Gates *Energy Products*

FAULT TREE ANALYSIS

NiH$_2$ AEROSPACE CELLS

FOR LEO MISSION

Glenn C. Klein
Gates Aerospace Batteries

Donald E. Rash, Jr.
Reliability Analysis Center

FAULT TREE ANALYSIS, NiH$_2$ AEROSPACE CELLS FOR LEO

Glenn C. Klein
Gates Aerospace Batteries

Donald E. Rash Jr.
Reliability Analysis Center

Abstract

The Fault Tree Analysis (FTA) is one of several reliability analyses or assessments applied to battery cells to be utilized in typical Electrical Power Subsystems for spacecraft in LEO missions. FTA is generally the process of reviewing and analytically examining a system or equipment in such a way to emphasize the lower-level fault occurrences which directly or indirectly contribute to the major fault or top-level event. This Qualitative FTA addresses the potential of occurrence for five specific top-level events: **HYDROGEN LEAKAGE** through either discrete leakage paths or through pressure vessel rupture; and, four distinct modes of performance degradation - **HIGH CHARGE VOLTAGE, SUPPRESSED DISCHARGE VOLTAGE, LOSS OF CAPACITY,** and **HIGH PRESSURE.**

Relationship Between Reality, System Model, and Decision Process

Figure 1 schematically depicts one decision making process wherein we may explore the relationship between reality, some model of our system, and the decision process. **REALITY** is defined by a system of internal and external boundaries. **OUR PERCEPTION OF REALITY** is defined by the Fault Tree. **BASIS FOR DECISION**, in this case some measured acceptance of risk, is justified by the degree to which redesign, qualification tests on parts and materials and discrete inspection or test points were utilized. Figure 2 illustrates a generic system to be analyzed with external and internal boundaries. Hence, **ITEM E** is the Power Sub-System and **ITEM F** is the Battery Assembly wherein items a-to-r would be individual cells.
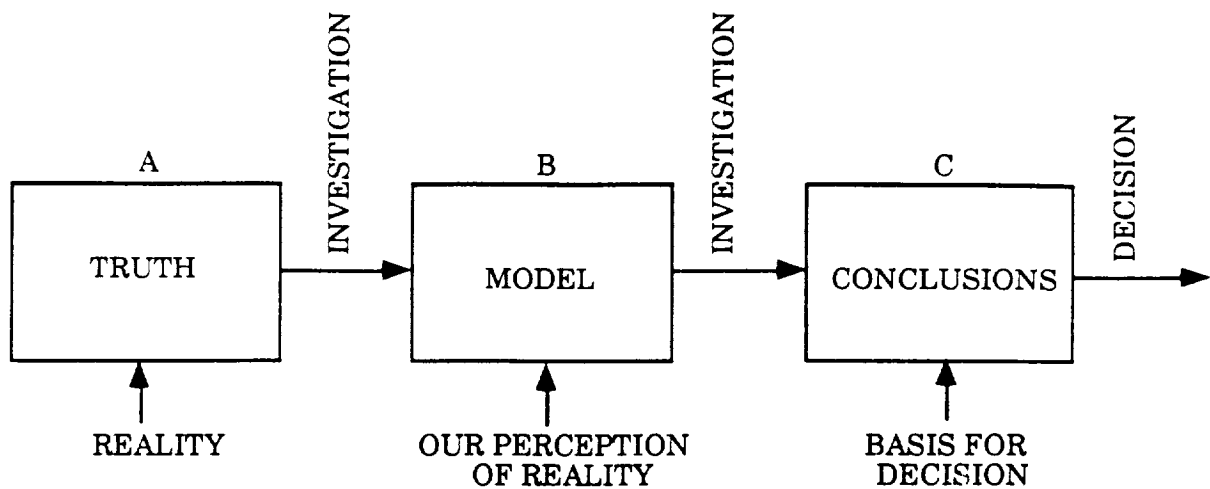
FIGURE 1: RELATIONSHIP BETWEEN REALITY, SYSTEM MODEL, AND
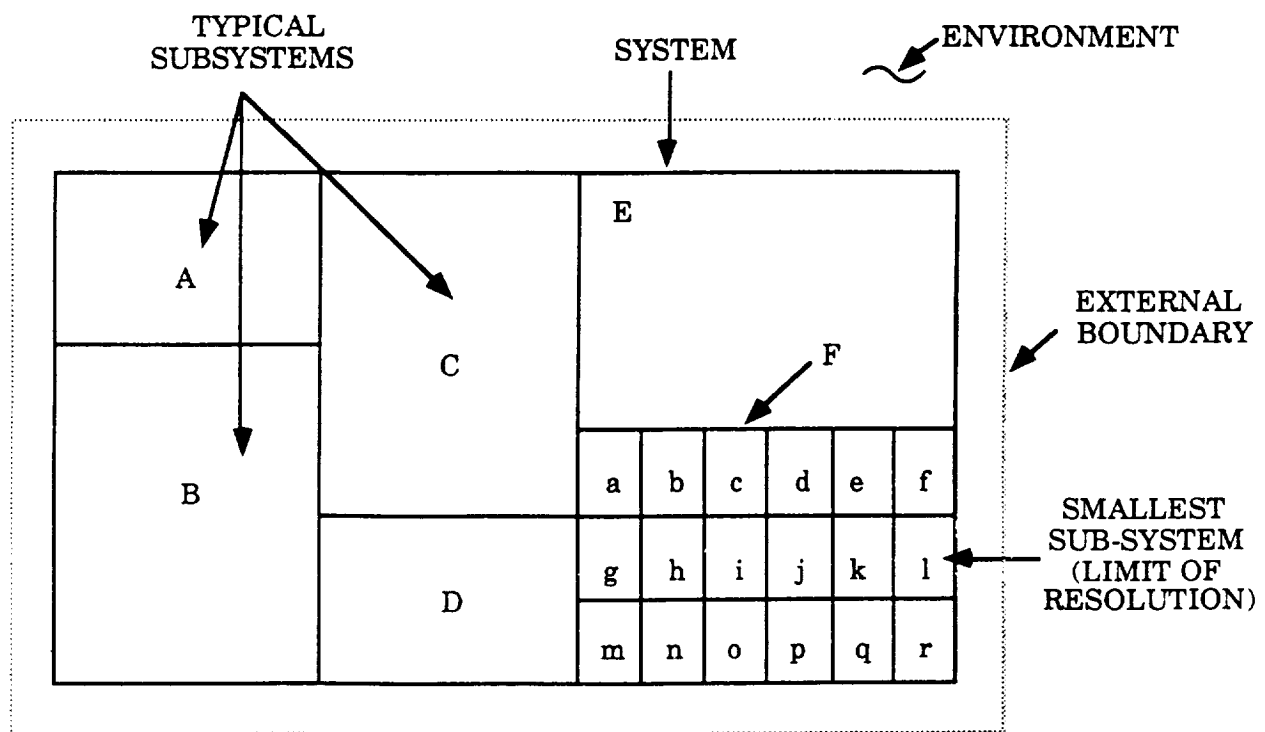DECISION PROCESS

FIGURE 2: SYSTEM DEFINITION: EXTERNAL AND
INTERNAL BOUNDARIES

The external boundaries describe the interface which the battery assembly, and ultimately the individual cells, experiences in the LEO mission profile. A typical profile requires continuous duty in combination with a solar array to store energy for use during peak power demands and eclipse periods, and may include:

a)   35% Depth of Discharge within 35 to 40 minutes followed by a C/1.67 rate recharge in 50 to 60 minutes

b)   nominal temperature range of 0 to 30°C

c)   a dynamic mechanical environment during the launch phase including a wide, but well defined spectrum, of random vibration; typical sustained acceleration of 20 g; and broad range of shock spectra

d)   life and reliability requirements including on station calendar life of 5.5 years MTBF and a design cycle life of 41,000 cycles

The internal boundaries are described by the cell design and include the rudimentary details such as pressure vessel material composition and thickness, and the electrochemical characteristics of the nickel-hydrogen couple as well as the decision to use a recirculating stack design.

The degree to which a fault described in the Fault Tree may result in battery failure or performance degradation is masked somewhat by the availability of in-flight data; this could be equated to the Limit of Resolution in our generic system of Figure 2. The degree to which the actual mission profile conforms to the intended profile combined with the ability of the NiH_2 cell to perform its intended function, irregardless of the nonconformance, is a measure of "robustness of design."

Basics of Fault Tree Analysis (FTA)

Figure 3 illustrates symbols typical of those used in our NiH_2 FTA; numerous others are available see Reference 2. The **rectangle** contains a brief description of the top-level event and appears at top of the tree. The **rectangle** is also used in this tree to signify a lower-level event and contains a brief description; these lower-level events occur throughout the tree and have both their input and output from a logic gate. The **circle** represents a basic or the lowest-level event which may cause a fault to occur and is used as an input to a logic gate. The **diamond** is a transfer
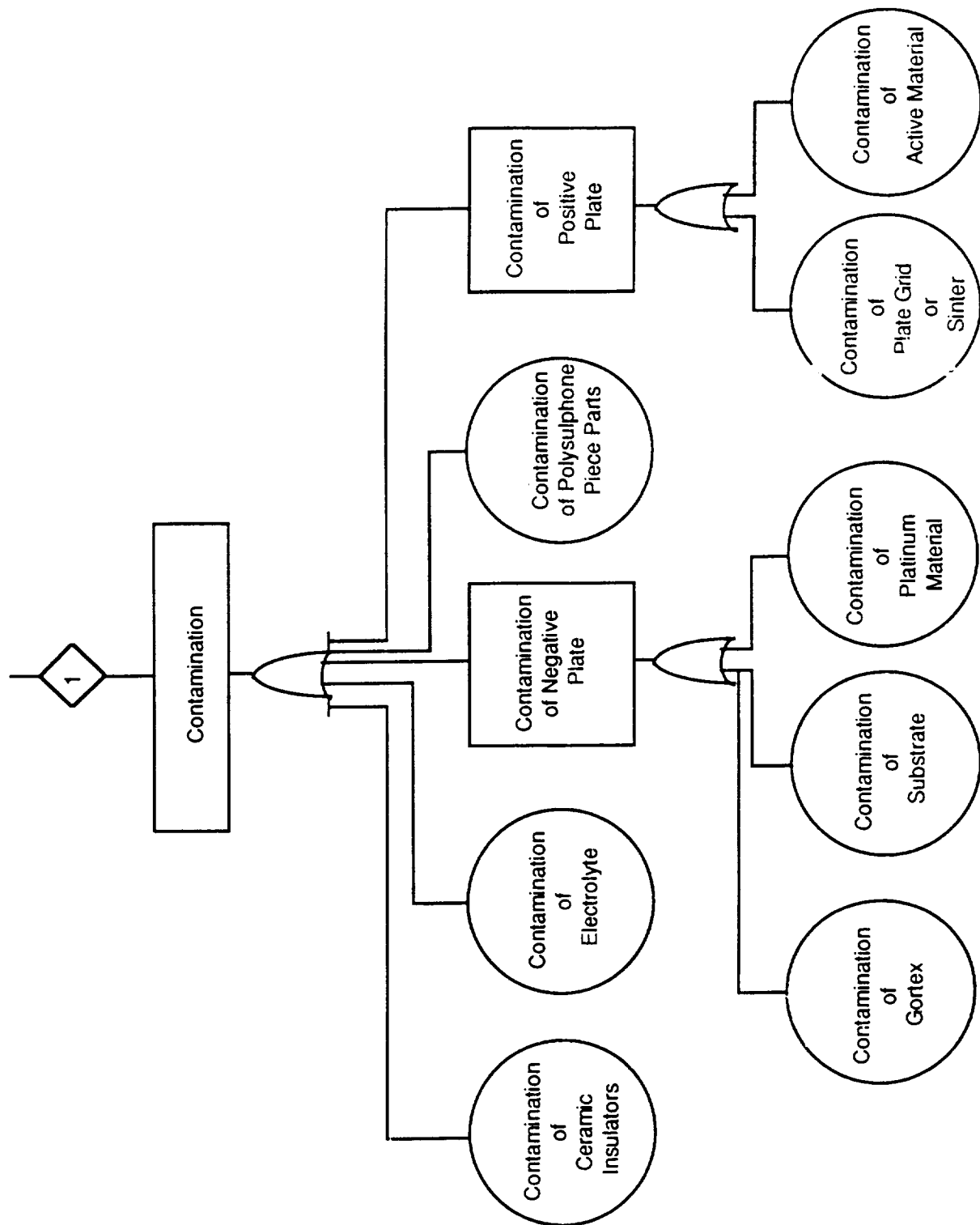
FIGURE 3: FAULT TREE SYMBOLOGY

