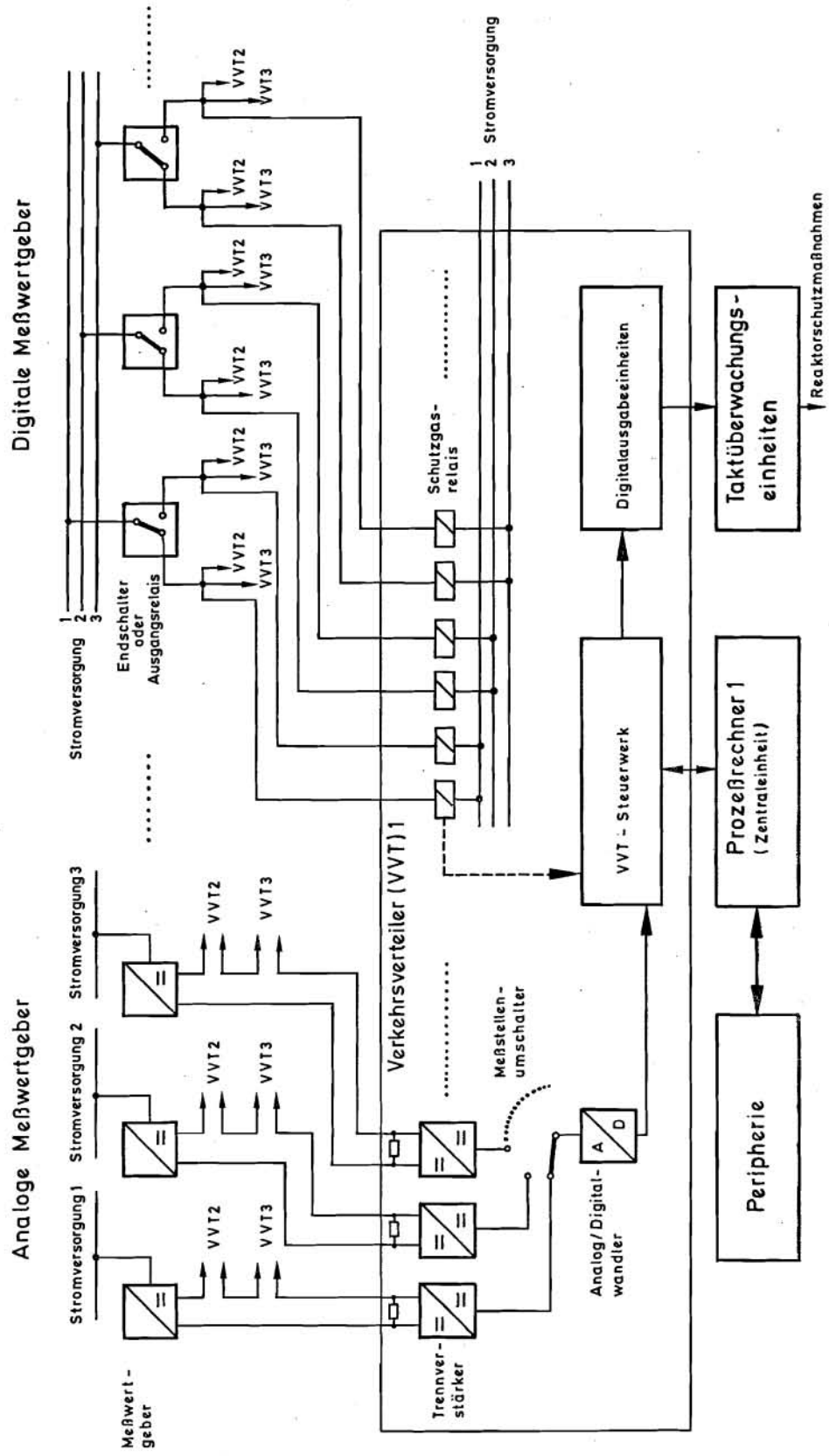


Abb. 8: Aufbau des Rechnerschutzsystems (aus Teil 1)

