

# FAILURE AND CRITICALITY ANALYSIS

**ME 481 Senior Design I**

**Fall 2022**

**Dr. Trevor C. Sorensen**

# The Engineer's Crystal Ball



<https://clipground.com/pics/get>

# The Engineer's Crystal Ball

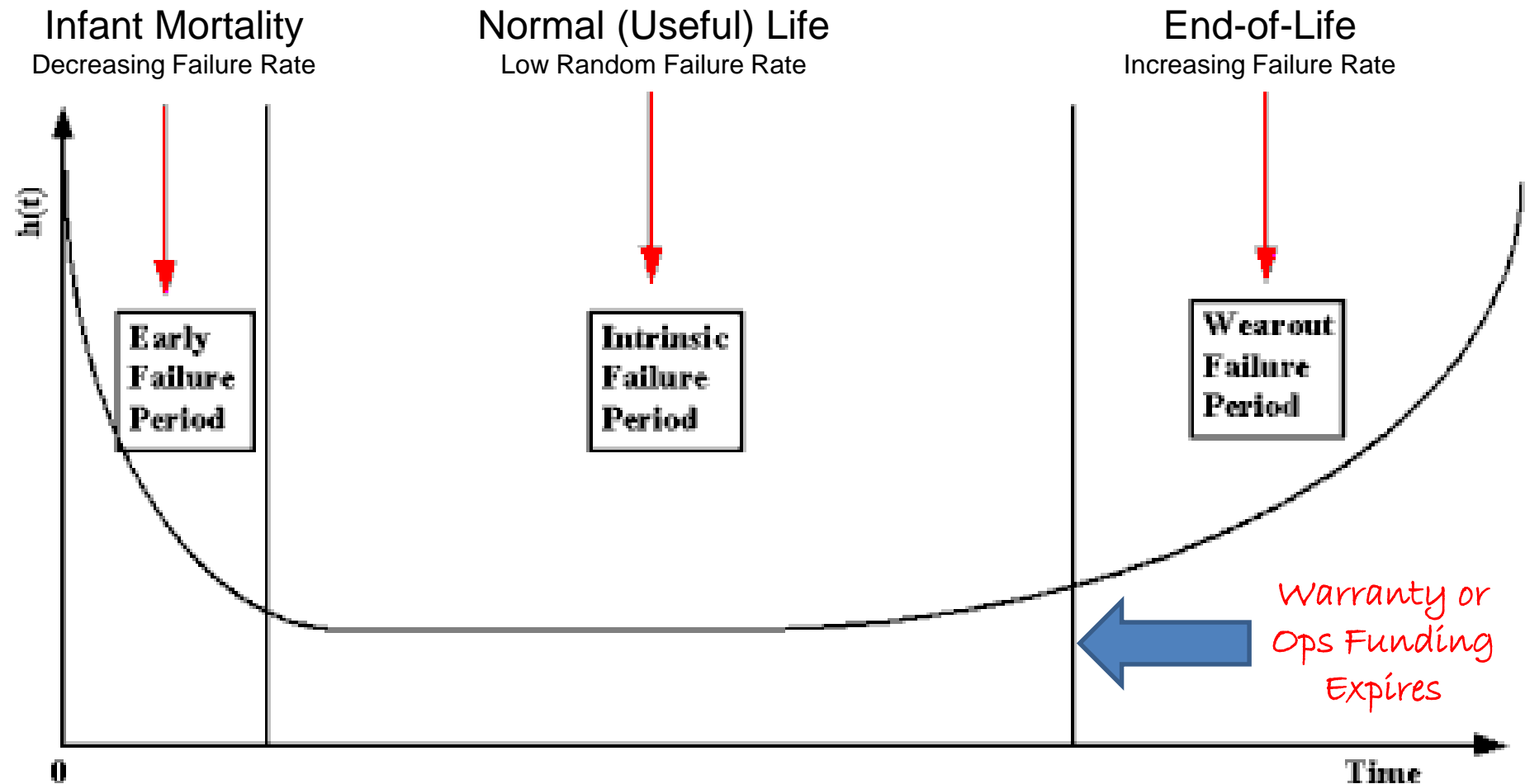
---

- *Quality* is a relative term often based on customer perception or the degree to which a product meets customer expectations
- Traditionally quality activities have focused on detecting manufacturing and material defects that cause failures early in the life cycle
- Today, activities focus on finding and preventing failures before they can occur

