Some points of advanced alarm system design

Forskningscenter Risø, Roskilde

Publication date:
1977

Document Version
Publisher's PDF, also known as Version of record

A. E. K. Risø

Risø - M - 1908

Risø - M - 1908

Title and author(s)

Some Points of Advanced Alarm System Design

by

Elod Hollo *

Date January 1977

Department or group

Electronics

Group's own registration number(s)

R-2-77

pages + tables + illustrations

Abstract

In this report some of the more relevant questions of advanced alarm analysis systems for nuclear power plant installations are described. The development of such alarm systems poses three main tasks:

- the development of formal alarm handling methods,
- the design of alarm patterns,
- and the development of alarm analysis system.

This paper deals with the major aspects of these three points. The close relation between the alarm analysis and the plant disturbance analysis procedure is emphasized.

* Permanent address:
Institute for Electrical Power Research (VEIKI)
H-1050 Budapest
Zrinyi-street 1
HUNGARY

Copies to

Available on request from the Library of the Danish Atomic Energy Commission (Atomenergikommissionens Bibliotek), Risø, DK-4000 Roskilde, Denmark
Telephone: (03) 35 51 01, ext. 334, telex: 43116

Fi 25-204

ISBN 87-550-0443-1

CONTENTS

1. INTRODUCTION

An alarm system is a basic feature of a nuclear power plant control and supervision system. If an equipment is not in a specified state or a process variable goes outside specified limits an alarm is produced. Due to the growing unit size of plants, the number of alarms presented during a disturbed plant situation has been increasing. It is often a difficult task for the operator to interpret the large number of rapidly arriving alarms, therefore an advanced alarm analysis system is highly desirable.

The purpose of the alarm analysis design is to devise a systematic method which when an alarm or alarm pattern occurs makes it possible:

- to deduce the possible prime causes of alarms,
- to predict the resulting significant failures or events ahead,
- to determine the rough probability categories of consequences,
- to present the information for the operator in a suitable, simple, clear form.

Alarms are the names given to the signals arising from threshold detectors, such as contact switches, pressure switches, comparators, etc.

It is evident that to perform these tasks a highly advanced alarm analysis system is needed. In addition in a lot of cases the existing alarm pattern is not adequate due to instrumentation insufficiency. Therefore alarms must not be used as the only basis of the analysis procedure, but must rather be used as an initiator for a further analysis. From this aspect, an alarm pattern may be adequate if it only indicates the presence of significant component failures or extreme parameter changes which require more detailed analysis to find the prime cause, the possible consequences, the operations to be taken. In other words <u>the alarm analysis forms a part of a more detailed disturbance analysis system.</u> The disturbance analysis will reduce any ambiguity in the alarm analysis, and make the analysis more precise, by using information from non-threshold devices such as pressure recorders, and operator supplied information.

The importance of an alarm analysis system depends on the advanced state of the detailed disturbance analysis system. In simple disturbance analysis systems the alarm analysis may play an important role of performing the tasks formerly mentioned, but there will generally be a relatively large range of undefined causes and consequences, i.e. in this case the question of alarm pattern adequacy is very important. In advanced disturbance analysis systems it is not necessary that in all cases the alarm patterns directly be related to the disturbance situation. The closer the better, but it is not necessary to have unique identification of cause. The disturbance analysis system may include diagnosis steps, but this will be as a support for diagnosis within a fixed time limit and for a fixed range of possible causes.

The development of an advanced alarm system poses three main tasks:

- the development of formal alarm handling methods,
- the design and investigation of alarm patterns,
- and the development of alarm analysis system.

In this paper some aspects of these problems are examined. Special attention is directed to the interactive real time alarm analysis being capable of handling several types of alarm sequence; non serious alarms with slow arrival or multiple non serious alarms with rapid arrival, or multiple serious alarms with rapid arrival which are accompanied by their own designed protective action. In case of rapid arrival of multiple serious alarms, the designed plant protection system is activated and only "post mortem" (post shutdown) alarm analysis may be carried out.

