Automatic fault tree construction with RIKKE - a compendium of examples. Volume 1. Basic models

Taylor, J.R.

Publication date:
1981

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

RISØ-M-2311

AUTOMATIC FAULT TREE CONSTRUCTION WITH RIKKE - A COMPENDIUM OF EXAMPLES, VOLUME I BASIC MODELS

J.R. Taylor

Abstract. Examples of automatically constructed fault trees are given. In this first volume, simple component configurations which illustrate individual component model types are treated.

INIS descriptors. CONTROL EQUIPMENT; ELECTRICAL EQUIPMENT; FAULT TREE ANALYSIS; INDUSTRIAL PLANTS; POWER PLANTS; RISK ANALYSIS.

UDC 614.8 : 658.58

September 1981
Risø National Laboratory, DK-4000 Roskilde, Denmark

ISBN 87-550-0794-5
ISSN 0418-6435

Risø repro 1981

CONTENTS

I' 'RODUCTION

The examples given here are intended to illustrate the principles of fault tree construction using the RIKKE failure analysis system, and the FTLIB library of component failure models. The theory underlying the fault tree construction is given in "An algorithm for fault tree construction", J.R. Taylor, IEEE Trans. Reliability 1981, and in "Automatic fault tree and cause consequence diagram construction", J.R. Taylor and J.V. Olsen, 1978. Further examples of fault tree and consequence diagrams will follow in later compendia.

The FTLIB library contains models of the common process plant and electrical components. It allows the causes of small and large process variable disturbances to be investigated. Small disturbances are defined as those which can be corrected by a control loop. Large disturbances can be corrected by shutting off or opening up various flows.

In this volume, basic component configurations are investigated which illustrate the form of coding of models, and serve to document the basic models

- resistive load
- pipe
- shut off valve
- regulator valve
- tank
- tee junctions

Generally, other models can be created from these basic models via a simple editing process, based on analogy for example between hydraulic and electric flow equations. As another example, a heat exchanger can be regarded as two pipes, with a heat exchange between them.

In later volumes, more complex component arrangements are investigated.

Model Coding Principles

The list of variable values actually included are as follows

large disturbance	HI
small disturbance	DISTHI
small disturbance	DISTLO
large disturbance	LO
absolute level	ZERO/NO
relative level	NEG.
absolute level	ON
absolute level	OFF

Disturbance values are relative to normal values. These value level codes are combined with prefixes and suffixes, in order to allow correct matching of variable values in tracing event chains. For example LOSUPP is the code for "low supply pressure".

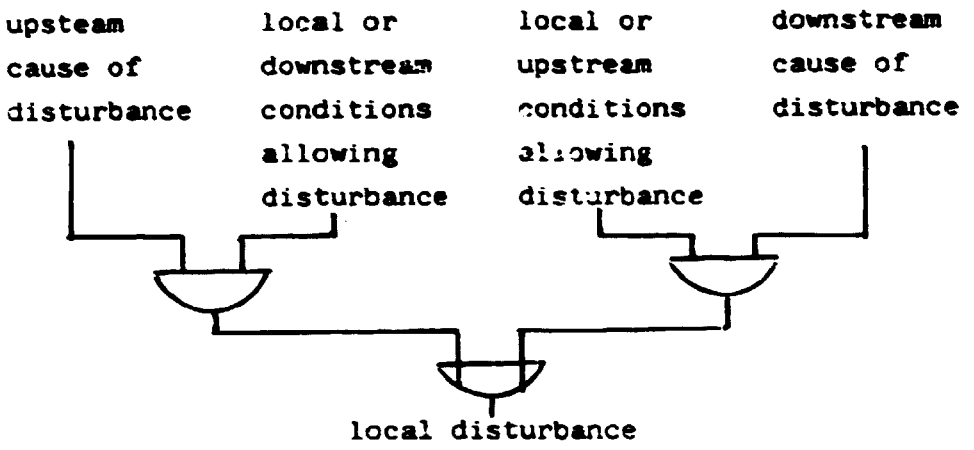
Additional zero values ATM (atmospheric), BLOCKED (shut against flow) and NOP (no pressure) are provided in order to be able to evaluate zero pressure and zero flow. Roughly, ATM means no pressure and no resistance to flow. BLOCKED means zero flow and infinite resistance to flow. NOP means no pressure supply is present.

The principle underlying the construction of the FTLIB models are as follows.

1) Disturbances are traced along flow paths in a component network.

2) Transfer functions for components, which map input disturbances to output disturbances are obtained by inspection of component physical equations of mass and energy balance, using the cause and effect graphs described in the references.

3) Given a TOP event, the search used in building up the fault tree has the following pattern.



4) The general pattern for flow and pressure disturbance is that some failure event affects pressure. The pressure disturbance is traced, and its effect on flow is derived locally within each component. Exceptions to this rule are disturbances arising from positive displacement pumps, and valve closure.

5) It is not generally possible to determine the effect of a pressure disturbance without determining the resistance pattern it meets. A fall in pump speed may cause a fall in pressure if the pump is feeding a long pipe, or a fall in flow if the pump is feeding a tank directly. For this reason, changes in pressure or flow are not traced in building up the fault trees, but rather potential causes of changes in pressure or flow. For example LOSUPP means a low supply pressure, which is a potential cause of low pressure or low flow. HIBACKP means high back pressure, which is a potential cause of high pressure or low flow. The effect of the causes is determined locally within a component, e.g. (OUT→HIBACKP) + (IN IS RESistive) =>(IN→HIP).

6) The transfer function of a TEE junction presents difficulties. The effect of a high supply pressure on the output will

depend on whether the output is resistive, and whether the second input flow is resistive. If the output is resistive, there will be no disturbance at the output unless the second input is resistive. In order to treat both the local and distant effects of wye junctions, disturbances are coded with the suffix -R if they can cause a disturbance in a resistive load, and a suffix -C if they can cause a disturbance in a capacitative load.

7) Generally the component models have been minimised so that major branching in the resulting fault trees is found only at the TOP event and at TEE junctions.

   This is done by making the transformations

   A → X, B → X ⇒ AB → X

   i.e. two causes of a disturbance are coded as a complex event.

   A + B → X, A + C → X ⇒ B + C → Y , A + Y → X

   i.e. cause A, under conditions B and C, is investigated once, in combination with the complex condition B + C, rather than being investigated twice.

8) For control components, disturbances only pass if there is no control action, for example

   (IN → DISTHISUPP) + (POS ISNT COMPLO) ⇒ (OUT → DISTHISUPP)

   Compensating actions are coded with the prefix COMP- for proportional control actions and DELTA- for derivative (fast) control actions.

9) In order to avoid tracing causes of disturbances through a control system, and finding that a low disturbance is caused by a high disturbance, etc., which can rapidly lead to combinatorial explosion, high and low control signals have the prefix CONT- or FAIL-, depending on whether the values

are caused by control actions or failures. Sensor components have the events IN - HI-INPUT and IN - LO-INPUT, to remind the user that the fault tree has been curtailed. In most cases the user will wish to delete these events.

Examples

The following comments are intended to highlight particular features of the examples, and should be read in parallel with examination of the examples.

1) The system shown on page one is a collection of small component arrangements, intended to demonstrate the principles of model construction. It includes a supply (SUP) of fluid, a sink (DRAIN) for fluid, NOZZLE which is a standard resistive flow load, an on off VALVE, a non-resistive PIPE, and a regulating valve REGVLV.

2) The first fault tree is for high pressure (HIP) at the output of the NOZZLE, N3. The obvious sources og high pressure are the supply (HISUPP) and the drain (HIBACKP). Note that high supply pressure gives high pressure only if the output from N3 meets a resistive load (IS R). The nozzles have an additional failure mode FAILNOR which indicates that they become none resistive.

   The top event is given as IOUT - HIP. IOUT is an internal variable, corresponding to the external variable OUT. If event chains are to be searched in two directions then the top event in a fault tree should always represent a change in an internal variable when using RIKKE.

3) The same fault tree as 2), after cutting (pruning), with mode 223, which removes almost all unnecessary parts of a fault tree. Intermediate events, and the "normal state" N4: NS BECOMES R have disappeared.

4) A fault tree similar to 2, but for low pressure. The FAILNOR failure modes are now found on the downstream side of the top event.

5) A fault tree similar to 2, but on the input side of the nozzle N3.

6) As 5, but cut with option 223, removing all superfluous event types.

7) If the TOP event is HIP at the output of N4, the fault tree is similar to that of 2). But HIP is dependent on blockage in drain D5.

8) High flow is also a possible top event, and in this case, is not dependent on the load being resistive.

9) The top event is no pressure, NOP at the input of nozzle N3.

10) The full fault tree for no pressure, NOP, at the output of nozzle N3. The first major branch of the tree, N3: IIN BECOMES X involves an intermediate event intended to gather together NOSUPP and BLOCKED. Blockage and lock of supply are the causes of NOP here, and note that they are conditional on there being no back pressure. Generally drain DS would open to atmosphere, so that D5:WS ATM would be true, and the second branch of the first AND gate would disappear.

    The remaining branches of the tree investigate the possibilities for the system to become open to the atmosphere.

11) After cutting example 11, there still remain many gates in the NOP fault tree. Generally, the causes of NO pressure involve quite complex logical dependencies.

12) The conditions for NOFLO are, in the first branch of this fault tree example similar to the conditions for NOP in

example 10. But in the remaining branches, BLOCKED is a cause of NOFLO, whereas in 10), BURST is a cause of NOP.

13) The examples now take in the on-off valve V8. Note that we get low pressure downstream of V8 only if the valve remains open. If we close the valve the result is generally zero pressure (NOP), unless there is some downstream source of pressure (SUP). Broken lines indicate an event without potential cause.

14) High pressure at the output of on-off valve V8. Note the dependency on SUP again. On editing, the NOSUPPR branch of the tree will disappear, because there is no potential cause of N9: OUT BECOMES SUP.

15) The causes of NOP, no pressure, at the output of shut off valve V8.

16) Causes of NOFLO in V8.

17) Causes of high pressure, HIP, at the outlet of control valve RV13. Note that if the position of the valve becomes failhi, high output pressure will result. But there is no potential cause of failhi in the model. (Broken lines around this event). This event is naturally included in the model for a valve actuator.

Note also that a condition for high pressure in the first branch of the fault tree is that the valve is open, andremains open. This condition provides a link to a potential control circuit input, although the control components are not included in the model.

18) Low pressure at the valve outlet.

19) Disturbed low pressure, DISTLO at the outlet of the regulating valve. Such slightly low disturbances can be compensated by adjusting the valve position to COMPHI (compensating high). Because there is no control circuit, this possibility is shown with broken line.

20) As for 19, but with DISTHIP.

21) The no pressure case.

22) The no flow case for the regulating valve.

23) High pressure in the pipe.

24) Zero pressure in the pipe.

25) High flow in the pipe.

26) No flow in the pipe.

27) A new model is introduced, for the two types of tee junctions, mix and divide.

28) High pressure at the mixer. Here the importance of the resistive condition R can be seen. All branches of the mixer junction must be resistive, if high pressure is to result from disturbances.

29) No pressure at the mixer junction (after cutting, mode 223).

30) No pressure at the divider junction.

31) A simple flow loop model is introduced with a transmitter and a pneumatic regulator.

32) This example shows the result of investigating a disturbance in the control loop. Loop failure modes are recorded. The fault tree has been cut, mode 223.

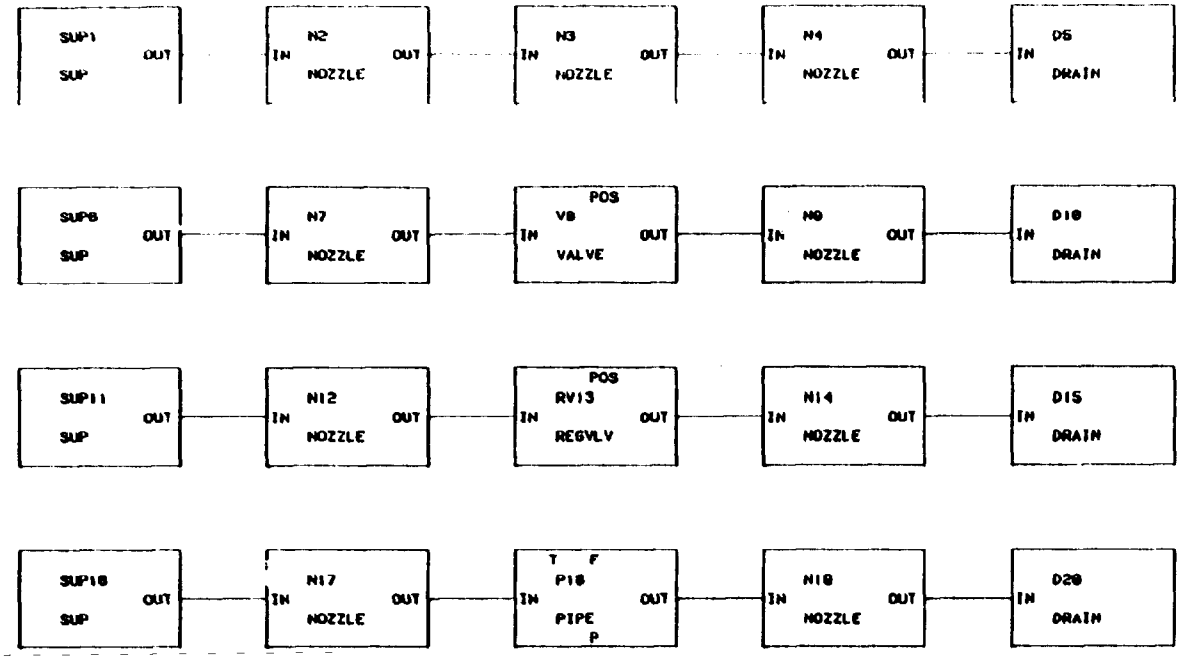
33) As for 32, except that the disturbance is investigated further downstream. The fault tree has been cut with mode 207, so intermediate events are shown.

34) Pressure disturbances at the outflow of the control loop. The control loop has no effect on these, since it is designed to regulate flow.

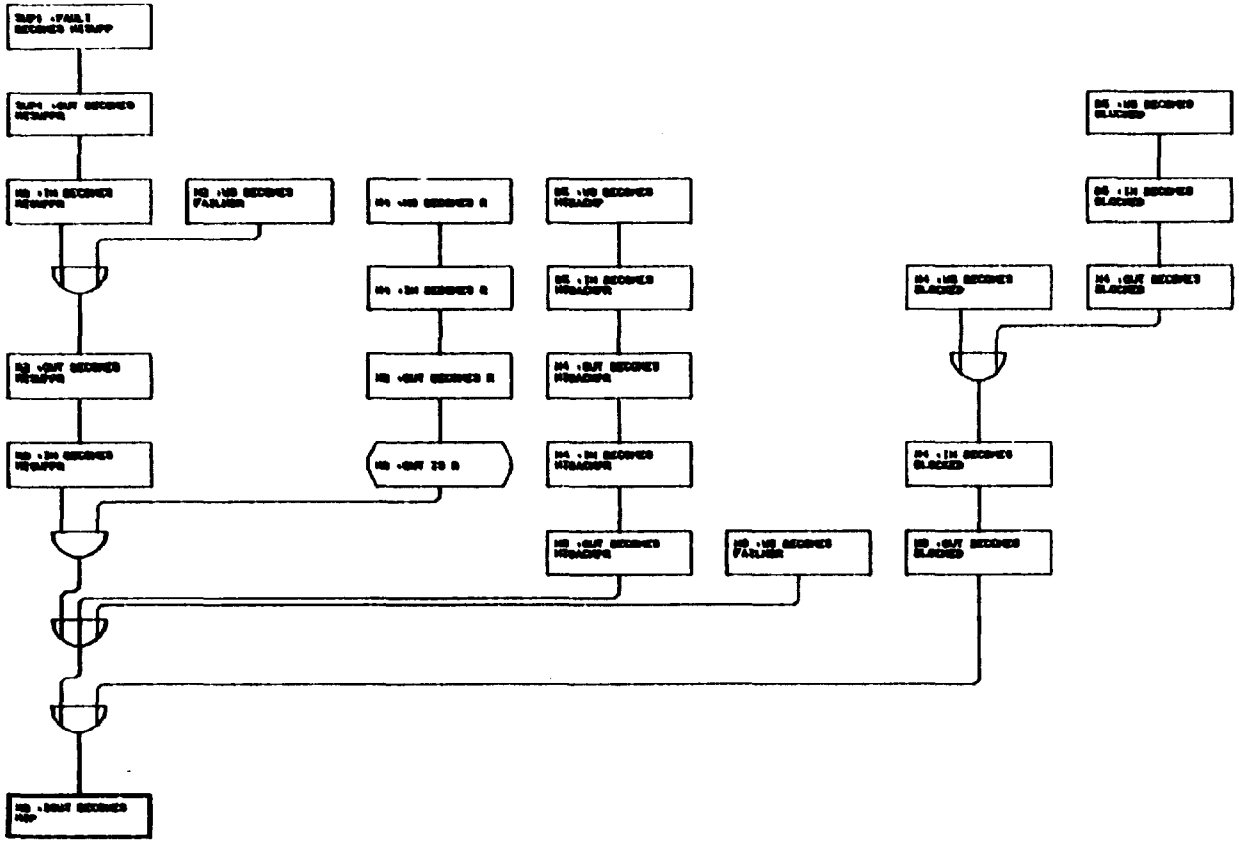
35) A new model is introduced, for tank level control. The input here is graphic, using the DRAFT command rather than the DIAGRAM command in RIKKE.

