KfK 2909
Februar 1980

Untersuchung des Zusammenhangs zwischen Fehlerbaumanalyse und Störfallanalyse am Beispiel des Photometer-Leitfähigkeits-Meßstandes

G. Weber
Institut für Datenverarbeitung in der Technik
Projekt Nukleare Sicherheit

Kernforschungszentrum Karlsruhe

KERNFORSCHUNGSZENTRUM KARLSRUHE

Institut für Datenverarbeitung in der Technik

Projekt Nukleare Sicherheit

KfK 2909

Untersuchung des Zusammenhangs zwischen Fehlerbaumanalyse und Störfallanalyse am Beispiel des Photometer-Leitfähigkeits-Meßstandes

G. Weber

Kernforschungszentrum Karlsruhe GmbH, Karlsruhe

Kernforschungszentrum Karlsruhe GmbH
ISSN 0303-4003

Zusammenfassung

Am Beispiel des automatischen Photometer-Leitfähigkeits-Meßstandes wird der Zusammenhang zwischen Störfallanalyse und Fehlerbaumanalyse untersucht. Es wird gezeigt, wie man Fehlerkombinationen eines Störfalldiagramms und Minimalschnitte eines Fehlerbaums einander zuordnen kann. Diese Vorgehensweise erlaubt eine gegenseitige Kontrolle von Fehlerbaum- und Störfallanalyse. Mit Hilfe einer Matrizendarstellung aller Fehlerkombinationen des Systems erhalten wir eine Kontrolle der Analyse. Wir erhalten auch heuristische Regeln zur Verbesserung und Vereinfachung der Störfallanalyse. Notwendige Voraussetzungen für die Anwendbarkeit der Regeln werden diskutiert. Methodisch kann der Zusammenhang von Fehlerbaum und Störfalldiagramm (unter bestimmten Voraussetzungen) als Zusammenhang von Boole'scher Funktion und binärem Entscheidungsbaum dargestellt werden.

An Investigation of the Relations between Fault Tree Analysis and Cause Consequence Analysis with Special Reference to a Photometry and Conductimetry System

Abstract

For an automated photometry and conductimetry system, the relations between cause consequence analysis and fault tree analysis have been investigated. It has been shown how failure combinations of a cause consequence diagram and minimal cuts of a fault tree can be identified. This procedure allows a mutual control of fault tree analysis and cause consequence analysis. From a representation of all failure combinations of the system by means of a matrix we obtain a control of our analysis. Moreover, heuristic rules improving and simplifying the cause consequence analysis can be found. Necessary assumptions for the validity of these rules are discussed. Methodologically, the relation of a fault tree and a cause consequence diagram can be represented (under certain conditions) as a relation of a Boolean function and a binary decision tree.

Inhalt

		Seite
1.	Problemstellung	1
2.	Sicherheit des automatisierten Labors	2
2.1	Allgemeine Beschreibung des Analysenstandes	2
2.2	Automatische Ablaufsteuerung und Ablauftabelle	6
3.	Fehlerbaumanalyse (FBA)	9
3.1	Beispiele der Fehlerbaumanalyse (FBA)	10
3.2	Zusammenfassung der Resultate	17
4.	Störfallanalyse	21
4.1	Beispiele der Störfallanalyse	22
4.2	Zusammenfassung der Resultate der Störfallanalyse	28
5.	Methodische Überlegungen zum Zusammenhang von Fehlerbaumanalyse und Störfallanalyse	50
5.1	Beobachtungen an einigen Resultaten der FBA und Störfallanalyse	50
5.2	Aussagen über Ereigniskombinationen	51
5.3	Gegenseitige Kontrolle der Analysen	53
6.	Vereinfachung der Störfallanalyse	55
6.1	Voraussetzungen zu einer vereinfachten Störfallanalyse	55
6.2	Heuristische Regeln zur Vereinfachung der Störfallanalyse	56
7.	Schlußbemerkung	58
8.	Literatur	59
ANHANG A:	Ein Boole'sches Modell zum Zusammenhang von Fehlerbäumen und Störfalldiagrammen	61
A.1	Einleitung	61
A.2	Boole'sche Ausdrücke mit Verzögerung	62
A.3	Vorkommen von Minimalschnitten bei Störfalldiagrammen	65
A.4	Vorkommen von Minimalschnitten bei einem Fehlerbaum	69

Abbildungen, Tabellen

		Seite
Abb. 1:	Schematische Darstellung von Bauteilen	4
Abb. 2:	Vereinfachtes Apparateschema	5
Abb. 3:	MESSEN, KÜV füllen, Nr. 4	11
Abb. 4:	MESSEN, KÜV voll, Nr. 5	12
Abb. 5:	Teilergebnis für {PU1} (Zustände Nr. 4, 5)	13
Abb. 6:	Teilergebnis für {PU2} (Zustände Nr. 4, 5)	15
Abb. 7:	Teilergebnis für {PU4} (Zustände Nr. 4, 5)	16
Abb. 8:	Fehlerbaum für den Überlauf von Puffer 1	18
Abb. 9:	Fehlerbaum für den Überlauf von Puffer 2	19
Abb. 10:	Fehlerbaum für den Überlauf von Puffer 4	20
Abb. 11:	MESSEN, KÜV füllen, Nr. 4	24
Abb. 12:	MESSEN, KÜV voll, Nr. 5	25
Abb. 13:	Störfalldiagramm, Nr. 4	26
Abb. 14:	Störfalldiagramm, Nr. 5	27
Abb. 15 bis 33:	Vereinfachtes Apparateschema, Zustände Nr. 2 bis 20 (MESSEN, SPÜLEN, BLASEN)	30 bis 48
Abb. 34:	Verzweigung im Störfalldiagramm	51
Abb. 35:	Bedingung im Störfalldiagramm	52
Abb. 36:	Verzögerung	62
Abb. 37:	Negation und Verzögerungsglied	63
Abb. 38:	UND-Tor und Verzögerungsglied	63
Abb. 39:	ODER-Tor und Verzögerungsglied	64
Abb. 40:	Störfalldiagramm	66
Abb. 41:	Fehlerbäume	68
Abb. 42:	Fehlerbaum	69
Abb. 43:	Weg im Störfalldiagramm	71
Tab. 1:	Ablauftabelle	8
Tab. 2:	Zusammenfassung der Störfallanalysen	49

1. Problemstellung

Die Fehlerbaumanalyse definiert ein "Unerwünschtes Ereignis" und fragt dann nach seinen Ursachen. Die Störfallanalyse legt ein plausibles "Anfangsereignis" fest und sucht dann nach seinen Folgen. In diesem Bericht sollen anhand eines übersichtlichen Systems die folgenden Fragen beantwortet werden:

(a) Lassen sich methodische Überlegungen zum Zusammenhang zwischen Fehlerbaumanalyse und Störfallanalyse aufstellen?

(b) Kann eine Analyse durch eine andere kontrolliert werden?

(c) Gibt es Regeln zur Vereinfachung der Störfallanalyse?

2. Sicherheit des automatisierten Labors

Als Grundlage für unsere methodischen Überlegungen sollen Untersuchungen zur Sicherheit und Zuverlässigkeit von DV-Systemen und -Komponenten in einem analytischen Labor dienen /1/. Diese Untersuchungen wurden insbesondere für den Photometer-Leitfähigkeits-Meßstand des geplanten automatisierten Labors der WAK ausgeführt. Andere Untersuchungen zu Sicherheitsfragen des automatisierten Labors wurden bereits früher abgeschlossen bzw. stehen noch aus. Sie sollen jedoch hier nicht behandelt werden.

Wir wollen zunächst

- eine allgemeine Beschreibung des Photometer-Leitfähigkeits-Meßstandes machen (Abschn. 2.1),
- ein vereinfachtes Apparateschema zeigen (Abb. 1, 2),
- sowie in einer Ablauftabelle die im Normalbetrieb vorkommenden Zustände der wichtigsten Komponenten angeben (Abschn. 2.2, Tab. 1).

Diese Informationen sind ausführlicher bereits an anderer Stelle gegeben worden /1/. Es ist jedoch wichtig, den normalen Betriebsablauf für unsere Überlegungen zu kennen. Nur dann ist es möglich, die Störfälle zu finden.

2.1 Allgemeine Beschreibung des Analysenstandes

Die Prozeßmeßtechnik umfaßt die Methoden und Geräte zur Gewinnung von Information zum Zwecke der Regelung und Steuerung technischer Prozesse. So ist es wichtig, Proben aus dem Prozeß der Wiederaufbereitung zu untersuchen. Eine analytische Mehrkomponentenanalyse kann z.B. mit Hilfe der Spektralphotometrie und Leitfähigkeitsmessung gemacht werden. Aus Gründen der Sicherheit und der Effizienz wird man dies in einer vollautomatisierten Vorrichtung (Analysenstand) durchführen.

In geeigneten Gefäßen werden über eine sogenannte Rohrpost die zu untersuchenden Lösungen bis zum Eingang des Analysenstandes transportiert.

Der Ablauf der Analyse wird durch einen dazu programmierten Rechner gesteuert. Dieser Ablauf umfaßt drei Phasen:

- Messen,
- Spülen,
- Trockenblasen.

Abb. 2 gibt ein vereinfachtes Apparateschema für den Photometer-Leitfähigkeits-Meßstand.

Nun gehen wir auf die drei Phasen des Analysenablaufs etwas näher ein. Schließlich geben wir eine Übersicht aller dazu notwendigen Einstellungen und Funktionen von Komponenten des Meßstandes (Tab. 1, Ablauftabelle).

Die Bauteile des Apparateschemas (siehe Abb. 2) werden in Abb. 1 erklärt.

Nun wollen wir die einzelnen Phasen des Analysenablaufs kurz beschreiben. Jede Phase hat mehrere Schritte.

Phase 1: MESSEN (vgl. Abb. 2)

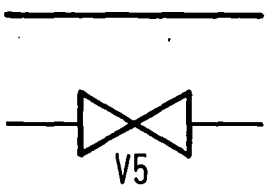
Aus dem Probengefäß (PTR) wird durch Druckluft die Analysenflüssigkeit in die Leitfähigkeitsmeßzelle (LFZ) gebracht. Dazu ist es notwendig, daß das Ventil V8 zwischen Druckluft und PTR offen ist (Einstellung a), aber V7 zwischen Druckluft und PU4 nicht offen ist (Einstellung a). Nun soll der Weg zwischen PTR und LFZ frei werden. Dazu muß V1 zwischen PTR und V2 offen sein. Jedoch soll die Flüssigkeit noch nicht nach der Küvette (KÜV) fließen (V1 Einstellung b). Außerdem muß V2 zwischen V1 und LFZ und PU3 offen sein (Einstellung b). Von den Feuchtefühlern meldet

L4 "feucht" (1) sowie
L1 und L3 "Übergang von trocken auf feucht" (O→1) .

Dieser Schritt heißt: "LFZ füllen". Wir fassen zusammen:

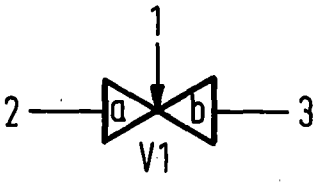
Schritt	Ventile					Fühler			
	V1	V2	V3	V7	V8	L1	L2	L3	L4
LFZ füllen	b	a	b	a	a	O→1	O	O→1	1

Diese Einstellungen können alle der Ablauftabelle entnommen werden (Tab. 1).



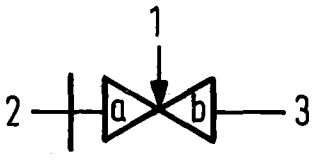
Rohrleitung

Einweg-Ventil (z.B. V5):
kann zwischen 1 und 2 offen oder geschlossen sein.

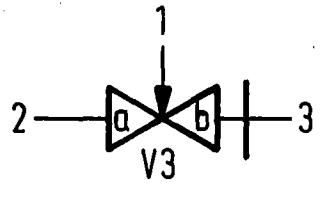


Zweiweg-Ventil (z.B. V1):
kann von 1 nach 2 oder von 1 nach 3 offen sein, aber nicht von 2 nach 3 offen sein.

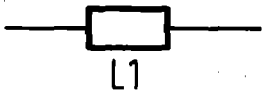
An vielen Stellen zeigt ein Strich quer zur Rohrleitung, in welcher Richtung das Ventil nicht offen ist:



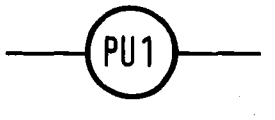
V3 ist auf b, d.h. von 1 nach 2 nicht offen.



V3 ist auf a, d.h. von 1 nach 3 nicht offen.



Feuchtefühler (z.B. L1):
zeigt an, ob der betreffende Teil der Rohrleitung feucht (1) oder trocken (0) ist.



Puffergefäß (z.B. PU1):
schützt vor Überfließen der in dem Apparat befindlichen Flüssigkeit.

Abb. 1: Schematische Darstellung von Bauteilen

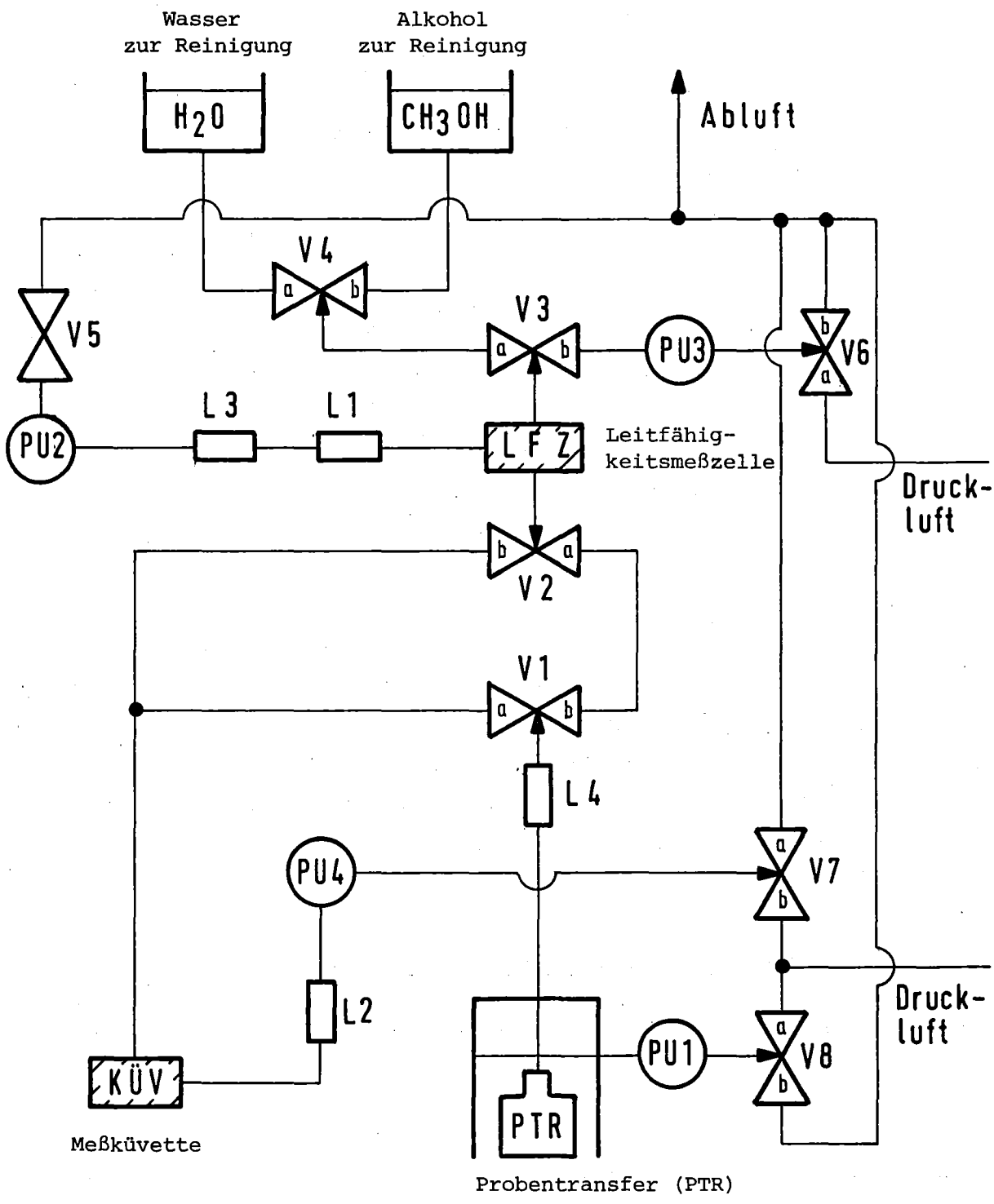


Abb. 2: Vereinfachtes Apparateschema.

Ist LFZ mit Flüssigkeit gefüllt, so wird ein weiteres Abfüllen abgestellt und eine Leitfähigkeitsmessung findet statt. Darauf kann die Probenflüssigkeit durch eine geeignete Einstellung von V2 in die Küvette (KÜV) fließen. Dann findet eine Photometermessung statt. Darauf wird durch Druckluft die Probenflüssigkeit wieder nach PTR gebracht. Das Probengefäß PTR wird dann automatisch entfernt.

Phase 2: SPÜLEN (vgl. Abb. 2)

Für die Präzision der Messung ist ein gründliches Spülen erforderlich. Durch eine geeignete Einstellung von V3 (Öffnung zwischen Wasser- bzw. Alkoholgefäß und LFZ, Einstellung a) kommt Wasser bzw. Alkohol in die gesamte von der Probenflüssigkeit benetzte Apparatur. Darauf wird die Spülflüssigkeit durch Druckluft nach außen gebracht in einen (nicht eingezeichneten) Abfallbehälter.

Phase 3: BLASEN (vgl. Abb. 2)

Durch Blasen wird die Anlage wieder getrocknet, so daß keine Meßfehler durch verbleibende Flüssigkeitsreste entstehen können. Durch geeignete Einstellung der Ventile kann erreicht werden, daß alle von den Reinigungsflüssigkeiten benetzten Teile des Meßstandes schnell getrocknet werden. Darauf ist es möglich, eine neue Probe (PTR) zu untersuchen.

2.2 Automatische Ablaufsteuerung und Ablauftabelle

Alle für den Normalbetrieb des Analysenstandes möglichen Kombinationen von

- Einstellungen der Ventile und
- Anzeigen der Feuchtefühler

sind in der Ablauftabelle (Tab. 1) zusammengefaßt. Jede dieser Einstellungen wird als Zustand bezeichnet. Es ist zudem nützlich, die wichtigsten Auswirkungen des Normalbetriebes in einem Apparateschema (Abb. 2) eintragen zu können (siehe insbesondere die Abschnitte 4.1, 4.2).

Der Photometer-Leitfähigkeitsmeßstand erhält zur Erhöhung der Sicherheit noch folgende Komponenten:

Puffergefäße: Sie werden im Normalbetrieb nicht gebraucht und kommen in Tab. 1 nicht vor. Sie werden mit PU1, PU2, PU3, PU4 bezeichnet (vgl. Abb. 1) und liegen an folgenden Stellen:

PU1 zwischen V1, PTR und V8 (Abluft),
PU2 zwischen LFZ und V5 (Abluft),
PU3 zwischen LFZ und V6 (Abluft),
PU4 zwischen KÜV und V7 (Abluft), (siehe Abb. 2).

Feuchtefühler: Sie werden im Normalbetrieb immer gebraucht und können die automatische Ablaufsteuerung beeinflussen. Sie liegen an folgenden Stellen:

L1 und L3 zwischen LFZ und PU2,
L2 zwischen KÜV und PU4,
L4 zwischen PTR, PU1 und V1 (siehe Abb. 2).

Die automatische Ablaufsteuerung (mit den Einzelschritten der Phasen Messen, Spülen, Blasen) ist durch eine Diagnose gestützt. Bei allen Komponenten wird ein Ist/Soll-Vergleich gemacht. So wird z.B. bei zwei möglichen Einstellungen eines Zweiwegventils (a/b) jede Abweichung vom Sollwert durch ein Diagnoseelement erkannt. Weicht der Ist-Wert vom programmierten Soll-Wert ab, so bricht eine automatische Ablaufsteuerung den Meßvorgang ab. Diese Soll-Werte sind alle in Tab. 1 gegeben. Außerdem existiert für jeden Analysenschritt eine Zeitschranke. Nach deren Ablauf ohne Erreichen des Soll-Zustandes wird ein Fehler gemeldet. Diese und ähnliche Gesichtspunkte werden in dieser Arbeit nicht weiter verfolgt. Sie gehören ins Gebiet der Fehlerdiagnose.

Alle relevanten Schritte (Zustände) des Analysenablaufs sind in der Ablauftabelle (Tab. 1) wiedergegeben.

Analysen-		Nr.	V e n t i l e								Feuchtefühler			
Phase	Zustand		V1	V2	V3	V4	V5	V6	V7	V8	L1	L2	L3	L4
	Grundzust.	1	a	a	b	-	offen	b	a	b	O	O	O	O
MESSEN	LFZ füllen	2	b	a	b	-	offen	b	a	a	O→1	O	O→1	1
	LFZ voll	3	a	a	b	-	offen	b	a	b	1	O	1	O
	KÜV füllen	4	b	b	b	-	offen	b	a	b	1→O	O→1	1→O	O
	KÜV voll	5	a	a	b	-	offen	b	a	b	O	1	O	O
	KÜV leeren	6	a	a	b	-	offen	b	b	b	O	1→O	O	1
	KÜV leer	7	a	a	b	-	offen	b	a	b	O	O	O	O
SPÜLEN	LFZ füllen	8	a	a	a	-	offen	b	a	b	O→1	O	O→1	O
	LFZ voll	9	a	a	b	-	offen	b	a	b	1	O	1	O
	KÜV füllen	10	b	b	b	-	offen	b	a	b	1→O	O→1	1→O	O
	KÜV voll	11	a	a	b	-	offen	b	a	b	O	1	O	O
	KÜV leeren	12	a	a	b	-	offen	b	b	b	O	1→O	O	1
	KÜV leer	13	a	a	b	-	offen	b	a	b	O	O	O	O
	wie 8	14												
	wie 9	15												
	LFZ-V2-V1	16	b	a	b	-	offen	b	a	b	1→O	O	1→O	1
	LFZ leer	17	a	a	b	-	offen	b	a	b	O	O	O	O
BLASEN	V6-V3-LFZ -PTF	18	b	a	b	-	geschl.	a	a	b	O	O	O	O
	V6-LFZ-KÜV-V7	19	b	b	b	-	geschl.	a	a	b	O	O	O	O
	V6-LFZ-PU2-V5	20	a	a	b	-	offen	a	a	b	O	O	O	O

- Die Bezeichnung O→1 bedeutet: Der Wert, den der Feuchtefühler anzeigt, ändert sich von O auf 1.

Tab. 1: Ablauftabelle (nach /1/).

3. Fehlerbaumanalyse (FBA)

Es entsteht für den Photometer-Leitfähigkeitsmeßstand folgende Frage:

Bei welchen Ausfällen einzelner Geräteteile kann es zu gefährlichen Situationen bzw. zu Verfälschungen der Meßergebnisse kommen? Die Überlegungen liegen mehr auf logischer als auf gerätetechnischer Ebene. Zahlenangaben über Zuverlässigkeitskenngrößen waren dabei noch nicht verfügbar.

Es ist jedoch möglich, diese Frage durch eine (qualitative) Fehlerbaumanalyse zu beantworten (siehe /2/, /3/, /4/, /5/). Auch soll nicht die FBA von /1/ in allen Einzelheiten nachvollzogen werden. Es scheint jedoch wichtig, im Zusammenhang mit unserer Fragestellung auf einige spezielle Punkte einzugehen.

Zum Aufbau eines Fehlerbaums ist eine gefährliche Situation ("Unerwünschtes Ereignis" (UE)) zu definieren. Dazu sind dann Ursachen zu suchen. Dafür kommt in Frage:

> "Überfließen eines Puffers (PU1 oder PU2 oder PU3 oder PU4) mit Flüssigkeit, die radioaktive Bestandteile enthalten kann" (UE).

Einschränkung auf qualitative Untersuchungen

Es zeigte sich, daß eine quantitative Analyse (die Ausfallwahrscheinlichkeiten ergeben würde) beim heutigen Kenntnisstand noch nicht möglich ist /1/. Natürlich kann man trotzdem sehen, wo z.B. das Einzelfehlerkriterium zutrifft, was bereits eine Beurteilung erlaubt und Verbesserungen möglich macht /5/.

Beim "Einzelfehlerkriterium" handelt es sich um die Frage, ob bereits der Ausfall eines Bauelements zum Systemausfall führen kann. Ist dies der Fall, so sagt man, das Einzelfehlerkriterium sei erfüllt.

Es ist besonders zu beachten, daß für jeden einzelnen Analysenzustand ein Unterbaum entsteht. Es gibt dann wenigstens eine kritische Menge von Komponenten, die in einem Analysenzustand notwendig und hinreichend zum Systemausfall ist. Sie ist minimal (eine kleinere Menge von Komponenten würde keinen Systemausfall ergeben). Diese Menge wird auch Minimalschnitt genannt. Wir stellen fest: Jeder Minimalschnitt kann nur in einem bestimmten Prozeßschritt

(Analysenzustand i) auftreten. Während dieses Prozeßschritts sind auch andere Ausfallkombinationen möglich, die zu anderen Unerwünschten Ereignissen führen.

3.1 Beispiele der Fehlerbaumanalyse (FBA)

Wir zeigen - von zwei Analysenzuständen (Nr. 4, Nr. 5 der Tab. 1) ausgehend - die FBA. Alle Analysenzustände im Normalbetrieb wurden in Tab. 1 wiedergegeben.

Als Unerwünschte Ereignisse definieren wir:

{PU1} = Puffer 1 fließt über
{PU2} = Puffer 2 fließt über
{PU3} = Puffer 3 fließt über
{PU4} = Puffer 4 fließt über .

Es zeigte sich, daß {PU3} nur in einem wenig plausiblen Zusammenhang vorkommen kann. Wir bringen {PU3} nicht weiter in unserer Darstellung /1/.

Als Zustände nehmen wir hier an:

Nr. 4, MESSEN, KÜV füllen (Abb. 3)
Nr. 5, MESSEN, KÜV voll (Abb. 4) (Tab. 1) .

{PU1} - Ursachen (Abb. 5)

Im Zustand Nr. 4 erhalten wir als Ursache für {PU1}:

Übergehen von V3 auf a (kurz 3a) und
Übergehen von V2 auf a (kurz 2a) und
Ausfall von L4 (Nichtanzeigen der Feuchtigkeit), (kurz L4) .