It is noted that no attempt is made to treat all aspects of the design of an alarm system, only the most relevant questions are mentioned.

2. ALARM HANDLING METHODS

Up to the present several different methods have been developed for alarm handling during abnormal situations in nuclear reactors and power plants. In practice three of them are used: alarm combinations (decision tables), alarm trees, and cause--consequence diagrams. Each of them has advantages and drawbacks to be taken into consideration before the method is implemented.

2.1. Alarm Combinations (Decision Tables)

Decision tables were firstly used and nowadays they are mainly applied in simple alarm handling systems.

Their advantages:
- simple method with a well-arranged table or list
- easy to change according to experience
- suitable for computer storage

Their drawbacks:
- all possible disturbance situations must be determined beforehand. Able to handle only alarm patterns involved in the table or list.

2.2. Alarm Trees (Fault Trees)

Presently fault trees are generally used for disturbance analysis.

Their advantages:
- relatively simple method
- relatively easy to change (though not more so than decision tables)
- suitable for computer storage
- time delays and event sequence may be recorded

Their drawbacks:
- see advantages of cause-consequence diagrams.

2.3. Cause-Consequence Diagrams

Lately cause-consequence diagrams have been used for disturbance analysis of nuclear plant status.

Their advantages:
- directly related to the process physical structure
- directly express the event sequences
- operator interaction is made easy because of natural sequencing
- vulnerable states can be handled
- probabilities, time delays may be easily handled

Their drawbacks:
- in real-time interactive analysis systems full advantage can only be obtained with relatively slow changing processes,
- analysis, checking and input of cc diagrams can be time consuming.

Comparing the advantages to drawbacks of the different alarm handling methods mentioned above the cause-consequence diagrams combined with fault trees seem to be most effective for using in nuclear power plants. The methodology of ccd's is described in (1).

3. ALARM PATTERN DESIGN

Alarm patterns form the part of the presented information by the process control and information system shown in Fig. 1. Two main tasks arise: The possible alarm pattern design in a new system or alarm pattern analysis in a given fixed system.

The design of alarm patterns can be performed during the design of the process instrumentation system or if modifications may be introduced in a given system and the existing alarm patterns are not adequate. To develop proper alarm patterns the following questions must be answered:

- How many alarms do we need?
- Where are the alarms needed?
- What kind of alarms are needed?

The answers to these questions are determined by technical and philosophical aspects. The technical aspects comprise the complexity and type of the process, the philosophical ones are

formed by the problems of the general human way of thinking. Considering only the technical aspects to answer the previously mentioned questions the following analysis steps must be carried out:

1. All of the possible classes of prime disturbance events producing significant different consequences or requiring different safety actions must be distinguishable (either by individual alarms or alarm combinations).
2. The time behaviour of the plant variables closely associated with a prime disturbance event must be determined (for all prime events).
3. The possible sensor allocations, observable plant variables must be identified.
4. By considering points of 2. and 3. an observable alarm pattern must be defined for all considered disturbance situations.

Due to the process instrumentation hardware limitations and very rapidly changing events the presented alarm pattern in a given alarm situation may be inadequate.

During the design of a new alarm system the adequacy is automatically investigated by answering to the following questions:

- can the necessary sensors be built in or not,
- have they sufficiently rapid response or not,
- will the operator presumably be capable of following the events subsequent to each other, or not (if not: only post mortem analysis can be used).

In a given alarm system the problem of adequacy may be investigated by

- experiments on the real process (within limited possibilities)
- or by simulation on an analog or digital model.

During the tests the steps listed above must be followed. In the 3. step the given sensor allocations and the given observable process variables must be regarded. It must be noted that the simulations and possible experiments can form an important part of the operator training.