function and is used to signify a connection between two or more sections of the fault tree. Logic Gates include the **OR Gate** for which output occurs when one or more of the input events occur; whereas, the **AND Gate** only occurs if all the inputs exist simultaneously.

Failure Effects, Failure Mode, and Failure Mechanism

Understanding and defining how a specific failure mechanism produces a discrete failure mode which may effect system operation is important for determining the proper inter-relationships among the events. In addition, the orientation of the analysis, that is whether to concentrate on system response symptoms or specific signatures generated by active components, determines both the success of the analysis and the effectiveness of resulting remedial actions. Failure Effects: what are the effects of the failure, if any, on the system. Failure Mode: what aspect, condition, or position is of concern. Failure Mechanism: what particular mechanism or vehicle prompts the failure mode to occur and what likelihood of occurrence exists. Thereafter, failures may be classified as to component, environmental, human, or software. Component failures occur at the lowest level of examination and may in fact be discrete parts or materials. Environmental failures occur when the system is placed in an environment which the system was not designed to operate in and where overstress has now occurred. Human failures occur due to operator error and are most difficult to quantify given the unpredictably of humans in the elevated stress levels typically accompanying sophisticated, high reliability systems. Software failures are simply errors in the controlling software, but may be considered a sub-set of human failures or component failures. Notwithstanding these failure definitions, their existence simply becomes the further definition of internal and external boundaries of the system under analysis.

Top-Down Approach of the Fault Tree versus Bottoms-Up Approach of the FMECA

The top-down approach of the FTA presupposes sufficient examination of the system to enumerate the top-level events or major system performance failures. Thus, the examination and resulting analyses are limited to events which cause the top event to occur. This deductive approach postulates the opportunity for top level failure thereafter reconstructing events or behavior at the lower levels which contribute to this failure. The bottoms-up approach of the FMECA is inductive in

nature. This approach postulates numerous faults or initiating conditions and then attempts to determine the effect of that fault or condition on system operation and integrity. Generally, the FMECA tends to be initially more descriptive as a risk analysis and risk reduction tool because their format typically includes existing/projected compensation or control measures.

Qualitative Fault Tree for NiH$_2$ LEO

The discussion of faults versus failures necessarily assumes that the fault condition is of sufficient significance and magnitude to cause upper level failure events. Therefore, the role of various contaminants is not an idle reference in the fault tree of Figures 4 thru 22. There is no further assumption nor is there an attempt to yet quantify the level of contamination since some contaminants in small ppm may cause significant events which may lead to failure. No further assumption as regards passive versus active components and their significance is made either. When we analyze the pressure vessel for catastrophic burst and find the present design to leak before burst, there can not be an accompanying assumption which relegates this vessel to a passive component. The fault tree clearly shows a leaking pressure vessel to be an active contributor to upsetting the electrochemistry of the nickel-hydrogen couple which may eventually lead to either outright failure or performance degradation.

Five specific primary faults or top-level events addressed in the fault trees of Figure 4 are: **HYDROGEN LEAKAGE** through either discrete leakage paths or through pressure vessel rupture (discounted as a potential failure through both this analysis and the Fracture Control Plan); and four distinct modes of performance degradation (1) **HIGH CHARGE VOLTAGE, (2) SUPPRESSED DISCHARGE VOLTAGE, (3) LOSS OF CAPACITY,** and (4) **HIGH PRESSURE.**

Hydrogen Leakage

The critical fault, hydrogen leakage, was created in the classical fault tree analysis. By assuming the worst case scenario it was determined that the hydrogen leakage was and is the worst possible fault. All construction techniques were assessed from the top down to determine the different paths the leakage might occur. This event is typical of most NiH$_2$ pressure vessels and presents a generic path of construction criticality. By placing probabilities in each of the

lower fault events a manufacturer will be able to construct a detailed quantitative fault tree.

High Charge Voltage

This fault is divided into three generic failure modes of which two are identical to Loss of Capacity. These generic failure modes are further divided into specific failure modes which can be identified or traced back to respective FMEA failure modes. Some of these failure modes have been traced to their failure causes. These expanded fault trees may have no failure modes associated with them because either they are failure causes or are under review for inclusion into the growing Operational FMEA database.

High Pressure

Only two generic failure modes cause high pressure and one is unique to this fault. The flooding of the negative membrane is an operational fault that is a result of various contamination failures. We do not have FMEA worksheets filled out for contamination as it usually is identified in various FMEA worksheets as a failure cause.

Loss of Capacity

This fault tree is the least extensive of the operational critical faults. This is because it is associated with wearout mechanisms of the NiH_2 battery cell that are not modeled and has duplicity in other failure modes. The purpose of this fault tree is to show unique failure mechanisms associated with just Loss of Capacity. The loss of capacity has been divided into two larger groups of generic failure modes. These in turn have been broken down into other root causes and easily identifiable failure modes.