Konvention

Für dieses Ereignis verwenden wir von jetzt ab die folgende Schreibweise:

{3a und 2a und L4} = 3a·2a·L4 .

Im Zustand Nr. 5 erhalten wir als Ursache für {PU1}:

{3a und 1b und L4} = 3a·1b·L4 .

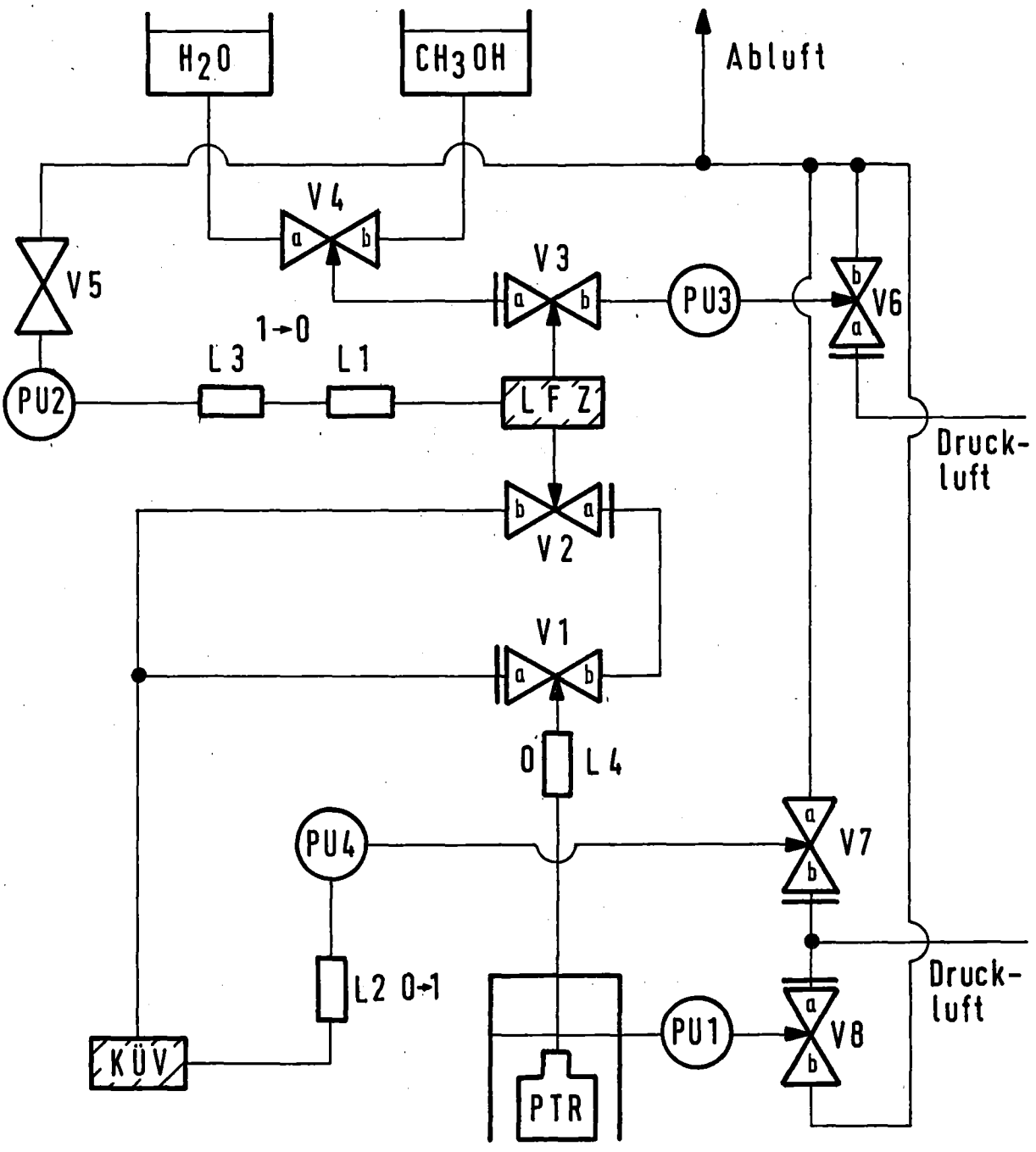


Abb. 3: MESSEN, KÜV füllen, Nr. 4.

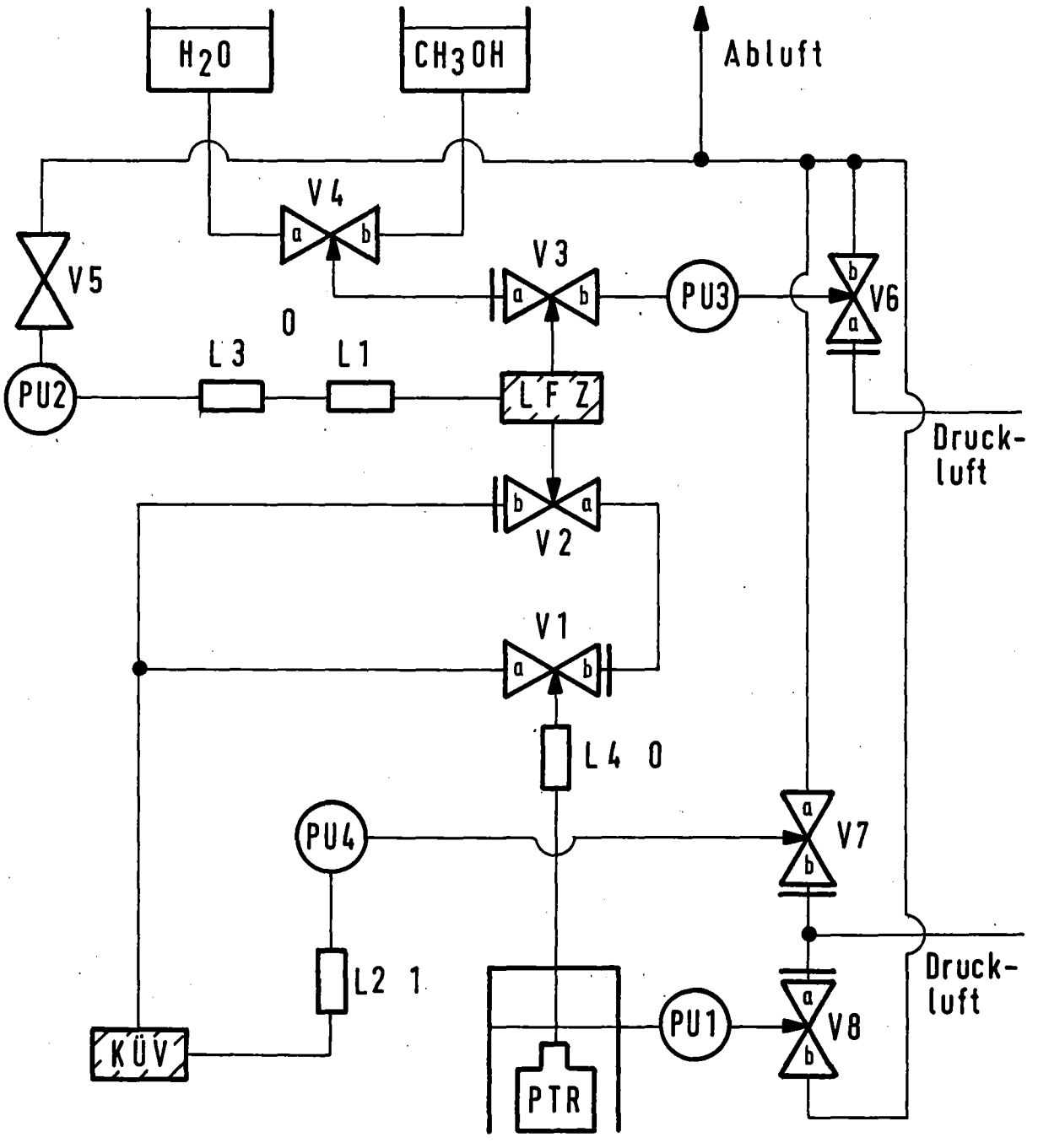


Abb. 4: MESSEN, KÜV voll, Nr. 5.

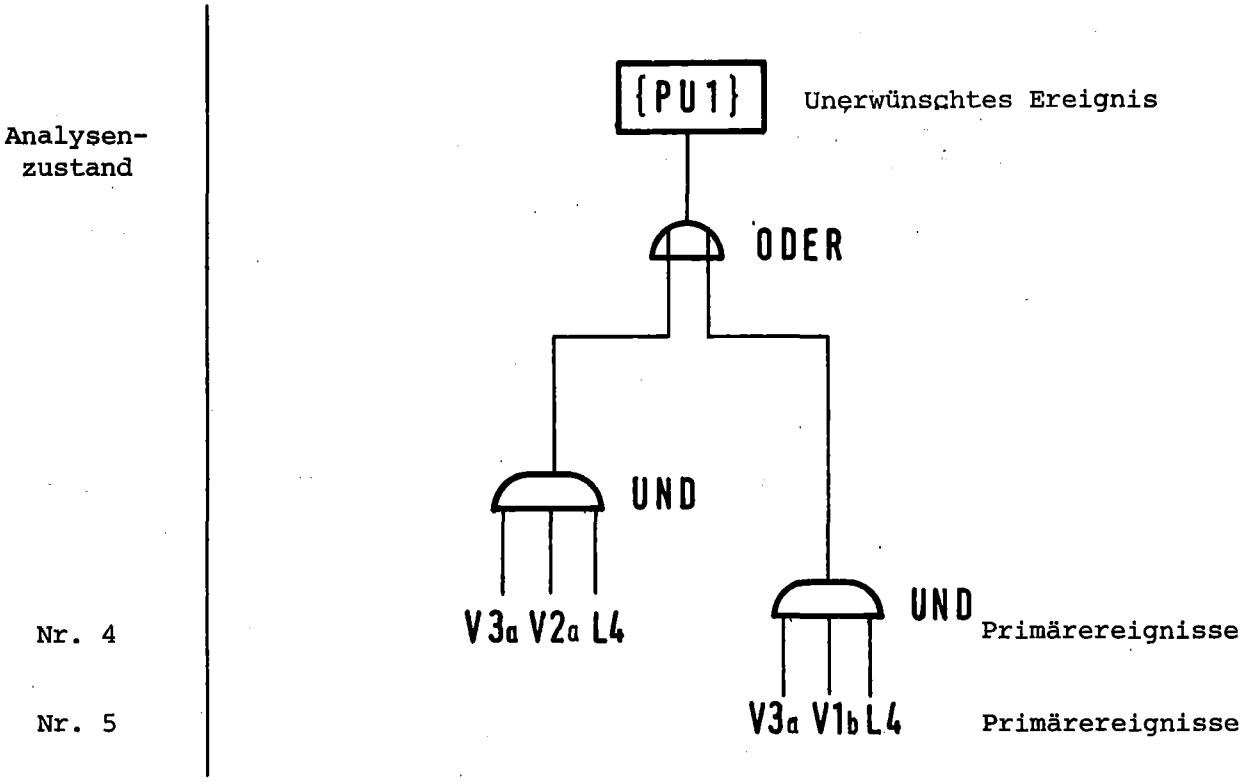


Abb. 5: Teilergebnis für {PU1} (Zustände Nr. 4, 5).

{PU2} - Ursachen (Abb. 6)

Im Zustand Nr. 4 erhalten wir als Ursache für {PU2}:

Übergehen von V3 auf a (kurz 3a) und
Übergehen von V2 auf a (kurz 2a) und
Übergehen von V1 auf a (kurz 1a) .

Also

{3a und 2a und 1a} = 3a·2a·1a .

(L1, L3 zeigen im Normalbetrieb Feuchte an, sie können nicht wie bei 3a·2a·L4 zu {PU2} beitragen.)

Im Zustand Nr. 5 erhalten wir als Ursache für {PU2}:

{3a und L1 und L3} = 3a·L1·L3 .

(L1, L3 zeigen im Normalbetrieb keine Feuchte an. Wird nach Übergang von V3 auf a von L1, L3 Feuchte gemeldet, so wird {PU2} verhindert.)

{PU4} - Ursachen (Abb. 7)

Im Zustand Nr. 4 erhalten wir als Ursache für {PU4}:

Übergehen von V3 auf a (kurz 3a) und
Ausfall von L2 (Nichtanzeigen der Feuchtigkeit) (kurz L2) .

Also

{3a und L2} = 3a·L2 .

Im Zustand Nr. 5 erhalten wir als Ursache für {PU4}:

{3a und 2b} = 3a·2b .

Dies führt mit den Abbildungen (Abb. 3, Abb. 4) zu folgenden Fehlerbäumen (Abb. 5, Abb. 6, Abb. 7), die Teilbäume der Fehlerbäume für {PU1}, {PU2}, {PU4} (Abb. 8, Abb. 9, Abb. 10) sind.

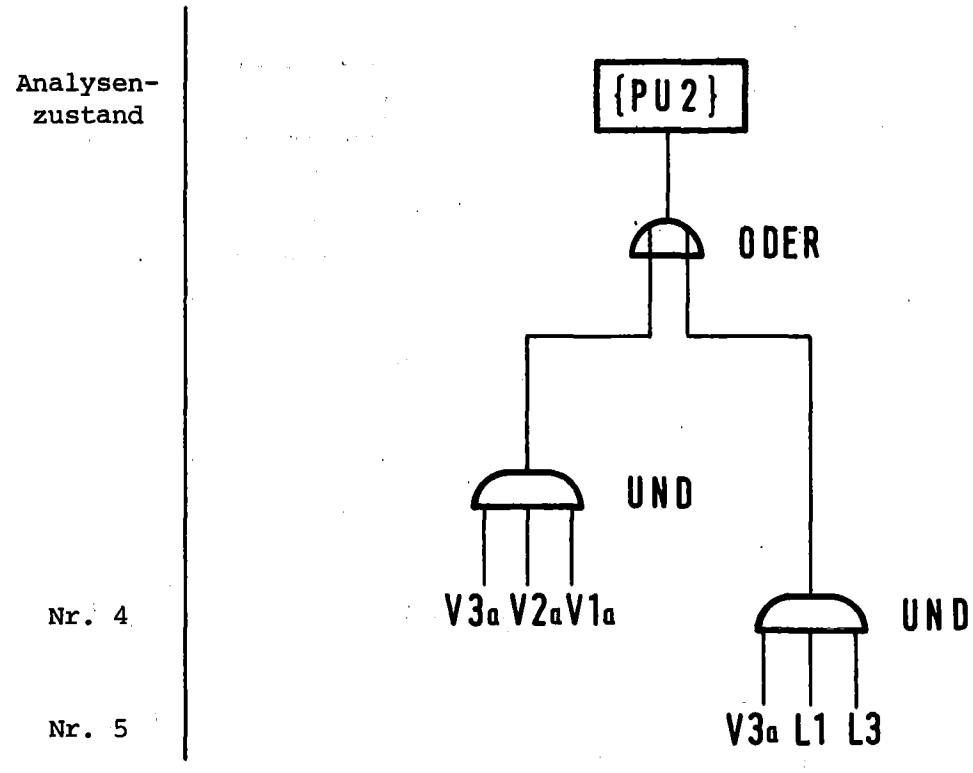


Abb. 6: Teilergebnis für {PU2} (Zustände 4, 5).

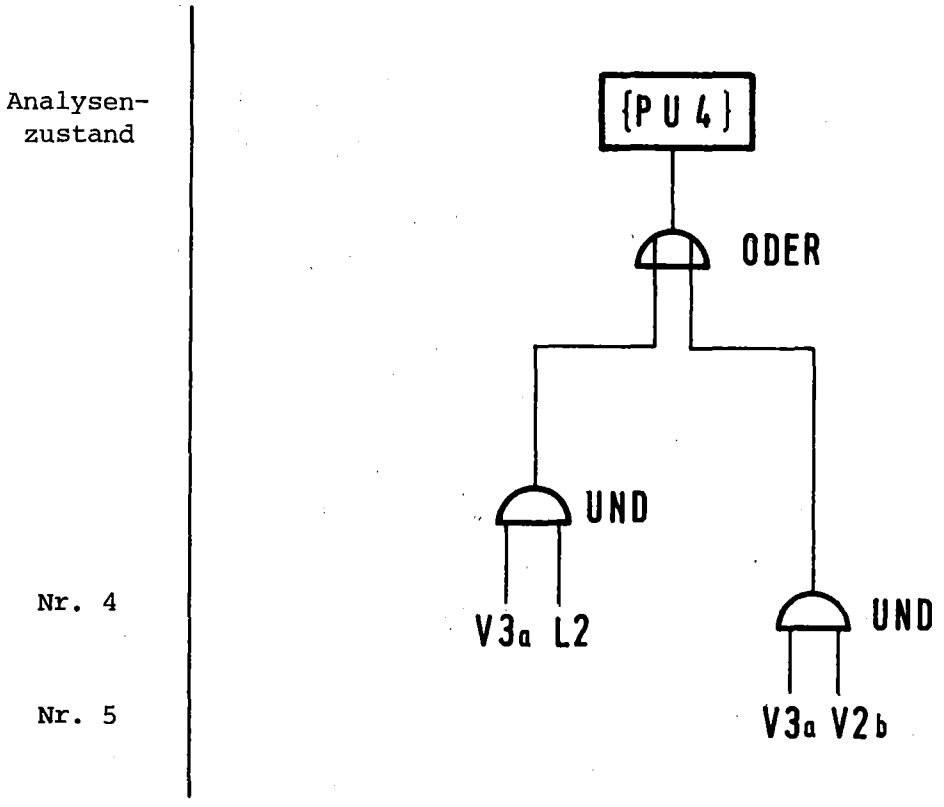


Abb. 7: Teilergebnis für {PU4} (Zustände Nr. 4, 5).

3.2 Zusammenfassung der Resultate

Wir fügen die in 3.1 besprochenen Beispiele in den Gesamtzusammenhang ein. Wir geben Fehlerbäume für folgende Unerwünschte Ereignisse

{PU1} = Puffer 1 läuft über,

{PU2} = Puffer 2 läuft über,

{PU4} = Puffer 4 läuft über,

in Abhängigkeit von den in den einzelnen Analysenphasen (MESSEN, SPÜLEN, BLASEN) vorkommenden Analysenzuständen (Abb. 8, Abb. 9, Abb. 10).

Diese Fehlerbäume zeigen i.a. folgendes /1/:

- "Ventil V3 geht (ohne Anforderung) auf a" ist ein Ausfall, der bei den meisten Minimalschnitten beteiligt ist. Das einwandfreie Funktionieren von V3 ist also von entscheidender Wichtigkeit.
- Für verschiedene Analysenzustände gibt es im allgemeinen keine gleichen Minimalschnitte.

Eine ausführliche Darstellung aller Ausfallkombinationen ist in Tab. 2 zu finden. Tab. 2 faßt die Resultate der Abschnitte 3 und 4 zusammen und ist der Ausgangspunkt für die methodischen Betrachtungen in Abschnitt 5.

Analysenphase bzw. -zustand	Nr.
MESSEN	
Füllen der LFZ mit Probenfl.	2
KÜV voll	5
Leeren d. KÜV in PTF	
SPÜLEN	
KÜV voll	11
KÜV leeren	12
LFZ-V2-V1	16

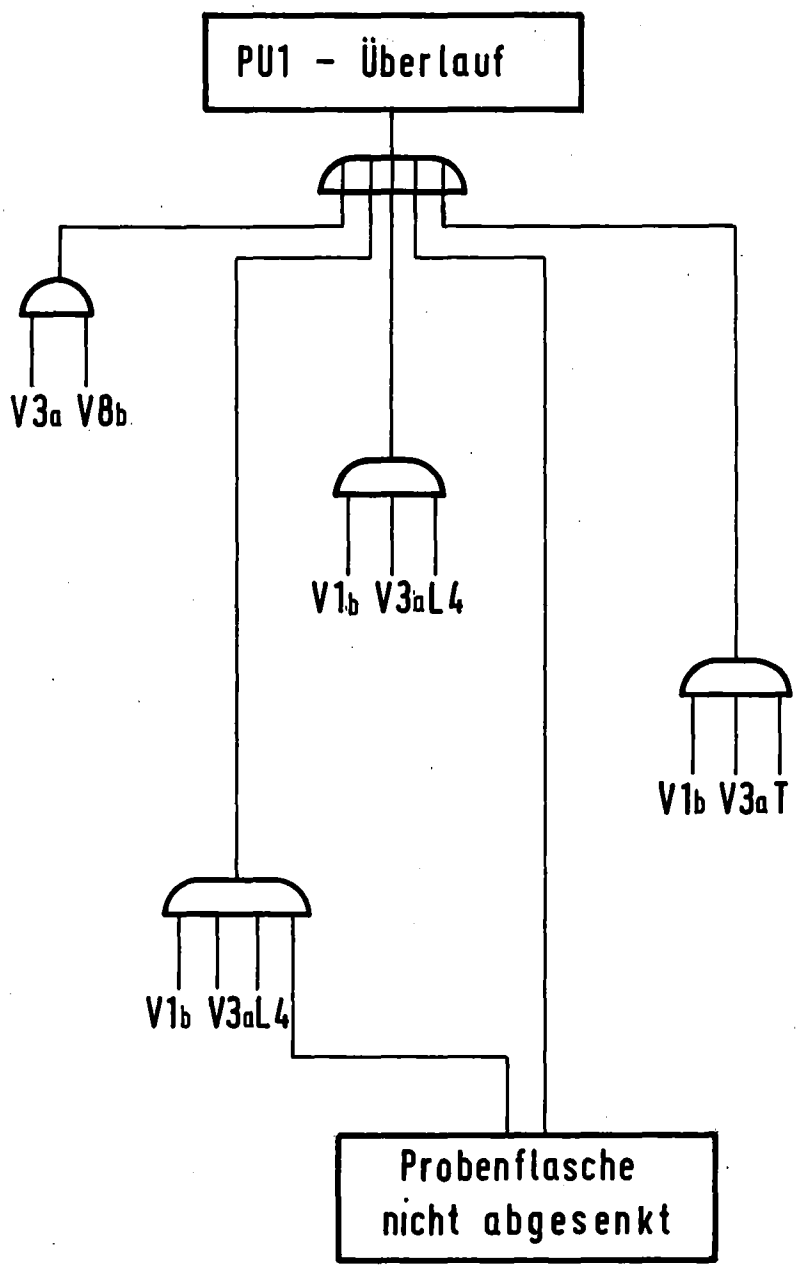
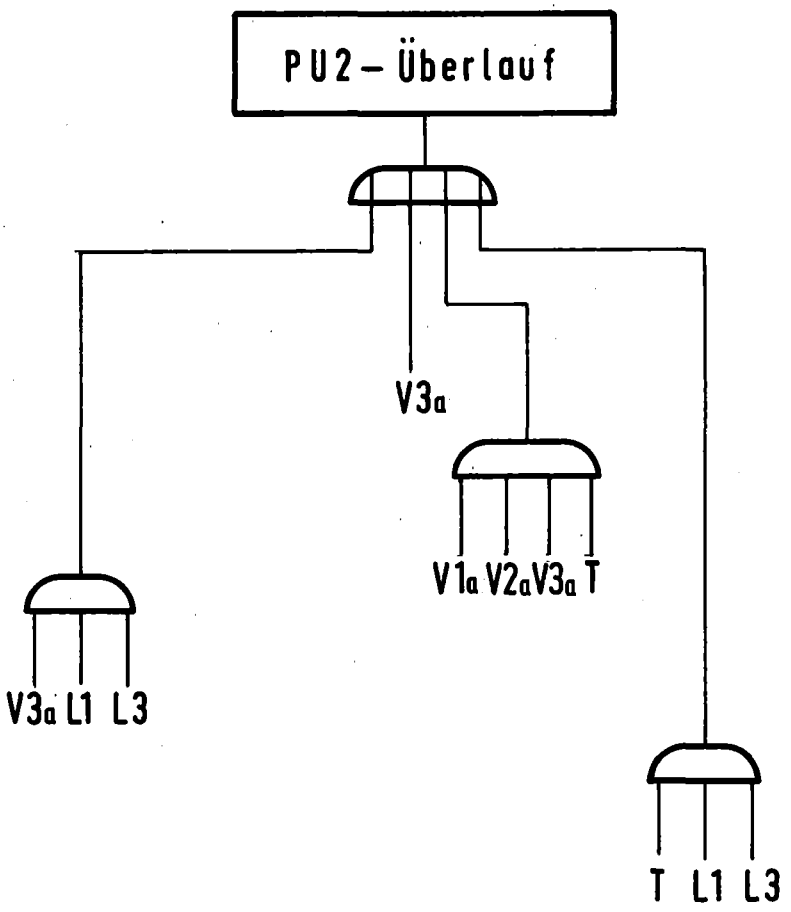


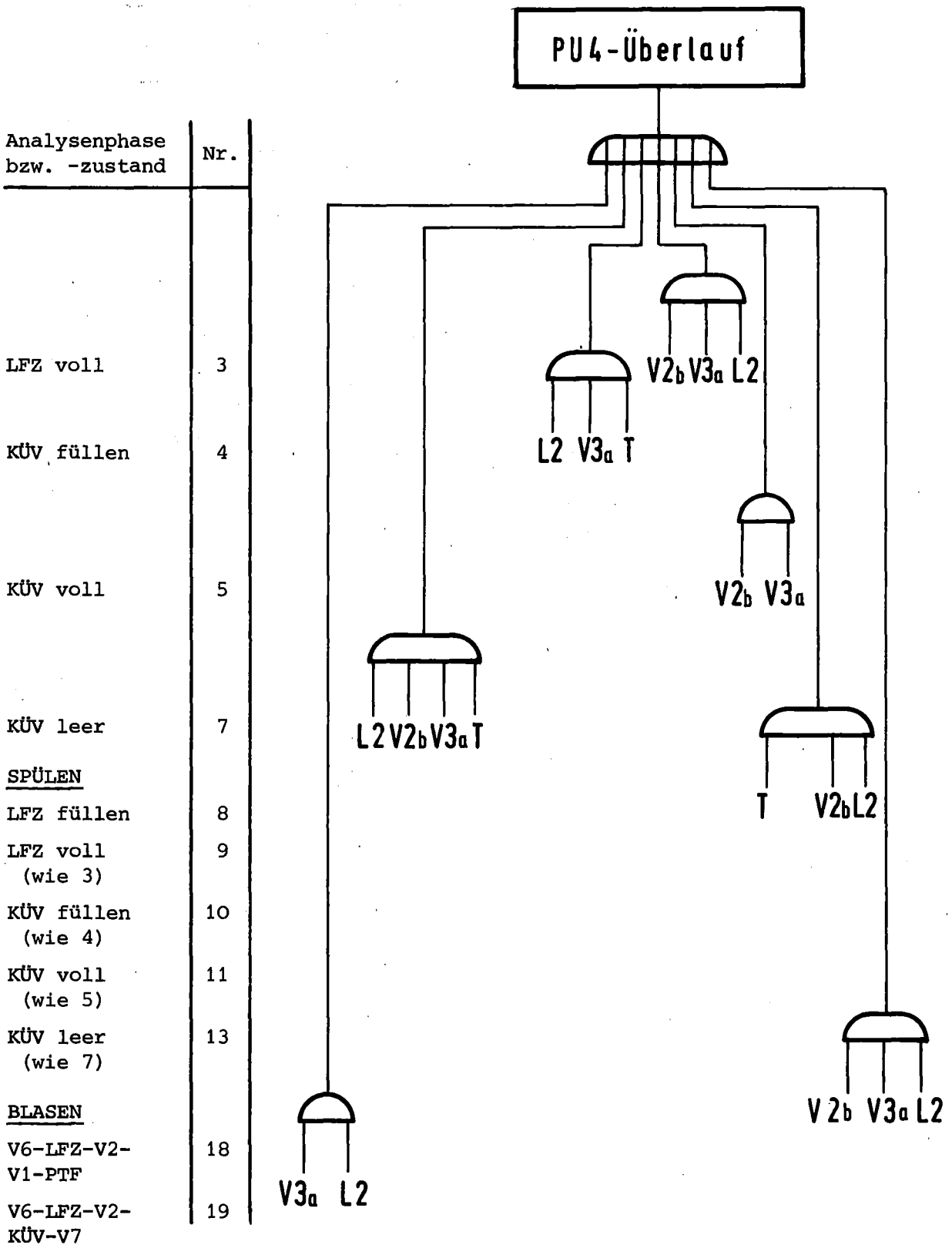
Abb. 8: Fehlerbaum für den Überlauf von Puffer 1

Analysenphase bzw. -zustand	Nr.
MESSEN	
LFZ füllen	2
LFZ voll	3
KÜV füllen	4
KÜV voll	5
KÜV leeren	6
KÜV leer	7
SPÜLEN	
LFZ füllen	8
LFZ voll (wie 3)	9
KÜV füllen (wie 4)	10
KÜV voll (wie 5)	11
KÜV leeren (wie 6)	12
KÜV leer (wie 7)	13
Spülen Ende (wie 7)	17
BLASEN	
V3-LFZ-PU2-V5 (wie 7)	20



Zustände sind äquivalent mit den entsprechenden Zuständen in der Meßphase.