4. ALARM ANALYSIS

4.1. Role of Alarms and Operators

In an advanced process analysis system using ccd's and fault trees the role of alarms can be summarized as follows:

- informing the operator that something happened (simple abnormality reporting). It may be acceptable if it relates to a functional unit or a group of equipments closely connected with each other, e.g. it indicates "PUMP FAILURE" instead of "BEARING TEMPERATURE HIGH",
- informing the operator of the temporary consequences of an event (potential consequence reporting), e.g. it indicates "PUMP OUT",
- initiating a detailed analysis procedure,
- simplifying the analysis procedure by eliminating impossible or redundant event paths,
- presenting higher level alarm patterns (alarm reduction),
- making decision automatically, e.g. shutdown of the reactor, to prevent serious consequences, such as damage to equipment, injuries to operators, etc. (temporary response),
- indicating possible future events and time horizons.

The role of the operator and advanced status of the analysis system are closely connected and complementary to each other. Namely, the more advanced analysis system we have, the less role is played by the operator and vice versa. In a computerized analysis system some aspects of the operator's role can be summarized as follows:

- during disturbed plant situation the first analysis cycle can be initiated manually be the operator or automatically when some condition is fulfilled. The further on-line cycles of the cc-analysis may either be carried out at fixed intervals cyclically, or on request by the operator, or on initiating by some conditioning events,
- for all actions, except "designed protective actions", intervention into the physical process may be taken only by the operator or under the operator's supervision. The operator can make actions considering the alarms presented directly by the plant instrumentation system and using the messages displayed by the diagnosis system,

- during the interactive analysis the operator can receive evaluation questions from the computer and by answering them he can become the main component of the interactive decision making procedure,
- it is the operator who must take into account failures
  - which the designer has not thought of,
  - which the designer could not have considered due to the hardware instrumentation difficulties,
  - where there are no ccd's available.

Specially considering the last point it can be seen that the alarm analysis system forming a part of the process disturbance diagnosis system may only be a useful tool for the operator which helps him to select the proper actions. The aim is not to replace the operator but to help him.

4.2. Steps of Analysis

The background information on plant behaviour during a disturbance situation is stored in the computer storage in the form of passive ccd's and alarm (fault) trees. The algorithms for ccd and fault tree constructions are given in (2.5). During a disturbed situation this passive model is activated by the alarms supplied by the plant information system.

Whether cause or consequence search should be executed first depends on the speed at which analysis can be carried out, compared with the plant response time. If the analysis can be made sufficiently fast, cause search should precede consequence search. In this case the different steps of the alarm analysis procedure can be summarized as follows:

1. The first alarm occurs.
2. It informs the operator on some event and requests the initiating of the first analysis cycle.
3. The cause search is initiated.

If we suppose only one possible prime failure of a critical event, then only the first alarm in a cause diagram unit must be taken into account.

Example 1. (Fig. 2):

A2, A3, A4 active alarms → probable event: E5 (only A2 must be considered).

In case of the supposition of simultaneous failures generating the same critical event (possible, but unlikely case) all prime events must be regarded. The active alarms together with the observable events in the cause tree will help to find the most likely events. This method is described in (3).

Example 2.:

A2, A3, A4 active alarms → probable event: E5, possible event: E4.

Example 3.:

A1, A4 active alarms → probable event: $(E2 \vee E3) \wedge E1$.

When a new alarm arrives the alarm sequence must be reevaluated up to date to discover if there are any new causes to be added as multiple events. To evaluate the new failure events all of the alarms present at any stage must be regarded. By keeping a pointer to the current position in a ccd, the work involved may be reduced.

Example 4.:

A2, A3, A4 active alarms → probable event: E5.
A5 new active alarm → probable events: E5, C1

4. The consequence search is initiated.

After having finished the cause search, an actual alarm pattern exists at the initial time moment of the consequence search. This alarm pattern is formed by the individual alarms received in a given time sequence. To find the possible event consequence chains the time sequential alarm pattern should be split into several corresponding alarm sets, i.e. causal alarm sets should be identified. Each causal alarm set corresponds to an event chain where the events are both time sequential and causal ones, too.

