CENG 5334
Fault Tolerant Computing
Fall 2017

Wrap Up Lecture

Outline (Thoughts and excerpts from past classes)

- Risk
  - Probabilistic Risk Assessment (PRA)
  - Business Continuity
- Hardware
  - Comments on High Reliability without Redundancy
  - 1553 Busses
  - XTMR Tool
  - X-38 System Integration and Test Facility (SITF)
  - Stratus and the Stock Exchange of India
  - Commercial Aircraft
- Software: Associated Technologies
  - COCOMO
  - Nano Technology
  - Error Tolerant Computing
  - CMMI
  - FT in UPC (Universal Product Codes)
  - FEMA
  - SIL – Safety Integrity Level
- FT In Our Daily Life
  - Automobiles
  - Health Care Systems
  - Warranty: Product Lifespan
- What I've Learned

PROBABILISTIC RISK ASSESSMENT & MANAGEMENT

TOOLS, TECHNIQUES AND APPLICATIONS

LECTURE OUTLINE

1. Basic Definitions
2. Risk Assessment
   - Categories of Risk Analysis
   - Types of Risk Assessment
   - Elements of Risk Assessment
   - Probabilistic Risk Assessment
   - Strength of PRA
3. Risk management
   - Cost-Benefit Analysis
   - Decision Making Techniques Using Risk Information

DEFINITION OF RISK

- Consequences of human or natural actions result in losses and gains.
- Risk implies something unwanted or to be avoided.
- One takes risk for possible gains.
- Questions: "does the ***gain*** outweighs the ***risk***"?
- If we only associate risk with losses (not gains) then one can say that we are risk averse, i.e., we only control and reduce our risks (Note that actions taken to reduce a risk can be considered gain in the sense that possible losses are reduced.)
- Risk has two components

  (1) Unwanted consequence (or loss) expressed in magnitude

  (2) Uncertainty in the occurrence of that loss (expressed in probability or frequency)

DEFINITION OF RISK

- Risk is a measure of the
  - potential loss occurred due to natural or human activities.
  - Potential losses are the adverse consequences of such activities in form of loss of human life, adverse health effects, loss of property, and damage to the natural environment.
- Risk analysis is the process of
  - characterizing,
  - managing and
  - informing others about existence, nature, magnitude, prevalence, contributing factors, and uncertainties of the potential losses.
- From an engineering point of view, the risk or potential loss is associated with exposure of the recipients to hazards, and can be expressed as a combination of the *probability* or *frequency*

- the loss may be external to the system, caused by the system to one or more recipients (e.g., human, organization, economic assets, and environment).
- Also the loss may be internal to the system, only damaging the system itself. An engineering system is defined as an entity composed of hardware, software and human organization.

DEMAND FOR RISK ANALYSIS

- We worry more about risk today exactly because we have more to lose and we have more disposable income to spend on risk reduction.

- A mechanism to control and avert risk has been to regulate manufacturing, operation and construction of complex systems.

- The conventional view of safety risk regulation is that the existence of risks is undesirable and, with appropriate technological interventions, we can eliminate those risks. However, this perspective does not recognize the risk reduction costs involved; the fact that a no-risk society would be so costly and infeasible.

- Risk analysis and especially Probabilistic Risk Assessment (PRA) can play pivotal roles in making design, manufacturing, operation, policy and regulatory decisions. Progress in the field of risk analysis and especially in PRA has been enormous.

CATEGORIES OF RISK ANALYSIS

- Health risk analysis

  Estimating potential diseases and losses of life affecting humans, animals and plants

- Safety risk analysis

  Estimating potential harms caused by accidents occurring due to natural events (climatic conditions, earthquakes, brush fires, etc.) or human-made products, technologies and systems (i.e., aircraft crashes, chemical plant explosions, nuclear plant accidents, technology obsolescence or failure);

- Security risk analysis

  Estimating access and harm caused due to war, terrorism, riot, crime (vandalism, theft, etc.) and misappropriation of information (national security information, intellectual property)

- Financial risk analysis

  Estimating potential individual, institutional and societal monetary losses such as currency fluctuations, interest rates, share market, project losses, bankruptcy, market loss, misappropriation of funds, and property damage;

- Environmental risk analysis

  estimating losses due to noise, contamination, and pollution in ecosystem (water, land, air and atmosphere) and in space (space debris)

TYPES OF RISK ANALYSIS

Risk analysis attempts to measure the magnitude of a loss (consequences) associated with complex systems, including evaluation, risk reduction and control policies. Generally there are three types of risk analysis:

- ✓Quantitative
- ✓Qualitative
- ✓A Mix of the two

ELEMENTS OF RISK ANALYSIS

Risk assessment is the process through which the chance or frequency of a loss and the magnitude of the loss (consequence) is measured or estimated.

Risk management is the process through which the potential (likelihood or frequency) of magnitude and contributors to risk are estimated, evaluated, minimized, and controlled.

Risk communication is the process through which information about the nature of risk (expected loss) and consequences, risk assessment approach and risk management options are exchanged, shared and discussed between the decision makers and other stakeholders.

RISK ASSESSMENT

- Risk assessment is the process of providing answer to four basic questions:

  1. What can go wrong?
  2. How likely is it?
  3. What are the losses (consequences)?

- Answering these questions could be simple or require a significant amount of analysis and modeling.

QUANTITATIVE DEFINITION OF RISK

Answers to:

(1) What can go wrong?
(2) What is the likelihood?
(3) What is the damage (loss or consequence)?

Scenario	Likelihood	Damage
S_1	l_1	X_1
S_2	l_2	X_2
S_3	l_3	X_3
⋮	⋮	⋮
S_N	l_N	X_N

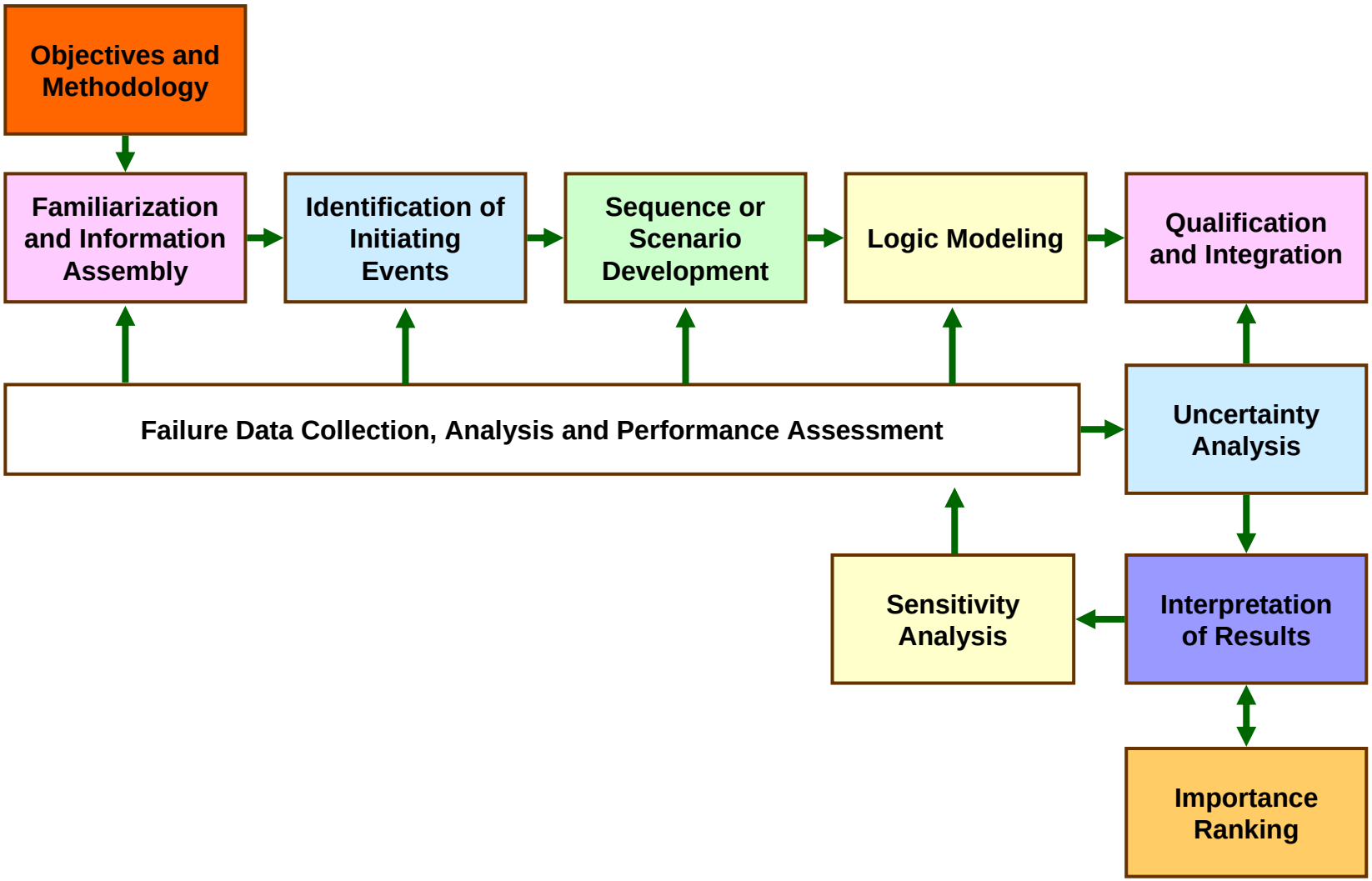
$$R = \text{RISK} = \{\langle S_1, l_1, X_1 \rangle\}$$