Abb. 9: Fehlerbaum für den Überlauf von Puffer 2.



Analysenphase bzw. -zustand	Nr.
LFZ voll	3
KÜV füllen	4
KÜV voll	5
KÜV leer	7
SPÜLEN	
LFZ füllen	8
LFZ voll (wie 3)	9
KÜV füllen (wie 4)	10
KÜV voll (wie 5)	11
KÜV leer (wie 7)	13
BLASEN	
V6-LFZ-V2-V1-PTF	18
V6-LFZ-V2-KÜV-V7	19

Abb. 10: Fehlerbaum für den Überlauf von Puffer 4

4. Störfallanalyse

Die in Abschnitt 2 beschriebene Anlage (Photometer-Leitfähigkeitsmeßstand) wird nunmehr aus folgenden Gründen einer Störfallanalyse unterworfen:

- Es soll eine Kontrolle der FBA des Abschnitts 3 durchgeführt werden.
- Es können methodische Überlegungen zum Zusammenhang von Fehlerbäumen und Störfalldiagrammen ausgeführt werden (siehe Abschnitt 5).
- Es können Überlegungen zur Vereinfachung von Störfallanalysen gezeigt werden (siehe Abschnitt 6.2).

Die Störfallanalyse wurde an verschiedenen Stellen ausführlich dargestellt (z.B. /4/, /7/, /8/, /9/).

Zum Aufbau eines Störfalldiagramms ist ein geeignetes Anfangsereignis festzulegen. Dafür kommt nach den Ergebnissen der FBA in Frage:

"Ventil V3 geht auf a (ohne Anforderung)"

Dieses Ereignis ist plausibel. Man ersieht aus Abschnitt 3.2, daß der Ausfall V3a in den meisten Minimalschnitten beteiligt ist (vgl. Abb. 8 bis 10). Dann hat man nach möglichen Folgeereignissen zu suchen. Wenn es nur um Kombinationen, von Ereignissen, aber nicht um Ursache/Wirkungsbeziehungen geht, so kann man grundsätzlich auch ein anderes Ereignis als Anfangsereignis wählen.

Dann hat man nach möglichen Folgeereignissen (bzw. Kombinationen von Ereignissen) zu suchen. Dabei sind diejenigen zu beachten, die zu gefährlichen Auswirkungen führen können.

Mögliche Einschränkung auf qualitative Untersuchungen

Im Gegensatz zur FBA liegt bei der Störfallanalyse der Schwerpunkt auf qualitativen Analysen oder auf Handrechnungen.

Im allgemeinen ist auf die Ursache/Wirkungsbeziehung und die Reihenfolge von Ereignissen zu achten. Für unsere Problemstellung ist jedoch vor allem nach Kombinationen von Fehlern gefragt.

Es ist zu bemerken, daß für jeden Analysenzustand genau ein Störfalldiagramm

das Ausfallverhalten beschreibt. Störfalldiagramme, die für verschiedene Zustände zum gleichen Endereignis führen sind jedoch möglich.

Wir bringen nun Beispiele für die Störfallanalyse (4.1) mit

- einer verbalen Beschreibung des Störfalls,
- einer Darstellung mittels eines Apparateschemas,
- einer Darstellung im Störfalldiagramm.

4.1 Beispiele der Störfallanalyse

Wir führen für zwei Zustände (Nr. 4, 5) eine Störfallanalyse durch (vgl. Abb. 13, 14).

Es zeigt sich, daß die Anwendung der Störfallanalyse leicht zu sehr großen Diagrammen führen kann (durch die möglichen Verzweigungen des Störfalldiagramms). Unter bestimmten Bedingungen, die in den Abschnitten 5 und 6 noch genauer ausgeführt werden sollen, läßt sich eine Vereinfachung der Störfallanalyse erreichen. Wir führen mögliche Vereinfachungen jedoch schon hier durch, ohne damit relevante Ergebnisse zu verlieren.

Als Anfangsereignis für die Störfallanalysen legen wir fest:

"Ventil V3 geht auf a (ohne Anforderung)"

Dieses Anfangsereignis wird mit 3a abgekürzt (vgl. Abb. 13, 14).

Wir untersuchen den Analysenstand in folgenden Zuständen:

Zustand Nr. 4 MESSEN, KÜV füllen (Abb. 11) .

(a) Wenn V3 auf a geht, so kann (durch Schwerkraft) die Spülflüssigkeit nach PU4 gelangen. Wenn L2 ausgefallen ist, so kann der Fehler nicht erkannt werden und somit wird keine Gegenmaßnahme automatisch eingeleitet. PU4 fließt über, kurz {PU4}.

(b) Wenn V3 auf a geht, sowie V2 auf a geht, so kann die Spülflüssigkeit nach PU1 gelangen. Wenn L4 ausgefallen ist, so wird keine Gegenmaßnahme

automatisch eingeleitet.
PU1 fließt über, kurz {PU1}.

(c) Wenn V3 auf a geht, sowie V2 auf a und V1 auf a gehen, so können L1, L3 keine Gegenmaßnahmen einleiten, da sie schon im Normalfall Feuchte anzeigen.
PU2 fließt über, kurz {PU2}.

(d) Da durch den Zweiweghahn V3 ein Übergang vom Spülflüssigkeitsbehälter nach PU3 unmöglich ist, können wir {PU3} ausschließen.

Wir fassen (a) - (d) kurz zusammen (vgl. Abb. 13):

{PU4}	{PU1}	{PU2}
3a·L2	3a·2a·L4	3a·2a·1a

Zustand Nr.5 MESSEN, KÜV voll (Abb. 12)

(a) Wenn V3 auf a geht, so kann die Spülflüssigkeit nach PU4 gelangen. Da KÜV voll ist, kann L2, das schon im Normalfall Feuchte anzeigt, keine Gegenmaßnahmen einleiten.
PU4 fließt über, kurz {PU4}.

(b) Wenn V3 auf a geht, sowie V1 auf b geht, so kann Spülflüssigkeit nach PU1 gelangen. Wenn L4 ausgefallen ist, so kann der Fehler nicht erkannt werden und somit wird keine Gegenmaßnahme automatisch eingeleitet.
PU1 fließt über, kurz {PU1}.

(c) Wenn V3 auf a geht, so kann Spülflüssigkeit nach PU2 gelangen. Wenn L1, L3 ausgefallen sind, kann der Fehler nicht erkannt werden und somit wird keine automatische Gegenmaßnahme eingeleitet.
PU2 fließt über, kurz {PU2}.

(d) Kein Folgen für PU3.

Wir fassen (a) - (d) kurz zusammen (vgl. Abb. 14):

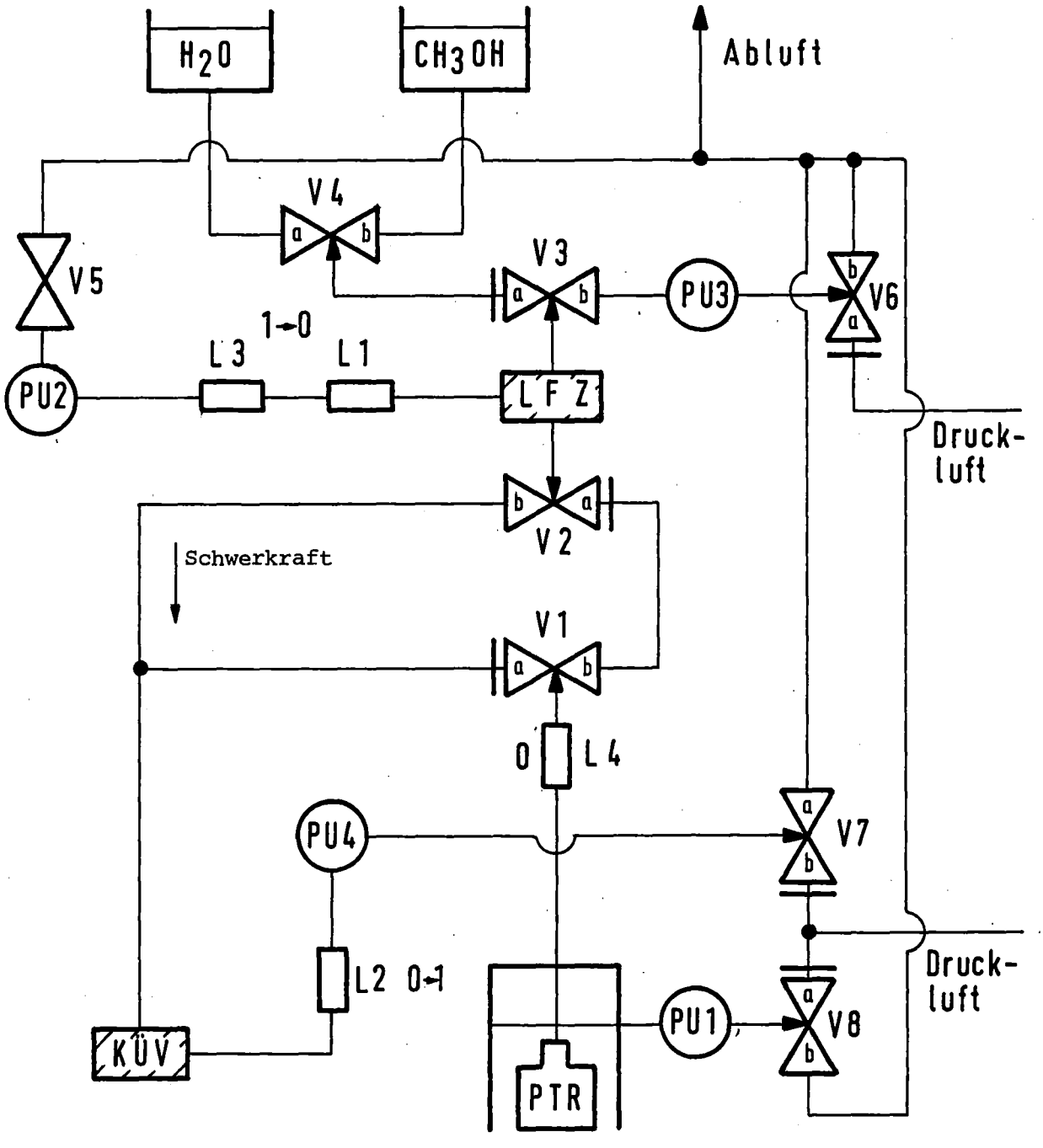


Abb. 11: MESSEN, KÜV füllen, Nr. 4.

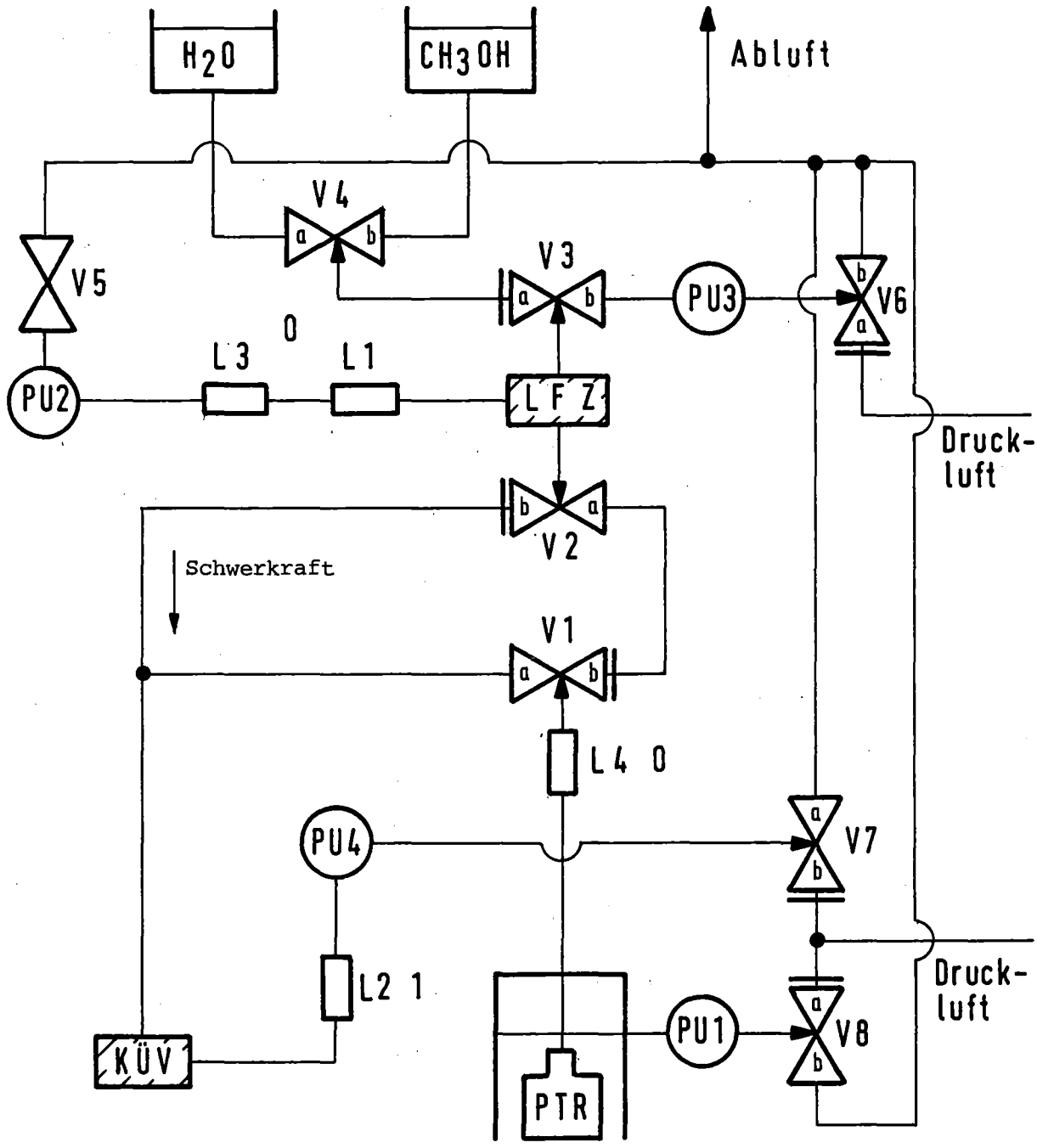
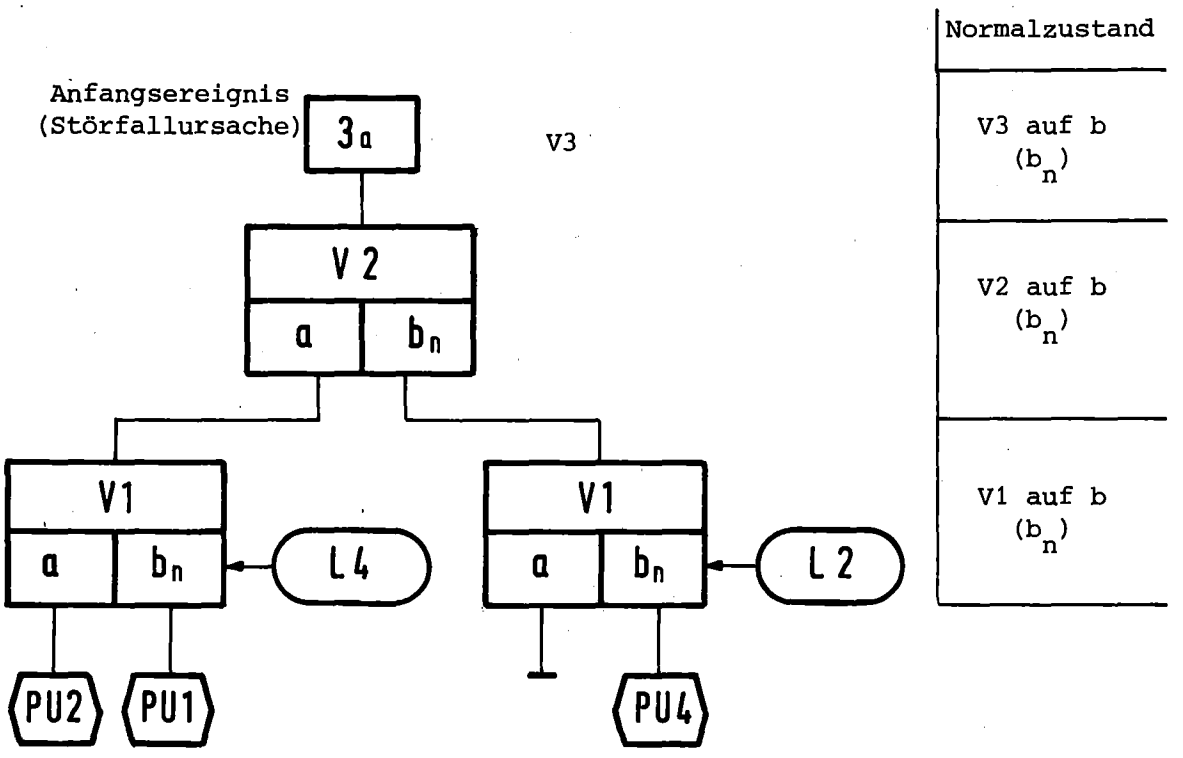


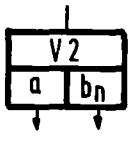
Abb. 12: MESSEN, KÜV voll, Nr. 5.



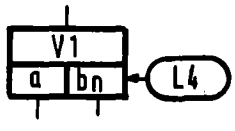
Bezeichnungen:

Anfangsereignis, Störfallursache

gefährliche Störfallauswirkungen



Verzweigung: Das Ventil kann entweder auf a oder auf b geschaltet sein. Dabei bezeichnet: a_n bzw. b_n (mit Index n) den Normalzustand und b bzw. a (ohne Index n) den Ausfallzustand.



Durch ←(L4) wird das Fehlen von Gegenmaßnahmen (z.B. bei Ausfall des Feuchtefühlers L4) gekennzeichnet.

Es erfolgt ein Abbruch des Störfalldiagramms, da keine Störfallauswirkung zu erwarten ist oder da die Auswirkung schon in einer kürzeren Ereignisfolge enthalten ist.

Abb. 13: Störfalldiagramm, Zustand Nr. 4, MESSEN, KÜV füllen.

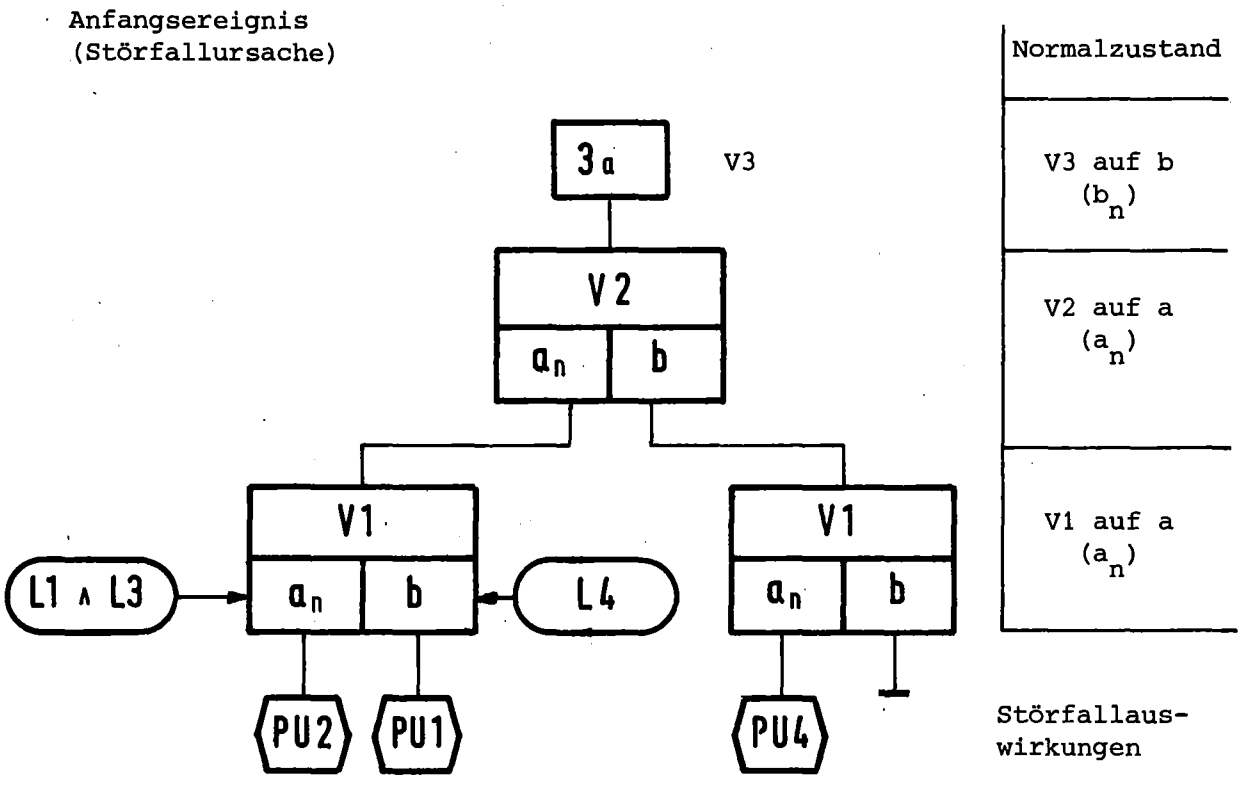


Abb. 14: Zustand Nr. 5 (MESSEN, KÜV voll).

Anmerkung:

Es zeigte sich, daß die Störfalldiagramme in vielen Zuständen der Analyse für bestimmte Teile gleichartig aufgebaut waren. Dies ist eine zusätzliche Kontrollmöglichkeit (siehe auch Tabelle 2 und Abschnitt 6.2).

{PU4}	{PU1}	{PU2}
3a·2b	3a·1b·L4	3a·L1·L3

Anmerkung:

Wir schreiben nur diejenigen Komponenten aus, die im Defektzustand sind. Diese Vereinfachung konnten wir bei der Zusammenfassung von Störfallereignissen zu Zustand Nr. 4 und Nr. 5 machen. Diese Vereinfachung werden wir auch bei unserer Zusammenfassung (Abschnitt 4.2) machen.

4.2 Zusammenfassung der Resultate der Störfallanalyse

Nach der Beschreibung einiger Störfallanalysen wollen wir alle Resultate zusammenfassen. Dabei gehen wir in zwei Schritten vor:

Zuerst geben wir für jeden Analysenzustand ein Apparateschema (Abb. 15-33) und zusätzliche Information:

Darin findet man

- Ein Apparateschema, das die Einstellung der Ventile und die Anzeige der Fühler zeigt.
- Den Analysenzustand
  (z.B. MESSEN, LFZ füllen, Nr. 2)
- Eine Zusammenfassung der für diesen Zustand möglichen Fehlerkombinationen, mit einer Bezeichnung der möglichen Auswirkungen:

  z.B.

{PU1}	{PU2}	{PU4}	Auswirkungen
3a·8b	3a	3a·2b·L2	Fehlerkombinationen

Daraus lassen sich in einer Kurzform alle möglichen Störfallabläufe entnehmen.

Dann fassen wir in Tab. 2 alle Resultate der Störfallanalyse zusammen. Daraus können wir methodische Schlüsse über den

Zusammenhang von Fehlerbaumanalyse und Störfallanalyse ziehen (siehe Abschnitt 5) sowie Regeln zur Vereinfachung der Störfallanalyse ableiten und illustrieren (siehe Abschnitt 6).

