AAEC-LIB/Trans-731

AUSTRALIAN ATOMIC ENERGY COMMISSION RESEARCH ESTABLISHMENT

GERMAN STANDARD : DIN-25419/1

# INCIDENT SEQUENCE ANALYSIS EVENT TREES : METHODS AND GRAPHICAL SYMBOLS

Translated from the German by
A. Bicevskis

November 1980

AUSTRALIAN ATOMIC ENERGY COMMISSION

LIB/TRANS SERIES

Translations in this series were prepared as working documents for the use of research scientists at the Australian Atomic Energy Commission.

In order that they might be made available with the least possible delay, no attempt has been made to edit them, nor have all typing errors necessarily been identified and corrected.

Copies of translations in this series are made available to interested organizations and individuals only on the express understanding that they may be imperfect and do not aim to meet the standards of a published document. The Commission will not be held responsible for any inaccuracies in the translated text or for any errors resulting therefrom.

If any further reproduction of this translation is made by the recipient thereof, this note must be reproduced together with the text of the translation.

GERMAN STANDARD JUNE 1977

# INCIDENT SEQUENCE ANALYSIS
# EVENT TREES
# METHODS AND GRAPHICAL SYMBOLS

DIN 25 419 Part 1

The analysis of Event Trees is to be distinguished from "Fault-Tree Analysis". In the case of Event Trees, some initiating events are specified and the problem is to find the resultant undesirable event or consequences, whilst in the case of Fault Trees the undesirable result is given and the problem is to find the combination of events which brings it about. This standard contains a description of symbols as well as a clarification of their use for a graphical representation of incident or failure sequences.

## 1. Area of Application

The methods described here can be used to represent incident sequences for a wide variety of plants. The letters used here do not constitute a standard.

## 2. Purpose

Event Trees can be used to both represent in a clear manner and analyse incident sequences, that is, the logical and time dependent progression of event sequences which are brought about by the failure of some plant items as incorrect operation. The graphical symbols adopted facilitate a qualitative representation of the relationships as well as a numerical assessment of the failure sequences. The purpose of this Standard is to achieve a uniform graphical representation of the failure sequences. To this end, use should be made of the graphical symbols given in this Standard.

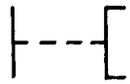
## 3. Method

The method treats the sequence where an Initiating Event (for example, failure of a plant item as incorrect operation), leads to subsequent events as a result of time dependent physical (dynamic) processes which, in turn, bring

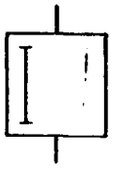
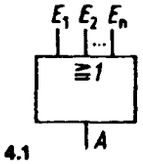
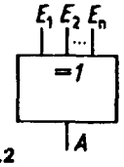
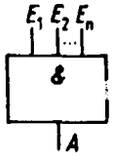
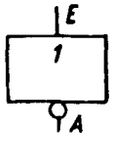
..../2

about further events. In the absence of such physical processes, the failure remains limited to the defective plant item under consideration. In such a case a graphical representation is not necessary. However, in many cases the logical junctions and physical processes associated with the failures are so complex that it is hardly possible to grasp the essence of the problem without a graphical representation. Of particular importance are the active and passive safety devices in the case of large installations - they introduce the possibility of their own failure. As a result of the logical connections of actions (input events) with the "failed" or "not failed" condition of the various units under consideration (plant items, sub-systems or systems) various failure sequences can take place with a specific associated end result. A set of failure sequences can be represented as a network with a large number of possible end results (failure effects). A particular aim of the graphical analysis is to facilitate the calculation of the probabilities of the various results - a failure sequence is only fully characterised when, besides the possible outcome, the corresponding probability is also assessed.