Risk "is" a set of triplets

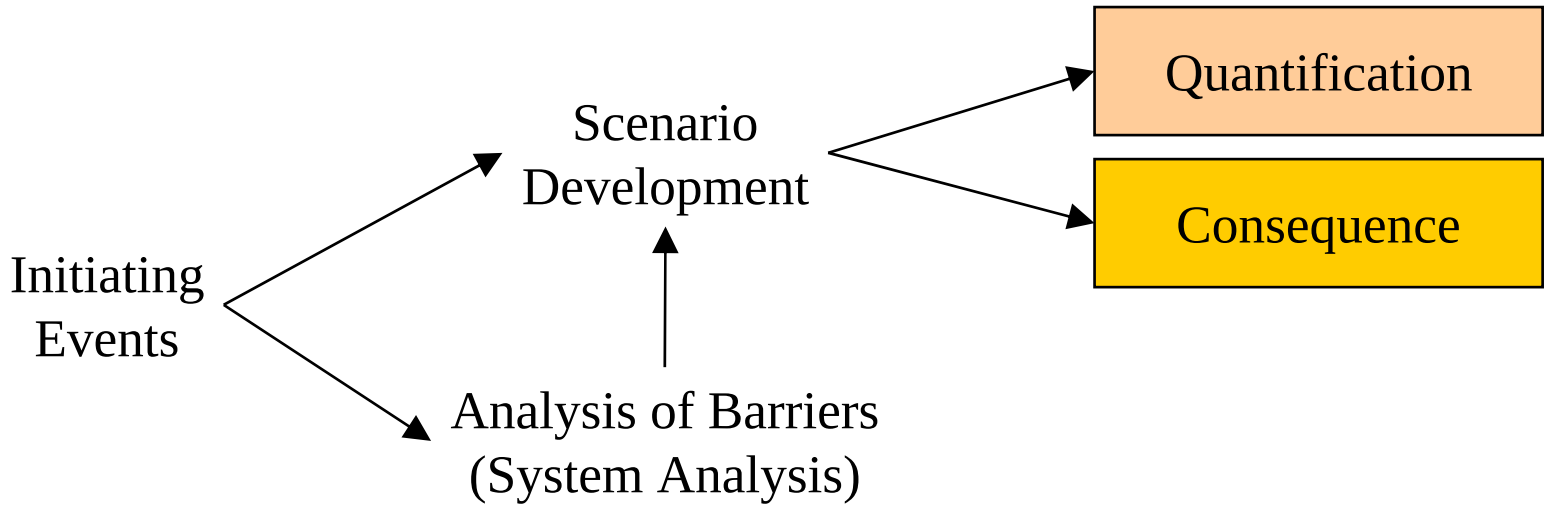
1. IDENTIFICATION OF HAZARDS

- Chemical (e.g., toxins, corrosive agents, smoke)
- Biological (e.g., viruses, microbial agents, bio-contaminants)
- Thermal (e.g., explosions, fire)
- Mechanical (e.g., impact from a moving object, explosions)
- Electrical (e.g., electromagnetic fields, electric shock)
- Ionizing radiation (e.g., x-rays, gamma rays)
- Nonionizing radiation (e.g., microwave radiation, cosmic rays)
- Information (e.g., propaganda, computer virus)

COMPONENTS OF THE OVERALL PRA PROCESS

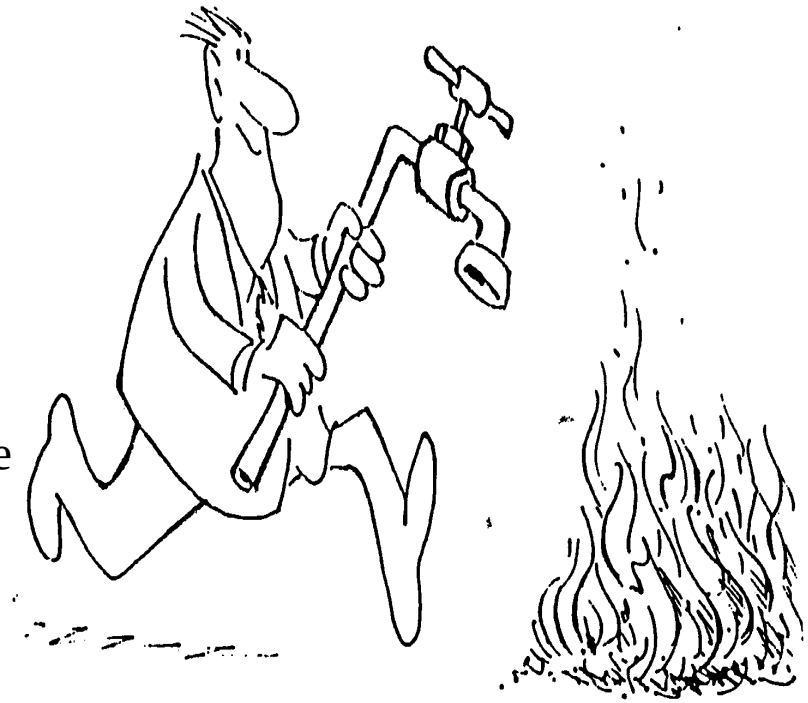


PROBABILISTIC RISK ASSESSMENT (PRA)



THE HUMAN ELEMENT

- **Nuclear** (Maintenance Error, Control Room Crew Error)
- **Aviation** (Maintenance Error, Flight Crew Error, Air Traffic Controller Error)
- **Chemical and Process** (Maintenance Errors)
- **Land and Sea Transportation** (Maintenance and Operator Errors)
- **Healthcare Industries** (Procedural Error, Operator Error)
- **Telecommunication** (Procedural Errors)



FAILURE DATA COLLECTION, ANALYSIS, AND PERFORMANCE ASSESSMENT

The following procedures should be followed in this step of the PRA:

1. Determine generic values of material strength or endurance, load or damage agents, failure times, failure occurrence rate and failures on demand for each item (hardware, human action, or software) identified in the PRA models. This can be obtained either from facility-specific or system-specific experiences, from generic sources of data, or both (see Chapter 4 for more details on this subject)
2. Gather data on hazard barrier tests, repair, and maintenance data primarily from experience, if available. Otherwise use generic performance data.
3. Assess the frequency of initiating events and other probability of failure events from experience, expert judgment, or generic sources. (See Chapter 4).
4. Determine the dependent or common cause failure probability for similar items, primarily from generic values. However, when significant specific data are available, they should be primarily used (see Chapter 4.)

QUANTIFICATION AND INTEGRATION

The following procedures should be followed as part of the quantification and integration step in the PRA:

1. Merge corresponding fault trees associated with each failure or success event modeled in the event tree scenarios (i.e., combine them in a Boolean form). Develop a reduced Boolean function for each scenario (i.e., truncated minimal cut sets).
2. Calculate the total frequency of each sequence, using the frequency of initiating events, the probability of barrier failure including contributions from test and maintenance frequency (outage), common cause failure probability, and human error probability.
3. Use the minimal cut sets of each sequence for the quantification process. If needed, simplify the process by truncating based on the cut sets or probability.
4. Calculate the total frequency of each scenario.
5. Calculate the total frequency of all scenarios of all event trees.

UNCERTAINTY ANALYSIS

Steps in uncertainty analysis include:

1. Identify models and parameters that are uncertain and the method of uncertainty estimation to be used for each.
2. Describe the scope of the PRA and
3. Estimate and assign probability distributions depicting model and parameter uncertainties in the PRA.
4. Propagate uncertainties associated with the hazard barrier models and parameters to find the uncertainty associated with the risk value.
5. Present the uncertainties associated with risks and contributors to risk in an easy way to understand and visually straightforward to grasp.

RISK RANKING AND IMPORTANCE ANALYSIS

Applications of importance measures may be categorized into the following areas:

1. (Re)Design: To support decisions of the system design or redesign by adding or removing elements (barriers, subsystems, human interactions, etc.)
2. Test and Maintenance: To Address questions related to the plant performance by changing the test and maintenance strategy for a given design.
3. Configuration and Control: To measure the significance or the effect of failure of a component on risk or safety or temporarily taking a component out of service.
4. Reduce uncertainties in the input variables of the PRAs.

