Bendix
Aerospace
Systems Division

COMPARATIVE SAFETY ANALYSIS

LSP TIMERS

NO. ATM 1104
REV. NO.

PAGE 1 OF 11

DATE 16 June 1972

Submitted by: W. J. Lavin
W. J. Lavin
System Safety Engineer

Approved by:
W. Tosh, Supervisor
ALSEP Mission Support

B. J. Rusky, Manager
ALSEP System Support

1.0 INTRODUCTION

An analysis has been performed on the LSP direct drive timers to determine if the inherent safety of the experiment has been compromised by the recent changes in the safe arm slide timer and battery timer designs. The analysis shows the new timers do not, in fact, compromise the safety of the experiment but have actually increased it. All of the safety features in the rachet release design are still present in the direct drive design and several failure modes that cause safety degradation have been eliminated.

The analysis performed was a comparative analysis of the old (rachet release) design against the new (direct drive) design for both safe arm timer and battery timer. The analysis was strictly qualitative in nature but the results were significant. A system safety fault tree logic diagram (see Attachment A) was generated for each design. Consideration was given to all identifiable failure modes; however, only those modes which cause safety related events became a part of the fault tree. Other failure modes do not contribute to a safety significant event. The failure mode information for the rachet release design was derived from ATM 976, Failure Mode, Effects and Criticality Analysis, LSPE, ALSEP Array E. The information on the direct drive design was derived from the timer PDR held at BxA on 17 May.

The top event used for developing the safe arm timer fault tree was "Explosive Package Arms Prematurely". The top event used for the battery timer fault tree was "Firing Pin strikes thermal battery prematurely". The trees were developed down to events that could not be further developed (primary events) except for those events related to the hack watch movement. Since the hack watch is identical in each timer design its fault tree was not developed for the purpose of this analysis.

The developed trees are attached to this report. Figure 1 and Figure 2 are the fault tree logic diagrams for the old and new design of the safe arm timer. Figures 3 and 4 are the fault tree logic diagrams for old and new design of the battery timer.

2.0 SAFE ARM TIMER COMPARISON

A study of the two fault tree logic diagrams shows that the complexity of the design is reflected in the fault tree. The fault tree logic diagram for the direct drive timer is considerably simpler than the rachet release fault tree logic diagram. Each design contains two sequential AND gates, showing that each design has two safety constraints. In fact, the safety constraints are identical in both designs. They are as follows: 1) Each timer has a pull pin that must be removed to cause activation. Should the timer start previous to this action, the timer will hang up and prevent pull pin removal. 2) Although not part of the timer design, the safe arm slide pull pin, pull pin No. 2 also acts as a timer safety device. Should the timer release the arm pin, the safe arm slide will be constrained by the safety pin. The design is such that the pin cannot be removed under that condition.

Analysis of the rachet release fault tree reveals that there are eight (8) failure modes (X01-X08) which can decrease the safety of the timer; in the direct drive design there are only three (3) failure modes (X01-X03) which can decrease safety. These three (3) failure modes are identical to three of the eight identified for the rachet release design. It can be concluded that the direct drive design is superior from a safety viewpoint due to the decreased number of failure modes that become a part of the fault tree diagram.

3.0 BATTERY TIMER COMPARISON

A study of the rachet release battery timer reveals that there are two (2) sequential AND gates which correspond to the two safety devices in the design of the timer. Each device is a pull pin. The first pin restricts drum movement and timer operation. If the timer starts previous to removal of the pin, the timer drum will hang up on the pin, stopping the timer and preventing pin removal. The second pin is the firing pin safety pin. Should time-out occur prior to safety pin removal, the firing pin will hang up on the safety pin, preventing thermal battery activation and safety pin removal. There are eight (8) identified failure modes (X01-X08) that can reduce the safety of the timer although none of the failure modes by themselves will cause timer activation.

In the direct drive design there are three (3) safety features as shown by the three (3) sequential AND gates. Two of the features are identical to the safety features in the rachet release design. The third feature is the new firing pin and drum arrangement. The firing pin and drum are so designed that when the firing pin is released, it must pass through a notch in the timing drum. This notch is aligned with the firing pin only during the time out period. Premature release of the firing pin would result in the pin hanging up on the drum and stopping the timer. There are only four failure modes (X01-X04) in the direct drive design that can contribute to the construction of the fault tree as compared to eight for the rachet release design.

The direct drive design is significantly safer than the rachet release design. This is due to the reduction of safety significant failure modes and the addition of a safety feature.