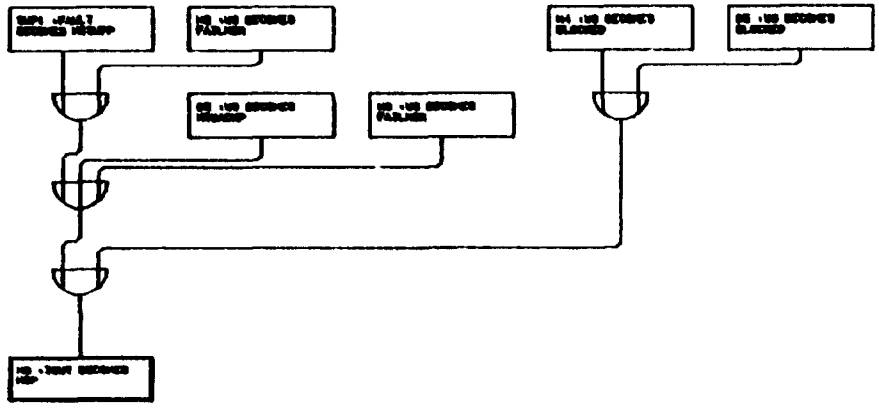
36) Tank level control failure.

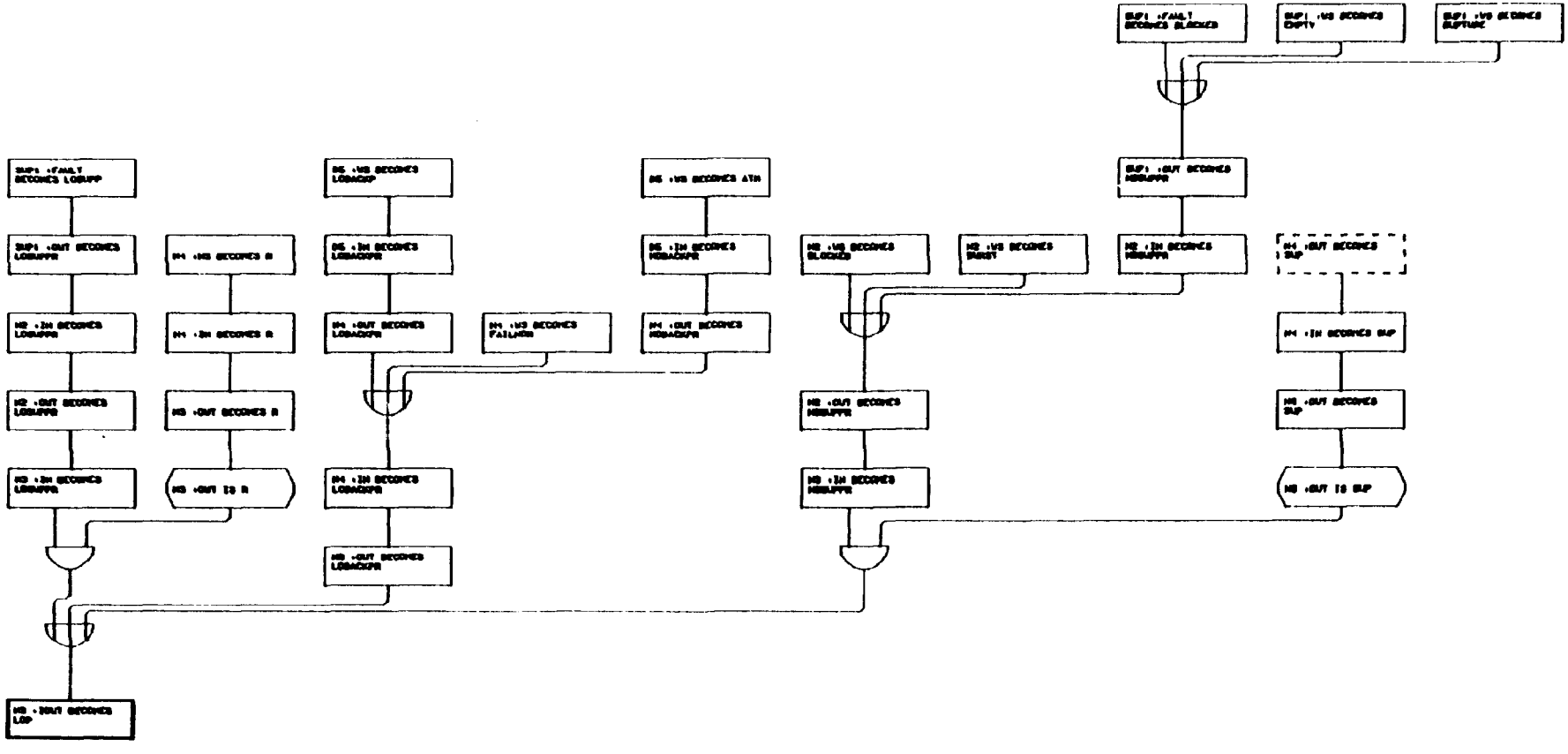
TEST 1 OF FTLIB MODELS

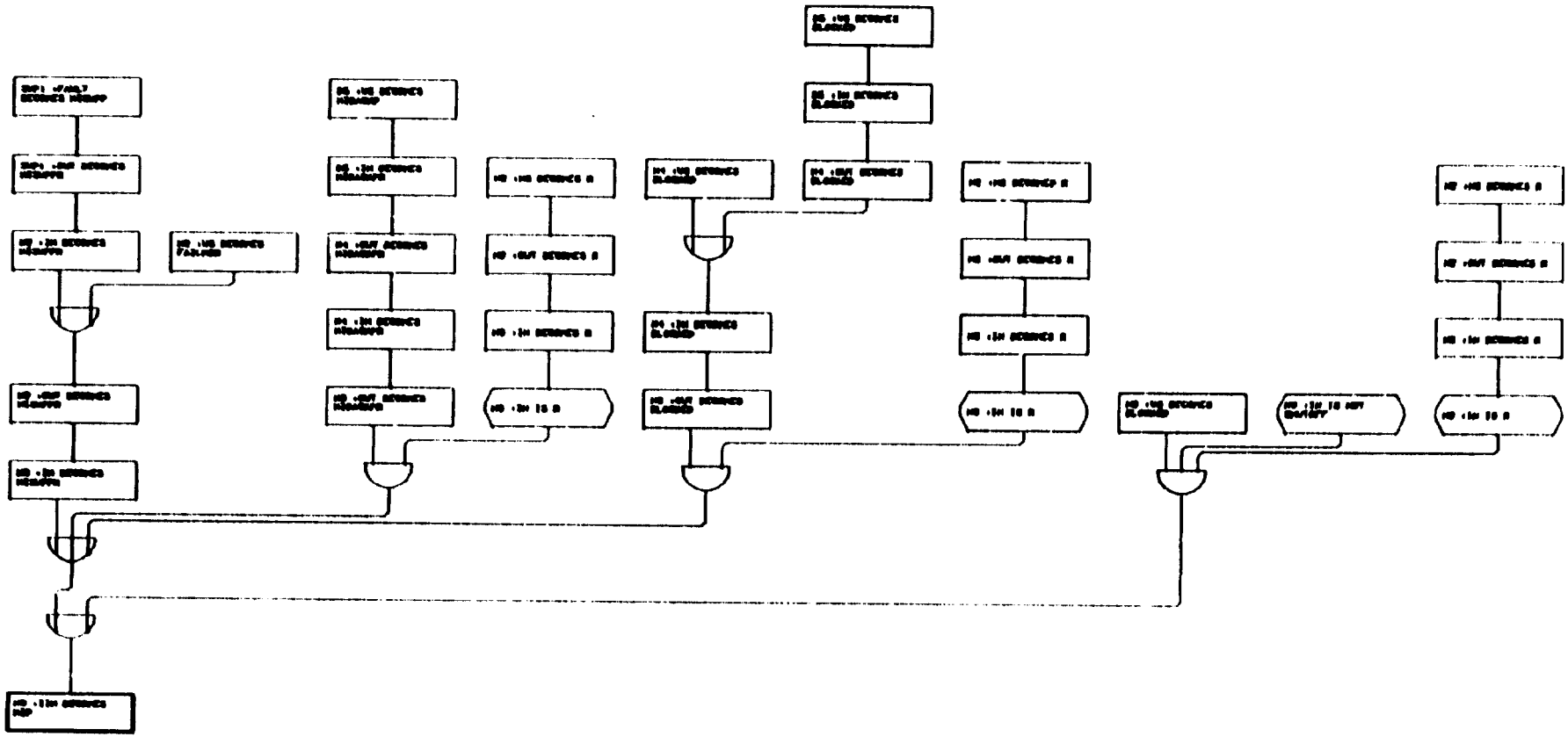


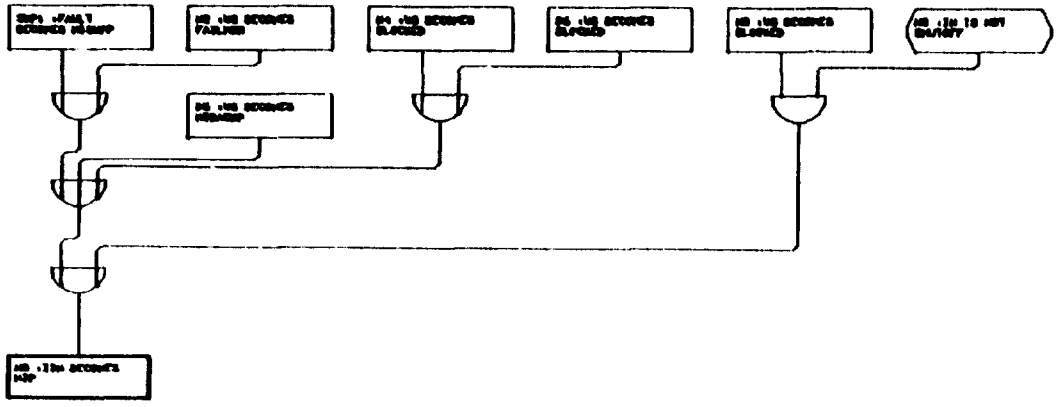
(1)