Example 5.:

Alarm sequence: A2, A3, A4, A5, A6, A10 → causal alarm sets: A4 - A5 - A10 and A4 - A6.

According to these new alarm sets, the possible event paths, the consequences, their probabilities and time horizons can be determined.

Example 6.:

Taking Example 5 → probable path: P2
possible paths: P1
impossible paths: P3, P4

When a new alarm arrives the existing causal alarm sets must be reevaluated up to date. As a result the previous alarm sets may be changed or new causal sets may by generated occasionally altering the possible event paths and their probabilities.

Example 7.:

Taking Ex. 5 and Ex. 6.

A9 new alarm → causal alarm sets: A4 - A6 - A9, A4 - A5 - A10
probable paths: P1, P2
possible paths: -
impossible paths: P3, P4

The alarms presented during a disturbed plant situation can contradict or overlap each other, therefore during the alarm pattern evaluation the consistency of alarms and the possibility of alarm reduction must be investigated. The consistency of alarms can be examined by using the logical elements of the ccd (e.g. if both branches of a decision vertex are indicated as TRUE), but to explore the cause of an existing contradiction other methods must be generally applied, for example operator interaction or creditibility evaluation. The methods of alarm reduction can be somewhat different within an interactive analysis algorithm and during a post-mortem analysis procedure. The possibility of alarm reduction within an analysis algorithm is given by the connections of the logical elements included in the different possible event paths of the ccd. During the consequence search the actual alarm pattern and the generated causal alarm sets may be pruned in the way that if an event followed by an alarm is a necessary cause to another event followed by another alarm and the latter alarm occurs, then the former alarm may be omitted. In this way a simplified alarm pattern and alarm sets being on a higher level may be formed. Finally in this alarm set an alarm may represent a critical

event or may be the last alarm of a true event path.

Example 8.:

Taking Ex. 7.

The reduced causal alarm sets: A4 - A9, A4 - A10.

The aim of post "designed protective action" diagnosis is to help the operator to understand why his plant shuts itself down. The problem of large number of alarms is not so great as when the operator has a critical safety role, but even here it is preferable to present "more important" alarm information first. There are several alarm reduction techniques which could be used, some rules can be the following ones:

- if A and B alarms (or more alarms) are always signalled together, one of them (or some of them) may be omitted, depending on which requires most direct action,
- causal alarms may be suppressed until requested by the operator, attention must be focused on critical events,
- redundant or parallel alarms may be arranged in groups and only group alarms must be signalled in the first instance.

4.3. Data Presentation

During plant disturbance situation the operator receives alarms presented by the plant instrumentation system and different pieces of information sent by the plant analysis system. The latter ones may be the following:

- messages on automatically initiated actions or on actions which must be taken by the operator,
- questions to be answered,
- dynamic intermediate report on analysis status,
- final report on results of the analysis.

To present a dynamic status report the simplified ccd seems to be useful because it is closely adapted to the operator's mode of thinking. It must be a matter of further investigation how other methods could be used, e.g. block diagram method adapted for data presentation. In a simplified ccd only the relevant causes, events, consequences, and alarms should be

displayed. The irrelevant parts of the diagram, e.g. non-actual prime causes, impossible branches, intermediate events with less importance may be omitted.