4.0 CONCLUSION

It is readily apparent from a qualitative comparison of the fault tree logic diagram that, from a safety standpoint, the direct drive design is superior to the ratchet release design although both designs provide the degree of safety necessary for the experiment. No failure modes identified in either the old or new designs would, by themselves, cause premature functioning of the timer and premature activation of either or both timers would not cause detonation of the package.

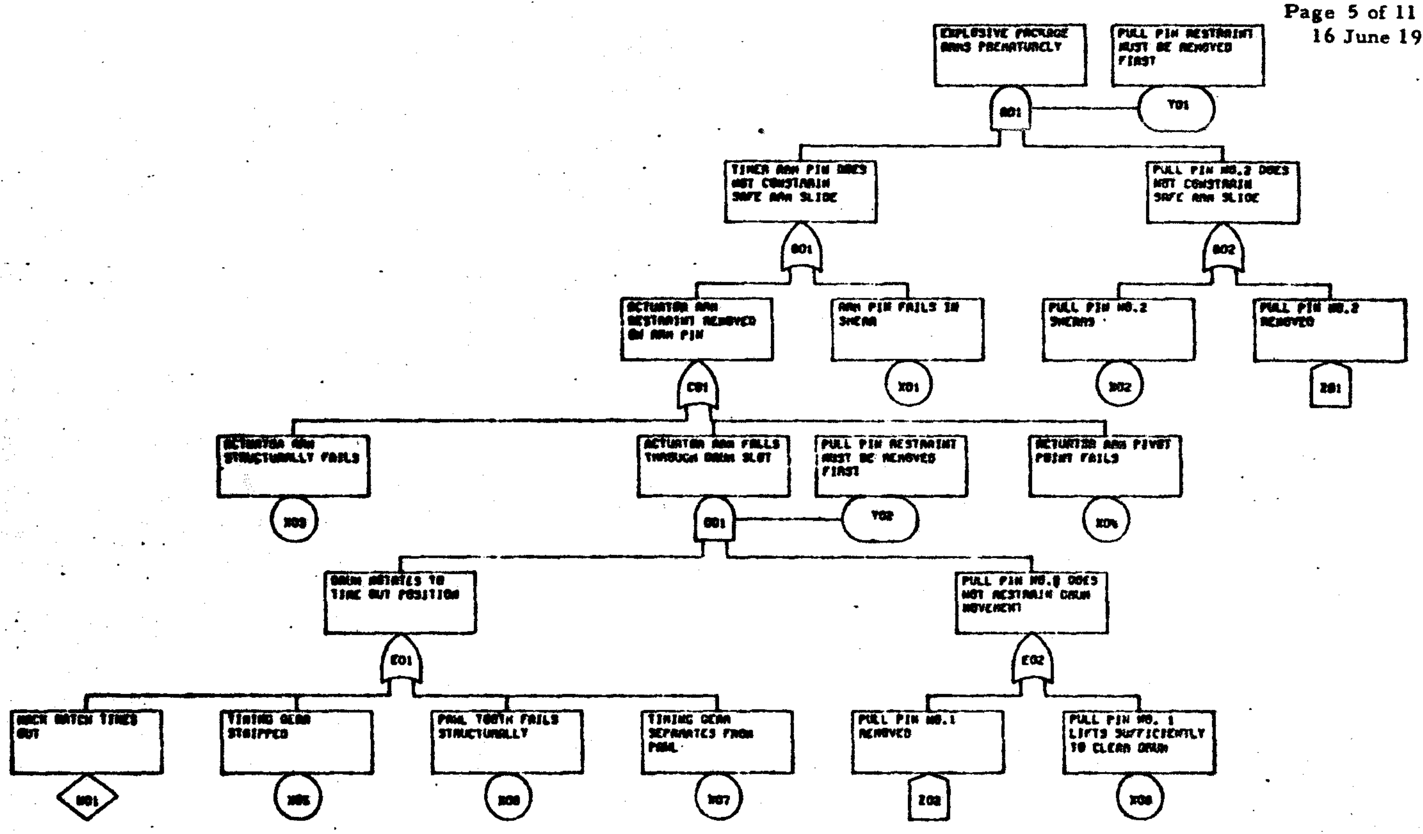

EXPLOSIVE PACKAGE ARMS PREMATURELY
PULL PIN RESTRAINT MUST BE REMOVED FIRST
A01
Y01
TIMER ARM PIN DOES NOT CONSTRAIN SAFE ARM SLIDE
PULL PIN NO.2 DOES NOT CONSTRAIN SAFE ARM SLIDE
B01
B02
ACTUATOR ARM RESTRAINT REMOVED BY ARM PIN
ARM PIN FAILS IN SHEAR
PULL PIN NO.2 SHEARS
PULL PIN NO.2 REMOVED
C01
X01
X02
Z01
ACTUATOR ARM STRUCTURALLY FAILS
ACTUATOR ARM FALLS THROUGH DRUM SLOT
PULL PIN RESTRAINT MUST BE REMOVED FIRST
ACTUATOR ARM PIVOT POINT FAILS
X03
D01
Y02
X04
DRUM ROTATES TO TIME OUT POSITION
