EECE 499/693: Computers and Safety Critical Systems

5 Design Evaluation of Safety-Critical Computer Systems

A. Fault Tree Analysis

Instructor: Dr. Charles Kim

Electrical and Computer Engineering
Howard University

www.mwftr.com/CS2.html

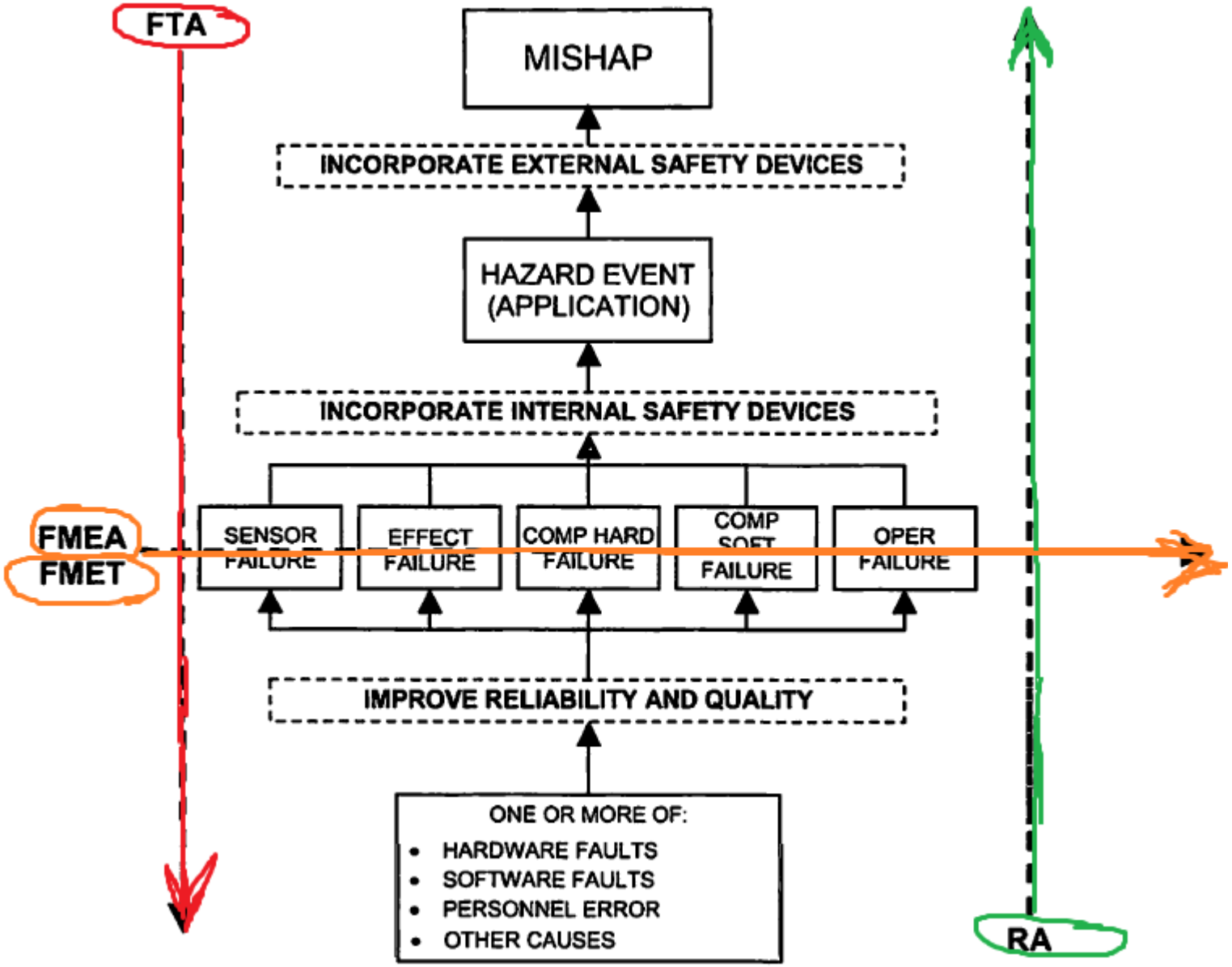
Overview

- Chap 2 – Basic Computer System --- meeting normal functional requirements (without safety features for handling component failures)
- Chap 3 – Component failure and hazards
- Chap 4 – Mitigation measures applied to the basic system to detect faults and failures and to bring the system to a **safe state**
- **Question**: Can they [mitigation measures] be expected to reduce mishap risk to an acceptable level?
- Mishap risk acceptance
  - Estimation of risk
  - Validation of the risk estimates by simulations and field experiences
  - Accurate risk estimates and risk acceptance cannot usually be achieved during the design phase of the system development
  - **Question:** Are there any Coarse analyses and tests that can be performed during the design phase? And, based on the analyses, apply risk mitigation measures?
- Chap 5:Design evaluation methods

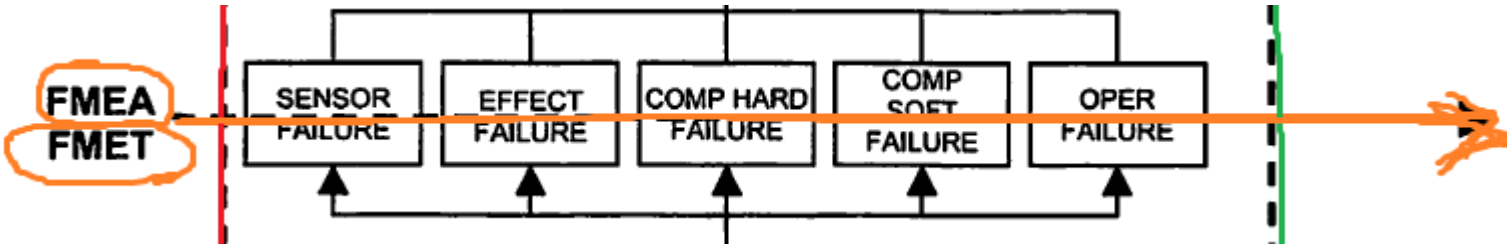
Design Evaluation

- 4 Evaluation methods
  - Failure modes and effects analysis (FMEA)
  - **Fault tree analysis (FTA)**
  - **Risk Analysis (RA)**
  - Failure modes and effects testing (FMET)
- Chapter 5 Organization
  - Design evaluation in 3 separate categories
    - Qualitative analysis (focused on FMEA and **FTA**)
    - Risk analysis – Part B
    - Failure modes testing

Design Evaluation - Overview



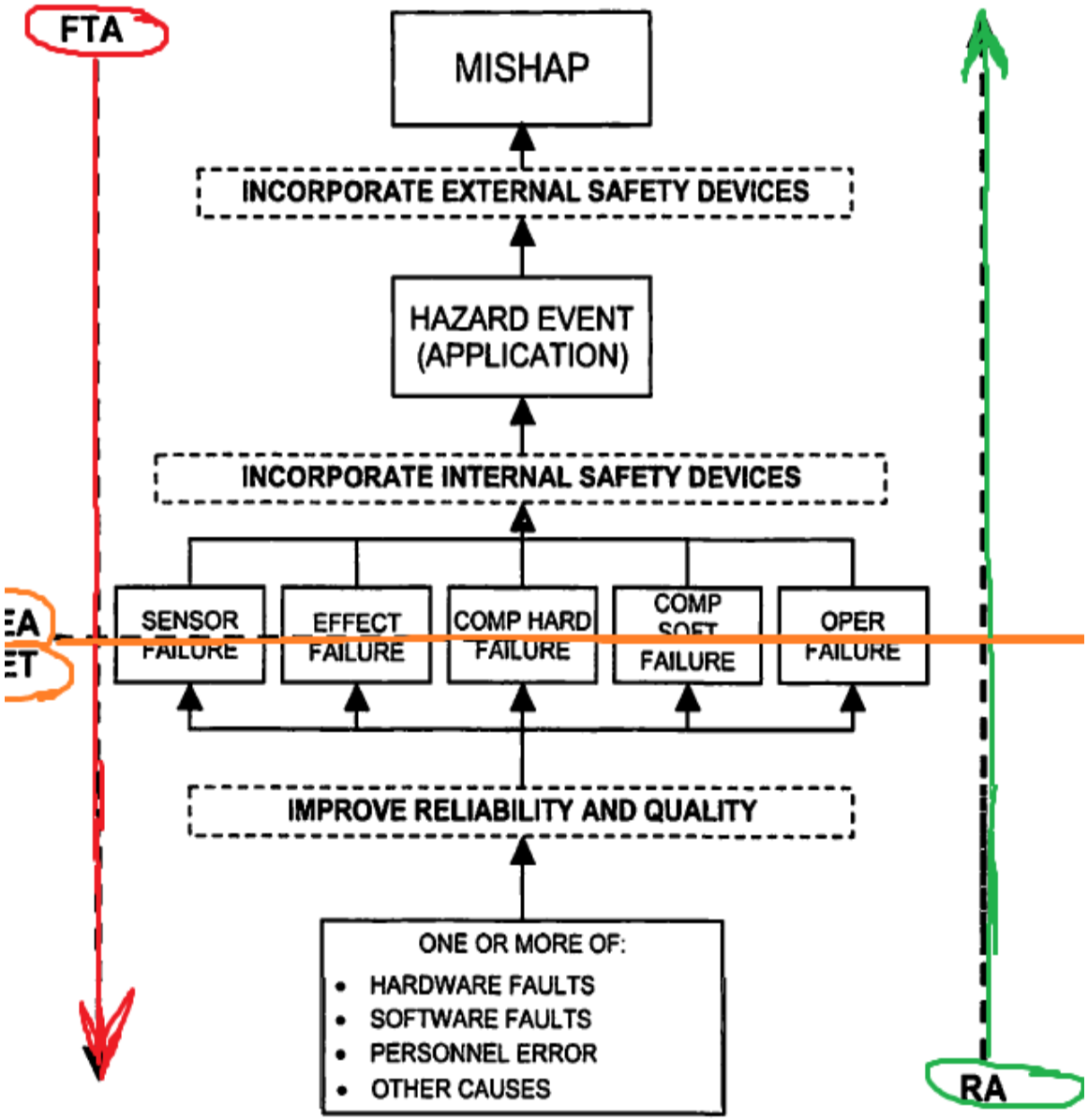
Design Evaluation: FMEA & FMET



- Failure modes and effects analysis (FMEA)
  - Across component in the system, considers the ways that the component can fail
  - Determines the effect each failure has on the system
  - Help identify hazards associated with the basic system
  - Help verify that all failure modes leading to hazard events or mishaps are mitigated by the design modifications made to the basic system
- Failure modes and effects testing (FMET)
  - Follow the FMEA
  - Simulated or actual failure modes are injected into working system to verify if actual system mitigates all failure modes

Design Evaluation: FTA & RA

- Fault Tree Analysis (FTA)
  - Starting with an identified mishap or hazard event
  - Working downward to determine their causes
- Risk Analysis (RA)
  - Verify that the risk mitigation measures during the design will lead to a system with an acceptable level of mishap risk
  - Moving upward



Qualitative Analysis - FMEA

- "What happens if" basis
- FMEA is formulated on the "What happens if" line of thinking; provides an organized and systematic approach to identifying hazard events and verifying that no single component failure will lead to mishap

FAILURE MODES AND EFFECTS ANALYSIS (FMEA) WORKSHEET

SYSTEM: ①

SUBSYSTEM:

Page of

Prepared by: Date:

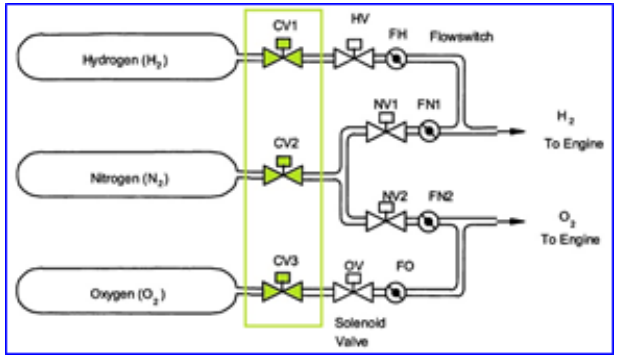
Checked by: Date:

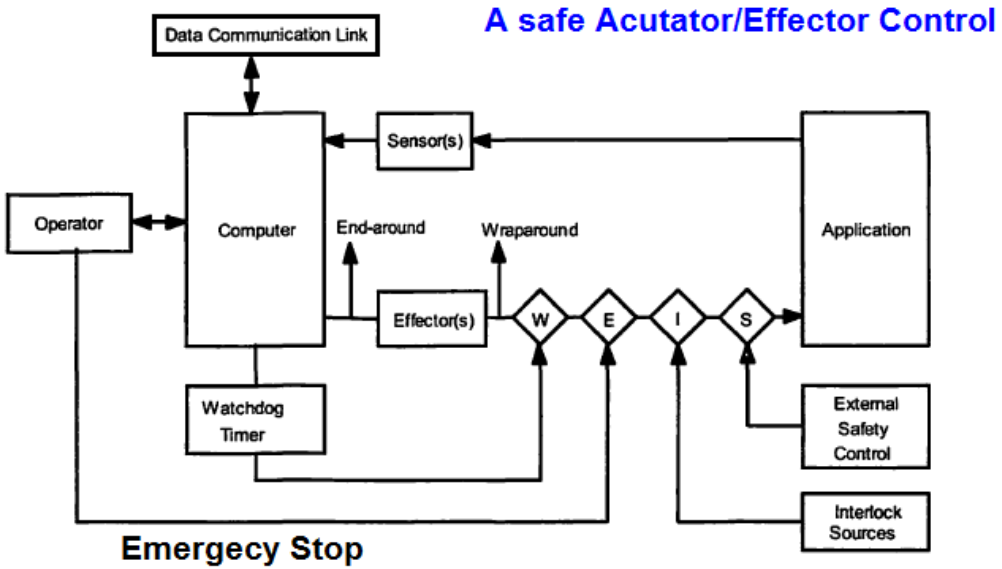
OPERATING MODE: ②

Component ③	Failure Mode ④	Failure Effect ⑤ / mitigation measures

FMEA Example – Jet Engine Propellant

- Modified Computer System
- Safety modification (ALL of the discussions we had in Chapter 4)
  - Sensor state test
  - Wraparound test
  - Safety Cutoff Valve
  - Valves closes to fail-safe position on power down
  - End around test
  - Watchdog timer
  - CPU self-test
  - Memory test
  - Valve safety interlock from engine control





FMEA – Jet Engine Propellant Supply System

FAILURE MODES AND EFFECTS ANALYSIS (FMEA) WORKSHEET

SYSTEM: Jet Engine Propellant Supply System **Page** 1 **of** 4
SUBSYSTEM: All
OPERATING MODE: Standby

Component	Failure Mode	Failure Effec / mitigation measures
SENSORS Flow switch FH Flow switch FO Flow switch FN1 Flow switch FN2	Indicates On position	Sensor state test detects. All valves signaled closed.
EFFECTORS Solenoid valve HV Solenoid valve OV Solenoid valve NV1 Solenoid valve NV2	Leaks, fails to open position	Failure not detected in this mode. Closed cutoff valves prevent gas flow.
SYSTEM ELECTRICAL POWER Sensor power Effector power	Off, intermittent, transient	Not detected in this mode. All valves including cutoff valves remain closed.
Computer power	Off, intermittent, transient	Watchdog timer times out. All valves remain closed.

effect

mitigation

FMEA – Jet Engine Propellant Supply System

FAILURE MODES AND EFFECTS ANALYSIS (FMEA) WORKSHEET

SYSTEM: Jet Engine Propellant Supply System **Page** 2 **of** 4
SUBSYSTEM: All
OPERATING MODE: Standby

Component	Failure Mode	Failure Effect / mitigation measures
ELECTRICAL INTERCONNECT Sensor-computer	Open circuit	Apparent flowmeter "On" reading. Sensor state test detects. All valves (including safety) signaled closed.
	Short circuit to ground	Not detected in this mode. All valves remain closed.
Computer-effector	Open circuit	Not detected in this mode. All valves remain closed.
	Short circuit to ground	Not detected in this mode. All valves remain closed.
	Short circuit to valve power source	Possible opening of all valves including safety cutoff valves.
OPERATOR	Activates PURGE or RUN switch during standby operation	Violates external run permissive. All valves (including safety) signaled closed.
COMPUTER Discrete/digital converter	Incorrect input state	1) Apparent flowmeter "On" reading. Sensor state test detects . All valves (including safety) signaled closed. 2) Apparent PURGE or RUN switch activation. Violates software permissive. All valves (including safety) signaled closed.