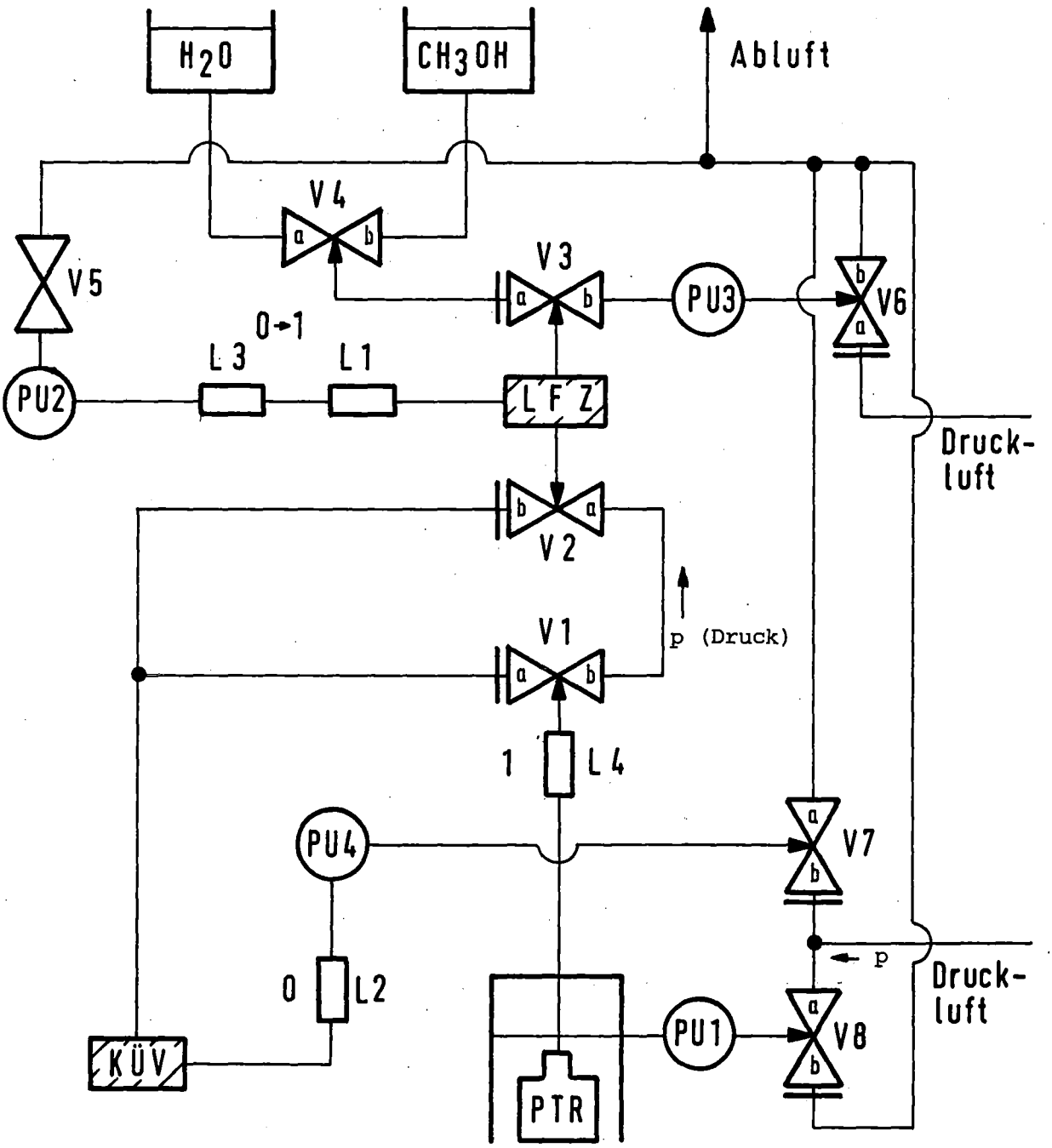


Abb. 15: MESSEN, LFZ füllen, Nr. 2.

{PU1}	{PU2}	{PU4}
3a·8b	3a	3a·2b·L2

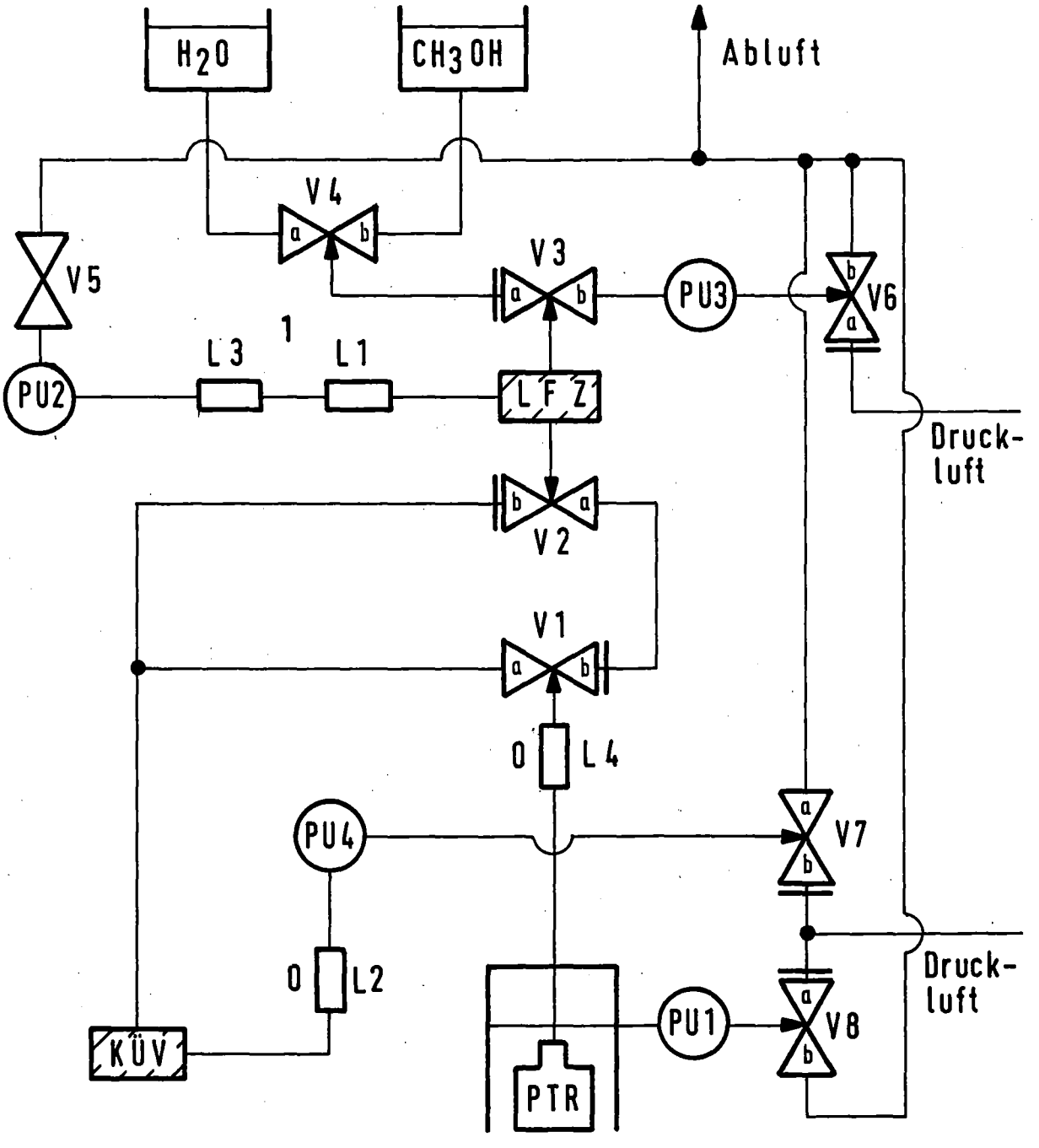


Abb. 16: MESSEN, LFZ voll, Nr. 3.

{PU1}	{PU2}	{PU4}
3a·1b·L4	3a	3a·2b·L2

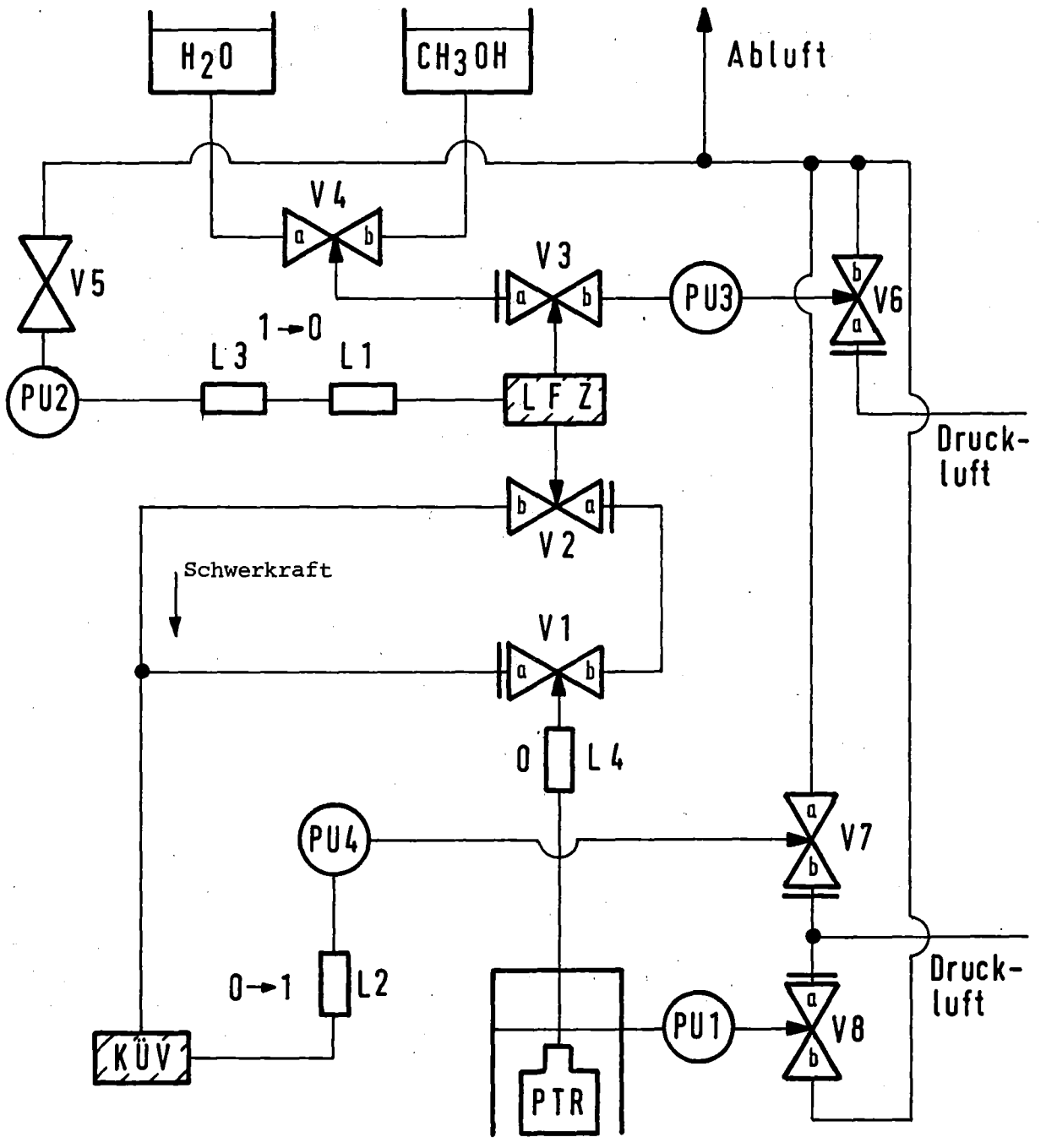


Abb. 17: MESSEN, KÜV füllen, Nr. 4

{PU1}	{PU2}	{PU4}
3a·2a·L4	3a·2a·1a	3a·L2

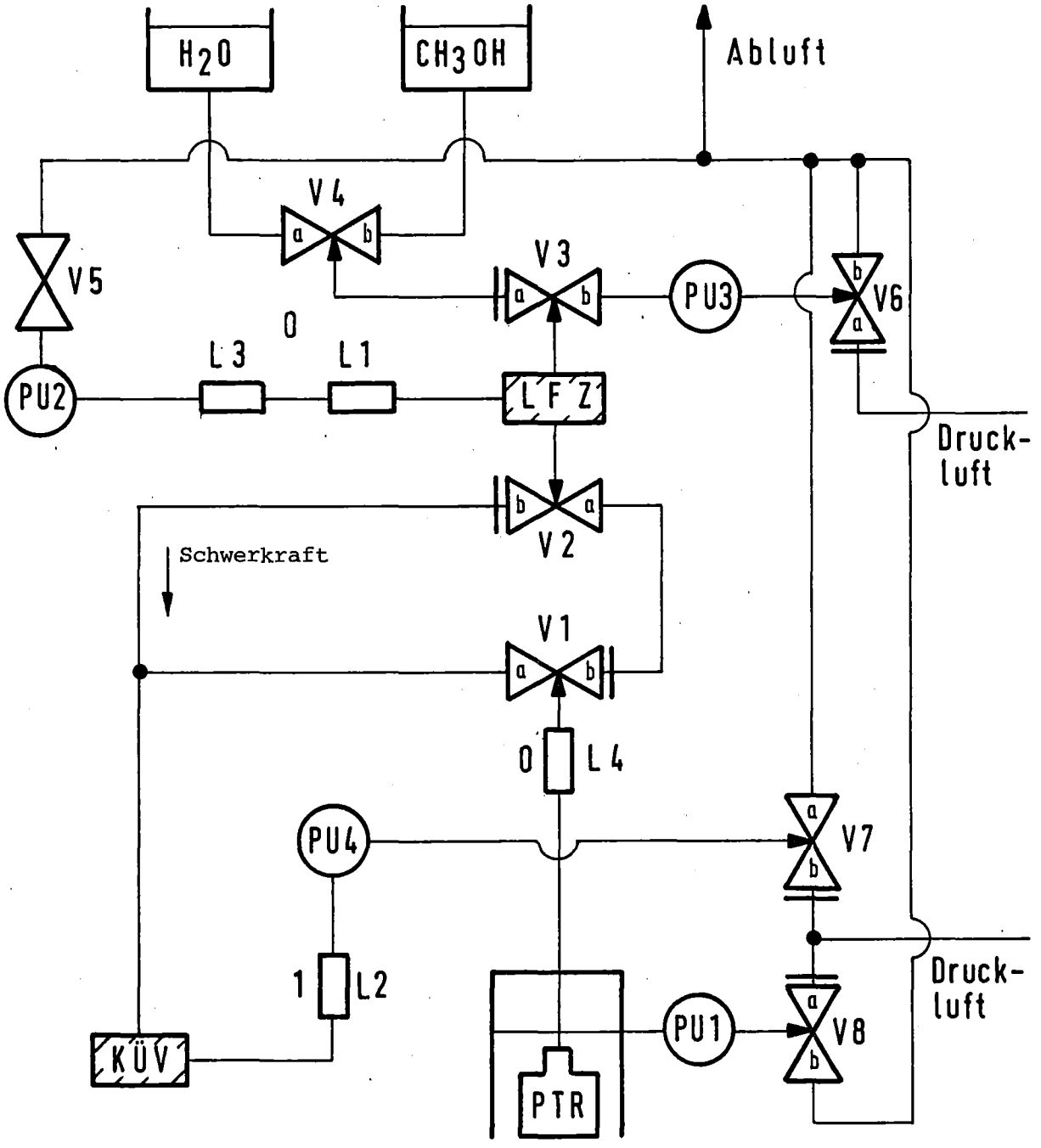


Abb. 18: MESSEN, KÜV voll, Nr. 5.

{PU1}	{PU2}	{PU4}
3a·1b·L4	3a·L1·L3	3a·2b

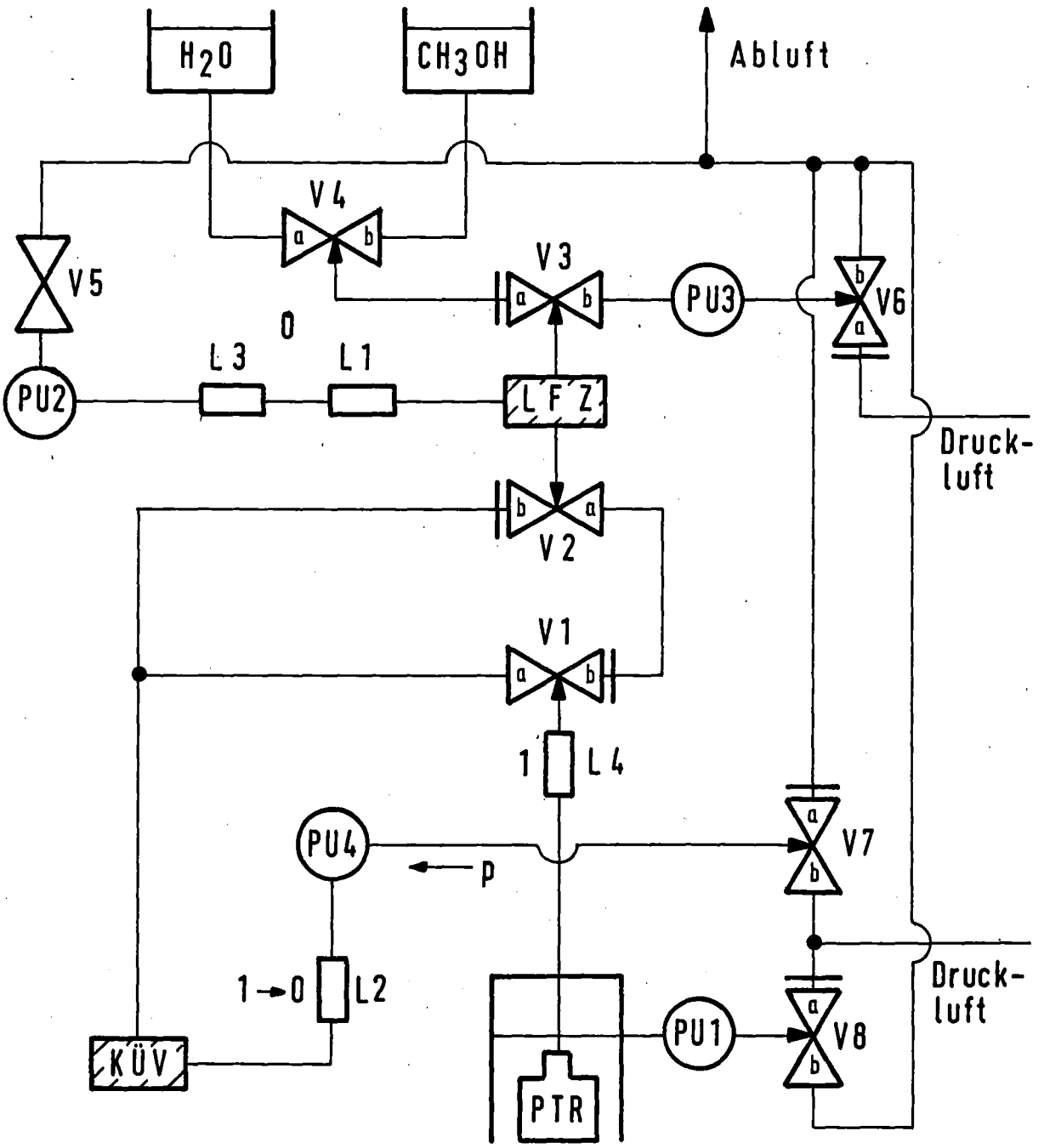


Abb. 19: MESSEN, KÜV leeren, Nr. 6.

{PU1}	{PU2}	{PU4}
3a·1b	3a·L1·L3	3a·2b·7a

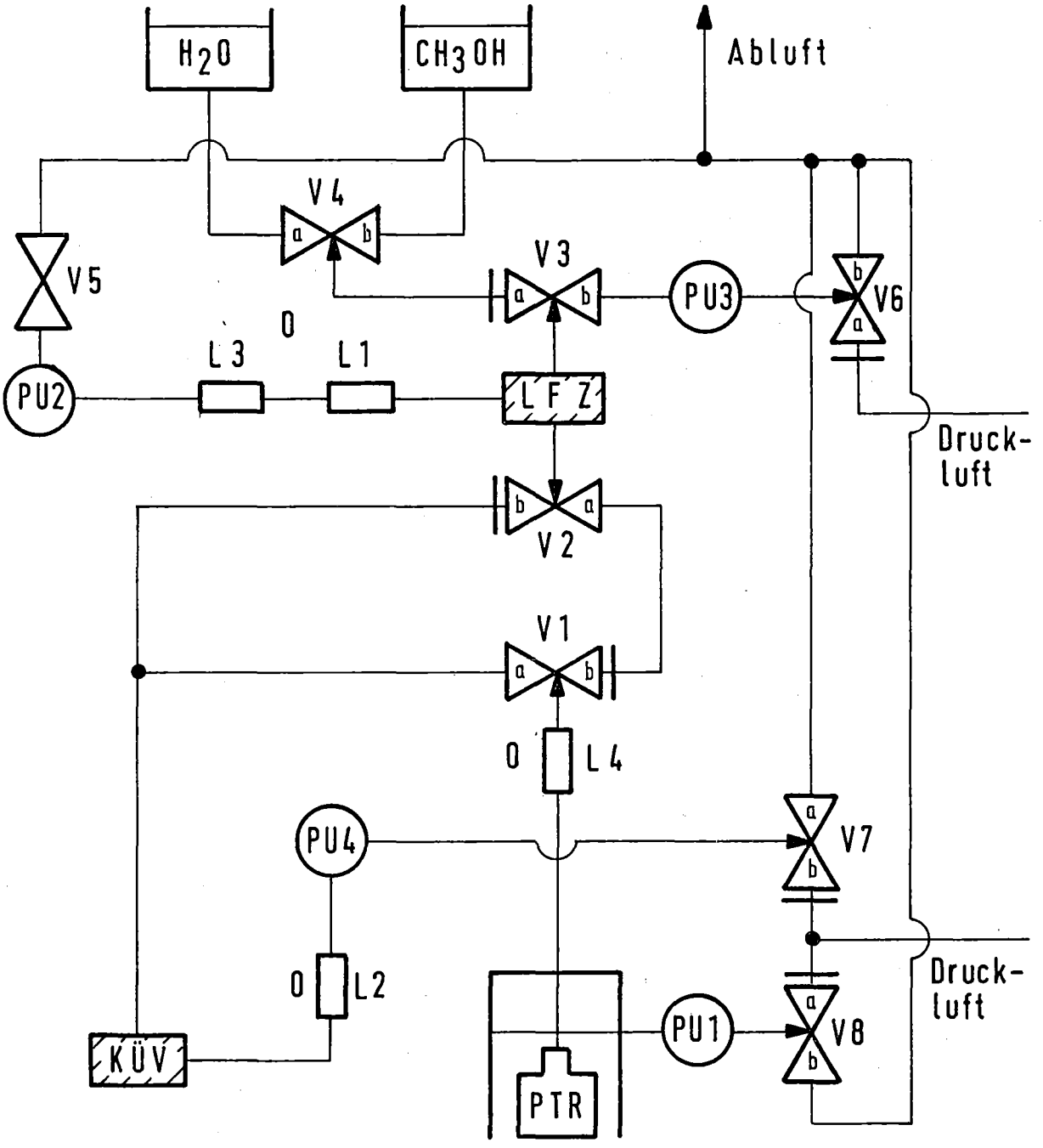


Abb. 20: MESSEN, KÜV leer, Nr. 7.

{PU1}	{PU2}	{PU4}
3a·1b·L4	3a·L1·L3	3a·2b·L2

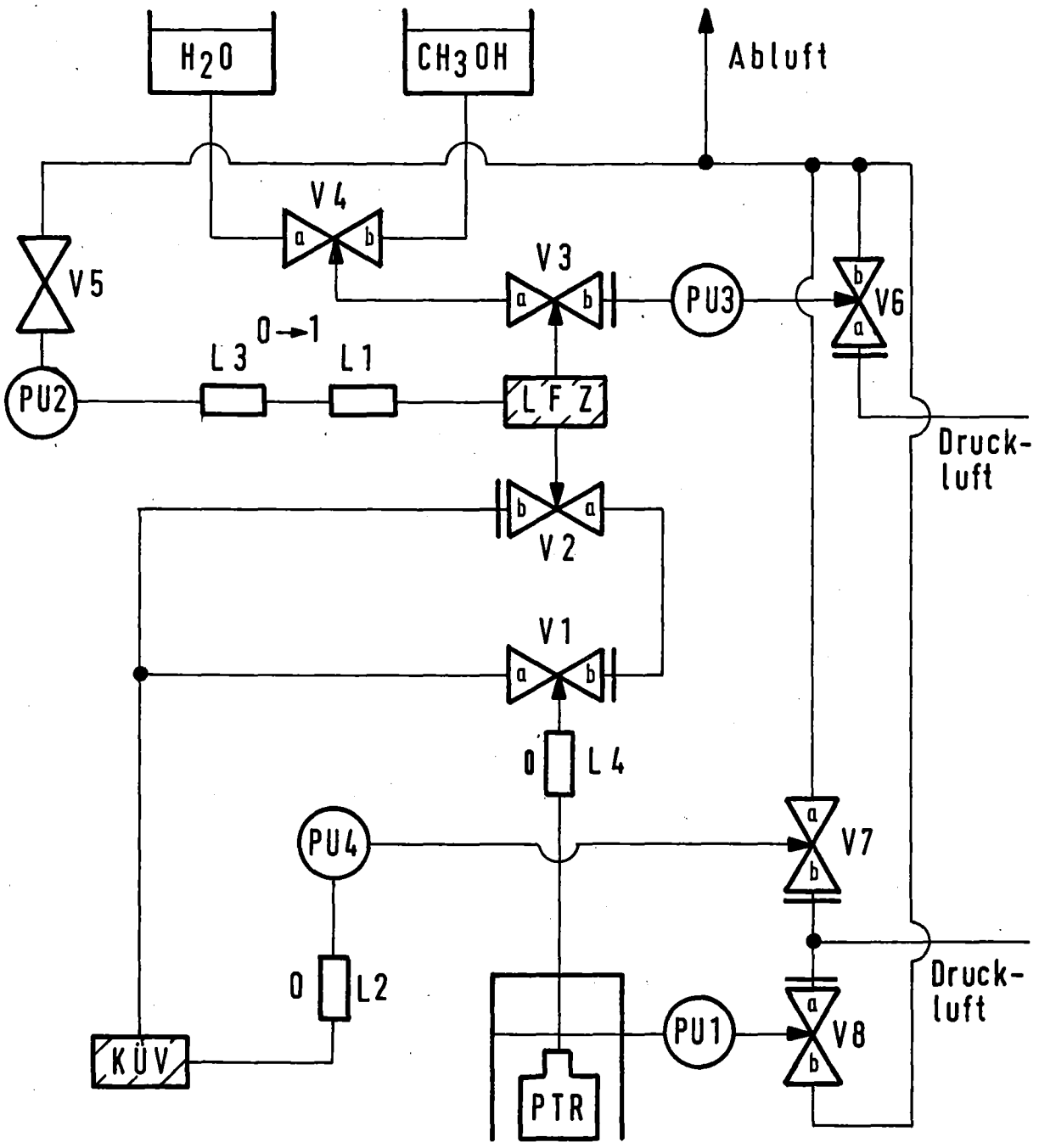


Abb. 21: SPÜLEN, LFZ füllen, Nr. 8.