RISK RANKING AND IMPORTANCE ANALYSIS

The following are the major steps of importance ranking:

1. Determine the purpose of the ranking and select appropriate ranking importance measure that has consistent interpretation for the use of the ranked results.
2. Perform risk ranking and uncertainty ranking, as needed.
3. Identify the most critical and important elements of the system with respect to the total risk values and total uncertainty associated with the calculated risk values.

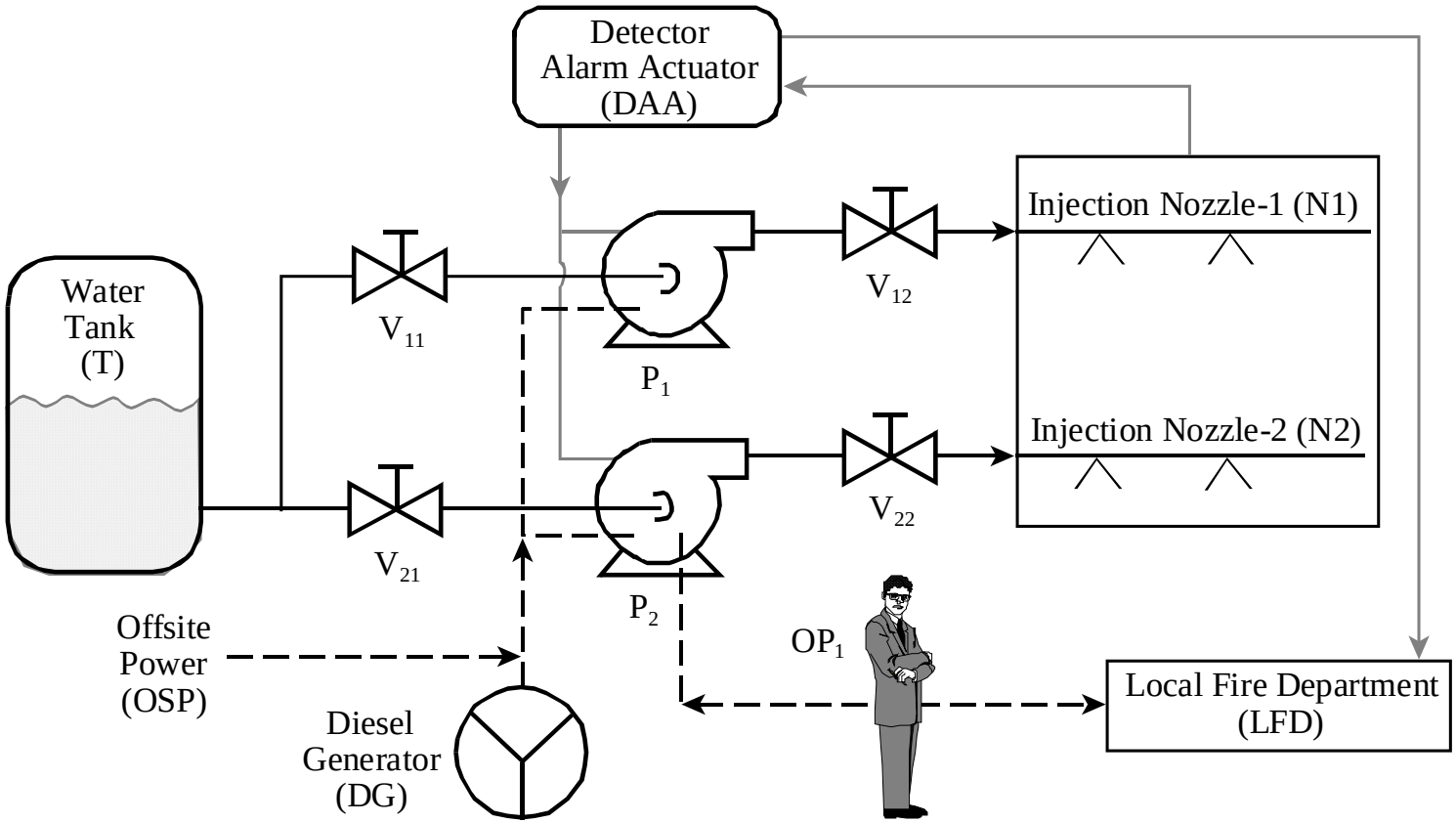
STRENGTH OF PRA

The most important strengths of the PRA, as the formal engineering approach to risk assessment are:

1. Provides an integrated and systematic examination of a broad set of design and operational features of an engineered system.
2. Incorporates the influence of system interactions and human-system interfaces.
3. Provides a model for incorporating operating experience with the engineered system and updating risk estimates.
4. Provides a process for the explicit consideration of uncertainties.
5. Permits the analysis of competing risks (e.g., of one system vs. another or of possible modifications to an existing system).
6. Permits the analysis of (assumptions, data) issues via sensitivity studies.
7. Provides a measure of the absolute or relative importance of systems, components to the calculated risk value.
8. Provides a quantitative measure of overall level of health and safety for the engineered system.

A SIMPLE EXAMPLE OF PRA

Risk Assessment of Fire Protection System



Example of PRA: Steps

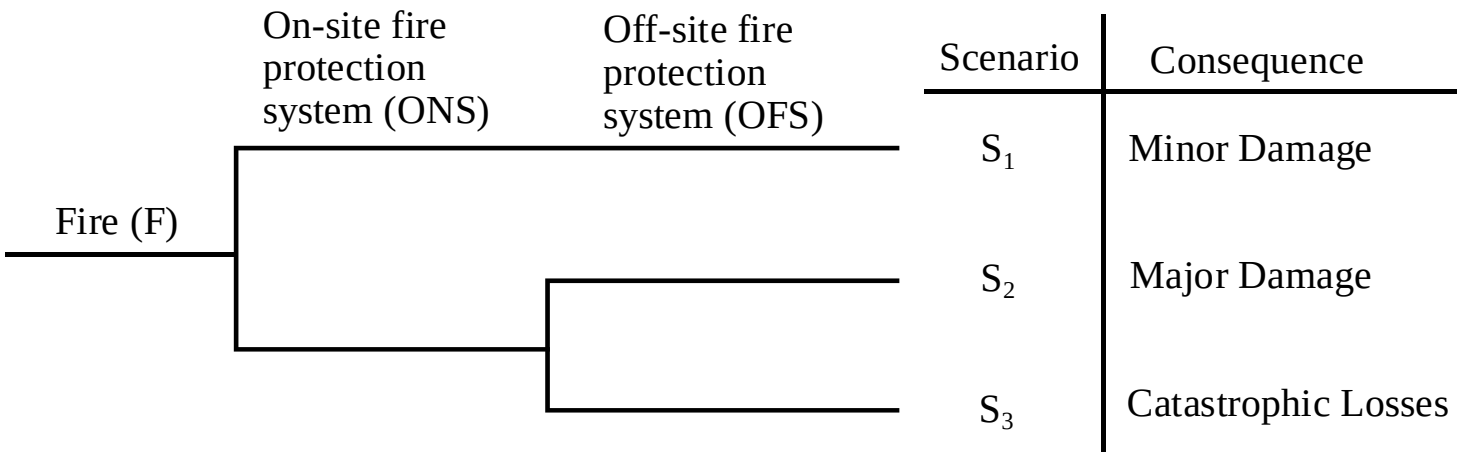
- Identification of Initiating Events
- Scenario Development
- Logic Modeling
- Failure Data Analysis
- Quantification
- Consequences
- Risk Value Calculation and Evaluation

EXAMPLE OF PRA (cont)