One possible method using colour CRT's for ccd-display is described in (4). The dynamic ccd is displayed in a four colour alphanumeric form. Taking into account a white/black CRT, a simpler method is illustrated in Fig. 3 and 4. The considered full-scale hypothetical cause-consequence diagram is shown in Fig. 2. If e.g. we suppose an A2-A3-A4-A5-A10 sequential alarm pattern, the ccd can be pruned to one shown in Fig. 3. The continuous line indicates the PROBABLE event path, the dashed line indicates the POSSIBLE path, the impossible paths and irrelevant logical connections, alarms are omitted. When a new alarm arrives or conditions are triggered the figure must be changed, e.g. if C4 condition is triggered into PROBABLE and C5 is FALSE, then P1 path is indicated PROBABLE by the A9 alarm and the ccd must be changed shown in Fig. 4. It must be noted that these figures could further be simplified shown in Fig. 5. The probabilities and time horizons could also be displayed.

A final report can be presented automatically (at the end of the analysis) or on request by the operator (detailed information is needed). After having finished the disturbance analysis procedure, first of all a summary report must be presented containing:

- the prime cause(-s)
- the critical event
- true/possible consequences with their probabilities and time horizons
- the actions to be taken by the operator to prevent further serious troubles, e.g. damage, injury.

The form of the summary display can be simplified cause-consequence diagram (see Fig. 5) or a data list. On request the whole ccd having been investigated should be presented. To gain more further information the final sequential and causal alarm sets, detailed plant drawings in hierarchical fashion, all messages, questions-answers, automatical-manual actions may be displayed. For documentation this should be produced in the hard copy form, also.

CONCLUDING REMARKS

This paper summarizes some major questions of alarm analysis system design. During application of the principles described here several difficulties should be overcome, such as development of fast real-time analysing programs and proper man-machine communication system. As a first step cause-consequence analysis algorithms and programs specially intended for alarm analysis purposes have been developed and described in (5). Presently the main efforts are made for getting sufficient experience with these programs on complex systems. One of the plants in which the programs are planned to be used for alarm analysis is the Paks Atomic Power Station in Hungary.

ACKNOWLEDGEMENT

The author is highly indebted to J.R. Taylor for numerous inspiring and stimulating discussions on the subject.

REFERENCES

(1) - D.S. Nielsen:
Use of Cause-Consequence Charts in Practical Systems Analysis. Risø-M-1743, 1974.

(2) - J.R. Taylor:
Sequential Effects in Failure Mode Analysis. Risö-M-1740, 1974.

(3) - G. Dahll:
Methods to Use Observables in the Finding of Prime Causes to an Alarm Situation. Halden PC-Note 1489, 1974.

(4) - G. Dahll, R. Grumbach, et. al.:
On-Line Analysis of Abnormal Plant Situations, Paper to be Presented at the Enlarged Halden Programme Group Meeting, Sandersstölen, Norway, 1976.

(5) - E. Holló, J.R. Taylor:
Algoritms and programs for consequence diagram and fault tree construction. Risø-M-1907.

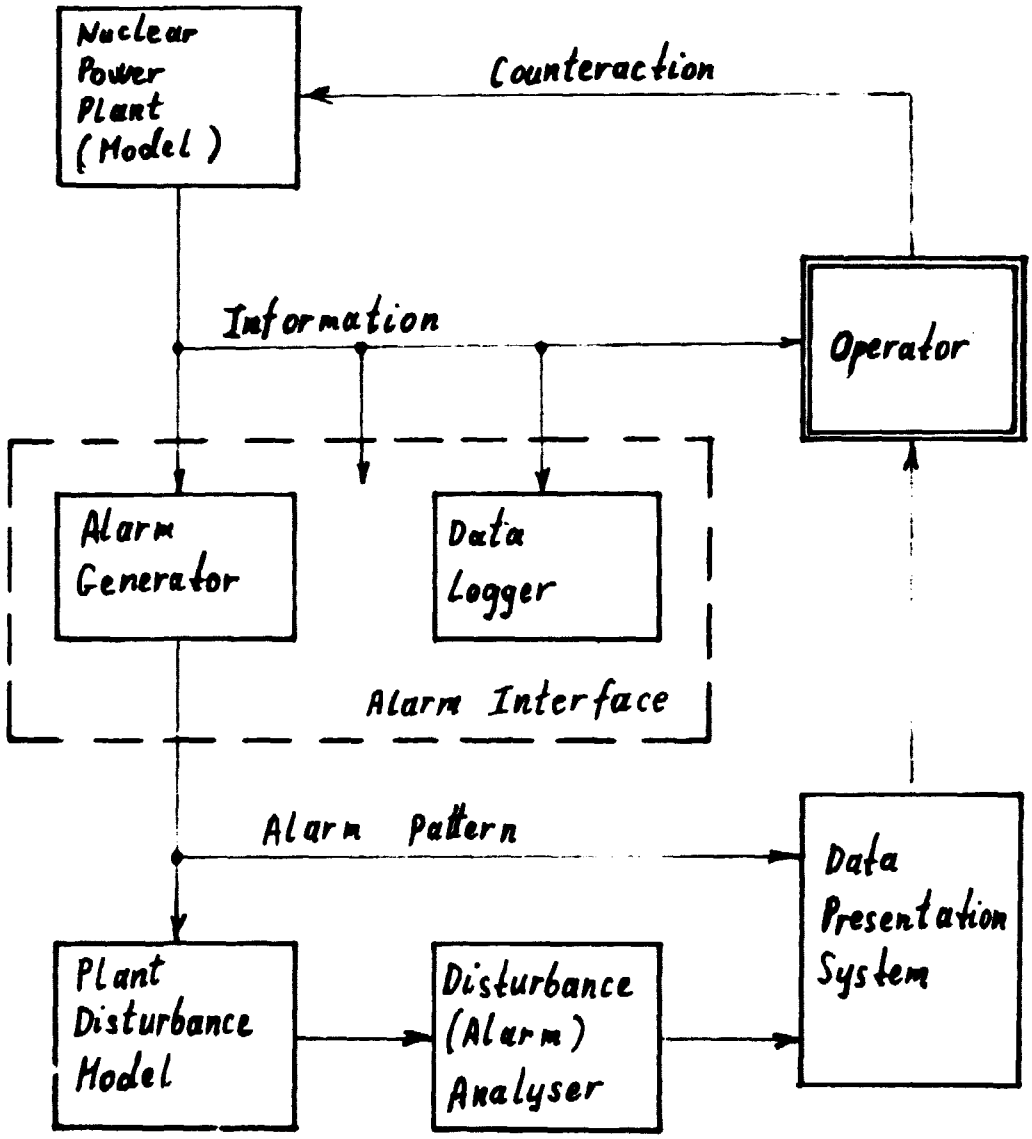

Fig. 1. Block-scheme of the disturbance (alarm) analysis procedure.

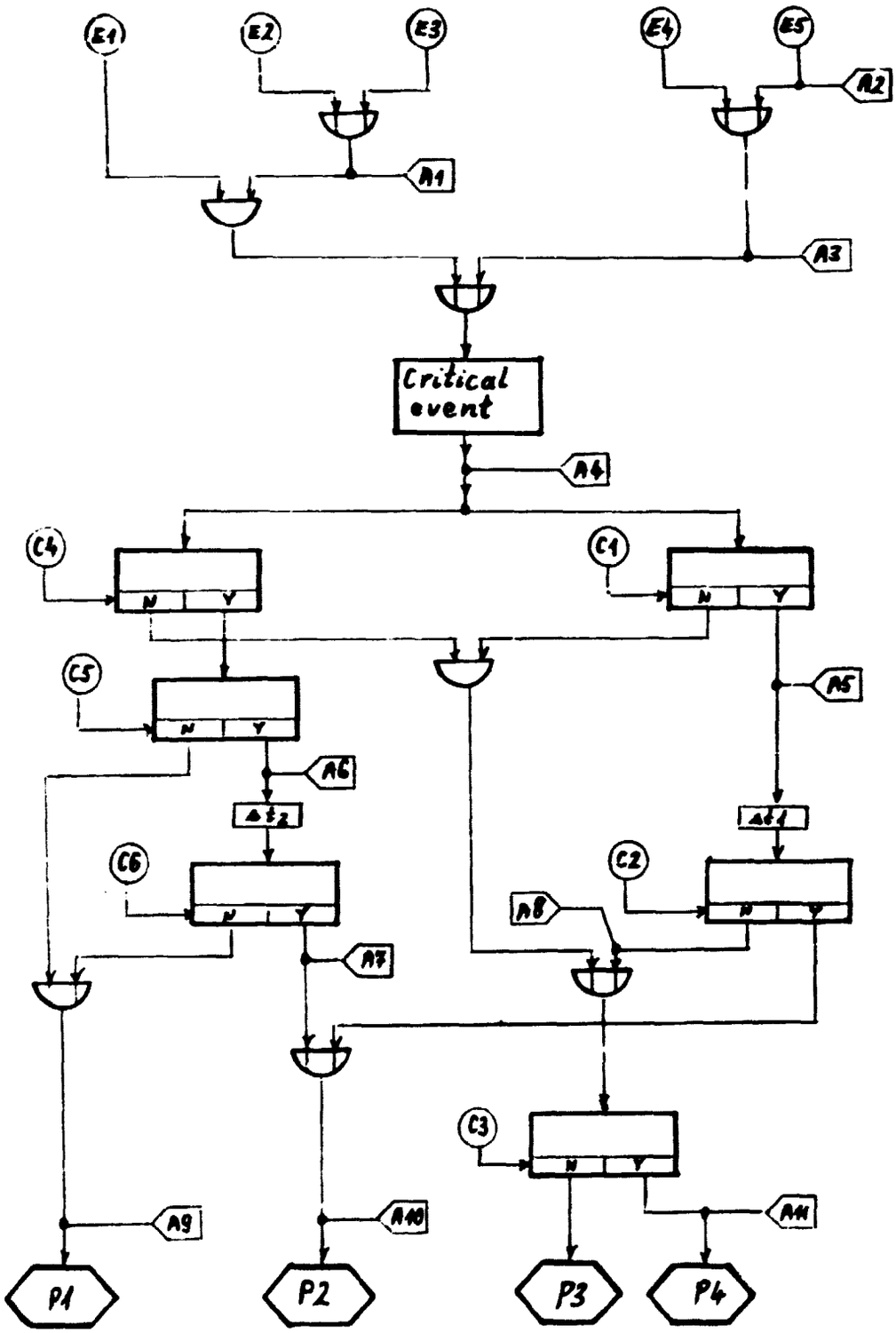

Fig. 2. Hypothetical cause-consequence diagram for a disturbance situation.

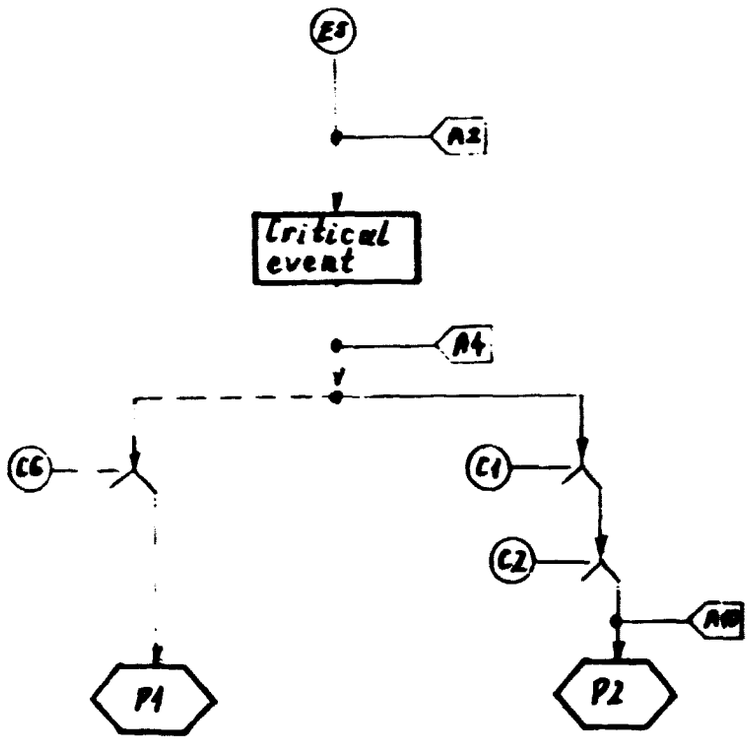

Fig. 3. Simplified ccd presentation with probable/possible event paths.

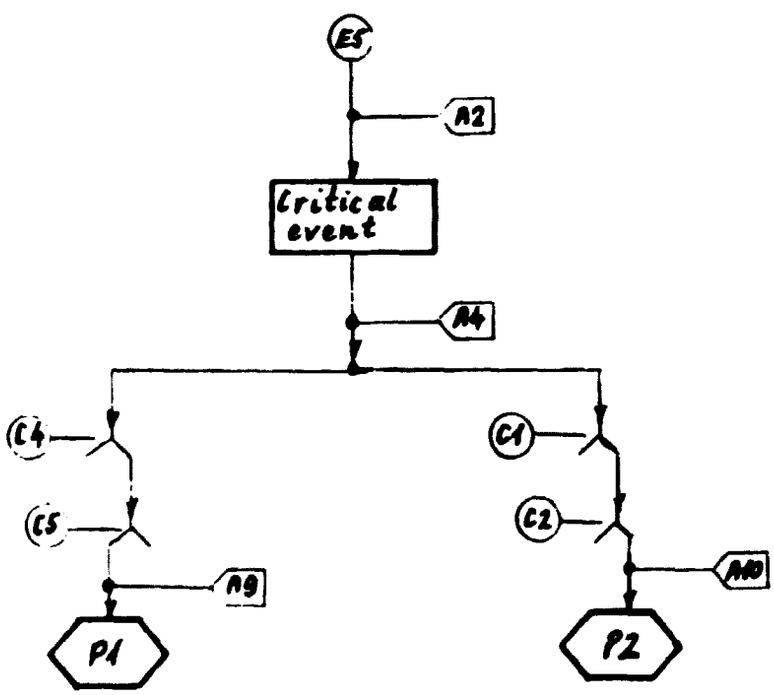

Fig. 4. Simplified ccd presentation with probable event paths.

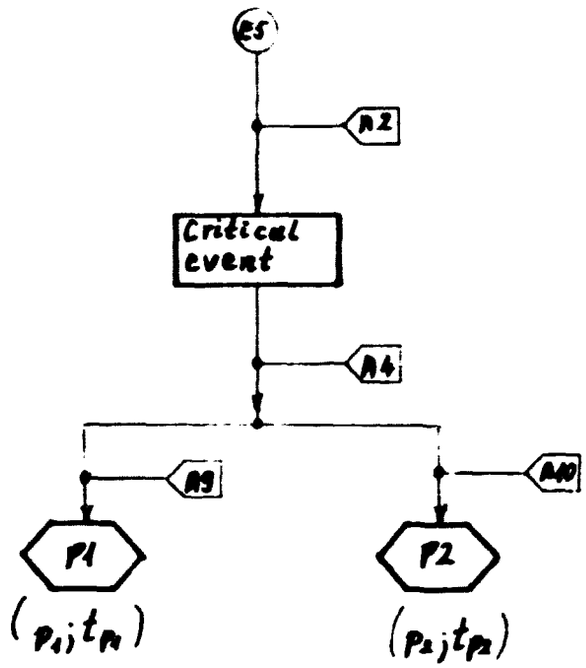

Fig. 5. Final ccd presentation.