Chapter 5: Design Evaluation of Safety-Critical Computer Systems

Howard University Department of Electrical and Computer Engineering

EECE 692 System Safety

Isaac Collins

Overview

- Design Evaluation Methods
  - Qualitative Analyses
    - Failure Modes and Effects Analysis (FMEA)
    - Fault Tree Analysis (FTA)
    - Event Tree Analysis (ETA)
  - Risk Analysis (RA)
  - Operation Hazard Analysis (OHA)
  - Failure Modes and Effects Testing (FMET)

Design Evaluation Methods

- Failure Modes and Effects Analysis
  - ▫ Look at each component, how will they fail, what are the effects?
- Fault Tree Analysis
  - ▫ Start with mishap, work down
- Risk Analysis
- Failure Modes and Effects Testing

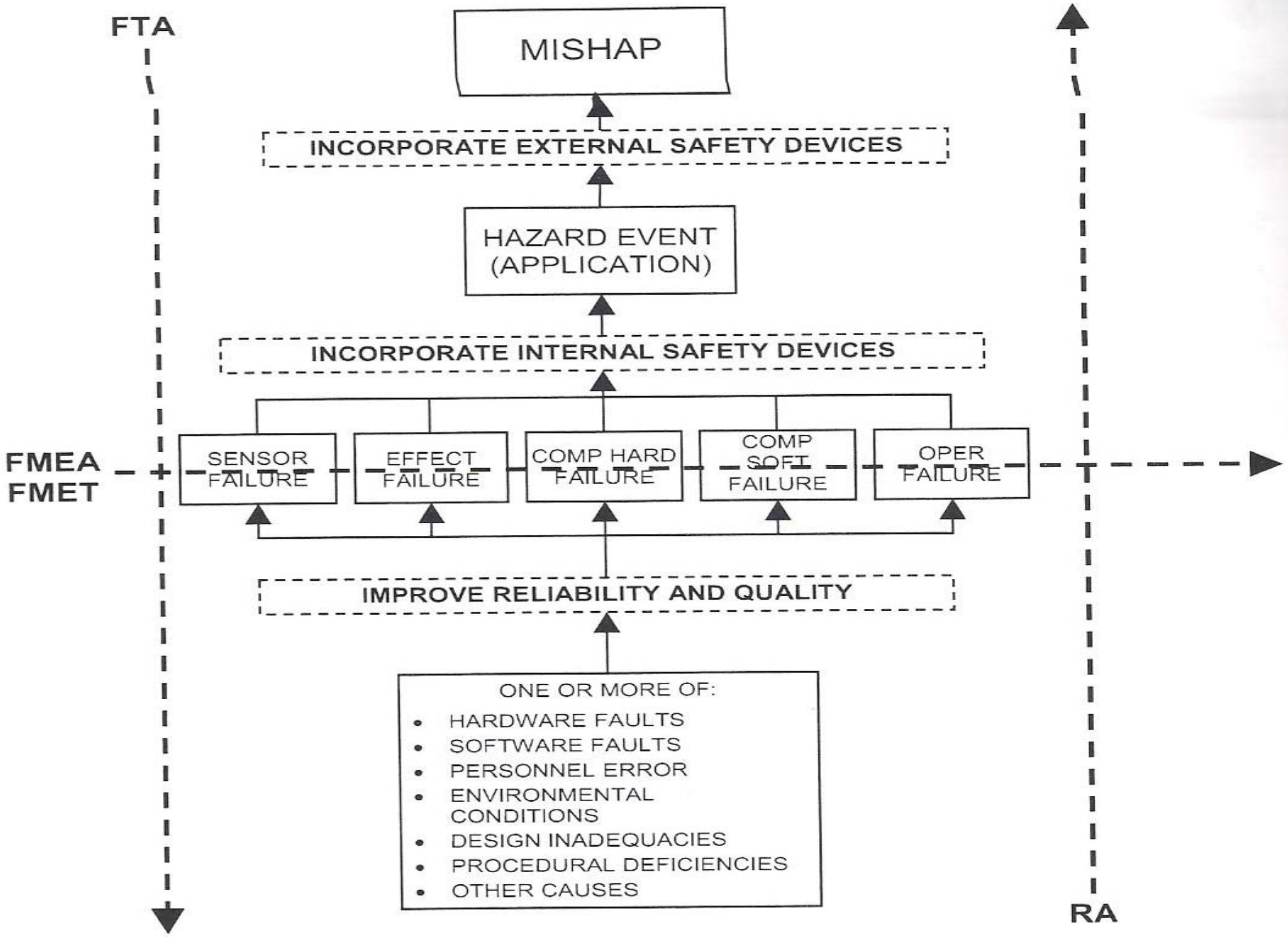
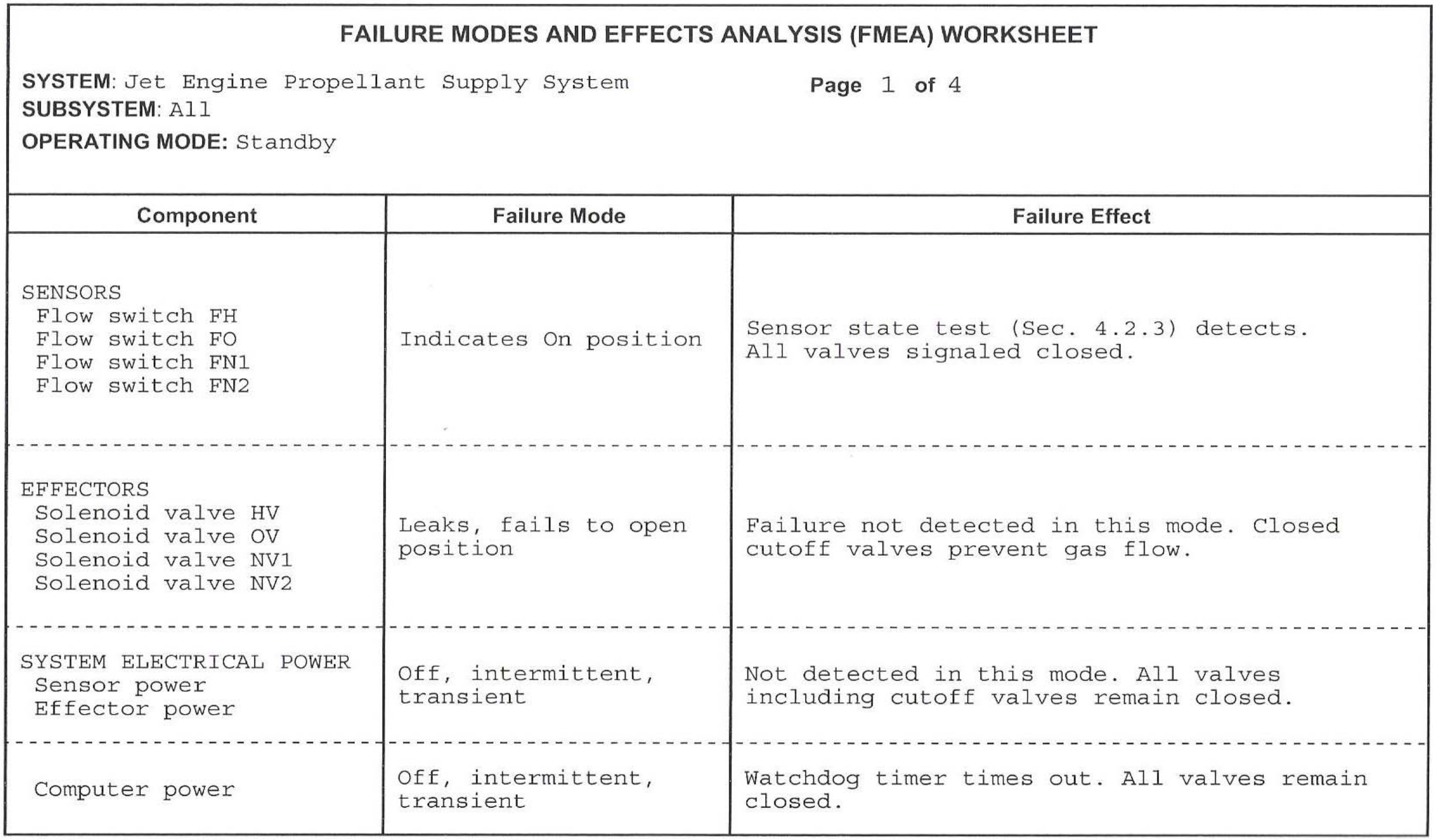