**Emphasis on Failure Prevention**

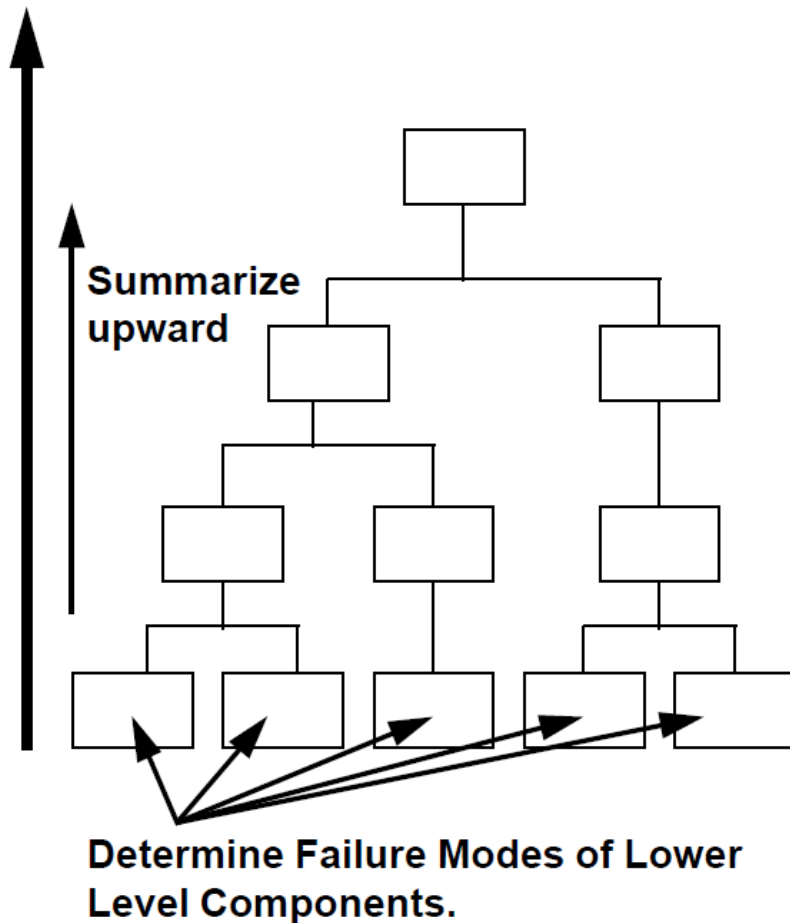
# The Engineer's Crystal Ball

## The Bathtub Curve

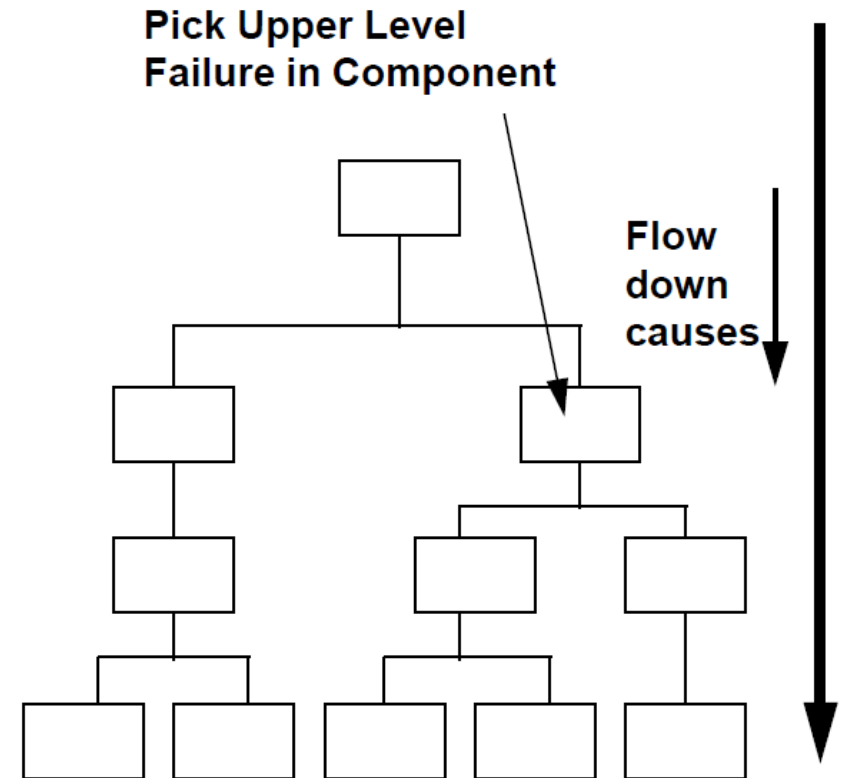


# The Engineer's Crystal Ball

## INDUCTIVE PROCEDURES (Bottom-Up Analysis)

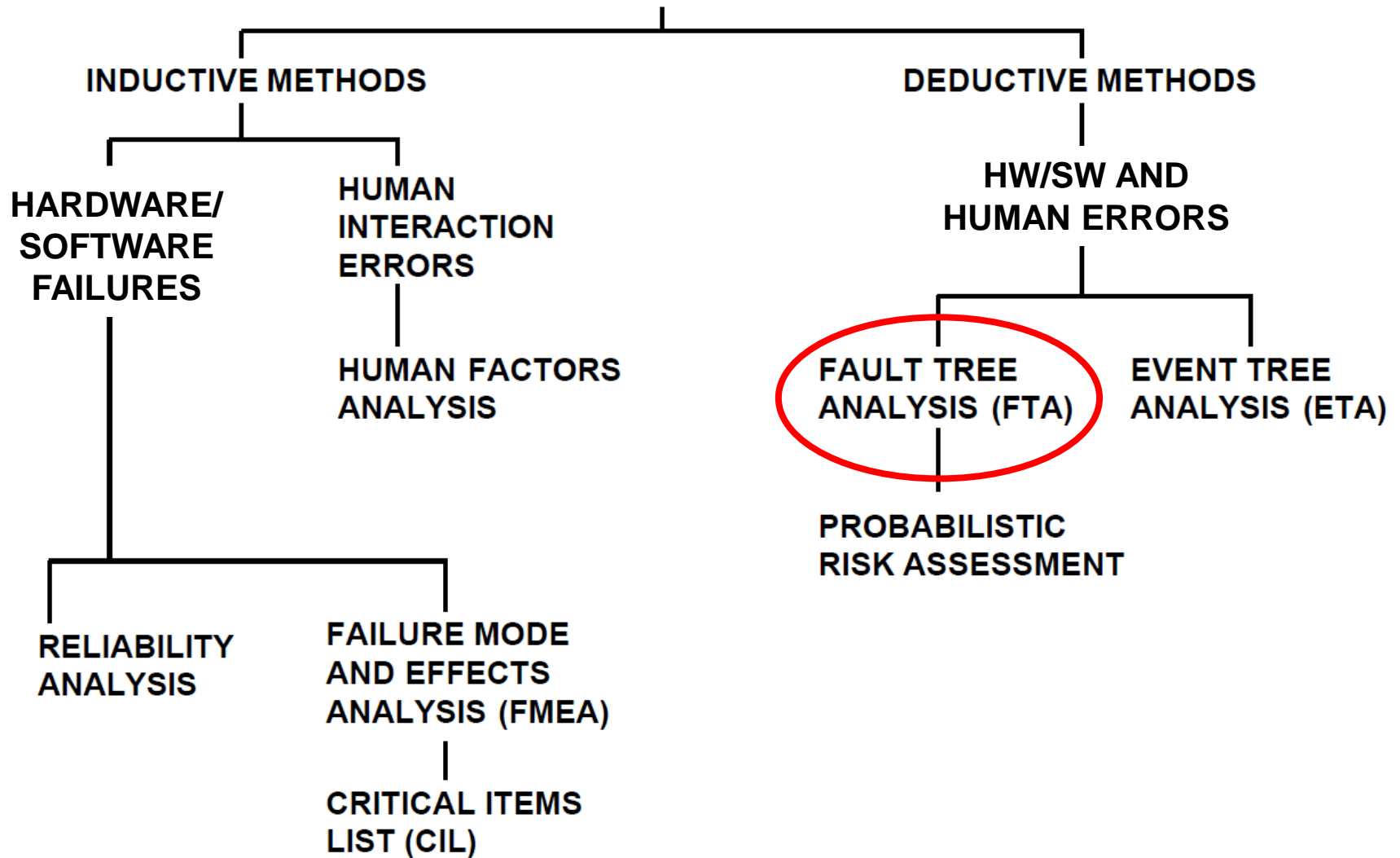


## DEDUCTIVE PROCEDURES (Top-Down Analysis)



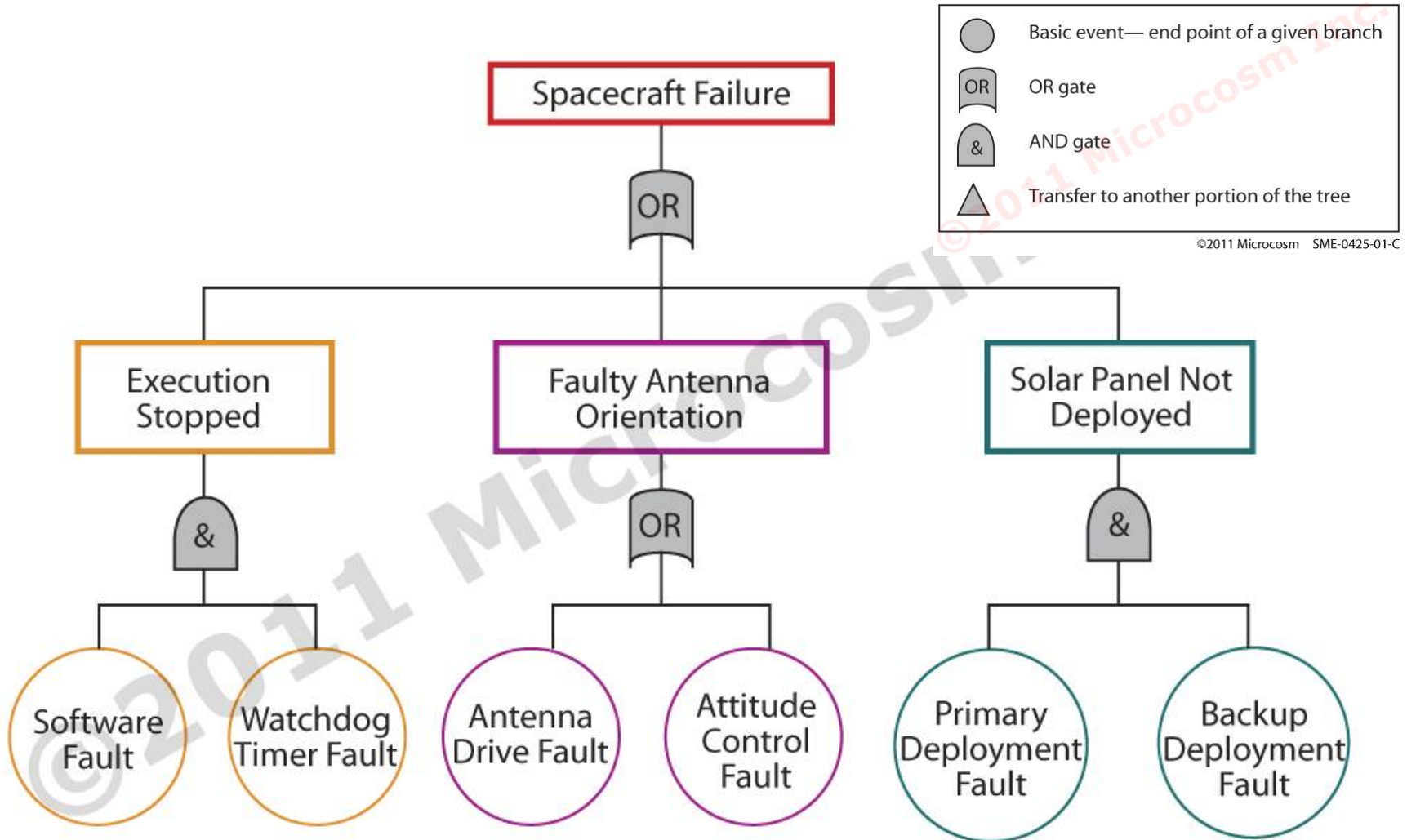
# The Engineer's Crystal Ball

## RELIABILITY/FAULT ANALYSIS PROCEDURES



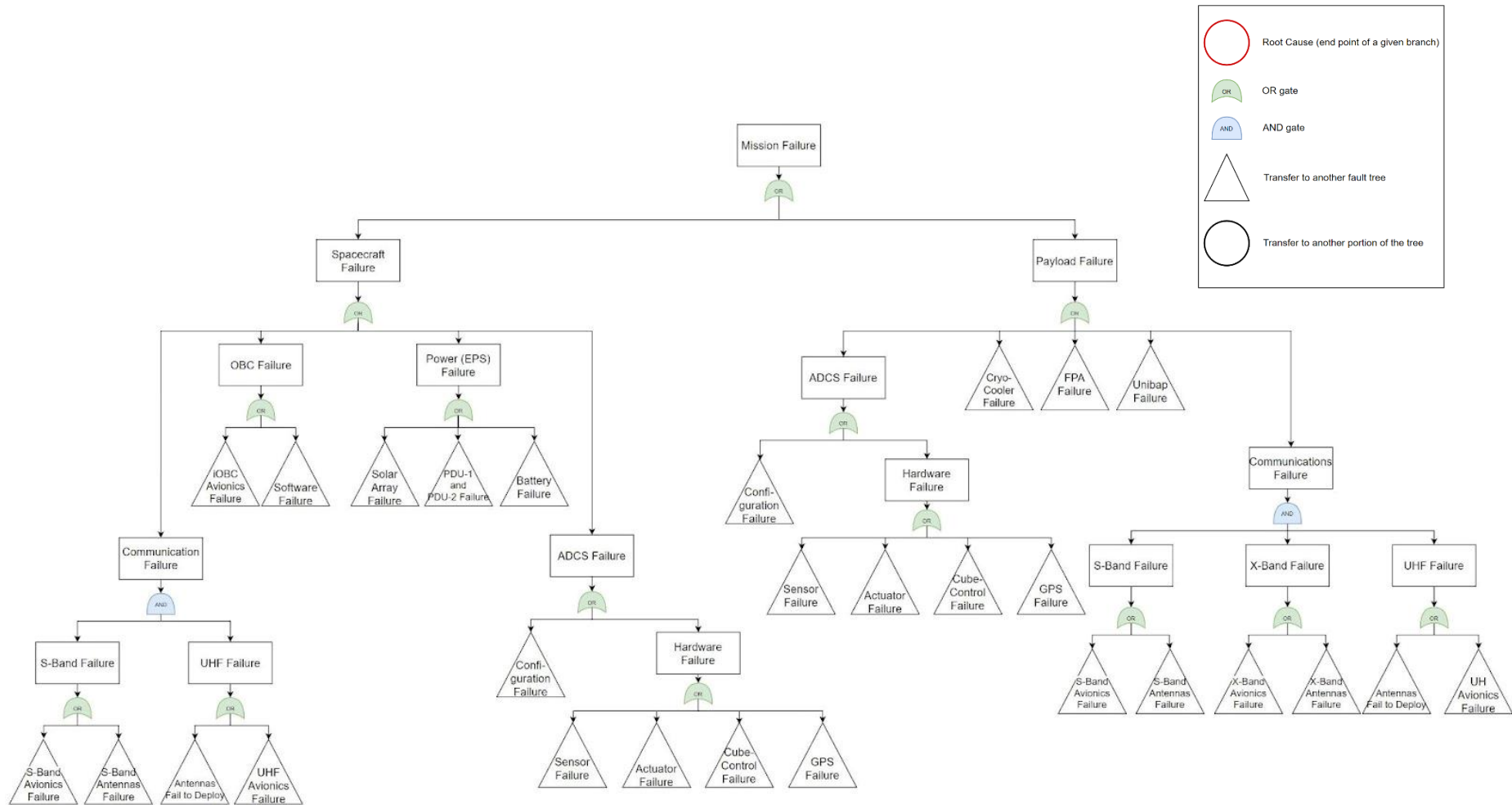
# The Engineer's Crystal Ball

## Fault Tree



# The Engineer's Crystal Ball

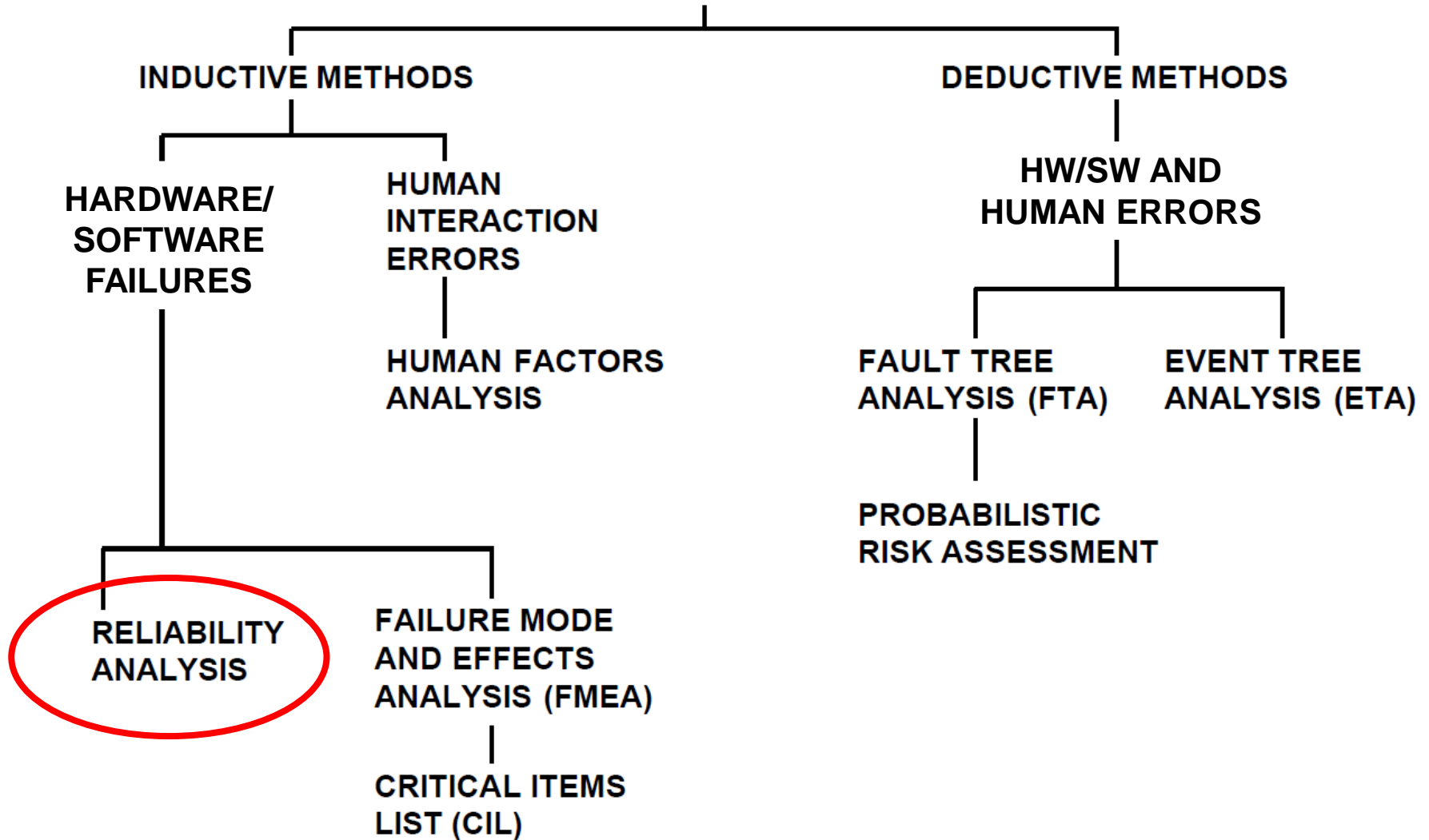
## HSFL/NASA HyTI Mission Fault Tree





# The Engineer's Crystal Ball

## RELIABILITY/FAULT ANALYSIS PROCEDURES



---

# Reliability Analysis

# Reliability Analysis

- **Reliability** is “the probability that a device will function without failure over a specified time period or amount of usage.” [IEEE, 1984]
  - **basic reliability** is for no failure of any kind
  - **mission reliability** is for no failure that impairs the mission - this is the more important reliability for space missions and if no qualifier appears before the word “reliability” it is assumed to mean “mission reliability”
  - Basic equation for reliability for a single function not subject to wear-out failures:

$$R = e^{-\lambda t}$$

where  $R$  is the probability that the item will operate without a failure for time  $t$  (success probability) and  $\lambda$  is the failure rate

# Reliability Analysis

- The *probability of failure*,  $F$  is:

$$F = 1 - R$$

- For a vehicle made up of  $n$  nonredundant elements, all equally essential for vehicle operation, the ***system*** (or series) ***reliability***,  $R_s$ , is:

$$R_s = \prod_1^n R_i = e^{-\sum \lambda_i t}$$

where  $R_i (i=1 \dots n)$  is the reliability and  $\lambda_i$  the failure rate of individual components.

- For failure probabilities  $(\lambda t) < 0.1$  or  $R > 0.9$ , then

$$e^{-\lambda t} \approx 1 - \lambda t$$

# Reliability Analysis

- For a system with  $n$  elements in parallel where each of these elements can by itself satisfy the requirements, the *parallel* (or *redundant*) *reliability*,  $R_p$ , is given by:

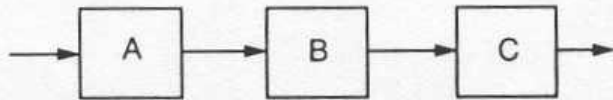
$$R_p = 1 - \prod_1^n (1 - R_i)$$

- When the reliability of the parallel elements is equal ( $R_a$ ) the above equation simplifies to:

$$R_p = 1 - (1 - R_a)^n$$

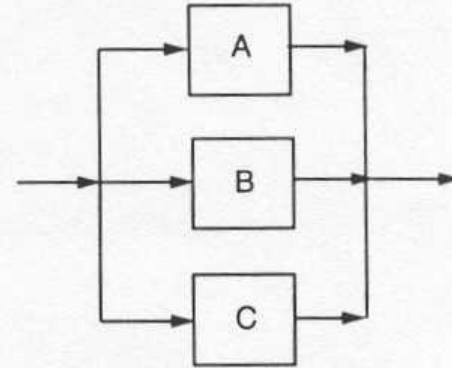
# Reliability Analysis

## Series and Parallel Reliability Models



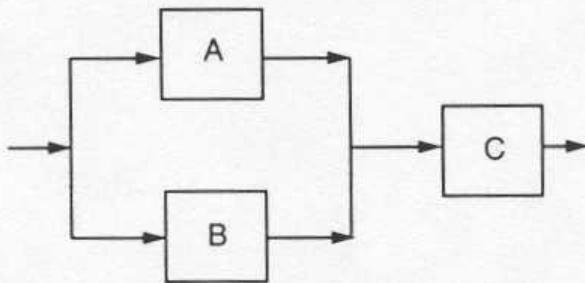
$$R_S = R_A R_B R_C$$

**CASE 1**  
**Series Reliability**



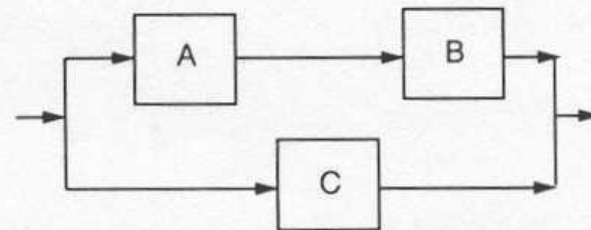
$$R_S = 1 - (1 - R_A)(1 - R_B)(1 - R_C)$$