Suppressed Discharge Voltage

This fault tree is broken down into three specific failure modes identified by the operational FMEA worksheet numbers and one failure mode associated with NiH_2 wearout. A particularly interesting feature of this fault tree is that both hard and soft shorts can be caused by conductive particles. The conductive particle fault tree shows how these particles can be inherent to a fault process or introduced as foreign particles from material handling.
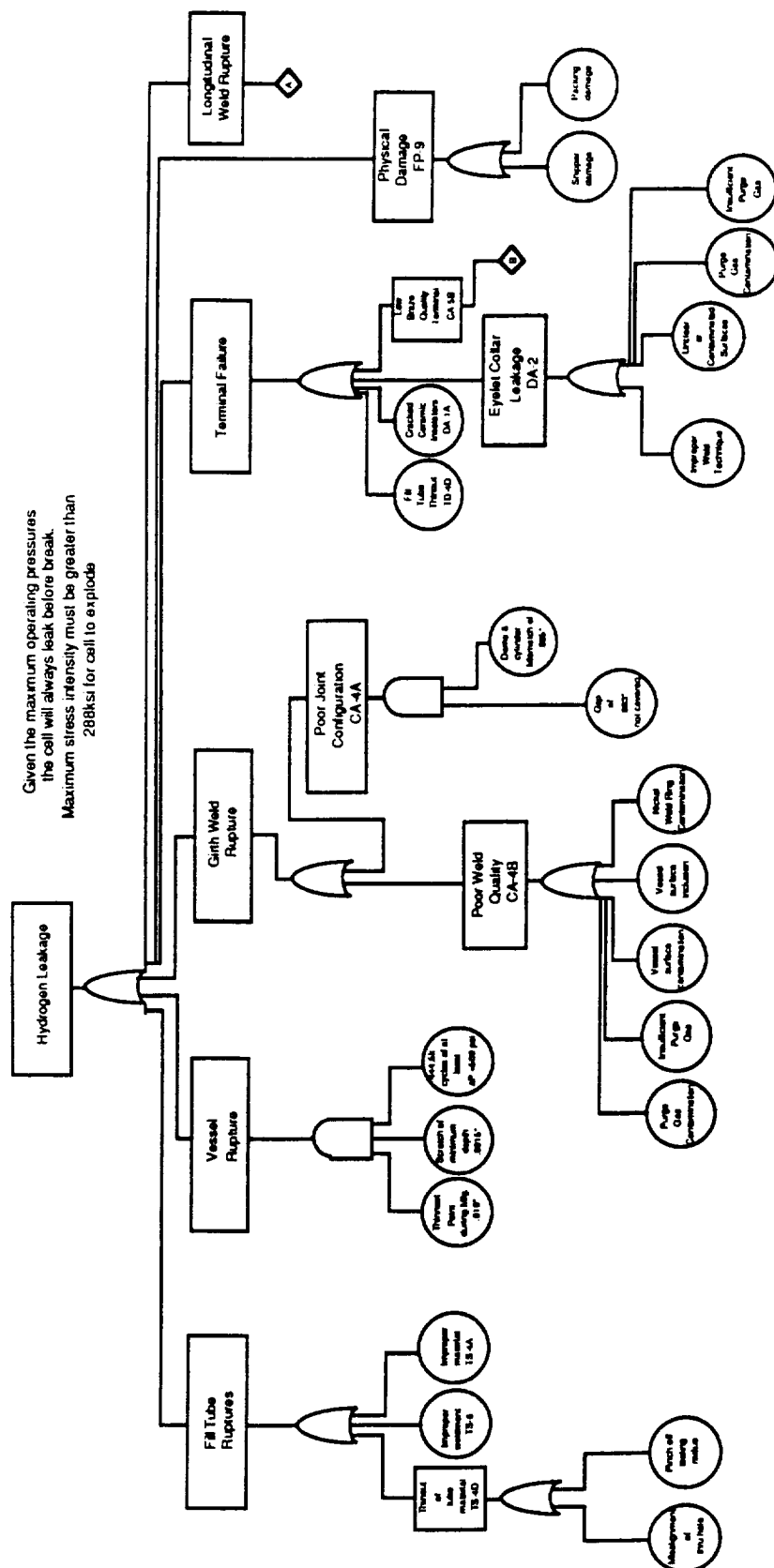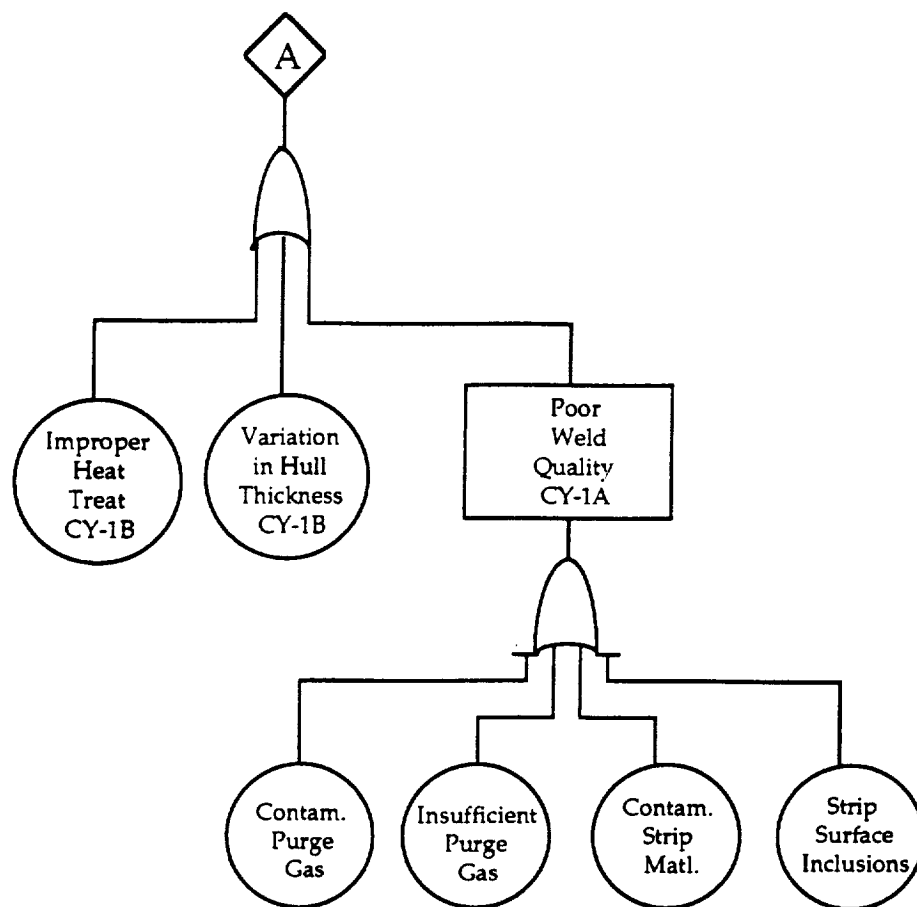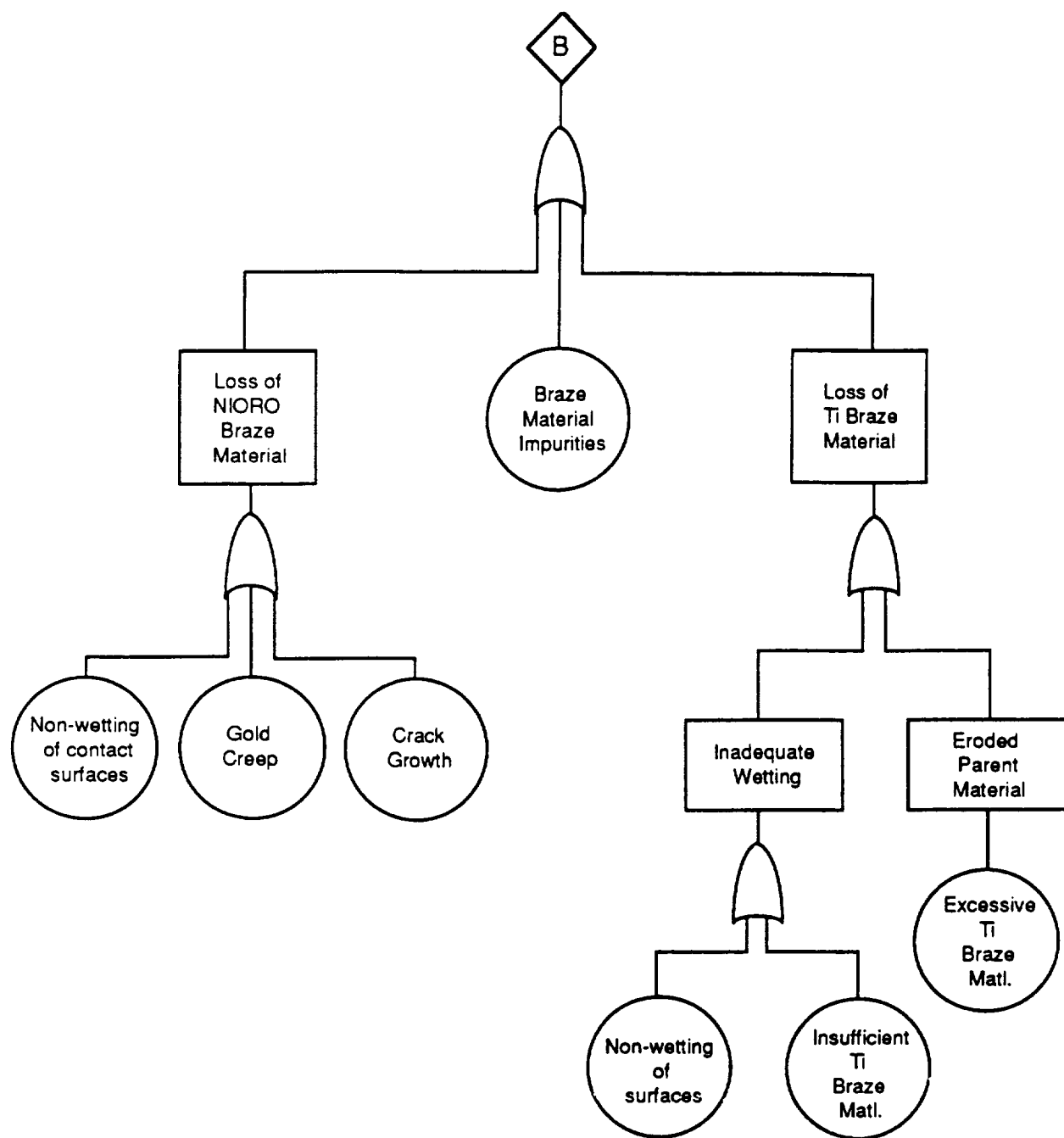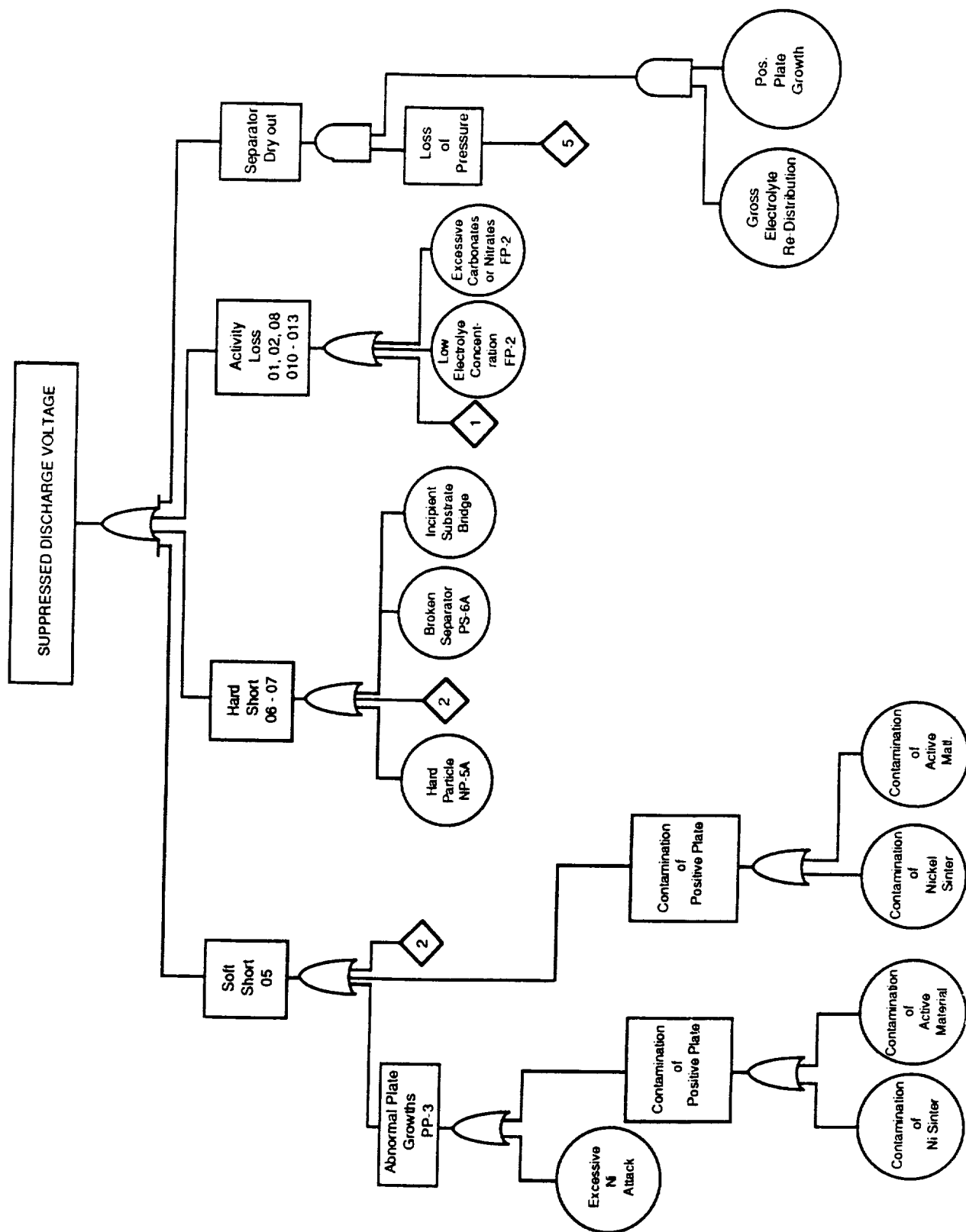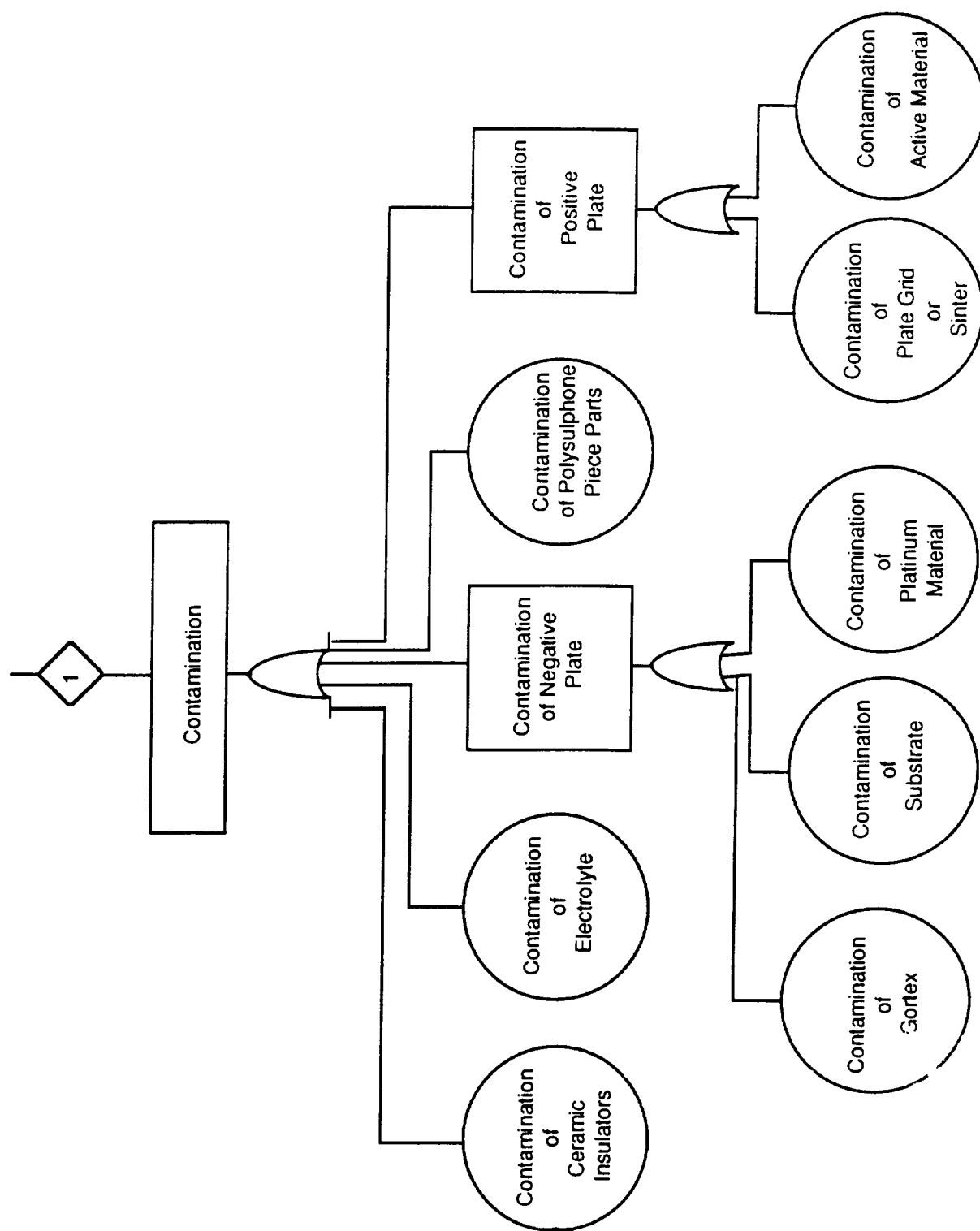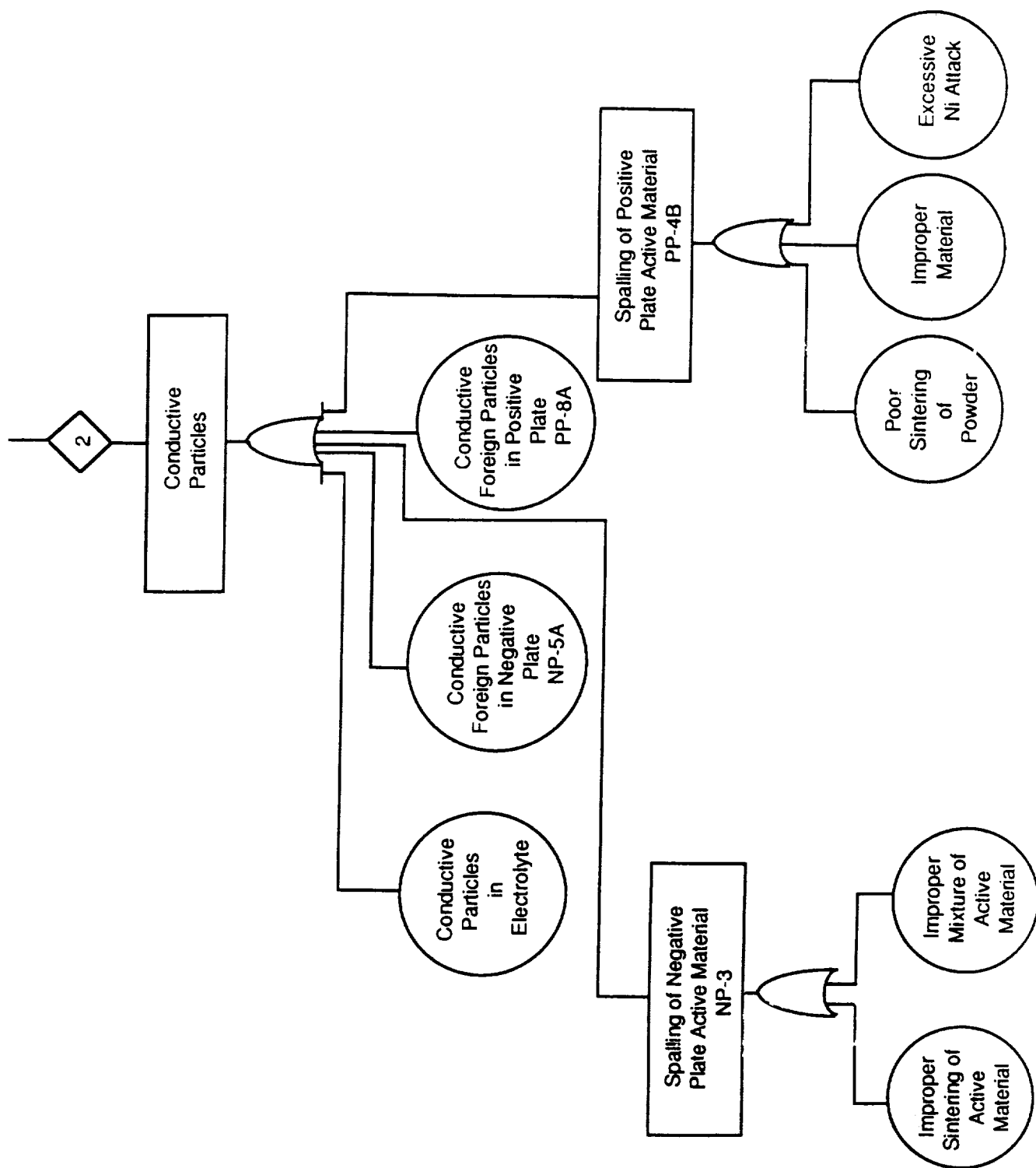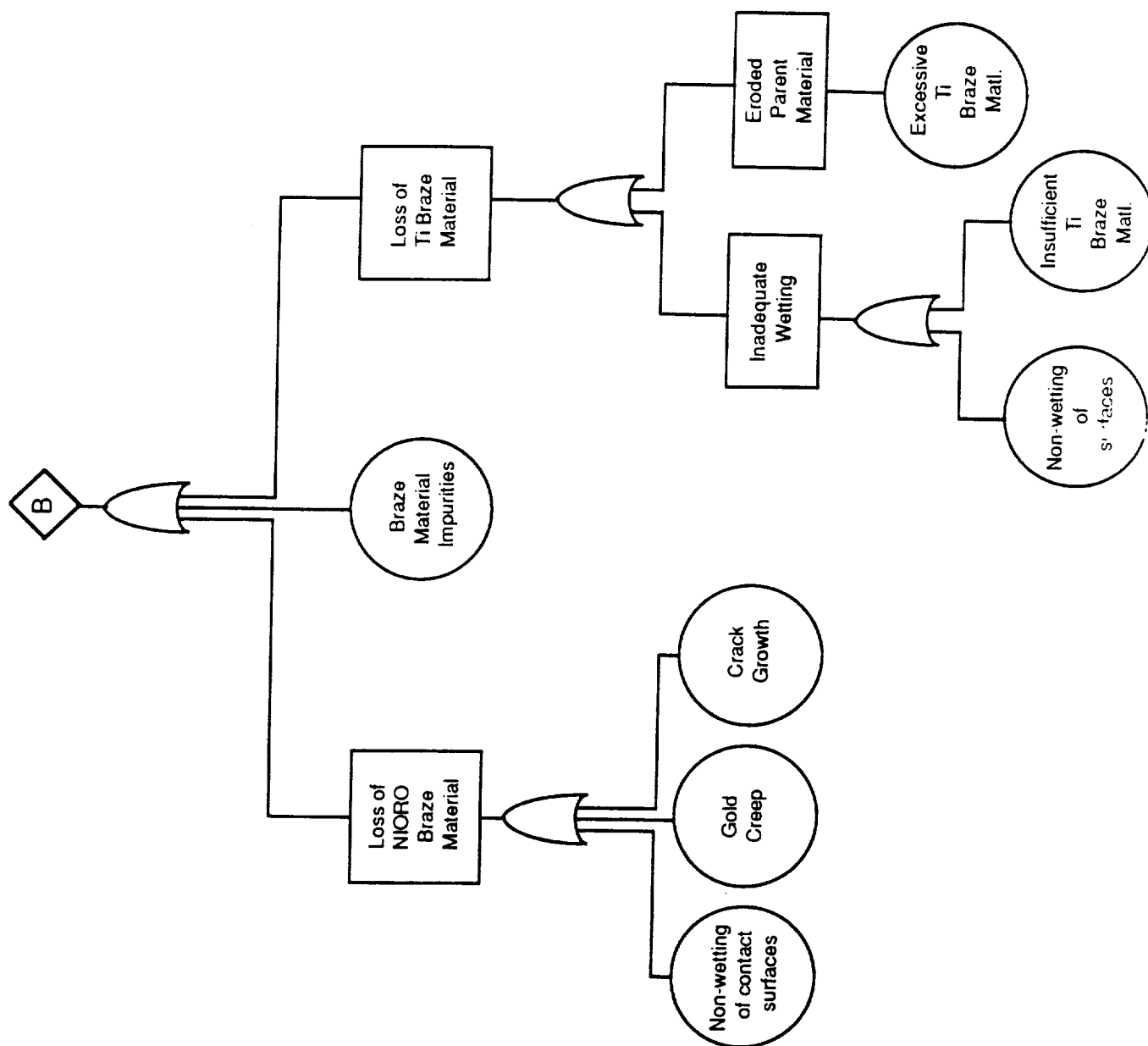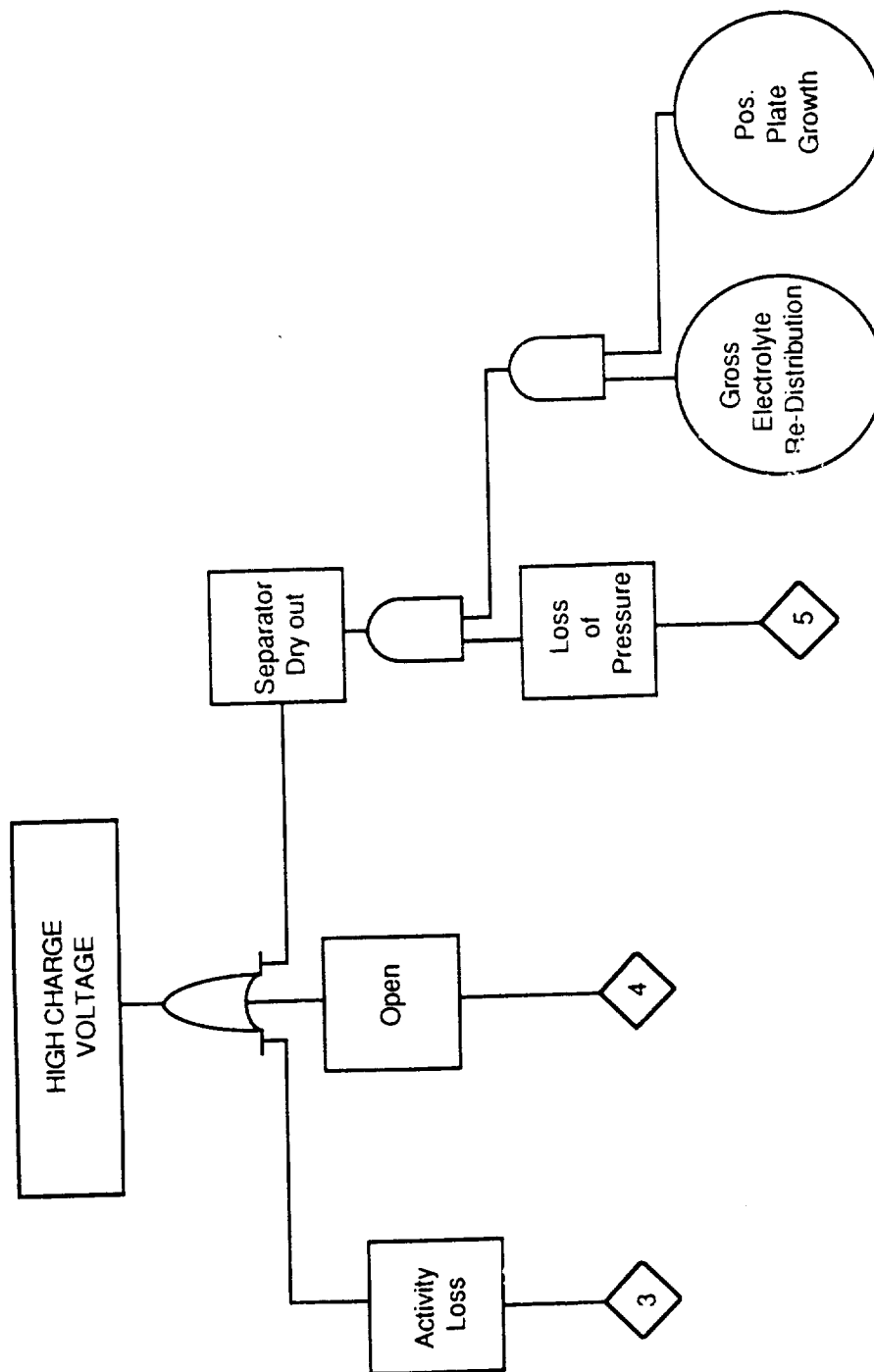
FIGURE 4