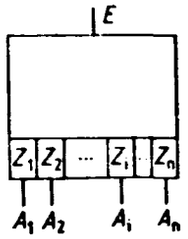
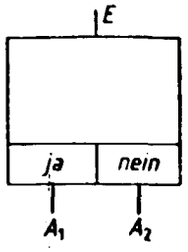
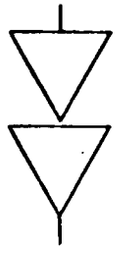
4. Symbols for Graphical Representation of Failure Sequences

| No. | Symbol | Description | Remarks |
|---|---|---|---|
| 1 |  | Initial event, initiating event.<br>Intermediate event.<br>End effect of failure sequence, end of failure sequence. | The symbol contains the description of the initiating, intermediate or end event.<br>Note.Symbols (1),(15) & (21) in example<br>If the Event-Tree is used to develop a computer program, the symbol can be used as shown in DIN 66001, Edition October 1969, Section 4.3.3. |
| 2 |  | Line of action with remarks | See Symbol (12) in example. |

..../3

| No. | Symbol | Description | Remarks |
|---|---|---|---|
| 3 |  | Delayed action. | See Symbol (11) in example. DIN 40 700 Part 14, Edition July 1976, No. 65. |
| 4 |   4.1 | "OR" (inclusive OR). Disjunction of events (actions) $E_1$, $E_2$, ...$E_n$ $A = E_1 \vee E_2 \vee \ldots E_n$ A takes place if one or more of the events $E_1$ to $E_n$ occur. | See Symbol (3) in example. DIN 40 700 Part 14, Edition July 1976, No. 23. V in accordance with DIN 66 000 and DIN 5474. With many inputs the input side can be extended in accordance with DIN 40 719 Part 6, Edition March 1977, No. 12.3. |
| 4 |   4.2 | "OR" (exclusive OR). Disjunction of mutually exclusive events (actions) $E_1$, $E_2$ ...$E_n$ $A = E_1 \vec{\vee} E_2 \vec{\vee} \ldots E_n$ A takes place, if anyone of the mutually exclusive events ($E_1$ or $E_2$ or ...$E_n$) occurs. | See Symbol (10) in example. DIN 40 700 Part 14, Edition July 1976, No. 28. V in accordance with DIN 66 000 and DIN 5474. With many inputs the input side can be extended in accordance with Design DIN 40 719 Part 6, Edition March 1977, No. 12.3. |
| 5 |   | "AND". Conjunction of events (actions) $E_1$, $E_2$ ...$E_n$ $A = E_1 \wedge E_2 \wedge \ldots E_n$ The events $E_1$, $E_2$ ...$E_n$ are generally statistically related. A takes place if $E_1$ and $E_2$ and ...$E_n$ (all events) occur. | DIN 40 700 Part 14, Edition July 1976, No. 22. $\wedge$ in accordance with DIN 66 000 and DIN 5474. With many inputs the input side can be extended in accordance design DIN 40 719 Part 6, Edition March 1977, No. 11.3. In the case of independent input events, the independence can be highlighted by underlining &. |
| 6 |   | "NOT". Negation of the event (action) E. $A = \bar{E}$ A takes place with E absent ($\bar{E}$) and vice versa. | DIN 40 700 Part 14, Edition July 1976, No. 24. Dash ¯ on top of E in accordance with DIN 66 000. |

..../4

| No. | Symbol | Description | Remarks |
|---|---|---|---|
| 7 |  7.1 | Multiple branching. Event (action) E leads to a demand on the unit under consideration with several possible states. Branching of event E by conjunction with the disjunctive states $Z_i$ $A_i = E \wedge Z$ | Example: E = start-up signal for 2 pumps $A_1$ = 2 pumps start $A_2$ = 1 pump start $A_3$ = no pump start. If a computer program is developed from the Event Tree, the symbol[5] to be used can be obtained from DIN 66 001, Edition October 1969, Sections 4.1.1 and 4.4.1. |
| |  7.2 | Single branching. Event (action) E leads to a demand on the unit under consideration with 2 possible disjunctive states. Branching of E by conjunction with the state $Z_1$ (yes) and the state $Z_2$ (no) of the unit under consideration. $A_1 = E \wedge Z_1$; $A_2 = E \wedge Z_2$ Branching of the event (action) E can also take place by satisfying or not satisfying a criterion described in the symbol. | See symbols (5) and (20) in the example. The function of the unit under consideration as a physical criterion are described on the symbol. The outputs are marked "yes" or "no" or in a similar manner. If a computer program is developed from the Event Tree, the symbols to be used can be obtained from DIN 66 001, Edition October 1969, Section 4.1.1. |
| 8 |  | Indicates transfer or continuation. The Event Tree is terminated or continued at another place as indicated by this symbol. | See symbol (16) in example. It is useful to assign a letter or number to the symbol. If a computer program is developed from the Event Tree, the symbols to be used can be obtained from DIN 66 001, Edition October 1969, Section 4.3.2. |