FMEA – Jet Engine Propellant Supply System

FAILURE MODES AND EFFECTS ANALYSIS (FMEA) WORKSHEET

SYSTEM: Jet Engine Propellant Supply System **Page** 3 **of** 4
SUBSYSTEM: All
OPERATING MODE: Standby

Component	Failure Mode	Failure Effect / mitigation measures
COMPUTER (cont.) Digital/discrete converter	One or more valves signaled open.	End-around test detects failure. All valves (including safety) signaled closed.
Operator input panel	Open circuit	Not detected in this mode. All valves remain closed.
PURGE switch	Short circuit	Apparent PURGE switch activation. External run permissive blocks valve command.
RUN switch	Open circuit	Not detected in this mode. All valves remain closed.
	Short circuit	Apparent RUN switch activation. External run permissive blocks valve command.
CPU	Halt	Watchdog timer detects Power removed from all valves.
	Incorrect function	CPU self-test detects All valves (including safety) signaled closed.

FMEA – Jet Engine Propellant Supply System

FAILURE MODES AND EFFECTS ANALYSIS (FMEA) WORKSHEET

SYSTEM: Jet Engine Propellant Supply System **Page** 4 **of** 4
SUBSYSTEM: All
OPERATING MODE: Standby

Component	Failure Mode	Failure Effect / mitigation measures
COMPUTER (cont.)	Program bit(s) inverted	Memory test detects failure All valves (including safety) signaled closed.
Memory	Data bit(s) inverted	Possible opening of one or more valves. Valve safety interlock from engine prevents valve opening.
	Address logic fault	Watchdog timer detects. Power removed from all valves.
SOFTWARE	Spurious output	Possible opening of one or more valves. Valve safety interlock from engine prevents valve opening.
	Ceases to function	Watchdog timer detects. Power removed from all valves.

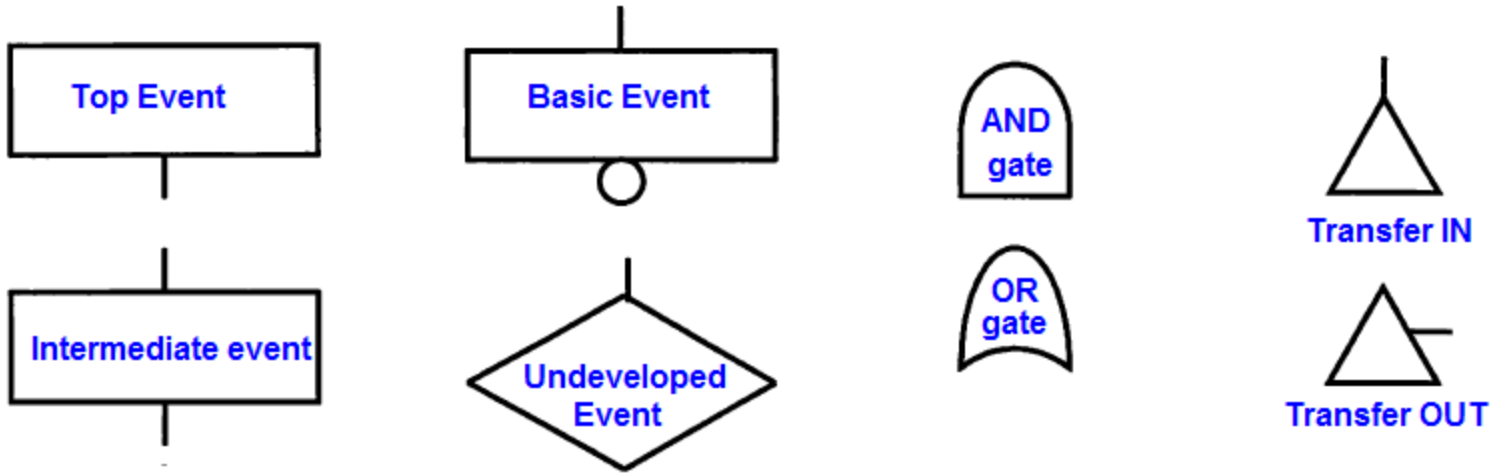
FMEA - Summary

- Tracing **component failures** out to **their consequences**
- Screening the effectiveness of the modified design's safety measures
- Identifying hazards that may have overlooked in the preliminary hazard analysis
- Basic Limitation:
  - FMEA examines system response to **single failures only**
  - Good enough for low-end fail-safe applications where limited property damage is the only safety concern
  - Must be supplemented, in safety-critical application, with more advanced techniques such as **Fault Tree Analysis**, Event Tree Analysis, etc.
- FMECA (Failure Mode Effects and Critical Analysis) ?
  - FMEA with assigned level of criticality (in terms of harm) to each component should the component fail
  - To allocate resources so that the more critical items in a system received more attention

Fault Tree Analysis

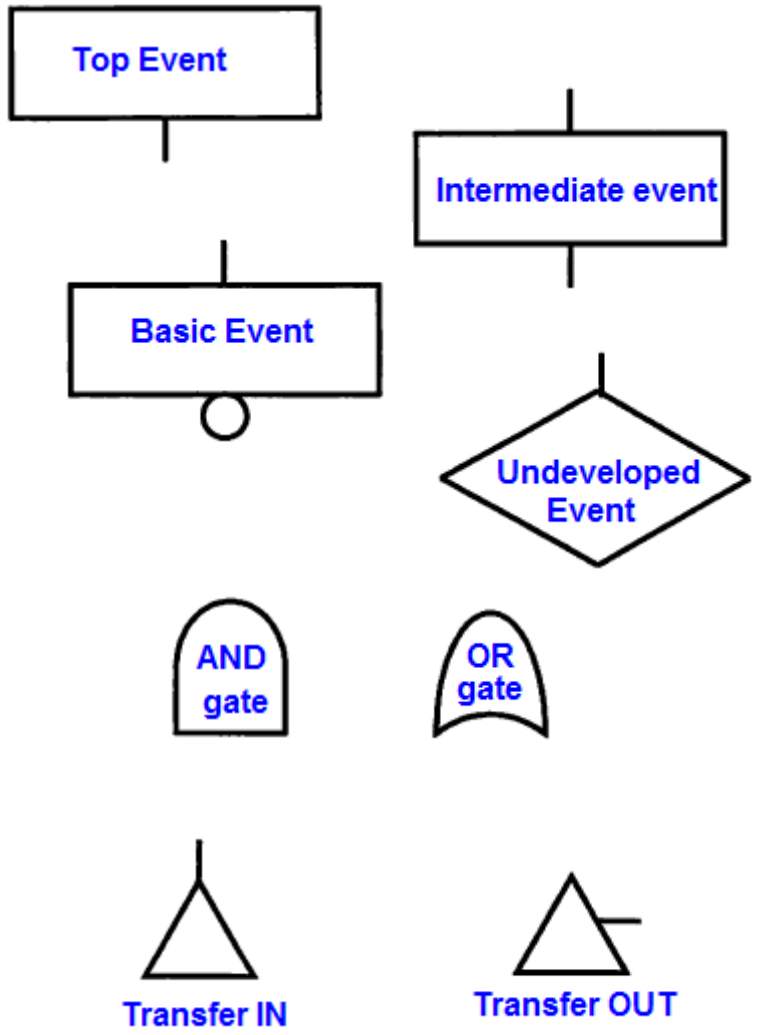
- A reverse process of FMEA
- FTA begins with a hazard event or mishap, and traces it back to the failure causing the event
- FTA is a graphical (as opposed to the tabular of FMEA)

- **FTA Symbols and FT Structure**



Fault Tree Analysis - Symbols

- **Top Event:** A event resulting from other fault events
- **Intermediate Event:** An event resulting from one or more previous (antecedent) causes acting through AND or OR
- **Basic Event:** A basic initiating event requiring no further development (INPUT)
- **Undeveloped Event**: An event which is not further developed **either** because it is of insufficient consequence **or** because information is not available (does not grow down)
- **AND gate:** Output fault occurs if all of the input faults occur
- **OR gate:** Output fault occurs if any one or more of the input faults occur
- **Transfer In:** Indicates that the tree is developed further on another sheet
- **Transfer Out:** Indicates that this portion of the tree must be attached to a corresponding **Transfer In** on another sheet



Fault Tree Analysis – Other Symbols

- NRC "Fault Tree Handbook" – NUREG-0492

BASIC EVENT – A basic initiating fault requiring no further development

CONDITIONING EVENT – Specific conditions or restrictions that apply to any logic gate (used primarily with PRIORITY AND and INHIBIT gates)

AND – Output fault occurs if all of the input faults occur

OR – Output fault occurs if at least one of the input faults occurs

EXCLUSIVE OR – Output fault occurs if exactly one of the input faults occurs

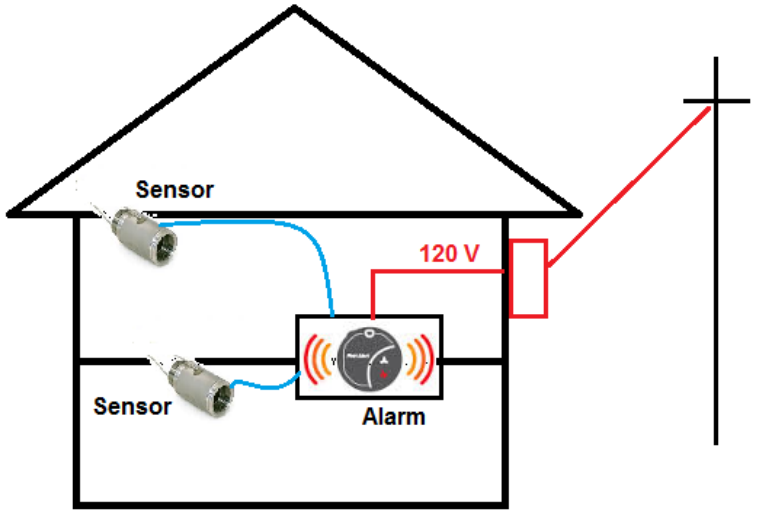
PRIORITY AND – Output fault occurs if all of the input faults occur in a specific sequence (the sequence is represented by a CONDITIONING EVENT drawn to the right of the gate)

INHIBIT – Output fault occurs if the (single) input fault occurs in the presence of an enabling condition (the enabling condition is represented by a CONDITIONING EVENT drawn to the right of the gate)

FTA Example 1

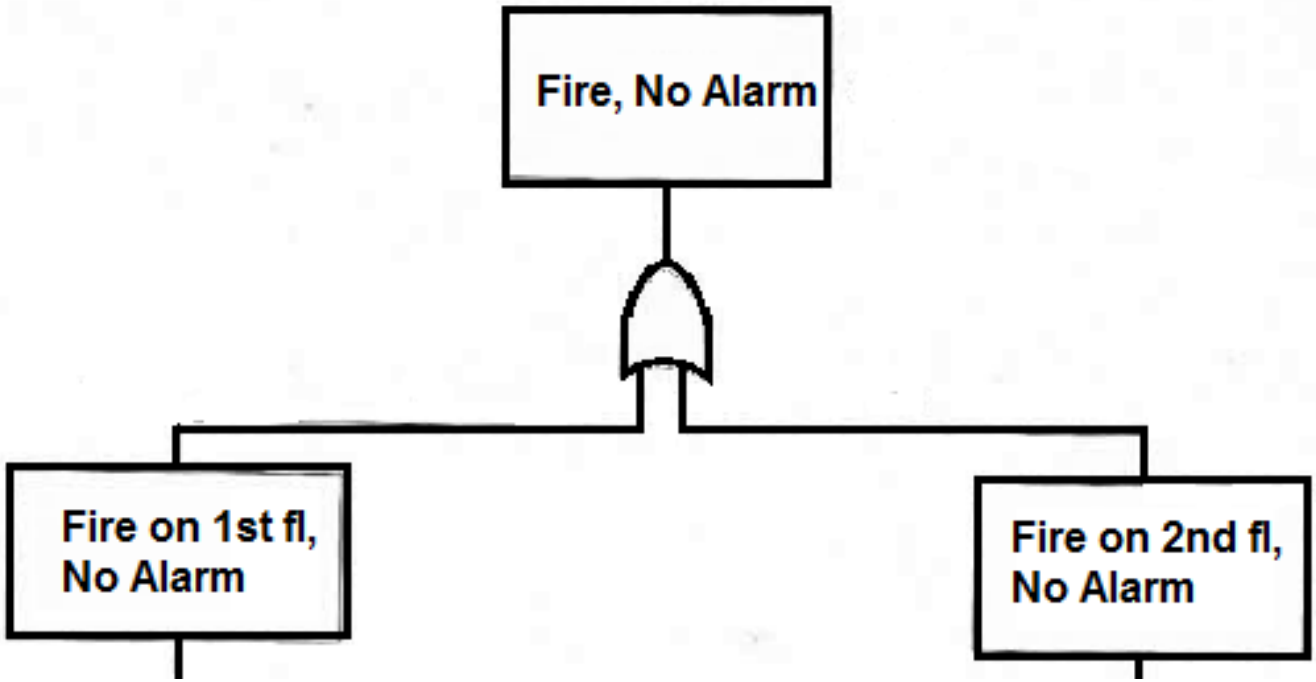
- A fire alarm system for residential use

- Normal Operation
  - No 1st floor fire or 2nd floor fire, No alarm
  - If 1st floor fire sensor or 2nd floor fire sensor detects fire in the 1st floor or 2nd floor, then Alarm

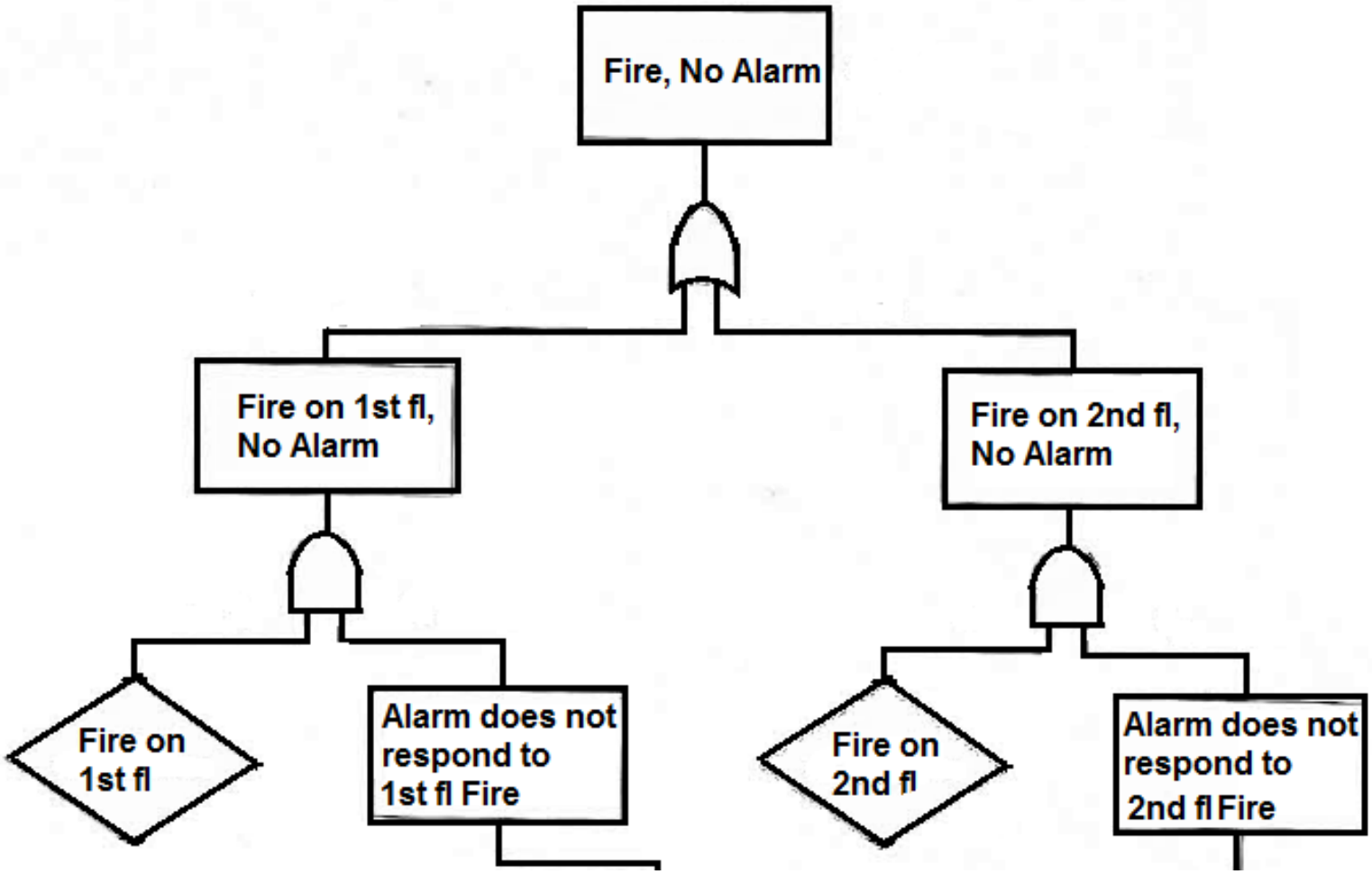


- The fault tree Top Event is "**Fire but No Alarm**"
  - Fire on 1st floor but no alarm OR Fire on 2nd floor no alarm
    - Fire on 1st floor → Alarm does not respond to 1st floor fire
      - Fire Sensor Failure OR Fire Alarm Inoperative
        - » Alarm Failed OR No Power to Alarm System OR Sensing Line Failure
          - » Power Line Failure OR Gird Power Failure