FIGURE 5
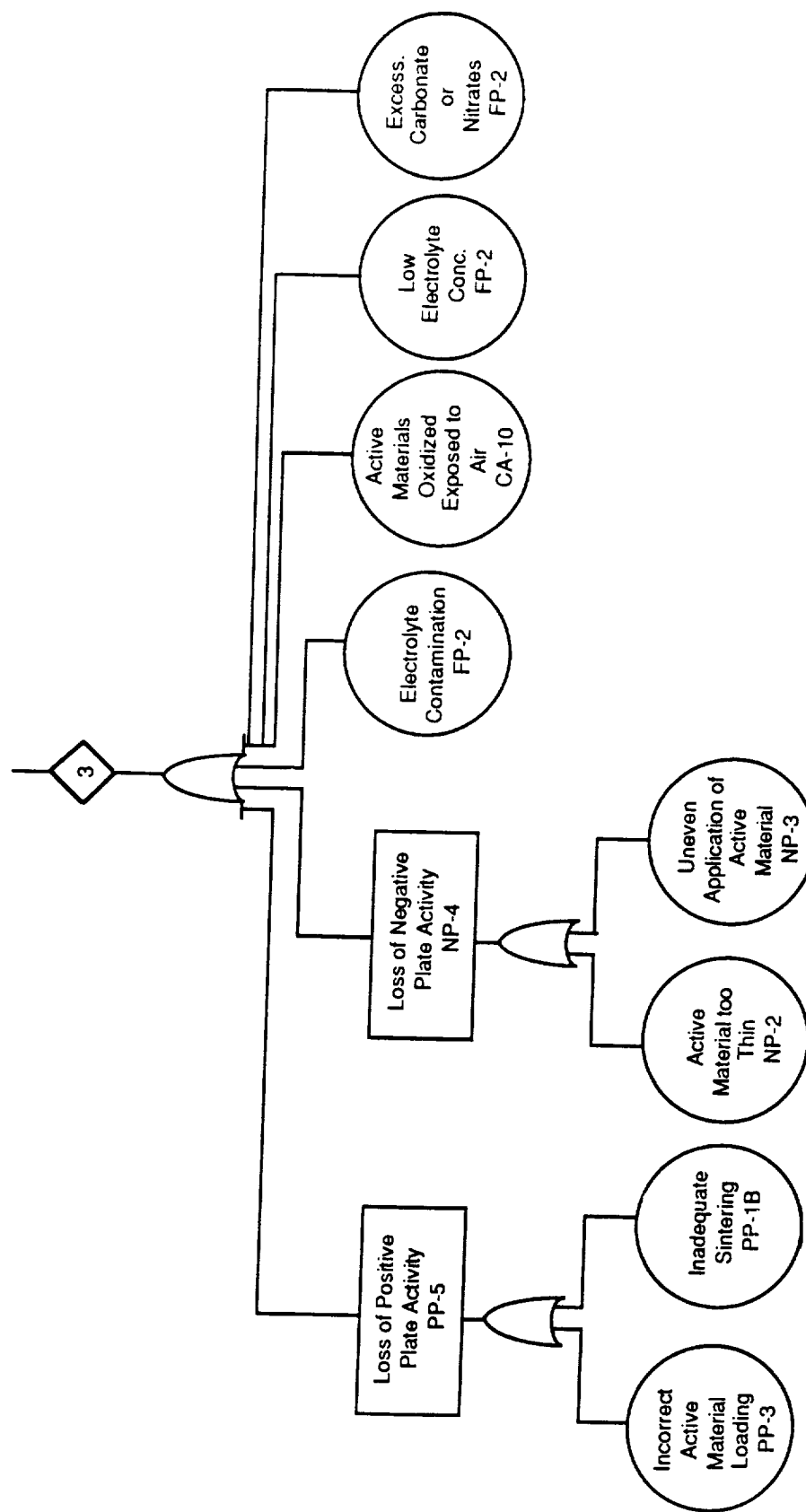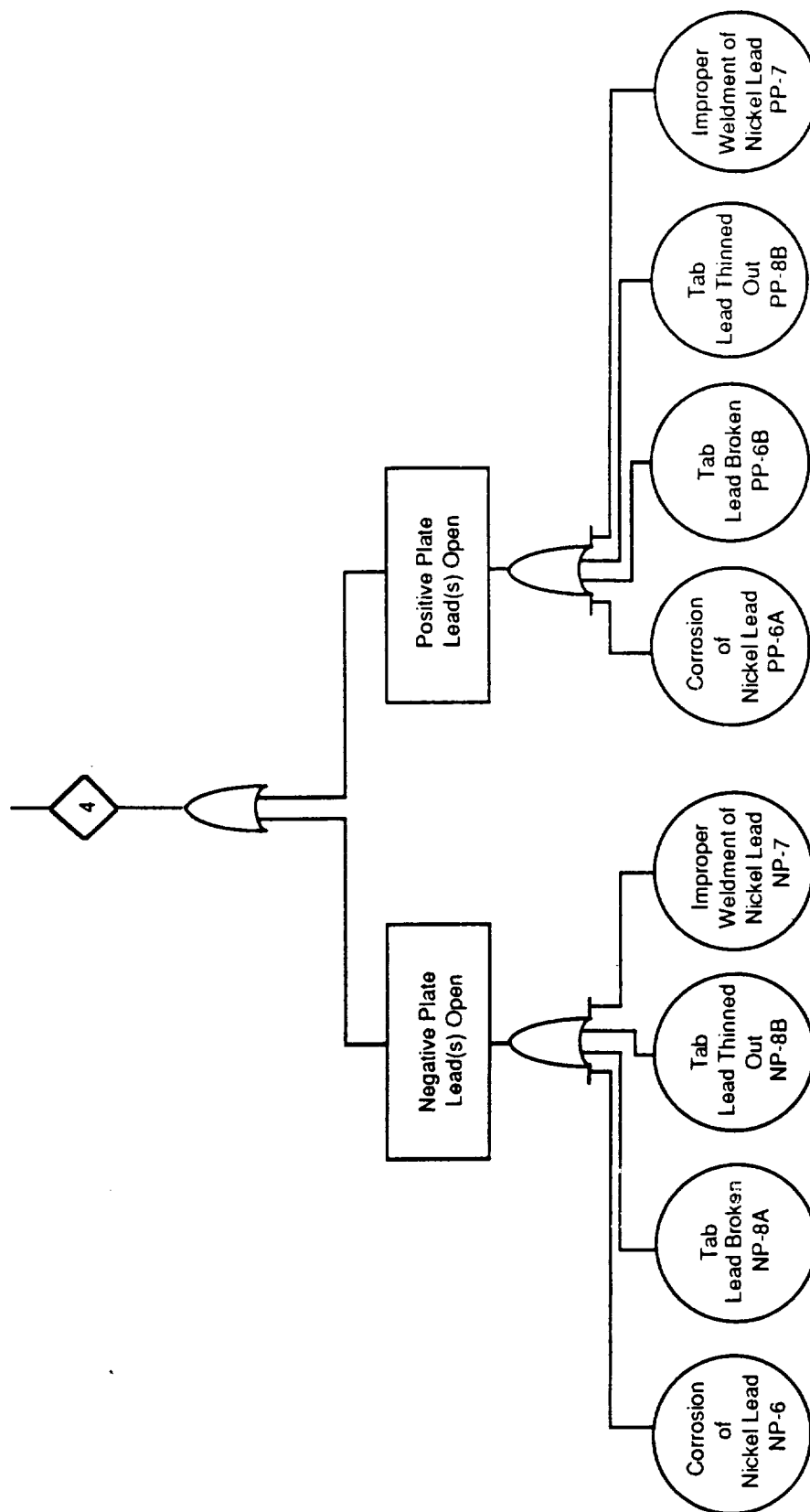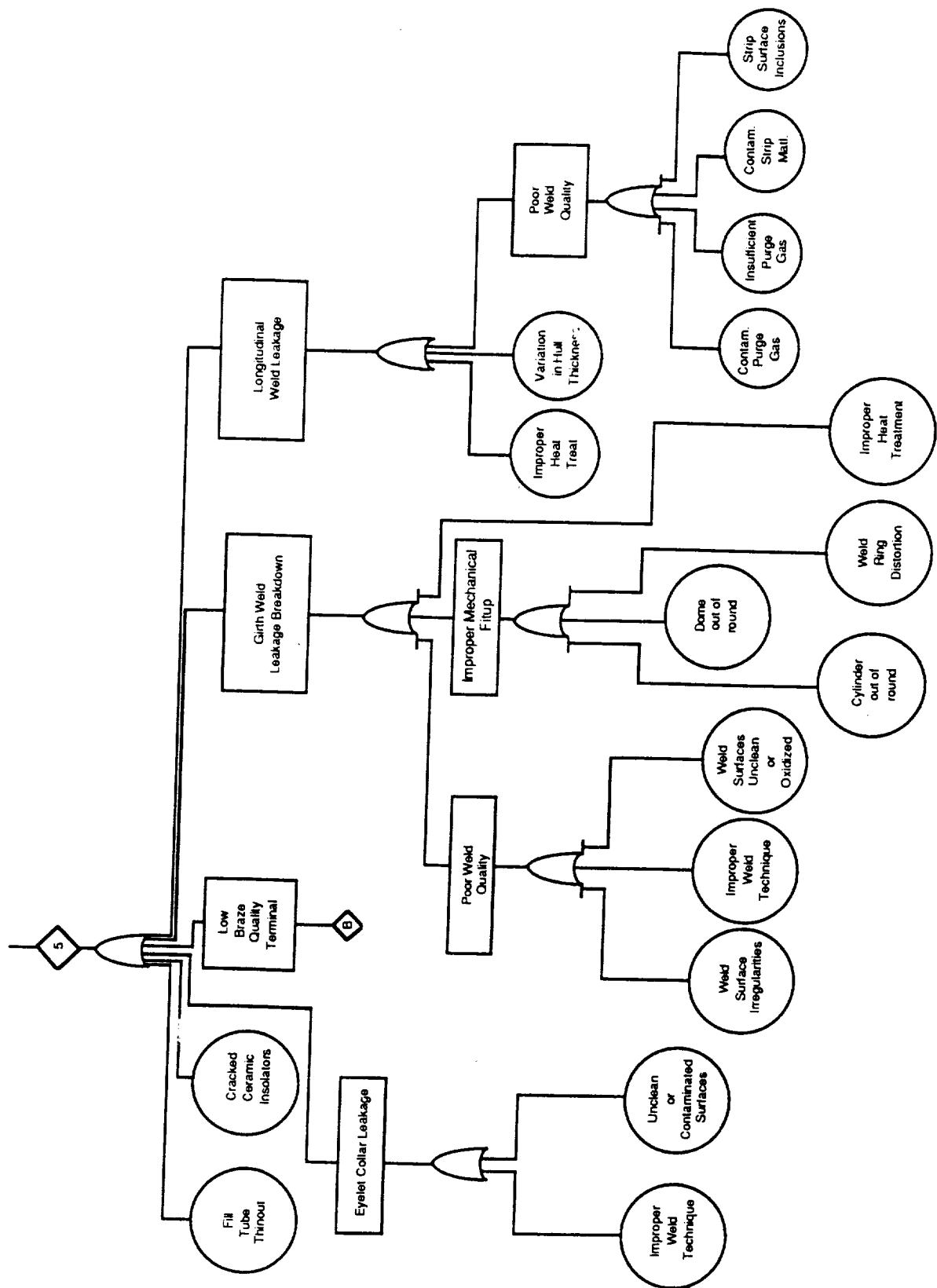
FIGURE 6