Initiating Events

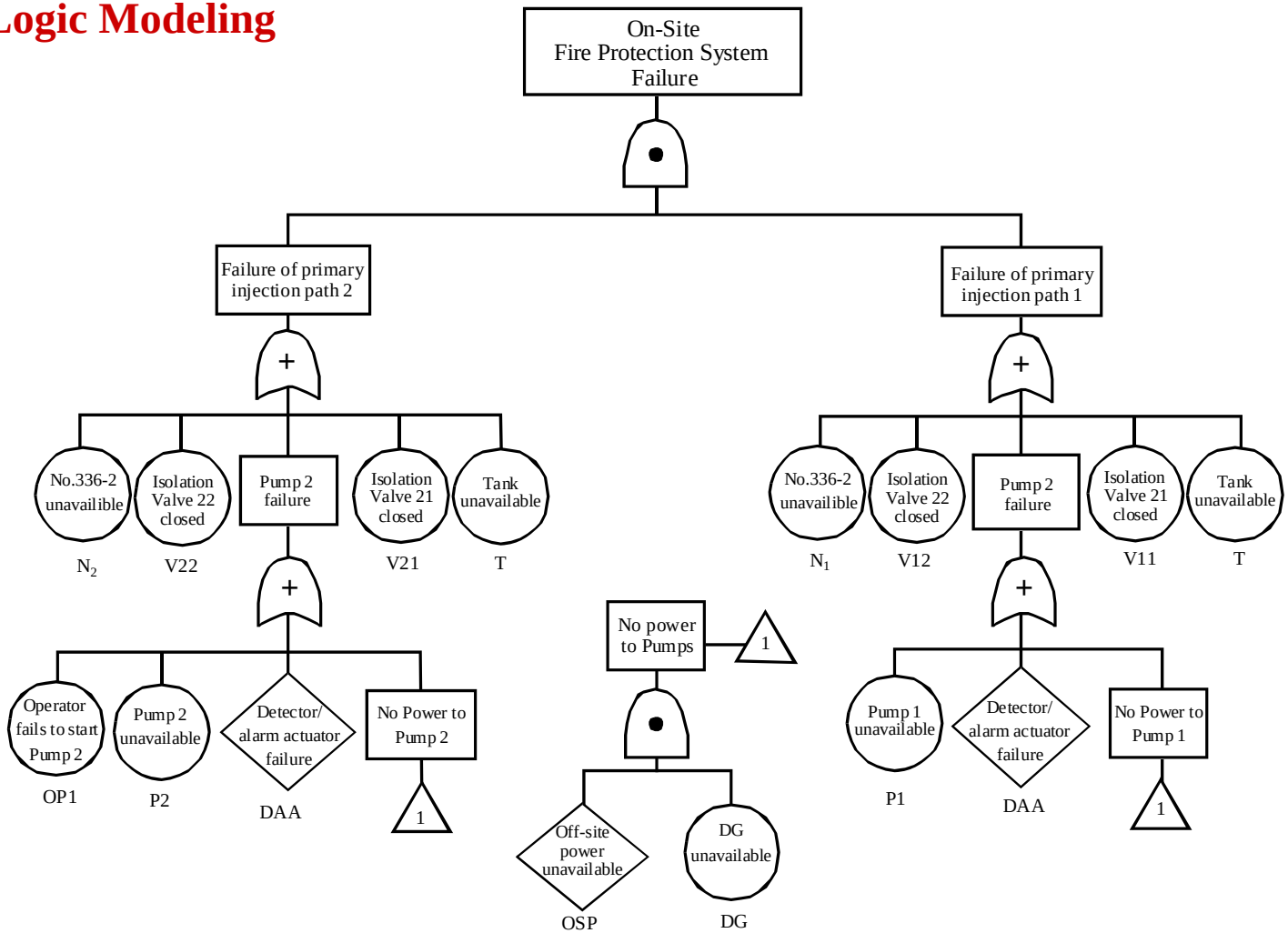
– Fire in Plant

Scenario Development



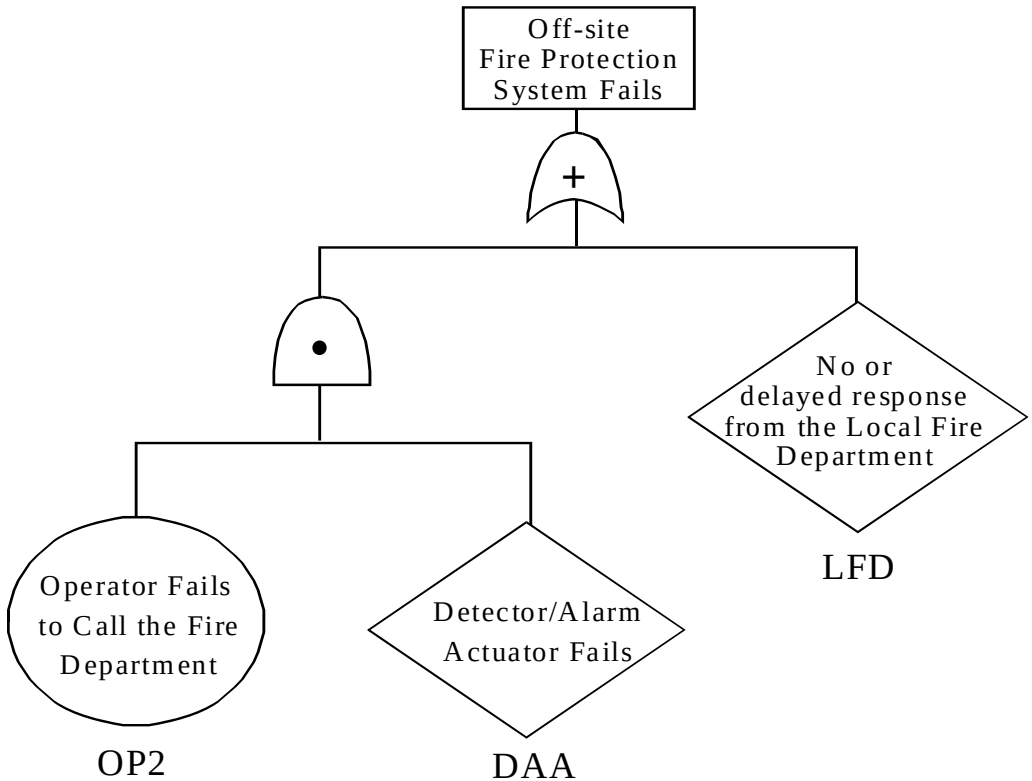
EXAMPLE OF PRA (cont)

Logic Modeling



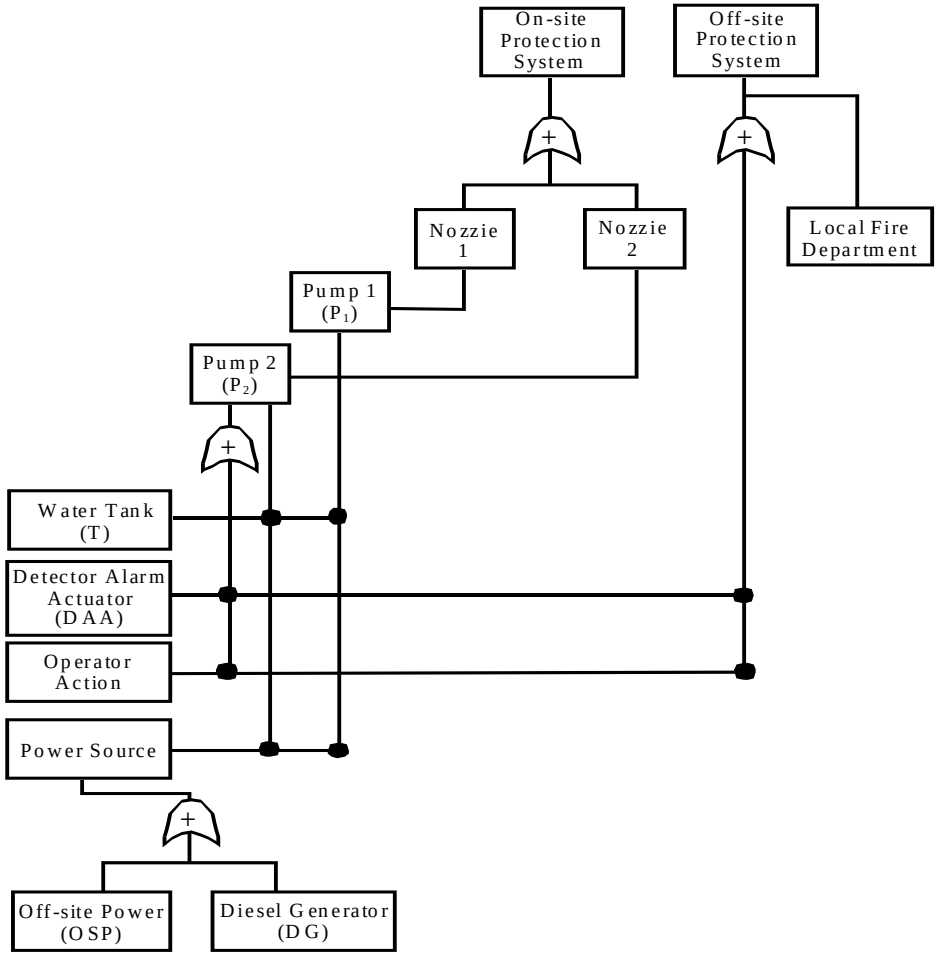
EXAMPLE OF PRA (cont)

Logic Modeling



A SIMPLE EXAMPLE OF PRA (cont)

Logic Modeling



EXAMPLE OF PRA (cont)

(Sources of Data and Failure Probabilities)

Failure Data Analysis

Failure Event	Plant-Specific Experience	Generic Data	Probability Used	Comments
Fire initiation frequency	No such experience in 10 years of operation.	5 fires in similar plants. There are 70,000 plant-years of experience.	F = 5/70,000 = 7.1E-4/yr.	Use generic data.
Pump 1 and Pump 2 failure	4 failures of two pumps to start per year each having an average of 10 demands (tests) per month. Repair time takes about 2.5 hours. No experience of failure to run.	Failure to run = 1×10^{-5} hr^{-1}.	$\frac{4}{2(12)(10)} = 1.7\times10^{-2}$/demand Unavailability $= 1.7\times10^{-2} + \frac{2.5(4)}{8760}$ $= 1.8\times10^{-2}$/demand $P_1 = P_2 = 1.8\times10^{-2}$	Failure to start is facility-specific. For failure to run is generic.