Anmerkung: Hier wird eine Zeitschranke eingeführt, deren Überschreiten dem Ausfall eines Bauteiles gleichkommt.

{PU1}	{PU2}	{PU4}
1b·L4·T	L1·L3·T	2b·L2·T

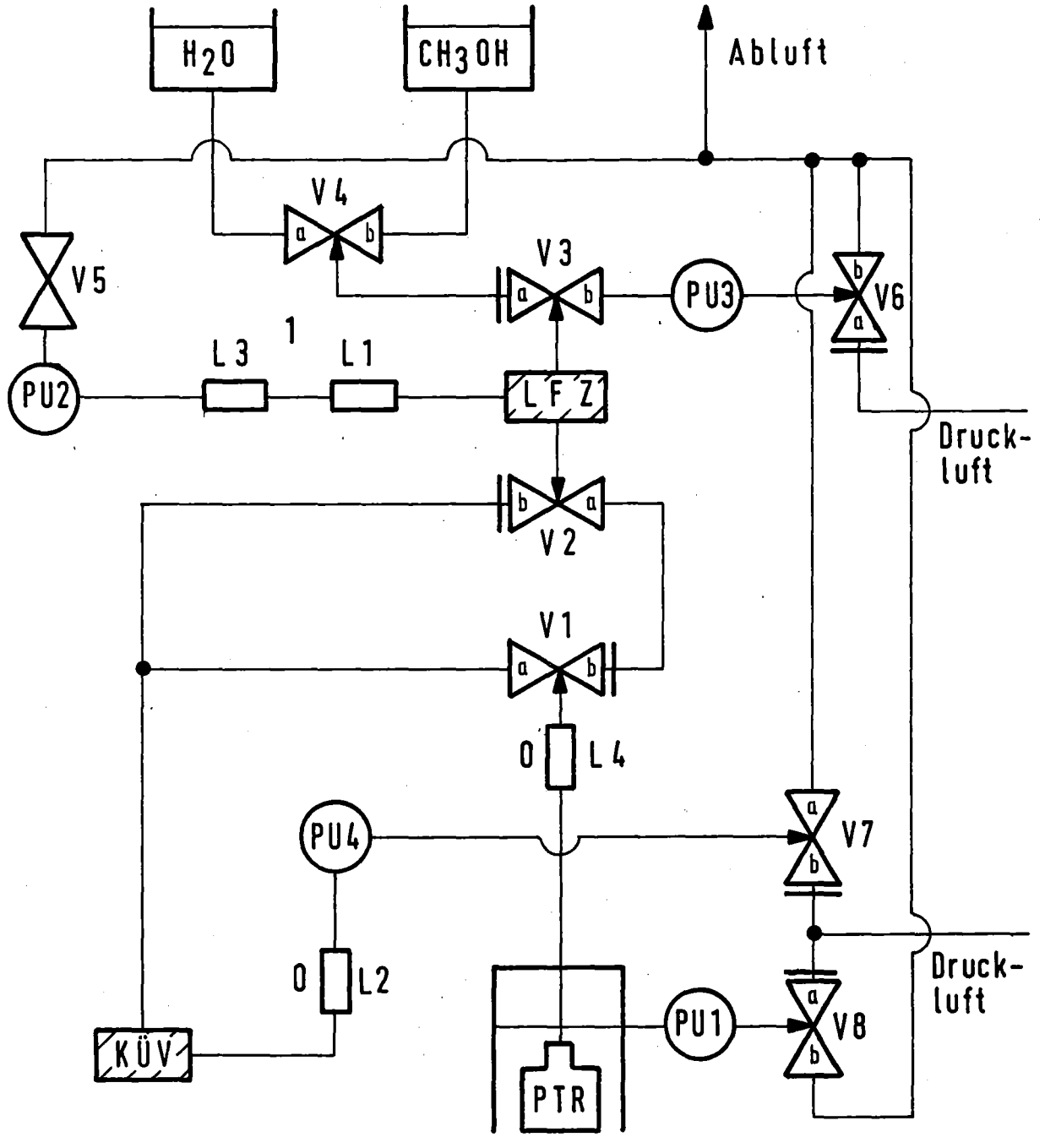


Abb. 22: SPÜLEN, LFZ voll, Nr. 9.

{PU1}	{PU2}	{PU4}
3a·1b·L4	3a	3a·2b·L2

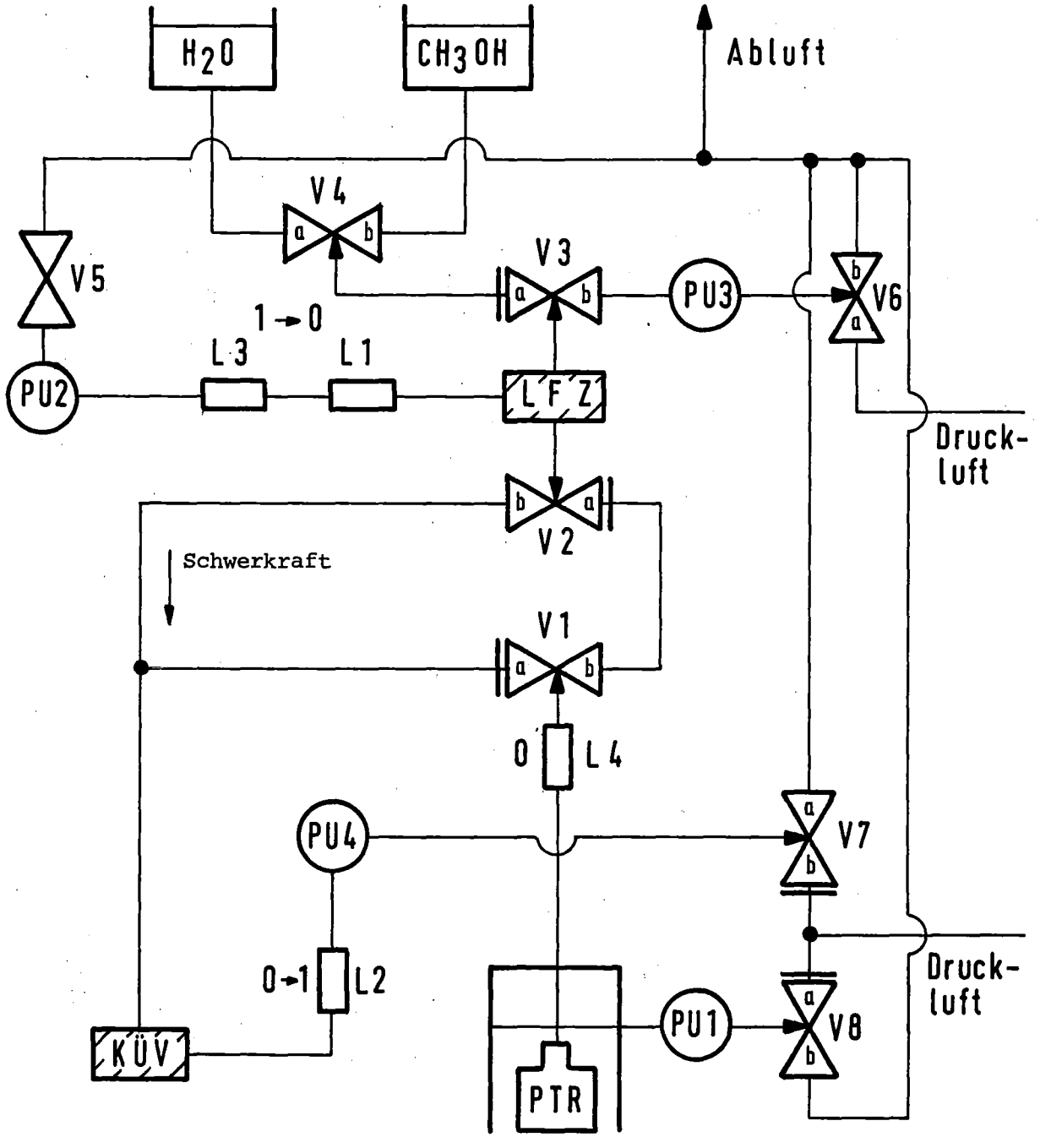


Abb. 23: SPÜLEN, KÜV füllen, Nr. 10.

{PU1}	{PU2}	{PU4}
3a·2a·L4	3a·2a·1a	3a·L2

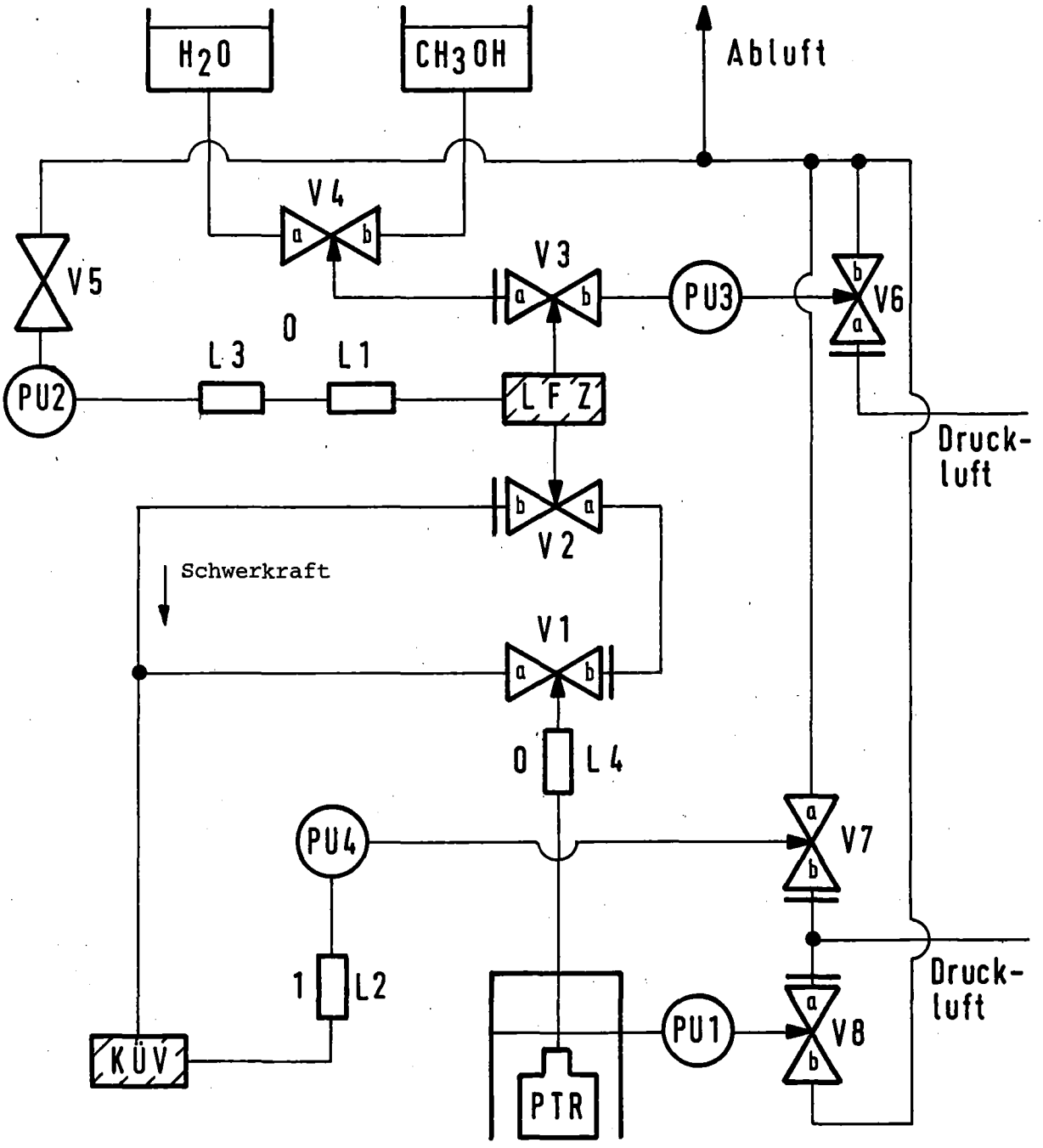


Abb. 24: SPÜLEN, KÜV voll, Nr. 11.

{PU1}	{PU2}	{PU4}
3a·1b·L4	3a·L1·L3	3a·2b

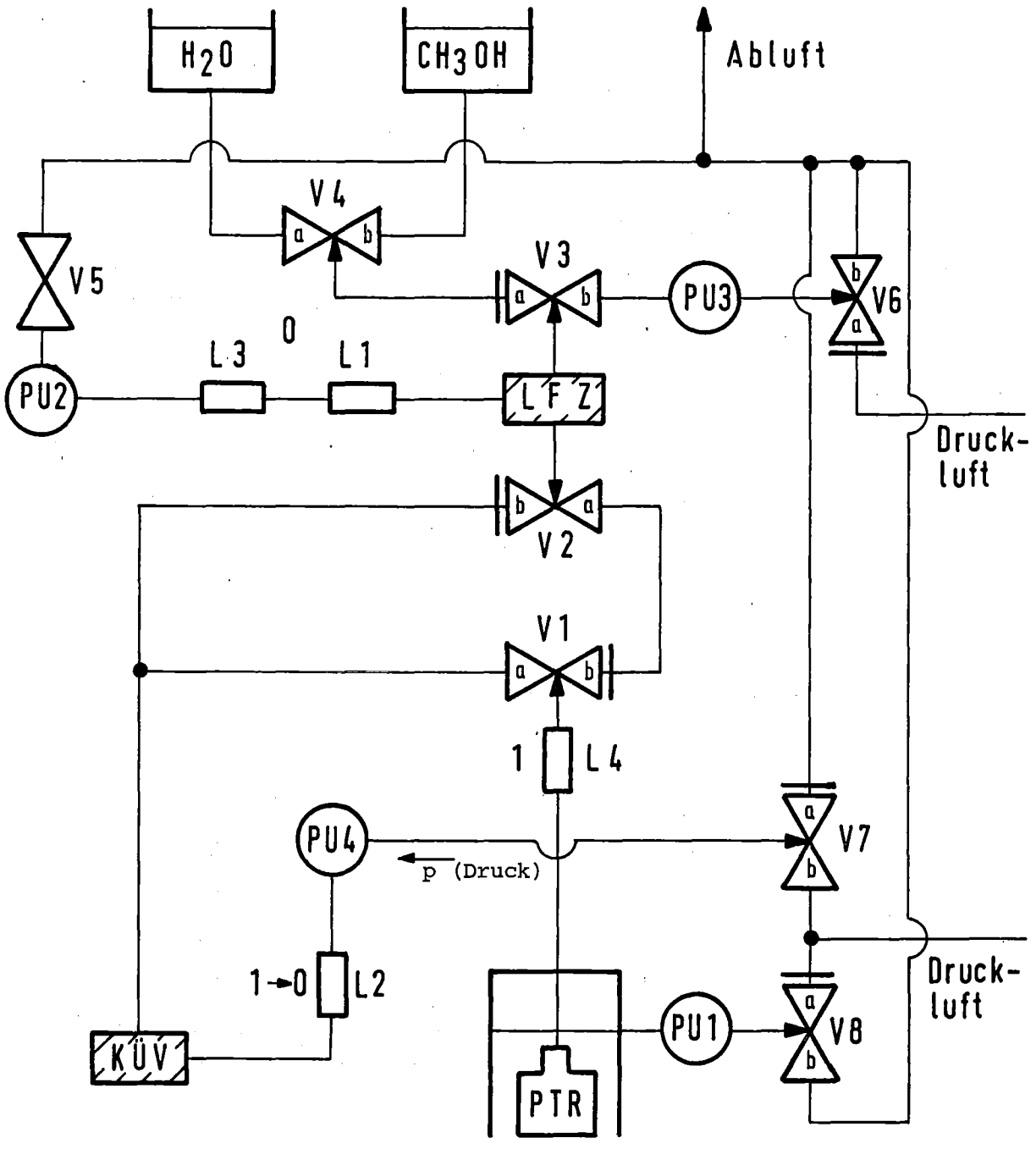


Abb. 25: SPÜLEN, KÜV leeren, Nr. 12.

{PU1}	{PU2}	{PU4}
3a·1b	3a·L1·L3	3a.2b·7a

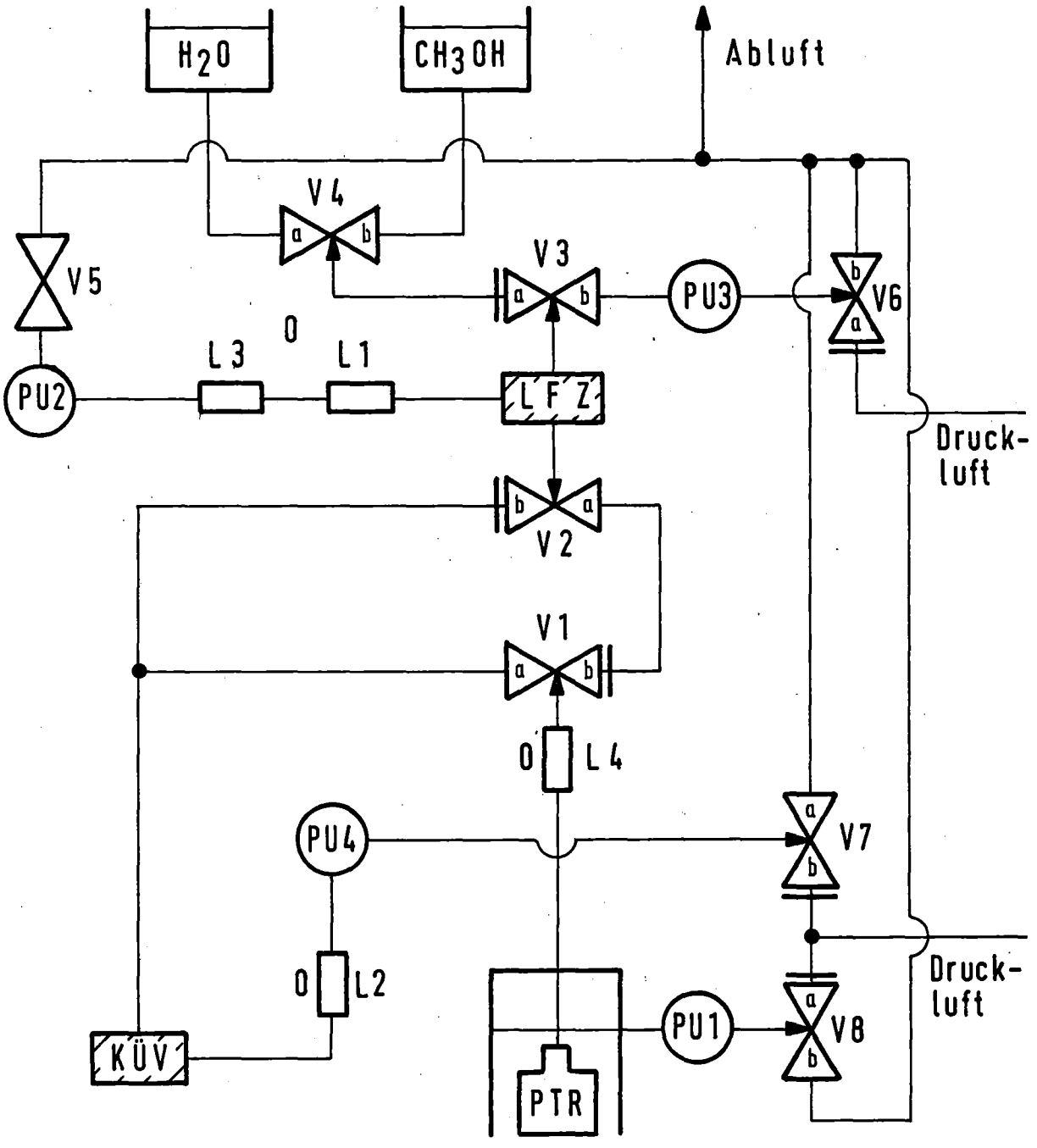


Abb. 26: SPÜLEN, KÜV leer, Nr. 13.

{PU1}	{PU2}	{PU4}
3a·1b·L4	3a·L1·L3	3a·2b·L2

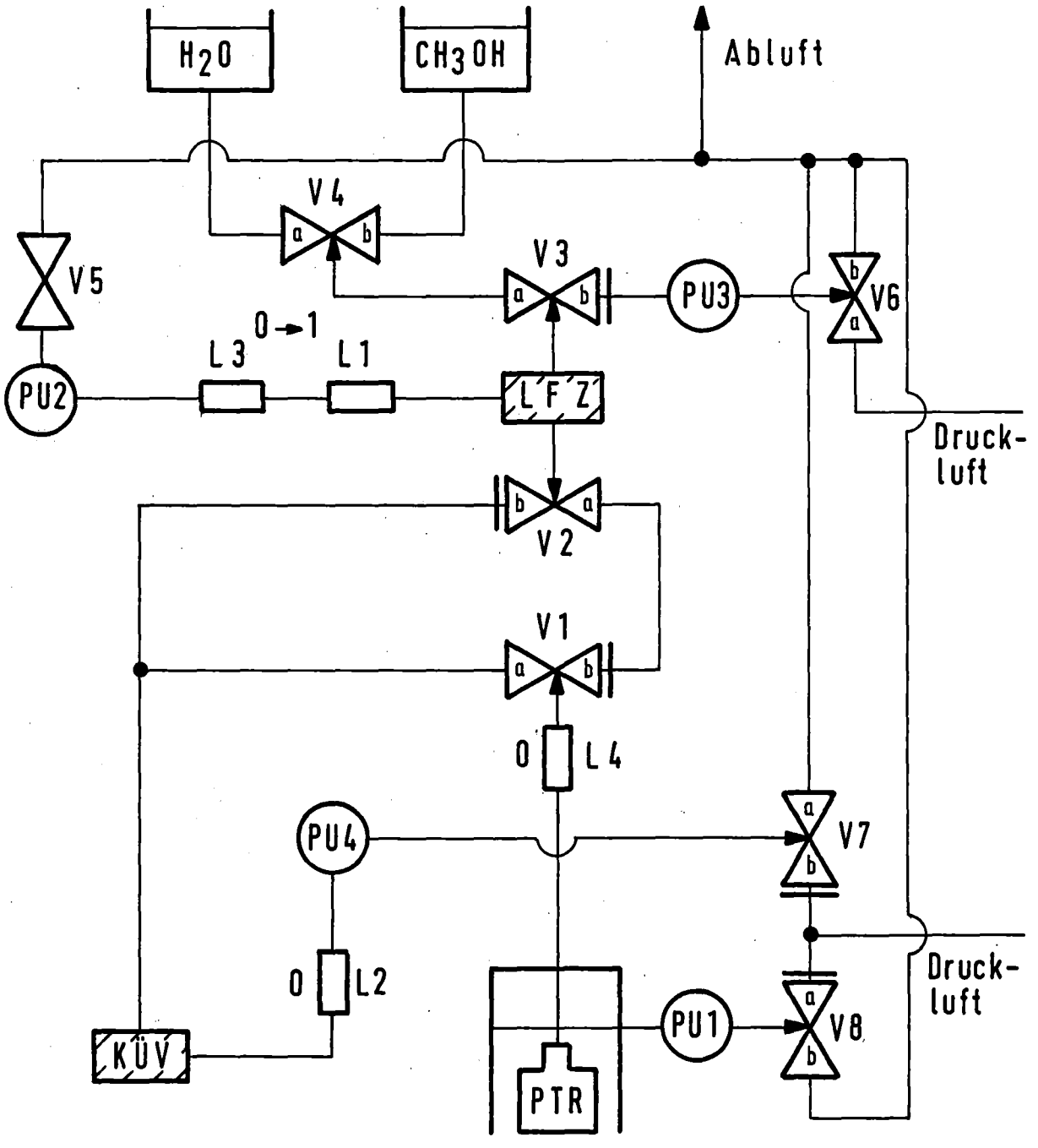


Abb. 27: SPÜLEN, LFZ füllen, Nr. 14.

Anmerkung: Für T siehe Abb. 21.