FIGURE 7
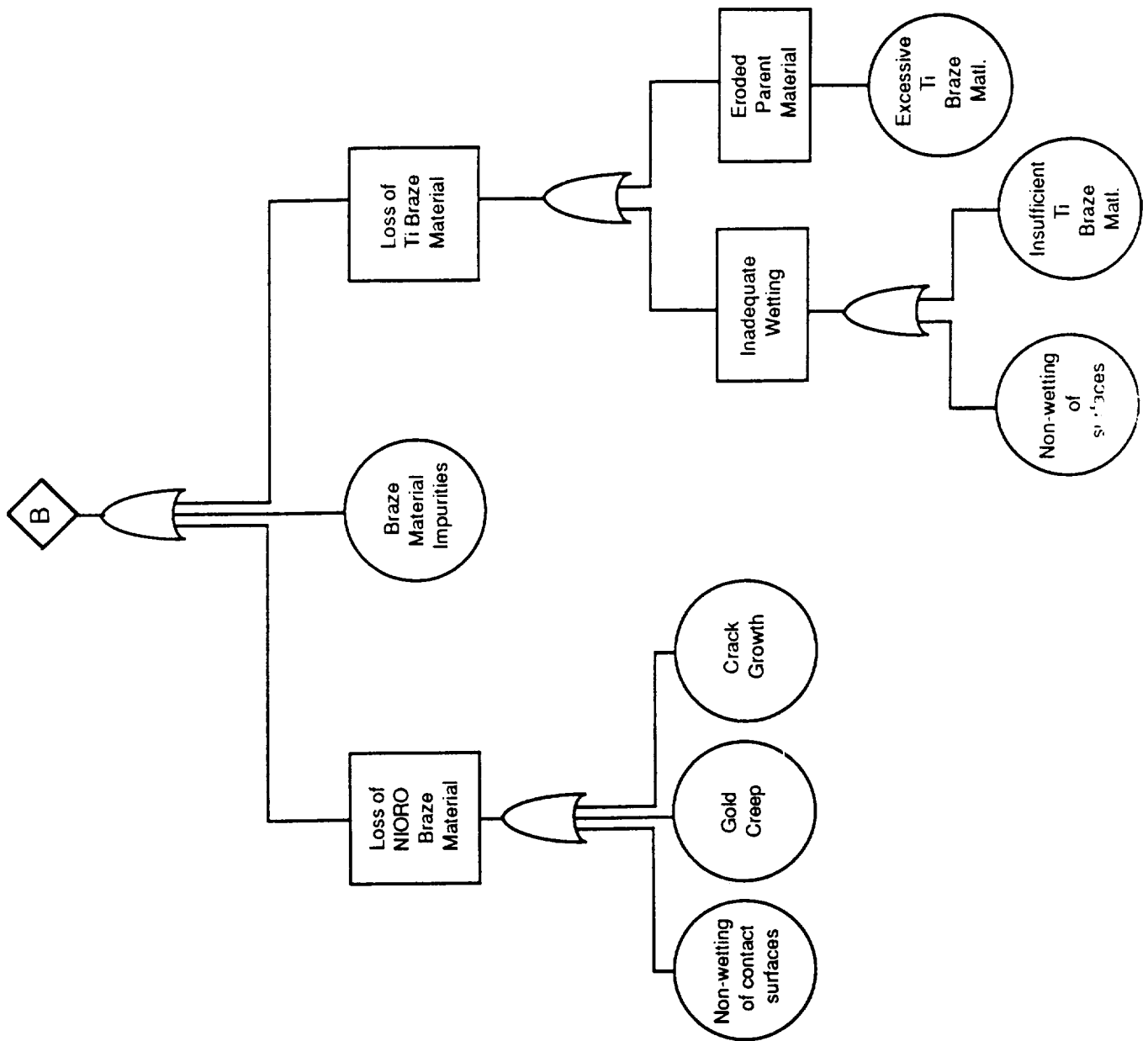
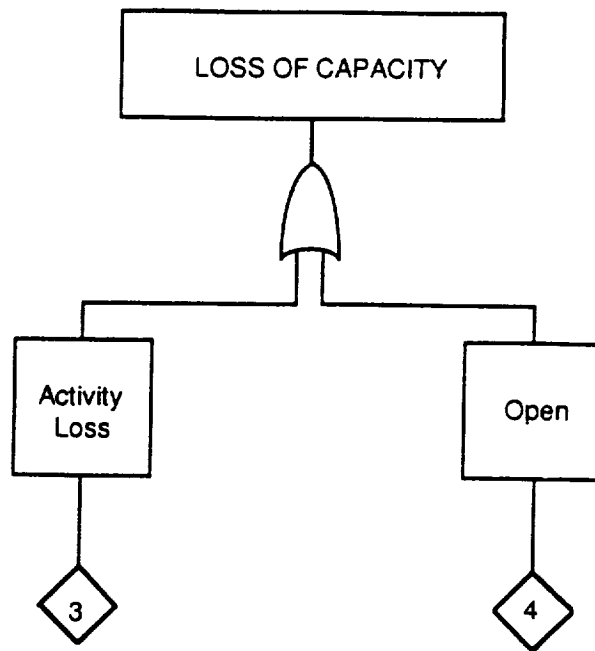FIGURE 8

FIGURE 9

FIGURE 10

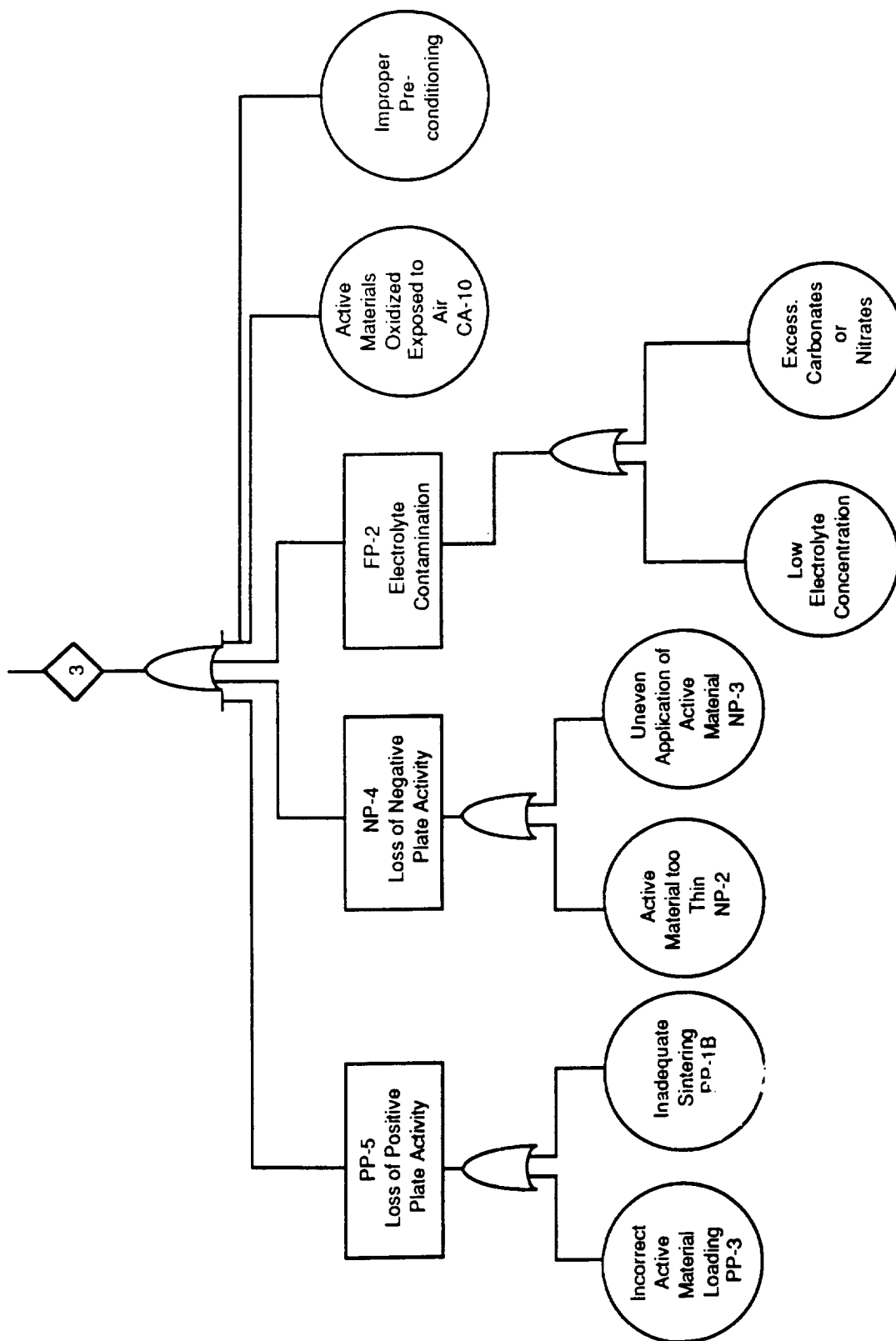FIGURE 11

FIGURE 12

FIGURE 13
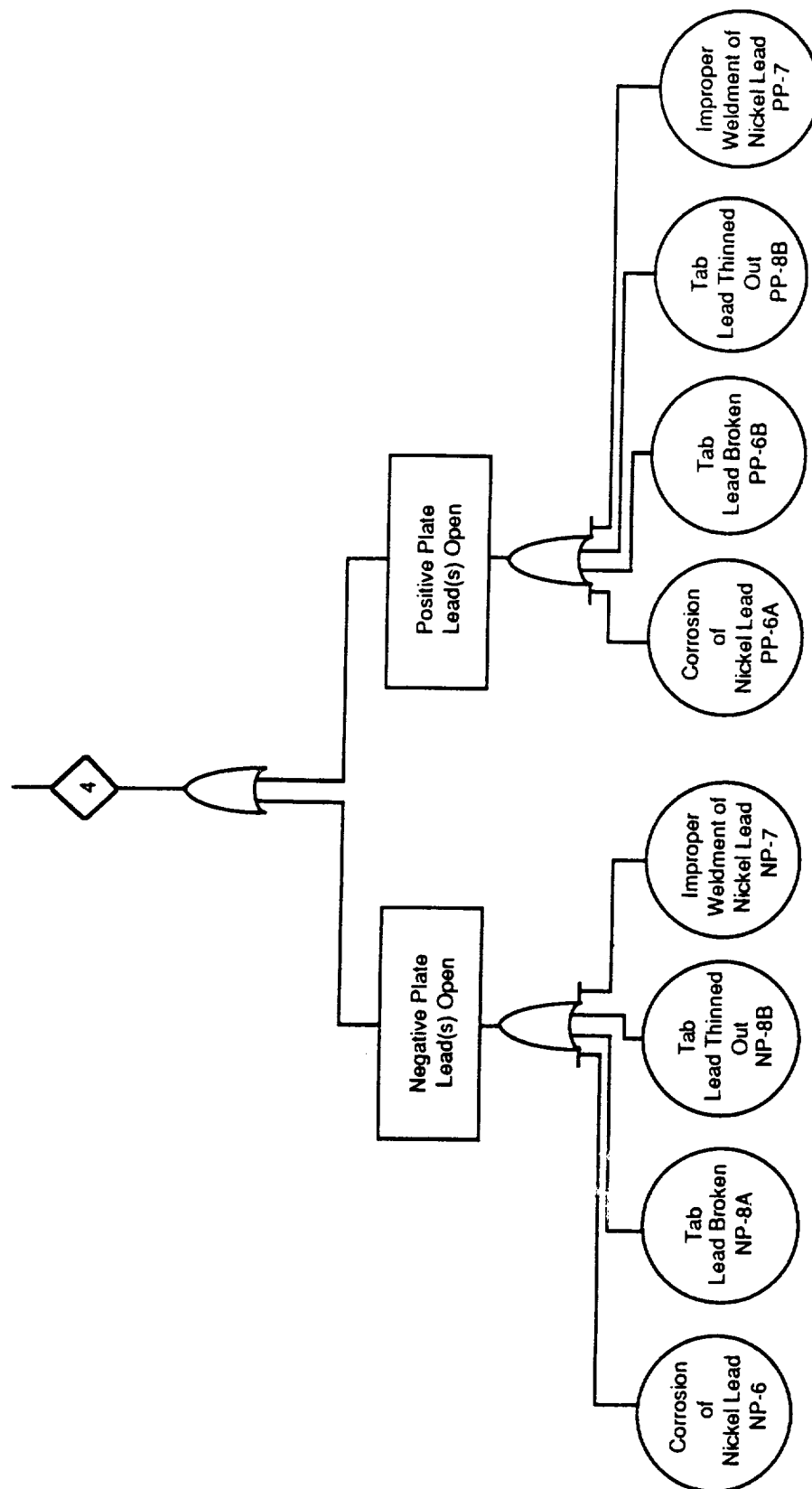
FIGURE 14

FIGURE 15

FIGURE 16
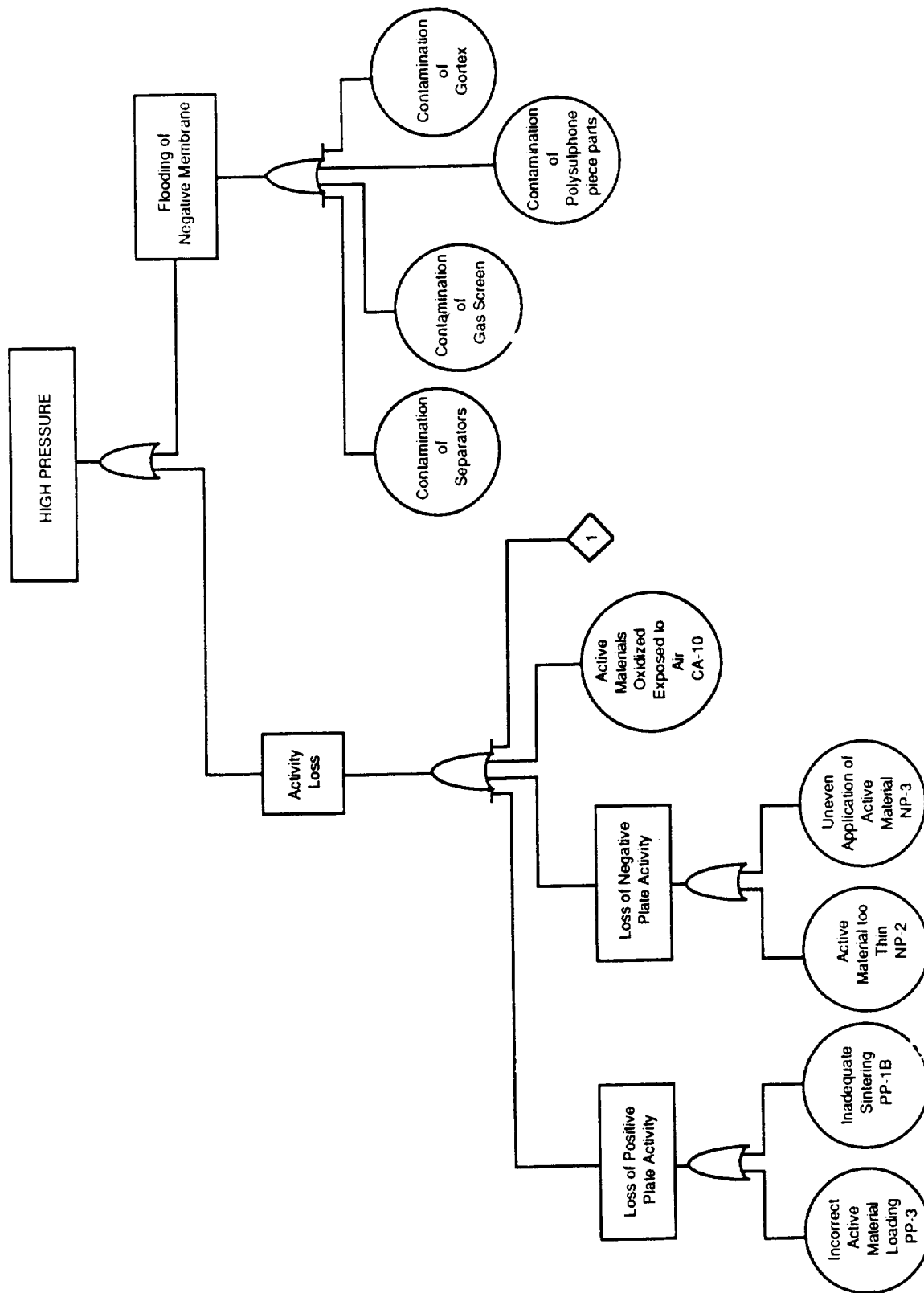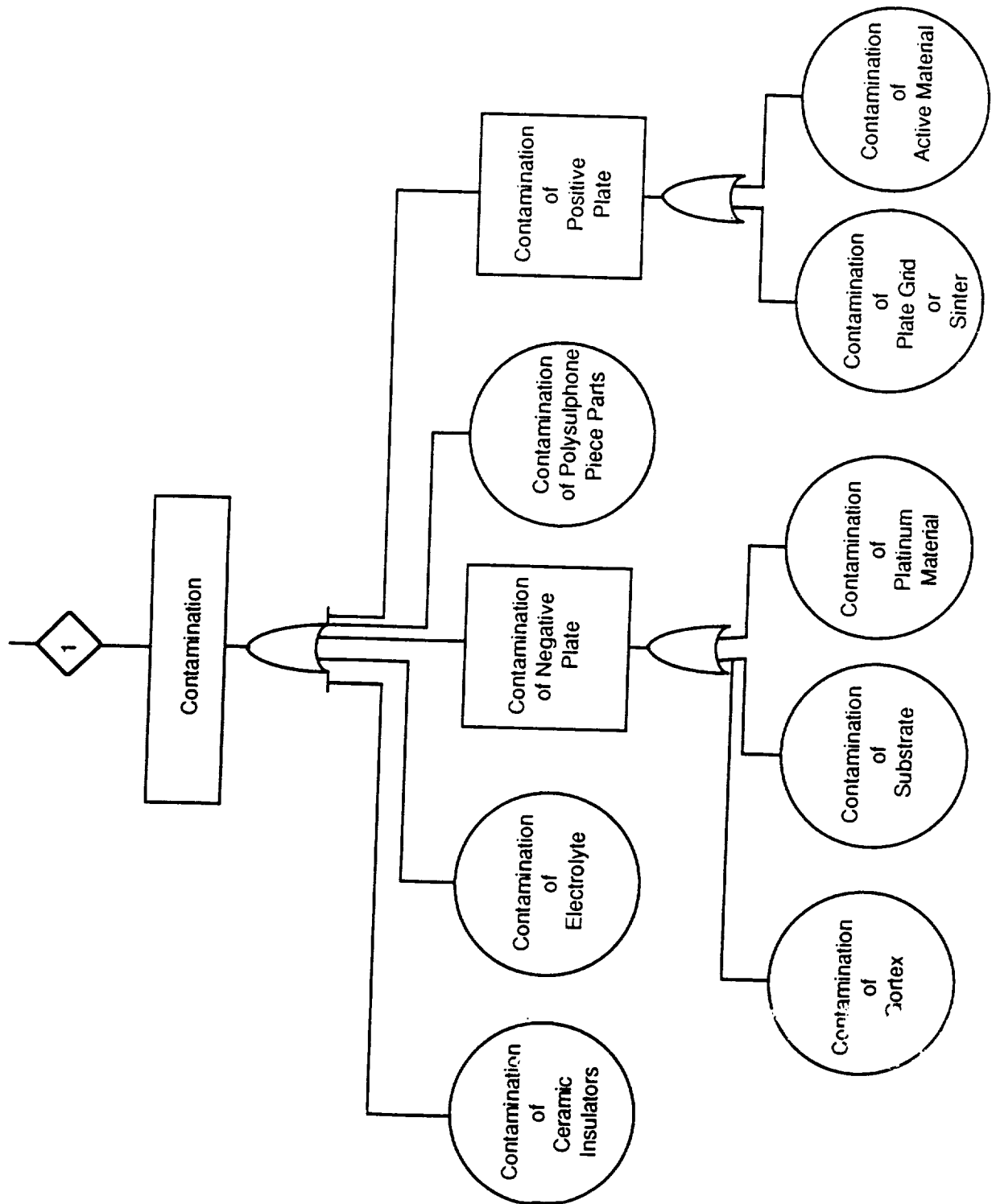
FIGURE 17