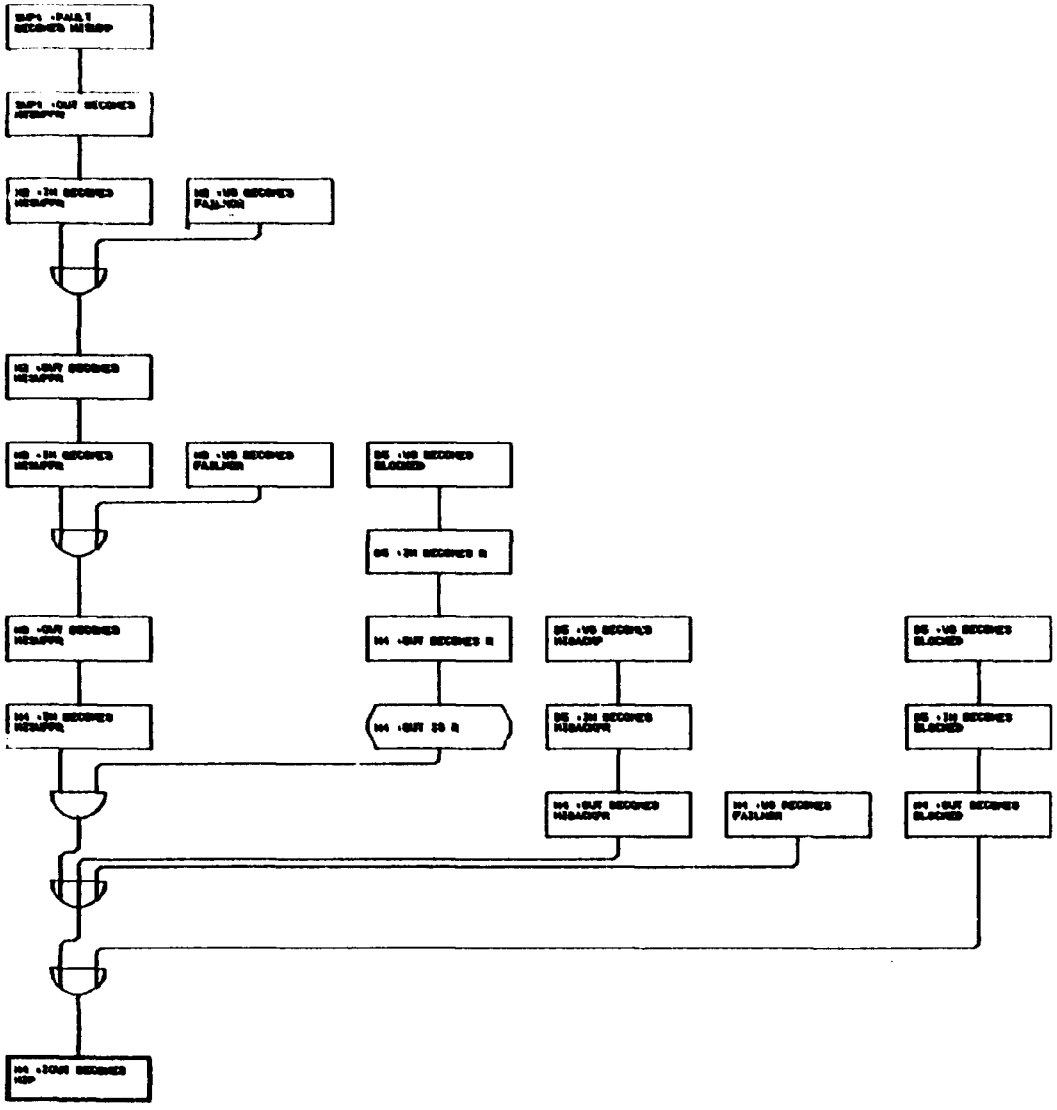


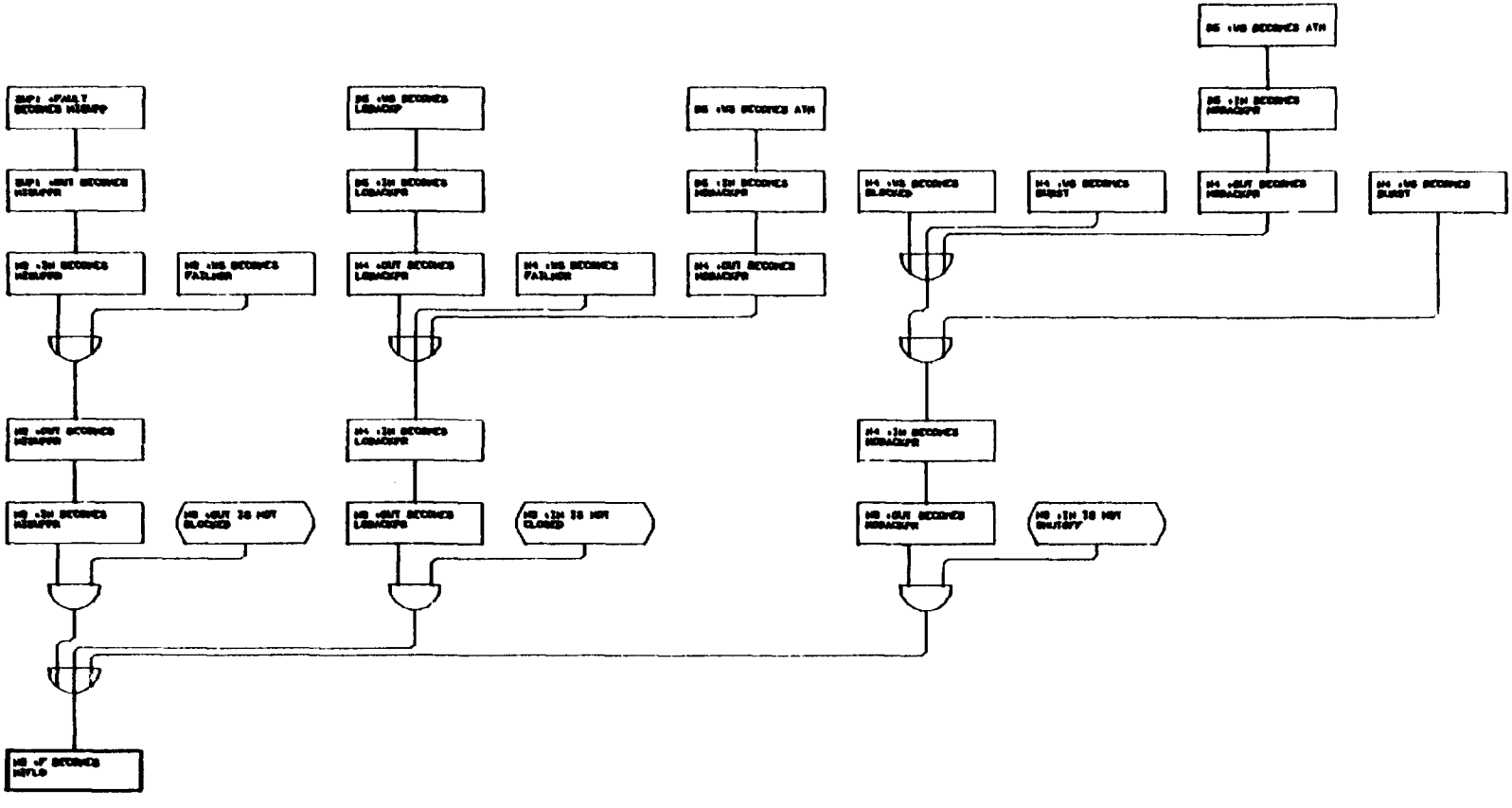


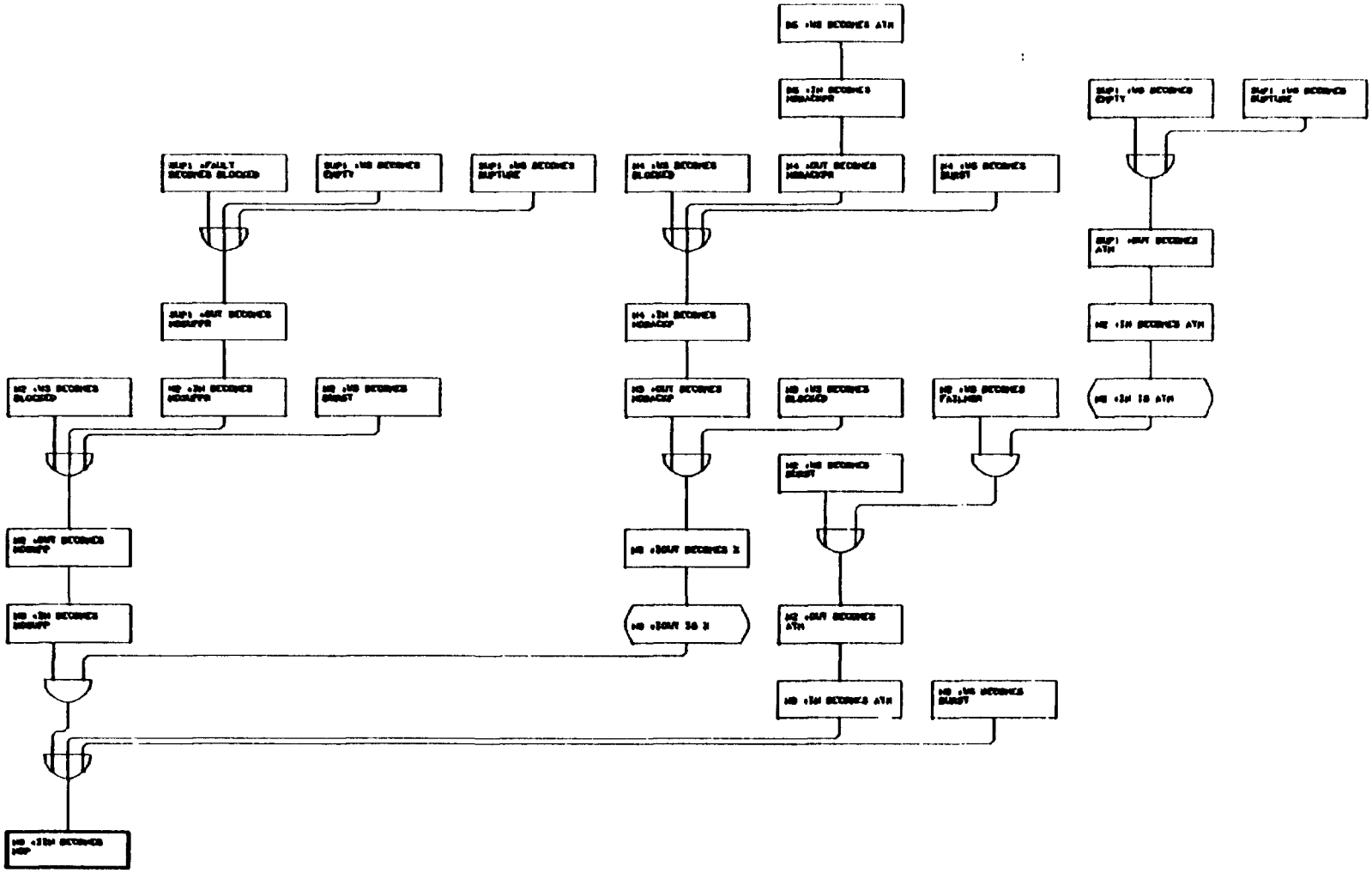


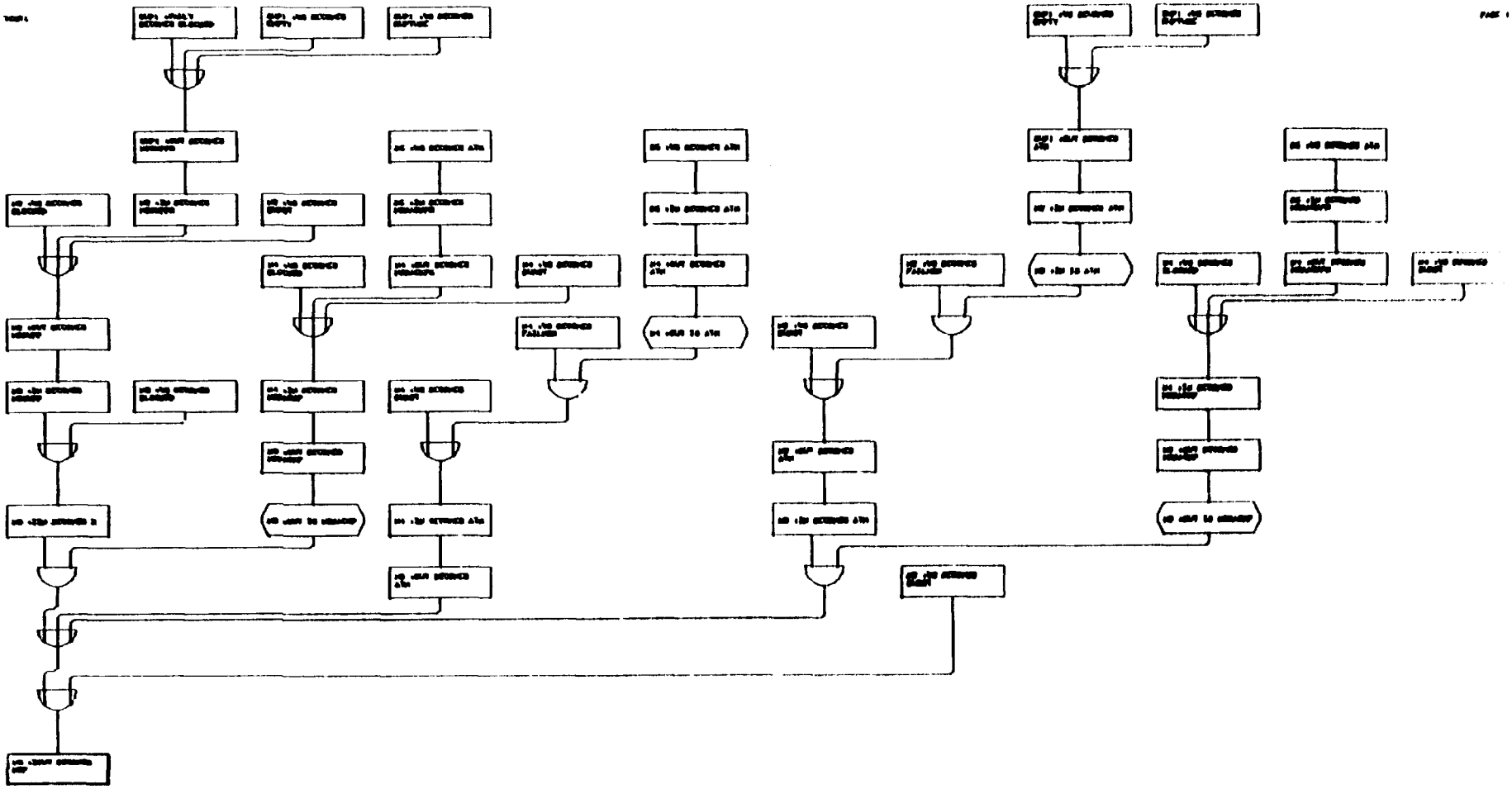


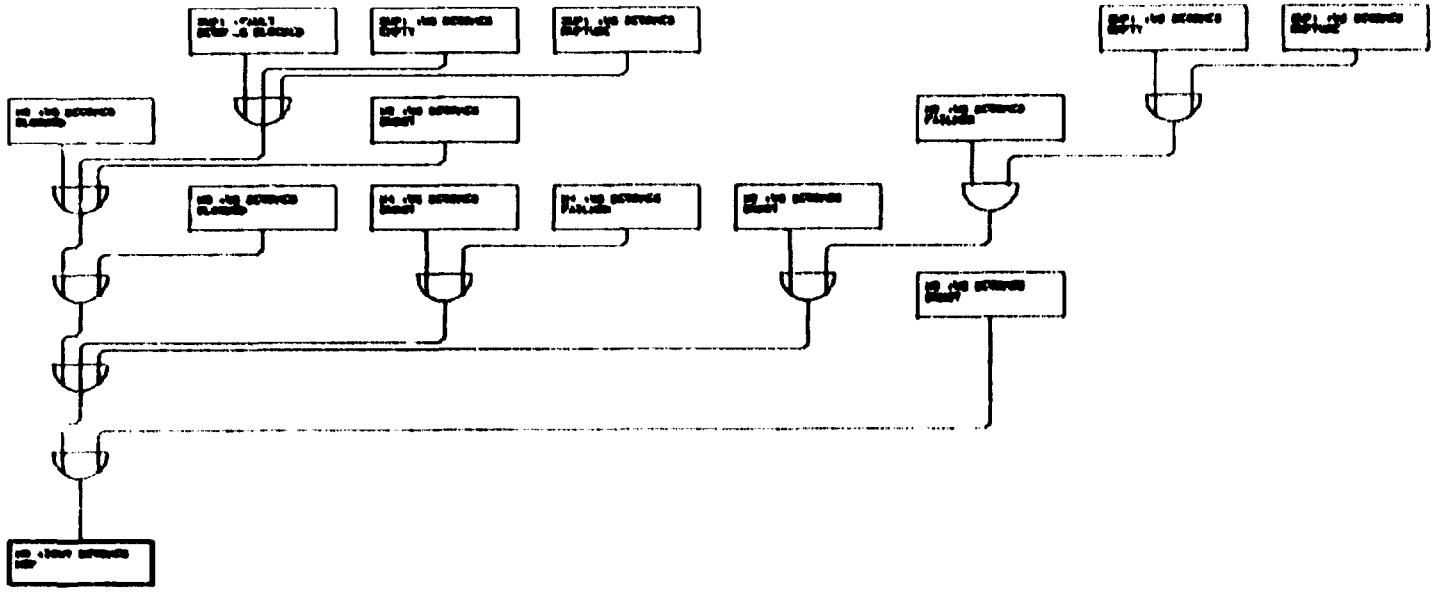


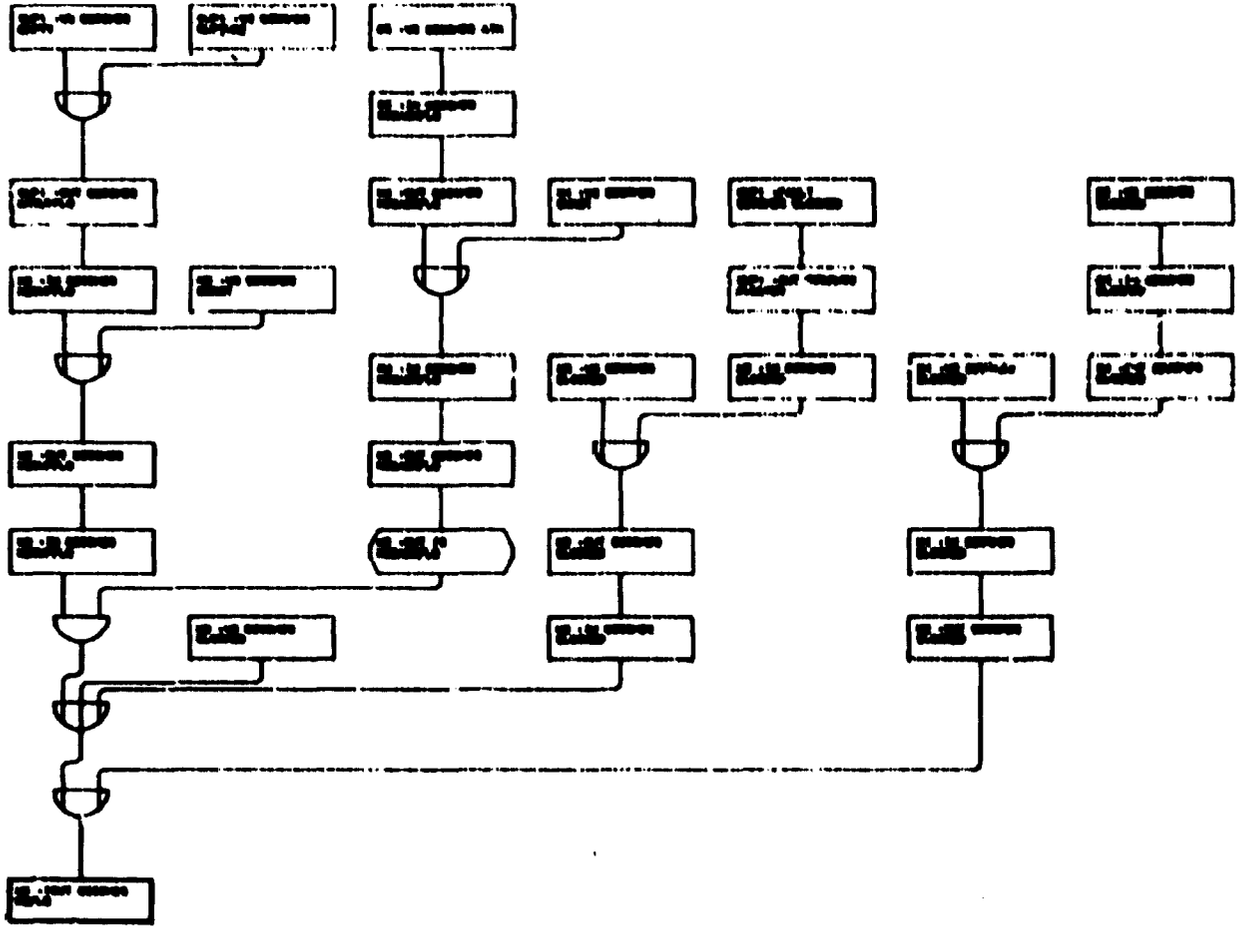


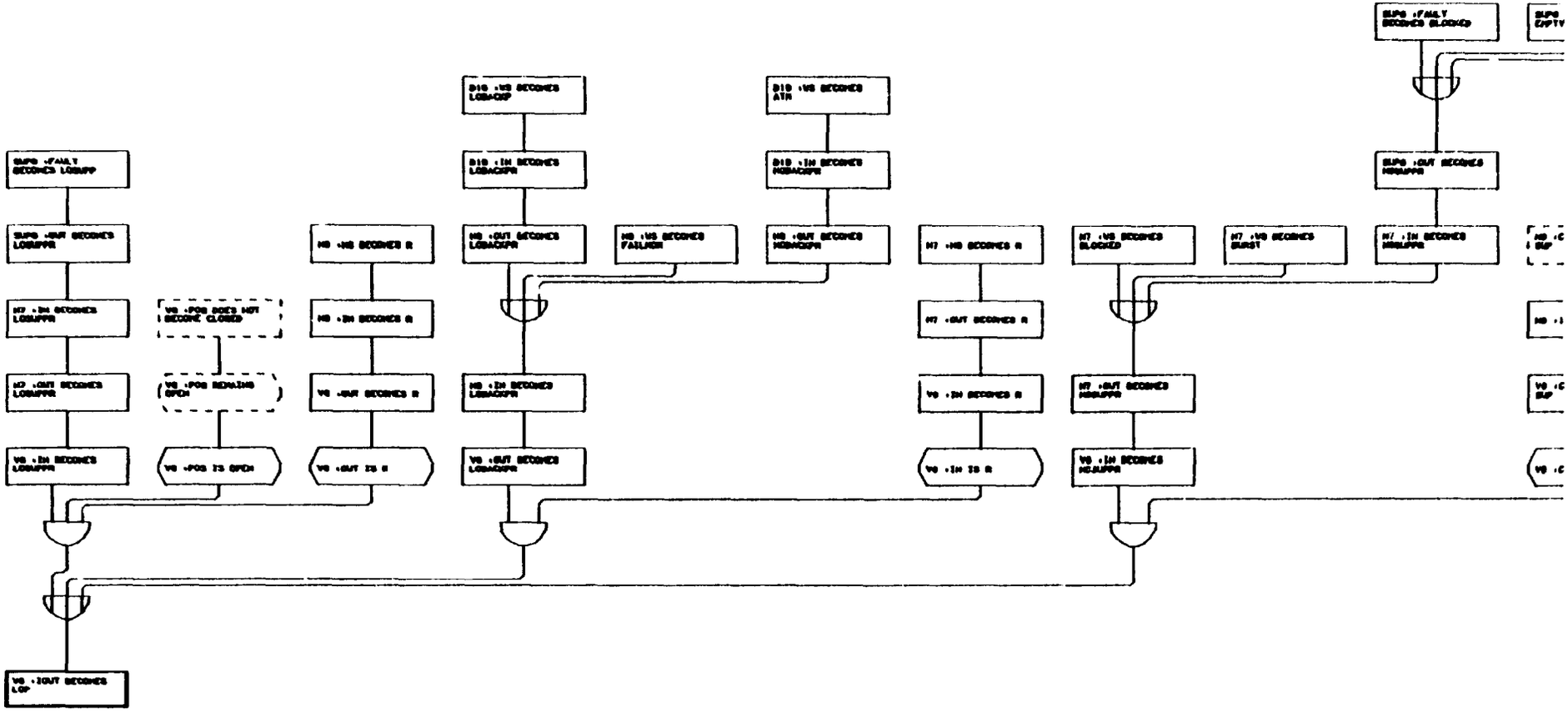


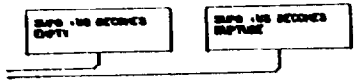


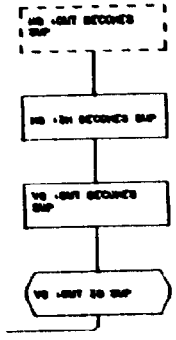


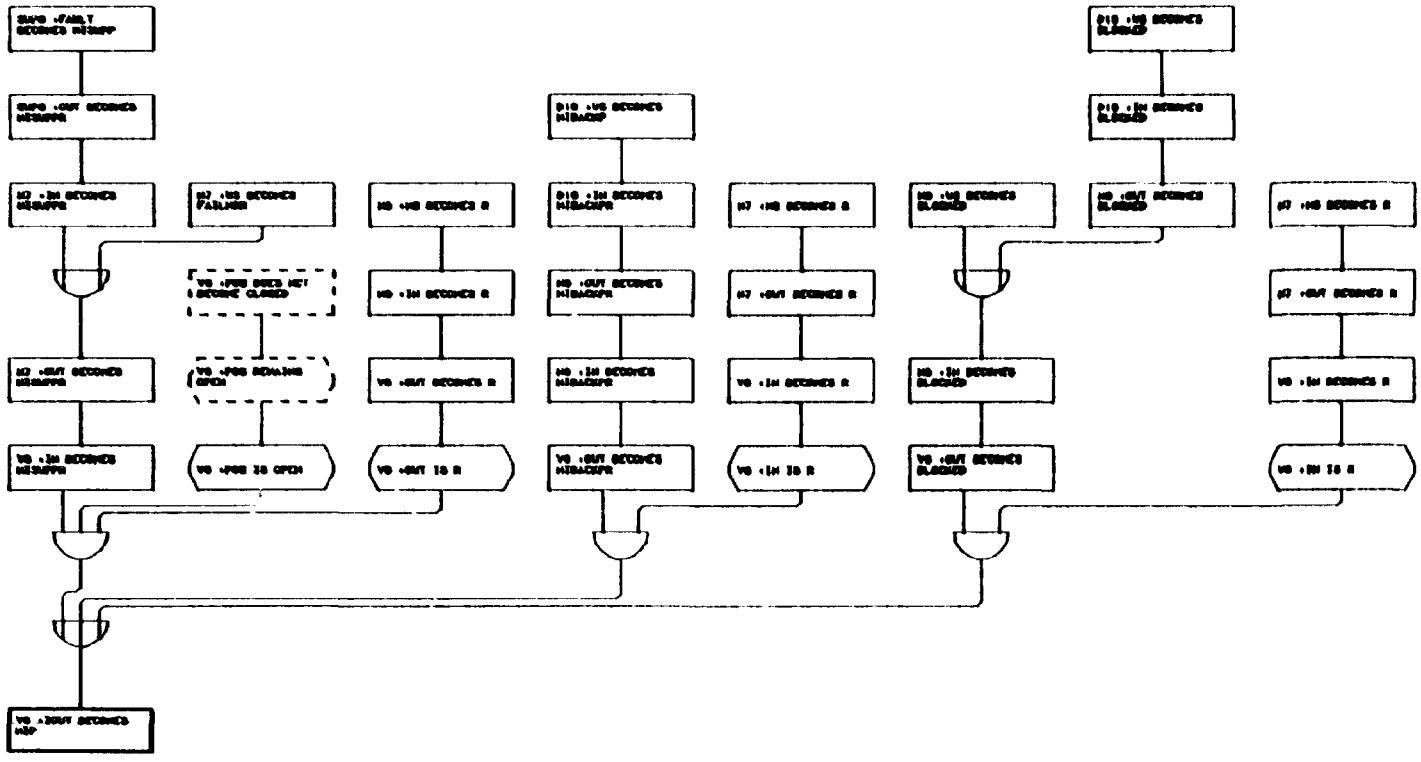