EXAMPLE OF PRA (cont)

(Sources of Data and Failure Probabilities)

Failure Data Analysis

Failure Event	Plant-Specific Experience	Generic Data	Probability Used	Comments
Common cause failure between Pump 1 and Pump 2	No such experience	Using the β-factor method, β = 0.1 for failure of pumps to start.	Unavailability due to common cause failure: $CCF = 0.1 \times 1.8 \times 10^{-2}$ $= 1.8 \times 10^{-3}/\text{demand}$	Assume no significant common cause failure exists between valves and nozzles.
Failure of isolation valves	2 failure to leave the valve in open position following 10 pump tests in one year.	Not used.	$v_{11} = v_{12} = v_{21} = v_{22}$ $= \frac{2}{10(12)(4)}$ $= 4.2 \times 10^{-3}/\text{demand}$	Facility-specific data used.

EXAMPLE OF PRA (cont)

(Sources of Data and Failure Probabilities)

Failure Data Analysis

Failure Event	Plant-Specific Experience	Generic Data	Probability Used	Comments
Failure of nozzles	No-such experience	1×10^{-5}/demand	$N_1 = N_2$ $= 1.0\times10^{-5}$/demand	Generic data used.
Diesel generator failure	3 failures in tests. 40 hours of repair per year.	3.0×10^{-2}/demand 3.0×10^{-3}/hr 40 run	failure on demand $= \frac{3}{12(10)}$ failure on demand = 2.5×10^{-2}/demand failure on run = 3.0×10^{-3}/hr Total failure of DG $= 2.5\times10^{-2} + 3.0\times10^{-3}$ $= 5.5\times10^{-2}$	Facility-specific data used for demand failure.

EXAMPLE OF PRA (cont)

(Sources of Data and Failure Probabilities)

Failure Data Analysis

Failure Event	Plant-Specific Experience	Generic Data	Probability Used	Comments
Loss of off-site power	No experience.	0.1/yr.	$\text{OSP} = 0.1 \times \frac{10}{8760} = 1.1 \times 10^{-4}/\text{demand}$	Assume 104 hours of operation for fire extinguisher and use generic data.
Failure of DAA	No Experience.	No data available.	DAA = 1×10^{-4}/demand.	This estimate is based on expert judgment.

EXAMPLE OF PRA (cont)

(Sources of Data and Failure Probabilities)

Failure Data Analysis

Failure Event	Plant-Specific Experience	Generic Data	Probability Used	Comments
Failure of operator to start Pump 2	No such experience	Using the THERP method	OP1 = 1×10^{-2}/demand	The method is discussed in Chapter 4
Failure of opera-tor to call the fire department	No such experience	1×10^{-3}	OP2 = 1×10^{-3}/demand	This is based on experience from no response to similar situations. Generic probability is used.
No or delayed response from fire department	No such experience	1×10^{-4}	LFD = 1×10^{-4}/demand	This is based on response to similar cases from the fire department. Delayed/no arrival is due to accidents, traffic, communication problems, etc.
Tank failure	No such experience	1×10^{-5}	T = 1×10^{-5}/demand	This is based on date obtained from rupture of the tank or insufficient water content.

EXAMPLE OF PRA (cont)

Quantification

These steps are described below:

1. The cut sets of the On-Site Fire Protection System Failure are obtained using the technique described in the section on Strength of PRA. These cut sets are listed in Table below.

Cut Sets of the On-Site Fire Protection System Failure

Cut Set No.	Cut Set	Probability (% contribution to the total probability)
1	T	1.0×10^{-5} (0.35)
2	DAA	1.0×10^{-4} (3.5)
3	OSP · DG	6.0×10^{-6} (0.21)
4	$N_2 \cdot N_1$	1.0×10^{-10} (~ 0)
5	$N_2 \cdot V_{12}$	4.2×10^{-8} (~ 0)
6	$N_2 \cdot P_1$	1.7×10^{-7} (~ 0)

EXAMPLE OF PRA (cont)

Cut Sets of the On-Site Fire Protection System Failure (cont)

Cut Set No.	Cut Set	Probability (% contribution to the total probability)
7	$N_2 \cdot V_{11}$	4.2×10^{-8} (~ 0)
8	$V_{22} \cdot N_1$	4.2×10^{-8} (~ 0)
9	$V_{22} \cdot V_{12}$	1.8×10^{-5} (0.64)
10	$V_{22} \cdot P_1$	7.1×10^{-5} (2.5)
11	$V_{22} \cdot V_{11}$	1.8×10^{-5} (0.64)
12	$V_{21} \cdot N_1$	4.2×10^{-8} (~ 0)
13	$V_{21} \cdot V_{12}$	1.8×10^{-5} (0.35)
14	$V_{22} \cdot P_1$	7.1×10^{-5} (2.5)
15	$V_{21} \cdot V_{11}$	1.8×10^{-5} (0.64)

EXAMPLE OF PRA (cont)

Cut Sets of the On-Site Fire Protection System Failure (cont)

Cut Set No.	Cut Set	Probability (% contribution to the total probability)
16	$OP_1 \cdot N_1$	1.0×10^{-7} (~ 0)
17	$OP_1 \cdot V_{12}$	4.2×10^{-5} (1.5)
18	$OP_1 \cdot P_1$	1.7×10^{-4} (6.0)
19	$OP_1 \cdot V_{11}$	4.2×10^{-5} (1.5)
20	$P_2 \cdot N_1$	1.7×10^{-7} (~ 0)
21	$P_2 \cdot V_{12}$	7.1×10^{-5} (2.5)
22	$P_2 \cdot P_1$	2.9×10^{-4} (0.3)
23	$P_2 \cdot V_{11}$	7.1×10^{-5} (2.5)
24	CCF	1.8×10^{-3} (63.8)
$Pr(ON) = \Sigma_i C_i = 2.8\times10^{-3}$		

EXAMPLE OF PRA (cont)

Quantification

These steps are described below (cont):

2. The cut sets of the Off-Site Fire Protection System Failure are similarly obtained and listed below.

Cut Sets of the Off-Site Fire Protection System

Cut Set No.	Cut Set	Probability (% contribution to the total probability)
1	LFD	1×10^{-4} (100)
2	$OP_2 \cdot DAA$	1×10^{-7} (~0)
Total $Pr^{(OFF)} \approx 1\times10^{-4}$		

EXAMPLE OF PRA (cont)

Quantification

These steps are described below (cont):

3. The cut sets of the three scenarios are obtained using the following Boolean equations representing each scenario:

$$\text{Scenario}-1=\text{F}\cdot\overline{\text{ONS}}$$

$$\text{Scenario}-2=\text{F}\cdot\text{ONS}\cdot\overline{\text{OFS}}$$

$$\text{Scenario}-3=\text{F}\cdot\text{ONS}\cdot\text{OFS}$$

4. The frequency of each scenario is obtained using data listed in Tables (Slide 185 to 188). These frequencies are shown in the Table "Dominant Minimal Cut-Sets of the Scenarios".

5. The total frequency of each scenario is calculated using the rare event approximation. These are also shown in the Table "Dominant Minimal Cut-Sets of the Scenarios".

EXAMPLE OF PRA (cont)

Consequences

In the scenario development and quantification tasks, we identified three distinct scenarios of interest, each with different outcomes and frequencies. The consequences associated with each scenario should be specified in terms of both economic and/or human losses. This part of the analysis is one of the most difficult for several reasons:

- Each scenario poses different hazards and methods of hazard exposure.
- The consequence of the scenario can be measured in terms of human losses.

Economic Consequences of Fire Scenarios

Scenario Number	Economic Consequence
1	$ 1,000,000
2	$ 92,000,000
3	$ 210,000,000

EXAMPLE OF PRA (cont)