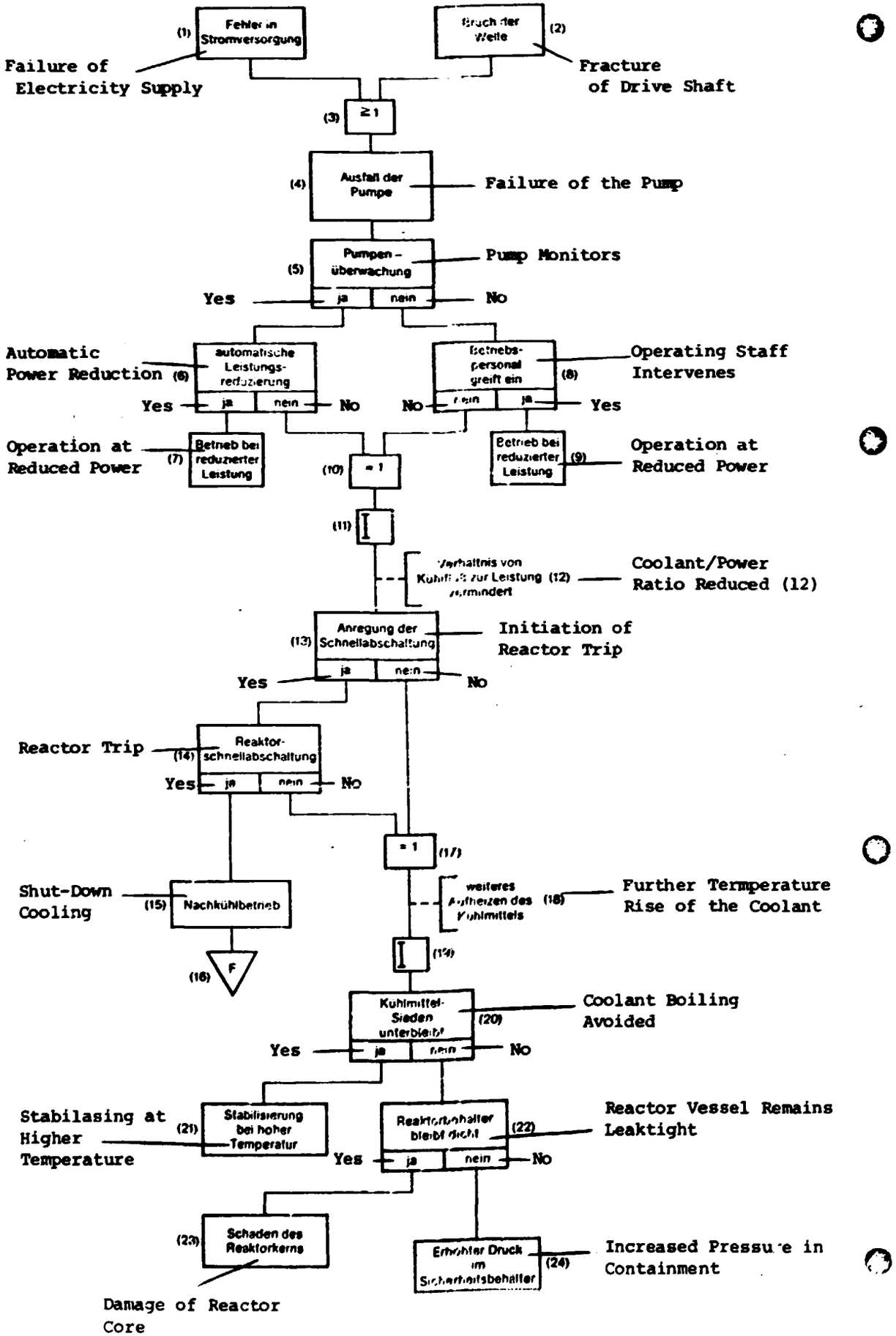
Remarks on the Use of Symbols

Two OR-symbols have been introduced because of different logical meaning. The difference is of particular value for the subsequent application of probability calculations.

The symbols can be varied in size and aspect ratio to suit the application in hand.

The graphical representation of a failure sequence is demonstrated by the following example - "Failure of a Reactor Primary Coolant Pump". The stress is here on the use of the symbols and their interconnection rather than on a realistic representation of a reactor incident. The symbols are numbered sequentially. The incident can be initiated by two different events (1) and (2). Both events lead to a loss of pump in the primary circuit. If the protection devices (5) are functioning correctly (for example, current and rotational speed monitors), the reactor power is reduced automatically (6). If the monitors fail, after a suitable delay (11) a reactor trip is initiated (13). The reactor is thus normally changed over to shut-down cooling (15). However, if the trip does not occur (14), under certain conditions boiling in the reactor core can take place (2). If the reactor vessel remains leaktight, damage can arise in the reactor core (23), but the coolant and radioactivity would not be released into the containment space. The final protection to the environment is provided by the containment (24).

Example
Beispiel
Pump Failure in Reactor Coolant Circuit
Ausfall der Pumpe eines Reaktorkühlkreislaufes