PULL PIN NO.1 DOES NOT RESTRAIN DRUM MOVEMENT
E01
E02
MACH WATCH TIMES OUT
TIMING GEAR STRIPPED
PAWL TOOTH FAILS STRUCTURALLY
TIMING GEAR SEPARATES FROM PAWL
PULL PIN NO.1 REMOVED
PULL PIN NO. 1 LIFTS SUFFICIENTLY TO CLEAR DRUM
W01
X05
X06
X07
Z02
X08

FIGURE 1

TITLE: FAULT TREE DIAGRAM-LSP-RATCHET RELEASE SAFE-ARM TIMER	DATE 05-10-72
FOR: COMPARATIVE SAFETY ANALYSIS, LSP TIMERS	NUMBER ALS001

BENDIX AEROSPACE SYSTEMS DIVISION

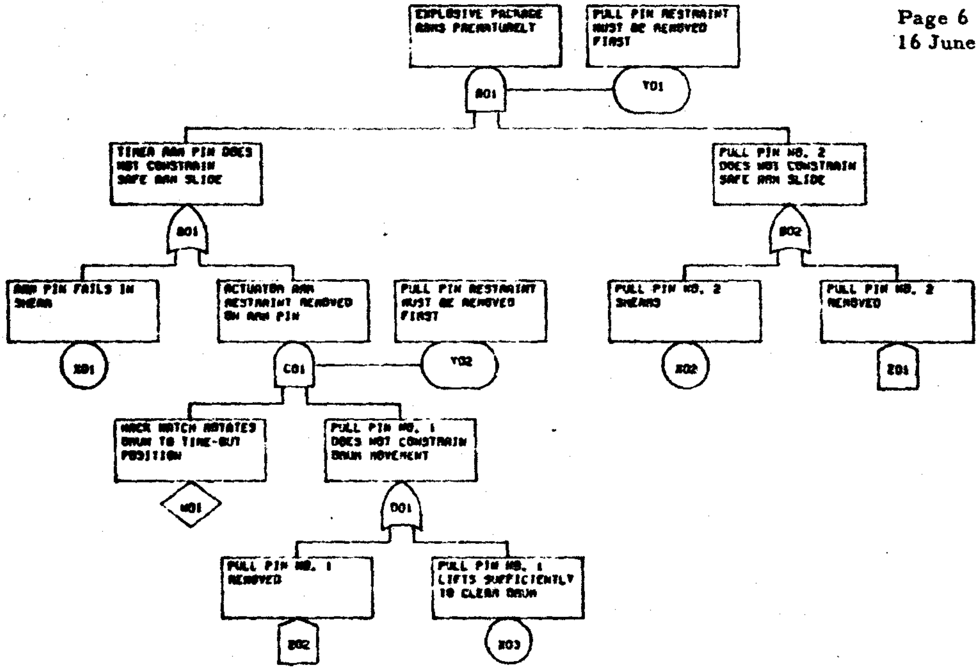

EXPLOSIVE PACKAGE ARMS PREMATURELY
PULL PIN RESTRAINT MUST BE REMOVED FIRST
A01
Y01
TIMER ARM PIN DOES NOT CONSTRAIN SAFE ARM SLIDE
PULL PIN NO. 2 DOES NOT CONSTRAIN SAFE ARM SLIDE
B01
B02
ARM PIN FAILS IN SHEAR
ACTUATOR ARM RESTRAINT REMOVED ON ARM PIN
PULL PIN RESTRAINT MUST BE REMOVED FIRST
PULL PIN NO. 2 SHEARS
PULL PIN NO. 2 REMOVED
X01
C01
Y02
X02
Z01
HACK WATCH ROTATES DRUM TO TIME-OUT POSITION
PULL PIN NO. 1 DOES NOT CONSTRAIN DRUM MOVEMENT
W01
D01
PULL PIN NO. 1 REMOVED
PULL PIN NO. 1 LIFTS SUFFICIENTLY TO CLEAR DRUM
Z02
X03