{PU1}	{PU2}	{PU4}
1b·L4·T	L1·L3·T	2b·L2·T

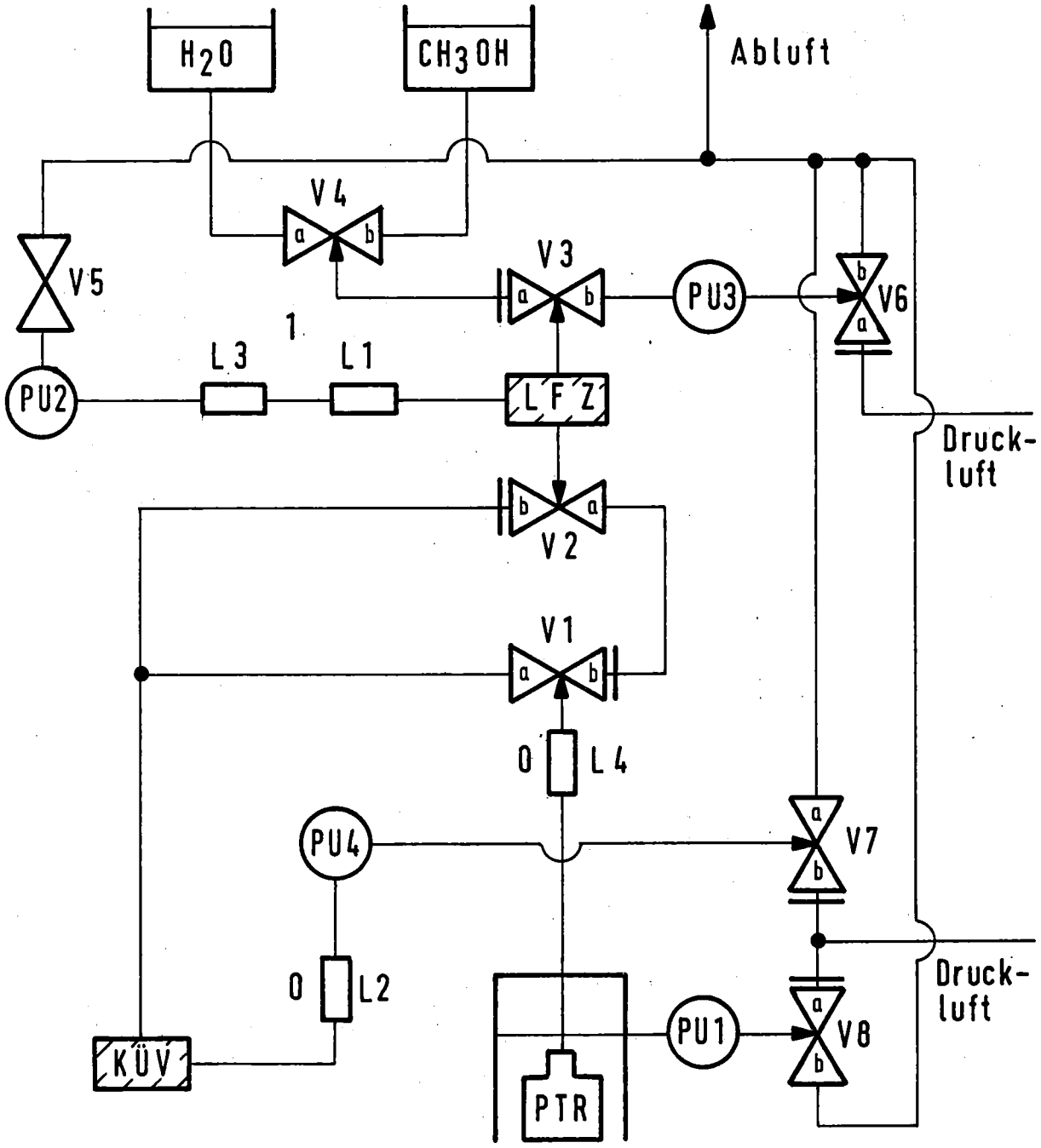


Abb. 28: SPÜLEN, LFZ voll, Nr. 15.

{PU1}	{PU2}	{PU4}
3a·1b·L4	3a	3a·2b·L2

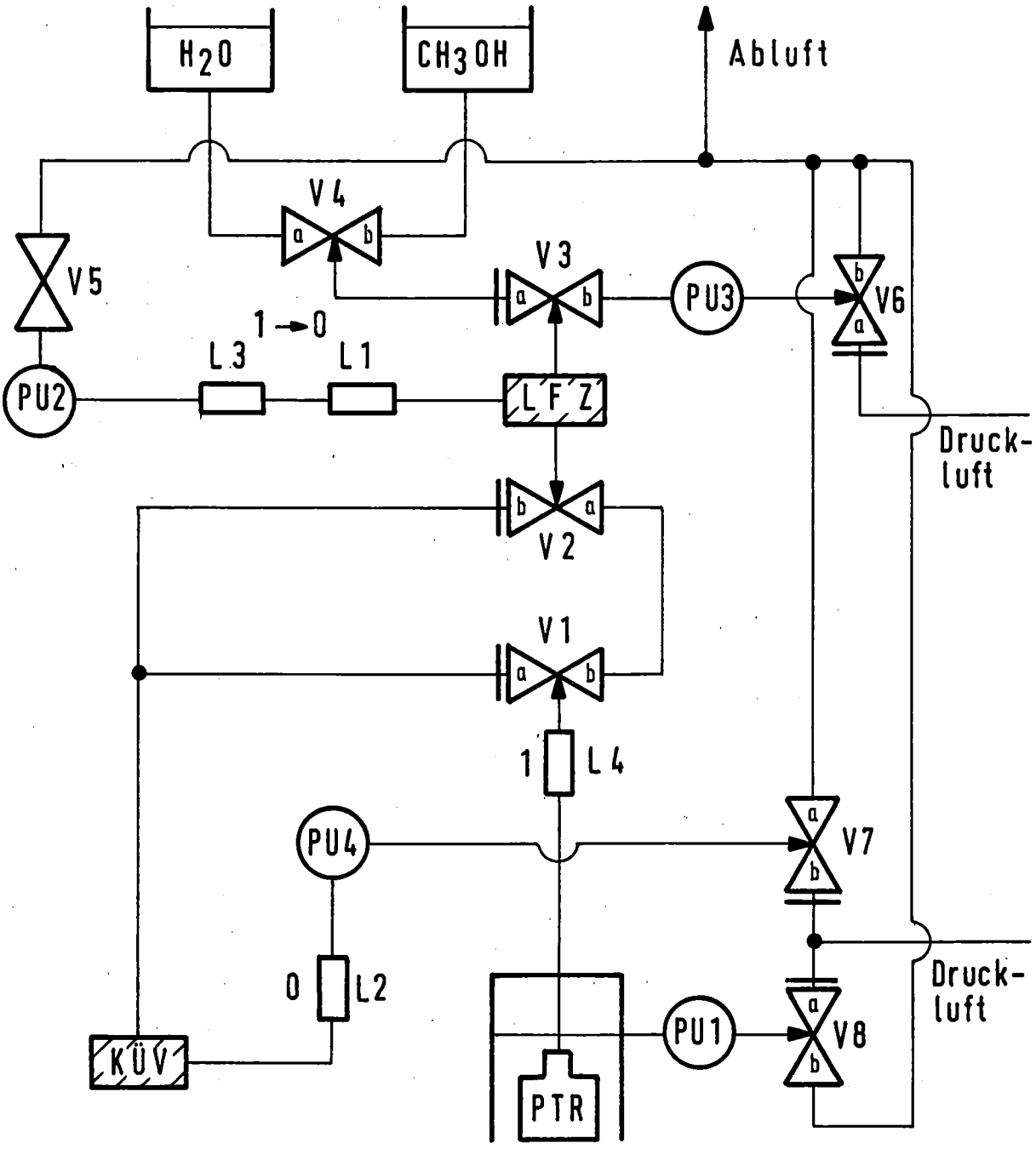


Abb. 29: SPÜLEN, durch LFZ-V2-V1, Nr. 16.

{PU1}	{PU2}	{PU4}
3a	3a·1a·L1·L3	3a·2b·L2

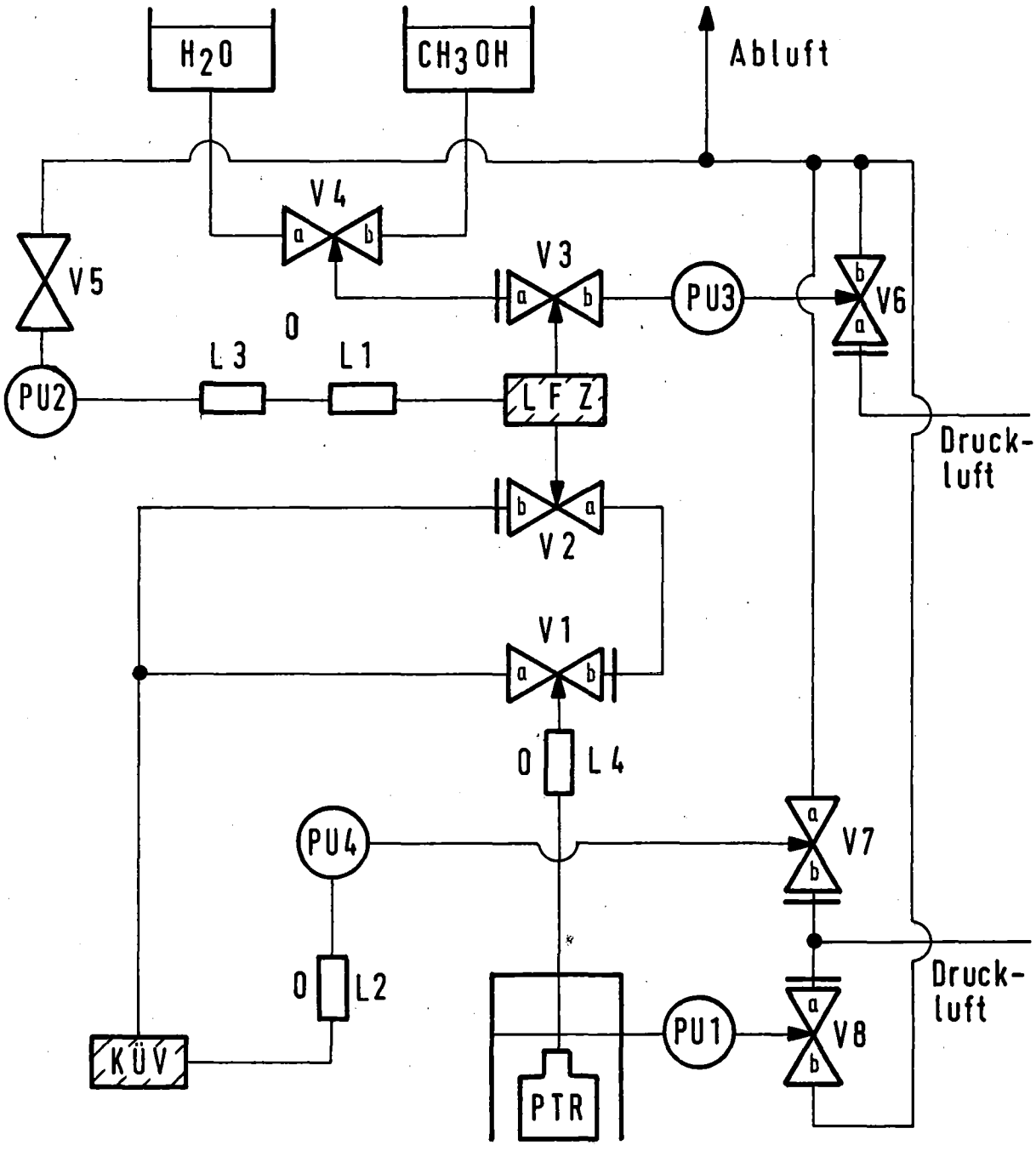


Abb. 30: SPÜLEN, LFZ leer, Nr. 17

{PU1}	{PU2}	{PU4}
3a·1b·L4	3a·L1·L3	3a·2b·L2

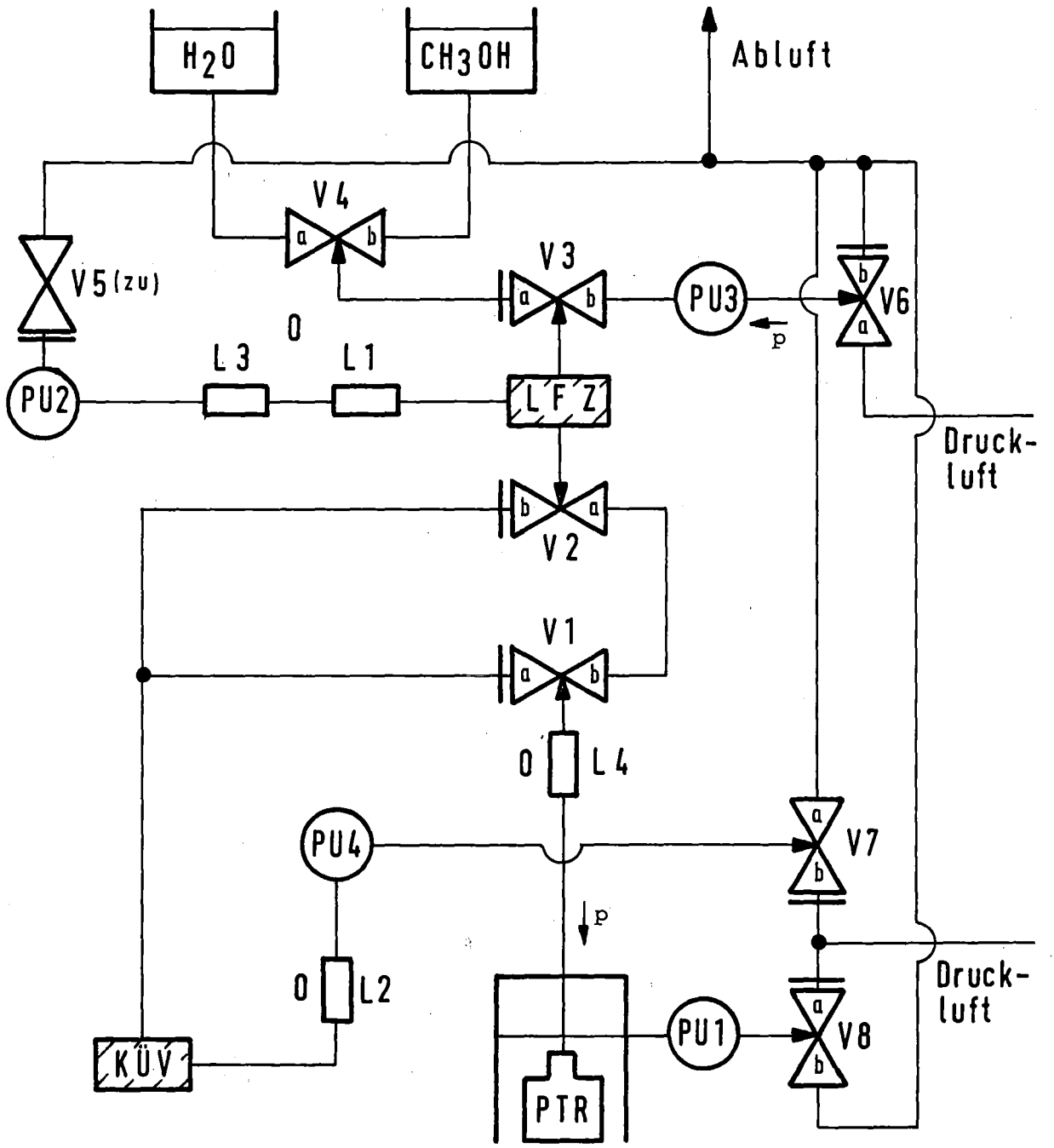


Abb. 31: BLASEN, durch V6-V3-LFZ-PTR, Nr. 18.

{PU1}	{PU2}	{PU4}
3a·L4	3a·1a·L1·L3	3a·2b·L2

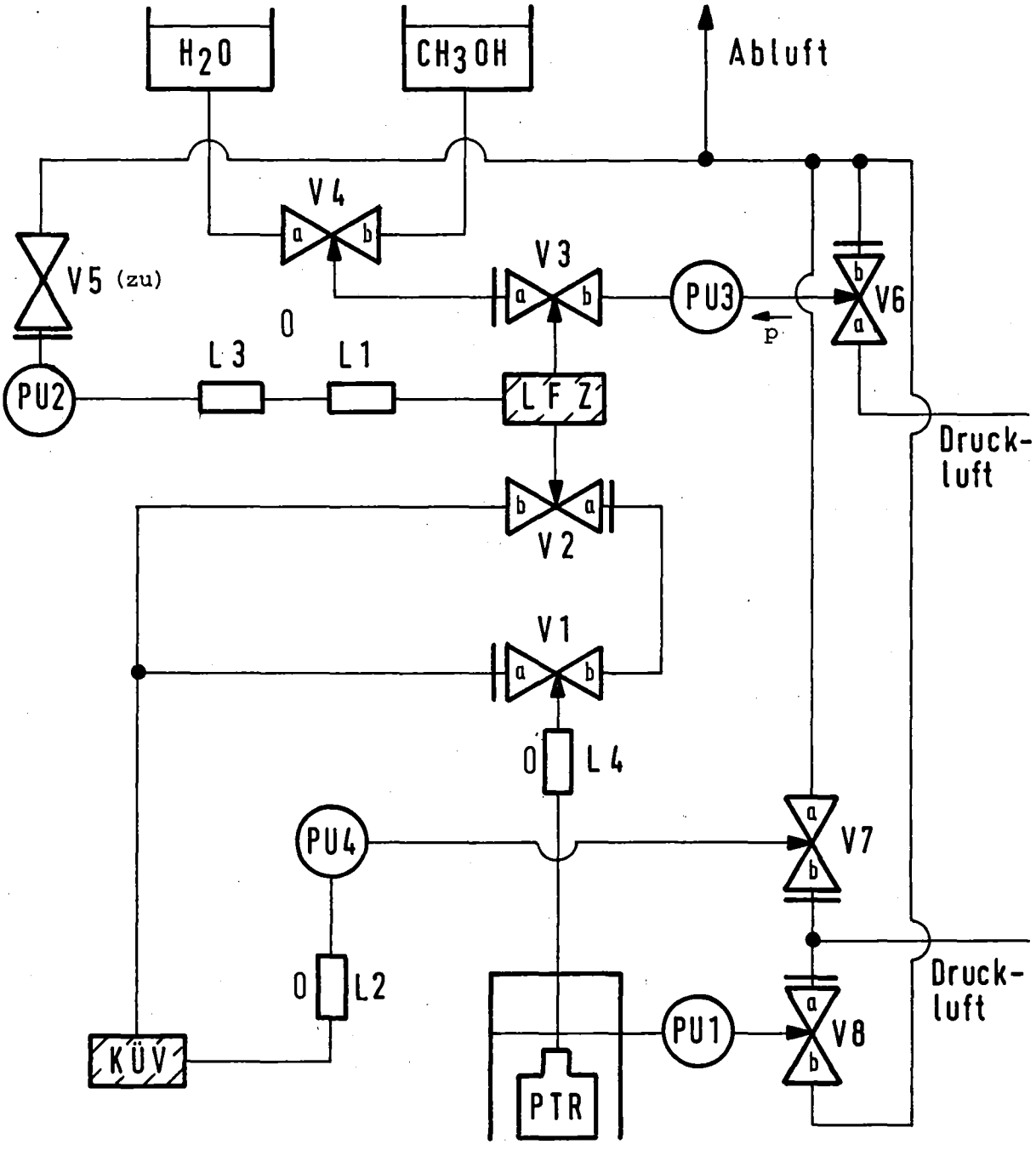


Abb. 32: **BLASEN**, durch V6-LFZ-KÜV-V7, Nr. 19.

{PU1}	{PU2}	{PU4}
3a·2a·L4	3a·2a·1a·L1·L3	3a·L2

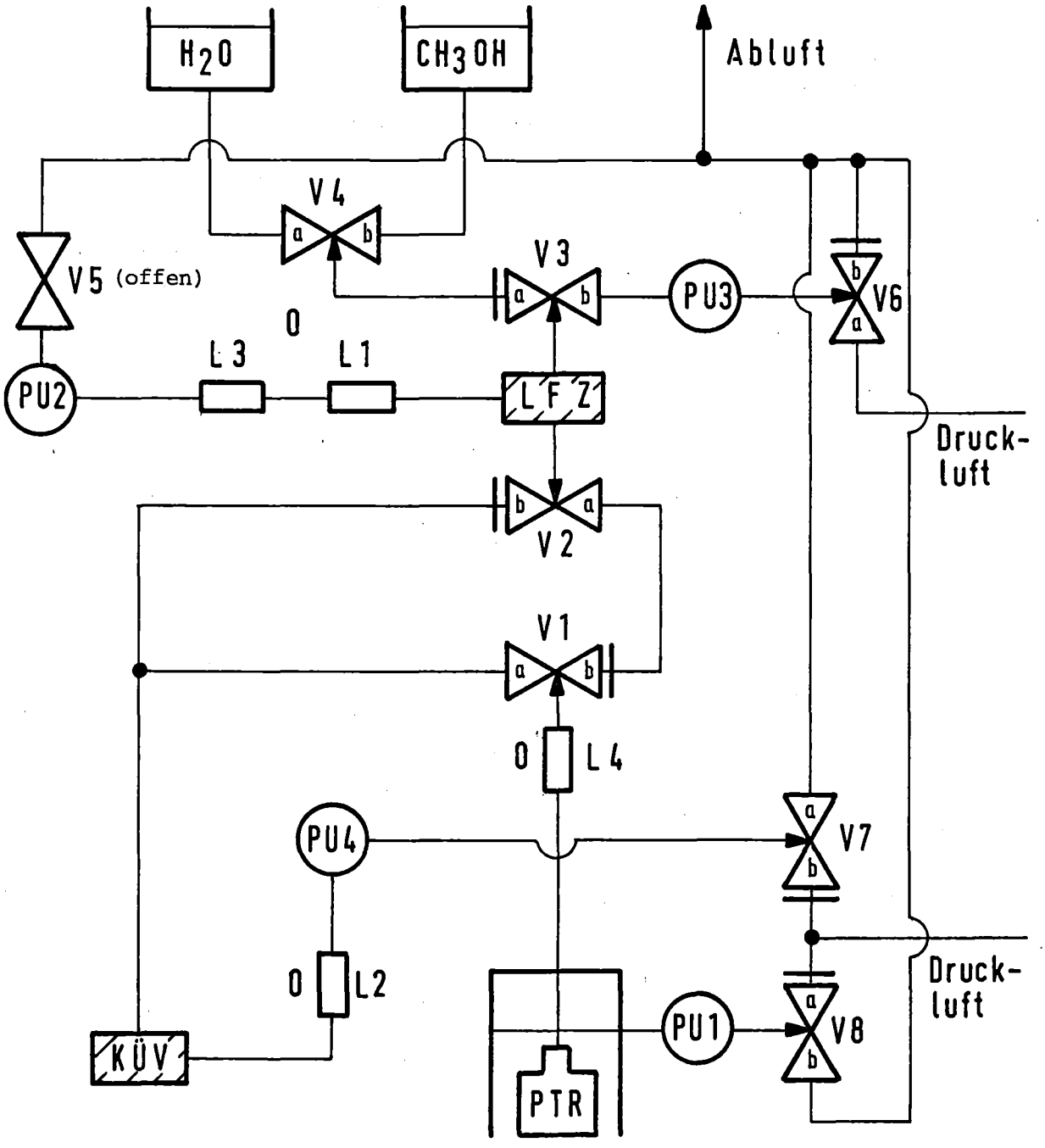


Abb. 33: BLASEN, durch V6-LFZ-PU2-V5, Nr. 20.

{PU1}	{PU2}	{PU4}
3a·1b·L4	3a·L1·L3	3a·2b·L2

Analysen-Phase	Zustand Nr.		{PU1}	{PU2}	{PU4}
MESSEN	2	-	3a·8b	3a (*)	3a·2b·L2
	3	-	3a·1b·L4	3a (*)	3a·2b·L2
	4	-	3a·2a·L4	3a·2a·1a	3a·L2
	5	-	3a·1b·L4	3a·L1·L3	3a·2b
	6	-	3a·1b	3a·L1·L3	3a·2b·7a
	7	-	3a·1b·L4	3a·L1·L3	3a·2b·L2
SPÜLEN	8	-	1b·L4·T	L1·L3·T	2b·L2·T
	9	wie 3	3a·1b·L4	3a (*)	3a·2b·L2
	10	wie 4	3a·2a·L4	3a·2a·1a	3a·L2
	11	wie 5	3a·1b·L4	3a·L1·L3	3a·2b
	12	wie 6	3a·1b	3a·L1·L3	3a·2b·7a
	13	wie 7	3a·1b·L4	3a·L1·L3	3a·2b·L2
	14	wie 8	1b·L4·T	L1·L3·T	2b·L2·T
	15	wie 9	3a·1b·L4	3a (*)	3a·2b·L2
	16	-	3a (*)	3a·1a·L1·L3	3a·2b·L2
	17	wie 7	3a·1b·L4	3a·L1·L3	3a·2b·L2
BLASEN	18	-	3a·L4	3a·1a·L1·L3	3a·2b·L2
	19	-	3a·2a·L4	3a·2a·1a·L1·L3	3a·L2
	20	wie 7	3a·1b·L4	3a·L1·L3	3a·2b·L2

Tab. 2: Zusammenfassung der Störfallanalysen.

Anmerkung zu Tab. 2:

(a) Die mit (*) gekennzeichneten Fehlerkombinationen sind Einzelfehler.

(b) Bei Nr. 8 und 14 wurde eine Zeitschranke T eingeführt. Andere Zeitschranken wurden weggelassen.

5. Methodische Überlegungen zum Zusammenhang von Fehlerbaumanalyse und Störfallanalyse

Aus den Abschnitten 3 und 4 können wir methodische Überlegungen ableiten.

5.1 Beobachtungen an einigen Resultaten der FBA und Störfallanalyse

Wir stellen einige Beobachtungen voran, die dann diskutiert werden.

(1) Die FBA von Abschnitt 3 lieferten Fehlerbäume mit den "Unerwünschten Ereignissen" {PU1}, {PU2}, {PU4} für die Analysenzustände Nr. 4, 5 (siehe Abb. 5, 6, 7).

(2) Die Störfallanalysen von Abschnitt 4 lieferten Störfalldiagramme mit den Störfallauswirkungen {PU1}, {PU2}, {PU4} für die Analysenzustände Nr. 4, 5 (siehe Abb. 13, 14).

Die Ergebnisse von (1) und (2) können wir als Auschnitt von Tabelle 2 zusammenfassen:

	{PU1}	{PU2}	{PU4}
Nr. 4	3a·2a·L4	3a·2a·1a	3a·L2
Nr. 5	3a·1b·L4	3a·L1·L3	3a·2b

Wir beobachten dabei (Tab. 2):

(1) Die Spalten {PU1}, {PU2}, {PU4} entsprechen in Minimalschnitte zerlegten Fehlerbäumen (siehe Abb. 8, 9, 10).

(2) Die Zeilen (Nr. 2 bis 20) entsprechen Störfalldiagrammen, in denen nicht ausgefallene Komponenten weggelassen werden (siehe Abb. 15 bis 33).

Reihenfolge von Ereignissen, Ursache/Wirkungsbeziehung

Die Reihenfolge (Nr. 4 vor Nr. 5) bleibt zwischen verschiedenen Minimalschnitten in einem Fehlerbaum (vgl. Abb. 5) bzw. zwischen verschiedenen Störfalldiagrammen (vgl. Abb. 13, Abb. 14) erhalten. Auch könnten wir eine Reihenfolge

und/oder eine Ursache/Wirkungsbeziehung zwischen einzelnen Ereignissen einführen (siehe Anhang A). Dies kann auch in einer geeigneten Form der Fehlerbaumanalyse berücksichtigt werden (siehe Taylor /10/ und unser Modell mit Zeitverzögerung in Anhang A). Bei dem hier besprochenen System war jedoch

- weder eine Reihenfolge bzw. Zeitverzögerung zwischen einzelnen Ereignissen (Ausfälle von Ventilen in bestimmter Reihenfolge bzw. Verzögerung eines Ausfalls gegenüber einem andern Ausfall),
- noch eine Ursache/Wirkungsbeziehung notwendig.