Figure 5.1 Design Evaluation Methods

Qualitative Analyses: Modes and Effects Analysis (FMEA)

- Think on a “What happens if…” basis
- Identify hazards, verify that no component will lead directly to mishap
- Common to start FMEA after design is finished: WRONG!
- Any safety-critical system is required to investigate effects of all component failure modes

Table 5.2 FMEA of 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 Effect
SENSORS Flow switch FH Flow switch FO Flow switch FN1 Flow switch FN2	Indicates On position	Sensor state test (Sec. 4.2.3) 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.

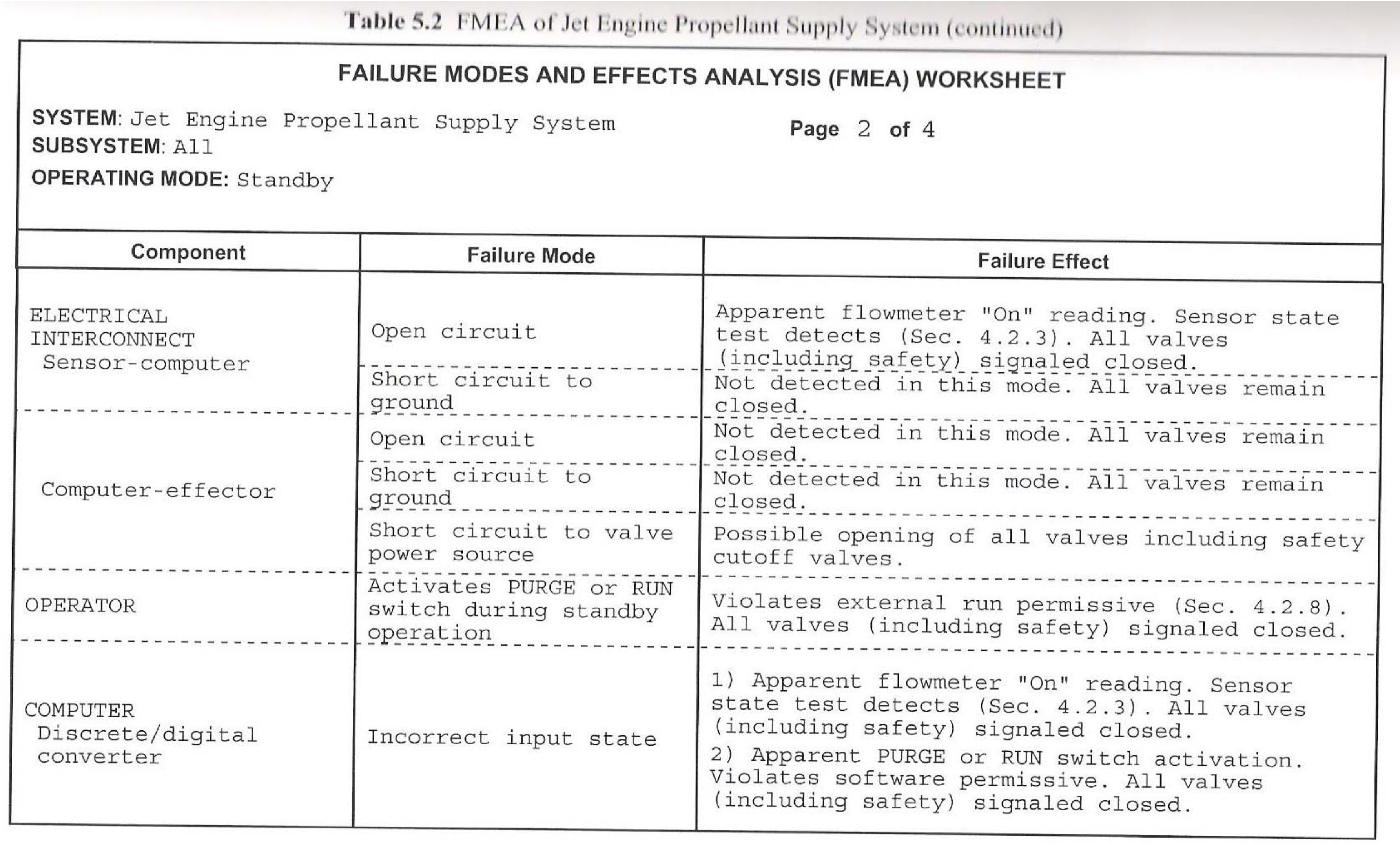


Table 5.2 FMEA of Jet Engine Propellant Supply System (continued)