**CASE 2**  
**Parallel Reliability = Full Redundancy**



$$R_S = R_C [1 - (1 - R_A)(1 - R_B)]$$

**CASE 3**  
**Partial Redundancy**

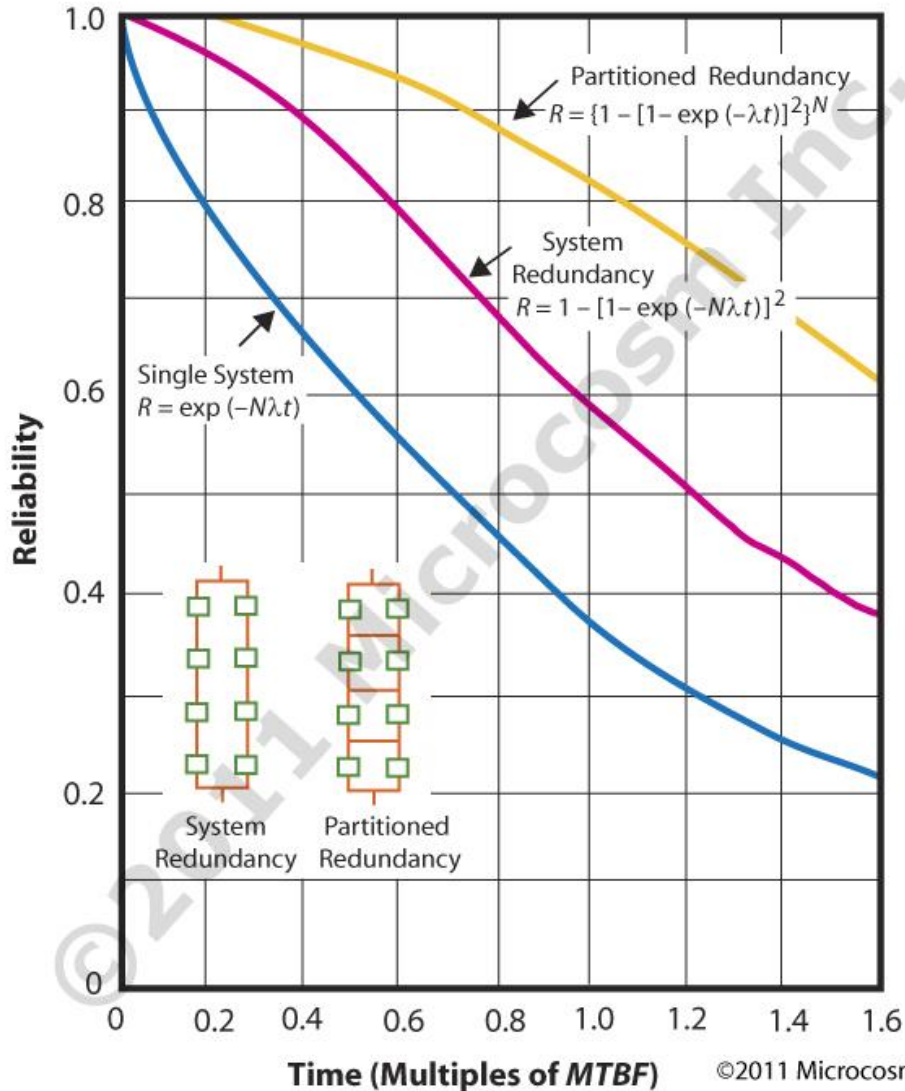


$$R_S = 1 - (1 - R_A R_B)(1 - R_C)$$

**CASE 4**  
**Non-identical, Full Redundancy**

# Reliability Analysis

## Effect of Partitioning on Reliability



$t$  is the time from start of the mission

$R$  is the mission reliability or the probability that at least essential mission elements will survive

$N$  is the number of individual blocks

$\lambda$  is the failure rate of an individual block

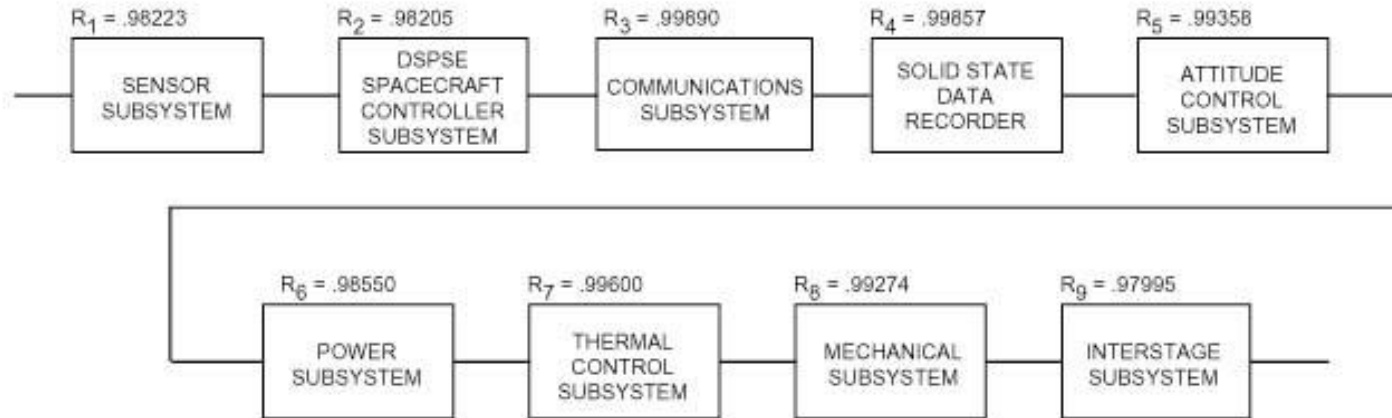
$\lambda \equiv 1/MTBF$ , where  $MTBF$  is the mean time between failures for each block

For the whole system:

$R_s = \exp(-\lambda_s t)$  where  $\lambda_s$  is  $1/MTBF$  for the whole system

# Reliability Analysis

## DSPSE Spacecraft Reliability Diagram (Mission Essential Scenario)



### MATHEMATICAL MODEL LEGEND

$R_{\text{DSPSE}}$  = The reliability of the DSPSE Spacecraft for mission essential scenario over a 220 day mission

$R_i$  = The reliability of the  $i^{\text{th}}$  DSPSE Subsystem assembly

### MATHEMATICAL MODEL

$$R_{\text{DSPSE}} = \prod_{i=1}^9 R_i$$

$R_1$  through  $R_9$  were calculated in subtier reliability diagrams.

### RELIABILITY PREDICTION

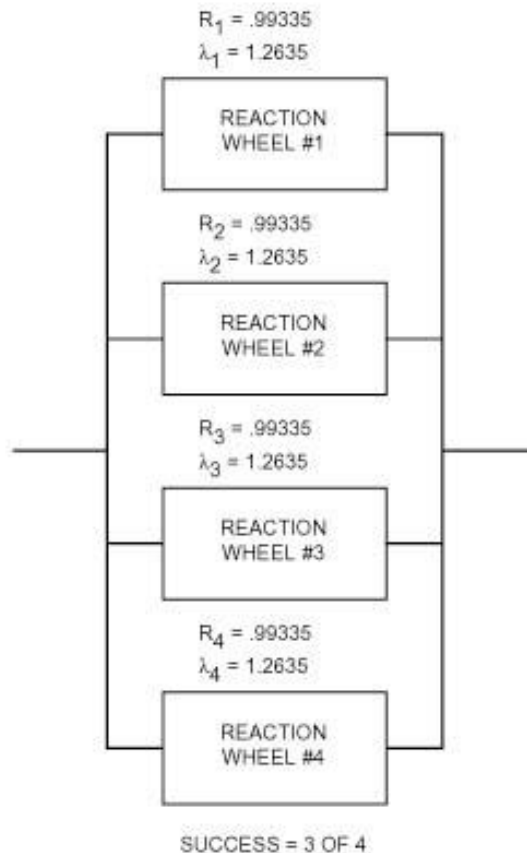
$R_{\text{DSPSE}} = .91286$

SE&R-31



# Reliability Analysis

## ACS Reaction Wheel Reliability Diagram (3 Out Of 4 Reaction Wheels Required)



### MATHEMATICAL MODEL LEGEND

$R_{RW}$  = The reliability of the Reaction Wheel function where 3 of 4 Reaction Wheels are required for success

$R_i$  = The reliability of the  $i^{\text{th}}$  Reaction Wheel

$\lambda_i$  = The failure rate of the  $i^{\text{th}}$  Reaction Wheel

$t_m$  = The DPSPE mission time of 220 days (5,280 hours)

### MATHEMATICAL MODEL

$$R_{RW} = \sum_M [C_M \cdot R_i^M (1 - R_i)^{N-M}]$$

Where:  $M = 3 \text{ and } 4$

$N = 4$

$$C_M = \frac{N!}{(N - M)! M!}$$

$R_1$  through  $R_4$  are of the form:

$$e^{-\lambda_i t_m}$$

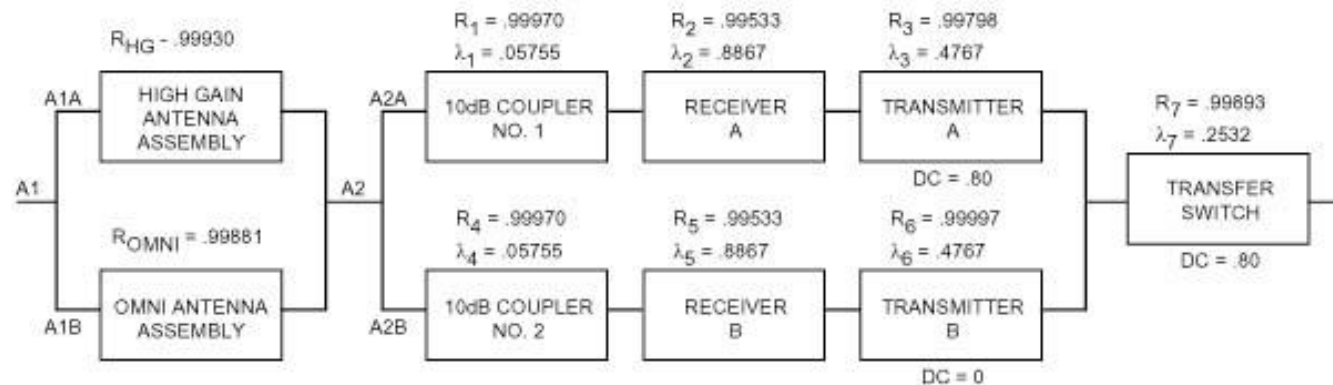
### RELIABILITY PREDICTION

$$R_{RW} = .99974$$

SE&R-07

# Reliability Analysis

## DSPSE Spacecraft Communications Subsystem Reliability Diagram



### MATHEMATICAL MODEL LEGEND

$R_{CS}$  = Reliability of the DSPSE Communications Subsystem for a 220 day mission

$R_i$  = The reliability of the  $i^{th}$  DSPSE Communications Subsystem assembly.

$\lambda_i$  = The failure rate of the  $i^{th}$  DSPSE Communications Subsystem assembly per million hours.

$t_m$  = The DSPSE mission time of 220 days (5,280 hours)

DC = Operational duty cycle = 1.0 unless otherwise noted

Kd = Operating-to-standby failure rate multiplier = .01

### MATHEMATICAL MODEL

$$R_{CS} = R_{A1} \times R_{A2} \times R_7$$

$$R_{A1} = R_{A1A} + R_{A1B} (1 - R_{A1A})$$

$$R_{A2} = R_{A2A} + R_{A2B} (1 - R_{A2A})$$

$$R_{A2A} = \prod_{i=1}^3 R_i$$

$$R_{A2B} = \prod_{i=4}^6 R_i$$

$R_{HG}$  AND  $R_{OMNI}$  are derived from the subtier communications subsystem reliability diagrams

$R_1$  through  $R_7$  are of the form:

$$e^{-\lambda_i t_m (DC + Kd (1-DC))}$$

### RELIABILITY PREDICTION

$$R_{CS} = .99890$$

$$R_{A1} = .9999992$$

$$R_{A2} = .99997$$

$$R_{A2A} = .99302$$

$$R_{A2B} = .99500$$

SE&R-39

# Reliability Analysis

- ***Design life*** is the intended operational time of mission
  - important parameter for reliability program
  - determines amount of consumables that must be provided
  - establishes quality and test requirements for items subject to wear-out (e.g., batteries, solar cells, bearings)
  - mission reliability calculated at the design life is the ***mission success probability*** ( $<1.0$ )
  - ***Expected life*** is less than the design life
  - ***Mean mission duration, MMD***, given by:

$$MMD = \int T dR$$

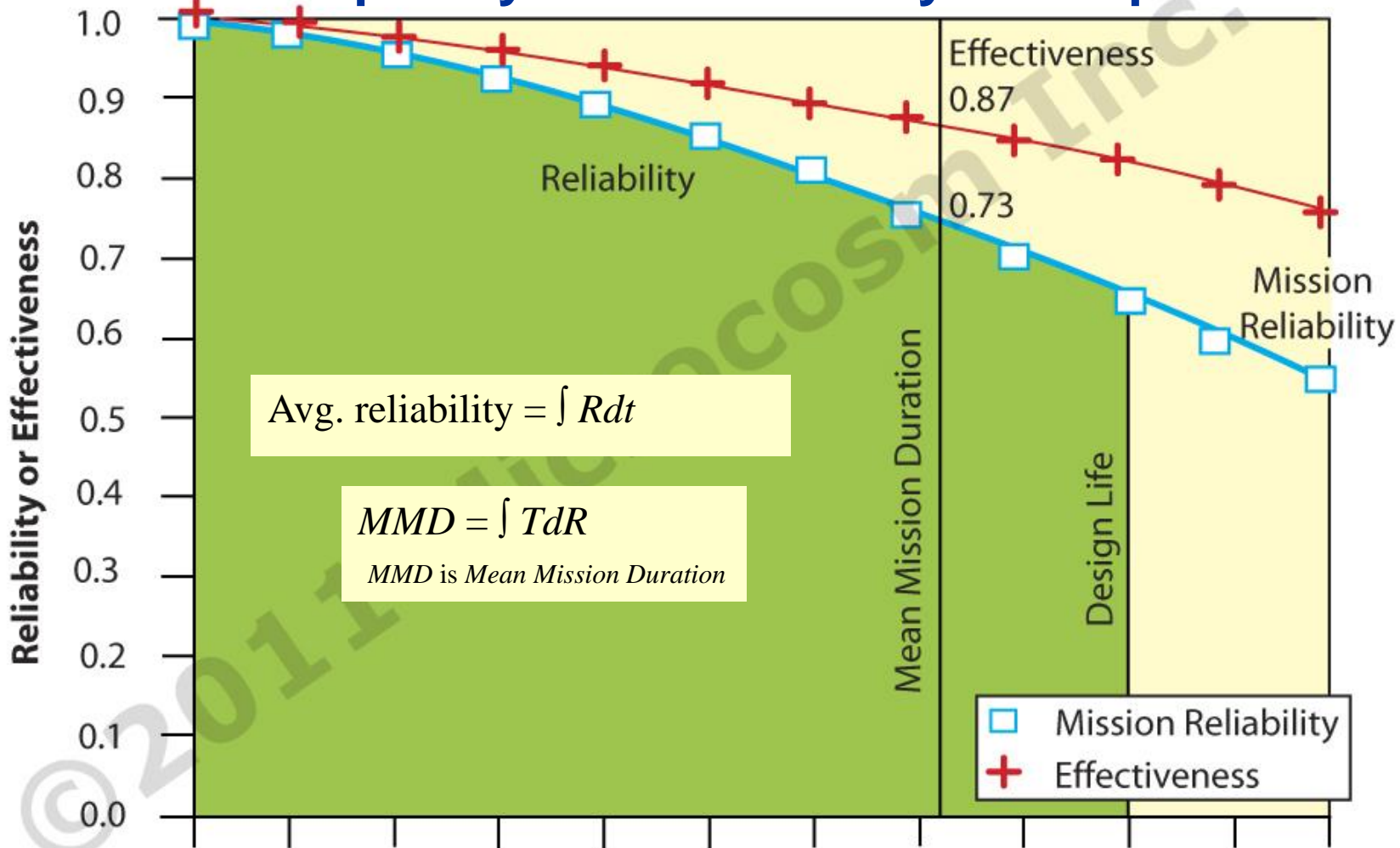
where  $T$  is horiz. time line and  $dR$  is the associated increment in reliability
  - ***MMD*** expresses avg. mission duration at 100% reliability
  - ***MMD*** is frequently used as a FoM for reliability