FIGURE 2

TITLE: FAULT TREE DIAGRAM-LSP-DIRECT DRIVE SAFE-ARM TIMER	DATE 05-15-72
FOR: COMPARATIVE SAFETY ANALYSIS, LSP TIMERS	NUMBER AL5002

BENDIX AEROSPACE SYSTEMS DIVISION

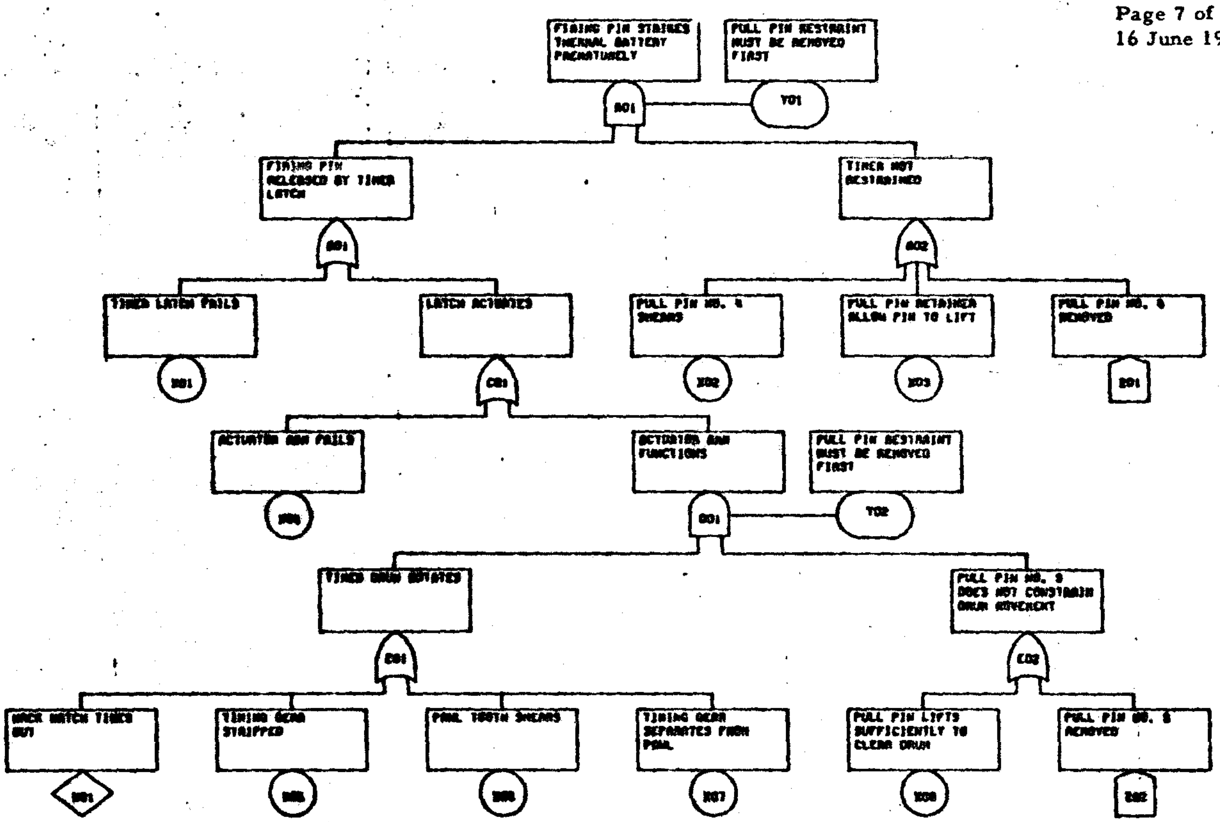

FIRING PIN STRIKES THERMAL BATTERY PREMATURELY
PULL PIN RESTRAINT MUST BE REMOVED FIRST
A01
Y01
FIRING PIN RELEASED BY TIMER LATCH
TIMER NOT RESTRAINED
B01
B02
TIMER LATCH FAILS
LATCH ACTUATES
PULL PIN NO. 4 SHEARS
PULL PIN RETAINER ALLOW PIN TO LIFT
PULL PIN NO. 6 REMOVED
X01
C01
X02
X03
Z01
ACTUATOR ARM FAILS
ACTUATOR ARM FUNCTIONS
PULL PIN RESTRAINT MUST BE REMOVED FIRST
X04
D01
Y02
TIMER DRUM ROTATES
PULL PIN NO. 3 DOES NOT CONSTRAIN DRUM MOVEMENT
E01
E02
HACK WATCH TIMES OUT
TIMING GEAR STRIPPED
PAWL TOOTH SHEARS
TIMING GEAR SEPARATES FROM PAWL
PULL PIN LIFTS SUFFICIENTLY TO CLEAR DRUM
PULL PIN NO. 6 REMOVED
W01
X05
X06
X07
X08
Z02