DK 62.004.64(084.21):52-192:003.62 DEUTSCHE NORMEN Juni 1977

DIN-25419/1

# Störfallablaufanalyse
## Störfallablaufdiagramm
## Methode und Bildzeichen

DIN
25 419
Teil 1

Incident sequence analysis; event tree, method and graphical symbols



Die Analyse von Störfallabläufen ist zu unterscheiden von der „Fehlerbaumanalyse". Während bei der Analyse von Störfallabläufen die unerwünschten Ereignisse, die aus einer bestimmten Ursache resultieren, gesucht werden, gibt man bei der „Fehlerbaumanalyse" das unerwünschte Ereignis vor und sucht aus Eingangsereignissen die Kombinationen zu finden, die zu diesem Ereignis führen. In dieser Norm werden Bildzeichen und Erläuterungen zur graphischen Darstellung von Störfallabläufen angegeben.

## 1 Anwendungsbereich

Das hier behandelte Verfahren kann zur Analyse von Störfallabläufen bei Anlagen aller Art angewandt werden. Verwendete Buchstaben sind nicht Gegenstand dieser Norm.

## 2 Zweck

Mittels des Störfallablaufdiagramms können Störfallabläufe, d. h. die logischen und zeitlichen Abläufe von Folgeereignissen, die durch den Ausfall eines Bauteils oder durch Fehlbedienung ausgelöst werden, in einfacher und übersichtlicher Weise dargestellt und analysiert werden. Die dazu benutzten Bildzeichen ermöglichen einerseits die qualitative Darstellung der Zusammenhänge, andererseits aber auch die Durchrechnung der Störfallabläufe. Der Zweck der Festlegungen ist, eine einheitliche graphische Darstellung von Störfallabläufen zu erreichen. Dazu sollen die in dieser Norm enthaltenen Bildzeichen benutzt werden.