# Reliability Analysis

- *Mission effectiveness* is a single metric that represents the reliability weighted by the operational capability level to which that reliability is applicable
  - mission effectiveness gives credit for what a vehicle can still do after a partial failure
  - can be used as an alternative to mission reliability to better express what is really required
  - specifying mission effectiveness generally reduces both cost and development time compared to specifying multiple reliability values
  - effectiveness curve will lie above the reliability curve when the latter is constructed for the entire system
  - complement of mission effectiveness (area above effectiveness curve) represents the failure probability weighted by the consequence of the failure

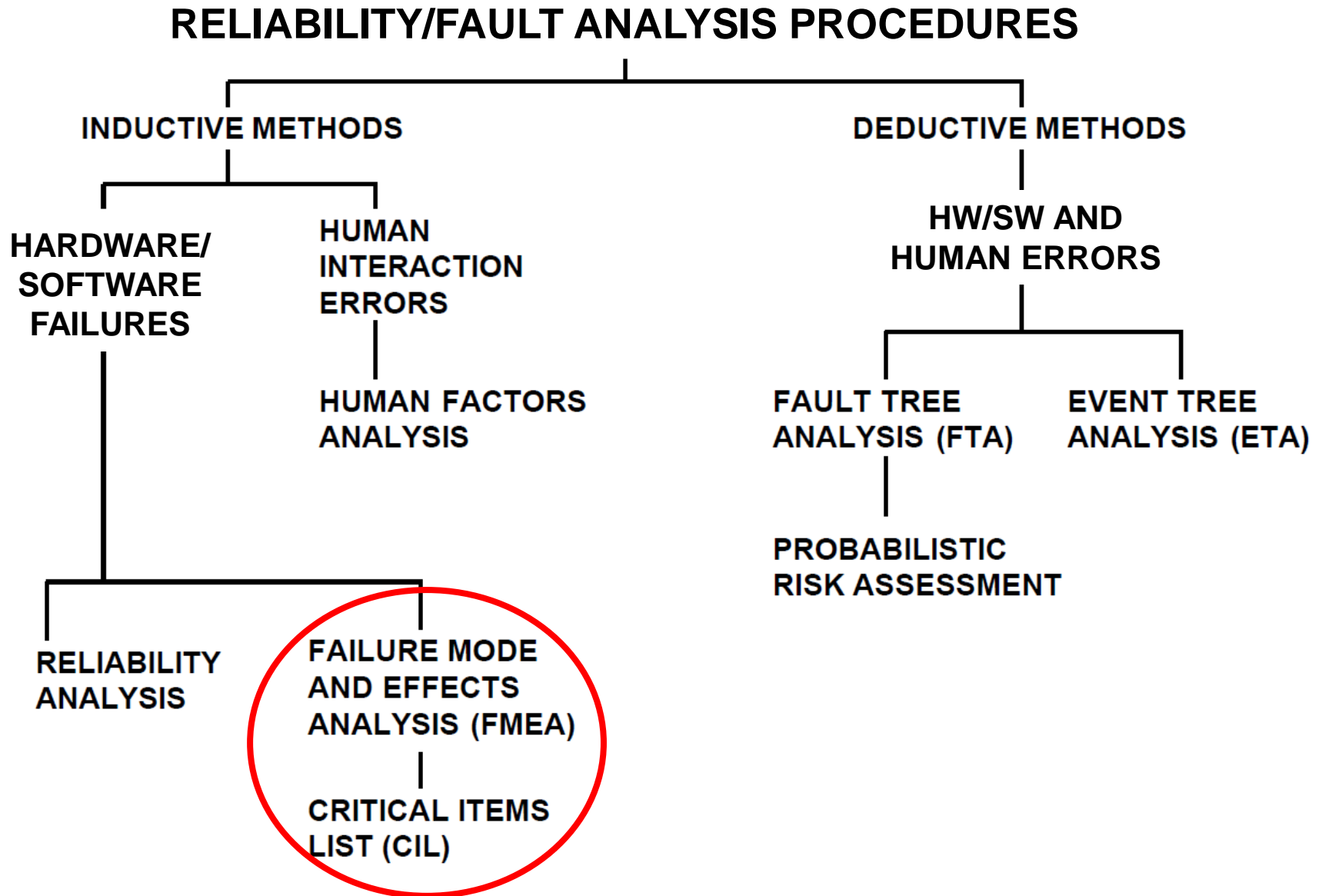
# Reliability Analysis

## Frequently Used Reliability Concepts



Design life is governed by wear-out and expendable stores. *Mean mission duration* is less than *design life* because failures can terminate a mission before end-of-life conditions are reached.

# The Engineer's Crystal Ball



---

# Failure Mode & Effects Analysis (FMEA)

## Failure Mode, Effects & Criticality Analysis (FMECA)

# FMEA/FMECA

---

## Definition

- A methodology to analyze and discover:
  - All potential failure modes of a system
  - The effects these failures have on the system
  - How to correct or mitigate the failures or effects on the system
- FMEA and CIL (Critical Items List) evaluations also cross check safety hazard analyses for completeness
- Together FMEA and CIL are sometimes call Fault Modes, Effect, and Criticality Analysis (FMECA)



# FMEA/FMECA

## Benefits

- FMECA is one of the most important tools of reliability analysis and failure prevention
  - If done early enough in the design process it can have tremendous impact on *removing causes for failure* of developing systems that can *mitigate their effects*.
  - FMECA *exposes single point failure modes* in a subsystem assumed to be redundant
  - FMECA identifies opportunities for *functional redundancy*
  - FMECA permits components to *assume a safe mode* in the absence of required signals or power
  - Failures are usually recorded at the part level

# FMEA/FMECA

---

## Benefits

- Cost benefits associated with FMECA are usually expected to come from the ability to identify failure modes earlier in the process, when they are less expensive to address.
  - “rule of ten”
    - If the issue costs \$100 when it is discovered in the field, then...
    - It may cost \$10 if discovered during the final test...
    - But it may cost \$1 if discovered during an incoming inspection.
    - Even better it may cost \$0.10 if discovered during the design or process engineering phase.

# FMEA/FMECA

---

## History

- The history of FMEA/FMECA goes back to the early 1950s and 1960s.
  - U.S. Navy Bureau of Aeronautics, followed by the Bureau of Naval Weapons
  - National Aeronautics and Space Administration (NASA)
- Department of Defense developed and revised the MIL-STD-1629A guidelines during the 1970s.

# FMEA/FMECA

---

## History (cont.)

- Ford Motor Company published instruction manuals in the 1980s and the automotive industry collectively developed standards in the 1990s.
- Engineers in a variety of industries have adopted and adapted the tool over the years.

# FMEA/FMECA

## Published Guidelines

- J1739 from the SAE for the automotive industry.
- AIAG FMEA-3 from the Automotive Industry Action Group for the automotive industry.
- ARP5580 from the SAE for non-automotive applications.
- Other industry and company-specific guidelines exist.  
For example:
  - EIA/JEP131 provides guidelines for the electronics industry, from the JEDEC/EIA.
  - P-302-720 provides guidelines for NASA's GSFC spacecraft and instruments.
  - SEMATECH 92022963A-ENG for the semiconductor equipment industry.

# FMEA/FMECA

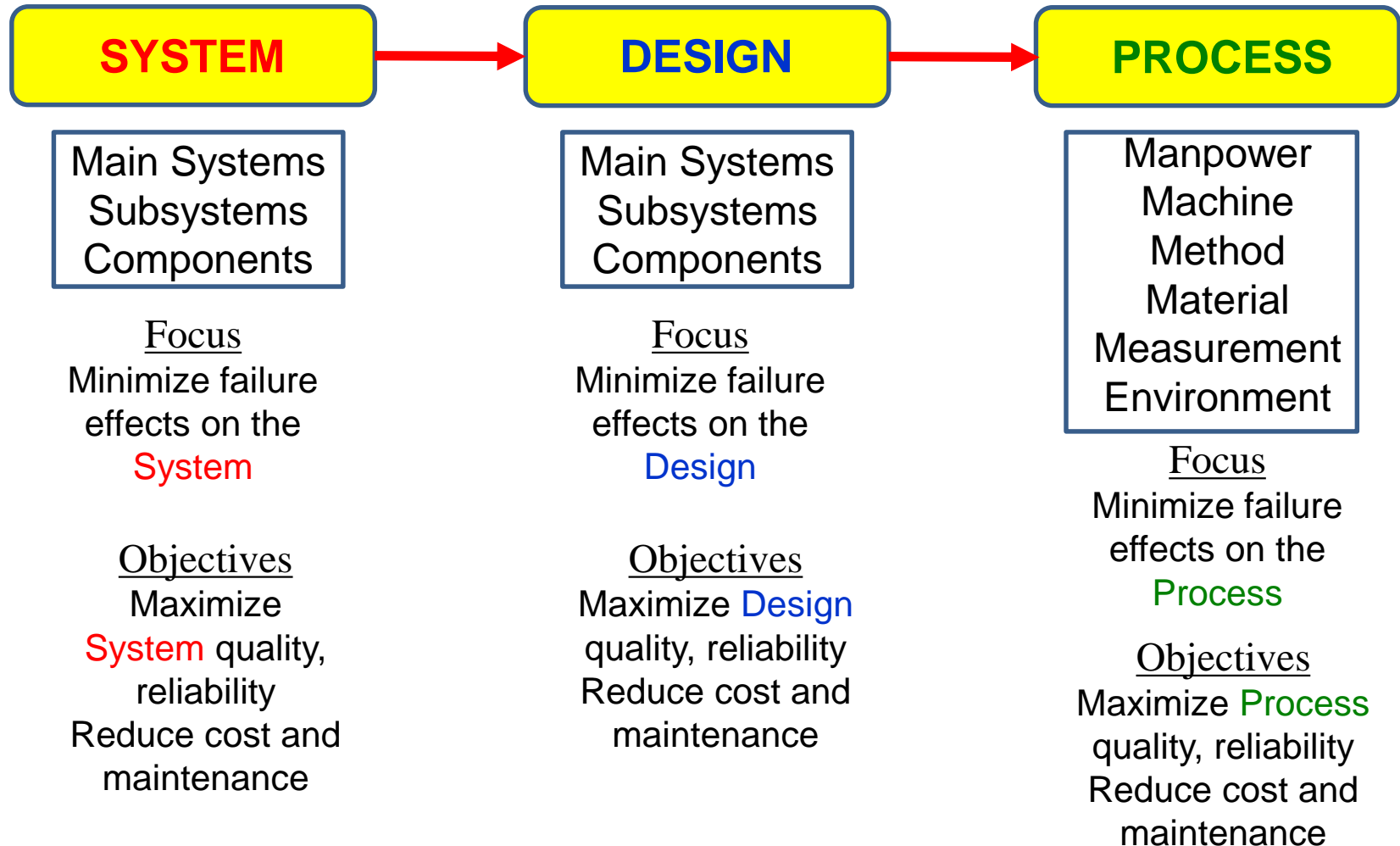
---

## SFMEA, DFMEA, and PFMEA

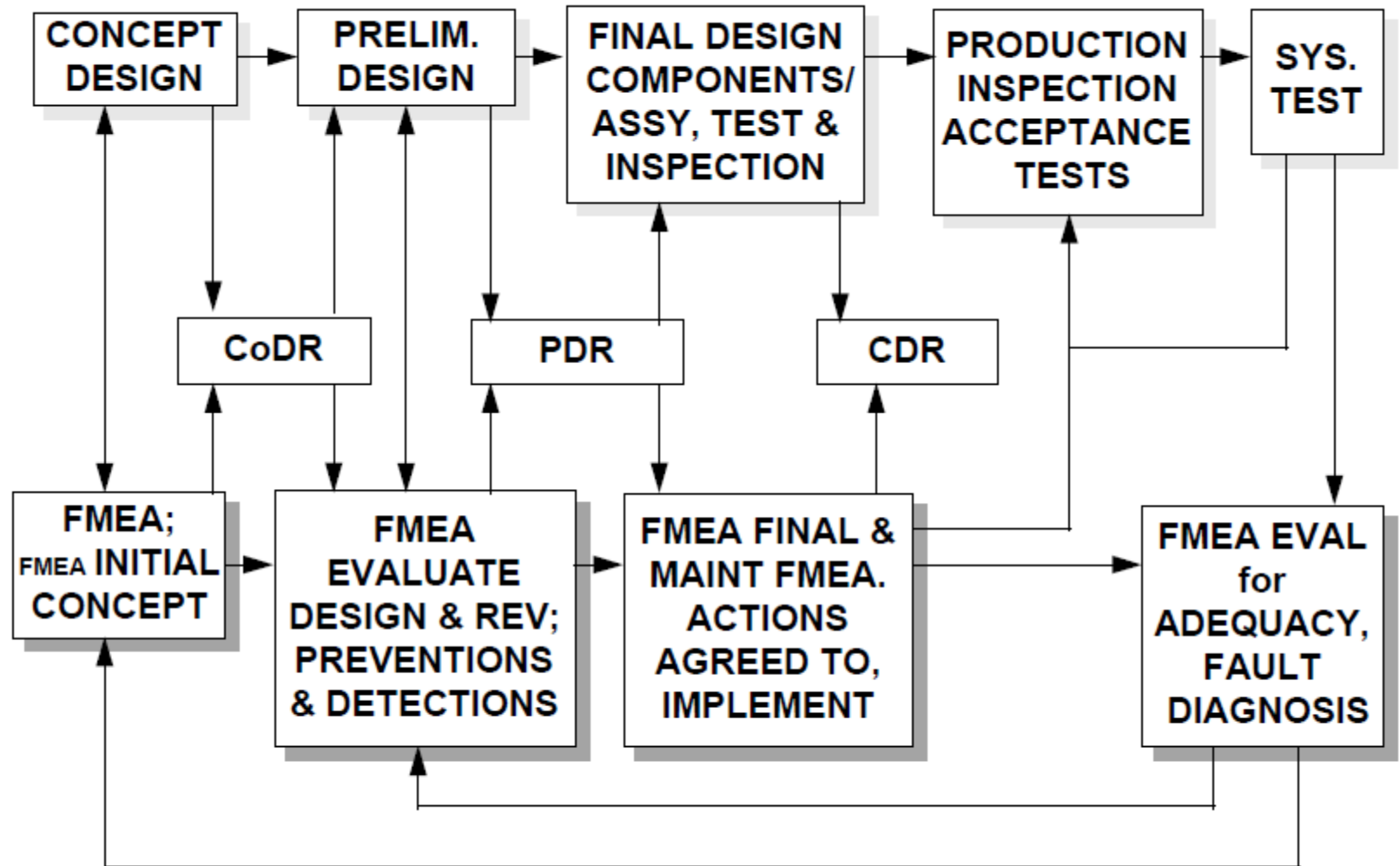
- When it is applied to interaction of parts it is called *System Failure Mode and Effects Analysis* (SFMEA)
- Applied to a product it is called a *Design Failure Mode and Effects Analysis* (DFMEA)
- Applied to a process it is called a *Process Failure Mode and Effects Analysis* (PFMEA).