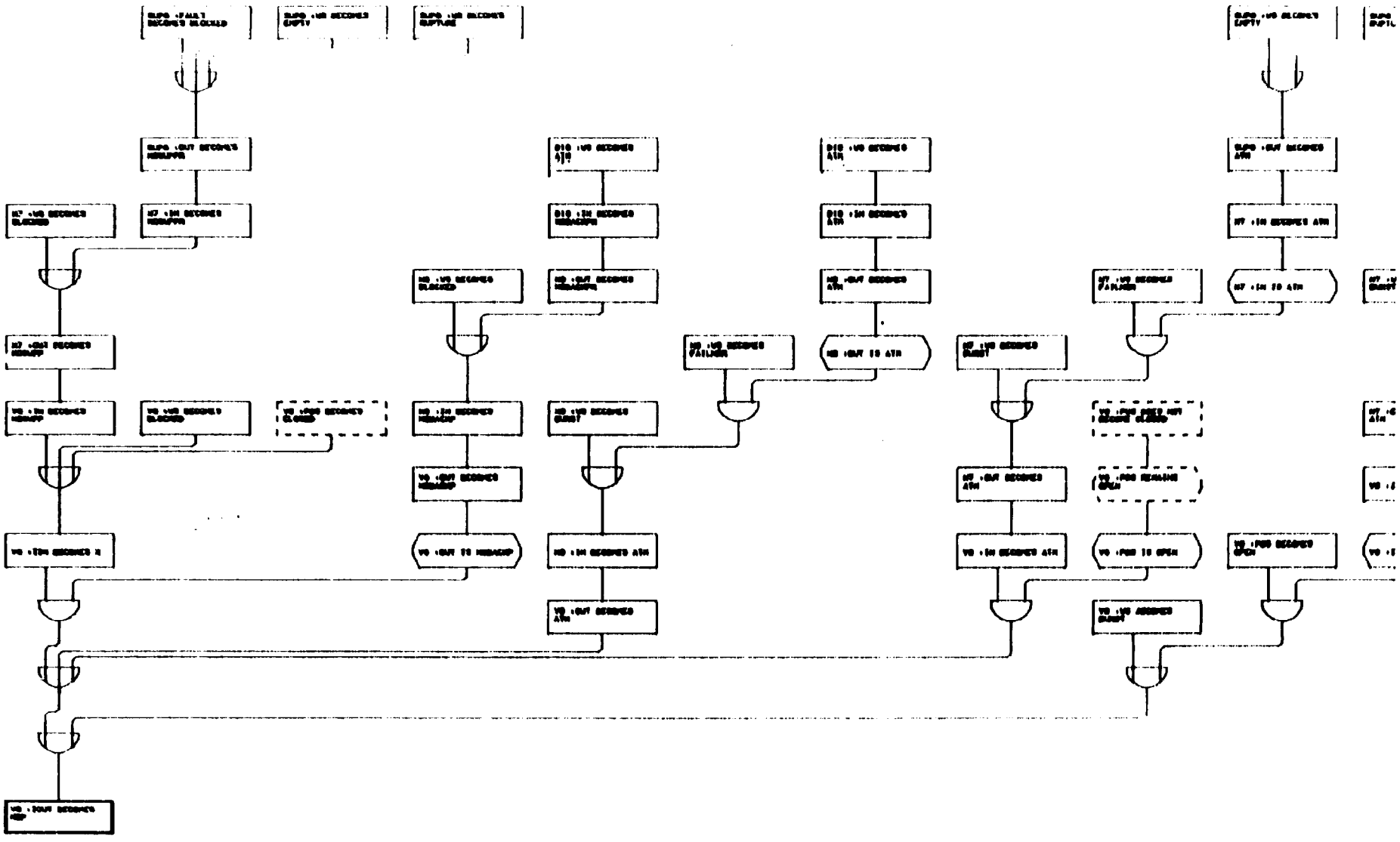


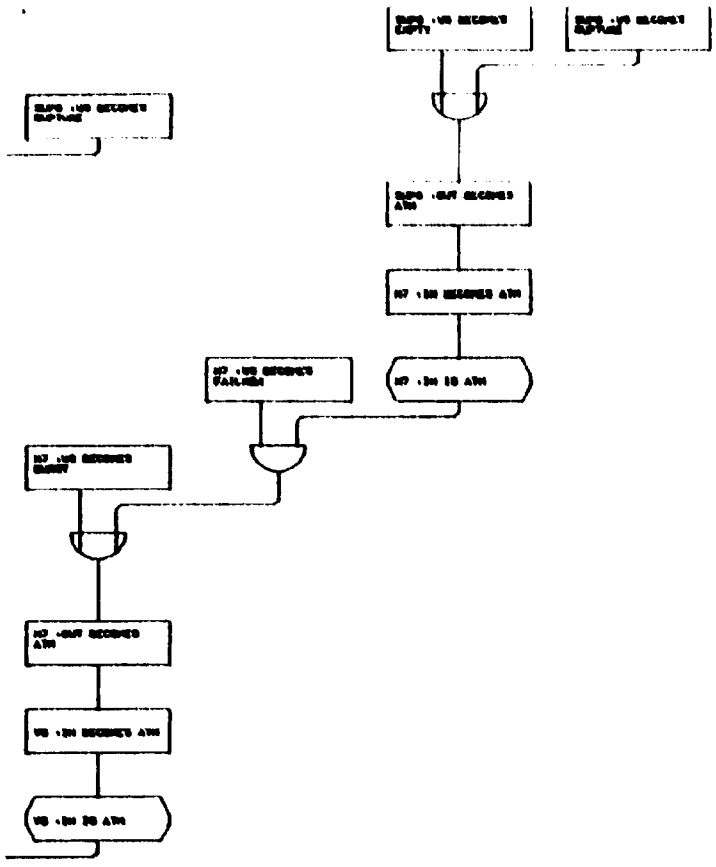


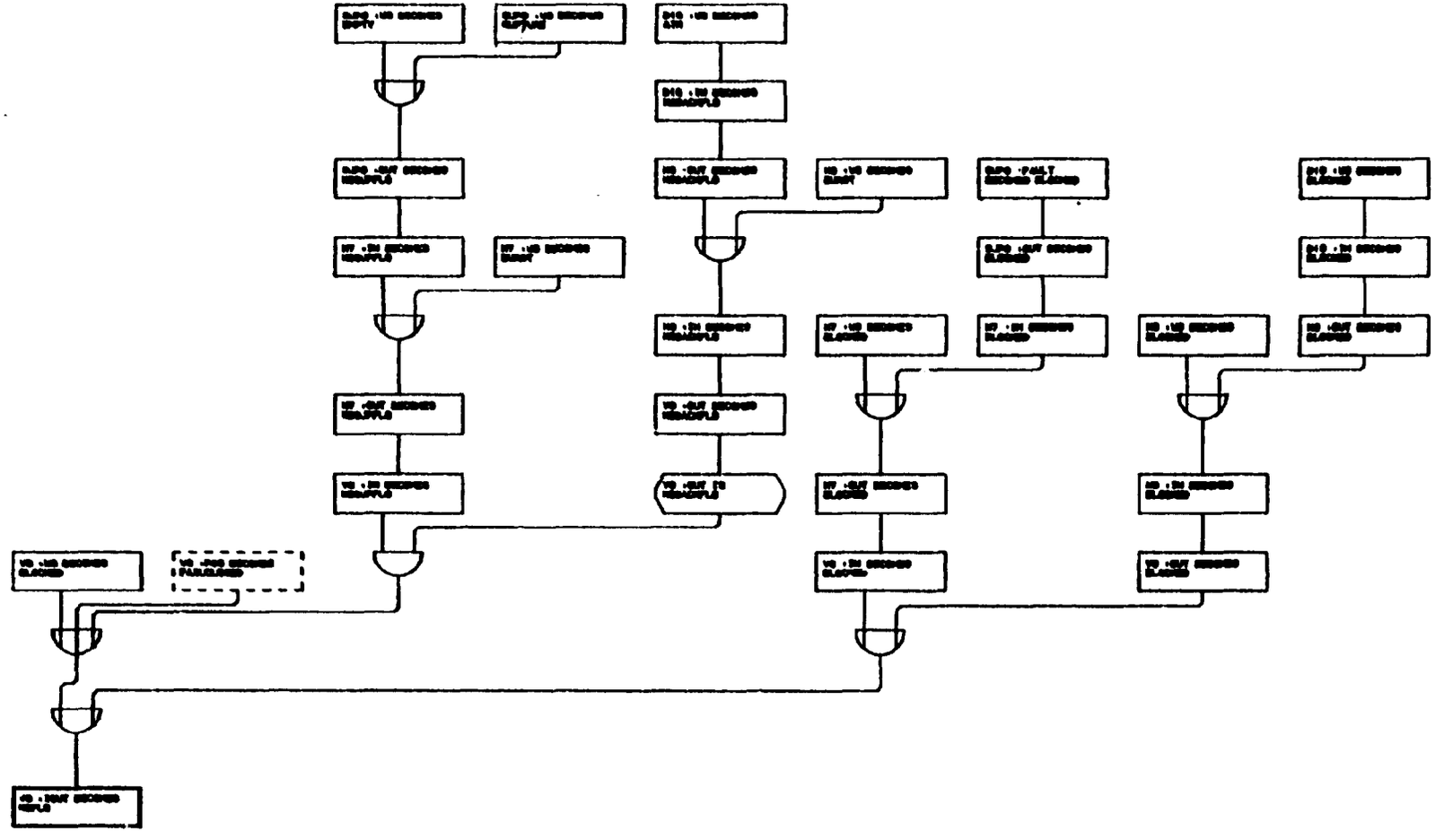


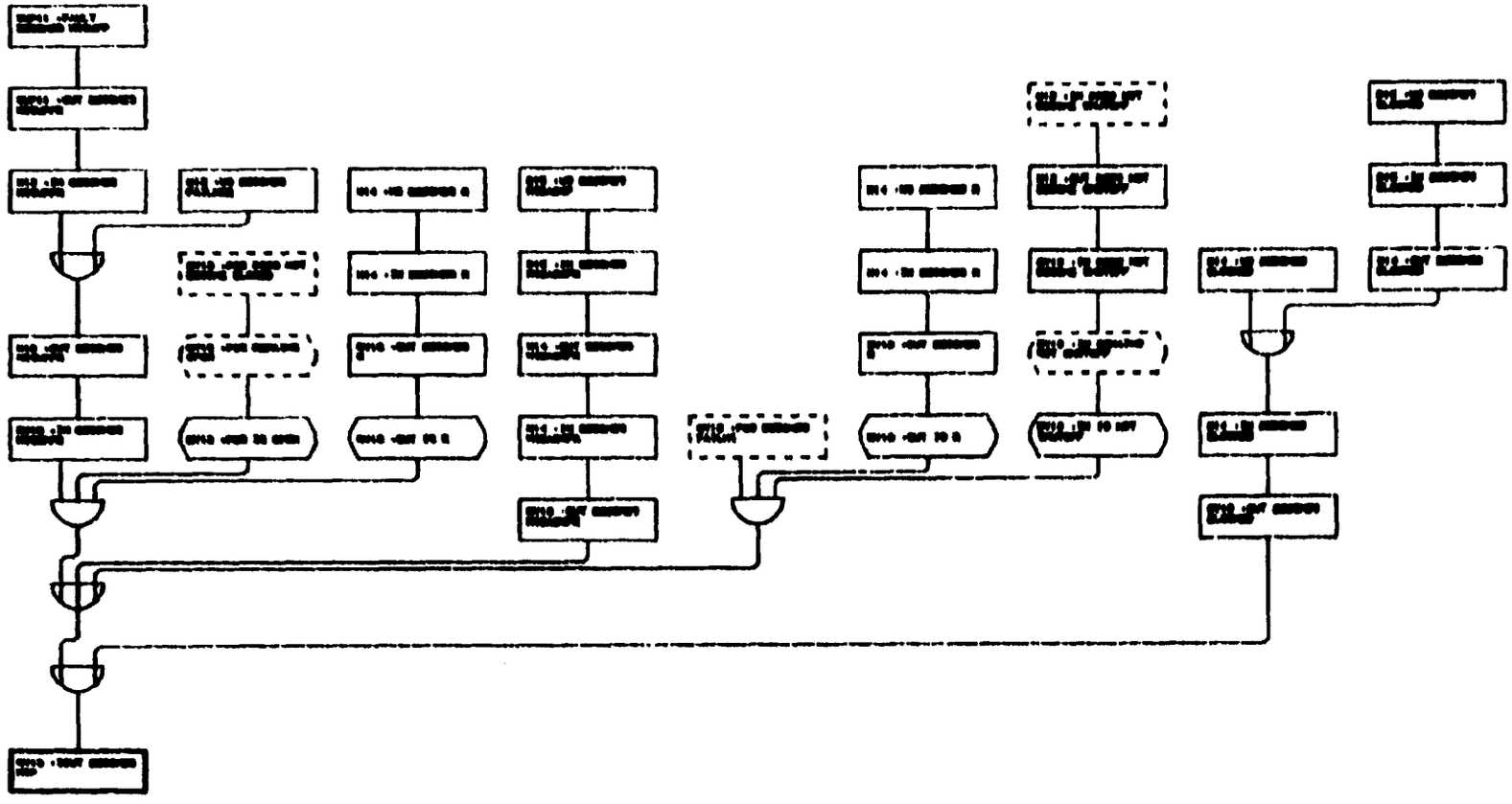


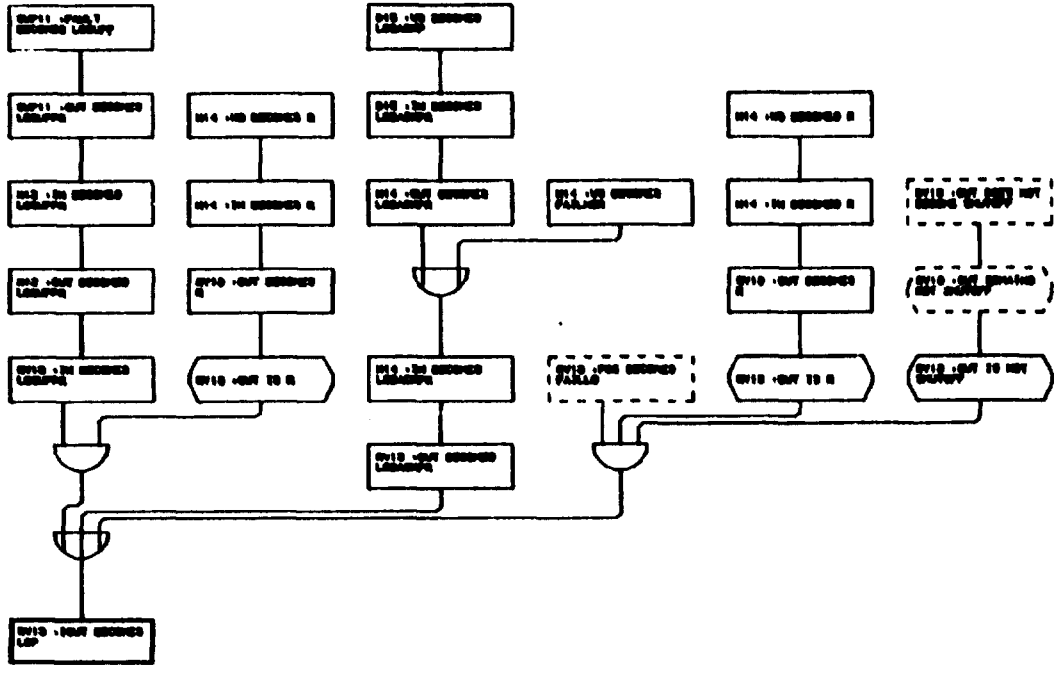


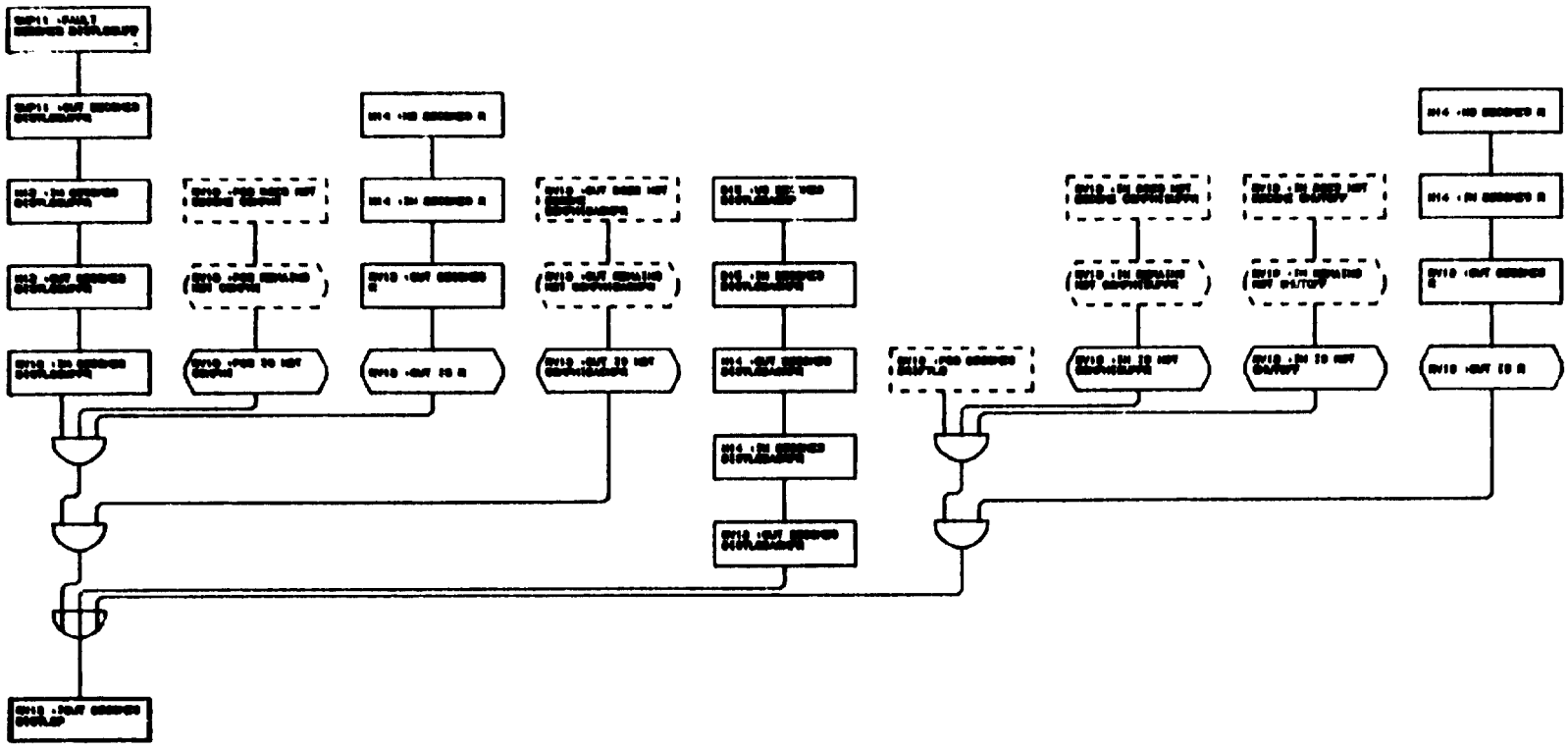


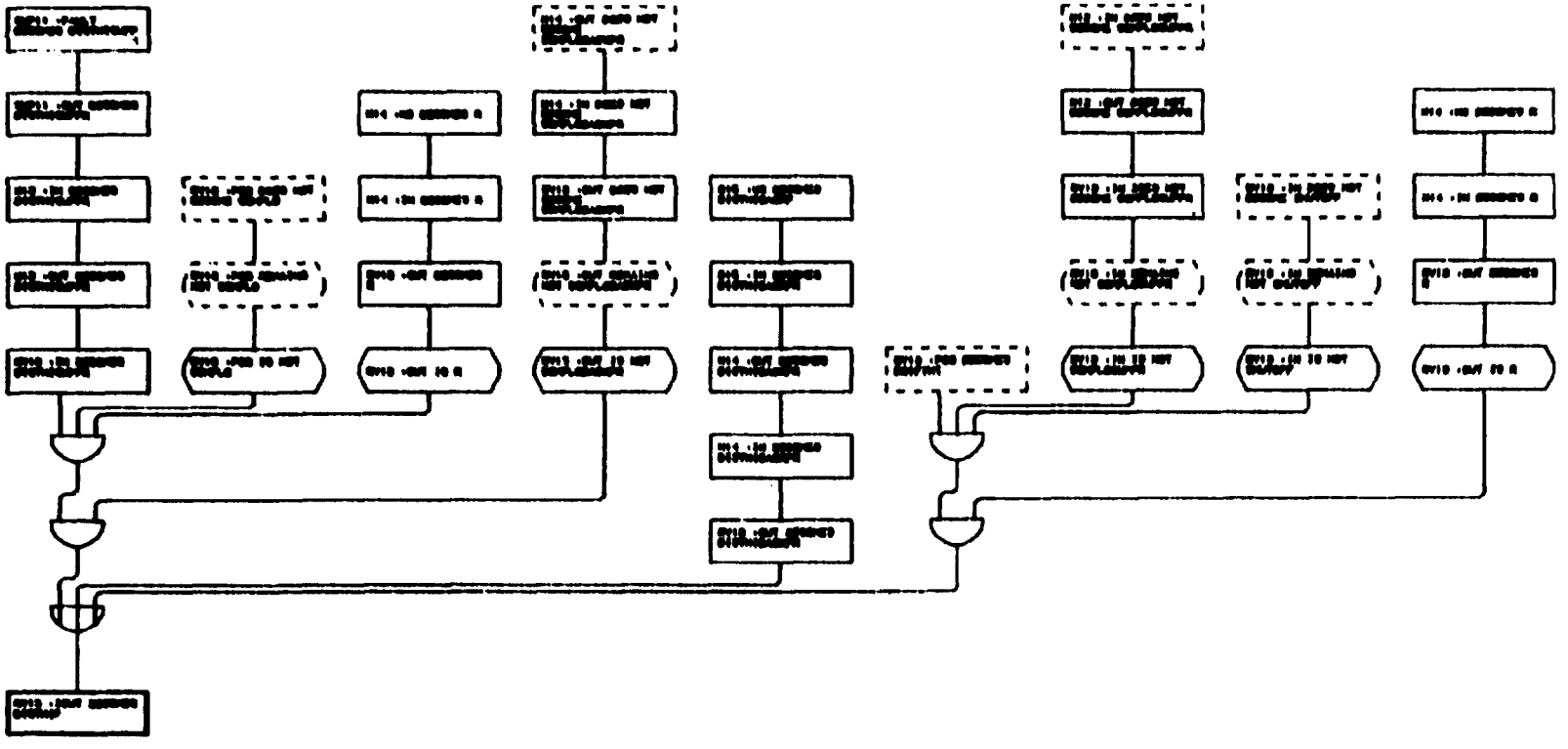


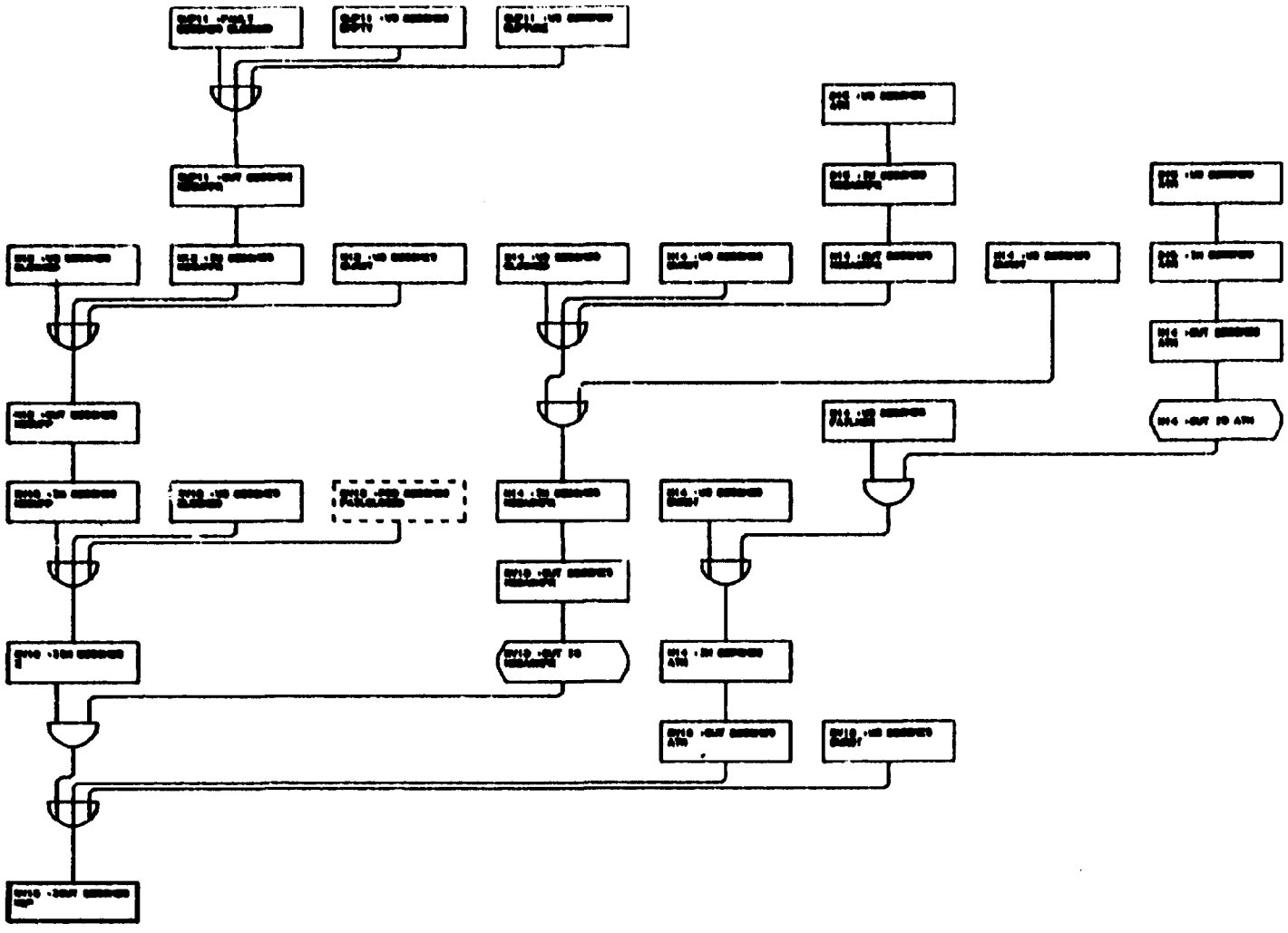


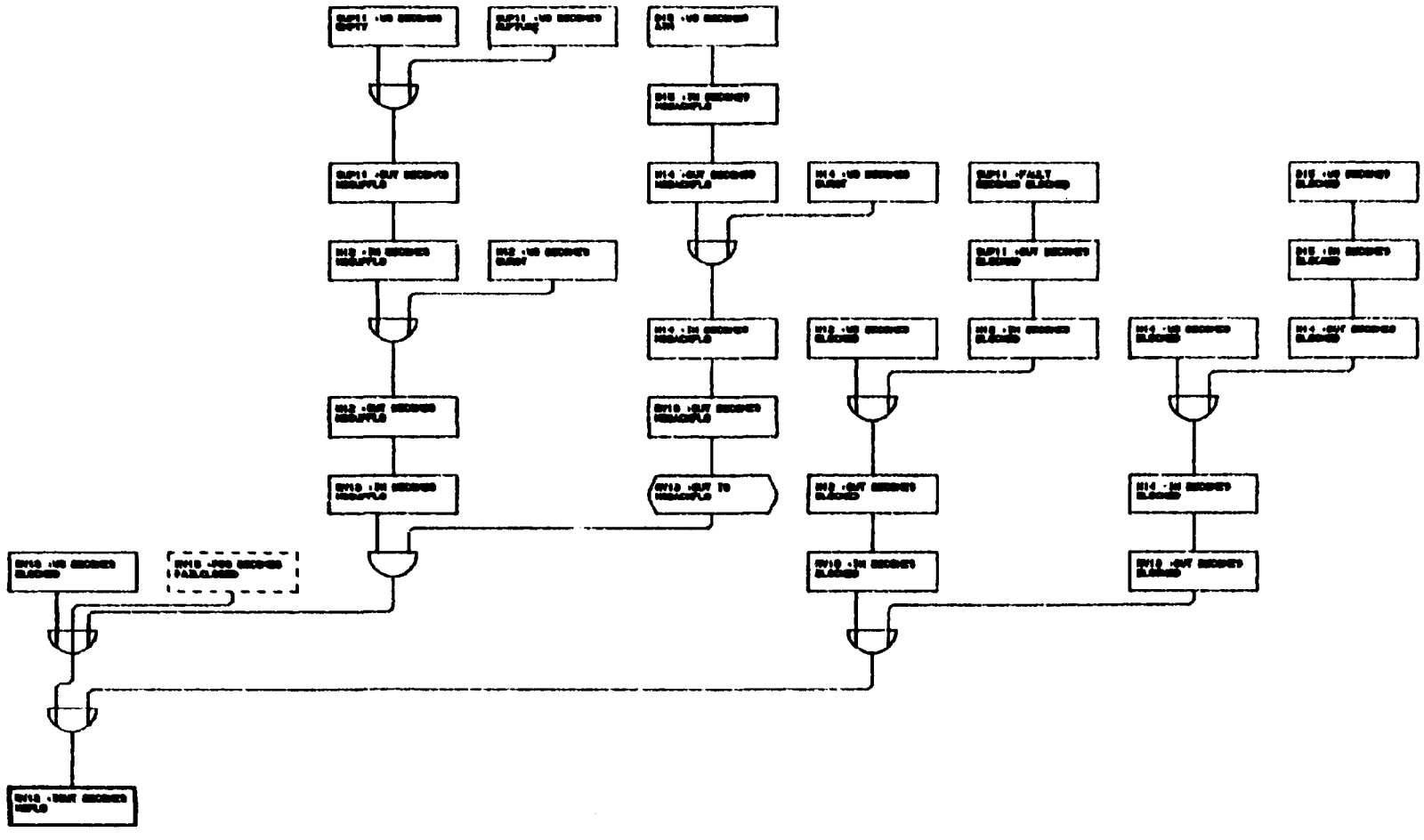


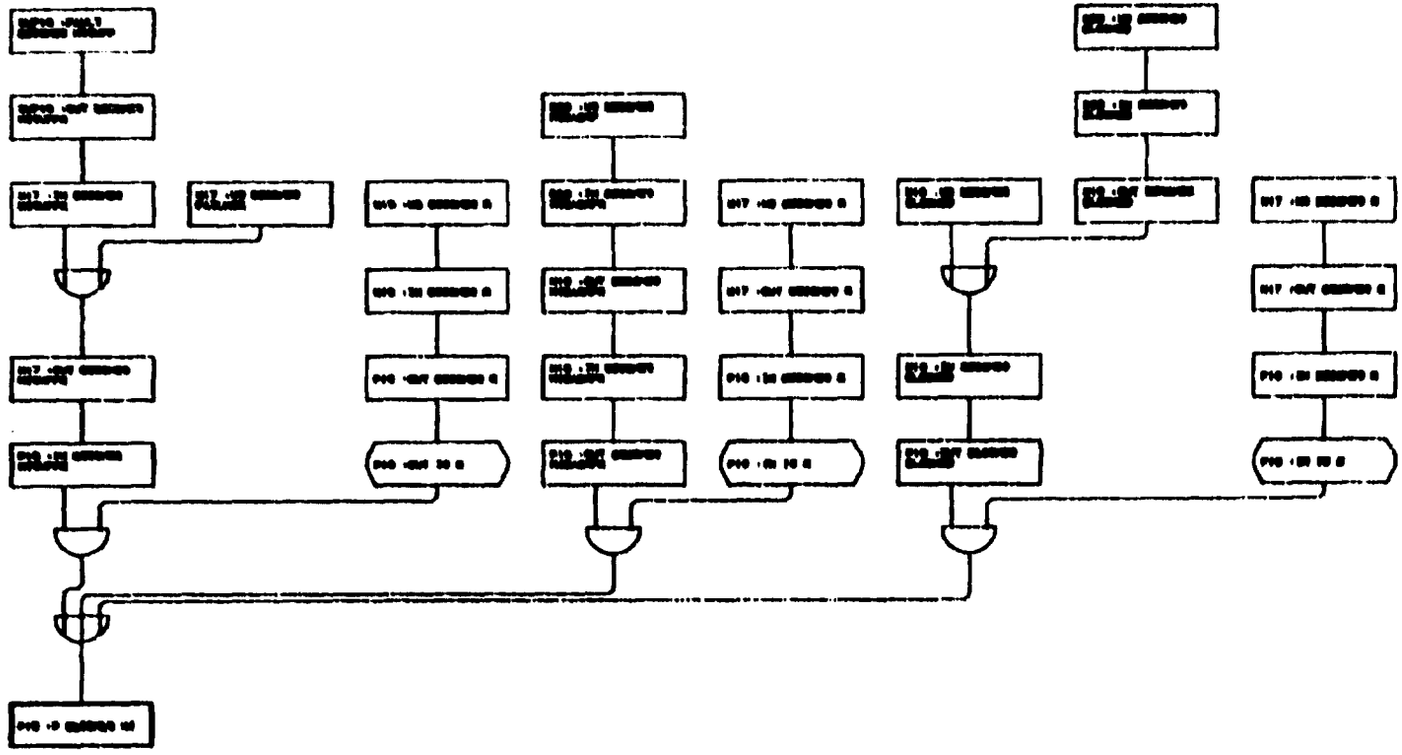


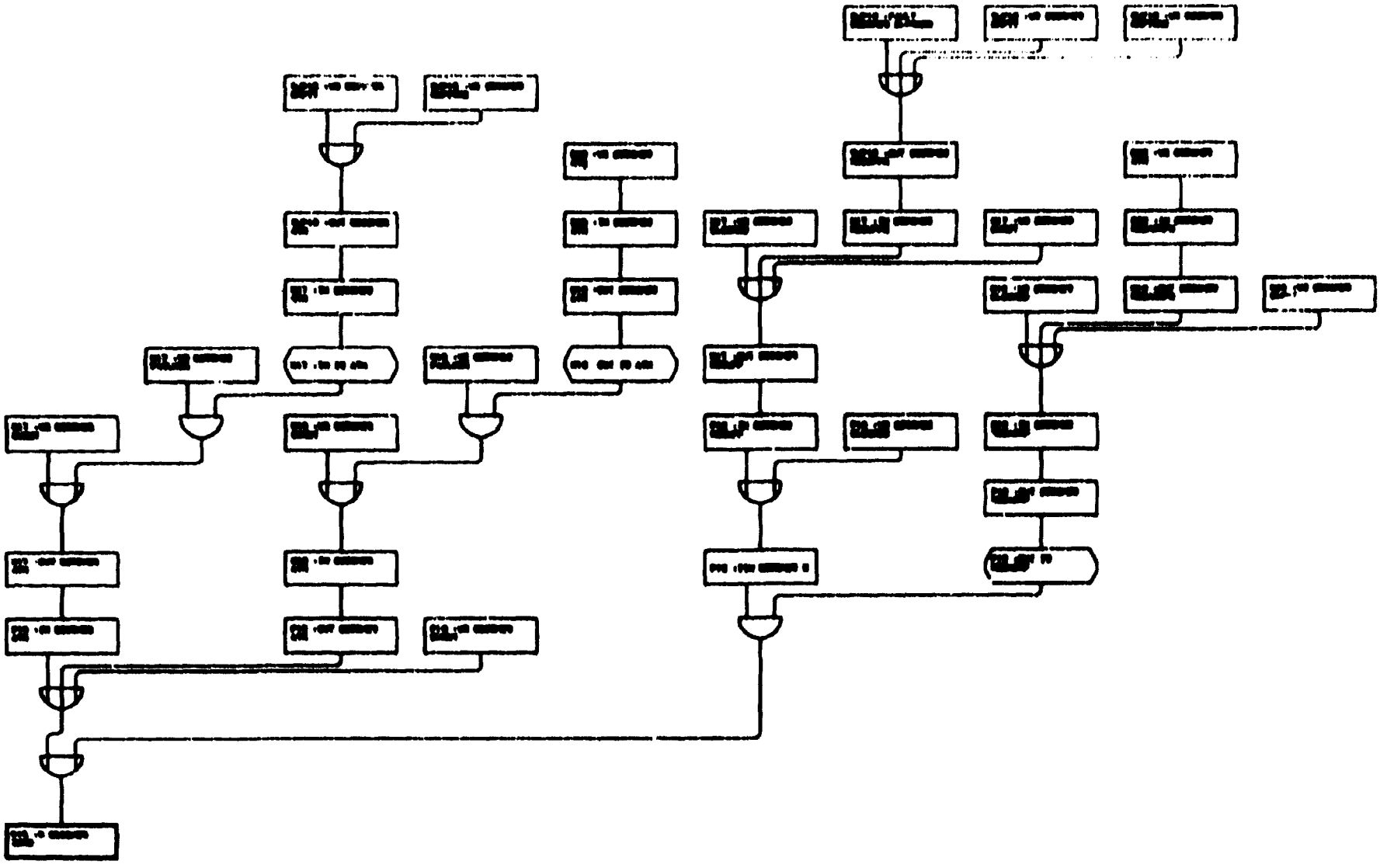