FIGURE 3

TITLE: FAULT TREE DIAGRAM-LSP-RACKET RELEASE BATTERY TIMER	DATE 05-15-72
FOR: COMPARATIVE SAFETY ANALYSIS, LSP TIMERS	NUMBER AL9003
BENDIX AEROSPACE SYSTEMS DIVISION	

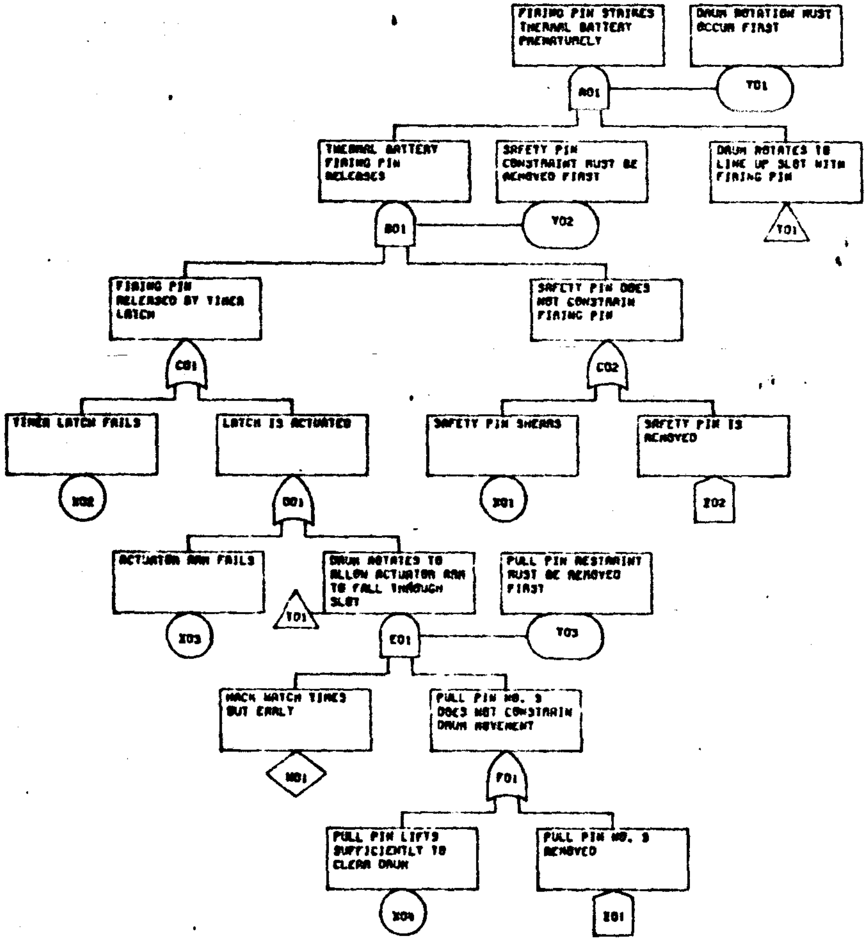

FIRING PIN STRIKES THERMAL BATTERY PREMATURELY
DRUM ROTATION MUST OCCUR FIRST
A01
Y01
THERMAL BATTERY FIRING PIN RELEASES
SAFETY PIN CONSTRAINT MUST BE REMOVED FIRST
DRUM ROTATES TO LINE UP SLOT WITH FIRING PIN
T01
B01
Y02
FIRING PIN RELEASED BY TIMER LATCH
SAFETY PIN DOES NOT CONSTRAIN FIRING PIN
C01
C02
TIMER LATCH FAILS
LATCH IS ACTUATED
SAFETY PIN SHEARS
SAFETY PIN IS REMOVED
X02
D01
X01
Z02
ACTUATOR ARM FAILS
DRUM ROTATES TO ALLOW ACTUATOR ARM TO FALL THROUGH SLOT
PULL PIN RESTRAINT MUST BE REMOVED FIRST
X03
T01
E01
Y03
HACK WATCH TIMES OUT EARLY
PULL PIN NO. 3 DOES NOT CONSTRAIN DRUM MOVEMENT
W01
F01
PULL PIN LIFTS SUFFICIENTLY TO CLEAR DRUM
PULL PIN NO. 3 REMOVED
X04
Z01