# FMEA/FMECA

## Relationship Between SFMEA, DFMEA, and PFMEA



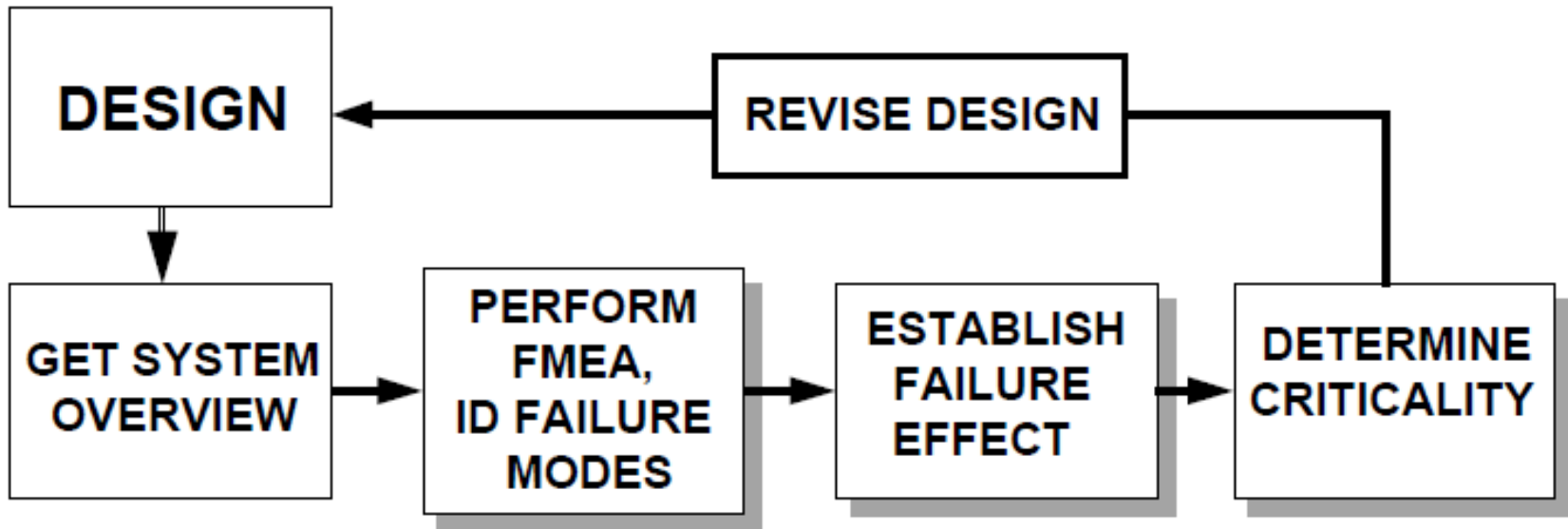
# FMEA/FMECA in Systems Engineering





# FMEA/FMECA

## FMEA/FMECA Procedure Flowchart



# FMEA/FMECA

## FMEA/FMECA Procedure

1. Review the design or process
  - Determine function of all components
  - Create functional and reliability block diagrams
  - Document all environments and missions of system
2. Brainstorm potential *failure modes*
3. List potential *failure effects*
4. Assign *severity* ratings
5. Identify potential *causes* of each failure mode
6. Assign *occurrence* ratings
7. List *current controls* for each cause
8. Assign a *detection* ratings
9. Calculate the *Risk Priority Number* (RPN)
10. Determine *criticality* of the failure, ranking & CIL
  - Develop Critical Items List (CIL)
11. Develop action plan for follow-up or corrective actions
12. Take action and reevaluate RPN

# FMEA/FMECA

## Step 2: Failure Modes

- Definition: *the manner in which a system, subsystem, or component could potentially fail to meet design intent*
- In what ways can they fail? How likely is this failure?
- Do one or more components interact to produce a failure?
- Is this a common failure?
- Who is familiar with this particular item?

### Remember to consider:

absolute failure  
partial failure  
intermittent failure  
over function  
degraded function  
unintended function

### Consider potential failure modes under:

#### Operating Conditions:

- hot and cold
- wet and dry
- dusty and dirty

#### Usage:

- above average life cycle
- harsh environment
- below average life cycle

# FMEA/FMECA

## Step 3: Potential Failure Effects

- Definition: *Effects of the failure mode on the function as perceived by the customer/user*
- Ask yourself- "What would be the result of this failure?" or "If the failure occurs then what are the consequences"
- Describe the effects in terms of what the customer might experience or notice
- State clearly if the function could impact safety or noncompliance to regulations
- Identify all potential customers. The customer may be an internal customer, a distributor as well as an end user
- Describe in terms of product performance

# FMEA/FMECA

---

## Step 3: Examples of Failure Effects

- noise
- loss of fluid
- seizure of adjacent surfaces
- loss of function
- no/low output
- loss of system
- intermittent operations
- rough surface
- unpleasant odor
- poor appearance
- potential safety hazard
- customer dissatisfied

# FMEA/FMECA

## Step 4: Severity

- Definition: *assessment of the seriousness of the effect(s) of the potential failure mode on the next component, subsystem, or customer if it occurs*
- Severity applies to effects
- For failure modes with multiple effects, rate each effect and select the highest rating as severity for failure mode
- Typical scale: 1= Not Severe to 10= Very Severe



- Examples (for car):
  - Cannot see out of front window – severity 9
  - Does not get warm enough – severity 5

# FMEA/FMECA

---

## Step 5: Causes of Failure Modes

- Definition: *an indication of a design weakness, the consequence of which is the failure mode*
- Why do things fail?
- Every conceivable failure cause or mechanism should be listed
- Each cause or mechanism should be listed as concisely and completely as possible so efforts can be aimed at pertinent causes

# FMEA/FMECA

---

## Step 5: Examples of Failure Modes

- Fatigue/fracture
- Structural overload
- Electrical overload
- Wear (lube failure or contamination)
- Seal failure
- Chemical attack
- Oxidation
- Material removal
- Radiation
- Software errors
- Etc.



# FMEA/FMECA

## Step 6: Occurrence

- Definition: *likelihood that a specific cause/ mechanism will occur and create failure modes*
- Obtain from past data if possible
- Removing or controlling the cause/mechanism through a design change is the only way to reduce the occurrence rating
- Typical scale: 1= Not Likely to 10= Very Likely



# FMEA/FMECA

## Step 7: Current Controls

- Definition: *activities which will assure the design adequacy for the failure cause/mechanism under consideration*
- Confidence Current Design Controls will detect cause and subsequent failure mode prior to production, and/or will prevent the cause from occurring
  - If there are more than one control, rate each and select the lowest for the detection rating
- Control must be allocated in the plan to be listed, otherwise it's a recommended action
- Two types of Controls
  1. *Prevention* from occurring or reduction of rate
  2. *Detection*
    - detect cause mechanism and lead to corrective actions
    - detect the failure mode, leading to corrective actions

# FMEA/FMECA

## Step 7: Examples of Current Controls

- Type *P* control
  - Warnings which alert product user to impending failure
  - Fail/safe features
  - Design procedures/guidelines/specifications
- Type *D* controls
  - Road test
  - Design Review
  - Environmental test
  - Fleet test
  - Lab test
  - Field test
  - Life cycle test
  - Load test

# FMEA/FMECA

## Step 8: Detection

- Definition: *Detection is the value assigned to each of the detective controls*
- If detection values are based upon internally defined criteria, a reference must be included in FMECA to rating table with explanation for use
- Detection values of 1 must eliminate the potential for failures due to design deficiency
- Typical scale:

1 = Easy to Detect to 10 = Difficult to Detect



# FMEA/FMECA

## Step 9: Risk Priority Number (RPN)

- Definition: *RPN is the product of severity, occurrence, and detection scores*
- Lowest detection rating is used to determine RPN

$$\text{Severity} \times \text{Occurrence} \times \text{Detection} = \text{RPN}$$

- RPN is used to prioritize concerns/actions
- The greater the value of the RPN the greater the concern
- RPN ranges from 1-1000
- The team must make efforts to reduce higher RPNs through corrective action
- General guideline is over 100 = recommended action

# FMEA/FMECA

---

## Step 10: Criticality and CIL

- Assign criticality categories based on redundancy, results of failure, safety, etc.
- Develop criteria for what failure modes are to be included in a Critical Items List (CIL)
- Develop screens to evaluate redundancy
- Analyze each critical item for ways to remove it, or develop “retention rationale” to support the premise that the risk be retained
- Cross check critical items with hazard reports

# FMEA/FMECA

## Step 10: Criticality Categories (Typical)

- **1** – Single failure point that could result in loss of vehicle or personnel
- **1R** – Redundant items, where if all failed, the result would be loss of vehicle or personnel
- **1S** – A single point of a system component designed to provide safety or protection capability against a potential hazardous condition or a single point failure in a safety monitoring system (e.g., fire suppression system)
- **1SR** – Redundant components, where if all failed, the result is same as 1S above
- **2** – Single point of failure that could result in loss of critical mission support capability
- **3** – All other

# FMEA/FMECA

## Step 10: Analyze Critical Items

- Prepare retention rationale for item
  - What current *design* features minimize the probability of occurrence?
  - What *tests* can detect failure modes during acceptance tests, certification tests, checkout for operation?
  - What *inspections* can be performed to prevent the failure mode from being manufactured into hardware?
  - What *failure history* justifies the CIL retention?
  - How does *operational use* of the unit mitigate the hardware failure effect?
  - How does *maintainability* prevent the failure mode?



# FMEA/FMECA

## Step 11: Actions Recommended

- Definition: *tasks recommended for the purpose of reducing any or all of the rankings*
- Only design revision can bring about a reduction in the severity ranking
- All critical or significant characteristics must have recommended actions associated with them
- Recommended actions should be focused on design, and directed toward mitigating the cause of failure, or eliminating the failure mode
- If recommended actions cannot mitigate or eliminate the potential for failure, recommended actions must force characteristics to be forwarded to process FMEA for process mitigation

# FMEA/FMECA

---

## Step 11: Examples of Actions

- Perform:
  - Designed experiments
  - Reliability testing
  - Finite element analysis
- Revise design
  - Revise test plan
  - Revise material specification

# FMEA/FMECA

## Step 12: Action and Reevaluation


- All recommended actions must have a person assigned responsibility for completion of the action
- Responsibility should be a name, not a title
- There must be a completion date accompanying each recommended action
- Unless the failure mode has been eliminated, severity should not change
- Occurrence may or may not be lowered based upon the results of actions
- Detection may or may not be lowered based upon the results of actions
- If severity, occurrence or detection ratings are not improved, additional recommended actions must be defined

# FMEA/FMECA


## Typical FMEA Form

Note: FMECA Form would have CIL column after RPN


<b>Process/Product</b> <b>Failure Modes and Effects Analysis Form</b> <b>(FMEA)</b>															
Process or Product Name:						Prepared by:				Page ____ of ____					
Responsible:						FMEA Date (Orig) _____ (Rev) _____									
Process Step / Input	Potential Failure Mode	Potential Failure Effects	S E V E R I T Y	Potential Causes	O C C U R R E N C E	Current Controls	D E T E C T I O N	R P N	Actions Recommended	Resp.	Actions Taken	S E V E R I T Y	O C C U R R E N C E	D E T E C T I O N	R P N
What is the process step and Input under investigation?	In what ways does the Key Input go wrong?	What is the impact on the Key Output Variables (Customer Requirements)?		What causes the Key Input to go wrong?		What are the existing controls and procedures (inspection and test) that prevent either the cause or the Failure Mode?		0	What are the actions for reducing the occurrence of the cause, or improving detection?		What are the completed actions taken with the recalculated RPN?				0
								0							0
								0							0
								0							0
								0							0
								0							0




Identify failure modes and their effects



Identify causes of the failure modes and controls



Prioritize



Determine and assess actions

# FMEA/FMECA

## HyTI FMECA Form

For ADCS Main Magnetometer (in progress)

ADCS FMECA

S = Severity, O = Occurrence, D = Detection, P = Prevention, RPN = Risk Priority Number, CIL = Critical Items List

Component	Potential Failure Mode	Potential Failure Effects	S	Potential Causes	O	Current Controls	D	RPN	CIL	Recommended Actions	Responsible	Actions Taken	S	O	D	RPN
Main Magnetometer	Unable to get accurate estimated rates	- unable to use estimation mode 2, 3, and 4 with main magnetometer - unable to get angular rates for estimation mode 5 - estimated rate measurements accuracy lessens in estimation mode 6	6	Power Control is set to 0		D: Get segmentation fault when try to send a command. Check with I.D. 132, offsets 12 & 13. CubeControl Signal Enabled and CubeControl Motor Enabled, reselectively. Also, get_power_control  P: Continuinly set power control to 1 before each adcs step.	3	0		Complete an ADCS Configuration check when the ADCS is turned on.  Complete an ADCS Configuration check when the ADCS configuration is changed. (When panels are deployed, when magnetometer is deployed). Also check config if experience any ramp up in angular rates.	If can't resolve issue, try sample main magnetometer through Motor instead of Signal. If this does not resolve the issue, switch to redundant magnetometer.					
				Run Mode is set to 0		D: Get segmentation fault when try to send a command. Check with I.D. 190, offset 8, ADCS Run Mode. Also can use get_run_mode  P: Continuinly set run mode to 1 before each adcs step.	2	0								
				Set to Redundant Magnetometer Mode		D: Get magnetometer mode using I.D. 206, offset 3006, Magnetometer Mode.  P: Complete an ADCS Configuration check when the ADCS is turned on.	3	0								
				Sensitivity configuration is incorrect	4	D: P: Complete an ADCS Configuration check when the ADCS is turned on.	3	72								
				Offset configuration is incorrect	4	D: P: Complete an ADCS Configuration check when the ADCS is turned on.	3	72								
				Transform angles configuration is incorrect	4	D: P: Complete an ADCS Configuration check when the ADCS is turned on.	3	72								
				Orbit Parameters are invalid: problem with TLE		D: P:		0								
				Orbit Parameters are invalid: problem with GPS		D: P:		0								

# FMEA/FMECA

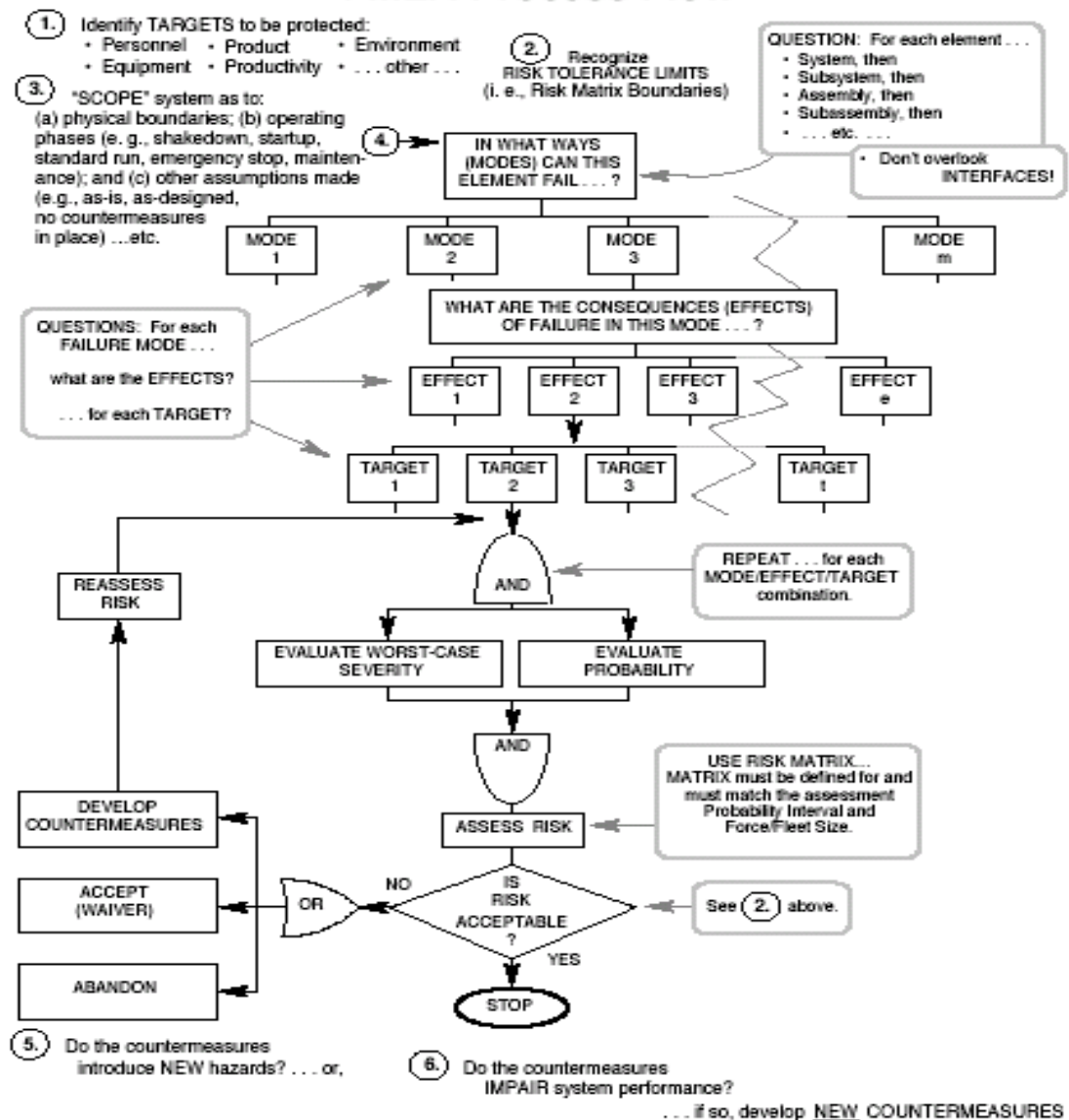
---

## General Instructions for FMECA Document

- Every FMECA should have an assumptions document attached (electronically if possible) or the first line of the FMECA should detail the assumptions and ratings used for the FMECA.
- Product/part names and numbers must be detailed in the FMECA header
- All team members must be listed in the FMECA header
- Revision date, as appropriate, must be documented in the FMECA header

# FMEA/FMECA

## FMEA Process Flow



# FMEA/FMECA

---

## Short Term Uses of FMEA/FMECA

- Identify critical or hazardous conditions.
- Identify potential failure modes
- Identify need for fault detection.
- Identify effects of the failures.



# FMEA/FMECA

---

## Long Term Uses of FMEA/FMECA

- Aids in producing block-diagram reliability analysis
- Aids in producing diagnostic charts for repair purposes.
- Aids in producing maintenance handbooks.
- Design of built-in test (BIT), failure detection & redundancy.
- For analysis of testability.
- For retention as formal records of the safety and reliability analysis, to be used as evidence in product safety litigation.

# Bibliography

---

- MIL-STD-1629A , *Procedures for Performing a Failure Mode, Effects and Criticality Analysis*, Nov. 1980.
- Sittsamer, *Risk Based Error-Proofing*, The Luminous Group, 2000
- MIL-STD-882B, 1984.
- O'Conner, *Practical Reliability Engineering, 3rd edition, Revised*, John Wiley & Sons, Chichester, England, 1996.
- QS9000 FMEA reference manual (SAE J 1739)
- Wertz, Everett, and Puschell (ed.), *Space Mission Engineering: The New SMAD*, Microcosm Press, Hawthorne, CA, 2011/
- McDermot, Mikulak, and Beauregard, *The Basics of FMEA*, Productivity Inc., 1996.
- TM 5-698-4, *Failure Modes, Effects and Criticality Analysis (FMECA) for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities*, HQ, Department of the Army, September, 2006.

# Space Spectaculars!



**STS-98 Launch**  
**2/7/2001**



**MMIII Launch**  
**VAFB 9/19/02**

**Clementine's View of  
Earth Over Lunar North  
Pole Mar. 1994**



---

# Backup Slides

# Alternative FMECA Form - 1

## Failure Mode, Effect, and Criticality Analysis (FMECA) Worksheet

1. Flow chart the selected process as it is designed (the intended process)
2. Flow chart the selected process as it is routinely conducted (the actual process)
3. List each step and each link between steps of the intended process in Column 5 below
4. Include discrepancies between the flow charts (steps 1 & 2) in Column 6 below

[illegible]

Joint Commission on Accreditation of Healthcare Organizations

Adapted, with permission, from model used by  
Good Samaritan Hospital, Dayton, Ohio

# Alternative FMECA Form - 2

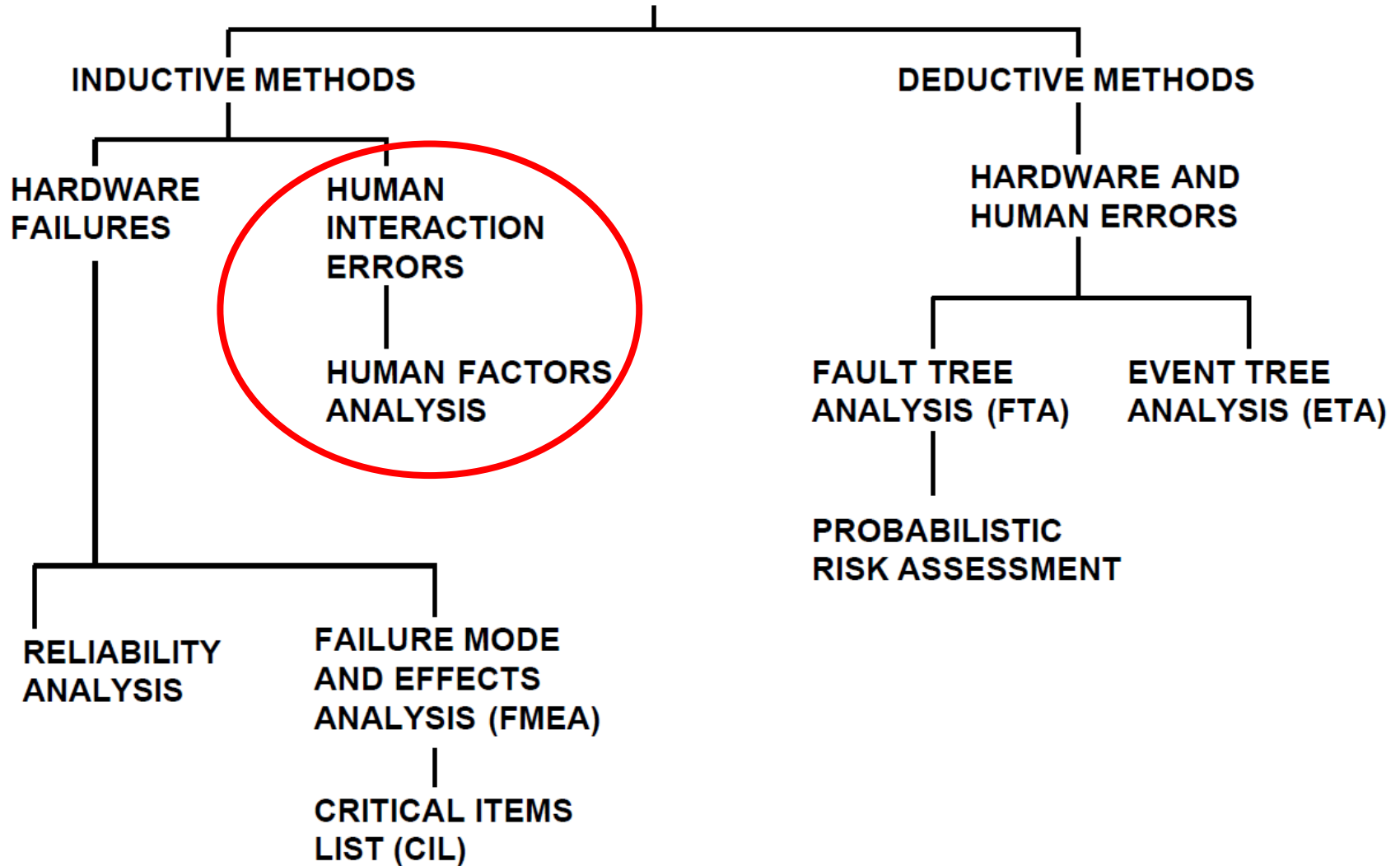
## Failure Mode, Effect, and Criticality Analysis (FMECA) Worksheet

Page 2: Analysis and Action Planning for Critical Failure Modes

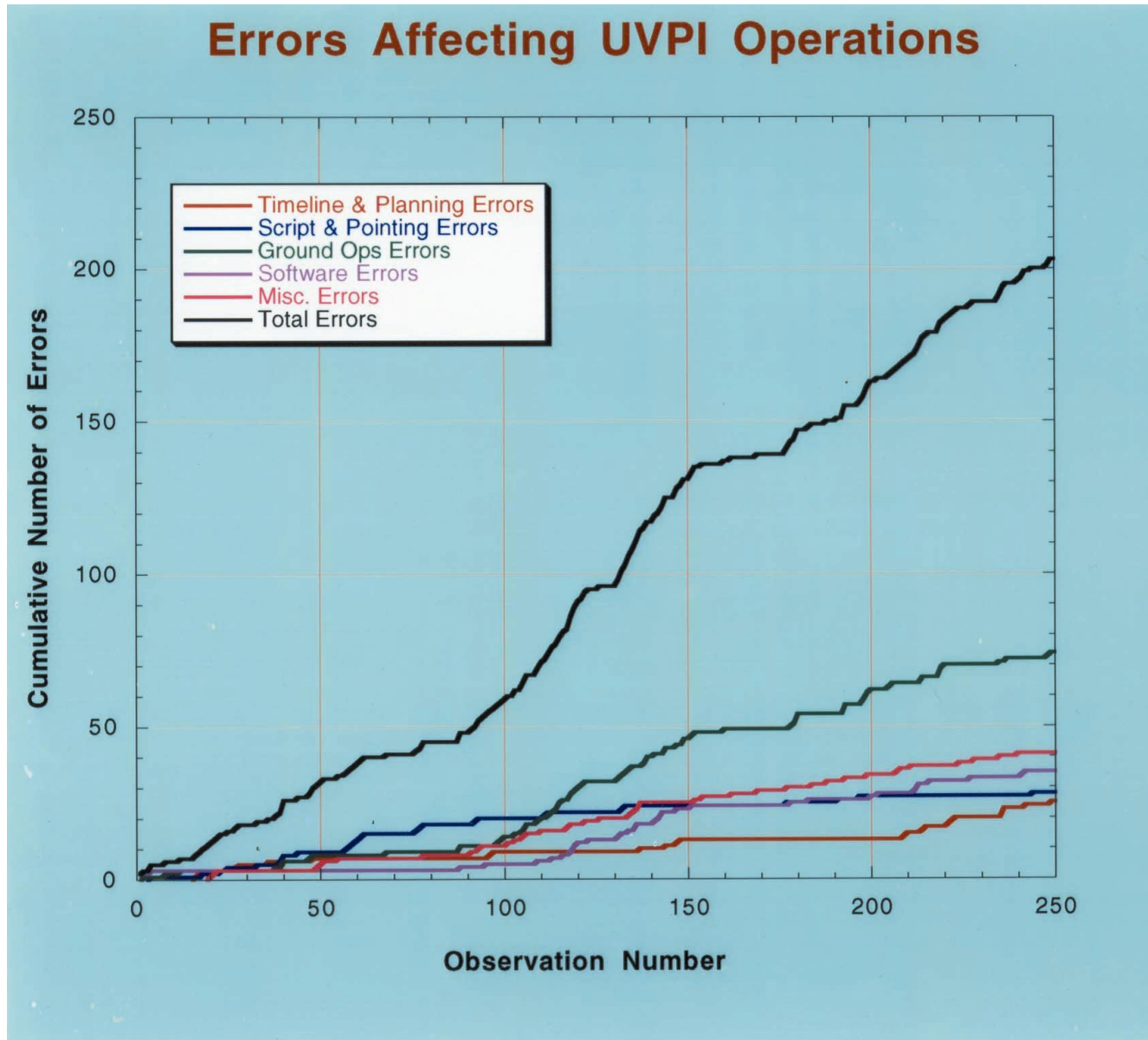
Critical Failure Mode	Actionable Causes	Potential Solutions / Redesigns	Time Req'd.	Cost

# The Engineer's Crystal Ball

## RELIABILITY/FAULT ANALYSIS PROCEDURES

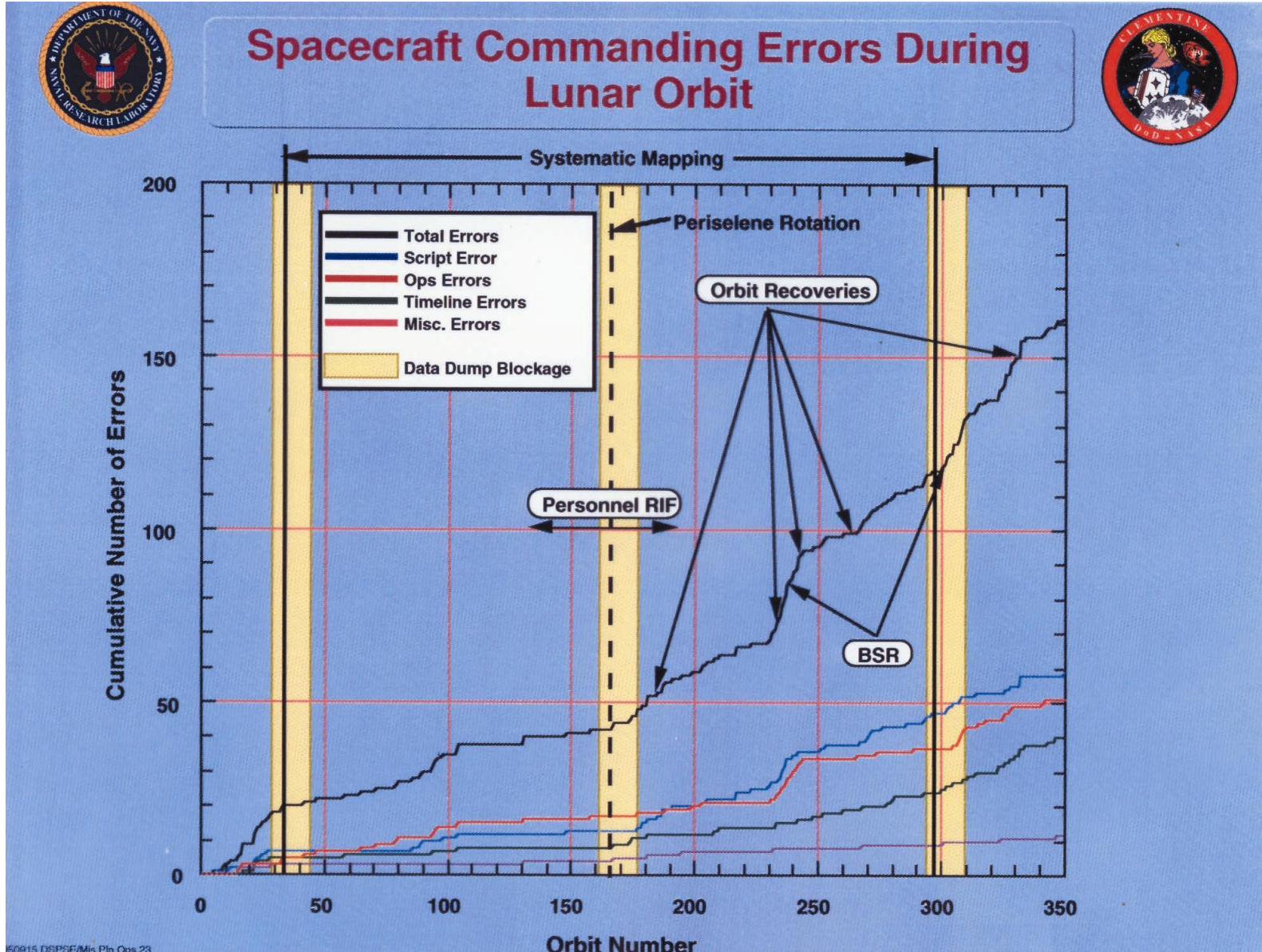


# Operational Errors



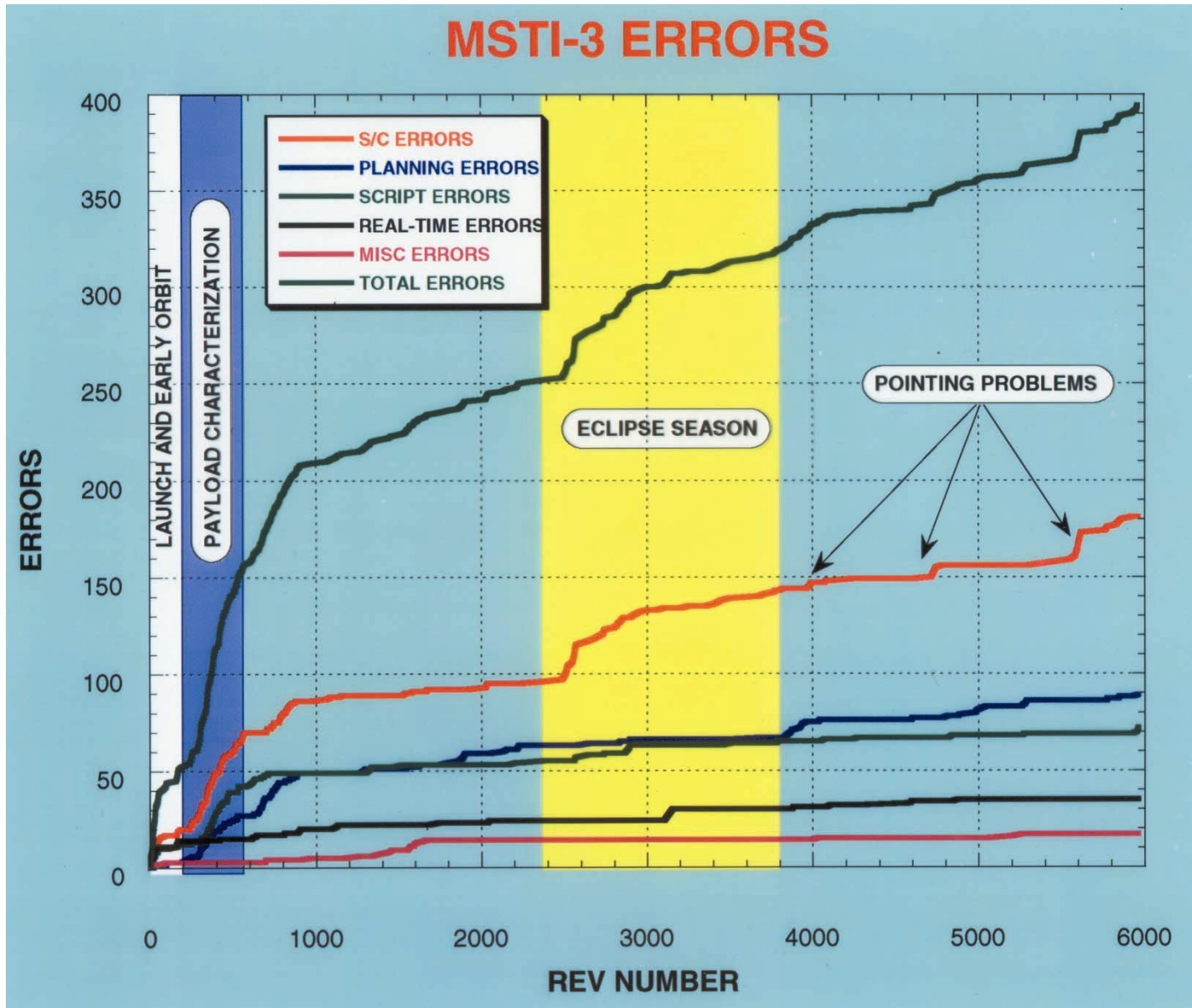


# Operational Errors



160915 DSPSE/Mis Ptn Ops.23

# Operational Errors



---

# Design for Reliability

# Design for Reliability

---

- ***Reliability Program Plan (RPP)*** specifies the reliability objectives, assigns responsibility for achieving them, and establishes milestones for evaluating the achievements
  - RPP adds little to the cost of the program and is useful for even the smallest spacecraft programs
  - RPP serves as an agreement with other spacecraft functions regarding their responsibilities in support of reliability
  - Most significant interfaces are with quality assurance, test, configuration management, and thermal control



# Design for Reliability

- ***Failure Reporting and Corrective Actions (FRACAS)***
  - FRACAS informs concerned parties that a failure has been observed
  - FRACAS furnishes a record through which trends and correlations can be evaluated at a future time
  - FRACAS permits reassessment of the predicted failure rates and is the basis for consequent modifications of the fault avoidance or fault tolerance provisions
  - an operating log is maintained for each part number with separate records for each serial number
  - To establish a FRACAS the following must be identified:
    - Scope of the activities (e.g., system test, field test, normal usage)
    - Responsibility for cost and for report initiation
    - Method and frequency of reporting (e.g., paper or electronic, each incident or by time interval)

# Design for Reliability

- A typical FRACAS will contain the following information:
  - Incident identification number (e.g., report serial number)
  - Date, time and locale of the incident
  - Part no., name of the failed component, and its serial number
  - Higher level part or system identifiers (subsystem or major component)
  - Lower level part or system identifiers (usually available only after diagnosis)
  - Operation in progress and environmental conditions when failure was detected
  - Immediate and higher level effects of failure
  - Names of individuals responsible for detection, verification, and analysis
  - Diagnosis of immediate, contributory and root causes of the failure
  - Dates and nature of repair and results of retest

# Design for Reliability

## Representative Piece Part Failure Rates for High Reliability Parts

Part Type	Space Flight	Launch	Applicability
<i>Bipolar Gate/Logic Array Dig</i>	0.9–19	17–300	Min 1–100 gates; Max 60,000 gates
<i>Bipolar Microprocessor</i>	7–27	60–215	Min 8 bits; Max 32 bits
<i>MOS Microprocessor</i>	12–47	70–250	Min 8 bits; Max 32 bits
<i>MOS Memory SRAM</i>	2–11	24–75	Min 16 K; Max 1 M
<i>Bipolar SRAM</i>	2–8	30–75	Min 16 K; Max 1 M
<i>Diodes General</i>	1.3	170	
<i>Transistors General</i>	0.05	5	
<i>Transistors RF Power</i>	165	900	
<i>Resistors</i>	0.01	1	Composition/film
<i>Capacitors</i>	0.1	10	
<i>Relays</i>	40	6,000	

Values are the failure rate,  $\lambda$  (failures in  $10^9$  hours)

# Design for Reliability

- Mission failure probability is allocated to subsystems and adjusted whenever requirements change
  - Allocation based on prior experience or uniformly to major subsystems
  - *Weak link* is a recognized subsystem whose complexity or degree of innovation will contribute greatly to the failure probability
  - The *failure/value ratio*,  $F/V$ , is the probability of mission failure,  $F$ , for a subsystem divided by its estimated resource requirements,  $V$

$$E \equiv F / V$$

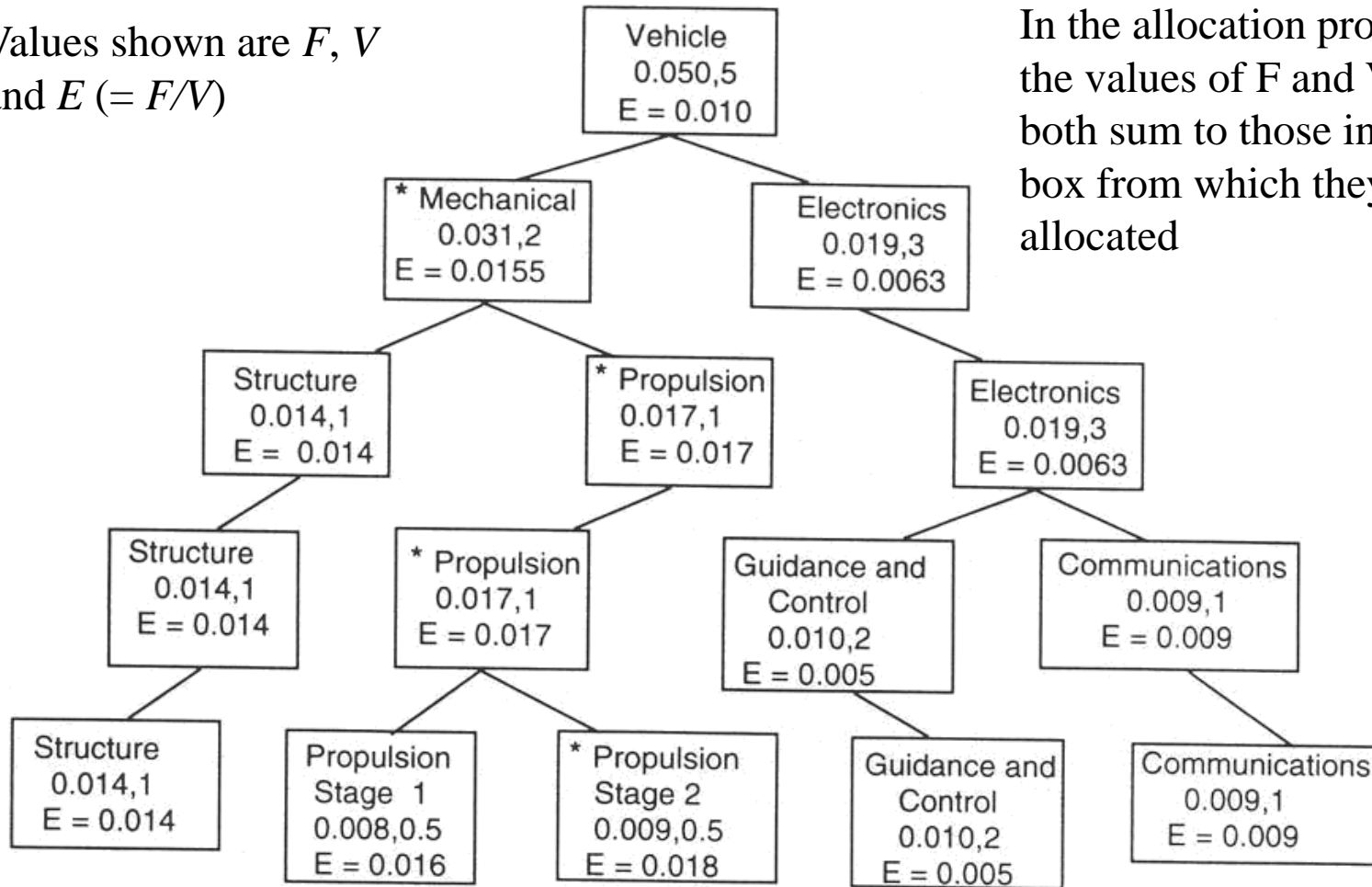


# Design for Reliability

## Reliability Allocation to Subsystems

Values shown are  $F$ ,  $V$   
and  $E (= F/V)$

In the allocation process,  
the values of  $F$  and  $V$  must  
both sum to those in the  
box from which they were  
allocated