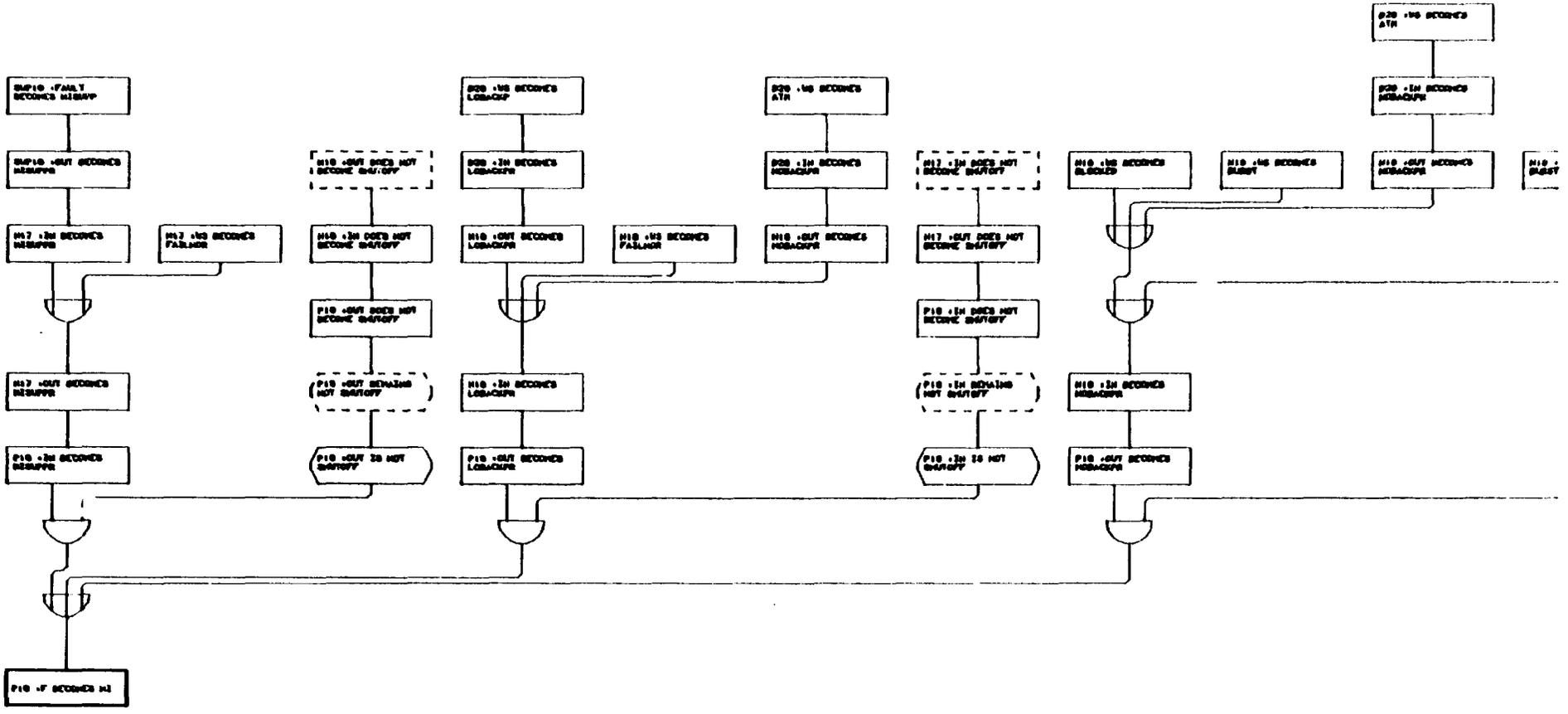


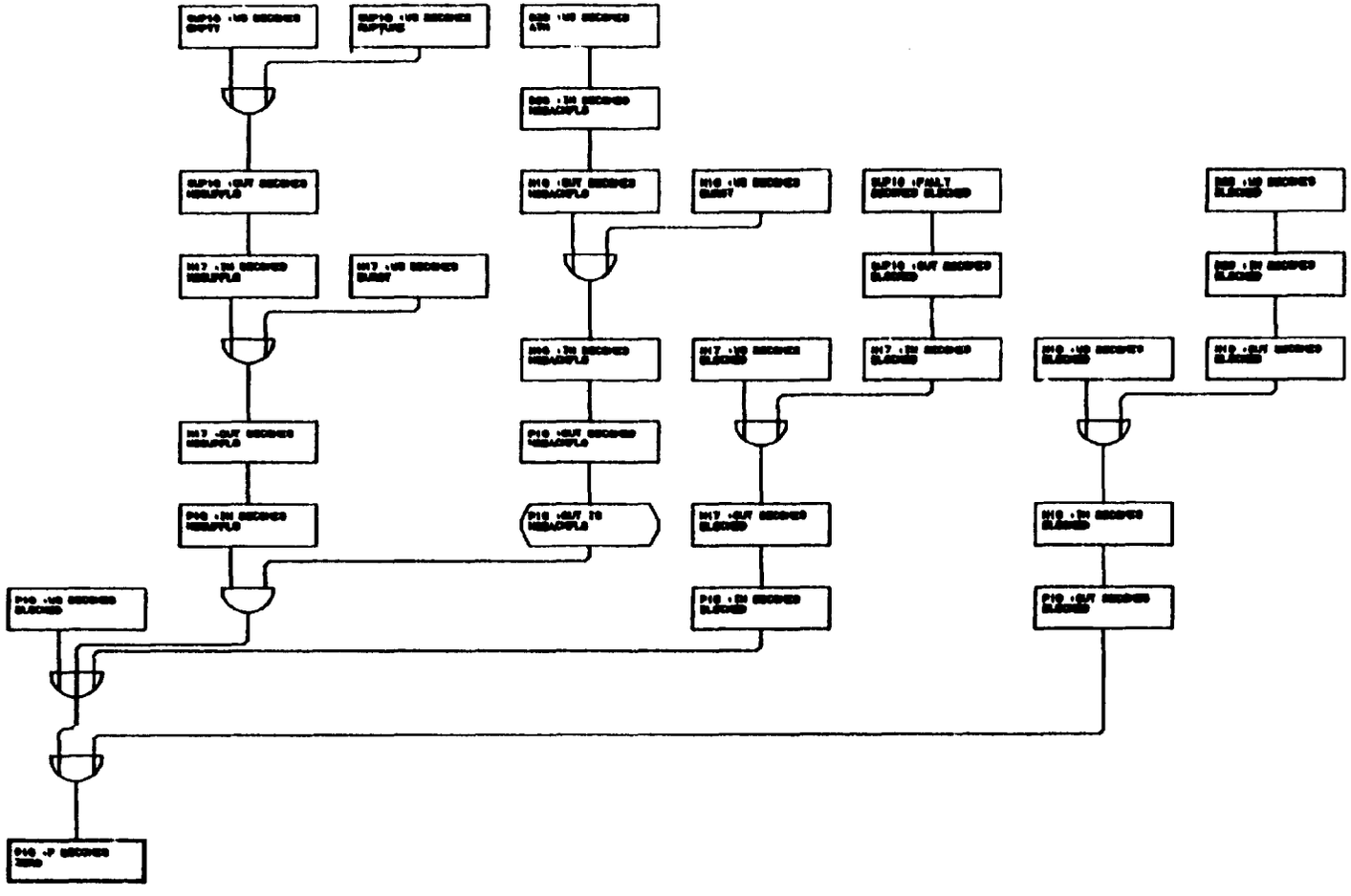




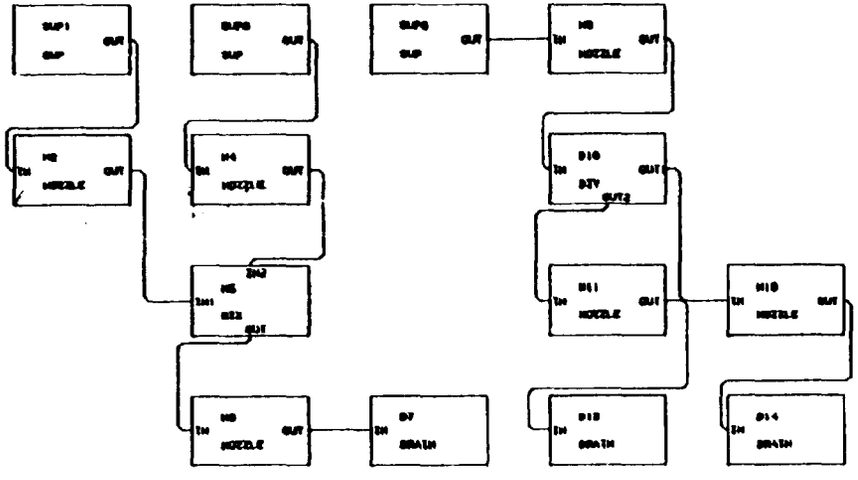


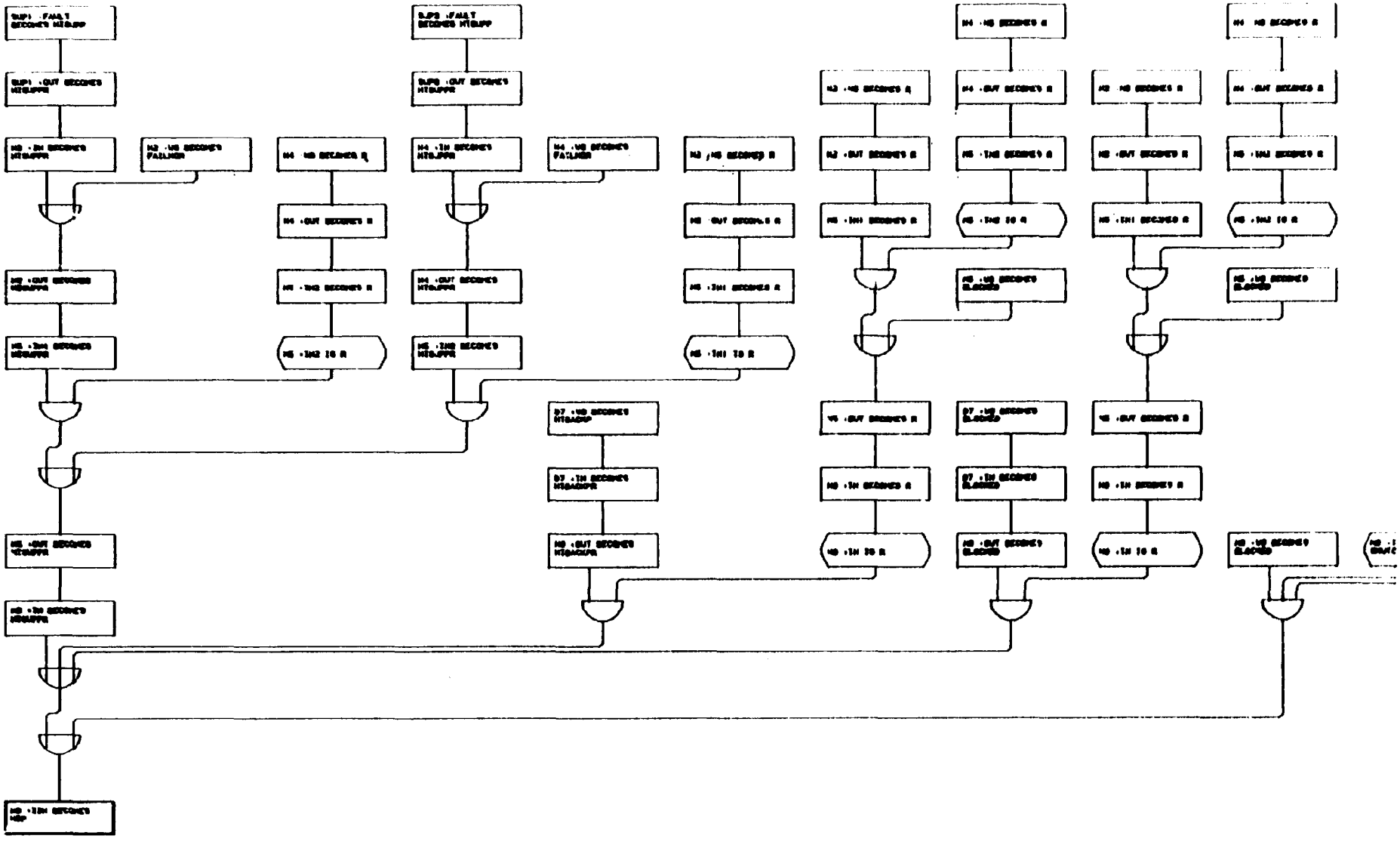


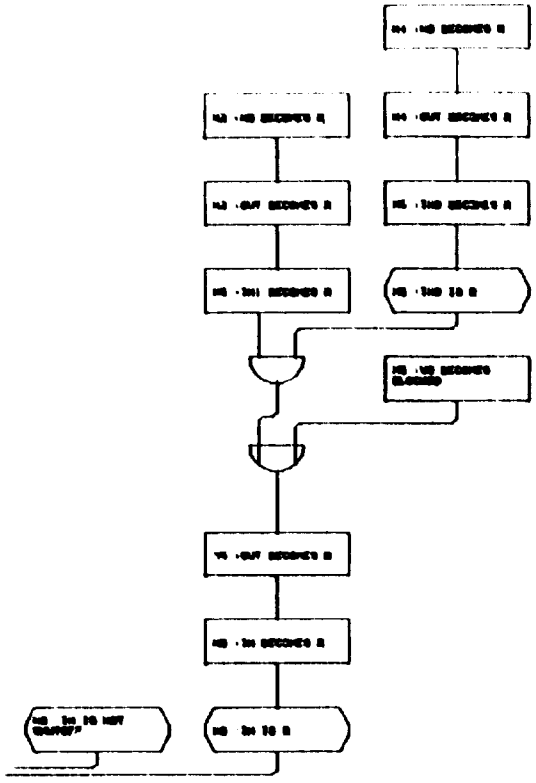


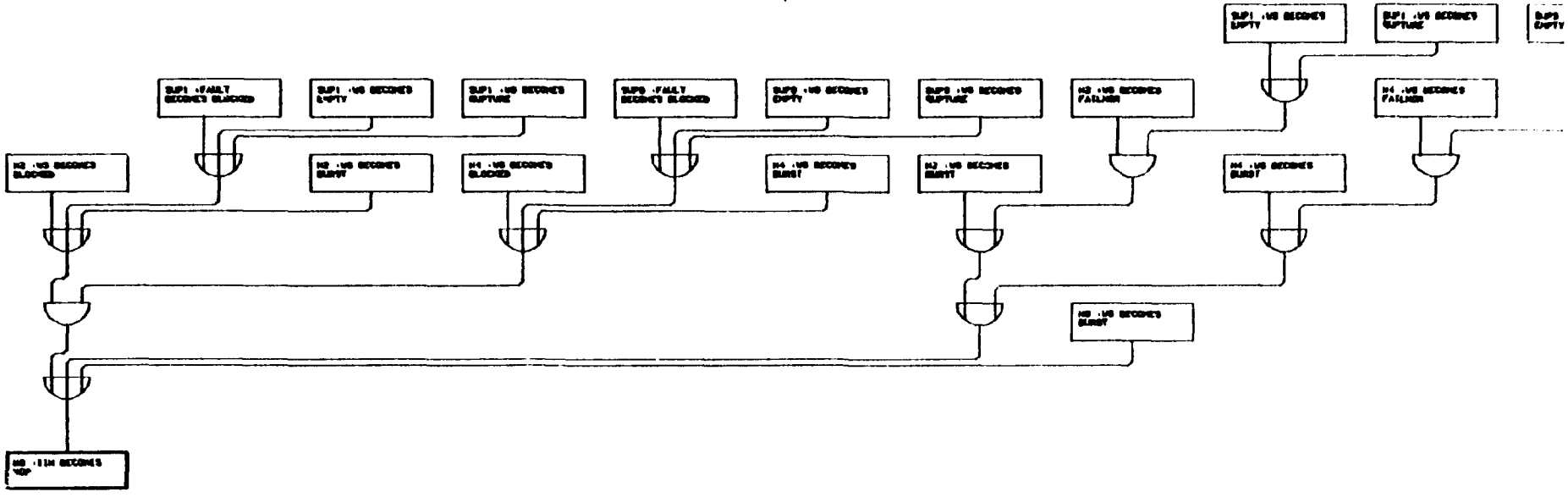


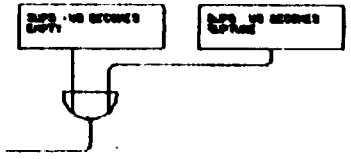
WYE AND LAMBDA TEST OF MIX AND DIV

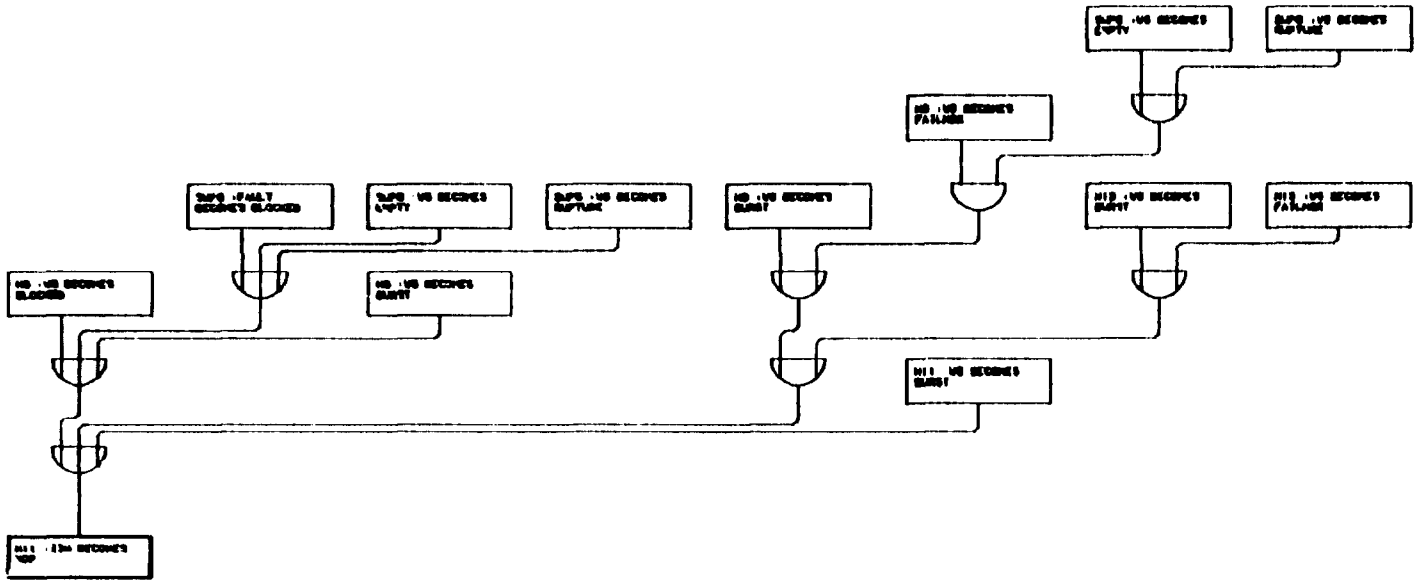




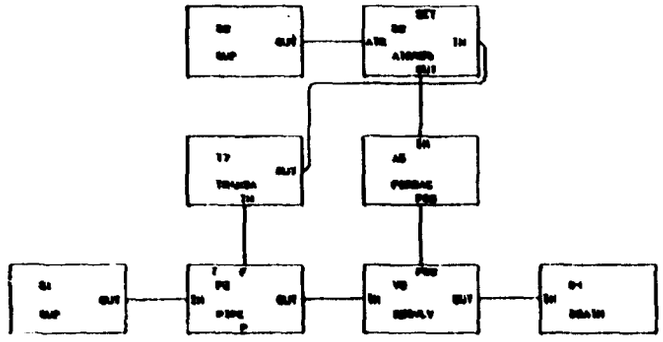