FAILURE MODES AND EFFECTS ANALYSIS (FMEA) WORKSHEET

SYSTEM: Jet Engine Propellant Supply System

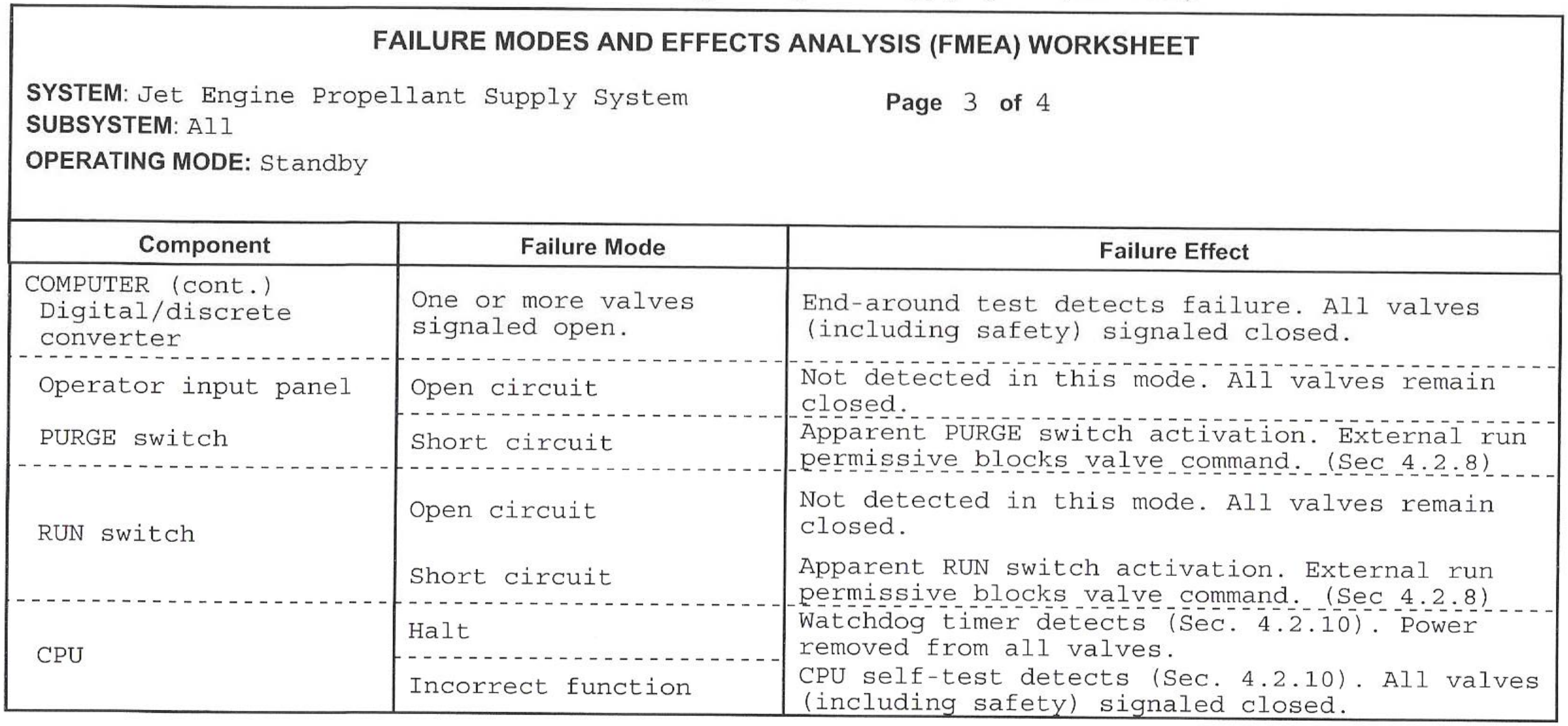
SUBSYSTEM: All

OPERATING MODE: Standby

Page 2 **of** 4

Component	Failure Mode	Failure Effect
ELECTRICAL INTERCONNECT Sensor-computer	Open circuit	Apparent flowmeter "On" reading. Sensor state test detects (Sec. 4.2.3). 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 (Sec. 4.2.8). All valves (including safety) signaled closed.
COMPUTER Discrete/digital converter	Incorrect input state	1) Apparent flowmeter "On" reading. Sensor state test detects (Sec. 4.2.3). All valves (including safety) signaled closed. 2) Apparent PURGE or RUN switch activation. Violates software permissive. All valves (including safety) signaled closed.

Table 5.2 FMEA of Jet Engine Propellant Supply System (continued)



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
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. (Sec 4.2.8)
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. (Sec 4.2.8)
CPU	Halt	Watchdog timer detects (Sec. 4.2.10). Power removed from all valves.
	Incorrect function	CPU self-test detects (Sec. 4.2.10). All valves (including safety) signaled closed.

Qualitative Analyses: Modes and Effects Analysis (FMEA) cont'd

- FMEA screens the effectiveness of modified design's safety measures
- Potentially identify hazards that may have been overlooked in preliminary analysis
- Limitation: only looks at system response to single failures, not multiple.
- When human safety is involved, FMEA is good first step, but not enough…

Qualitative Analyses: Modes and Effects Analysis (FMEA)

- Single-Points-of-Failure
  - Introduced when actual components are wired together
- Failure Modes, Effects, and Criticality Analysis (FMECA)
  - FMEA where level of criticality is assigned
    - Scale of how much harm can be done

Qualitative Analyses: Fault Tree Analysis (FTA)

- Fault Tree Analysis
  - Reverse of FMEA – start with mishap
  - Graphical Technique
    - Graph is “fault tree”

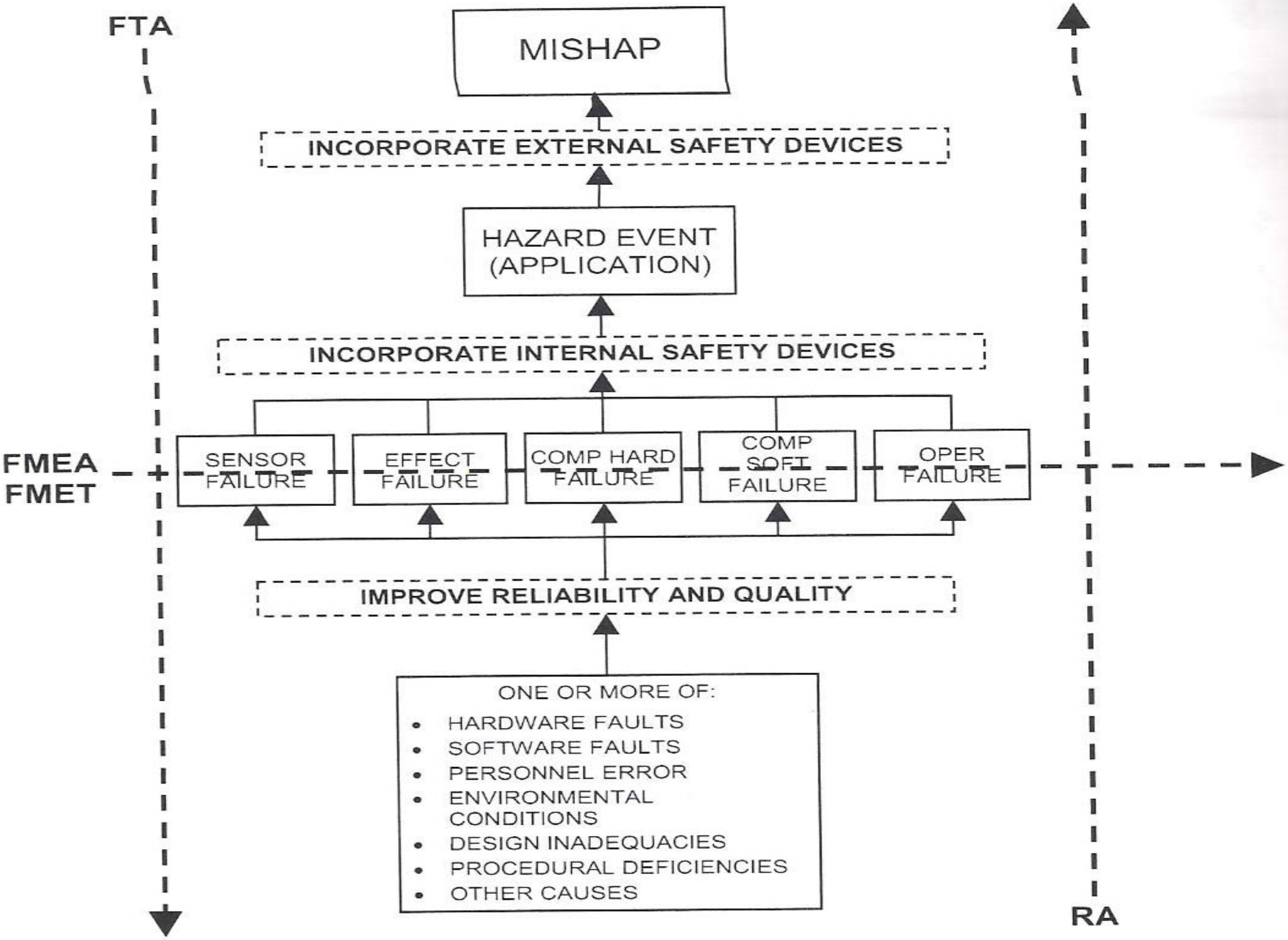
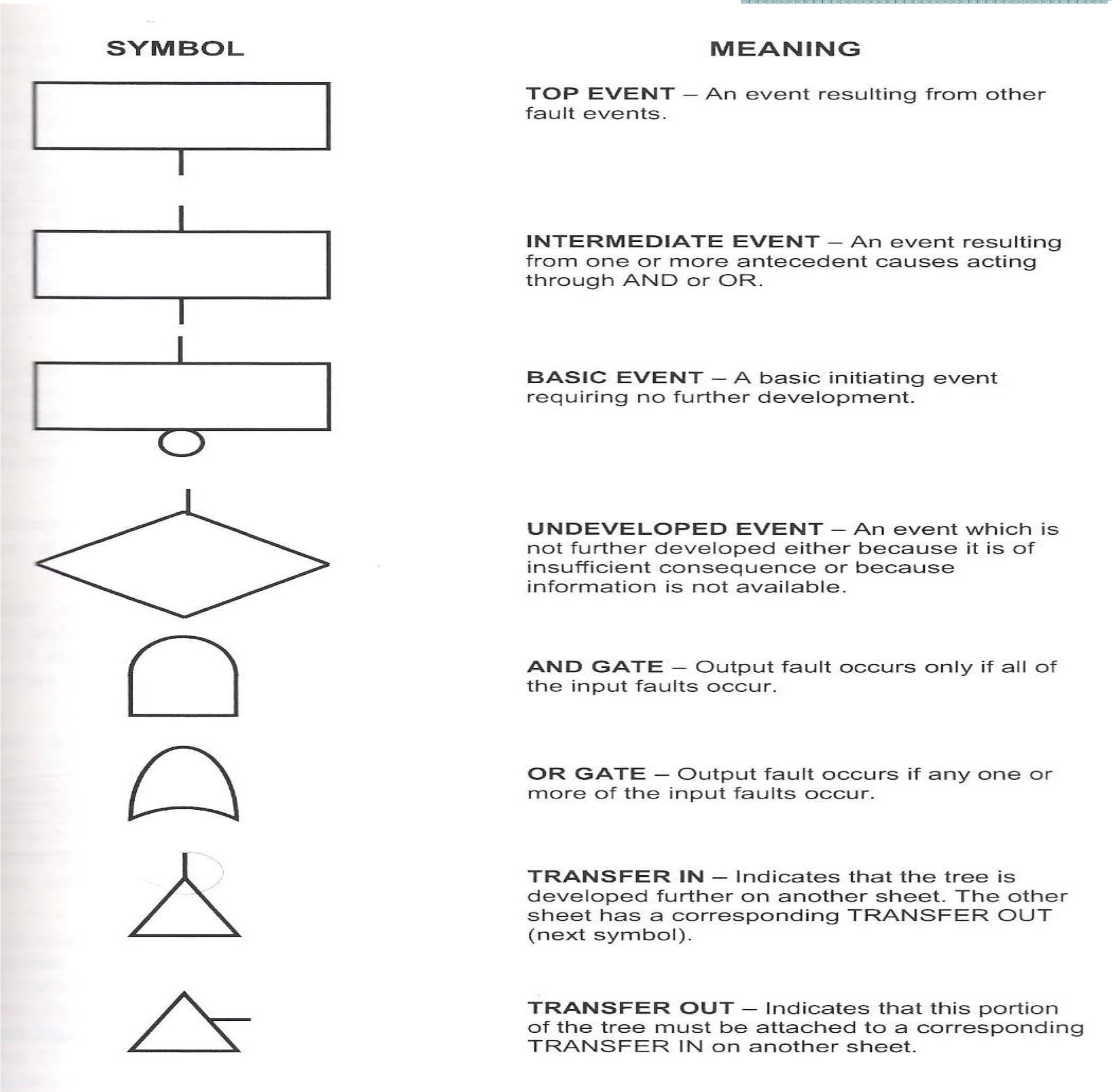


Figure 5.1 Design Evaluation Methods



SYMBOL **MEANING**

TOP EVENT – An event resulting from other fault events.

INTERMEDIATE EVENT – An event resulting from one or more antecedent causes acting through AND or OR.

BASIC EVENT – A basic initiating event requiring no further development.

UNDEVELOPED EVENT – An event which is not further developed either because it is of insufficient consequence or because information is not available.

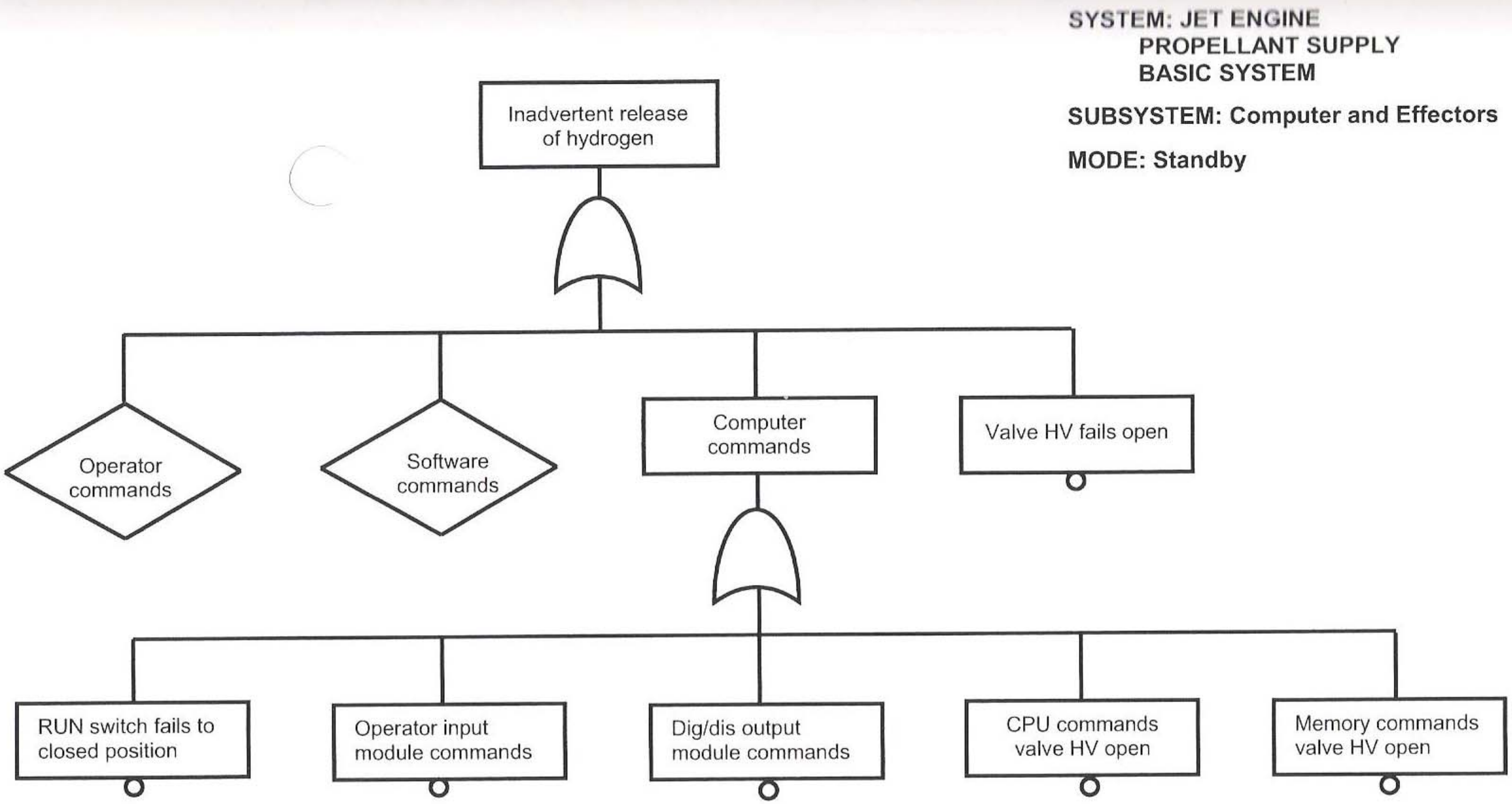
AND GATE – Output fault occurs only if all of the input faults occur.

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. The other sheet has a corresponding TRANSFER OUT (next symbol).

TRANSFER OUT – Indicates that this portion of the tree must be attached to a corresponding TRANSFER IN on another sheet.

Figure 5.2 Fault Tree Symbols



SYSTEM: JET ENGINE
PROPELLANT SUPPLY
BASIC SYSTEM

SUBSYSTEM: Computer and Effectors

MODE: Standby

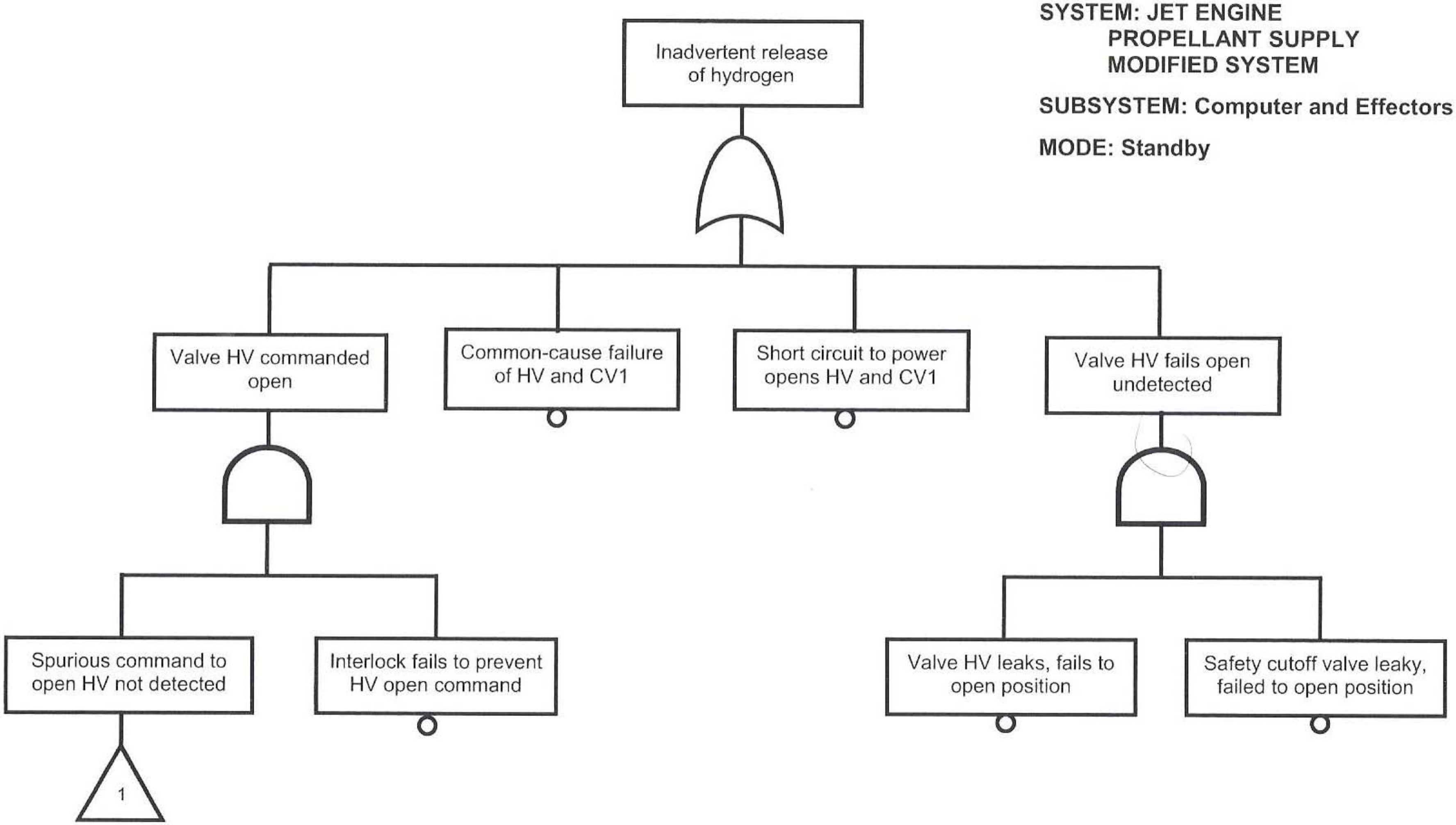
Inadvertent release of hydrogen
Operator commands
Software commands
Computer commands
Valve HV fails open
RUN switch fails to closed position
Operator input module commands
Dig/dis output module commands
CPU commands valve HV open
Memory commands valve HV open

Figure 5.3 A Fault Tree for Basic Propellant Supply System

SYSTEM: JET ENGINE
PROPELLANT SUPPLY
MODIFIED SYSTEM

SUBSYSTEM: Computer and Effectors

MODE: Standby



Inadvertent release of hydrogen

Valve HV commanded open

Common-cause failure of HV and CV1

Short circuit to power opens HV and CV1

Valve HV fails open undetected

Spurious command to open HV not detected

Interlock fails to prevent HV open command

Valve HV leaks, fails to open position

Safety cutoff valve leaky, failed to open position

1

To sheet 2

Figure 5.4 Fault Tree for Modified Propellant Supply System (Sheet 1 of 3)

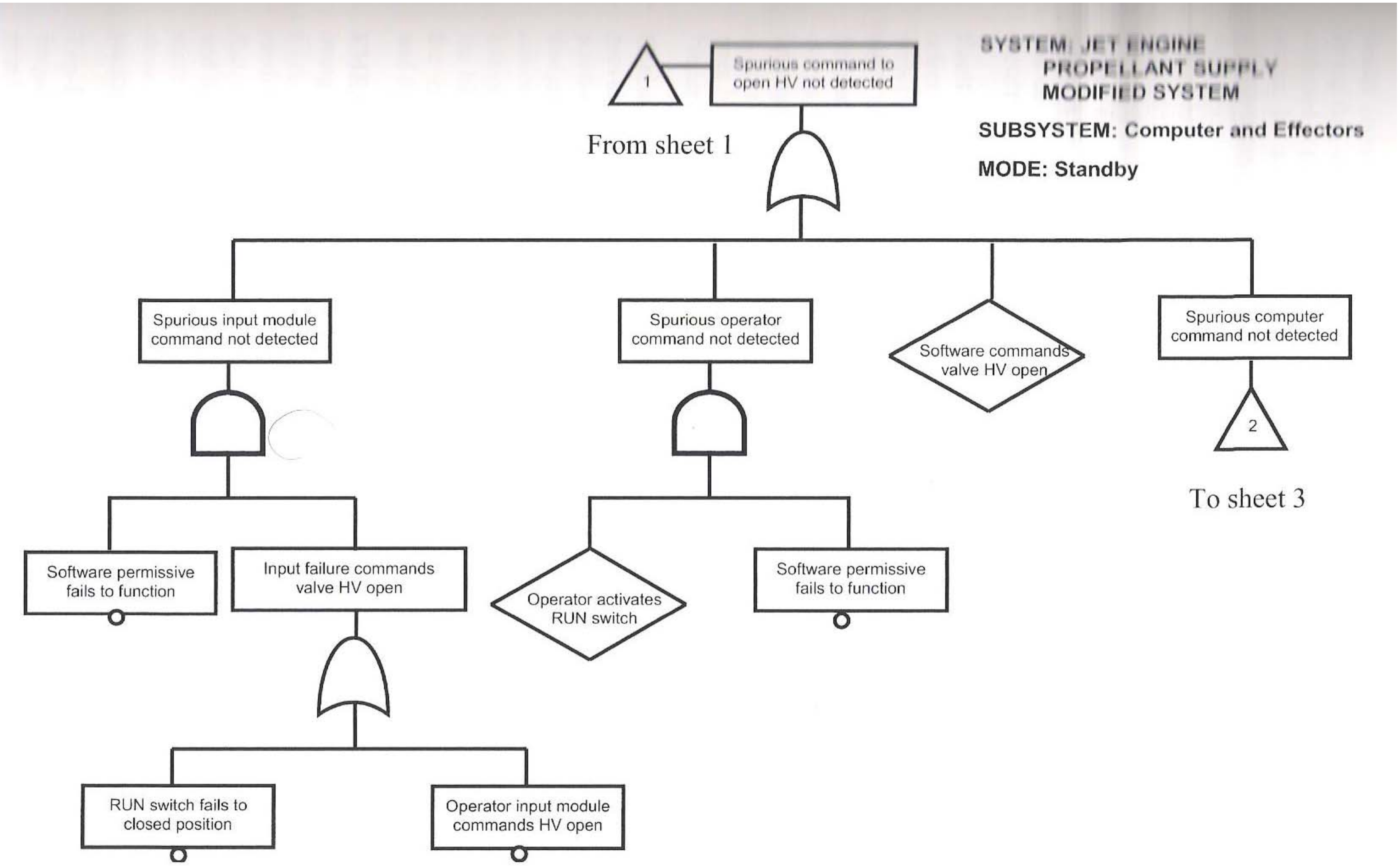
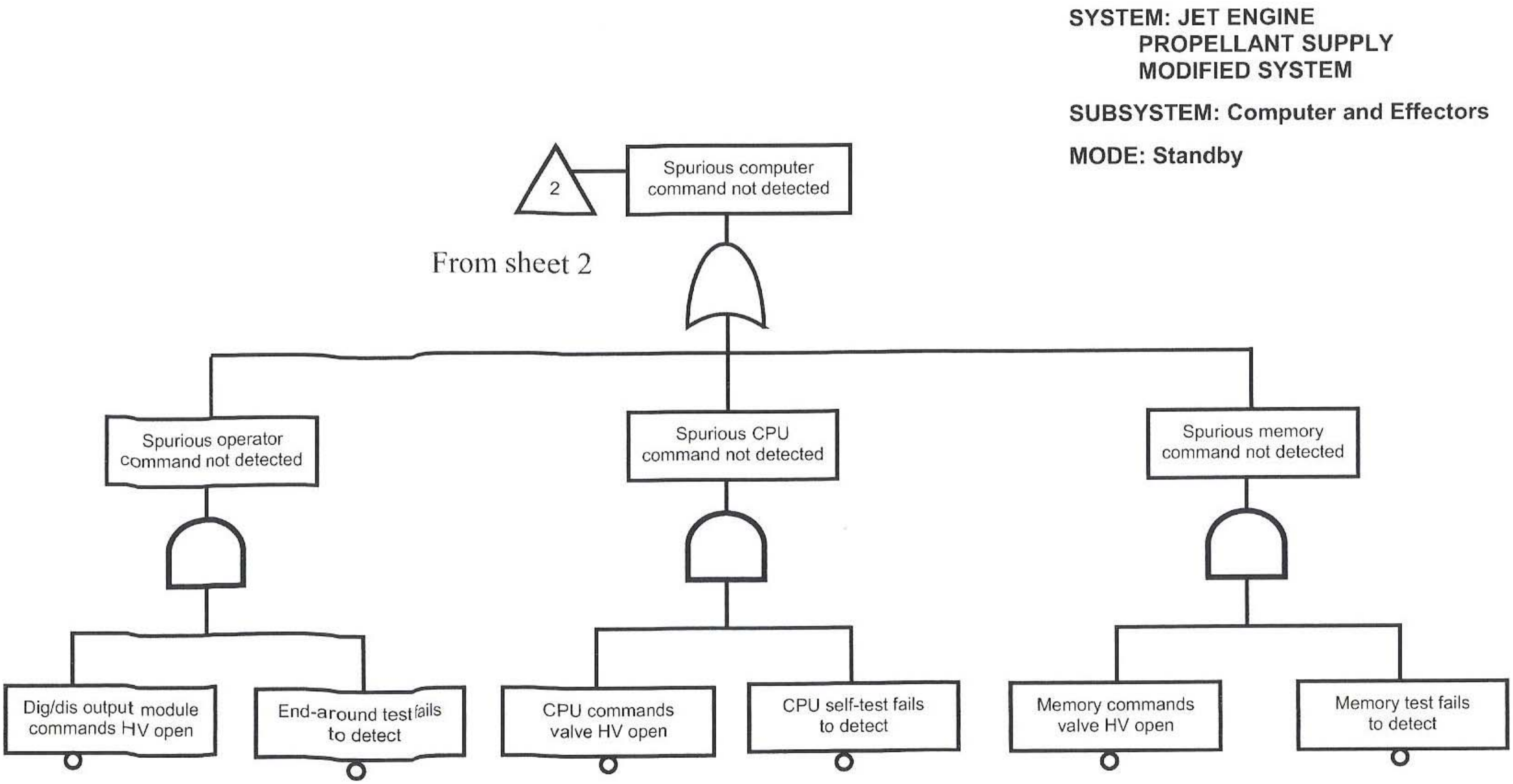

1
Spurious command to open HV not detected
From sheet 1
SYSTEM: JET ENGINE
PROPELLANT SUPPLY
MODIFIED SYSTEM
SUBSYSTEM: Computer and Effectors
MODE: Standby
Spurious input module command not detected
Spurious operator command not detected
Software commands valve HV open
Spurious computer command not detected
2
To sheet 3
Software permissive fails to function
Input failure commands valve HV open
Operator activates RUN switch
Software permissive fails to function
RUN switch fails to closed position
Operator input module commands HV open

Figure 5.4 Fault Tree for Modified Propellant Supply System (Sheet 2 of 3)



SYSTEM: JET ENGINE
PROPELLANT SUPPLY
MODIFIED SYSTEM

SUBSYSTEM: Computer and Effectors

MODE: Standby

2
From sheet 2
Spurious computer command not detected
Spurious operator command not detected
Spurious CPU command not detected
Spurious memory command not detected
Dig/dis output module commands HV open
End-around test fails to detect
CPU commands valve HV open
CPU self-test fails to detect
Memory commands valve HV open
Memory test fails to detect

Figure 5.4 Fault Tree for Modified Propellant Supply System (Sheet 3 of 3)

Qualitative Analyses: Fault Tree Analysis (FTA)

- Fault Tree vs Failures
  - Defect vs not performing correct function
  - Failure Tree?
- FMEA vs FTA
  - FTA represents multiple events, successive failures
  - Safety modifications can fail
  - More complex
- Top-Down vs Bottom Up Analysis
  - Deductive (why) vs Inductive (how)

Qualitative Analyses: Event Tree Analysis (ETA)

- Event Tree Analysis
  - ▫ Bottom-Up, more detailed than FMEA
    - Addresses sequence of failure events
    - Provides Event Tree
      - Response of system to initiating event

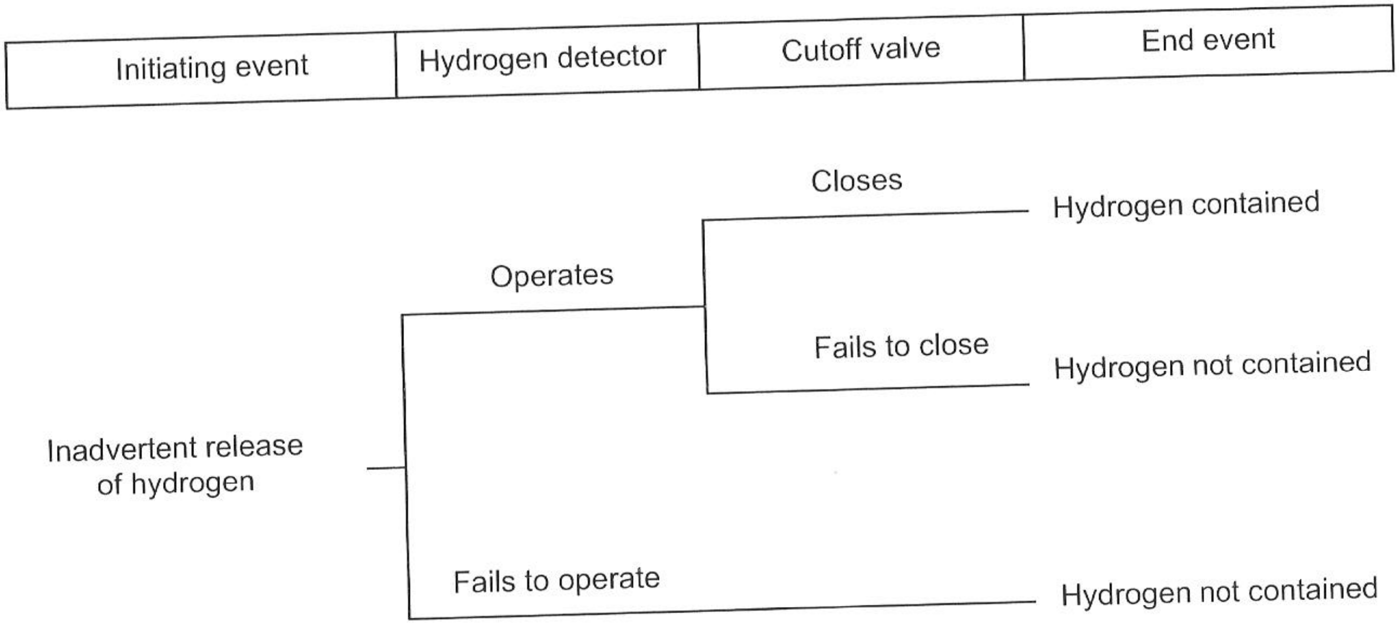


Figure 5.5 Event Tree for Propellant Supply System

Review

- Design Evaluation Methods
  - Qualitative Analyses
    - Failure Modes and Effects Analysis (FMEA)
    - Fault Tree Analysis (FTA)
    - Event Tree Analysis (ETA)
  - Risk Analysis (RA)
  - Operational Hazard Analysis (OHA)
  - Failure Modes and Effects Testing (FMET)