FIGURE 4

TITLE: FAULT TREE DIAGRAM-LSP-DIRECT DRIVE BATTERY TIMER	DATE 05-22-72
FOR: COMPARATIVE SAFETY ANALYSIS, LSP TIMERS	NUMBER AL5004
BENDIX AEROSPACE SYSTEMS DIVISION	

1.0 PHILOSOPHY

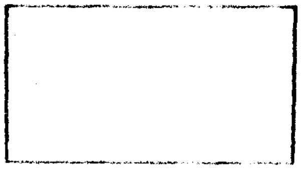
The Fault Tree Logic Diagram Analysis is a logical combination of functional fault events which can lead a path to a top undesired event or potential hazard. Each of the contributing fault events are further analyzed to determine the logical relationships of system faults which may cause them. In this manner, a diagram of logical relationships among fault events is developed to identify the basic faults which may cause the top undesired event.

2.0 LOGIC DEFINITIONS AND SYMBOLS

1) Events

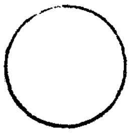
a. An "Event" is a system failure resulting from one or more contributing factors. These factors are due to either failures or malfunctions of an item of hardware, or of a subsystem.

b. The symbols used to represent the various events are:

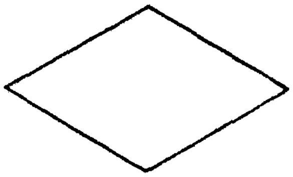


1. An event, (usually a fault or malcondition) resulting from multiple input events through a logic gate, expressed in functional terms.

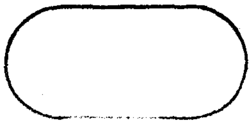
   It also represents a conditional input to an Inhibit Gate -- a condition that is assumed to exist for the life of the system. In this context, if an input event occurs, the condition is satisfied, and an output event is generated; if the condition is not satisfied, no output occurs.



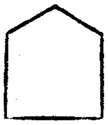
2. An "independent" event, arising from the failure of a basic hardware component; i. e., a basic fault event that requires no further development.



3. A fault event that is considered basic in a given logic diagram. The possible causes of the event are not developed either because the event is of insufficient consequence, or because the necessary information for further development is unavailable.



4. An event which describes a conditional input to any Gate. It defines the state of the system that permits or prevents occurrence of a fault. The condition may be either normal to the system, or may result from failures.



5. An event that is normally expected to occur, i.e., it does not represent a fault. An example is a phase change in a dynamic system, such as the takeoff, flight and landing phase of an aircraft flight.

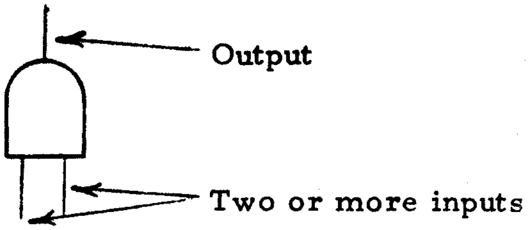
2) Gates

a. Gates are the decision elements of the logic diagram. Inputs to a gate always enter at the bottom; outputs always emanate from the top. In this manner, all event sequences move upward through the branches toward the top of the fault tree.

b. The symbols used to represent the various gates are:

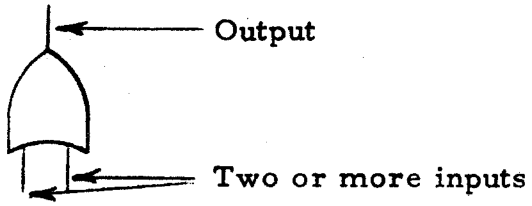
1. "AND" Gates

The "AND" gate is the logic function which requires the coexistence of all the input events in order to produce the output event.



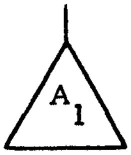
2. "OR" Gates

The "OR" gate is the logic function which requires the existence of only one of the input events to produce the output event.



3) Transfer Symbols

a. A sequence of events to be transferred is denoted as follows:



b. The location to which the sequence of events are transferred is denoted as follows: