Chapter 5: Design Evaluation of Safety-Critical Computer Systems, continued

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)
  - Failure Modes and Effects Testing (FMET)

Risk Analysis: Mishap Risk

- Mishap Severity (in terms of dollar loss, extent of damage to environment, and human suffering):
  - Catastrophic
  - Critical
  - Marginal
  - Negligible
- Have meaning within context of application
  - Start with mishap, work down

Risk Analysis: Mishap Risk

- Mishap Probability:
  - Probability of occurrence of event/hazard that create mishap
  - Ratio of number of undesirable events to total number of possible events (including desirable and undesirable)
    - P(n events occur) = n/N
    - n is equally likely (independent)

- Diesel Generator Example

Risk Analysis: Mishap Risk

- Diesel Generator Example:
  - 356 systems tested in simulated emergency condition
  - 4 fail to start
  - Probability that untested generator fails:

$$4/356 = 1.1 \times 10^{-2}$$

- Each system in actual test must be exactly the same condition
  - Maintenance, battery condition, fuel quality, ambient temperature, etc.

- MUST have large enough sample size…

Risk Analysis: Mishap Frequency

- Measures used to express mishap probability:
  - Probability per unit of time (hr./lifetime of operation)
  - Number of occurrences per unit of time (hr./year/lifetime)
  - Number of occurrences per event, population, item, or activity

- EXAMPLE 5.6

Risk Analysis: Component Failure

- Equation relating component failure probability and failure rate:

  (5.1)

- Assumptions:
  - Component works at time t=0 (at initialization)
  - Constant failure rates
- Used to model HW/SW failure behavior.
- EXAMPLE 5.7

Risk Analysis: Probability Approximation

Table 5.3 Approximate Versus Exact Probability Values

T (hours)	λT	P(approx.)	P (exact)
1	0.001	1.000×10^{-3}	1.000×10^{-3}
10	0.01	1.000×10^{-2}	0.995×10^{-2}
100	0.1	1.000×10^{-1}	0.952×10^{-1}
1000	1	1.000×10^{0}	0.632×10^{0}

Similar to Demand Failure Probability

EXAMPLE 5.10

Risk Analysis: Acceptable Risk Mishap

Mishap Frequency per Hour	Mishap
10^{-2}	
10^{-3}	
10^{-4}	● Passenger car injury (USA)
10^{-5}	● Passenger car fatality
10^{-6}	
10^{-7}	● Fatal airliner accident (global)
10^{-8}	● Workplace fatality (office related)
10^{-9}	
10^{-10}	● Lightning fatality

Figure 5.6 Mishap Statistics (c. 1995)

Risk Analysis: Calculating Mishap Risk Probability

- Risk Analysis Step 1 (already covered):
  - Use Fault Tree Analysis to trace mishap back to failure events/faults
- Risk Analysis Step 2:
  - Determine probability of each failure/fault
- Risk Analysis Step 3 (we'll start here):
  - Combine probabilities to yield mishap probability

Risk Analysis: Oil Heater System Example

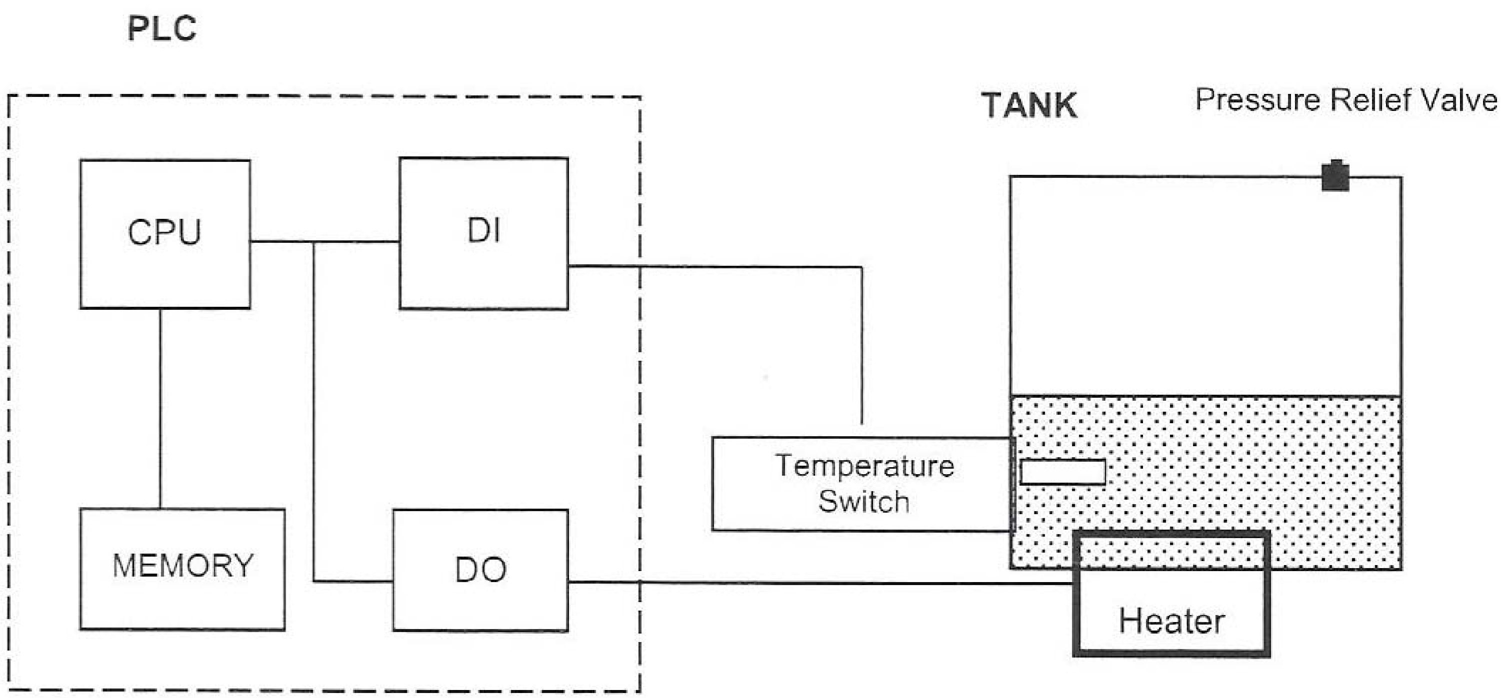

Figure 5.7 Oil Heater System

Risk Analysis: Oil Heater System Example

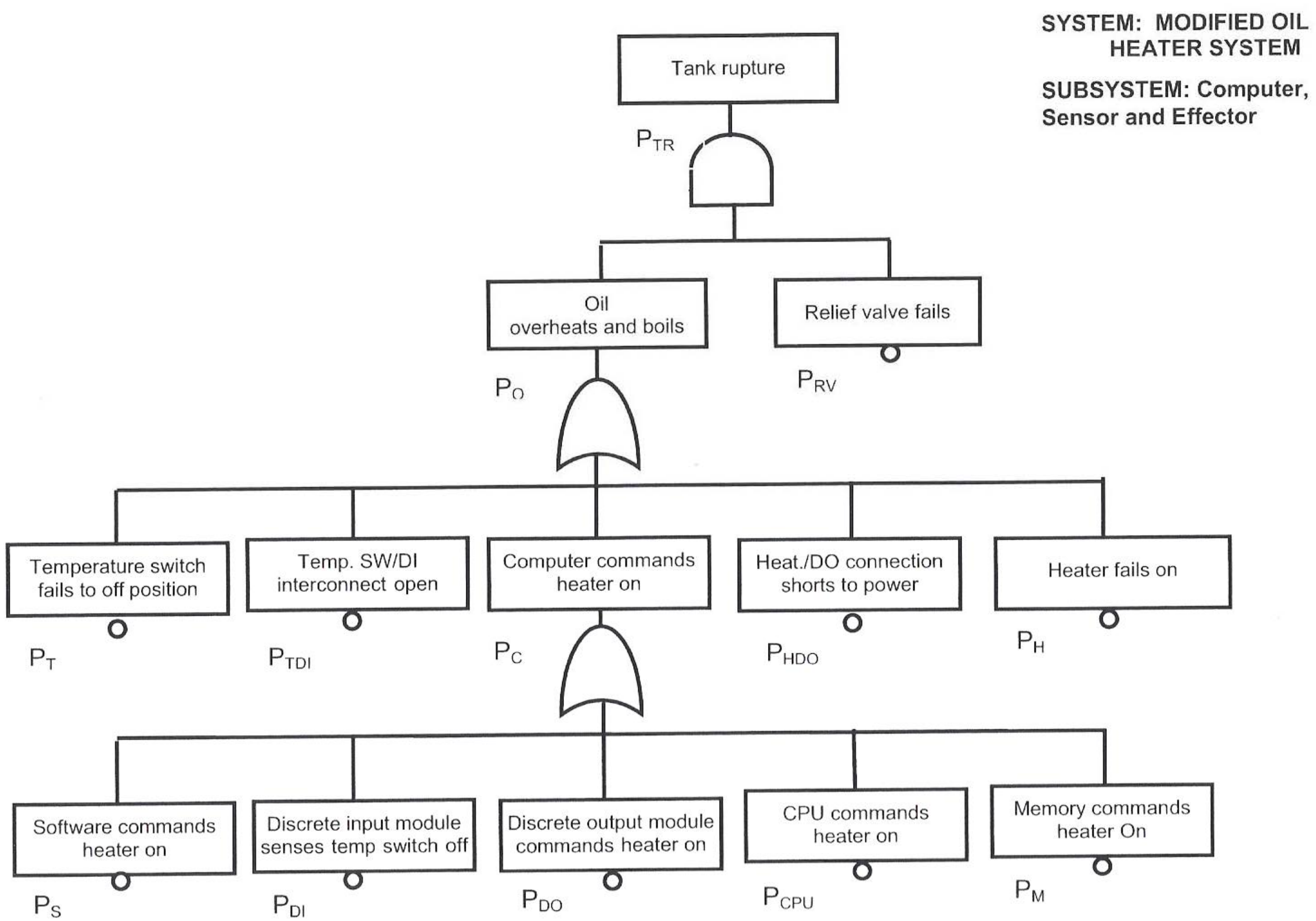

Figure 5.8 Fault Tree for Oil Heater Computer System

Risk Analysis: Excess Variables - More Boolean Algebra

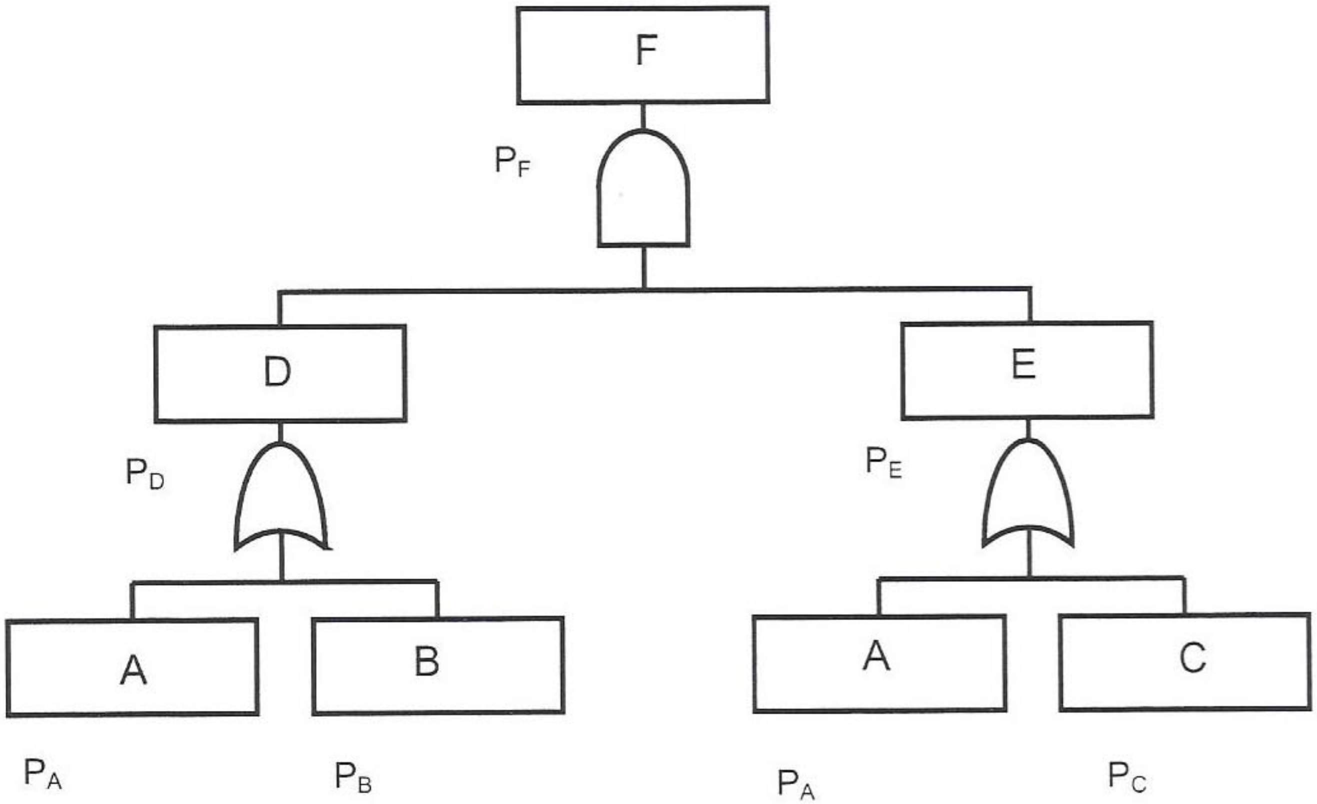

Figure 5.9 Fault Tree for Excess Variable Illustration

Risk Analysis: Quantifying Failure Modes

- Two Types of Probabilities:
  - The given HW component fails in given failure mode in given period of time
  - Demand probability of HW component will fail to perform intended safety function