FIGURE 18

FIGURE 19
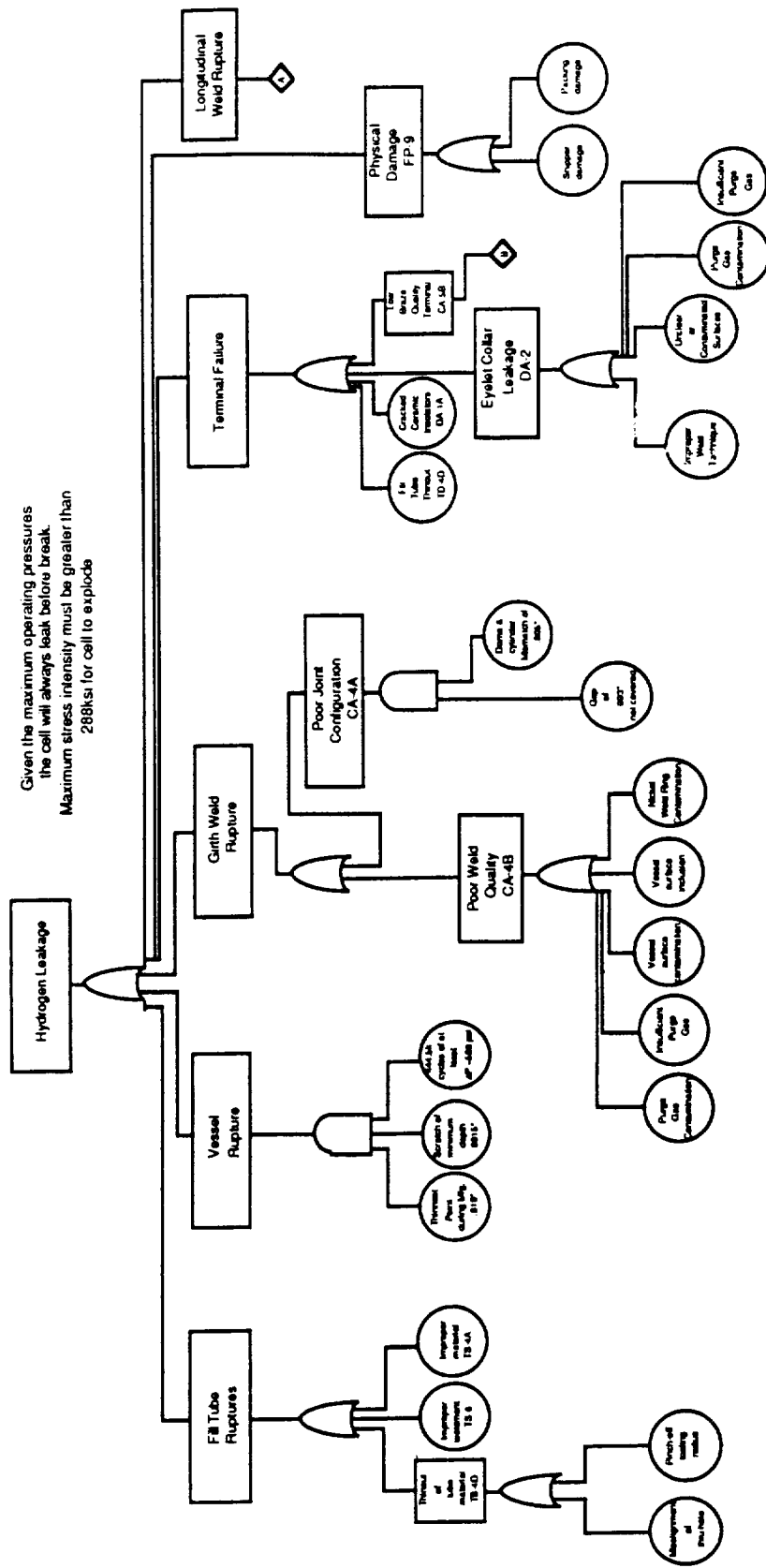
FIGURE 20

FIGURE 21

FIGURE 22

Failure Modes and Effects Analysis
on Gates NiH$_2$ Battery for LEO Mission

FMEA NO. CA-4B
Critical Item (Yes/No)   Yes
Item Name: Girth weld
Part Number: 149C1930AJ1
Quantity: 1
Hardware Location: (Internal)
System: NiH2 Battery
Subsystem: Cell assembly
Reference Designator: _____
Hardware (Including Redundancy)
  Operating Verification:
(A) Checkout
      (1) Prelaunch   PASS
      (2) On Orbit   FAIL
(B) Detectability   PASS
(Appropriate Mission Phases)

Document Number: RAC NiH2 Battery FMEA
Document/Revision Date: 14 June 1991
Critical Category: 1
Failure Effect Phase
X___(A)   Prelaunch
X___(B)   Transportation
X___(C)   Assembly
X___(D)   Permanently Manned Capability (PMC)
Is Function Restorable on Orbit? Battery Cell Only
ORU Level: TBD
Part Name: _____
Part Number: _____
ORU Failure Detectability: Yes   TBD

EVA Required (Yes/No):   TDB

Reliability Analysis Center		Gates Battery	
Prepared By:	D. Rash	Approved By:	_____
Approved By:	G. Ebel	Approved By:	_____

Function: Girth weld
Failure Mode: Poor weld quality (cracks, inclusions, low strength, porous)

Failure Cause(s):   Improper material choices, Improper weld techniques; Irregularities in weld surfaces; Weld surfaces contaminated; Weld gas contaminated; Inadequate purge gas flow

Failure Detection/Verification: Physical, visual, pressure and leakage tests
Correction Action: (A) Short Term: Article inspection
                      (B) Long Term: Control welding process

Time to Effect: Days

Failure Effect On: (A) Crew/TBD
                      (B) Mission Support _____
                      (C) System Loss of capacity
                      (D) Interfaces _____

Rational for Acceptability: (A) Design Safety factor of 3 for burst/operationg pressure & safety
(Note: Rational for   factor of 4 for burst/operating cycles
Acceptability is applicable   (B) Test Hydrogen leak, chemical leak, cycle, burst and proof tests
to CIL Items only)   (C) Inspection First article and first piece
                              (D) Failure History _____
                              (E) Operations _____
                              (F) Maintainability   N/A

Remarks/Hazards: HAZARD POTENTIAL - Leakage of Hydrogen

FIGURE 23

Establishing Parity with the FMECA

An example of a completed failure mode effects analysis worksheet (Figure 23) is provided to demonstrate how the failure causes are attributed to fault events, in this case Girth Weld Breakdown. The numbering system has been assigned to manufacturing flow steps and the example is FMEA number CA-4B. The failure mode corresponds directly to an event that has three distinct events associated to the upper level event.

Conclusion

The decision process for either qualitative or quantitative analyses is tempered by our view of reality and some model of our system under anlaysis; and, further constrained by our expectations of the external boundaries and robustness of the design. The Fault Tree Analysis is not a stand alone technique due to the top down approach which presupposes the determination of all Top-level or Major fault events; however, the Fault Tree when in a graphic, visual format is an excellent tool for technical reviews. Fault Tree Analyses can be quantified in areas such as System Assessment, Confidence Analysis, and Sensitivity Analysis. The Qualitative Fault Tree Analysis for NiH_2 cells in LEO Mission identifies and analyzes five specific Top-Level failure events; quantification of this Fault Tree has already begun.

References

1) Fault Tree Handbook, NUREG-0492, U.S. Nuclear Regulator Commission, Washington, DC, (1981)

2) Fault Tree Analysis Application Guide, Reliability Analysis Center, Rome, NY, (1990).