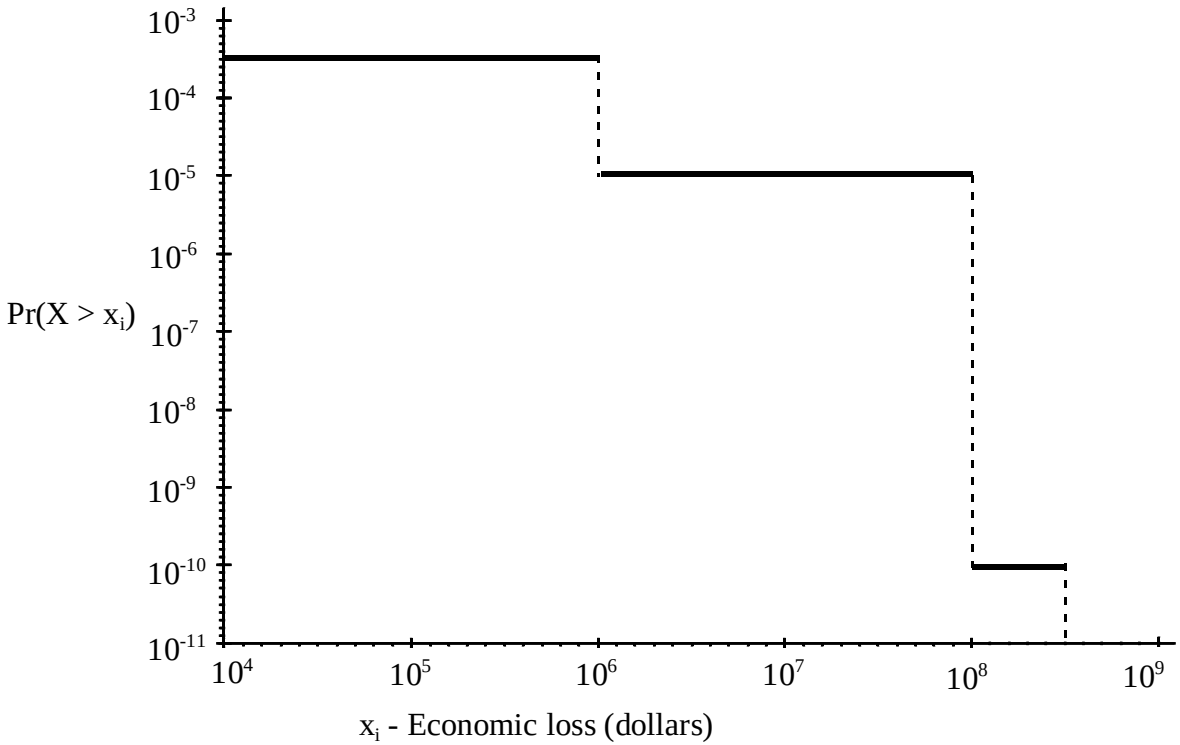
Risk Value Calculation and Evaluation

Using values from Table (Slide 190), we can calculate the risk associated with each scenario. These risks are shown in the Table below.

Scenario Number	Economic Consequence (expected loss)
1	(7.1×10^{-4}) ($1,000,000) = $ 710.000
2	(2.5×10^{-6}) ($92,000,000) = $ 230.000
3	(8.6×10^{-11}) ($210,000,000) = $ 0.018

EXAMPLE OF PRA (cont)

Risk Value Calculation and Evaluation



RISK MANAGEMENT

&

DECISION MAKING TECHNIQUES

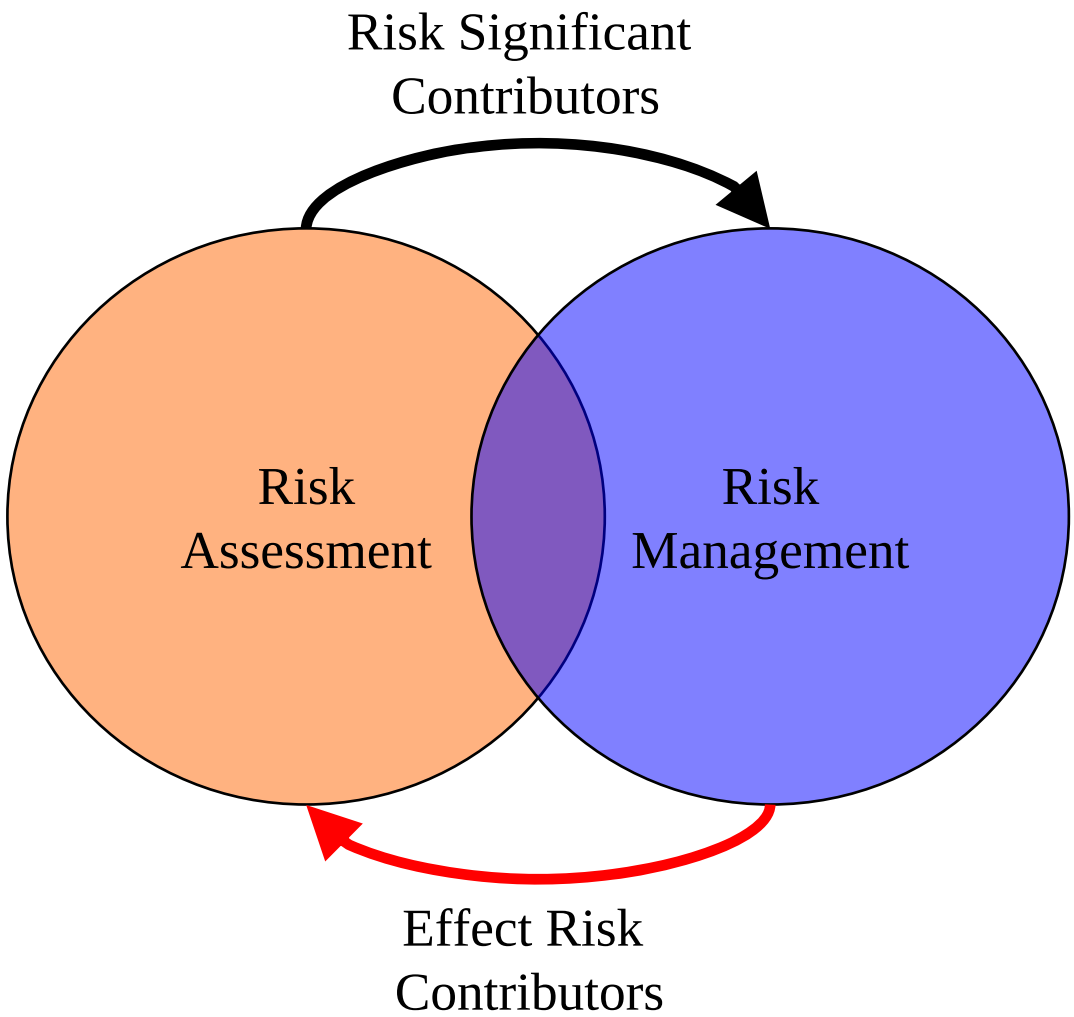
RISK MANAGEMENT

Is a practice involving coordinated activities to prevent, control and minimize losses incurred due to a risk exposure, weighing alternatives, and selecting appropriate actions by taking into account risks values, economic, technology constraints, legal and political issues.

- Continually assess the risk (what could go wrong?)
- Decide which risks are significant to deal with.
- Employ strategies to avert, control or minimize risks.
- Continually assess effectiveness of the strategies and revise them, if needed.

Risk management involves identifying the prime contributors to risk. Complex systems follow the 80:20 rules or the "Pareto's Principle“: more than 80% of the risk is contributed by less than 20% of risk scenarios or elements of the complex system. Risk management identify ways to avert control and minimize the 20%. That is, to achieve the highest risk reduction with the limited resources available

RISK ASSESSMENT-RISK MANAGEMENT SYNERGY



ECONOMIC METHODS IN RISK ANALYSIS

- **Cost-Benefit**
- Cost-Effectiveness
- Risk-Effectiveness Analysis

COST-BENEFIT METHOD

(As applied to Risk Management)

Risks are controlled (risk aversion) by reducing probability that a causative event will occurs or by minimizing exposure pathways.

Causative Control - quit smoking to avoid cancer, or use filtered cigarettes to hopefully reduce amount of cancer causing agent.

On the other hand smoking for example has both voluntary (smoker) and involuntary (premature death of the smoker or potential injuries to the passive smokers) risks.

Should risks and risk causing activities be regulated? When?

Cost-Benefit: (a measure of acceptability of risk)

Loss-Gain: So as to have one scale of measurement (for example $ or FLU)

COST-BENEFIT METHOD (cont)

Benefits: direct and indirect (can be voluntarily avoided)

Direct: profits from a new manufactured product

Indirect: benefit to the stores selling this product to the society gets the benefit of having a new product

Cost: direct loses are explicit and can not be voluntarily avoided when an activity is undertaken

A new plant commitment $\rightarrow$ investment of capital funds

Indirect costs or loses

Example: environmental pollution because of plant iteration

BALANCING GAINS AND LOSSES

Case	Direct Balance	Indirect Balance	Decision
1	$C_D < B_D$	$C_I < B_I$	Acceptable
2	$C_D > B_D$	$C_I > B_I$	Unacceptable
3	$C_D < B_D$	$C_I > B_I$	Unacceptable (unless allowed by Regulation)
4	$C_D > B_D$	$C_I < B_I$	Unacceptable (unless subsidized)

C_I - illegal drug operation in certain cause allowed under regulation (for example gambling operation) - nuclear power - between 2 and 4

B_I - since indirect societal benefit exceeds - direct balance so direct balance can be under written (development a new drug for curing cancer) - train subsidies

For comparing the effectiveness of multiple risk control measures, sometimes the benefit-cost ratio is used. The ratio is defined as

$$R_{b\text{-}c} = B/C$$

where, B is the benefit (direct, indirect or total) and C is the cost (direct, indirect or total).

COST-BENEFIT METHOD (cont)

Problem arises when using only analytical balance instead of subjective balance combination of both would be desirables

Example: Benefits are not ***always*** transferred to those receiving risk. So involuntary risk exist. For example, people near airport bear a high level of noise but they usually use airport least.