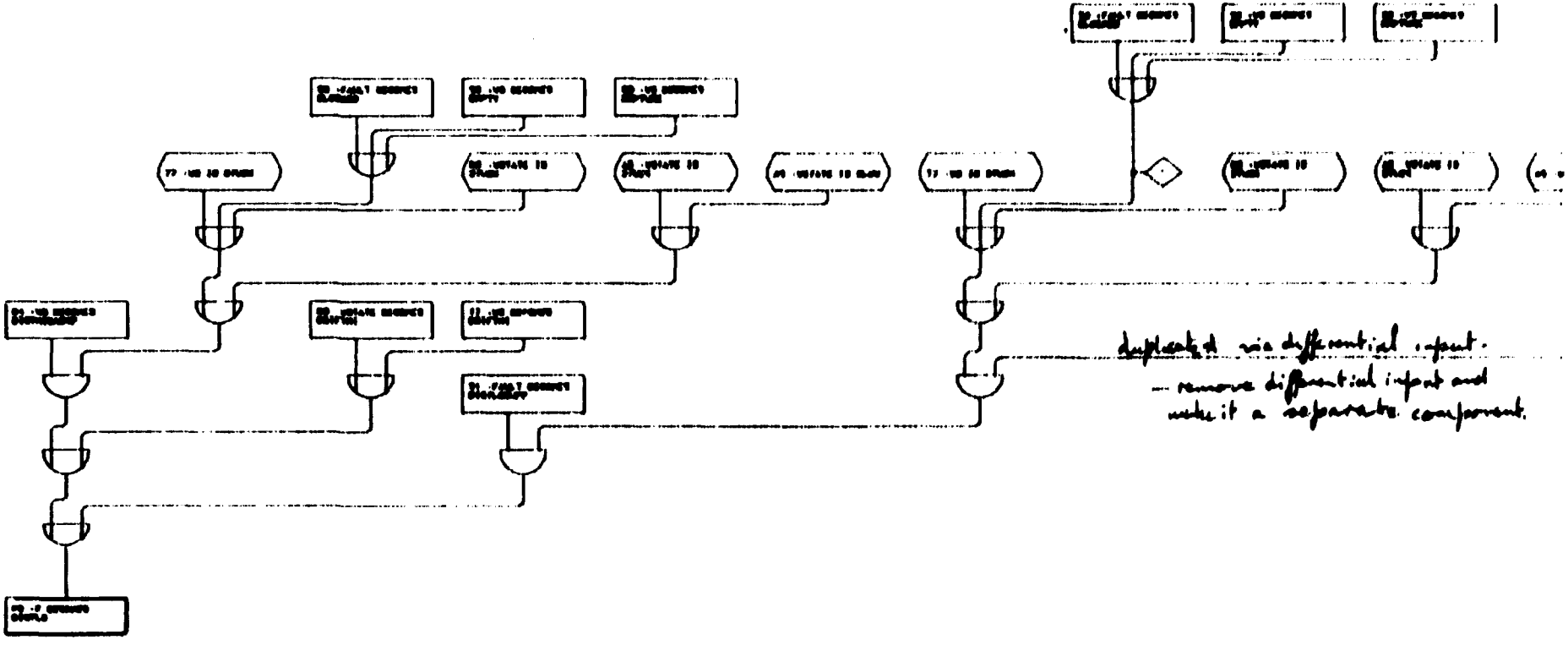


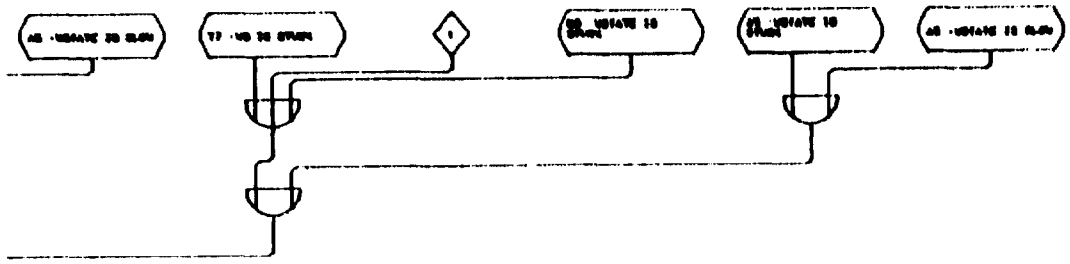


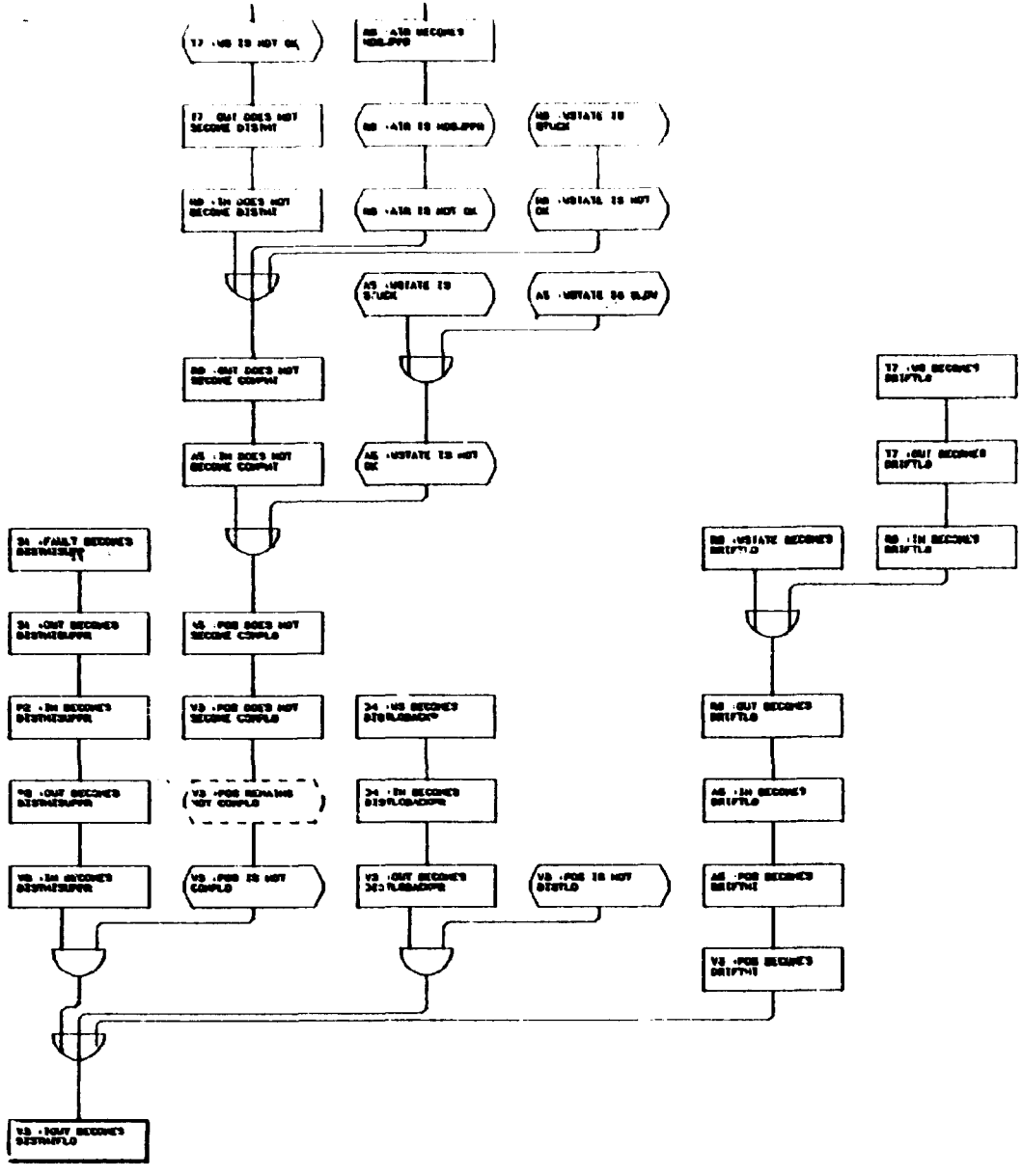


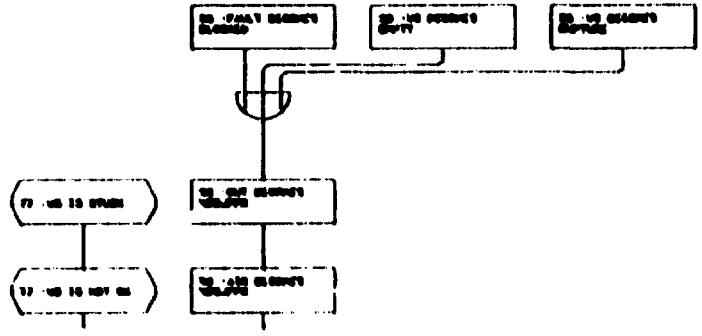
FLOW LOOP TEST OF CONTROL MODELS

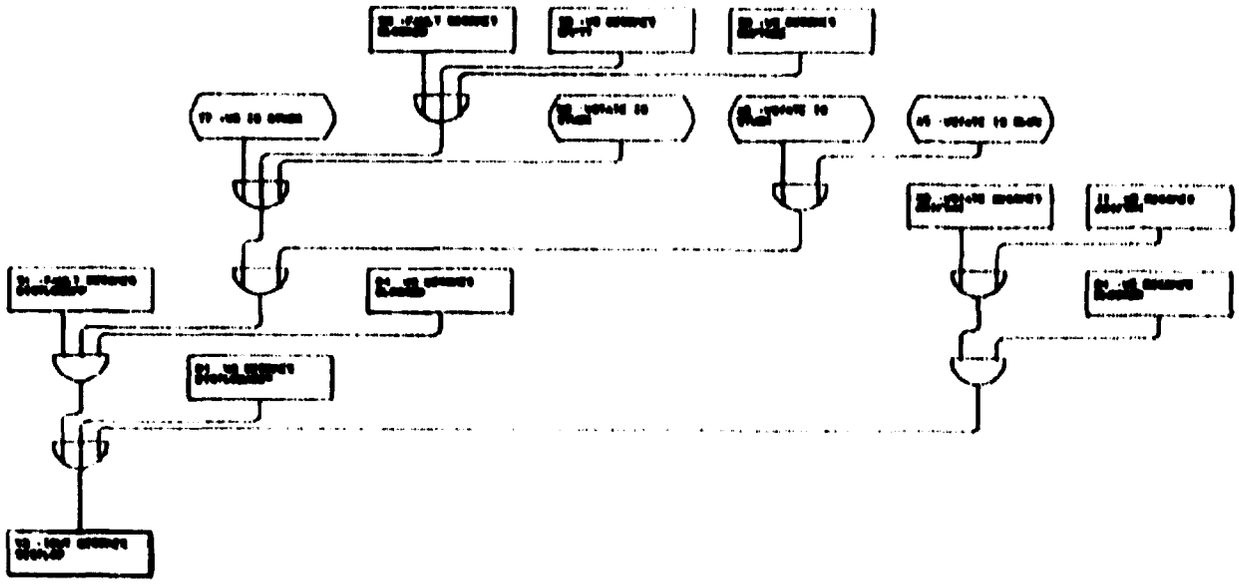


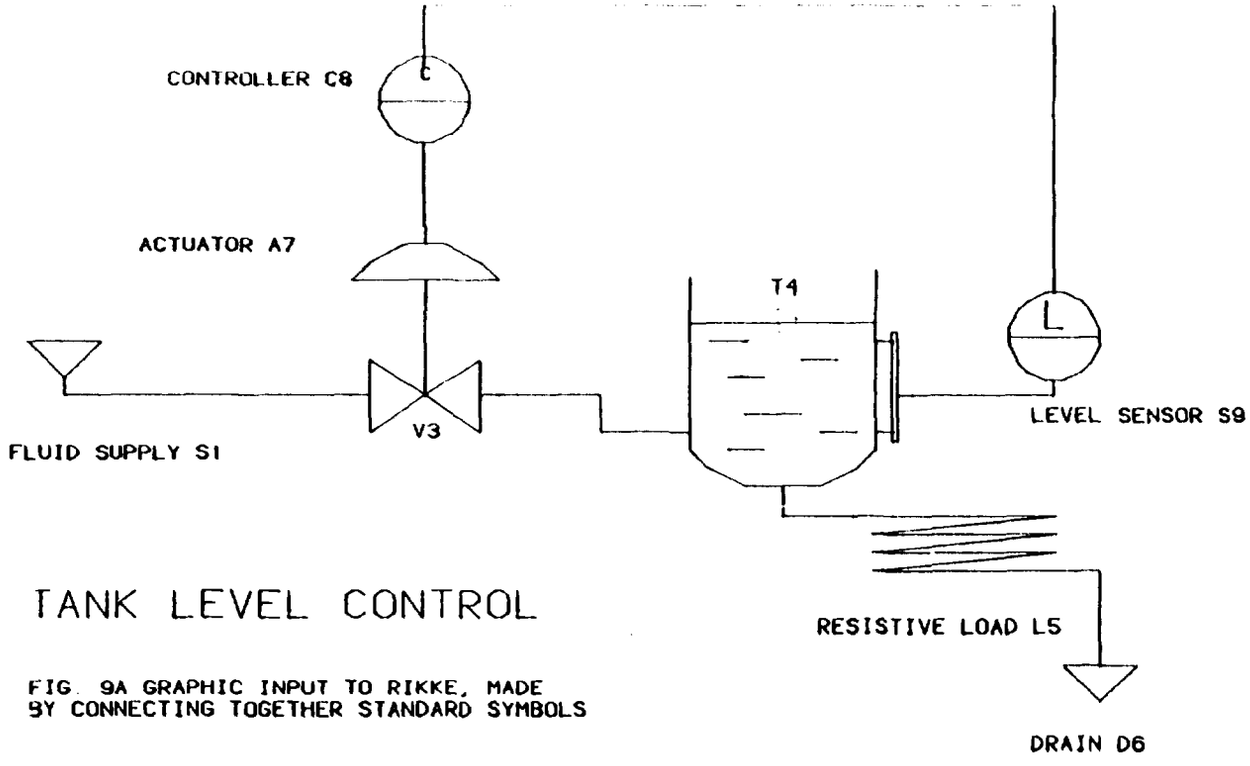

duplicated via differential input.
— remove differential input and
make it a separate component.





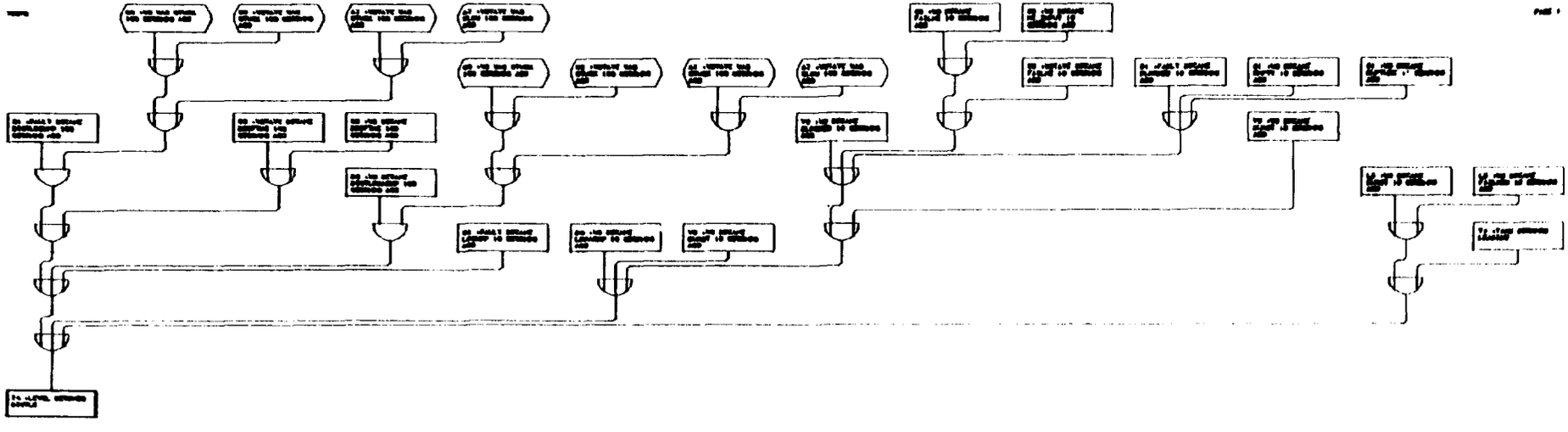


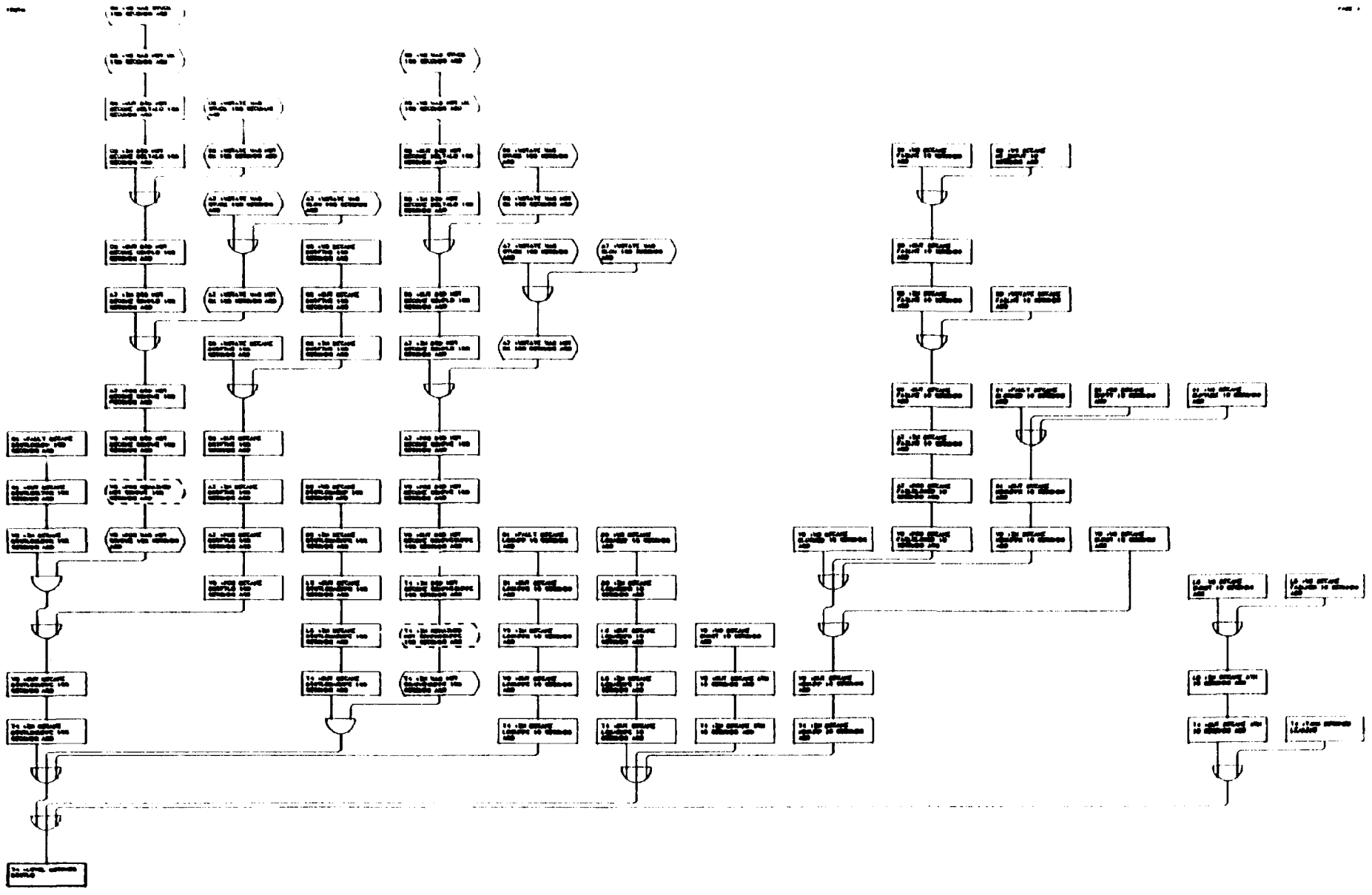