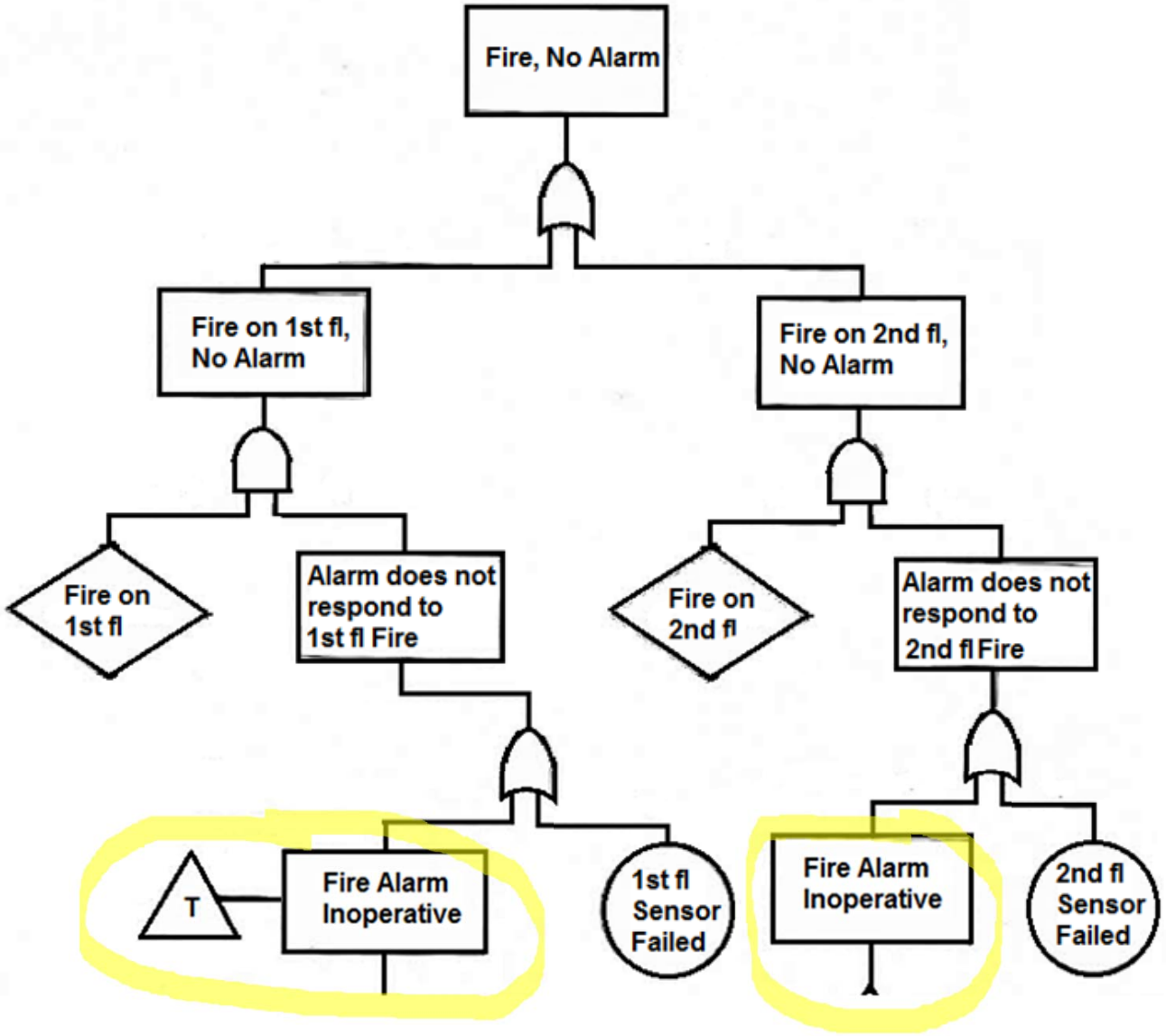
Step 1



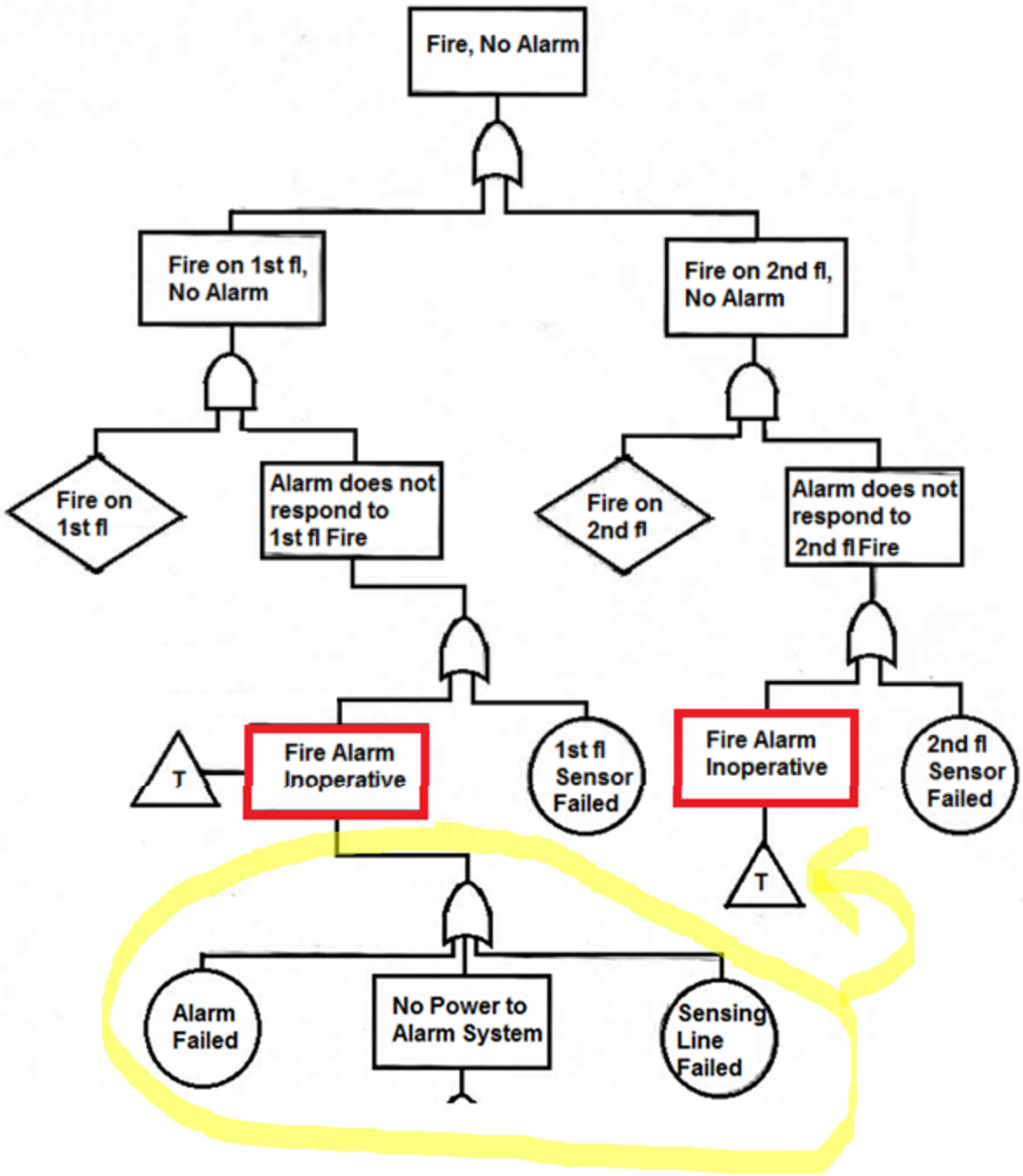
Step 2


Fire, No Alarm
Fire on 1st fl, No Alarm
Fire on 2nd fl, No Alarm
Fire on 1st fl
Alarm does not respond to 1st fl Fire
Fire on 2nd fl
Alarm does not respond to 2nd fl Fire

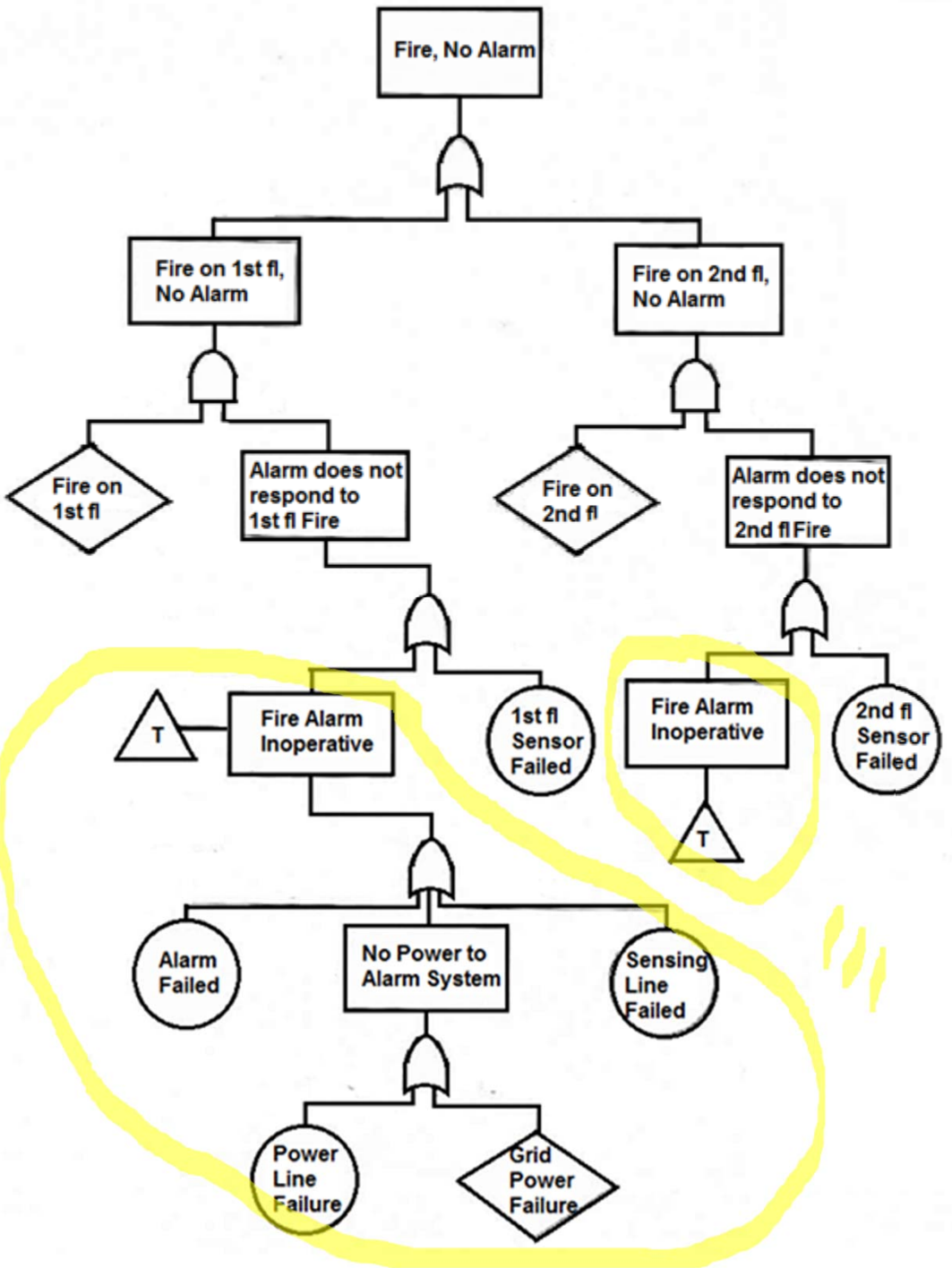
Step 3


Fire, No Alarm
Fire on 1st fl, No Alarm
Fire on 2nd fl, No Alarm
Fire on 1st fl
Alarm does not respond to 1st fl Fire
Fire on 2nd fl
Alarm does not respond to 2nd fl Fire
T
Fire Alarm Inoperative
1st fl Sensor Failed
Fire Alarm Inoperative
2nd fl Sensor Failed

Step 4


Fire, No Alarm
Fire on 1st fl, No Alarm
Fire on 2nd fl, No Alarm
Fire on 1st fl
Alarm does not respond to 1st fl Fire
Fire on 2nd fl
Alarm does not respond to 2nd fl Fire
T
Fire Alarm Inoperative
1st fl Sensor Failed
Fire Alarm Inoperative
2nd fl Sensor Failed
T
Alarm Failed
No Power to Alarm System
Sensing Line Failed

Step 5

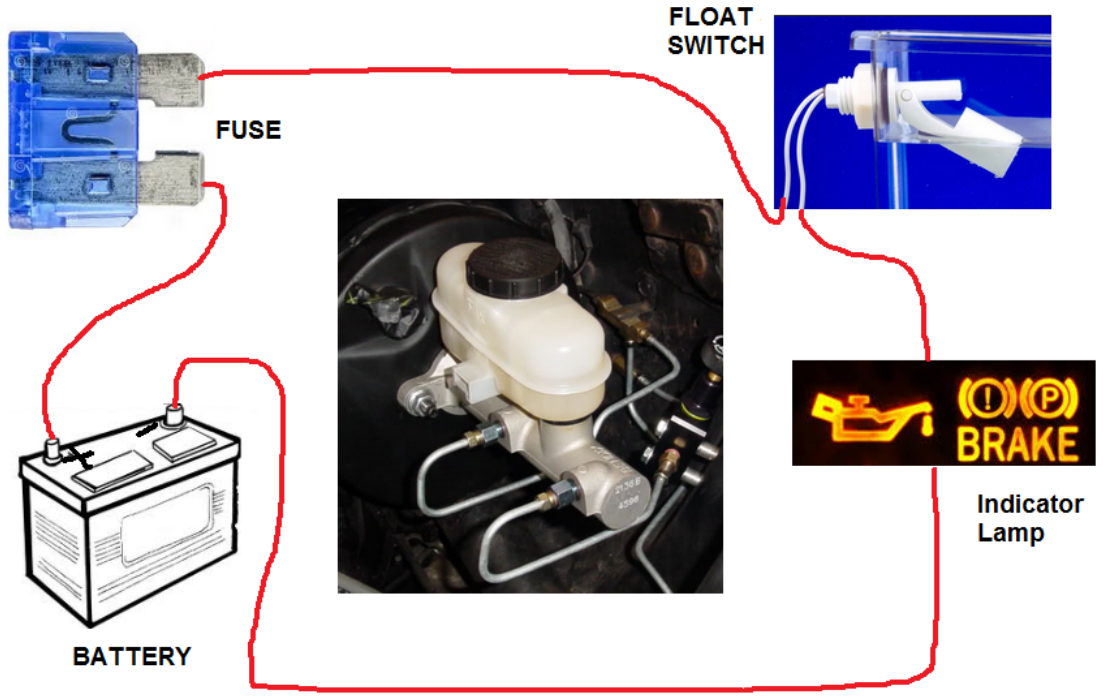

Fire, No Alarm
Fire on 1st fl, No Alarm
Fire on 2nd fl, No Alarm
Fire on 1st fl
Alarm does not respond to 1st fl Fire
Fire on 2nd fl
Alarm does not respond to 2nd fl Fire
T
Fire Alarm Inoperative
1st fl Sensor Failed
Fire Alarm Inoperative
2nd fl Sensor Failed
T
Alarm Failed
No Power to Alarm System
Sensing Line Failed
Power Line Failure
Grid Power Failure

FTA --- How to

- Top **Event**
  - Undesired event which we want to avoid
- Intermediate **Events**
  - An event which, combined with OR or AND condition, leads to the Top (or upper) Event
  - A dependent event
- **Basic Events**
  - An event that does not grow down further. An independent event.
  - It is an input condition to an Intermediate Event
  - Basic Events are Component failures which lead to another Event
- Intermediate Event or Basic Event?
  - Intermediate Event: If multiple failures are involved
  - Basic Event: Single component failure

FTA Exercise 1

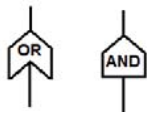
- **System:** An automotive brake fluid warning lamp



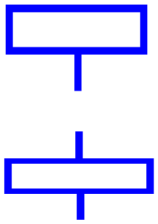
- **Normal Operation**: When the fluid level is low, the float switch closes and the warning lamp turns on

[Reminder] Fault Tree --- How to construct

1. Complete understanding of the system operation
2. Logical thinking in what would cause the Top event (which is an effect) – <u>serial</u> or <u>parallel</u> or <u>combined</u> **cause-effect**



Think about (and in terms of) **events** (not component faults – these come at the very last step) which lead to the **top event** (mishap, accident, etc)



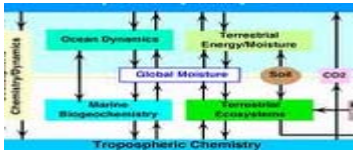
- **Top Event:** Undesired event which we want to avoid
- **Intermediate Events:** Events which, combined with OR or AND condition, lead to the Top (or upper) Event. Dependent events

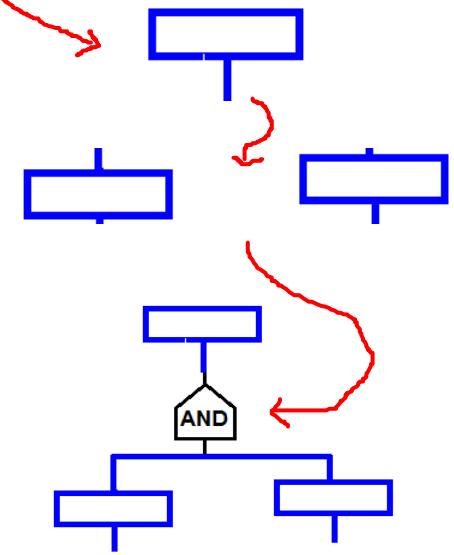
Connection of Intermediate Events to the Top Event

5. Then, grow <u>Basic Events (component faults)</u> from the **<u>upper events</u>**

- An event that does not grow down further. Independent events. It is an input condition to an Intermediate Event
- Connect them to the Events

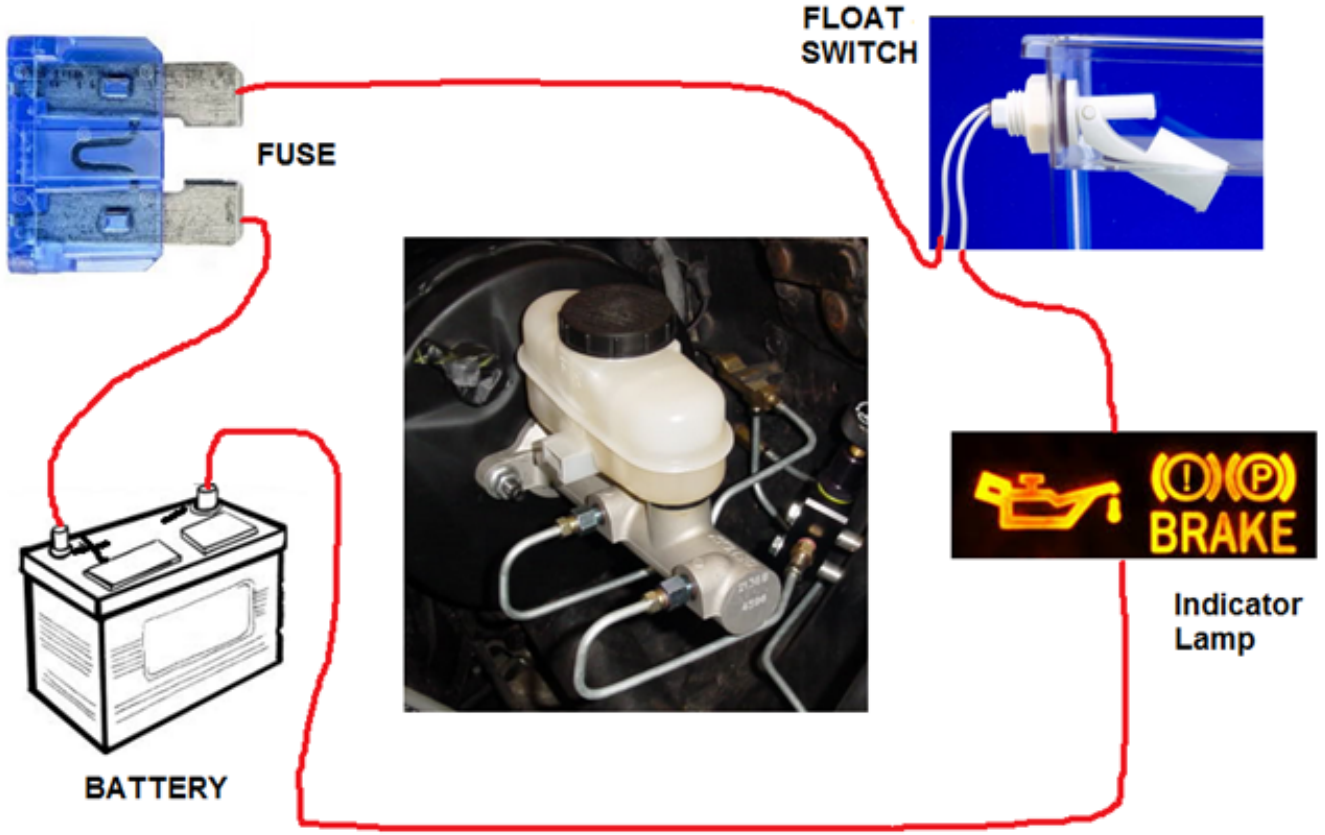
6. Some component is suspected of failure/fault but not 100% sure --- Undeveloped event



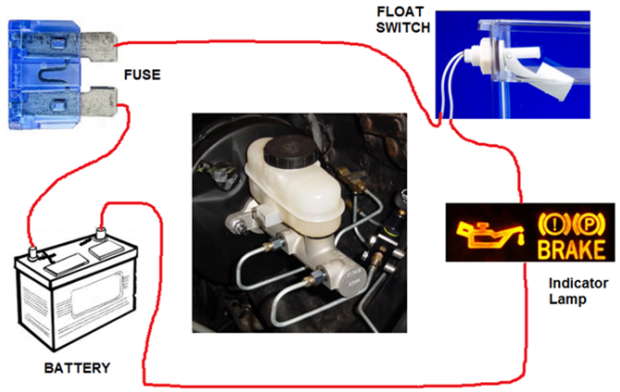


Class Activity

- **Undesired Event (Top Event):** The warning lamp fails to turn on when the brake fluid is low.
- **Construct a fault tree** for the top event of “Warning Lamp Does Not Operate When the Fluid is Low”



SOLUTION



Warning Lamp Doesn't Turn On

OR

Lamp Failure

No Power Supply to the Lamp

OR

Battery Failure

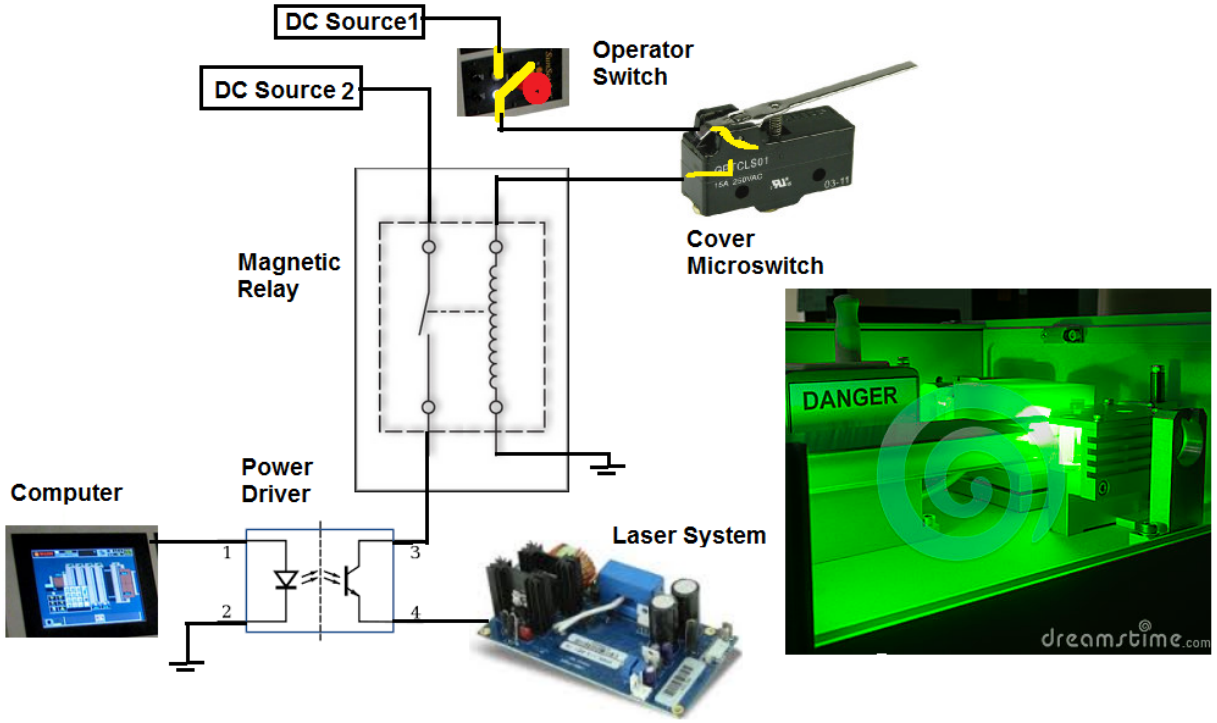
Fuse Open-Circuit

Float Switch Fail to Close

Cable Connector Failure

FTA Exercise 2

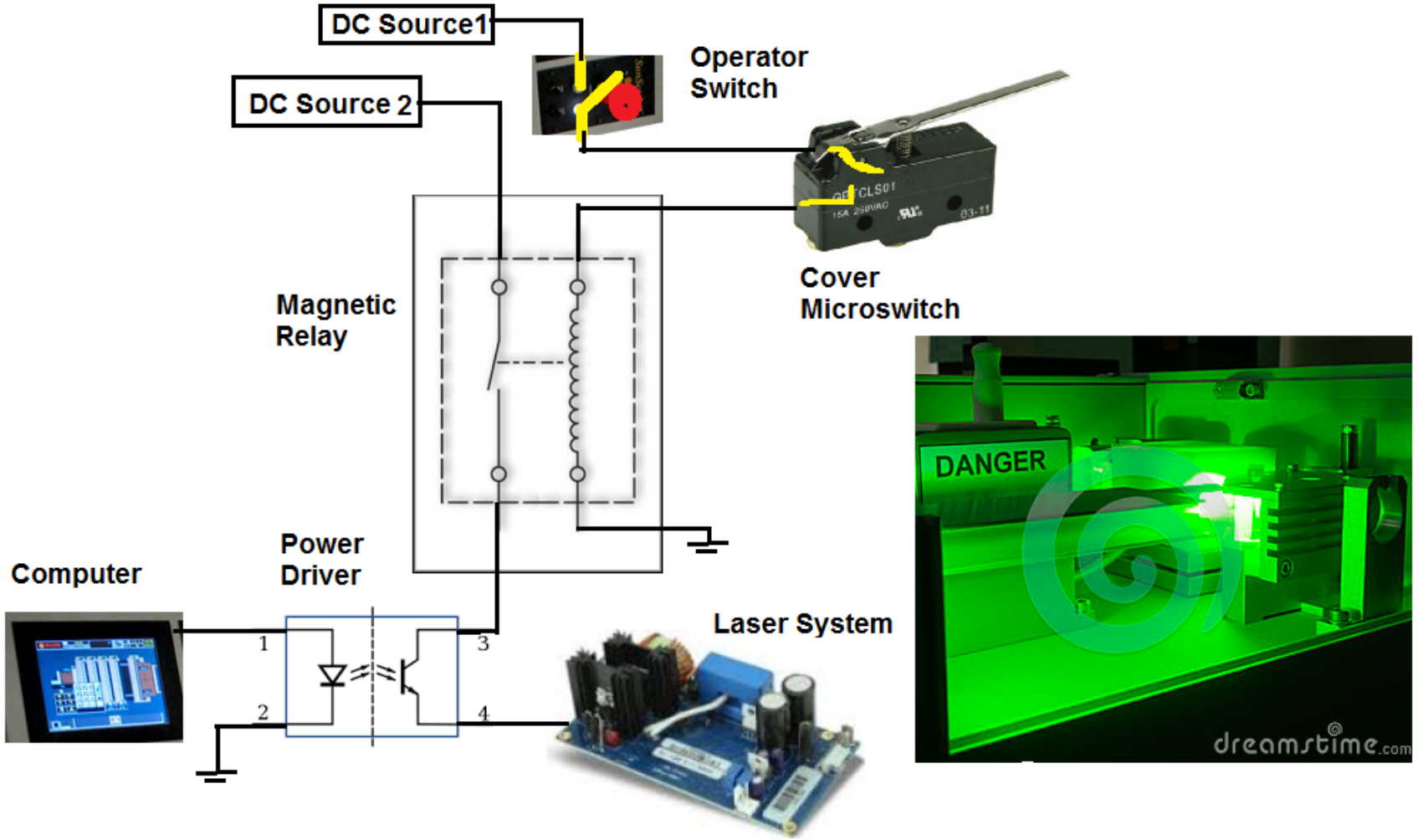
- **System: A Laser Control System**

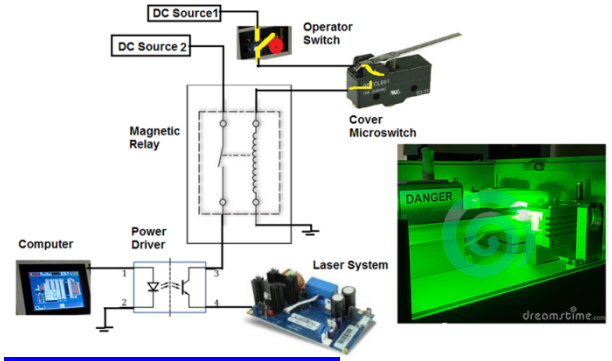


- **Normal Operation**: The Laser is controlled from a computer output line via a power driver and an electromagnetic relay. Firing of the laser is initiated by a human operator. There is a safety clover which woks as a safety interlock, which when opened disables the laser control signal.

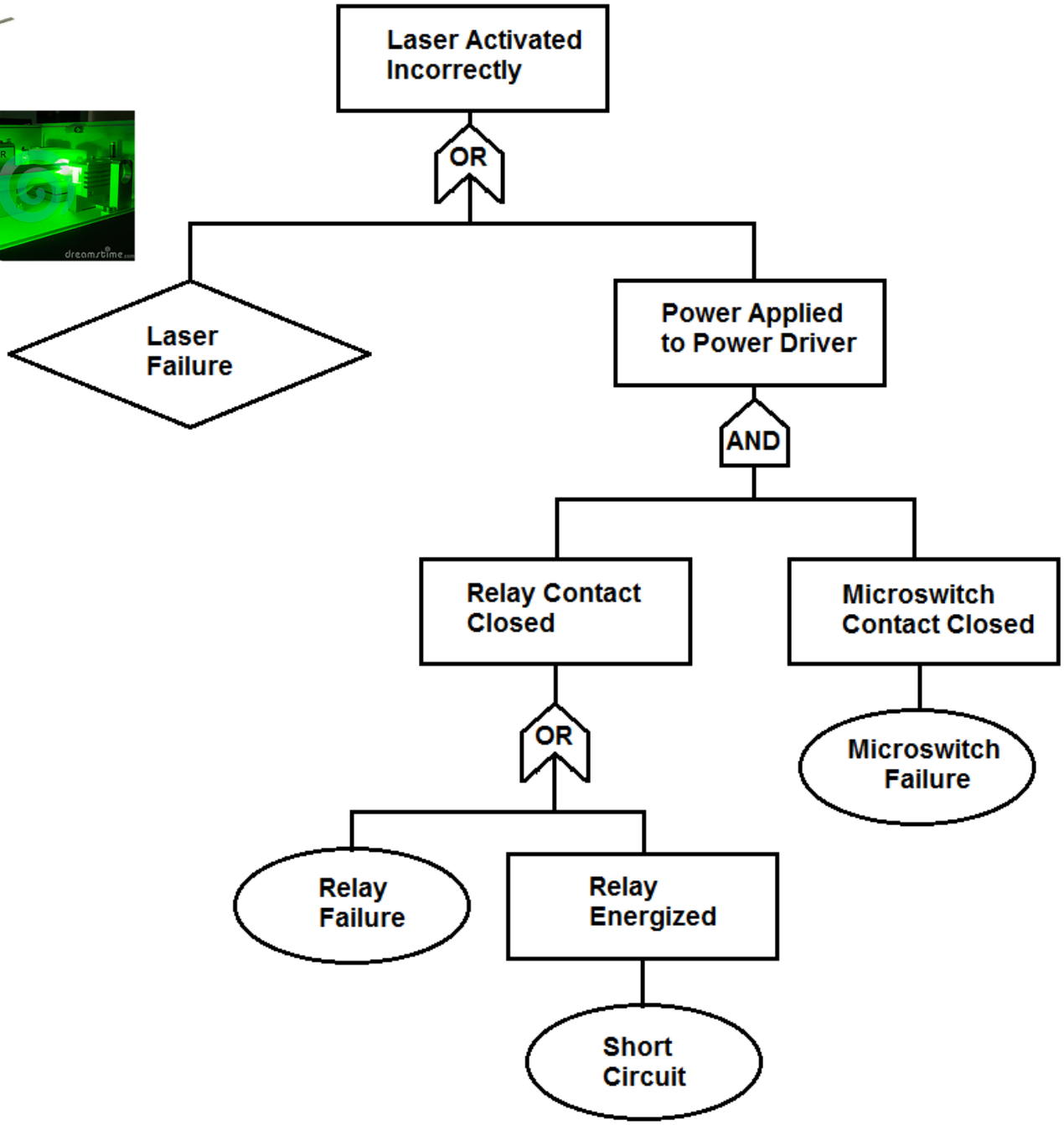
Class Activity

- Construct a Fault Tree for the Undesired Event (Top Event) of "**The laser control signal is enabled while the safety cover is open**"



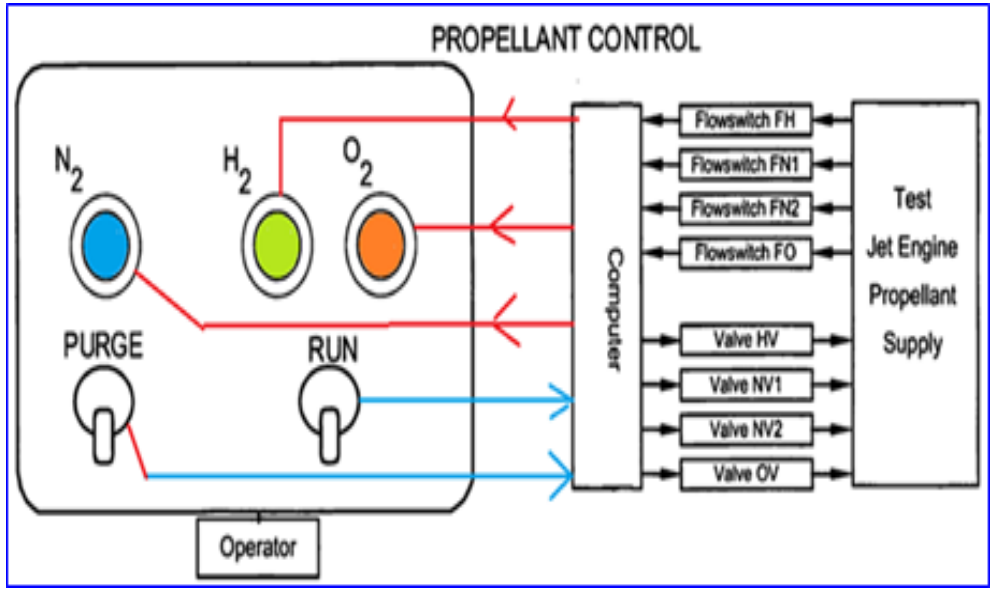

DC Source1
DC Source 2
Operator Switch
Cover Microswitch
Magnetic Relay
Computer
Power Driver
Laser System
DANGER

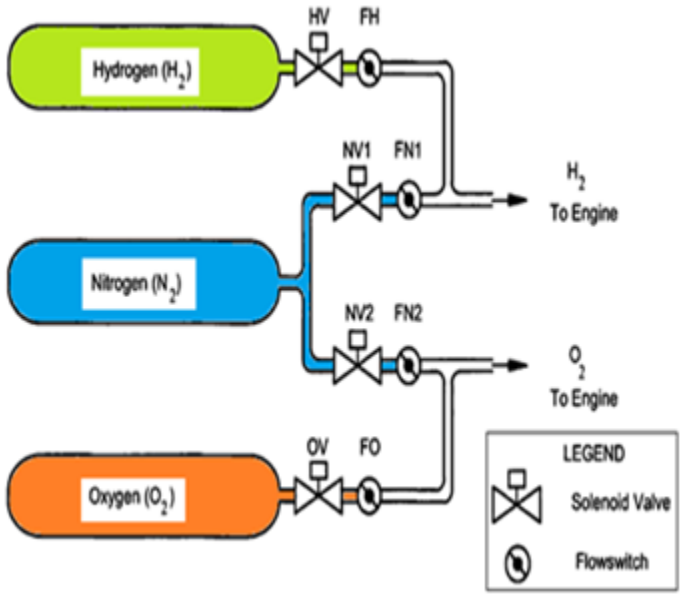
Solution


Laser Activated Incorrectly
OR
Laser Failure
Power Applied to Power Driver
AND
Relay Contact Closed
Microswitch Contact Closed
OR
Microswitch Failure
Relay Failure
Relay Energized
Short Circuit

Fault Tree Example – Jet Engine Propellant Case

- **Basic Computer System**

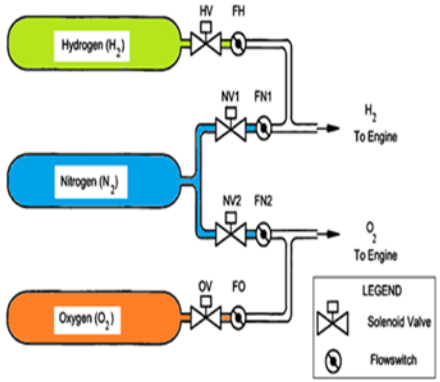


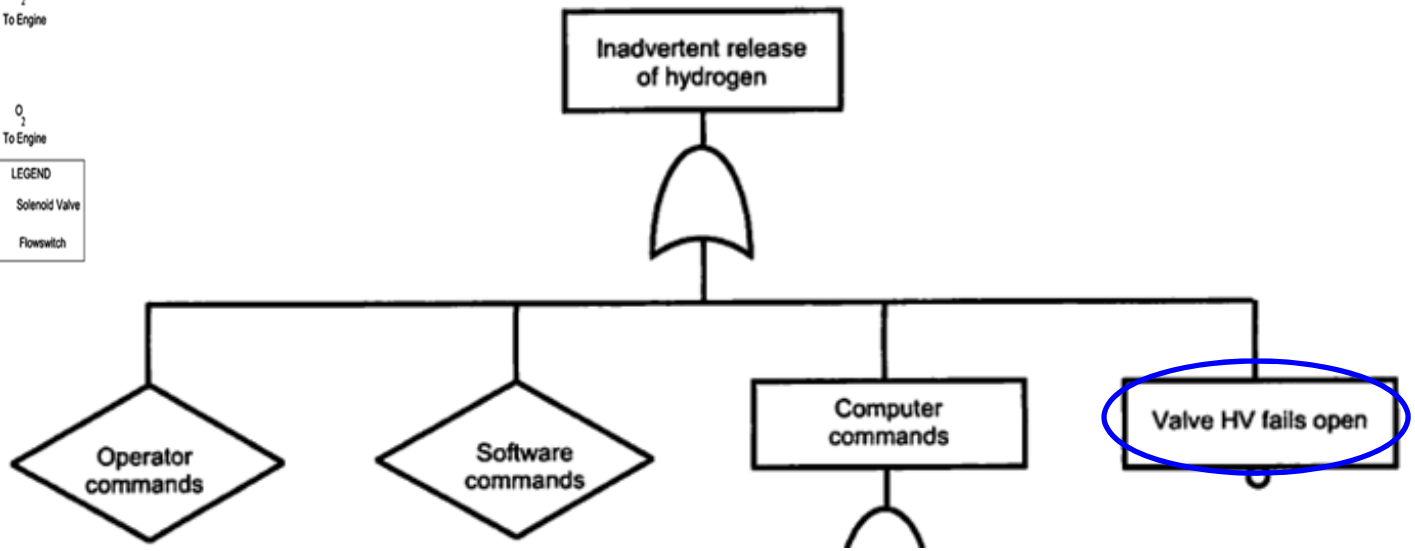


- Hazard Event: Inadvertent release of Hydrogen → Top Event
- Hazard Event can be caused by multiple events (→ connected by OR gates)

Fault Tree Analysis Example – in Plain English

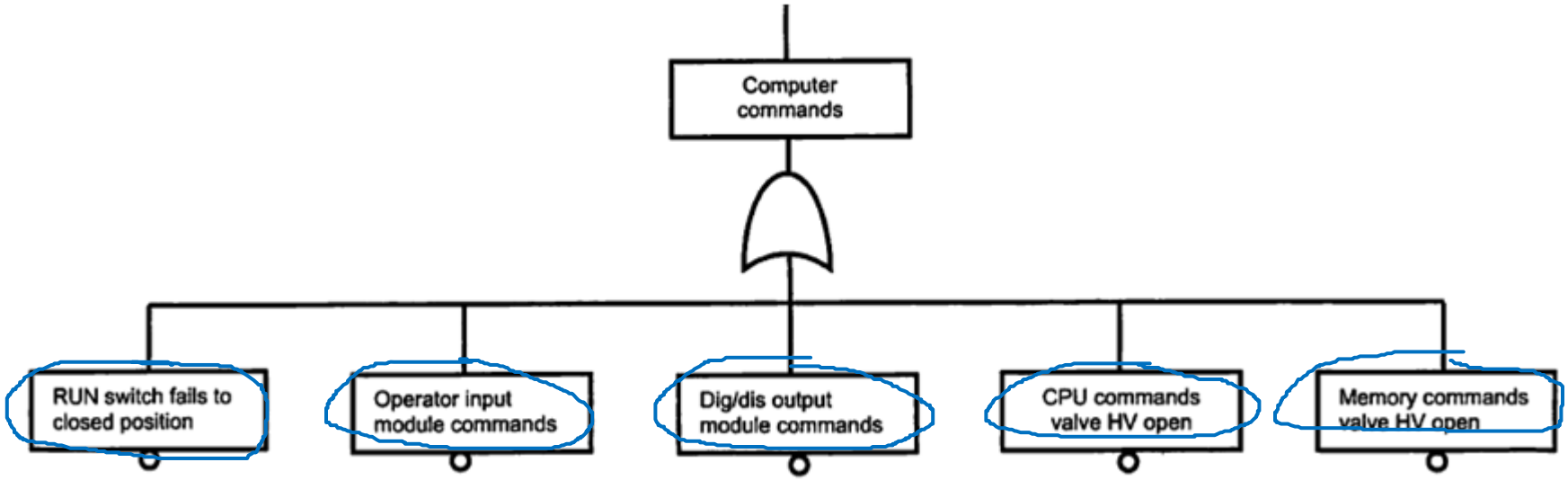
- First:
  - "Inadvertent release of hydrogen" could be due to failures of "operator commands hydrogen valve open" OR "software commands hydrogen valve open" OR "Computer commands hydrogen valve open" OR "hydrogen valve itself opens"





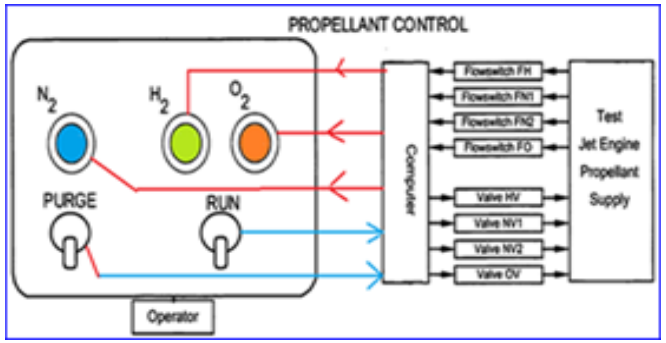
Fault Tree Analysis – in Plain English

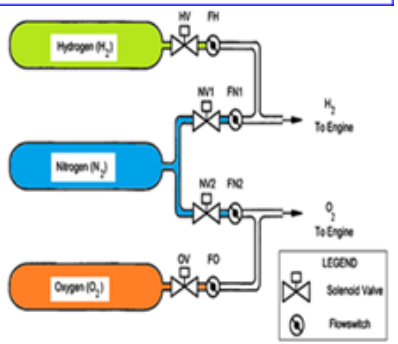
- Further:
  - The intermediate event, “Computer commands hydrogen valve open”, could be due to failures in “RUN switch fails open” OR “operator input module commands HV open” OR “digital/discrete output module commands HV open” OR “CPU commands valve HV open” or “Memory commands valve HV open”



Fault Tree Analysis

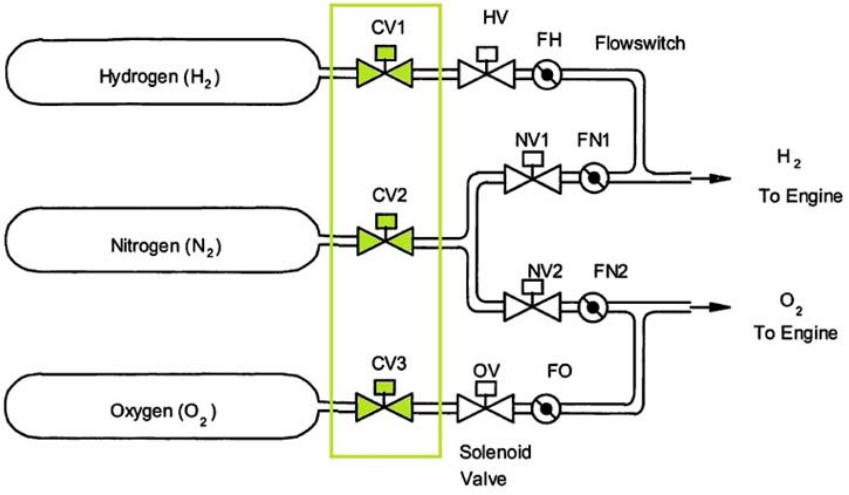
- **Finally**

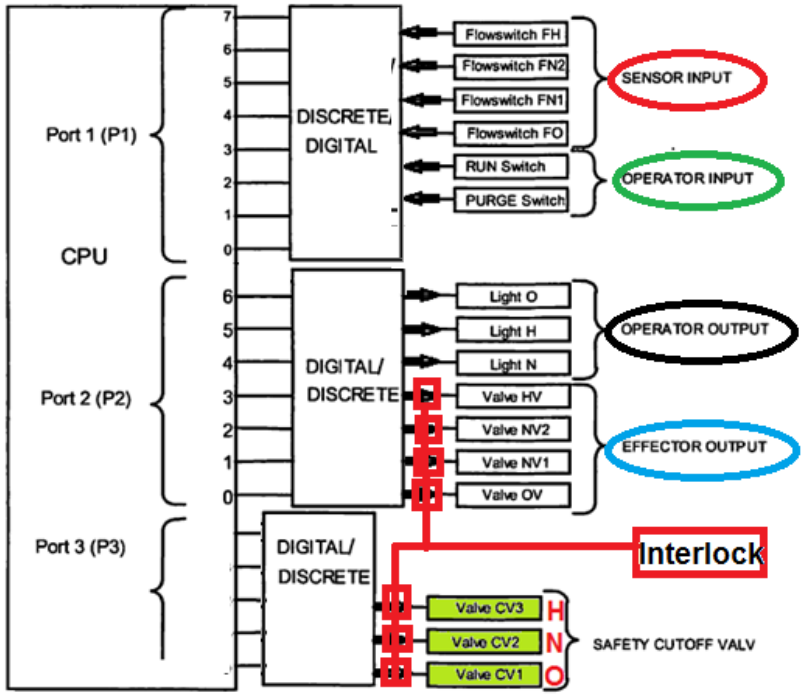




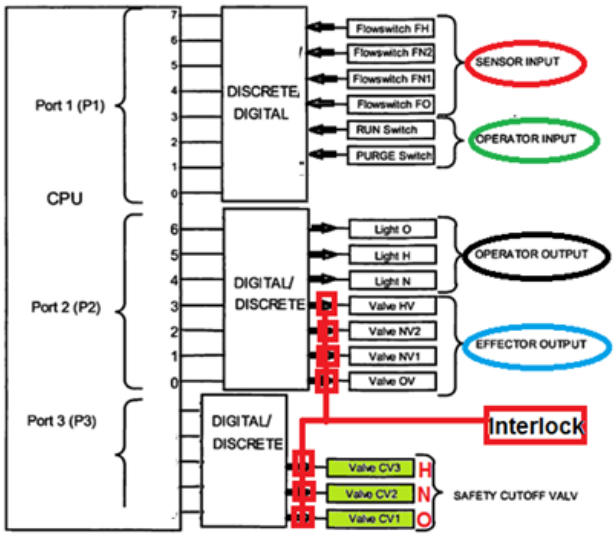
Fault Tree Analysis – Jet Engine Propellant

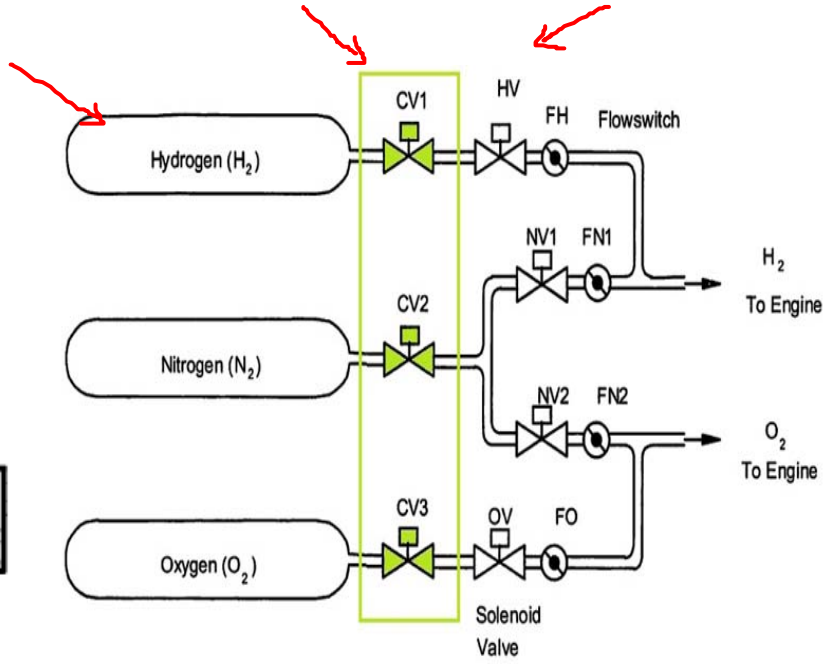
- **Modified Computer System**
  (as was used in FMEA)
  - Sensor state test
  - Wraparound test
  - Safety Cutoff Valve
  - Valves closes to fail-safe position on power down
  - End around test
  - Watchdog timer
  - CPU self-test
  - Memory test
  - Valve safety interlock from engine control
- Start with the Top Event and study the decomposition of the tree

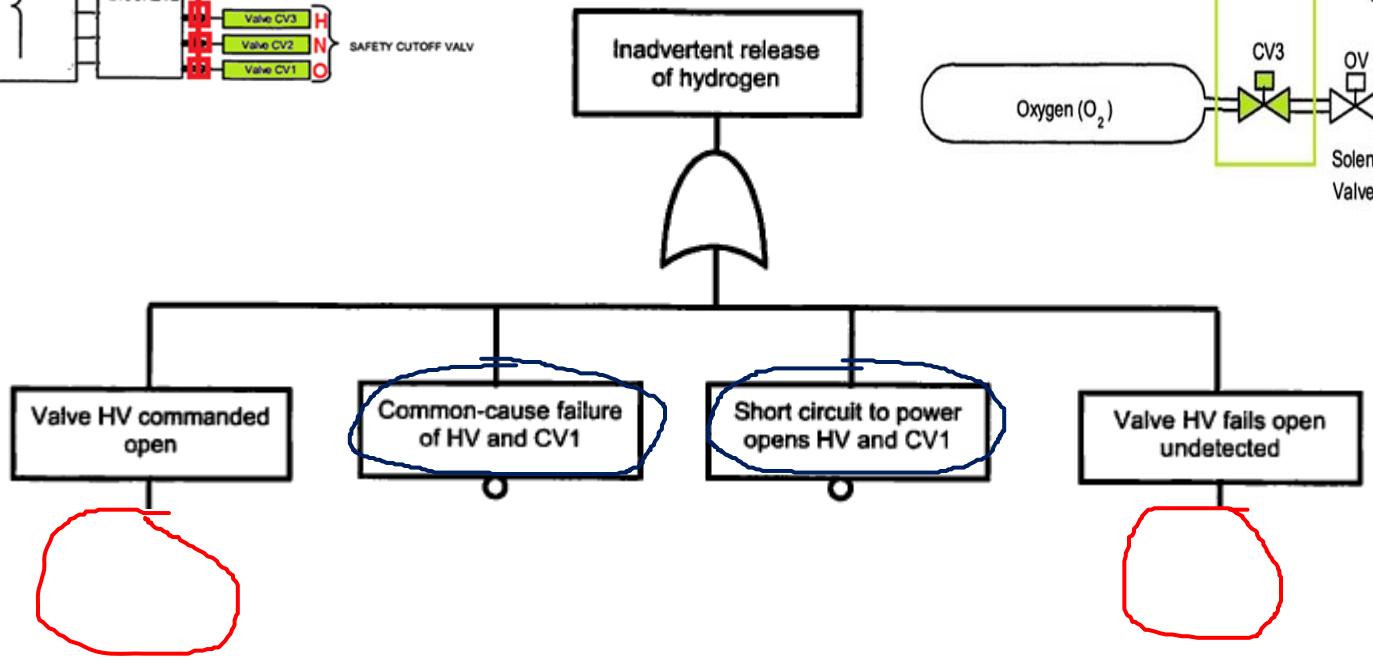




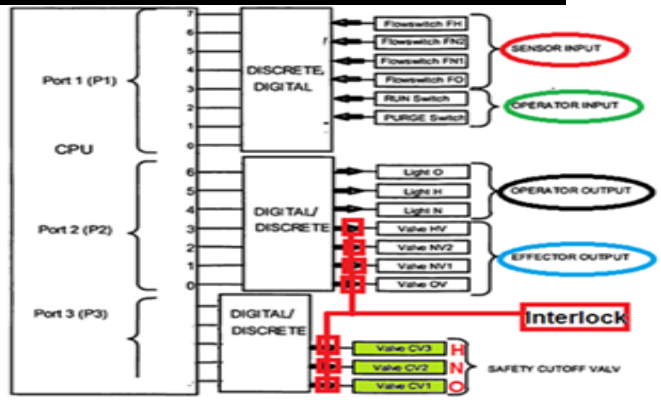
Fault Tree Analysis – Example Sheet 1



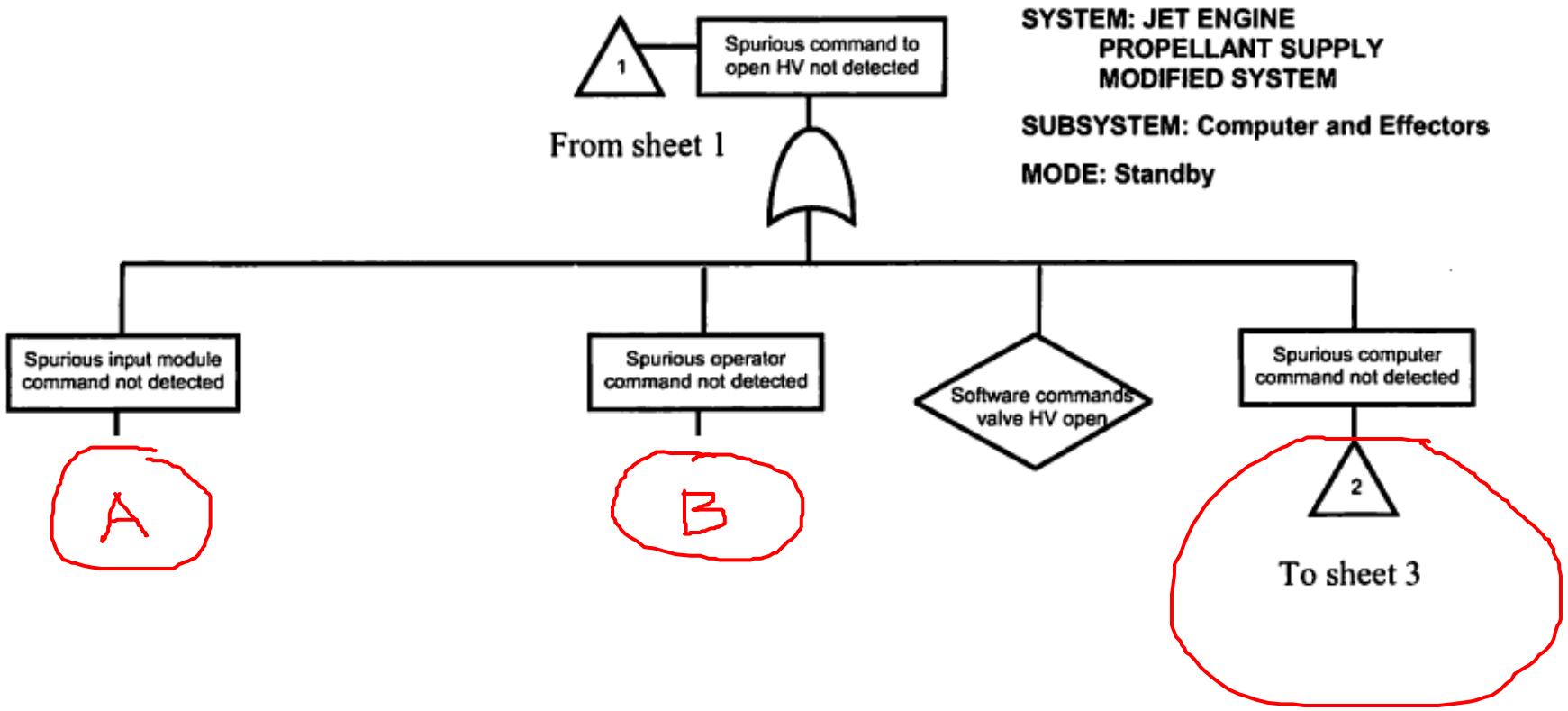




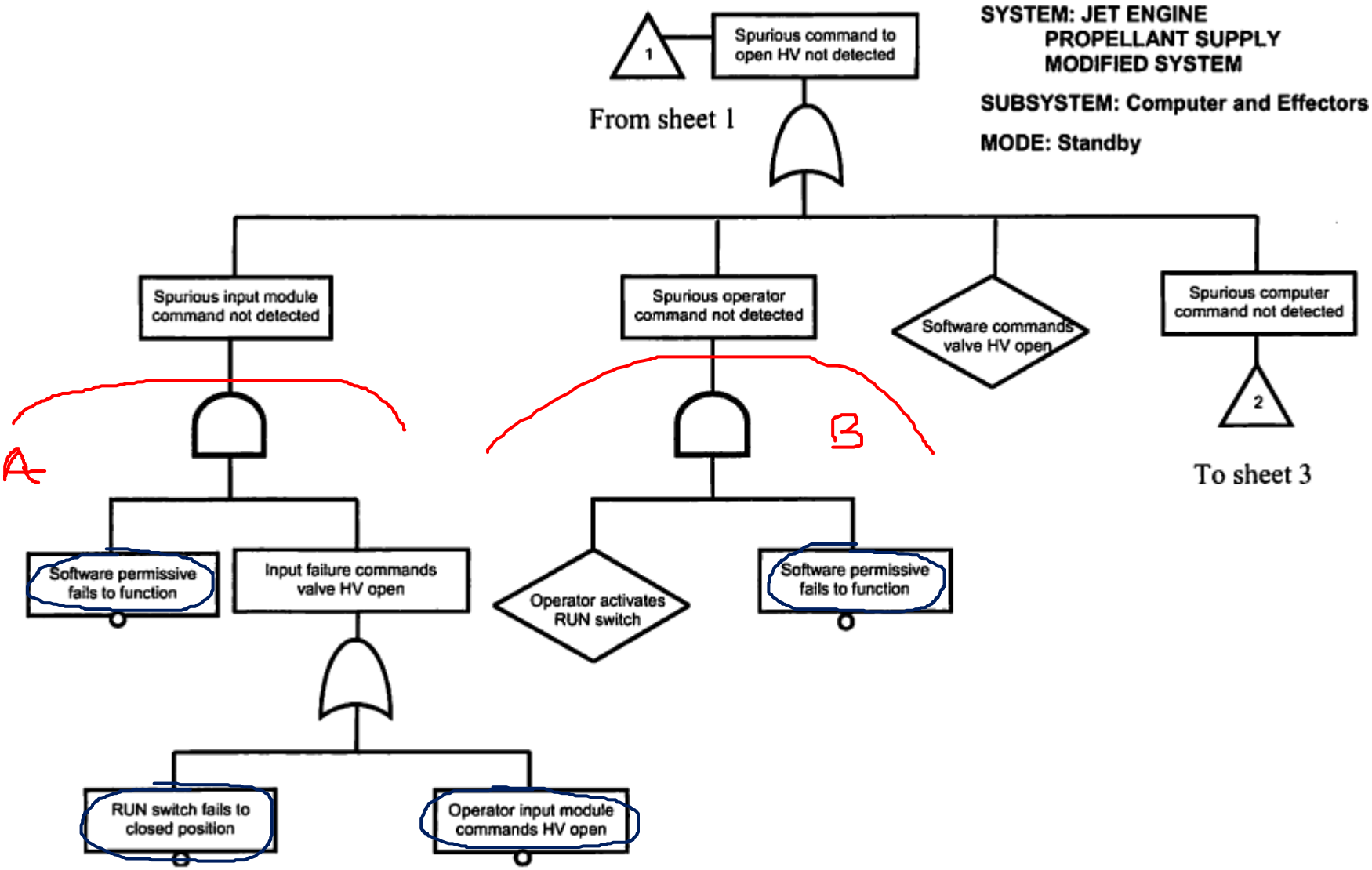
Fault Tree Analysis – Example Sheet 1



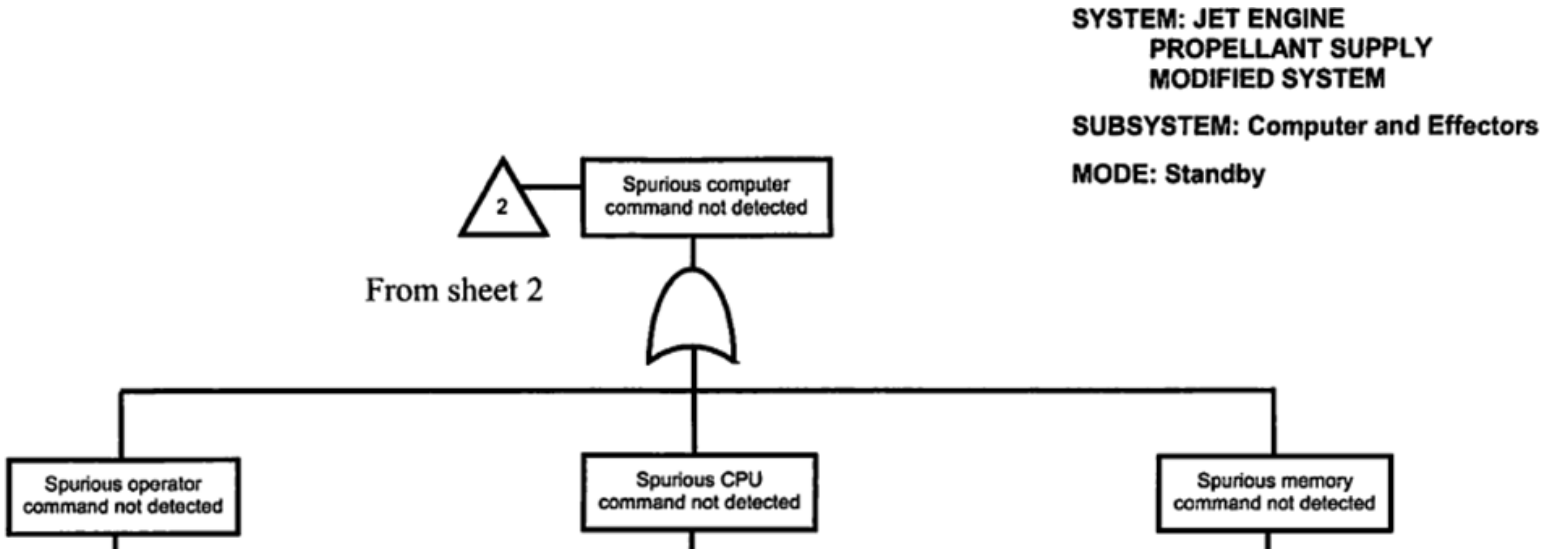
Fault Tree Analysis - Sheet 2



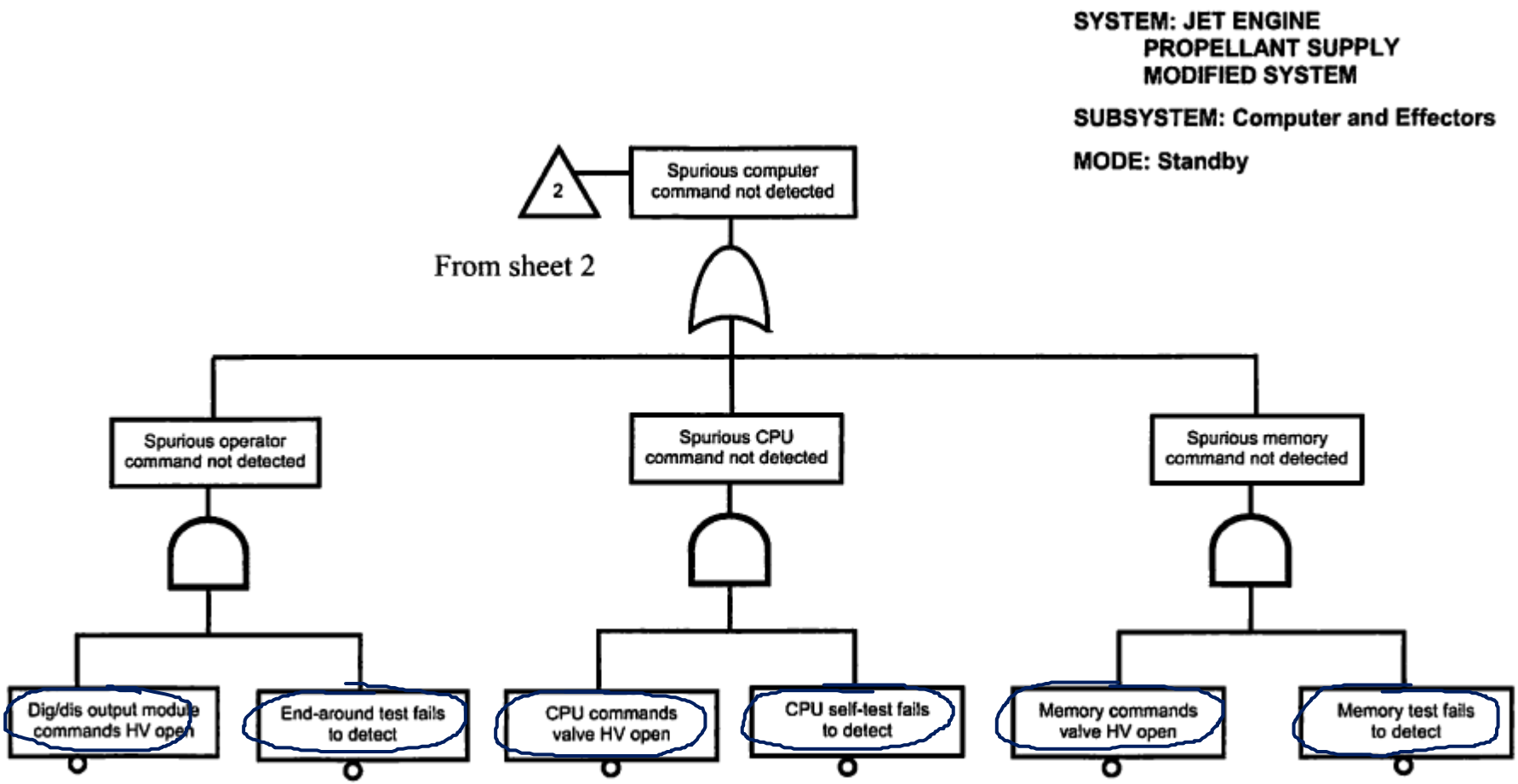
Fault Tree Analysis - Sheet 2



Fault Tree Analysis – Sheet 3



Fault Tree Analysis – Sheet 3

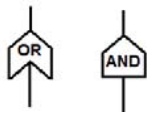


FTA summary

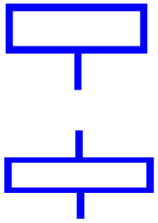
- FTA can represent multiple events including successive component failures
- FTA is considerably more complex than FMEA
- FTA must be constructed for **each subsystem**
- FTA must be constructed for **each hazard event** contributing to mishap
- FTA is a top-down analysis approach: “Deductive form of analysis [**Why** a system can fail]” (cf. FMEA is a bottom-up analysis approach → Inductive method [**How** a system can fail])
- FTA (like FMEA) is primarily confined to system hardware and software

[Reminder 2] Fault Tree --- How to construct

1. Complete understanding of the system operation
2. Logical thinking in what would cause the Top event (which is an effect) – <u>serial</u> or <u>parallel</u> or <u>combined</u> **cause-effect**



Think about (and in terms of) **events** (not component faults – these come at the very last step) which lead to the **top event** (mishap, accident, etc)



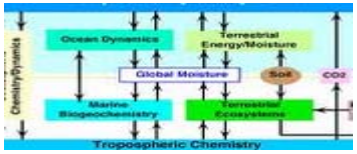
- **Top Event:** Undesired event which we want to avoid
- **Intermediate Events:** Events which, combined with OR or AND condition, lead to the Top (or upper) Event. Dependent events

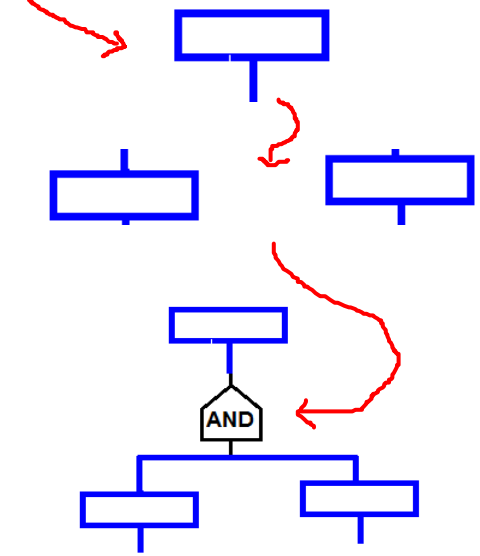
Connection of Intermediate Events to the Top Event

5. Then, grow <u>Basic Events (component faults)</u> from the **<u>upper events</u>**

- An event that does not grow down further. Independent events. It is an input condition to an Intermediate Event
- Connect them to the Events

6. Some component is suspected of failure/fault but not 100% sure --- Undeveloped event





Next Subject: Risk Analysis with FTA

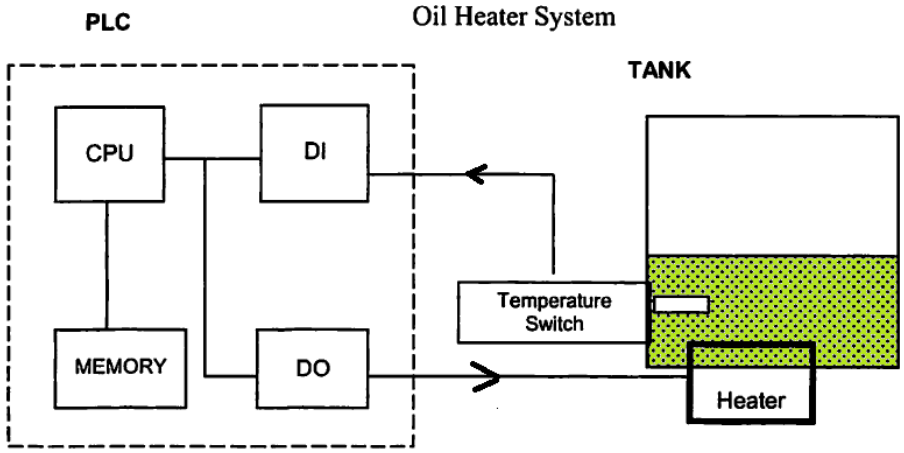
- Background:
  - A safety device is never perfect and can fail to perform when called upon
  - Any completed safety-critical computer system design, with layers of safety devices, can still produce a mishap
  - Then, what would be the likelihood of that mishap?
- Mishap Risk and Risk Analysis
- Objective of risk analysis:
  - Estimate the risk and verify that it meets an acceptable level of mishap risk

Mishap Risk Probability: Calculation Approach

- **Assumption**: Risk requirement is stated in terms of a probability of failure over a specified time interval
- **Approach**: Determination of the probability that the mishap will occur over the same time interval
- **Risk Analysis Steps**
  - Step 1: Use FTA and trace the mishap (top event) down to all of the basic component failure events (basic events) contributing to it
  - Step 2: Determine the probability of each of these failure events {**Assumed to be already found or provided**}
  - Step 3: Combine these probabilities to yield the probability of the mishap

Risk Analysis Example

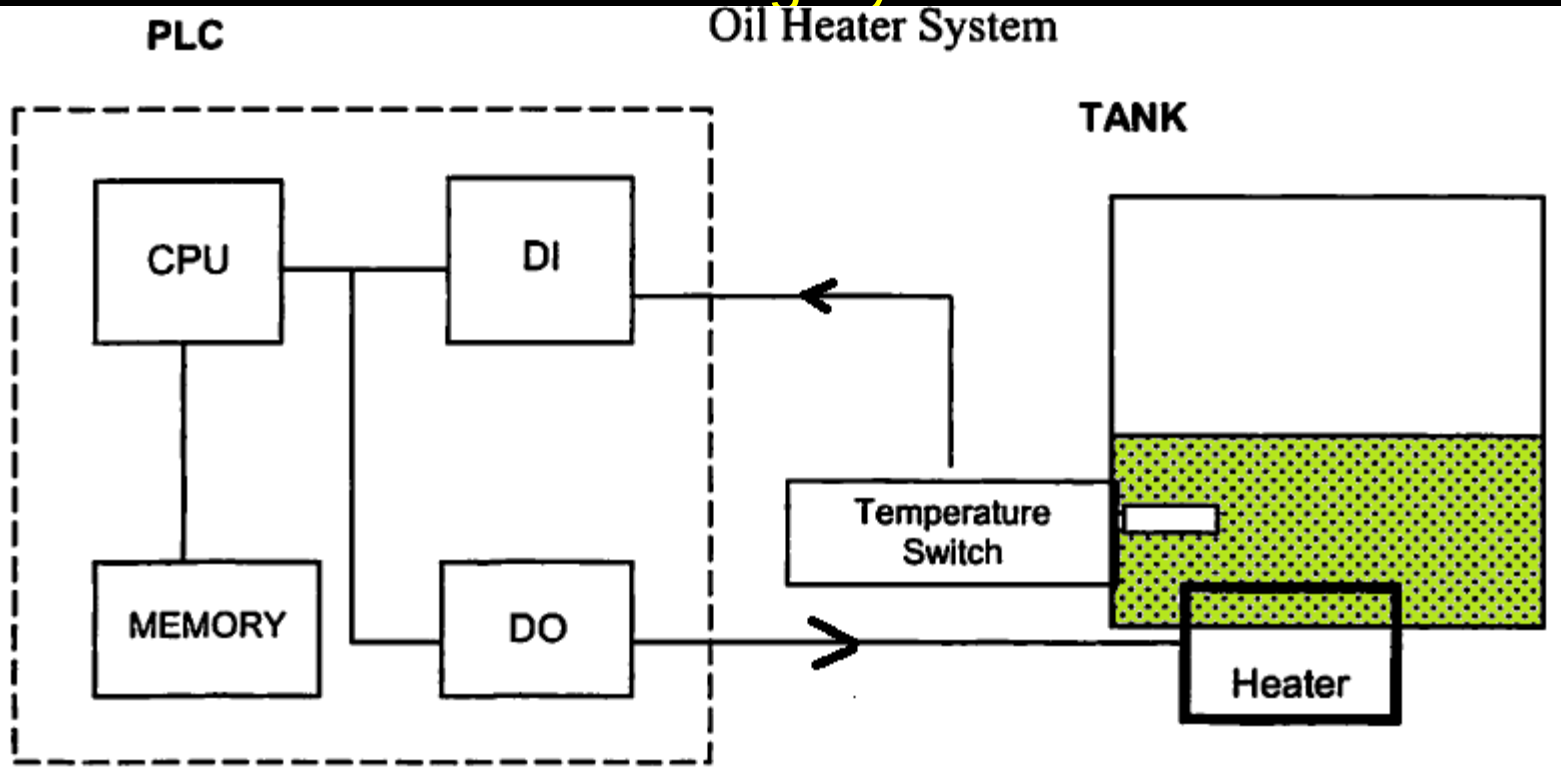
- Bottom-Up Method:
  - **1) Construct** a **fault tree**
  - 2**) Assign variable** names to all events **in the fault tree**
  - 3) Develop **probability** equations for all intermediate events and the top event
  - 4) Numerically e**valuate the equations to calculate the top event probability**
- Illustration of the Bottom-Up Method
  - Oil Heating System



Sensor: If the Temp is at or above a desired level Td, the Temp Switch indicates "OFF", otherwise, Temp Switch indciates "ON"

PLC: If the Sensor Swith is in "OFF", send out command to the Heater to turn ON Otherwise, send out comannd to the heather to turn OFF

Oil Heating System



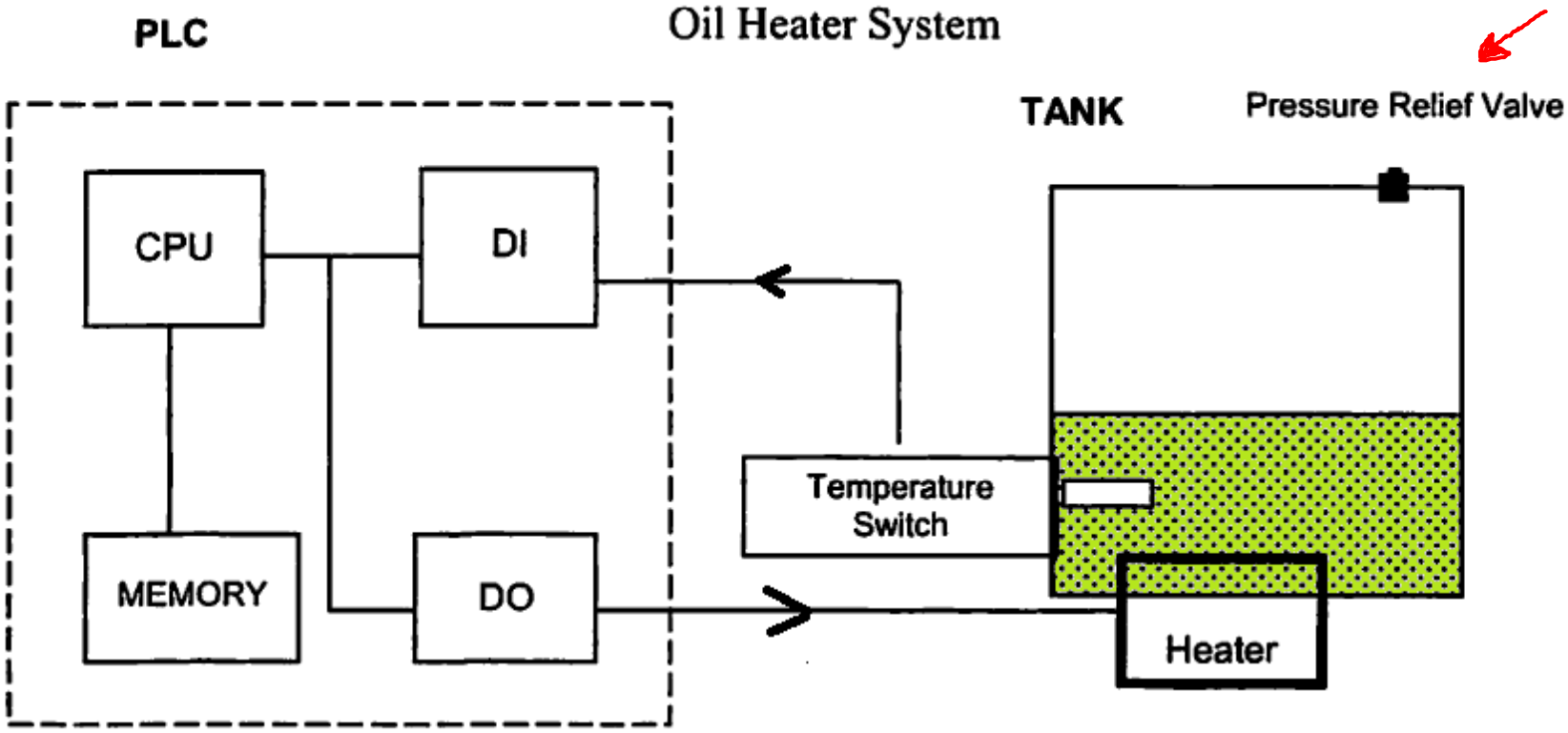
Sensor: If the Temp is at or above a desired level Td, the Temp Switch indicates "OFF", otherwise, Temp Switch indciates "ON"

PLC: If the Sensor Swith is in "OFF", send out command to the Heater to turn ON Otherwise, send out comannd to the heather to turn OFF

- Safety Concern (Mishap): **Tank rupture** by oil overheat and boiling caused by **heater staying in the ON state**

Oil Heating System – Safety Measure

- A pressure relief valve is installed at the tank
- Excessive pressure will open the valve and relieve the excessive pressure



Sensor: If the Temp is at or above a desired level Td, the Temp Switch indicates "OFF", otherwise, Temp Switch indciates "ON"

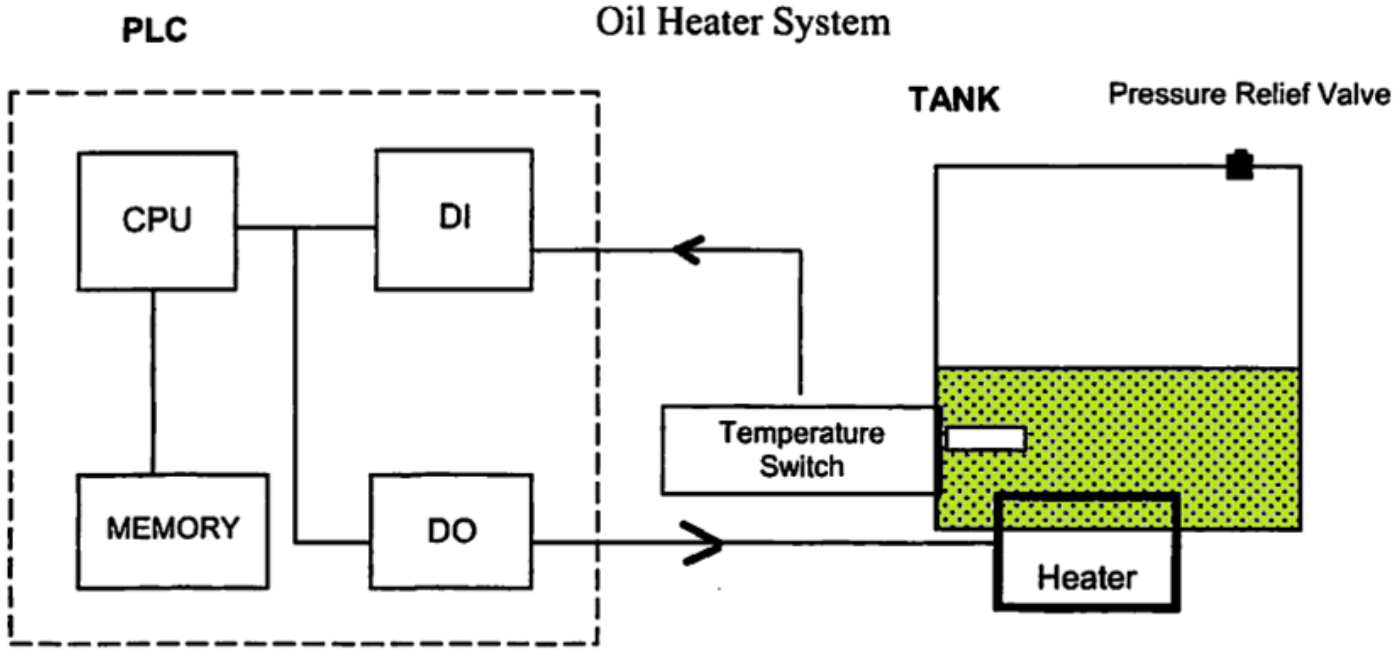
PLC: If the Sensor Swith is in "OFF", send out command to the Heater to turn ON Otherwise, send out comannd to the heather to turn OFF

Oil Heating System

- Safety Concerns (after the safety measure): A failure causing the oil to overheat AND a failure of the relief valve such that the **tank ruptures**

Exercise: Fault Tree Construction

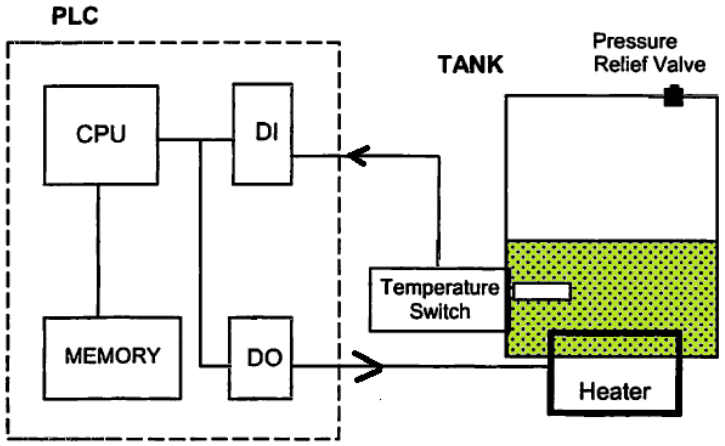
- Safety Concerns (after the safety measure): A failure causing the oil to overheat AND a failure of the relief valve which lead to **tank rupture**
- **Top Event : "Tank Rupture" → Construct a fault tree for the event**



Sensor: If the Temp is at or above a desired level Td, the Temp Switch indicates "OFF", otherwise, Temp Switch indciates "ON"

PLC: If the Sensor Swith is in "OFF", send out command to the Heater to turn ON Otherwise, send out comannd to the heather to turn OFF

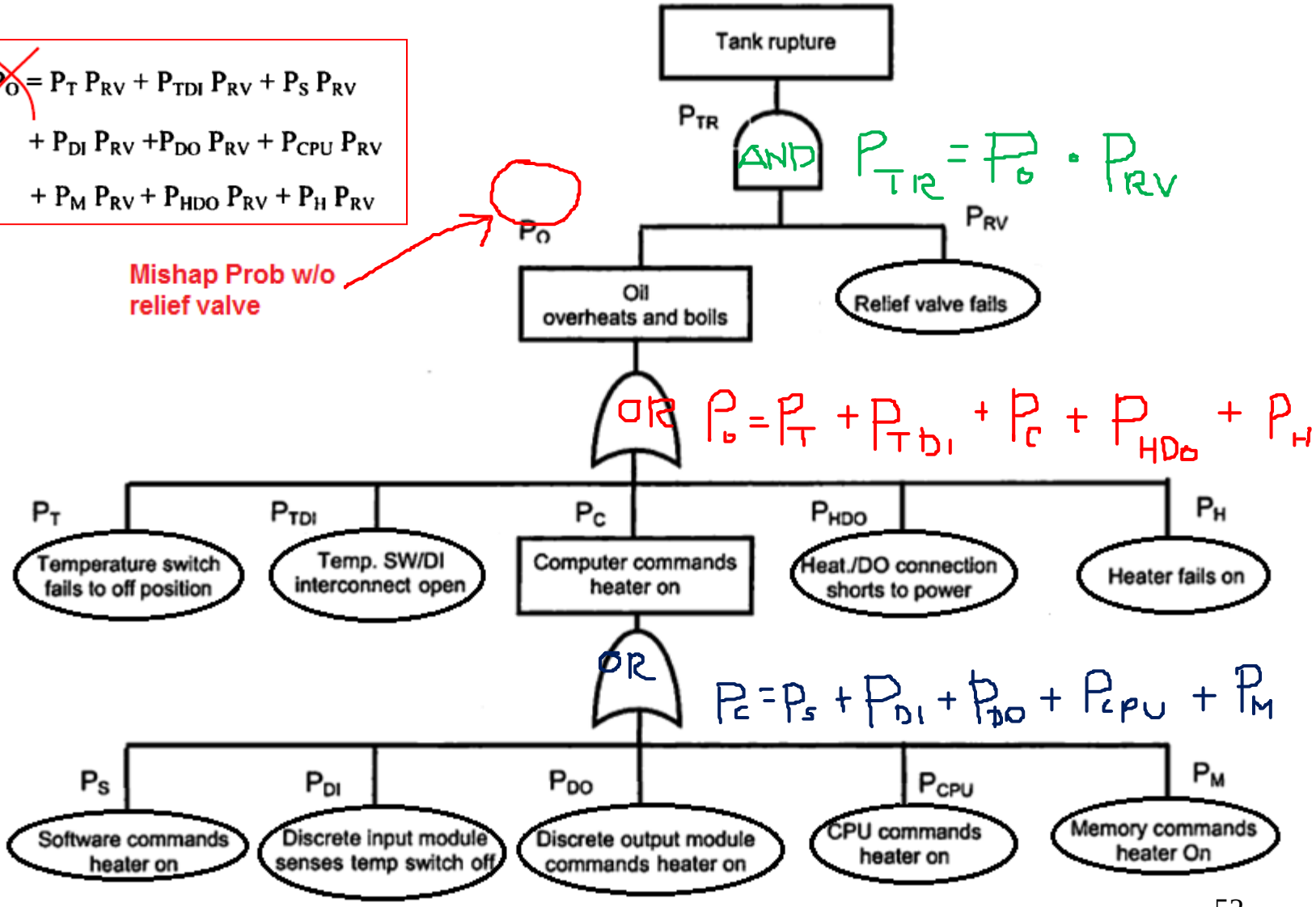
1) Fault Tree with Assigned Variables to the Events



2) Writing the Equations

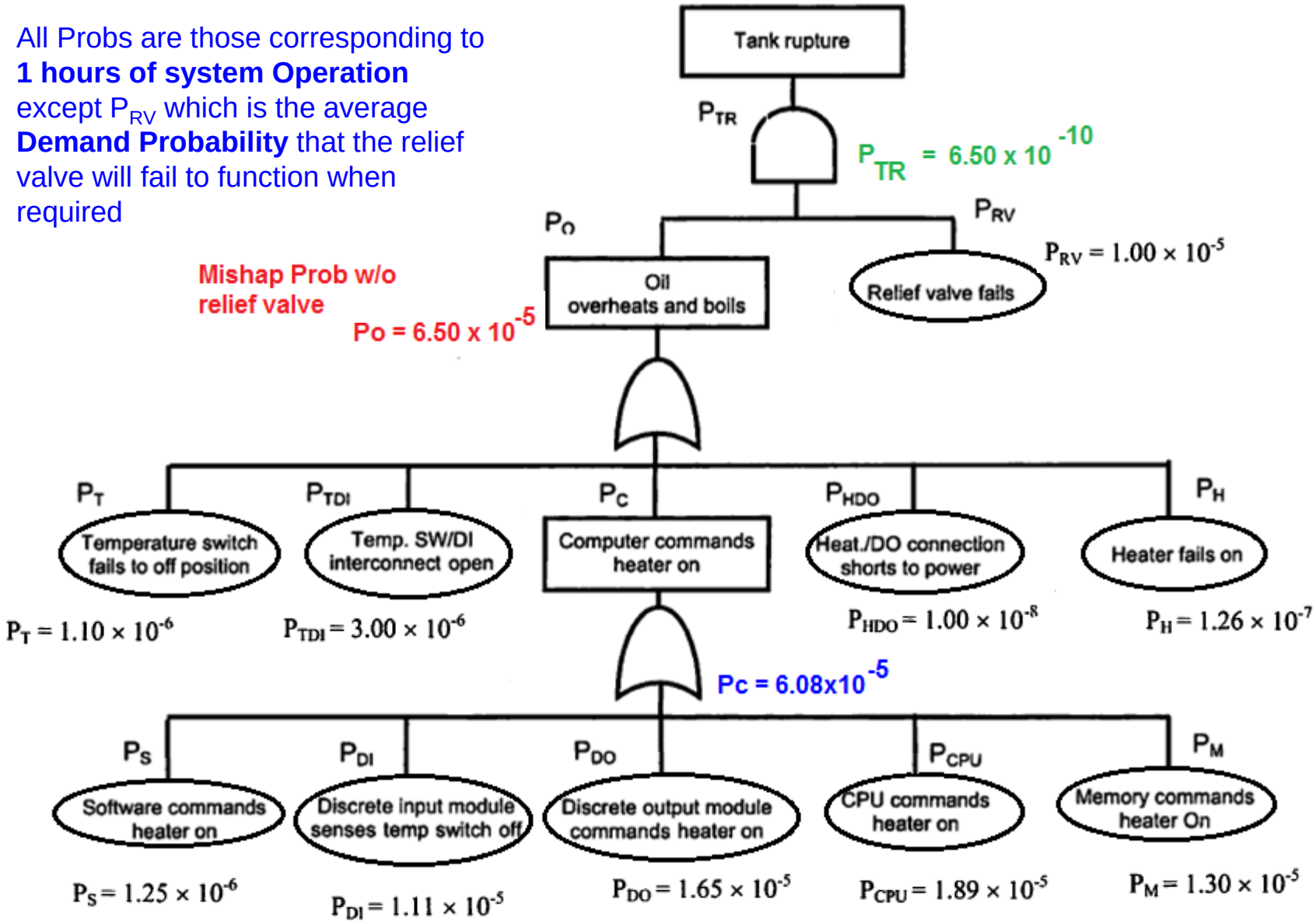
$$P_{TR} = P_O = P_T P_{RV} + P_{TDI} P_{RV} + P_S P_{RV} + P_{DI} P_{RV} + P_{DO} P_{RV} + P_{CPU} P_{RV} + P_M P_{RV} + P_{HDO} P_{RV} + P_H P_{RV}$$

Mishap Prob w/o relief valve



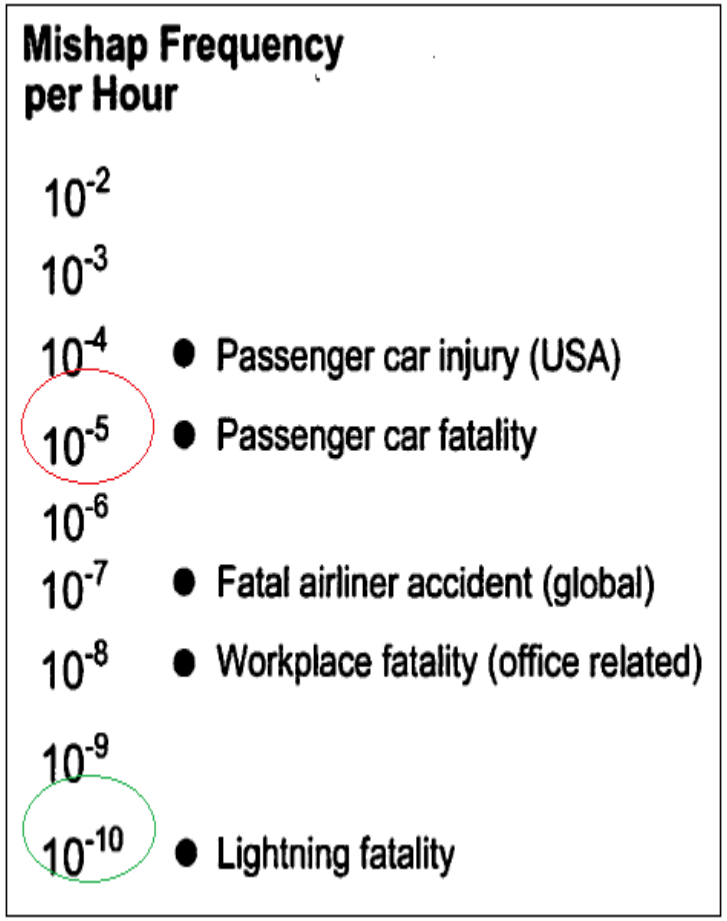
3) Combining Probabilities

- All Probs are those corresponding to **1 hours of system Operation** except P_{RV} which is the average **Demand Probability** that the relief valve will fail to function when required



Interpretation of Risk Analysis Result

- Mishap Probability of the Oil Heating System without relief valve: P_o = 6.50×10^{-5} → "Unsafe" for an industrial application
- Mishap Probability of the Oil Heating System with the relief valve: P_{TR} = 6.50×10^{-10} → "Safe" for an industrial application
- CAVEAT:
  - The probability calculated is based on a **model** of a heating system – **Not the actual** system itself
  - **Accuracy and quality** must be assured representing the basic events in the fault tree



Final Exam

- Time and Date:
  - 2:00 – 4:00pm Thursday, December 4, 2014 (in class)
  - Closed source exam
- Objectives
  - Understanding a situation which involves a mishap or accident
  - Logical thinking for sorting out cause-effect chains
  - Construction of a fault tree
  - Inclusion of safety measures to make a system fail safe
  - Relevant chapters: 3, **4, and 5**