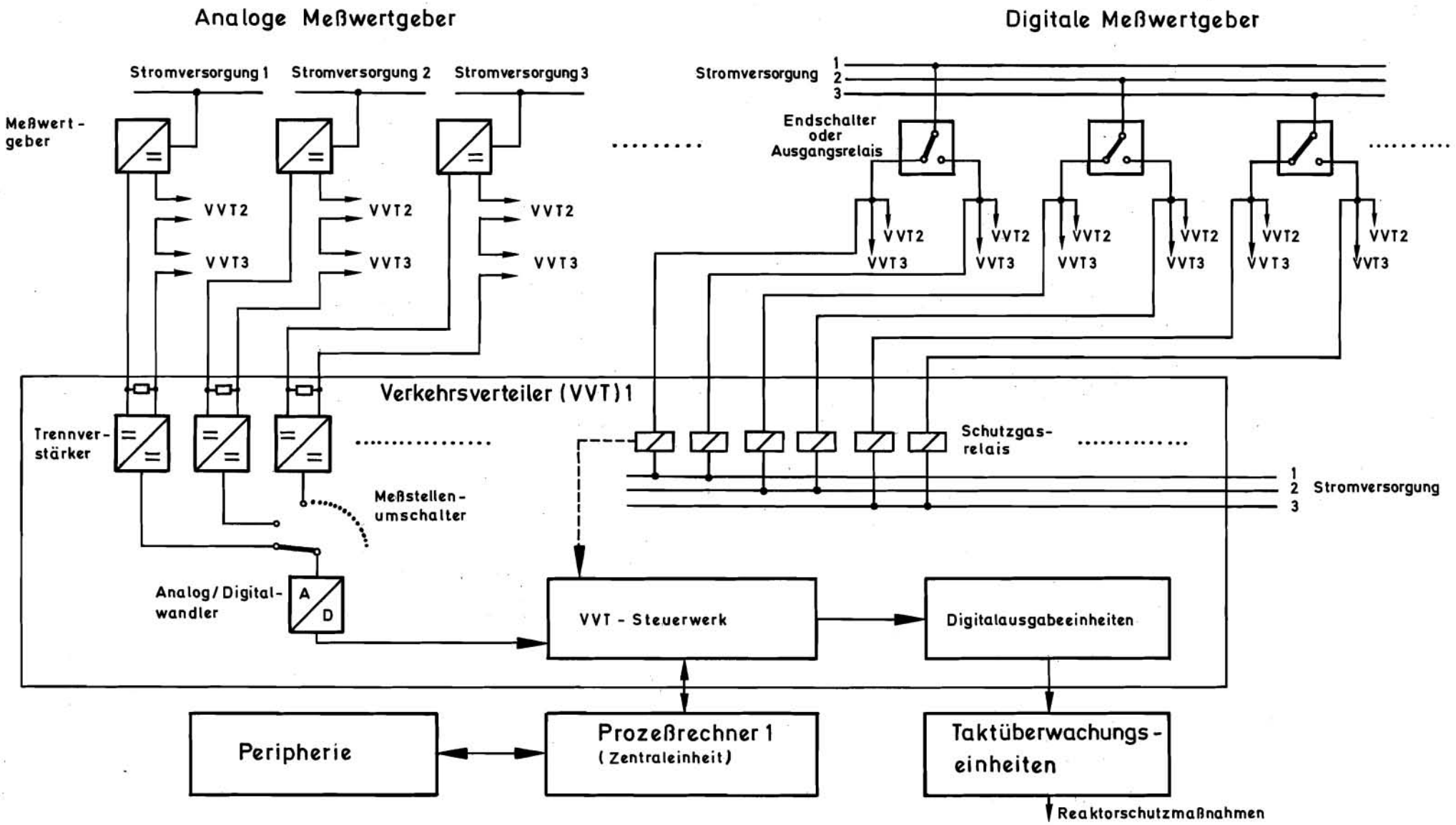


Abb. 8: Aufbau des Rechnerschutzsystems (aus Teil 1)

6. LITERATURVERZEICHNIS

/1/ Büttner, W.E.:

Sicherheitstechnischer Vergleich eines festverdrahteten dynamischen Reaktorschutzsystems mit einem Rechnerschutzsystem (Teil 1)

MRR 161, Juli 1976

/2/ Büttner, W.E.:

Comparison between a Dynamic Hard-wired and a Computerized Reactor Protection System in View of Technical Safety Aspects

Enlarged Halden Programme Group Meeting on Process Supervision and Control in Nuclear Power Plants Frederikstad, Norway, June 1977

/3/ Reaktorschutzsystem und Überwachung von Sicherheitseinrichtungen, sicherheitstechnische Anforderungen

DIN 25434, Okt. 1977 (wortgleich mit KTA-Regel 3501)

/4/ Technische Zuverlässigkeit

Herausgegeben von Messerschmitt-Bölkow-Blohm Springer-Verlag, 1971

/5/ Nieckau, E.:

Abschätzung der Zuverlässigkeit von Bausteinen der Meßwert- und Signalverarbeitung von Reaktorschutzsystemen

MRR-I-3, Februar 1973

/6/ Gieseler, H., und L. Quintus:

Ausfallanalyse von Reaktorschutzsystemen

MRR 82, Oktober 1970

/7/ Goßner, S.:

Theoretische Untersuchung des Ausfallverhaltens eines dynamischen Grenzwertmelders

MRR 143, Februar 1975

/8/ Rahmenspezifikation für Reaktorschutzsysteme mit Prozeßrechnern

Bericht der AEG, KKB FC/BA 005, Januar 1973

/ 9/ Ausfall- und Fehlereffektanalyse des Rechners AEG 60-10 für die Anwendung im Reaktorschutzsystem

Bericht der AEG, Mai 1972

/10/ Goßner, S.:

Experimentelle Bestimmung des Betriebs- und Ausfallverhaltens einer Taktüberwachungseinheit

MRR 130, August 1973

/11/ Brosch, J.:

Hybridrechnertest von zeitverzögerten Reaktorschutzmaßnahmen

Diplomarbeit am Lehrstuhl für Reaktordynamik und Reaktorsicherheit, TU München, April 1977

/12/ Fellinger, R., G. Eder, W. Ehrenberger und J. Brosch:

Fortführung des Hybridtests prompter Schutzrechnerreaktionen und Umstellung des Testsystems auf FORTRAN IV

Studienarbeit am Laboratorium für Reaktorregelung und Anlagensicherung, Garching, Februar 1976

/13/ Ehrenberger, W., und K. Okroy:

A Basis for an Automatic Analysis of Sequential Process Computer Programs

6. European Workshop on Real Time Programming in Roquencourt, France, Juni 1976

/14/ Plögert, K., und H. Schüller:

Process Control with High Reliability Data Dependent Failure Detection Versus Test Programs

Vortrag auf 5th IFAC/IFIP International Conference on Digital Computer Applications to Process Control, The Hague, The Netherlands, June 14-17, 1977

/15/ Bronstein und Semendjajew:

Taschenbuch der Mathematik

Verlag Harri Deutsch, Frankfurt, 4. Auflage, 1964

Farbfilestrom blatt

Grün (oder gelb?)

ANHANG

A N H A N G

In diesem Anhang sollen die Ableitungen der Gleichungen aus Kap. 3.1 und 3.5, soweit sie nicht aus dem Zusammenhang leicht zu ersehen sind, näher ausgeführt werden, um einen leichteren Nachvollzug zu ermöglichen.

Anhang I

In den Differentialgleichungssystemen Gl.(1) und (2) wurde die Fehlererkennungsrate ε nicht besonders betrachtet, sondern in die Reparaturrate einbezogen. Für sehr große Fehlererkennungszeiten und kleine Reparaturzeiten ist dies nicht mehr zulässig. In /13/ z.B. erfolgte eine entsprechende Aufteilung.

Die Lösung des Differentialgleichungssystems soll hier nur für das 2v3-System (Gl.(1)) angegeben werden, für das 2v4-System ändern sich nur die Parameter. Mit dem Gleichungssystem der Gl.(1) wird eine Laplace-Transformation durchgeführt, dann lautet das Gleichungssystem im Bildbereich

$$sP_1(s)-1 = -3\lambda P_1(s) + \mu P_2(s)$$

$$sP_2(s) = 3\lambda P_1(s) - (2\lambda+\mu)P_2(s)$$

$$sP_3(s) = 2\lambda P_2(s)$$

Durch schrittweises Einsetzen erhält man dann

$$P_1(s) = \frac{s+(2\lambda+\mu)}{s^2+s(5\lambda+\mu)+6\lambda^2} \qquad \text{und}$$

$$P_2(s) = \frac{3\lambda}{s+(2\lambda+\mu)} \cdot P_1(s) = \frac{3\lambda}{s^2+s(5\lambda+\mu)+6\lambda^2}$$

Die Wahrscheinlichkeit für eine Fehlauslösung des Schutzsystems ist dann nach Gl. (3)

$$P_{2v3}(s) = \frac{1}{s} - \frac{s+(5\lambda+\mu)}{s^2+s(5\lambda+\mu)+6\lambda^2}$$

$$= \frac{1}{s} - \left(\frac{s}{(s+a_1)(s+a_2)} + \frac{5\lambda+\mu}{(s+a_1)(s+a_2)}\right)$$

mit $a_1 = -\frac{1}{2}\{-(5\lambda+\mu)-\sqrt{\lambda^2+10\lambda\mu+\mu^2}\}$

$a_2 = -\frac{1}{2}\{-(5\lambda+\mu)+\sqrt{\lambda^2+10\lambda\mu+\mu^2}\}$

wobei $a_1 = -s_1$ und $a_2 = -s_2$ durch die Wurzeln des quadratischen Polynoms des Nenners bestimmt sind.

Die Rücktransformation ergibt dann

$$p_{2v3} = 1 - \{\frac{1}{a_1-a_2}(a_1e^{-a_1t} - a_2e^{-a_2t}) + \frac{5\lambda+\mu}{a_1-a_2}(e^{-a_1t} - e^{-a_2t})\}$$

Mit $b_1 = -a_2$ und $b_2 = -a_1$ kann obiger Ausdruck noch auf eine einfachere Form gebracht werden und lautet dann

$$p_{2v3} = 1 - \frac{b_1e^{b_2t} - b_2e^{b_1t}}{b_1-b_2} \qquad (4)$$

Anhang II

Die Ermittlung der MTBF erfolgt über Gl.(7) mit

$R(t) = 1 - p$

Nach Gl.(4) ist für ein 2v3- oder 2v4-System R(t) demnach

$$R(t) = \frac{b_1 e^{b_2 t} - b_2 e^{b_1 t}}{b_1 - b_2}$$

$$MTBF_{2v3} = MTBF_{2v4} = \int_0^\infty \frac{b_1 e^{b_2 t} - b_2 e^{b_1 t}}{b_1 - b_2} \, dt =$$

$$= \frac{1}{b_1 - b_2} \left(\frac{b_1}{b_2} e^{b_2 t} - \frac{b_2}{b_1} e^{b_1 t} \right) \Big|_0^\infty$$

Da immer $b_1 < 0$ und $b_2 < 0$ ist (siehe Ausdrücke für die Fehlauslösungswahrscheinlichkeit; dies gilt, weil immer $\lambda > 0$ ist), wird

$$MTBF_{2v3} = MTBF_{2v4} = \frac{1}{b_1 - b_2} \cdot \frac{b_2^2 - b_1^2}{b_1 b_2}$$

Setzt man b_1 und b_2 ein, so erhält man Gl.(9) und (10).

Anhang III

In Kap. 3.5 wurde eine Wahrscheinlichkeit p für den Ausfall aller drei redundanten Rechner angegeben. Diese Wahrscheinlichkeit läßt sich aus folgendem Differentialgleichungssystem berechnen (siehe Abb.1a):

$$\dot{P}_1 = -3\lambda P_1 + \mu P_2 \qquad P_1(t=0) = 1$$
$$\dot{P}_2 = 3\lambda P_1 - (2\lambda+\mu) P_2 + 2\mu P_3 \qquad P_2(t=0) = 0$$
$$\dot{P}_3 = 2\lambda P_2 - (\lambda+2\mu) P_3 \qquad P_2(t=0) = 0$$
$$\dot{P}_4 = \lambda P_3 \qquad P_4(t=0) = 0$$

Die Ausfallwahrscheinlichkeit ist dabei

$$p = 1-(P_1+P_2+P_3)$$

Im Bildbereich lautet dann das obige laplacetransformierte Gleichungssystem

$$sP_1(s)-1 = -3\lambda P_1(s)+\mu P_2(s)$$
$$sP_2(s) = 3\lambda P_1(s)-(2\lambda+\mu)P_2(s)+2\mu P_3(s)$$
$$sP_3(s) = 2\lambda P_2(s)-(\lambda+2\mu)P_3(s)$$
$$sP_4(s) = \lambda P_3(s)$$

Durch schrittweises Einsetzen erhält man dann

$$P_1 = \frac{s^2+s(3\lambda+3\mu)+(2\lambda^2+\lambda\mu+2\mu^2)}{s^3+s^2(6\lambda+3\mu)+s(11\lambda^2+7\lambda\mu+2\mu^2)+6\lambda^3}$$

$$P_2 = \frac{(s+\lambda+2\mu)3\lambda}{s^2+s(3\lambda+3\mu)+(2\lambda^2+\lambda\mu+2\mu^2)} \cdot P_1$$

$$P_3 = \frac{6\lambda^2}{s^2+s(3\lambda+3\mu)+(2\lambda^2+\lambda\mu+2\mu^2)} \cdot P_1$$

Somit ist dann

$$p(s) = \frac{1}{s} - \frac{s^2+s(6\lambda+3\mu)+(11\lambda^2+7\lambda\mu+2\mu^2)}{s^3+s^2(6\lambda+3\mu)+(11\lambda^2+7\lambda\mu+2\mu^2)+6\lambda^3} =$$

$$= \frac{1}{s} - \left(\frac{s^2}{(s+a_1)(s+a_2)(s+a_3)} + \frac{s(6\lambda+3\mu)}{(s+a_1)(s+a_2)(s+a_3)} + \frac{11\lambda^2+7\lambda\mu+2\mu^2}{(s+a_1)(s+a_2)(s+a_3)}\right)$$

Zur Rücktransformation muß der Nenner auf die Form

$$(s+a_1)(s+a_2)(s+a_3)$$

gebracht werden, wobei $a_1 = -s_1$, $a_2 = -s_2$ und $a_3 = -s_3$ durch die drei Wurzeln des kubischen Polynoms des Nenners bestimmt sind. Als Verfahren zur Bestimmung der Wurzeln empfiehlt es sich hier nicht, die Cardanische Formel anzuwenden, da sonst die drei reellen Wurzeln durch komplexe Größen ausgedrückt werden, sondern eine Methode unter Verwendung von Hilfsgrößen, wie sie z.B. in /14/ S. 117 und 118 beschrieben ist. Da eine sehr hohe Rechengenauigkeit bei der Bestimmung der Wurzeln erforderlich ist, empfiehlt sich eine Kontrolle der Näherungslösung mit dem Originalnenner. Nach der Rücktransformation erhält man dann

$$p = 1 - \left\{\frac{a_1^2 e^{-a_1 t}}{(a_1-a_2)(a_1-a_3)} + \frac{a_2^2 e^{-a_2 t}}{(a_1-a_2)(a_3-a_2)} + \frac{a_3^2 e^{-a_3 t}}{(a_1-a_3)(a_2-a_3)} + \right.$$

$$(6\lambda+3\mu)\left(\frac{a_1 e^{-a_1 t}}{(a_1-a_2)(a_3-a_1)} + \frac{a_2 e^{-a_2 t}}{(a_1-a_2)(a_2-a_3)} + \frac{a_3 e^{-a_3 t}}{(a_1-a_3)(a_3-a_2)}\right) +$$

$$\left.(11\lambda^2+7\lambda\mu+2\mu^2)\left(\frac{e^{-a_1 t}}{(a_1-a_2)(a_1-a_3)} + \frac{e^{-a_2 t}}{(a_1-a_2)(a_3-a_2)} + \frac{e^{-a_3 t}}{(a_1-a_3)(a_2-a_3)}\right)\right\}$$

Anhang IV

Die MTBF errechnet sich wieder nach Gl.(7). Somit ist

$$MTBF = \int_0^\infty \{ \frac{a_1^2 e^{-a_1 t}}{(a_1-a_2)(a_1-a_3)} + \frac{a_2^2 e^{-a_2 t}}{(a_1-a_2)(a_3-a_2)} + \frac{a_3^2 e^{-a_3 t}}{(a_1-a_3)(a_2-a_3)} +$$

$$(6\lambda+3\mu)\left(\frac{a_1 e^{-a_1 t}}{(a_1-a_2)(a_3-a_1)} + \frac{a_2 e^{-a_2 t}}{(a_1-a_2)(a_2-a_3)} + \frac{a_3 e^{-a_3 t}}{(a_1-a_3)(a_3-a_2)}\right) +$$

$$(11\lambda^2+7\lambda\mu+2\mu^2)\left(\frac{e^{-a_1 t}}{(a_1-a_2)(a_1-a_3)} + \frac{e^{-a_2 t}}{(a_1-a_2)(a_3-a_2)} + \frac{e^{-a_3 t}}{(a_1-a_3)(a_2-a_3)}\right)\}dt$$

Da a_1, a_2 und a_3 praktisch immer größer als Null sind, ist

$$MTBF = \frac{a_1}{(a_1-a_2)(a_1-a_3)} + \frac{a_2}{(a_1-a_2)(a_3-a_2)} + \frac{a_3}{(a_1-a_3)(a_2-a_3)} +$$

$$(6\lambda+3\mu)\left(\frac{1}{(a_1-a_2)(a_3-a_1)} + \frac{1}{(a_1-a_2)(a_2-a_3)} + \frac{1}{(a_1-a_3)(a_3-a_2)}\right) +$$

$$(11\lambda^2+7\lambda\mu+2\mu^2)\left(\frac{1}{a_1(a_1-a_2)(a_1-a_3)} + \frac{1}{a_2(a_1-a_2)(a_3-a_2)} +\right.$$

$$\left. + \frac{1}{a_3(a_1-a_3)(a_2-a_3)}\right)$$