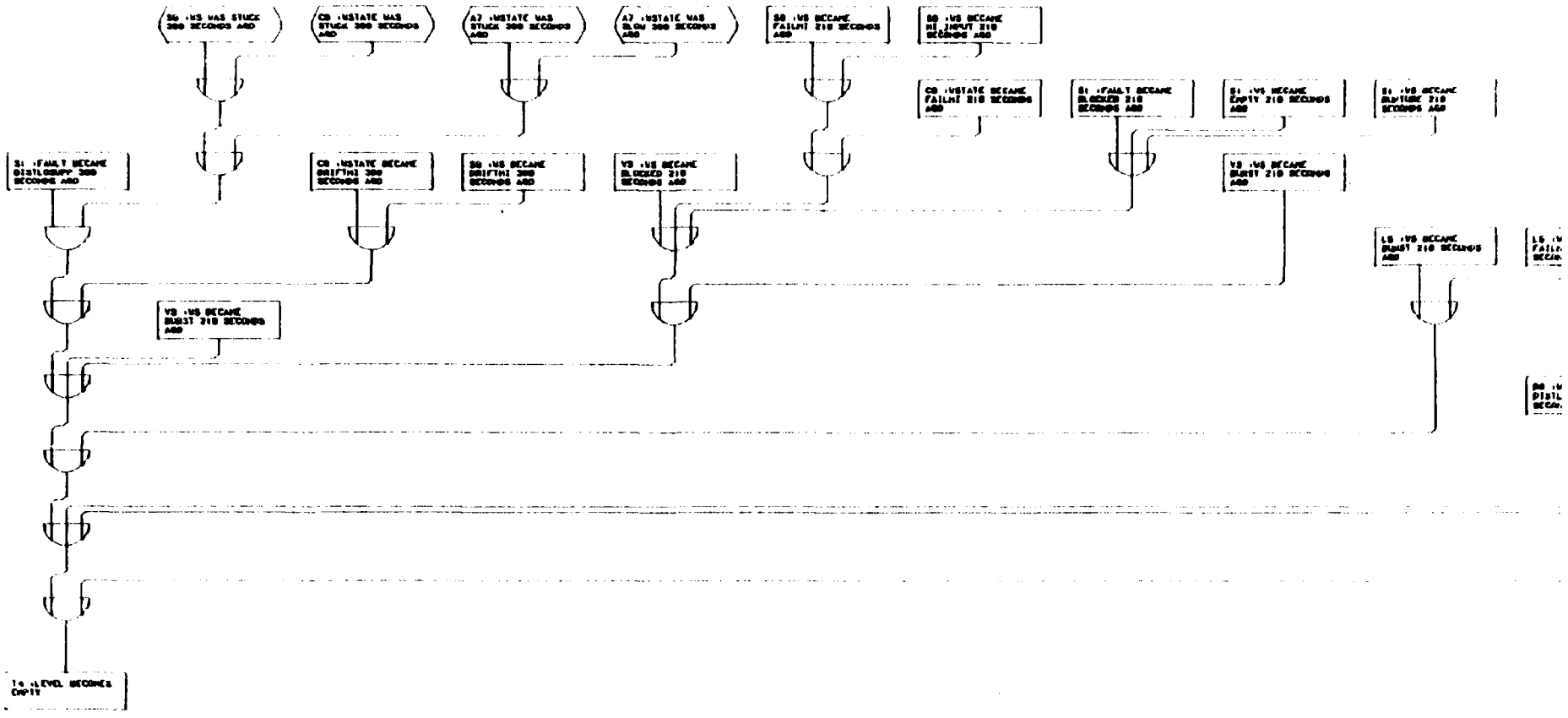


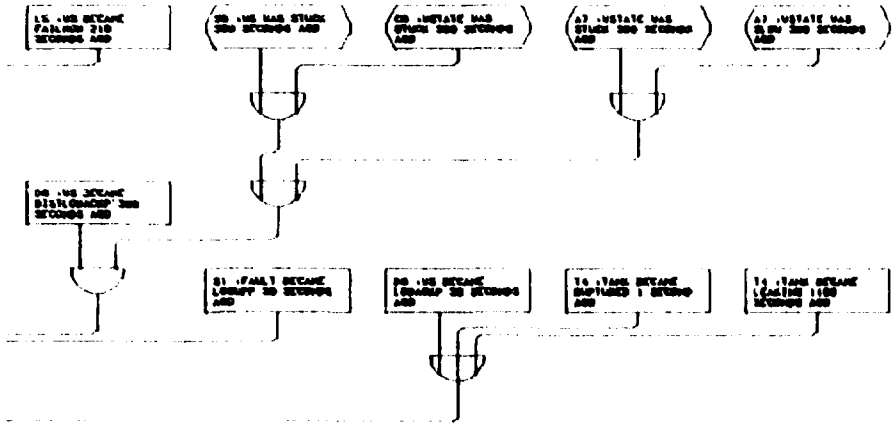
TANK LEVEL CONTROL

FIG. 9A GRAPHIC INPUT TO RIKKE, MADE BY CONNECTING TOGETHER STANDARD SYMBOLS









Risø National Laboratory **Risø-M-** 2311

Risø-M- 2311

Title and author(s)

Automatic Fault Tree Construction - A Compendium of Examples, Volume I. Basic Models.

J.R. Taylor

Date 1981-09-29

Department or group

Electronics

Group's own registration number(s)

R-12-81

pages + tables + illustrations

Abstract

Examples of automatically constructed fault trees are given. In this first volume, simple component configurations which illustrate individual component model types are treated.

Copies to

Available on request from Risø Library, Risø National Laboratory (Risø Bibliotek), Forsøgsanlæg Risø), DK-4000 Roskilde, Denmark
Telephone: (03) 37 12 12, ext. 2262. Telex: 43116