## 3 Methode

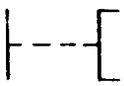
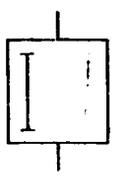
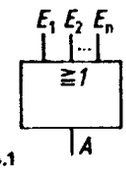
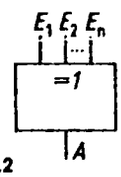
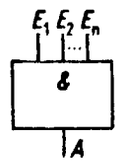
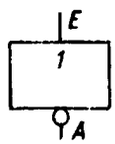
Die Methode geht davon aus, daß nach einem Anfangsereignis (z. B. Ausfall eines Bauelements oder Fehlbedienung) infolge zeitabhängiger physikalischer (dynamischer) Vorgänge Folgeereignisse auftreten, die wiederum Anlaß zu weiteren Folgeereignissen geben. Fehlen solche physikalischen Auswirkungen, so bleibt der Störfall auf den Ausfall des betrachteten Bauelements beschränkt. In diesem Fall erübrigt sich eine graphische Darstellung. Häufig sind jedoch bei Störfällen die physikalischen Vorgänge und logischen Verknüpfungen der Folgeereignisse so verwickelt, daß man ohne graphische Darstellung den Sachverhalt nur schwer durchschaut. Eine besondere Rolle spielen dabei in größeren Anlagen die aktiven und passiven Sicherheitseinrichtungen. Sie bergen ebenfalls die Möglichkeit des Versagens in sich. Aus der logischen Verknüpfung von Wirkungen (Eingangsereignissen) mit der Zuständen „intakt" oder „ausgefallen" der einzelnen Betrachtungseinheiten (Elemente, Teilsysteme oder Systeme) ergeben sich unterschiedliche Störfallabläufe mit einem jeweiligen Endzustand. Der ganze Störfallkomplex stellt sich daher als ein Netzwerk mit einer Vielzahl von möglichen Endzuständen (Störfallauswirkungen) dar. Ein besonderes Ziel der graphischen Analyse ist es, die Berechnung der Wahrscheinlichkeit dieser einzelnen Auswirkungen zu ermöglichen, da ein Störfall nur vollständig charakterisiert ist, wenn neben seinen möglichen Auswirkungen auch deren Wahrscheinlichkeiten bekannt sind.

Fortsetzung Seite 2 bis 4
Erläuterungen Seite 3

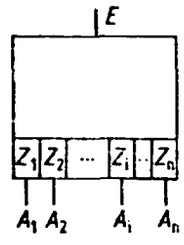
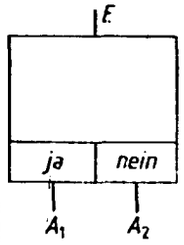
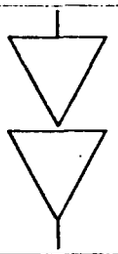
Normenausschuß Kerntechnik (NKe) im DIN Deutsches Institut für Normung e. V.

Alleinverkauf der Normen durch Beuth Verlag GmbH, Berlin 30 und Köln 1
06.77

## 4 Bildzeichen für die graphische Darstellung von Störfallabläufen

| Lfd. Nr | Bildzeichen | Aussage | Bemerkung |
|---|---|---|---|
| 1 |  | Anfangsereignis, auslösendes Ereignis.<br>Zwischenereignis.<br>Störfallauswirkung, Ende des Störfallablaufs. | In das Bildzeichen wird das auslösende Ereignis, das Zwischenereignis oder die Auswirkung eingetragen.<br>Siehe Bildzeichen (1), (15), (21) im Beispiel.<br>Wird aus dem Störfallablaufdiagramm ein Rechenprogramm entwickelt, so kann das Bildzeichen nach DIN 66001, Ausgabe Oktober 1969, Abschnitt 4.3.3, verwendet werden. |
| 2 |  | Wirkungslinie mit Bemerkung | Siehe Bildzeichen (12) im Beispiel. |
| 3 |  | Verzögerung der Wirkung | Siehe Bildzeichen (11) im Beispiel.<br>DIN 40700 Teil 14, Ausgabe Juli 1976, Nr 65. |
| 4<br>4.1 |  | „ODER" (einschließendes oder inklusives ODER) Disjunktion der Ereignisse (Wirkungen) $E_1, E_2 \ldots E_n$.<br>$A = E_1 \vee E_2 \vee \ldots E_n$.<br>$A$ ist vorhanden, wenn eines oder mehrere der Ereignisse $E_1$ bis $E_n$ vorhanden sind. | Siehe Bildzeichen (3) im Beispiel.<br>DIN 40700 Teil 14, Ausgabe Juli 1976, Nr 23.<br>$\vee$ nach DIN 66000 und DIN 5474.<br>Bei vielen Eingängen Seitenlinie auf der Eingangsseite verlängerbar entsprechend DIN 40719 Teil 6, Ausgabe März 1977, Nr 12.3. |
| 4<br>4.2 |  | „ODER" (ausschließendes oder exklusives ODER). Disjunktion der sich gegenseitig ausschließenden Ereignisse (Wirkungen) $E_1, E_2 \ldots E_n$.<br>$A = E_1 \vee E_2 \vee \ldots E_n$.<br>$A$ ist vorhanden, wenn eines der sich ausschließenden Ereignisse ($E_1$ oder $E_2$ oder $\ldots E_n$) vorhanden ist. | Siehe Bildzeichen (10) im Beispiel.<br>DIN 40700 Teil 14, Ausgabe Juli 1976, Nr 28.<br>$\vee$ nach DIN 66000 und DIN 5474.<br>Bei vielen Eingängen Seitenlinie auf der Eingangsseite verlängerbar entsprechend Entwurf DIN 40719 Teil 6, Ausgabe März 1977, Nr 12.3. |
| 5 |  | „UND"<br>Konjunktion der Ereignisse (Wirkungen) $E_1, E_2, \ldots E_n$.<br>$A = E_1 \wedge E_2 \wedge \ldots E_n$.<br>Die Ereignisse $E_1, E_2, \ldots E_n$ sind im allgemeinen voneinander statistisch abhängig. $A$ ist vorhanden, wenn $E_1$ und $E_2$ und $\ldots E_n$ (alle Ereignisse) vorhanden sind. | DIN 40700 Teil 14, Ausgabe Juli 1976, Nr 22.<br>$\wedge$ nach DIN 66000 und DIN 5474.<br>Bei vielen Eingängen Seitenlinie auf der Eingangsseite verlängerbar entsprechend Entwurf DIN 40719 Teil 6, Ausgabe März 1977, Nr 11.3. Bei unabhängigen Eingangsereignissen kann zur Herausstellung der Unabhängigkeit das & unterstrichen werden. |
| 6 |  | „NICHT"<br>Negation des Ereignisses (der Wirkung) $E$.<br>$A = \bar{E}$.<br>$A$ ist vorhanden, wenn $E$ nicht vorhanden ist ($\bar{E}$) und umgekehrt. | DIN 40700 Teil 14, Ausgabe Juli 1976, Nr 24.<br>Querstrich über dem $E$ nach DIN 66000 |

Fortsetzung der Tabelle

| Lfd. Nr | Bildzeichen | Aussage | Bemerkung |
|---|---|---|---|
| 7 |  7.1 | Mehrfachverzweigung<br>Ereignis (Wirkung) $E$ führt zur Funktionsanforderung einer Betrachtungseinheit mit mehreren möglichen Zuständen.<br>Verzweigung des Ereignisses $E$ durch Konjunktion mit den disjunkten Zuständen $Z_i$.<br>$A_i = E \wedge Z_i$ | Beispiel:<br>$E$ = Startsignal für 2 Pumpen.<br>$A_1$ = 2 Pumpen starten.<br>$A_2$ = 1 Pumpe startet.<br>$A_3$ = keine Pumpe startet.<br>Wird aus dem Störfallablaufdiagramm ein Rechenprogramm entwickelt, so kann das Bildzeichen nach DIN 66001, Ausgabe Oktober 1969, Abschnitte 4.1.1 und 4.4.1, verwendet werden. |
| |  7.2 | Einfache Verzweigung<br>Ereignis (Wirkung) $E$ führt zur Funktionsanforderung an eine Betrachtungseinheit mit 2 möglichen disjunkten Zuständen.<br>Verzweigung von $E$ durch Konjunktion mit dem Zustand $Z_1$ (ja) und dem Zustand $Z_2$ (nein) der Betrachtungseinheit.<br>$A_1 = E \wedge Z_1$; $A_2 = E \wedge Z_2$<br>Die Verzweigung des Ereignisses (der Wirkung) $E$ kann auch durch Erfüllen bzw. Nichterfüllen eines im Feld beschriebenen physikalischen Kriteriums eintreten. | Siehe Bildzeichen (5) und (20) im Beispiel.<br>Die Funktion der Betrachtungseinheit oder das physikalische Kriterium wird in das Bildzeichen eingetragen. Die Ausgänge werden mit „ja" und „nein" oder auf andere Weise sinngemäß gekennzeichnet.<br>Wird aus dem Störfallablaufdiagramm ein Rechenprogramm entwickelt, so kann das Bildzeichen nach DIN 66001, Ausgabe Oktober 1969, Abschnitt 4.1.1, verwendet werden. |
| 8 |  | Übertragungs- bzw. Fortsetzungsbildzeichen.<br>Das Störfallablaufdiagramm wird mit diesem Bildzeichen abgebrochen bzw. an anderer Stelle fortgesetzt. | Siehe Bildzeichen (16) im Beispiel. Das Bildzeichen wird zweckmäßigerweise mit einem Buchstaben oder einer Zahl gekennzeichnet.<br>Wird aus dem Störfallablaufdiagramm ein Rechenprogramm entwickelt, so kann das Bildzeichen nach DIN 66001, Ausgabe Oktober 1969, Abschnitt 4.3.2, verwendet werden. |

## Erläuterungen zur Anwendung der Bildzeichen

Die beiden ODER-Bildzeichen Nr 4.1 und 4.2 wurden wegen ihres unterschiedlichen logischen Sinngehaltes eingeführt. Die Unterscheidung ist insbesondere von Vorteil für die spätere Anwendung von Wahrscheinlichkeitsrechenregeln.

Die Bildzeichen können in Größe und Seitenverhältnis den jeweiligen Bedürfnissen angepaßt werden.

Als Beispiel ist die graphische Darstellung des Störfalls „Ausfall der Pumpe eines Reaktorkühlkreislaufes" beigefügt. Dabei geht es mehr um die Vorstellung der Bildzeichen und deren Verknüpfung als um die wirklichkeitsgetreue Darstellung eines Reaktorstörfalles. Die einzelnen Bildzeichen sind laufend durchnumeriert. Der Störfall kann durch zwei verschiedene Ereignisse (1), (2) eingeleitet werden. Beide Ereignisse führen zum Ausfall der Pumpe in einem Primärkreislauf. Funktionieren die Überwachungseinrichtungen (5) (beispielsweise Stromüberwachung und Drehzahlüberwachung), dann erfolgt automatisch eine entsprechende Reduzierung der Reaktorleistung (6). Bei Versagen der Überwachungseinrichtungen wird nach einer gewissen Verzögerung (11) die Reaktorschnellabschaltung angeregt (13). Der Reaktor geht dadurch normalerweise in den Nachkühlbetrieb (15) über. Erfolgt jedoch die Schnellabschaltung (14) nicht, dann kann es – unter gewissen Umständen – zum Sieden des Kühlmittels im Reaktor (20) kommen. Wenn der Reaktorbehälter dabei dicht bleibt, kommt es zwar zu Schäden im Reaktorkern (23), aber nicht zum Austritt von Kühlmittel und Radioaktivität in den Sicherheitsbehälter. Die letzte Sicherheitsfunktion bezüglich des Umgebungsschutzes hat schließlich der Sicherheitsbehälter (24).

Beispiel
Ausfall der Pumpe eines Reaktorkühlkreislaufes