Man könnte jedoch an eine Sonderstellung der Feuchtefühler denken, die vor den Ventilen ausfallen müssen.

5.2 Aussagen über Ereigniskombinationen

Verzweigung im Störfalldiagramm

Eine einfache Verzweigung in einem Störfalldiagramm wird folgendermaßen dargestellt:

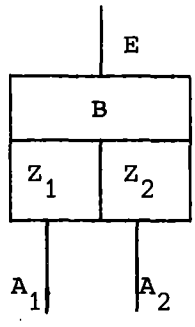


Abb. 34: Verzweigung im Störfalldiagramm.

Das Ergebnis E führt zu Funktionsanforderungen einer Betrachtungseinheit B mit zwei möglichen Zuständen (Z_1, Z_2). Es findet eine Verzweigung des Ereignisses E durch Konjunktion mit den sich ausschließenden Zuständen Z_1, Z_2 statt /7/:

$$A_i = E \wedge Z_i \quad (i=1,2) \tag{5-1}$$

(vgl. auch Anhang A).

Beispiel:

E = Ereignis "V3 geht auf a" (kurz 3a)

Z_1 = V2 ist auf a (kurz 2a) (5-2)

Z_2 = V2 ist auf b (kurz 2b) (5-3)

ergibt:

$A_1 = 3a \wedge 2a$ (5-4)

$A_2 = 3a \wedge 2b$. (5-5)

Nur wenn Z_i kein Normalzustand ist, wird es in unserem Formalismus aufgeführt. Diese Festlegung weicht vom üblichen Störfalldiagramm ab. Für $x \wedge y$ schreiben wir häufig $x \cdot y$.

Bedingungen im Störfalldiagramm

Für eine Bedingung C im Störfalldiagramm gilt:

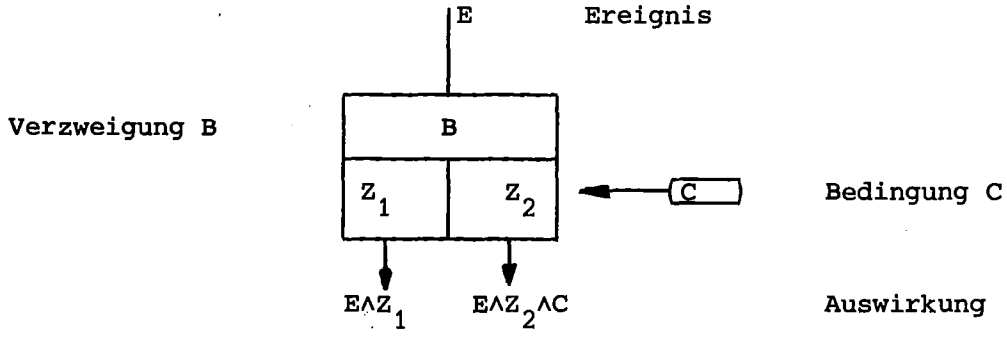


Abb. 35: Bedingung im Störfalldiagramm.

Beispiel (vgl. Abb. 13):

$E = 3a$ (Anfangsereignis) (5-6)

$Z_2 \wedge C = 2b \wedge L2$ (V2 auf b und L2 ausgefallen) (5-7)

ergibt:

$\{PU4\} = E \wedge Z_2 \wedge C = 3a \wedge 2b \wedge L2$ (5-8)

$= 3a \cdot 2b \cdot L2$.

Folgerung:

Damit lassen sich alle Ereigniskombinationen unseres Modells als Konjunktionen ausdrücken. Wir erhalten Minimalschnitte eines Fehlerbaums wenn wir

- alle Ereignisse, die keinen Ausfall bezeichnen, weglassen, sowie
- alle Kombinationen die echte Untermengen haben (die zur gleichen Störfallauswirkung führen) weglassen (siehe Anhang A und /11/).

Anmerkungen:

Von einem definierten Ereignis ausgehend, kann man nach Ursachen und Auswirkungen fragen. Dieses Vorgehen nennt man auch Entwicklung eines "Cause-Consequence-Diagrams" (CCD) /12/, /13/, /14/. Fragen wir nur nach den Ursachen, haben wir einen Fehlerbaum, fragen wir nur nach den Auswirkungen, haben wir ein Störfalldiagramm. Den Aufbau eines CCD kann man algorithmisch ausführen (Taylor /12/). Dieser Algorithmus erzeugt, wie sich beweisen läßt, Minimalschnitte. Nun ist das Störfalldiagramm ein Spezialfall des CCD. Damit gilt auch hier die Aussage von den Minimalschnitten. Unser Ziel war es, durch eine anschauliche Darstellung einen Einblick in diese Zusammenhänge zu geben. Wir werden in einem allgemeiner verwendbaren Modell diese Zusammenhänge im Anhang A aufgreifen.

5.3 Gegenseitige Kontrolle der Analysen

Es ist möglich, die Fehlerbaumanalyse durch die Störfallanalyse zu kontrollieren (und umgekehrt).

Die in /1/ beschriebene Fehlerbaumanalyse (FBA) wurde weithin durch die Störfallanalyse bestätigt. Trotzdem waren an einigen Stellen die Aussagen der Störfallanalyse weiterführend. Beispielsweise kam in der ursprünglichen Analyse für {PU1} (Zustand Nr. 4) kein Minimalschnitt

3a·2a·L4

vor. In der Störfallanalyse war er jedoch sofort zu finden. Er wurde auch in unser Beispiel zur FBA eingeführt (Abb. 5).

Es zeigte sich, daß in der üblichen Störfallanalyse nicht immer von vornherein zu erkennen war, ob ein Minimalschnitt vorliegt. Wenn man jedoch zu der für Tab. 2 vorgeschlagenen Schreibweise übergeht, so ist dies klar zu erkennen.

Beispielsweise hat man für Zustand Nr. 5 (Abb. 14) bei

	3a·2b·1b	keinen Minimalschnitt
jedoch bei	3a·2b	einen Minimalschnitt.

Beide Kombinationen führen zu {PU4}. Siehe auch die Regeln zur Vereinfachung der Analyse.

Noch eine Bemerkung zu den Grenzen der Kontrolle. Sind bereits für das Apparateschema oder den Ablauf des Normalbetriebs ungenügende oder falsche Informationen vorhanden, so kann dies durch keine Analysenform herausgefunden werden. Es ist darum große Sorgfalt und methodisches Vorgehen bei der Vorbereitung der Analyse notwendig. Dies kann z.B. durch eine gründlich durchgeführte Ausfalleffektanalyse untersützt werden. Dort wird eine möglichst vollständige Information über das Ausfallverhalten einzelner Bauteile angestrebt. Siehe auch den entsprechenden Normenentwurf /16/.

6. Vereinfachung der Störfallanalyse

Zu den methodischen Resultaten des Abschnitts 5 bringen wir noch weitere Ausführungen zur Störfallanalyse. Wie läßt sich diese Analyse vereinfachen? Dies kann Abschnitt 4 entnommen werden.

Es erscheint aber wichtig, auf die Voraussetzungen zu der dort beschriebenen vereinfachten Störfallanalyse hinzuweisen, sowie heuristische Regeln zur Vereinfachung der Analyse anzugeben.

Diese Regeln können sinngemäß auch auf andere Analysen angewandt werden.

6.1 Voraussetzungen zu einer vereinfachten Störfallanalyse

1. Gegeben sei ein vereinfachtes Apparateschema für ein zu untersuchendes System. (Die Vereinfachung soll keine wichtige Information über den zu betrachtenden Funktionsablauf unterschlagen).
2. Eine Ablauftabelle soll die N relevanten Schritte des Funktionsablaufs eindeutig kennzeichnen (z.B. Analysenphase und Zustand der Apparatur).
3. In N-facher Ausfertigung muß das vereinfachte Apparateschema vorliegen. In einem Apparateschema werden alle für den jeweiligen Normalzustand nötigen Einstellungen eingetragen (z.B. von Ventilen, Anzeigen von Feuchtefühlern). Es kann auch zweckmäßig sein, zu vermerken, wohin eine Flüssigkeit unter Schwerkraft einfließen kann sowie wo ein Überdruck vorliegt etc.
4. Von einem definierten Anfangsereignis ausgehend, kann man gezielt nach allen möglichen Endereignissen (gefährlicher Art) suchen.
5. Dann kann man mit dem Apparateschema Nr. ℓ ($\ell=1,\ldots,N$) ermitteln, welche Fehlerkombinationen zu Endereignissen (gefährlicher Art) führen, z.B. zu {PU1}, {PU2}, {PU4}.
6. Eine zusätzliche Angabe von Bauteilen im Normalzustand für Fehlerkombinationen ist nicht notwendig.

Anmerkung: Verschiedene Punkte (z.B. 6) tragen zu einer Vereinfachung der Störfallanalyse bei. Darüber hinaus sollen noch heuristische Regeln genannt werden.

6.2 Heuristische Regeln zur Vereinfachung der Störfallanalyse

Es gibt eine Anzahl von heuristischen Regeln, die z.B. bei Nielsen /13/, Taylor /14/ angegeben werden. Wir können dabei einige Regeln, die nur auf quantitativen Angaben beruhen, weglassen bzw. sie durch qualitative Formulierungen ersetzen.

1. Auswahl einer kürzesten Kombination

   Hat man ein Ereignis mit einer ernsthaften Konsequenz gefunden, so ist es manchmal möglich, andere Kombinationen, die mit weniger Elementen zum gleichen Ereignis führen, zu finden. (Dies gilt insbesondere für Minimalschnitte, siehe z.B. zwei mögliche Kombinationen bei Zustand Nr. 5, vgl. Abb. 14, 3a·2a·1b (nicht minimal), 3a·2b (minimal).

2. Abbruch bei ungefährlichen Folgen

   Man breche eine Ereigniskombination ab, wenn sie zu keinem gefährlichen Endereignis führt (z.B. wird die Kombination mit 3b meist nicht weiter verfolgt.)

3. Abbruch bei geringer Wahrscheinlichkeit der Ereigniskombination

   Sind Ausfallwahrscheinlichkeiten bekannt, so breche man eine Ereigniskombination ab, wenn die Wahrscheinlichkeit ihres Eintretens klein gegenüber anderen Kombinationen wird. (Sind Ausfallwahrscheinlichkeiten nicht bekannt, so kann man evtl. bei Ereigniskombinationen, die aus vielen Ereignissen bestehen, abbrechen.)

4. Von vornherein unkritische Bauelemente

   Es ist möglich, bei manchen Bauelementen ohne Störfallanalyse zu sagen, ob sie aus technischen Gründen überhaupt zu einem Störfall beitragen können.

   Man kann z.B. V4 aus dem Störfalldiagramm weglassen. Es entscheided nicht über die Frage, ob Spülflüssigkeit kommen kann oder nicht. Desgleichen fallen V5 und V6 in der Regel weg. Das gleiche gilt für V7 und V8. Damit baut sich das Störfalldiagramm häufig aus den Ventilen V1, V2, V3 auf (sowie L1, L2, L3, L4) (Abb. 11, Abb. 13).

5. Gleiche Zustände im Ablauf

   Wiederholen sich spezielle Zustände während einer Ablaufphase (MESSEN, SPÜLEN, BLASEN) so kann man damit für Störfalldiagramme Arbeit einsparen.

Z.B. zeigt sich aus der Ablauftabelle, wo sich Zustände wiederholen. Siehe Tabelle 2, "Zusammenfassung der Störfallanalysen" (z.B. ist Nr. 9 wie 3, Nr. 10 wie 4 usw.). Für weitere Zustände sind V1, V2, V3 in der gleichen Stellung, jedoch ist die Feuchte nicht immer gleich. Damit treten Fehlerkombinationen auf, die sich evtl. noch durch die Feuchtefühler unterscheiden (z.B. hat 7 dieselbe Ventileinstellung wie 3, jedoch ist die Feuchte nicht überall gleich).

6. Bedeutung des Einzelfehlers

Es ist immer wichtig, nach Einzelfehlern zu suchen.

Der Fehler 3a, der auch als Einzelfehler auftritt, dient als Ausgangsereignis. Der Fehler 3a ist immer Teil einer Ausfallkombination, wenn nicht V3 in der für den Betrieb notwendige Einstellung "a" ist. (Tab. 2 Analysenzustände Nr. 2, 3, 9, 15, 16, geben Beispiele für Einzelfehler.)

Zur Anwendung der Regeln

1. Diese Regeln bedeuten nicht, daß man sie ohne weiteres oder automatisch anwenden kann. Sie können jedoch heuristisch zur Vereinfachung beitragen. Diese Regeln sind auch nicht vollständig /14/. Bei Boole'schen Ausdrücken kann man jedoch alle Regeln angeben (Absorption usw.).

2. Diese Regeln wurden für Cause-Consequence-Diagramme aufgestellt /14/. Sie gelten darum auch für Störfallanalysen. Sie sind auch (sinngemäß) für den Aufbau von Fehlerbäumen verwendbar.

3. Es ist wichtig in diesem Zusammenhang auch auf die Entscheidungstabellentechnik hinzuweisen (vgl. z.B. /15/). Auch dort treten ähnliche heuristische Regeln auf. Auf die grundsätzlichen Zusammenhänge wurde in /16/, /17/ hingewiesen. Eine vergleichende Bewertung von Entscheidungstabellen, Fehlerbäumen und Cause-Consequence-Diagrammen findet man in /21/, /23/.

7. Schlußbemerkung

Die hier dargestellten Untersuchungen geben auf unsere in Abschnitt 1 gestellten Fragen folgende Antwort:

(a) Für ein System können wir Fehlerkombinationen oder Minimalschnitte eines Störfalldiagramms bzw. eines Fehlerbaums finden. In den Überlegungen der Fehlerbaumanalyse und Störfallanalyse (Abschnitte 3, 4) wurde dies im einzelnen durchgeführt. Der Zusammenhang über die Minimalschnitte wurde gezeigt (Abschnitt 5, und Anhang A).

(b) Eine Kontrolle der Analysen ist möglich. Eine Kontrolle durch Störfallanalyse führte zur Vervollständigung der Resultate der FBA.

(c) Es gibt eine Anzahl von heuristischen Regeln zur Vereinfachung der Störfallanalyse. Dies konnte an vielen Stellen gezeigt werden. Auch ist eine sinngemäße Anwendung auf FBA möglich. Die heuristischen Regeln sind nicht vollständig. Es sollte insbesondere keine automatische Anwendung der Regeln stattfinden.

8. Literatur

/1/ D. Stöckle, unveröffentlichte Ergebnisse.

/2/ DIN 25424, Fehlerbaumanalyse, Methode und Bildzeichen (1977), Beuth Verlag, Berlin.

/3/ VDI-Richtlinie 4008/Blatt 7 (Entwurf), Strukturfunktion und ihre Anwendung, Beitrag zum VDI-Handbuch "Technische Zuverlässigkeit", Bearbeiter L. Camarinopoulos, G. Weber (1979).

/4/ D.S. Nielsen, Use of Cause Consequence Charts in Practical Systems Analysis, Beitrag zu "Reliability and Fault Tree Analysis", Conf. Berkeley (3-7 September 1974), Editors R.E. Barlow, J.B. Fussell, N.D. Singpurwalla, SIAM, Philadelphia, Penn. (1975), S. 849-880.

/5/ IEEE-Trans. on Rel., Vol. R-25, No. 3 (1976), Special Issue on Nuclear System Reliability and Safety (Guest Editor J.B. Fussell).

/6/ J.B. Fussell, G.J. Powers, R.G. Bennets, Fault Trees - A state of the Art Discussion, IEEE-Trans on Rel., Vol. R-23, No. 1 (1974).

/7/ DIN 25419/Teil 1, Störfallablaufanalyse; Störfallablaufdiagramm, Methode und Bildzeichen (1977), Beuth Verlag, Berlin.

/8/ W.E. Büttner, Ein Konzept zur Störfallanalyse, dargestellt am Beispiel des Hauptkühlmittelpumpenausfalls in einem Druckwasserreaktor, Laboratorium für Reaktorregelung und Anlagensicherung Garching, MRR-141 (Oktober 1974).

/9/ H.P. Balfanz, Sicherheitsanalyse-Plan, (Anwendung verschiedener Sicherheits- und Zuverlässigkeitsanalysen zum richtigen Zeitpunkt und zu speziellen Problemen), IRS-W-2 (April 1972), Köln.

/10/ J.R. Taylor, E. Hollo, Experience with Algorithms for Automatic Failure Analysis, Int. Conf. on Nucl. Syst. Reliability Engineering and Risk Assessment, Gatlinburg, Tenn. (June 20-24, 1977).

/11/ G. Birkhoff, T.C. Bartee, Modern Applied Algebra, McGraw-Hill Book Company, New York (1970), S. 141-150 (Block Diagrams for Gating Networks).

/12/ J.R. Taylor, Sequential Effects in Failure Mode Analysis, Risö-M-1740 (August 1974), S. 23-28, Danish Atomic Energy Commission.

/13/ D.S. Nielsen, The Cause-Consequence-Diagram Method as a Basis for Quantitative Accident Analysis, Risö-M-1374 (May 1971), Danish Atomic Energy Commission.

/14/ J.R. Taylor, A Formalization of Failure Mode Analysis of Control Systems, Risö-M-1654 (September 1973), S. 36-38, Danish Atomic Energy Commission.

/15/ J.R. Metzner, B.H. Barnes, Decision Table Languages and Systems, Academic Press, New York (1977).

/16/ S.L. Salem, J.S. Wu, G. Apostolakis, Decision Table Development and Application to the Construction of Fault Trees, Nucl. Technol. Vol. 42 (1), (Jan. 1979), S. 51-64.

/17/ G. Weber, L. Gmeiner, U. Voges, Methoden der Zuverlässigkeitsanalyse und -sicherung bei Hardware und Software in Zuverlässigkeit von Rechensystemen, Hrsg. W. Görke (Fachberichte und Referate, Band 9), R. Oldenbourg Verlag, München (1979).

/18/ Z. Kohavi, Switching and Finite Automata Theory, McGraw-Hill Book Company, New York (1978).

/19/ W. Giloi, H. Liebig, Logischer Entwurf digitaler Systeme (Hochschultext) Springer Verlag, Berlin (1973).

/20/ V.N. Roginski, Dynamic Automata and Temporal Boolean Functions (I) Engineering Cybernetics, Vol. 8 No. 2 (March-April 1970), S. 299-307.

/21/ E. Hollo, Some Points of Advanced Alarm System Design, Risö-M-1904, (January 1977), Danish Atomic Energy Commission.

/22/ R.E. Barlow, F. Proschan, Statistical Theory of Reliability and Life Testing, Holt, Rinehart and Winston, Inc., New York (1975).

/23/ E. Cerny, D. Mange, and E. Sanchez, Synthesis of Minimal Binary Decision Trees, IEEE-Trans. on Comp., Vol. C-28, No. 7, S. 472-482 (1979).

A N H A N G A

Ein Boole'sches Modell zum Zusammenhang von Fehlerbäumen und Störfalldiagrammen

A.1 Einleitung

Wir stellten in den Abschnitten 4 und 5 einen Zusammenhang von Fehlerbaumanalyse und Störfallanalyse fest.

Es wurde bereits von Nielsen /4/ festgestellt, daß ein "Cause-Consequence-Diagram" zu Minimalschnitten führt (vgl. Abschnitt 5.2). Diese Aussage wurde verallgemeinert und bewiesen in einer Arbeit von Taylor /12/. Wir wollen hier nicht den gesamten Beweis aus /12/ nachvollziehen.

An einem Modell, das aus Boole'schen Ausdrücken und Verzögerungsgliedern besteht, wollen wir jedoch den Weg vom Störfalldiagramm zum Fehlerbaum und umgekehrt untersuchen. Ein zentraler Begriff ist dabei der Minimalschnitt /12/.

Definition:

Für ein Cause-Consequence-Diagram ist ein Minimalschnitt eine Menge von Ereignissen, die als Ganzes zu einem bestimmten "Unerwünschten Ereignis" (oder zu einer bestimmten Störfallauswirkung) führt, die aber keine Untermenge von Ereignissen besitzt, die bereits zu diesem "Unerwünschten Ereignis" führt.

Beispiel: Alle in Tab. 2 aufgeführten Fehlerkombinationen sind Minimalschnitte.

Nun gehen wir folgendermaßen vor:

1. Wir führen Boole'sche Ausdrücke mit Verzögerungsgliedern ein, die insbesondere in der Schaltalgebra weitgehend Verwendung finden /18/. /19/, /20/, (A.2).
2. Wir zeigen das Auftreten von Minimalschnitten bei Störfalldiagrammen und zeigen, daß ein Übergang vom Störfalldiagramm zum Fehlerbaum möglich ist (A.3).
3. Wir zeigen das Auftreten von Minimalschnitten bei Fehlerbäumen und untersuchen, in welchen Grenzen ein Übergang vom Fehlerbaum zum Störfalldiagramm möglich ist (A.4).

Mit weiteren Eigenschaften, z.B. Hinzufügen von "Ursache/Wirkungsbeziehungen" und von "Bedingungen" könnten wir unsere Überlegungen verallgemeinern (vgl. dazu /12/).

A.2 Boole'sche Ausdrücke mit Verzögerung

Wir wollen nun zur Behandlung von Störfalldiagrammen und Fehlerbäumen zeitabhängige Boole'sche Ausdrücke einführen, die zu diskreten Zeitpunkten die Werte 0, 1 annehmen können. Zu den üblichen Operationen (dargestellt durch UND-Tor, ODER-Tor, NEGATION) kommt noch ein "Verzögerungsglied" hinzu /19/, /20/. Dieses kann eine zeitabhängige Boole'sche Variable x(t) um den Betrag τ verzögern:

$$y(t) = x(t-\tau) \quad . \tag{A-1}$$

Dies wird zur Abkürzung im Folgenden als

$$y = x^{\tau} \tag{A-2}$$

geschrieben. Die Auswirkung eines Verzögerungsgliedes auf die Boole'sche Variable x ist in Abb. 36a und 36b anschaulich dargestellt.

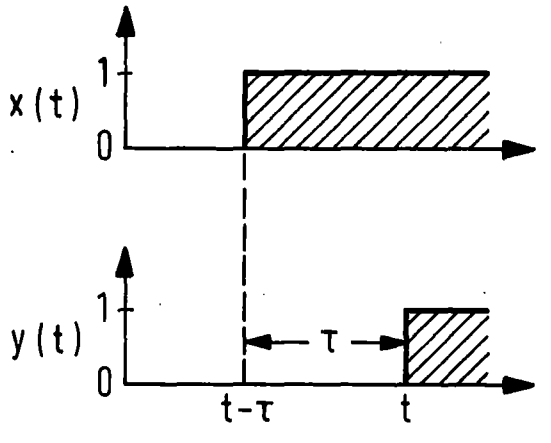


Abb. 36a: Verzögerung τ

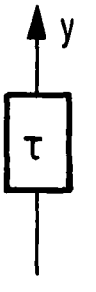


Abb. 36b: Verzögerungsglied

D.h. y(t) wird zur Zeit t gleich 1, wenn x(t-τ) zur Zeit t-τ gleich 1 geworden ist. Die hier eingeführte Verzögerung ist "linear" /20/, insbesondere gilt:

$$(x^{\tau_1})^{\tau_2} = x^{\tau_1+\tau_2} \quad . \tag{A-3}$$

Für ein logisches Diagramm, das keine gerichteten Schleifen besitzt (bei dem keine Rückkopplung vorliegt), gilt

$$y = (f(x_1,x_2,\ldots,x_n))^\tau = f(x_1^\tau,x_2^\tau,\ldots,x_n^\tau) \quad , \qquad \text{(A-4)}$$

wobei $f(x_1,x_2,\ldots,x_n)$ eine Boole'sche Funktion ist. Dieses Fehlen gerichteter Schleifen wird für jeden Fehlerbaum vorausgesetzt. Einige Beispiele für (A-4) sind:

Negation und Verzögerung

$$(\bar{x})^\tau = \overline{x^\tau} \quad . \qquad \text{(A-5)}$$

Anschaulich:

Abb. 37: Negation und Verzögerungsglied

D.h., das Verzögerungsglied τ kann an den Ausgang oder an den Eingang der Negation gesetzt werden.

Konjunktion und Verzögerung

$$(x_1x_2)^\tau = x_1^\tau x_2^\tau \quad . \qquad \text{(A-6)}$$

Anschaulich:

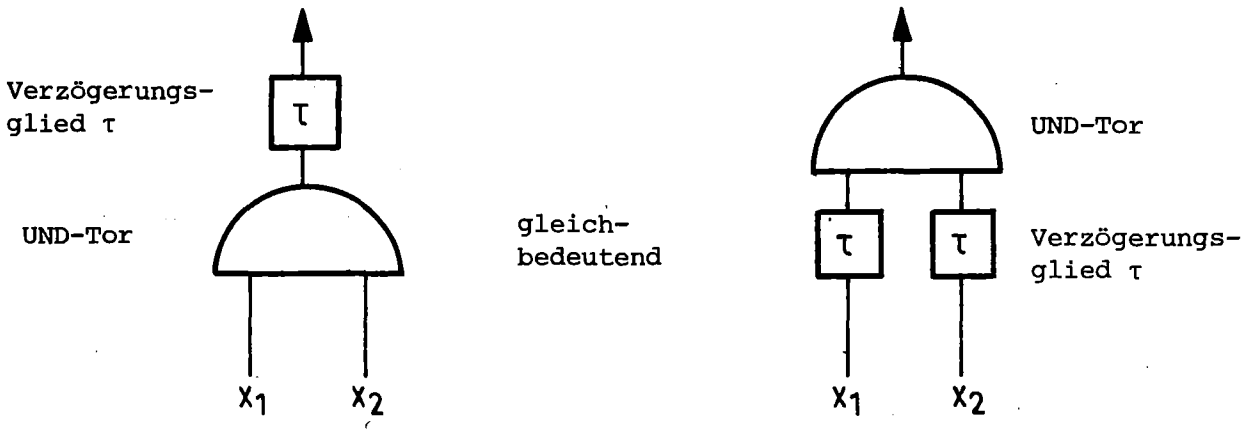


Abb. 38: UND-Tor und Verzögerungsglied

D.h., das Verzögerungsglied τ kann an den Ausgang oder an die Eingänge des UND-Tores gesetzt werden.

Disjunktion und Verzögerung

$$(x_1 \vee x_2)^{\tau} = x_1^{\tau} \vee x_2^{\tau} \quad . \tag{A-7}$$

Anschaulich:

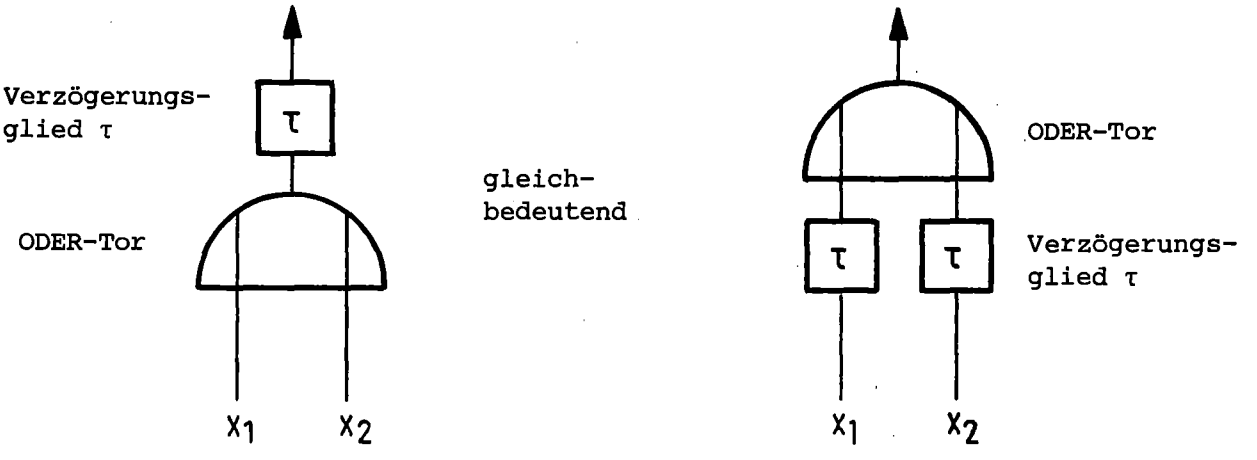


Abb. 39: ODER-Tor und Verzögerungsglied

D.h., das Verzögerungsglied τ kann an den Ausgang oder an die Eingänge des ODER-Tores gesetzt werden.

Im allgemeinen werden jedoch die Zeitverzögerungen von verschiedenen Variablen verschieden sein, so daß wir erhalten

$$y = f(x_1^{\tau_1}, x_2^{\tau_2}, \ldots, x_n^{\tau_n}) \quad . \tag{A-8}$$

Ein Beispiel ist:

$$y = x_1^{\tau} \cdot x_2^{2\tau} \quad . \tag{A-9}$$

D.h., y ist genau dann gleich 1, wenn x_1 (mit Verzögerung τ) und x_2 (mit Verzögerung 2τ) gleich 1 sind. Für irgendwelche andere Verzögerungen, z.B. τ=0, 3τ etc. ist damit nichts gesagt. Damit muß man auch folgenden beachten:

$$x \cdot \bar{x}^{\tau} \neq 0 \tag{A-10}$$

x und ein um τ verzögertes $\bar{x}$ sind nicht mehr identisch 0.

Es ist auch zu beachten, daß

$$x_1 \vee x_1^{\tau} \cdot x_2^{\tau} \neq x_1 \quad . \tag{A-11}$$

Würden wir hier absorbieren, so würde damit eine wirklich mögliche Ausfallart ($x_1^{\tau} \cdot x_2^{\tau}$, die gegen x_1 um τ verzögert ist) wegfallen. Natürlich gilt

$$x_1^{\tau} \vee x_1^{\tau} \cdot x_2^{\tau} = x_1^{\tau} \ ,$$

da hier beide Ausfallarten mit derselben Verzögerung auftreten.

Eine weitere Verallgemeinerung von Gl. (A-4) und (A-8) ist folgendes System von Boole'schen Funktionen:

$$\begin{aligned} y_1 &= f_1(x_1^{\tau_{11}}, x_2^{\tau_{12}}, \ldots, x_n^{\tau_{1n}}) \\ y_2 &= f_2(x_1^{\tau_{21}}, x_2^{\tau_{22}}, \ldots, x_n^{\tau_{2n}}) \\ &\vdots \\ y_\ell &= f_\ell(x_1^{\tau_{\ell 1}}, x_2^{\tau_{\ell 2}}, \ldots, x_n^{\tau_{\ell n}}) \quad . \end{aligned} \tag{A-12}$$

Für verschiedene Boole'sche Funktionen müssen die Verzögerungen τ_{ik}, τ_{jk} $(i \neq j)$ nicht mehr gleich sein. Ein einfaches Beispiel ist das System

$$\begin{aligned} y_1 &= x_1 \cdot x_2^{\tau} \\ y_2 &= x_1^{\tau} \cdot x_2^{2\tau} \quad . \end{aligned} \tag{A-13}$$

Damit haben wir die wichtigsten Regeln zur Verwendung von Boole'schen Ausdrücken mit Verzögerung zusammengestellt.

A.3 Vorkommen von Minimalschnitten bei Störfalldiagrammen

Wir gehen von einem Störfalldiagramm aus, bei dem neben Verzweigungen auch Verzögerungsglieder zugelassen sind (siehe Abb. 40).

Über die im Störfalldiagramm vorkommenden Verzweigungen machen wir folgende Festlegung:

1. Die negierten Elemente ($\bar{x}_1, \bar{x}_2, \ldots$) entsprechen immer dem Intaktzustand der

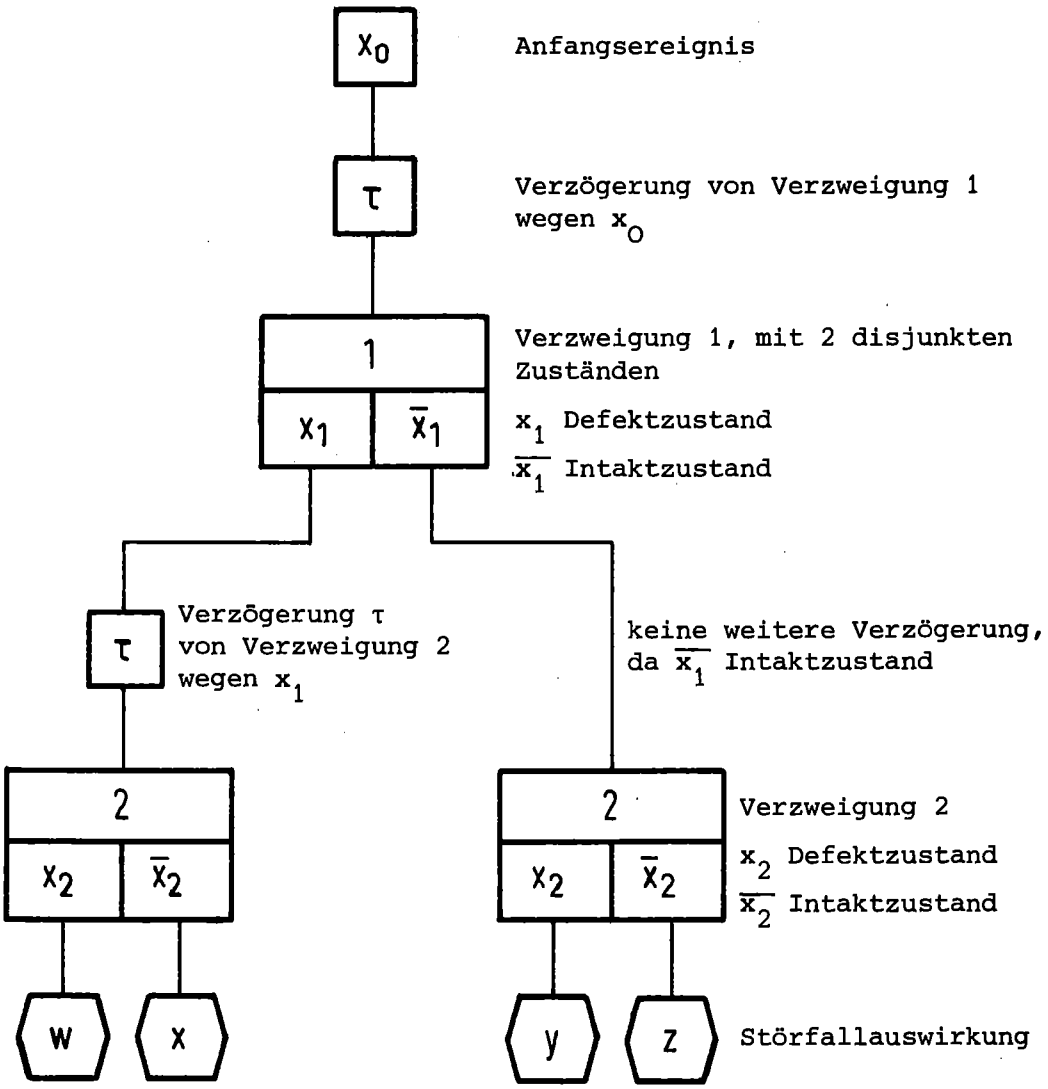


Abb. 40: Störfalldiagramm

Komponenten (1,2,...). Für x_0 wird angenommen, daß es nicht im Intaktzustand ist. Damit wird der in Abb. 13 eingeführte Index "n" (der auf Normalbetrieb verweist) ersetzt.

2. Es ist zu beachten, daß x_i und $\bar{x}_i$ nicht dieselbe Verzögerung haben müssen. Insbesondere wird der Intaktzustand keine weitere Verzögerung bringen, aber auch eine bereits vorliegende Verzögerung nicht mehr rückgängig machen.

Mit Gl. (5-1), (A-3), (A-6) erhalten wir für Verzweigungen:

$$y_1 = (x_0 \cdot x_1^{\tau})^{\tau} = x_0^{\tau} \cdot x_1^{2\tau}$$
$$y_2 = (x_0 \cdot \bar{x}_1^{\tau})^{\tau} = x_0^{\tau} \cdot \bar{x}_1^{\tau} \quad . \tag{A-14}$$

Damit erhalten wir aus dem Störfalldiagramm (Abb. 40) folgende Konjunktionsterme ($k_w, k_x, \ldots$):

$$k_w = x_0^{\tau} \cdot x_1^{2\tau} \cdot x_2^{2\tau}$$
$$k_x = x_0^{\tau} \cdot x_1^{2\tau} \cdot \bar{x}_2^{2\tau}$$
$$k_y = x_0^{\tau} \cdot \bar{x}_1^{\tau} \cdot x_2^{\tau} \tag{A-15}$$
$$k_z = x_0^{\tau} \cdot \bar{x}_1^{\tau} \cdot \bar{x}_2^{\tau} \quad \text{(Einzelfehler)} \quad .$$

Wir können also alle im Störfalldiagramm vorkommenden Ereigniskombinationen als Konjunktionsterme ausdrücken. Nach der in Abschnitt 5 eingeführten Konvention lassen wir alle Ereignisse weg, die nicht einen Ausfall beschreiben. Damit entfernen wir alle negierten Variablen ($\bar{x}_i$). Es ergeben sich aus (A-15) folgende Terme ($c_w, c_x, \ldots$):

$$c_w = x_0^{\tau} \cdot x_1^{2\tau} \cdot x_2^{2\tau}$$
$$c_x = x_0^{\tau} \cdot x_1^{2\tau} \tag{A-16}$$
$$c_y = x_0^{\tau} \cdot x_2^{\tau}$$
$$c_z = x_0^{\tau} \quad .$$

Aus dem Störfalldiagramm (Abb. 40) sehen wir, daß alle Ausdrücke zu definierten Störfallauswirkungen führen (w, x,...). Wir sehen weiterhin, daß keine Untermenge zur gleichen Störfallauswirkung führt. Damit gilt für alle Terme von (A-16), c_w, c_x, c_y, c_z, die Definition des Minimalschnitts. Man kann jedoch feststellen: Die Störfallauswirkung z wird durch ein Anfangsereignis (ohne zusätzliche Defektzustände) verursacht (x_0). Dagegen wird die Störfallauswirkung y durch ein Anfangsereignis und einen zusätzlichen Defektzustand verursacht ($x_0^{\tau} \cdot x_2^{\tau}$). Ebenso wird x durch ein Anfangsereignis und einen zusätzlichen

Defektzustand verursacht ($x_0^{\tau} \cdot x_1^{2\tau}$). Dagegen wird w durch ein Anfangsereignis und zwei zusätzliche Defektzustände verursacht ($x_0^{\tau} \cdot x_1^{2\tau} \cdot x_2^{2\tau}$). Auf keinen Fall gehören die vier Terme von (A-16) zur gleichen Boole'schen Funktion.

Wir können nun von einem Störfalldiagramm zu einem System von Fehlerbäumen übergehen. Dabei sehen wir auch, daß die unerwünschten Ereignisse w, x, y, z teilweise mit verschiedenen Verzögerungen eintreten (genau wie die entsprechenden Störfallauswirkungen).

Wir können unsere Ergebnisse folgendermaßen graphisch darstellen, was auch unsere soeben gemachten Bemerkungen unterstreicht (Fehlerbäume Abb. 41 a-d).

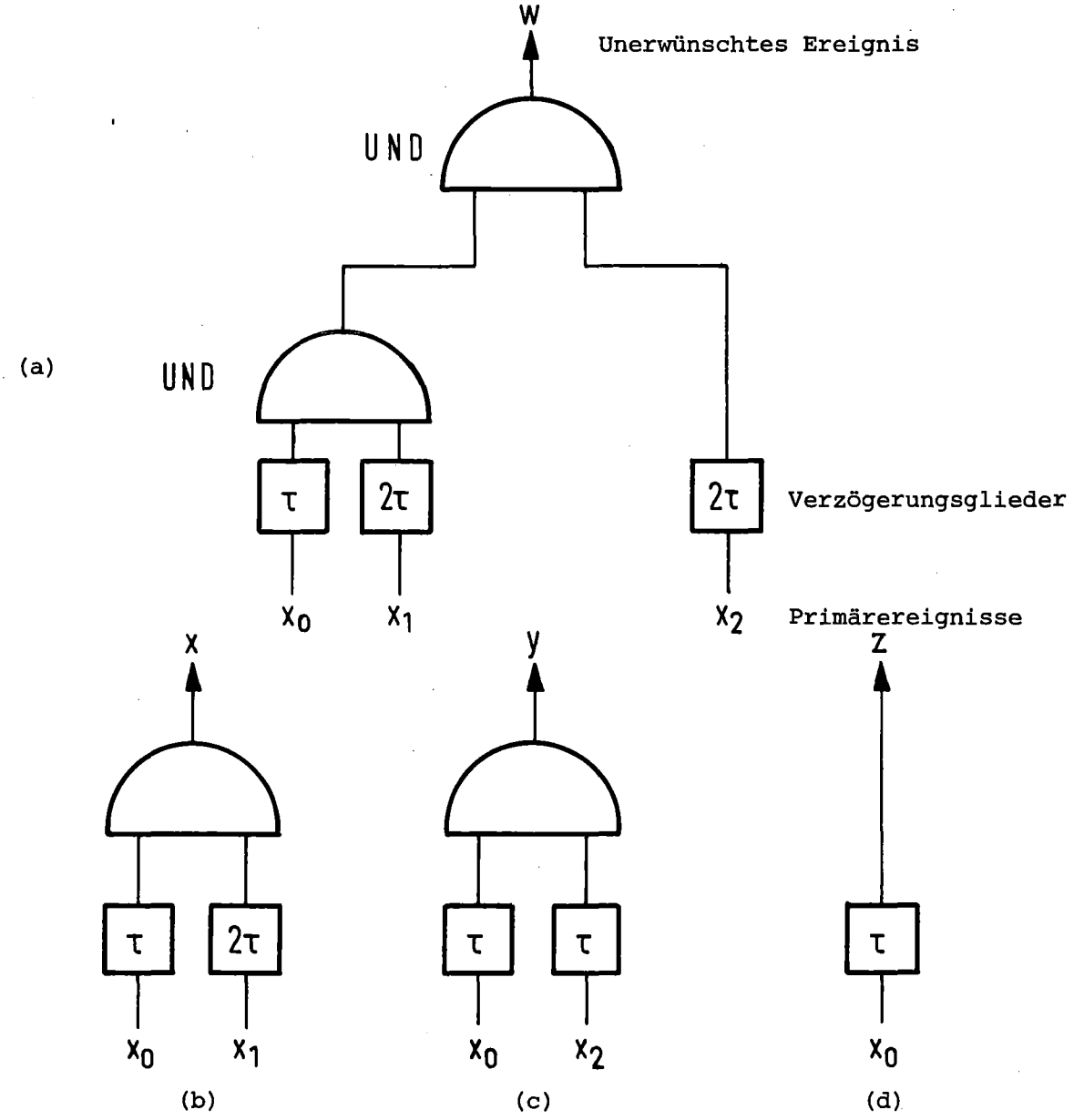


Abb. 41 a-d: Fehlerbäume

A.4 Vorkommen von Minimalschnitten bei einem Fehlerbaum

Wir gehen von einem Fehlerbaum aus, bei dem, entsprechend den Prozeßschritten eines Systems verschiedene Fehlerkombinationen zum "Unerwünschten Ereignis" w führen (vgl. z.B. Abb. 5, 6). Dazu nehmen wir an, daß die Boole'schen Variablen die zu einem Prozeßschritt gehören noch untereinander verzögert sein können (Abb. 42).

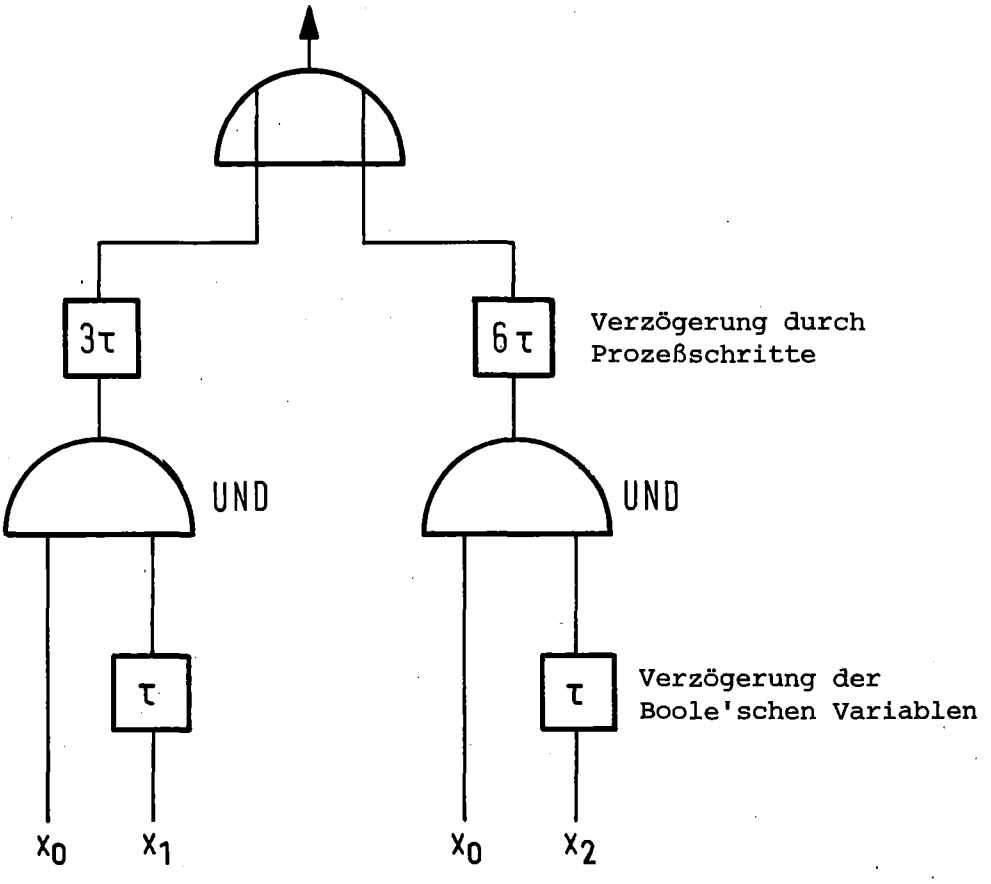


Abb. 42: Fehlerbaum

Es ist nun eine wichtige Aussage der Fehlerbaumanalyse, daß jeder kohärente Fehlerbaum eindeutig in Minimalschnitte zerlegt werden kann. (Ein Fehlerbaum ist kohärent, wenn kein Systemausfall durch den Ausfall weiterer Komponenten wieder rückgängig gemacht werden kann und wenn zusätzlich keine Komponente ohne Einfluß auf das Ausfallverhalten des Systems ist /22/). Wir erhalten so aus Abb. 42 zwei Minimalschnitte:

$$c_w^{3\tau} = (x_o \cdot x_1^{\tau})^{3\tau}$$
$$c_w^{6\tau} = (x_o \cdot x_2^{\tau})^{6\tau} \quad . \tag{A-17}$$

Damit läßt sich der gesamte Fehlerbaum auch schreiben

$$w = c_w^{3\tau} \vee c_w^{6\tau} = (x_o \cdot x_1^{\tau})^{3\tau} \vee (x_o \cdot x_2^{\tau})^{6\tau} \quad . \tag{A-18}$$

Nun fragen wir, ob es auch möglich ist, den Fehlerbaum in Störfalldiagramme zu übertragen. Dies ist im Allgemeinen nicht möglich. Dies läßt sich folgendermaßen zeigen. Wir sehen, daß in einem Konjunktionsterm, wie er in Gl.(A-15) auftritt, alle Informationen über Verzögerungsglieder enthalten sind. Daraus kann man eindeutig auf den entsprechenden Minimalschnitt schließen. Haben wir jedoch einen Minimalschnitt z.B. von der Form

$$c_x = x_o \cdot x_4^{\tau} \quad , \tag{A-19}$$

so können wir zwar sagen, daß x_4^{τ} nach x_o kommen wird und, daß $\bar{x}_1, \bar{x}_2$ nichts zur Verzögerung beitragen (als Intaktzustände). Jedoch können wir nicht sagen, ob

$$x_1 \text{ vor } x_2 \text{ oder } x_2 \text{ vor } x_1$$

angefordert wird. Damit ist das Störfalldiagramm nur bis auf eine Permutation festgelegt. Dieser Fall lag auch bei dem in den Abschnitten 4 bis 6 behandelten System vor. Wir haben dort keine Verzögerung. Es muß im einzelnen geprüft werden, ob eine Vertauschung von Verzweigungen zum selben Resultat führt. Wenn wir eine Ursache/Wirkungsbeziehung haben, so können wir die Verzweigungen nicht mehr vertauschen. Auch dann werden wir noch Minimalschnitte im Sinne unserer Definition erhalten. Weiterhin kann man diese Beziehungen in eine verallgemeinerte Fehlerbaumanalyse einbeziehen /12/.

Unter den soeben gemachten Einschränkungen erhalten wir aus (A-17) durch Hinzufügen der negierten Elemente folgende Konjunktionsterme:

$$k_w^{3\tau} = (x_o \cdot x_1^{\tau} \cdot \bar{x}_2^{\tau})^{3\tau}$$
$$k_w^{6\tau} = (x_o \cdot \bar{x}_1 \cdot x_2^{\tau})^{6\tau} \quad . \tag{A-20}$$

Es ist zu beachten, daß die Reihenfolge von x_1^{τ} und $\bar{x}_2^{\tau}$ nicht festgelegt ist. Jedoch wird x_1^{τ} nach x_o kommen.

Ein Ausdruck $k_w^{3\tau}$ entspricht einem Weg im Störfalldiagramm von Ausgangsereignis $x_0^{3\tau}$ bis zur Störfallauswirkung w. Dabei gelten $k_w^{3\tau}, k_w^{6\tau}$ für verschiedene Zeiten. Wir zeigen als Veranschaulichung ein Störfalldiagramm:

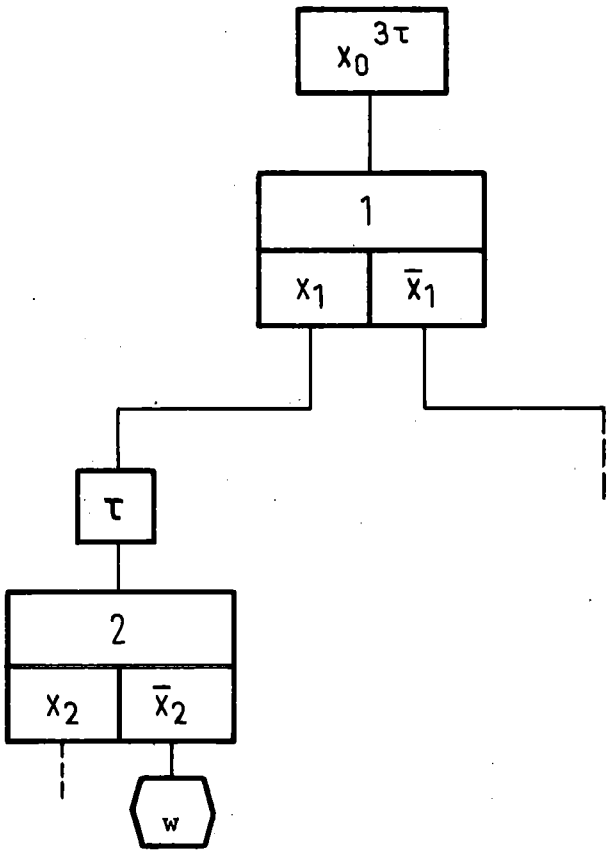


Abb. 43: Weg im Störfalldiagramm.

Zusammenfassend können wir sagen:

1. Es wurde für ein Modell mit Boole'schen Variablen und Verzögerungsgliedern gezeigt, daß im Störfalldiagramm und im Fehlerbaum Minimalschnitte auftreten.

2. Es wurde gezeigt, daß ein Störfalldiagramm sich in Fehlerbäume übertragen läßt. Es wurde auch gezeigt, daß ein Fehlerbaum nicht allgemein in ein Störfalldiagramm übertragen werden kann. Sind die dabei auftretenden Permutationen von Ereignissen ohne Einfluß auf den Störfall, so kann eine beliebige Darstellung des Störfalldiagramms verwendet werden. Dies war auch bei unserem Beispiel in Tab. 2 der Fall.