\* Weak Link (Element having highest value of  $E$ )

# Design for Reliability

## Failure Prevention

- Major causes of failures are workmanship and design
  - *workmanship* can be controlled by quality assurance
  - *design failures* occur primarily because:
    - the strength of the component is not adequate for the the environment in which it is used, or
    - the manufacturing process allows too much variability in component characteristics
  - Design failures can be controlled by allowing sufficient design margin and performing extensive testing

# Design for Reliability



Preliminary Design Review



## RMA System Requirement

- *“The DataLynx system shall have a minimum availability of 0.999 (This is taken to mean that during scheduled spacecraft support, the DataLynx will be available 99.9% of the passes)”*

**Note: RMA is Reliability, Maintainability, Availability**

# Design for Reliability

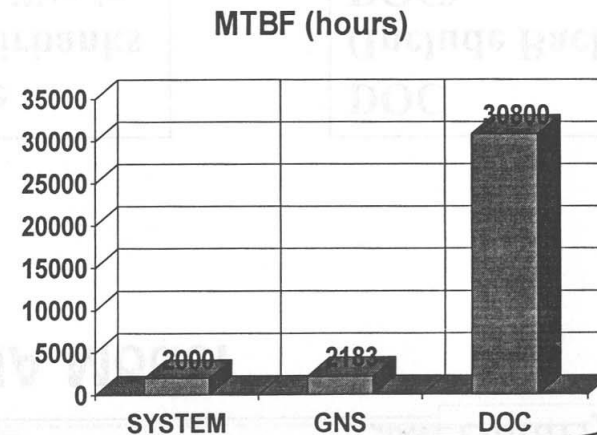
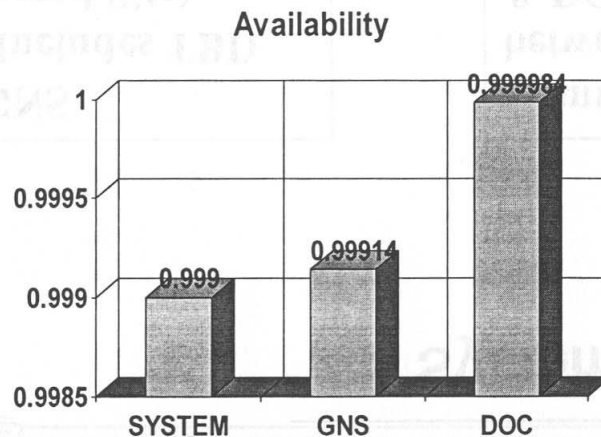
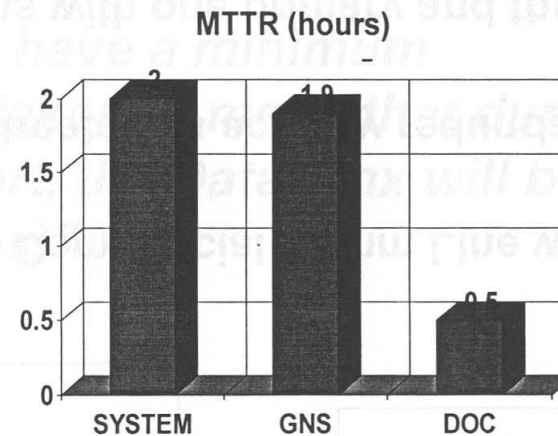


Preliminary Design Review



## Preliminary System/Subsystem Allocation

- Requirement: System A=0.999 of all scheduled passes
- System Allocation
  - MTBF = 2000 hrs
  - MTTR = 2 hrs
- Comm Line (TBR)
  - MTBF = 100,000 hrs
  - MTTR = 12 hrs
  - A = 0.99988



# Design for Reliability

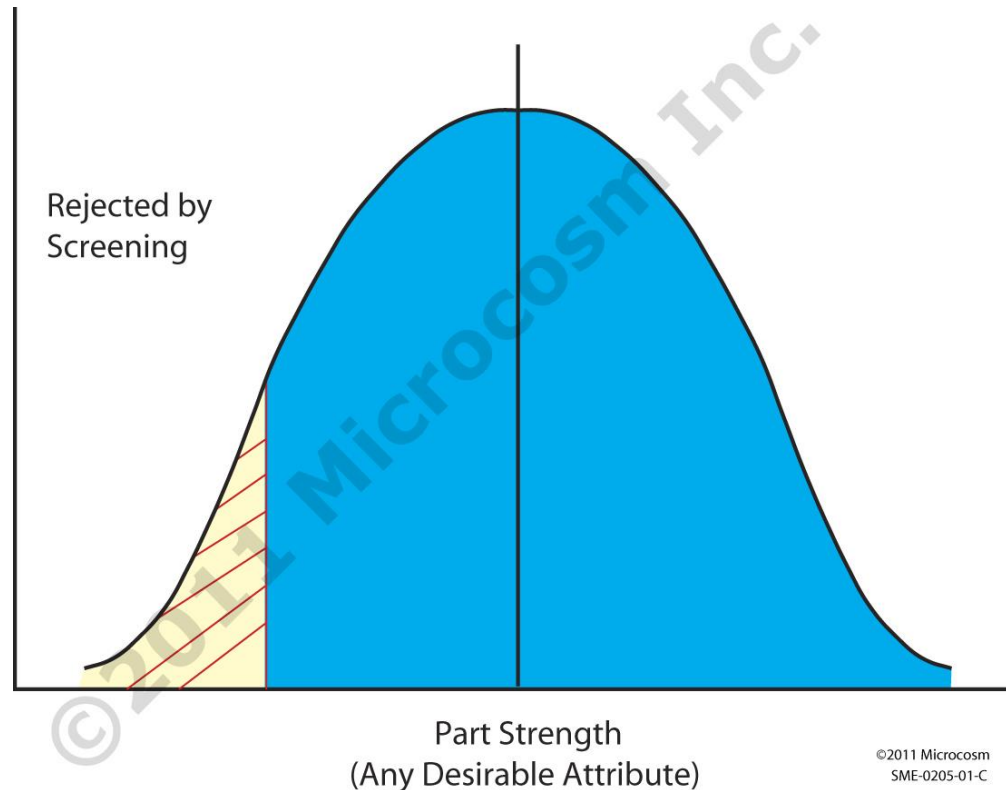
## Redundancy Strategies for Fault Tolerance

Strategy	Protection Against	Disadvantages
<b><i>Replication of the Same Design</i></b>	Random failures	Higher acquisition cost, weight, power
<b><i>Diverse Design for Each Channel</i></b>	Random failures and failures caused by design deficiencies	Higher acquisition cost, weight, power, design, and logistics costs
<b><i>Functional Redundancy</i></b>	Random failures and failures caused by design deficiencies	May not always be feasible—existence of diverse method is necessary
<b><i>Temporal Redundancy (Restart and Retry)</i></b>	Transient and intermittent failures; some classes of software failures	Not effective against permanent failures; failure will persist until system is restarted
<b><i>Information Encoding</i></b>	Single Event Upsets and digital transmission errors	Correction capabilities are usually limited to 1 or 2 bits per event

©2011 Microcosm Inc.

# Design for Reliability

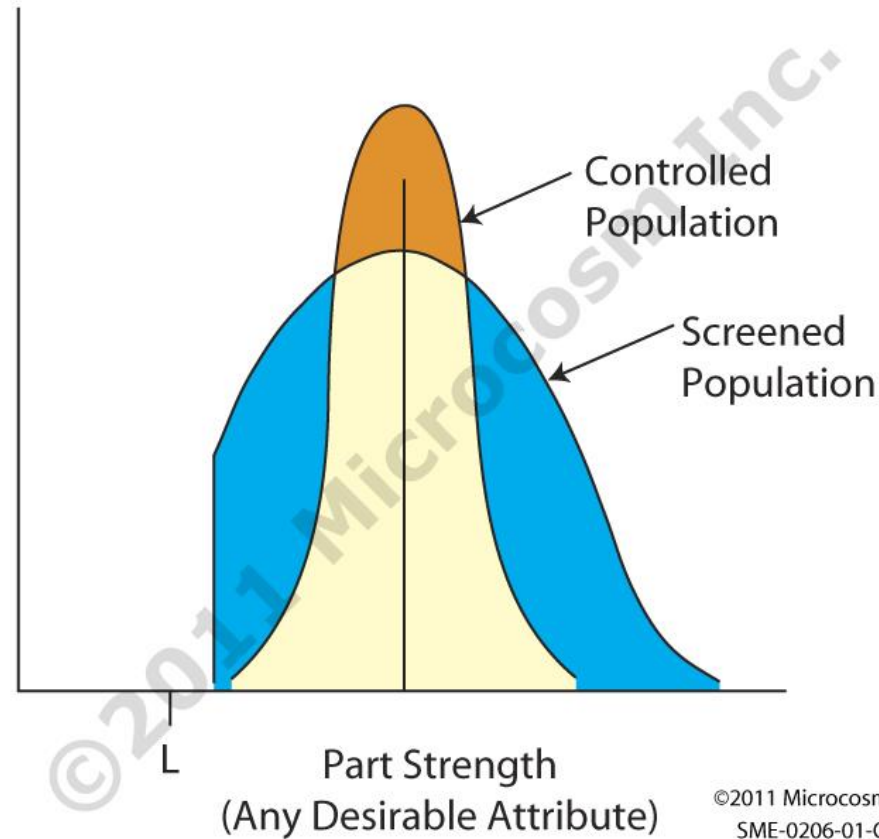
## Attribute Control by Screening



Screening rejects parts likely to fail in service.

# Design for Reliability

## Attribute Control by Process Control

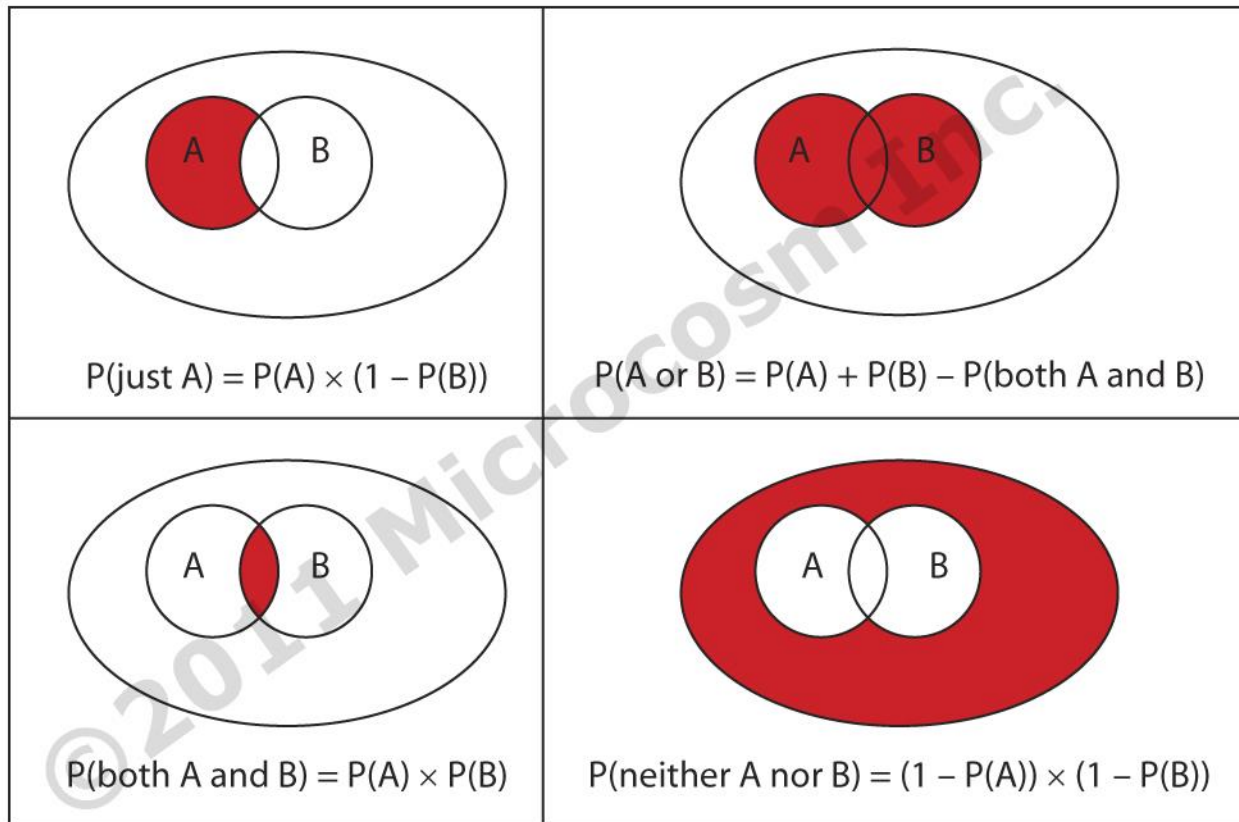


In a controlled population fewer parts are near the acceptance limit than in a screened population.



# Design for Reliability

## Four Possible Outcomes and Their Probabilities from Two Independent, Probabilistic Events



©2011 Microcosm SME-0304-01-C