- Generic data used in design phase
  - Sources available include:
    - Failure Rates
    - Failure Mode Distributions
    - Demand Failure Probabilities

Risk Analysis: Probabilistic Risk Assessment (PRA)

- Characterized by probability distribution
  - Provides average of data values
  - Provides measure of data dispersion (variance)
- PRA analysts generally use lognormal distribution
  - Overkill for little data/ lack of knowledge of components
- We will look at Nominal Value

$$V_{nom} = [V_{min} \times V_{max}]^{1/2}$$

Risk Analysis: (PRA) – Heater Example, again

- Source A: 7.0×10^{-8}/hr
- Source B: 5.2×10^{-7}/hr
- Source C: 3.8×10^{-6}/hr
- Source D: 2.8×10^{-5}/hr

- V_{nom} is Geometric Mean (represents middle value for wide range of data)
  - Not Arithmetic Mean (data with closer values)

Risk Analysis: (PRA) – Heater Example, Nominal Value Chart

Table 5.17 Component Data for Oil Heater Computer System Example

Component	Variable	Nominal Value	UF	Source in text
Software (100 lines; 10 year average)	P_S	1.25×10^{-6}	15	Eqn. 5.23
Discrete input	P_{DI}	1.11×10^{-5}	10	Table 5.6
Discrete output	P_{DO}	1.65×10^{-5}	10	Table 5.6
Processor	P_{CPU}	1.89×10^{-5}	10	Table 5.6
Memory	P_M	1.30×10^{-5}	10	Table 5.6
Temperature switch	P_T	1.10×10^{-6}	8	Table 5.4
Temp. sw./DI interconnect	P_{TDI}	3.00×10^{-6}	3	Table 5.7
Heater/DO interconnect	P_{HDO}	1.00×10^{-8}	10	Table 5.7
Electrical heater	P_H	1.26×10^{-7}	20	Table 5.5 & Table 5.11
Relief valve	P_{RV}	1.00×10^{-5}	3	Table 5.12

Risk Analysis: (PRA) – Nominal Value Failure Rates

Table 5.5 Effector Failure Rates – All Failure Modes
Commercial Ground-fixed Environment

COMPONENT	FAILURE RATE Nominal Value (Geometric Mean)	UF
Actuator, hydraulic	3.9×10^{-6}/hr	129
Clutch	6.5×10^{-7}/hr	22
Electric motor, DC	1.7×10^{-5}/hr	12
Heater, electrical	1.4×10^{-6}/hr	20
Pump, hydraulic	1.1×10^{-5}/hr	4
Pump, centrifugal	1.3×10^{-5}/hr	4
Relay, electromagnetic	5.2×10^{-7}/hr	41
Relay – fail to contact	3.2×10^{-7}/hr	3
Relay – short across contact	1.0×10^{-8}/hr	10
Relay – open contact	9.5×10^{-8}/hr	3
Servo, DC	2.2×10^{-6}/hr	6
Solenoid, electric	1.3×10^{-6}/hr	3
Solid state relay	1.4×10^{-7}/hr	24
Valve, electric motor	2.2×10^{-6}/hr	224
Valve, pneumatic	1.1×10^{-6}/hr	11

Sources: IEEE 500, NPRD-95, Wash 1400.

Risk Analysis: (PRA) – Nominal Value Failure Rates – Computer Modules

Table 5.6 Failure Rates for Computer Modules – All Failure Modes
Commercial Ground-fixed Environment
Uncertainty Factor (UF) = 10

COMPONENT CATEGORY	MODULE	FAILURE RATE Nominal Value (Geometric Mean)
CPU and memory	Processor	18.9×10^{-6}/hr
	Memory	13.0×10^{-6}/hr
Effector output	Analog output	17.9×10^{-6}/hr
	Discrete output	16.5×10^{-6}/hr
	Relay output	9.2×10^{-6}/hr
	Triac output	33.8×10^{-6}/hr
Sensor input	A/D converter	10.4×10^{-6}/hr
	Analog input	15.5×10^{-6}/hr
	Discrete input	11.1×10^{-6}/hr
	Contact closure	10.6×10^{-6}/hr
Communications	Bus controller	19.8×10^{-6}/hr
Host electronics	Rack	2.6×10^{-6}/hr
	Electrical power supply	33.0×10^{-6}/hr

Data source: See discussion.

Safety Related Testing: Failure Modes and Effects Testing (FMET)

- Failures inserted 2 ways:
  - Physically insert (HW)
    - Sensor/Effector alteration
    - Can be costly, cause damage
  - Data Alteration
    - Alter Signals

Review

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