Therefore groups receiving risk and benefit must be clearly identified.

- short term benefits and long terms loses. Difficult to consider not good techniques exist for discounting future risk. On the other hand the reverse (short term risk and long term benefits) are more recognized to the society and more favorably accepted.

EXAMPLE 1: COST-BENEFIT METHOD

The case in question involves a scenario involving fuel tank side impacts in traffic accidents involving a particular design of pickup truck that may lead to explosions and fire-related injuries. The manufacturer is considering three risk reduction options. Determine the benefit-to-cost ratios for each design option. The data apply to reduction or prevention. The following risk reduction options are considered:

Option 1: Install a protective steel plate. Cost $14. This will effectively prevent all explosions.

Option 2: Install a Lexan plastic plate. Cost $4. This will prevent 95% of explosions.

Option 3: Install a plastic lining inside the fuel tank. Cost $2. This will prevent 85% of explosions.

EXAMPLE 1: COST-BENEFIT METHOD (cont)

The following risk and cost data apply to this vehicle when no risk-reduction option is implemented:

- Possible fatalities from vehicles already shipped: 180
- Expected cost per fatality: $500,000
- Number of injuries expected (no fatality): 200
- Cost per injury: $70,000
- Expected number of vehicles damaged (no injury): 3,000
- Cost to repair the vehicle: $1200
- Number of vehicles to be manufactured: 6,000,000

EXAMPLE 1: COST-BENEFIT METHOD (cont)

Solution:

The cost for each option is the cost of implementing the change. The benefits are in terms of lives saved and avoidance of injury and damage.

Option 1:

Cost = \$14 x 6,000,000 vehicles = \$84,000,000

Benefits = (180 lives saved)(\$500,000) + (200 injuries prevented)

x (\$70,000) + (3000 damaged vehicles prevented)(\$1200)

= \$107,600,000

R = \$107,600,000/ \$84,000,000 = 1.28

EXAMPLE 1: COST-BENEFIT METHOD (cont)

Option 2:

Cost = $4 x 6,000,000 = $24,000,000

Benefits = (95% accidents prevented) x [(180 fatalities)($500,000)

+ (200 injuries) x ($70,000) + (3000 vehicles)($1200)]

Benefits = 0.95 x $107,600,000

= $102,220,000

R = $102,220,000 /$24,000,000 = 4.25

EXAMPLE 1: COST-BENEFIT METHOD (cont)

Option 3:

Cost = \$2 x 6,000,000 = \$12,000,000

Benefits = (85% accidents prevented)[(180 fatalities)(\$500,000)

+ (200 injuries) x (\$70,000) + (3000 vehicles damage)

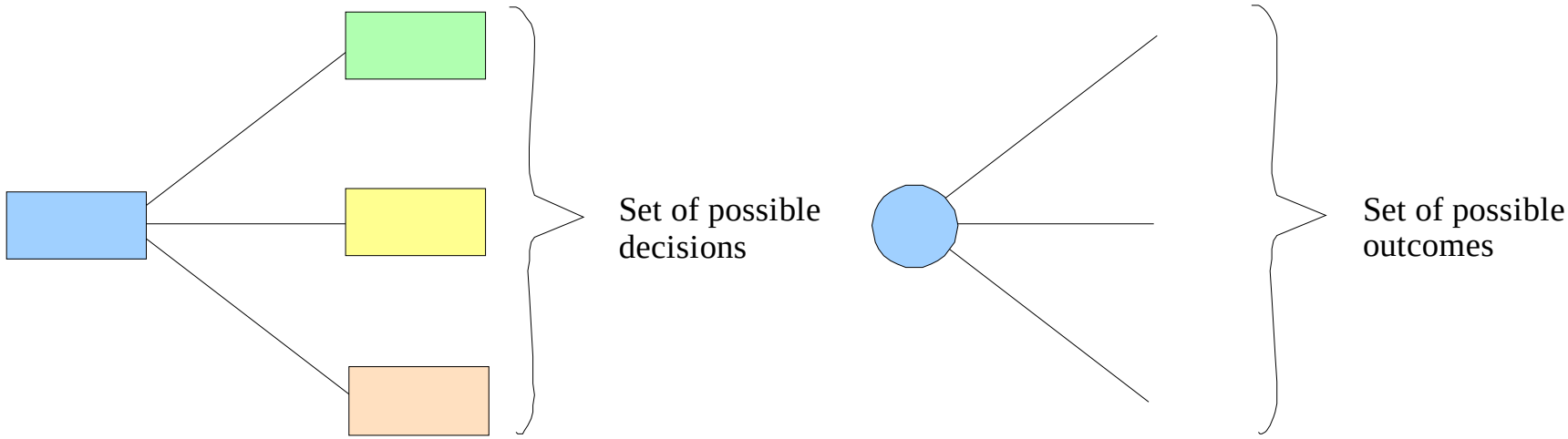
= 0.85 x \$107,600,000 = \$91,460,000

R = \$91,460,000/\$12,000,000 = 7.62

Option 3 has the highest benefit/cost ratio (R). As noted earlier, the decision should not be solely based on this figure of merit, as other indirect factors such as the manufacturer's reputation should also be considered.

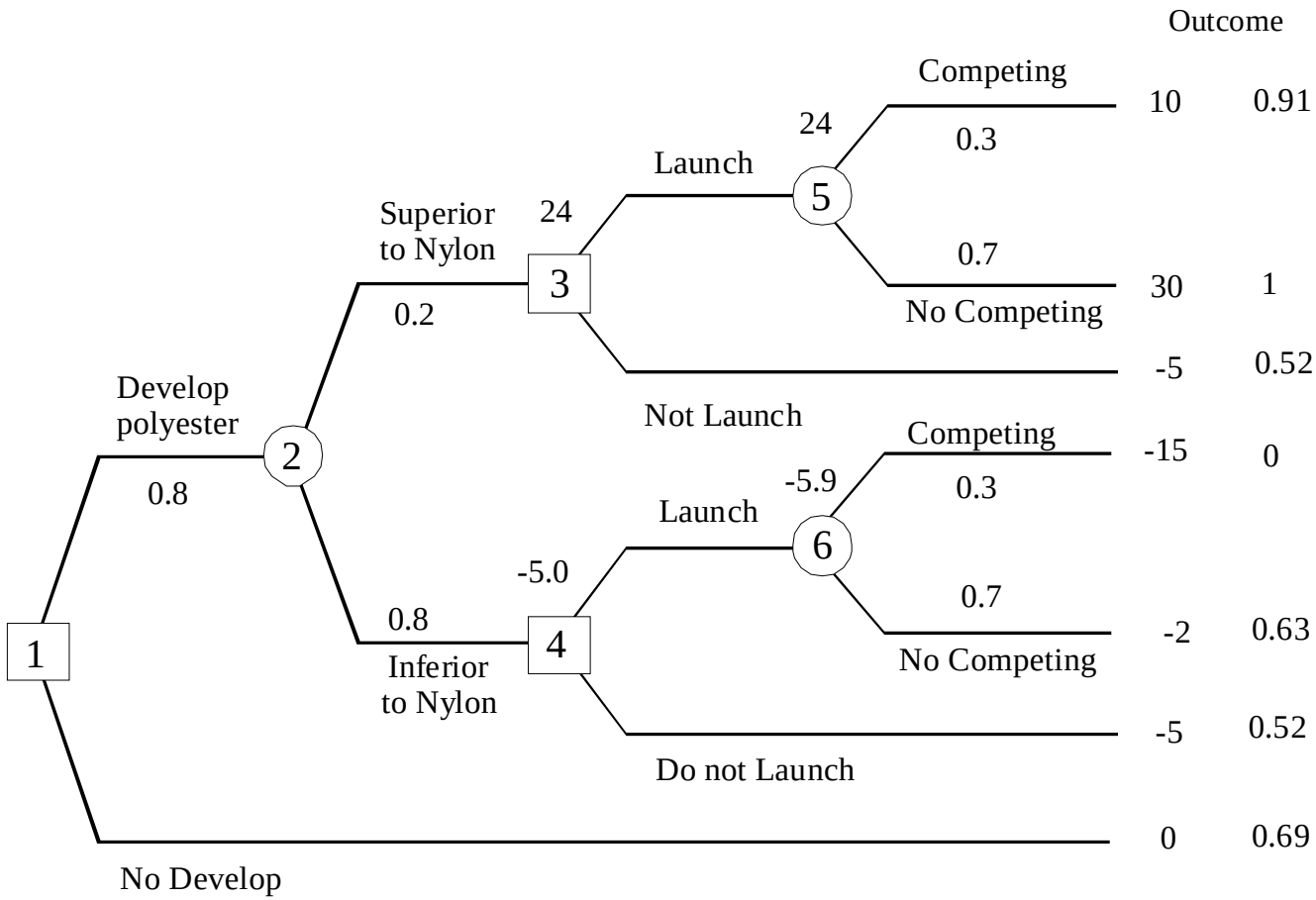
DECISION TREE ANALYSIS

Decision Trees are good for helping a risk manager to choose between several courses of risk control actions. They are highly effective structures within which one can lay out risk control solutions and investigate the possible outcomes of choosing such solutions



EXAMPLE 1: DECISION TREE

The tree below shows the developed decision tree and all sub-decisions and events involved



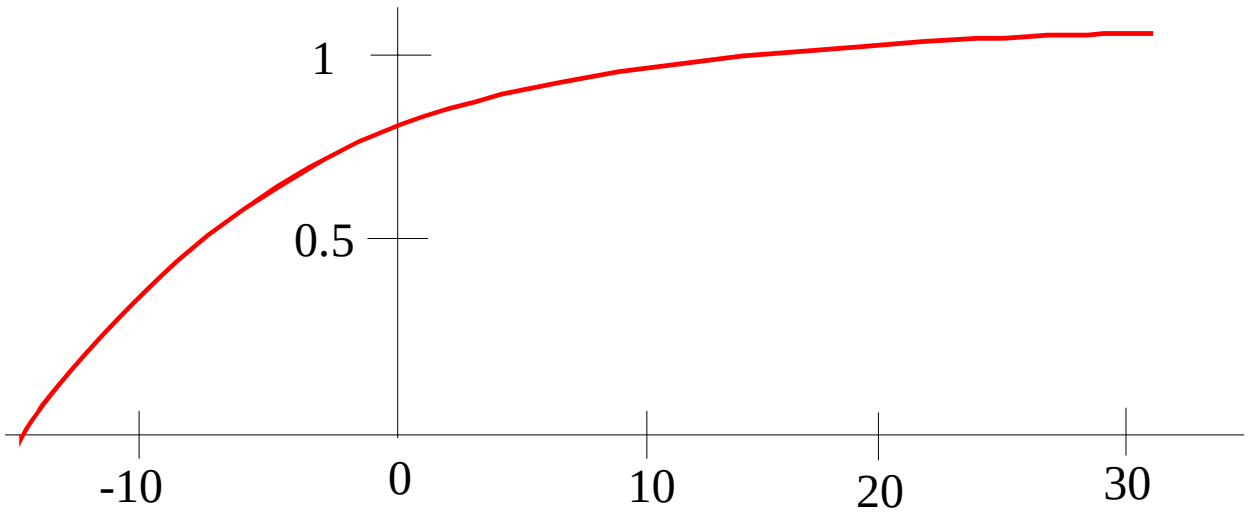
EXAMPLE 1: DECISION TREE (cont)

Risk = expected monetary value (EMV)

EMV

node 5 = 0.3 x 10 + 0.7 x 30 = 24

node 6 = 0.3 x -15 + 0.7 x -2 = -5.9



Utility Function for Payoff

EXAMPLE 1: DECISION TREE (cont)

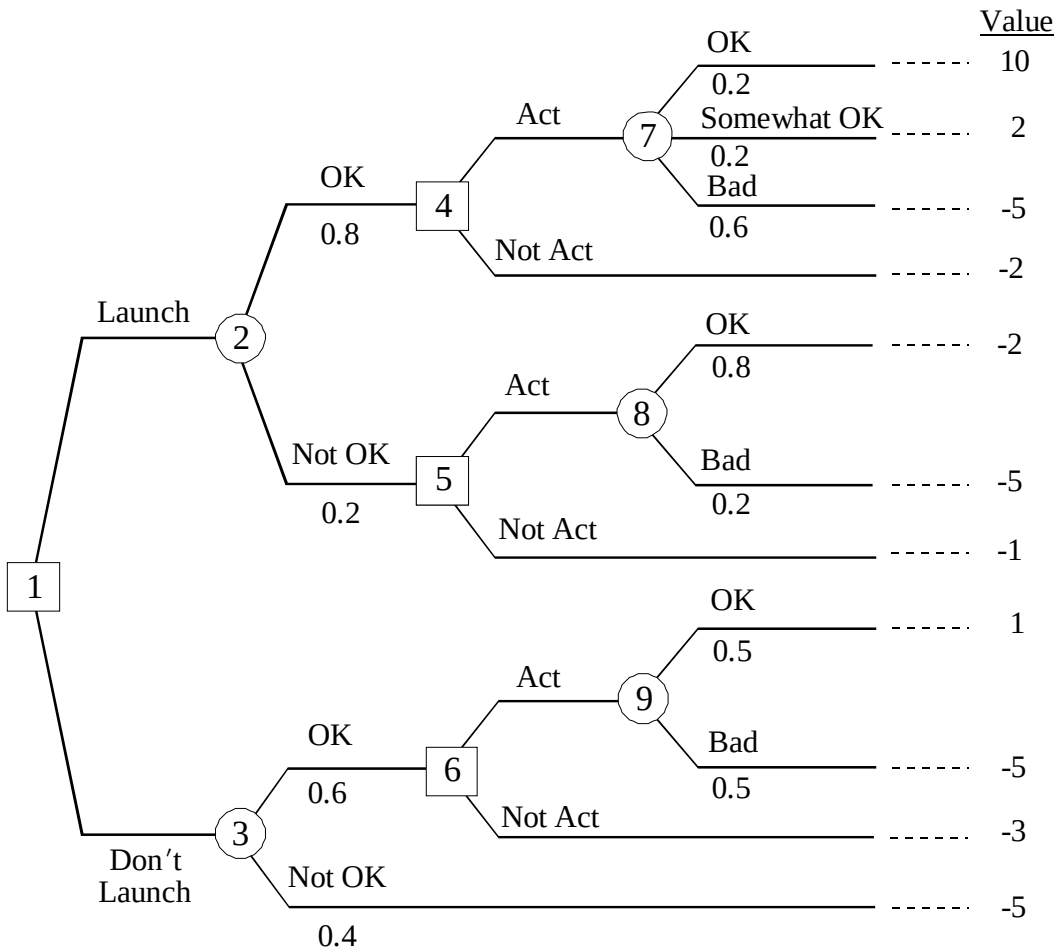
Based on the value function above, the value of each node is summarized.

Node	Expected Value Based on Actual Outcomes	Expected Value Based on the Value Judgment
1	0.8	0.69
2	0.8	0.61
3	24	0.97
4	-5	0.52
5	24	0.97
6	-5.9	0.44

Clearly in both evaluations, the value of node 1 (the main decision) is positive and, therefore, proceeding with the implementation of the proposed risk control solution is warranted.

EXAMPLE 2: DECISION TREE

For the following decision tree describe the outcome and the best decision



EXAMPLE 2: DECISION TREE (cont)

Solution:

The decision nodes (□) are 1, 4, 5, 6 and the chances nodes (o) are 2, 3, 7, 8, 9. For this decision tree, the outcome and the best decision are calculated according to the following:

Multiplying the payoff values by probability for chances nodes 7, 8 and 9:

Node 7: $(0.2 \times 10) + (0.2 \times 2) + (0.6 \times -5) = -0.6$
Node 8: $(0.8 \times -2) + (0.2 \times -5) = -2.6$
Node 9: $(0.5 \times 1) + (0.5 \times -5) = -2.0$

EXAMPLE 2: DECISION TREE (cont)

Using the above values and choosing the maximum at the decision nodes 4, 5 and 6:

At **Node 4** (maximum) between -0.6 and -2.0, choose -0.6.
At **Node 5** (maximum) between -2.6 and -1.0, choose -1.0.
At **Node 6** (maximum) between -2.0 and -3.0, choose -2.0.

Then, the values at chance nodes 2 and 3 will be:

Node 2: $(-0.6 \times 0.8) + (-1.0 \times 0.2) = -0.68$
Node 3: $(-2.0 \times 0.6) + (0.4 \times -5) = -3.2$

Therefore, the best decision is to "Launch" even though it has a negative payoff it is still greater than "Do Not Launch" negative payoff.

REMARKS ON DECISION TREES

Decision trees provide an effective method for policy and other decision making problems because they:

- clearly lay out the problem so that all options can be evaluated,
- analyze fully the possible consequences of a decision,
- provide a framework to quantify the values of outcomes and the probabilities of achieving them, and
- help to make the best decisions on the basis of existing information and best guesses.

As with all decision making methods, decision tree analysis should be used in combination with common sense, as decision trees are just one part of the actual risk management and control decision.

BUSINESS CONTINUITY/DISASTER RECOVERY PLAN

Syed Mohammad Ali Rizvi

Definition

"The purpose of business continuity/disaster recovery is to enable a business to continue operations in the event of a disruption and to survive a disastrous interruption to the information systems"

BCP / DRP

BUSINSS CONTINUITY PLAN (BCP)

It is a process designed to reduce the organization's risk for an unexpected disruption of the critical functions/operation necessary for the survival of the organization.

BUSINESS IMPACT ANALYSIS (BIA)

It is one of the key steps in developing the business continuity plan. This phase involves identifying the various events that could impact the continuity of operations and their impact on the organization.

BIA / DRS

DISASTER RECOVERY PLAN (DRP)

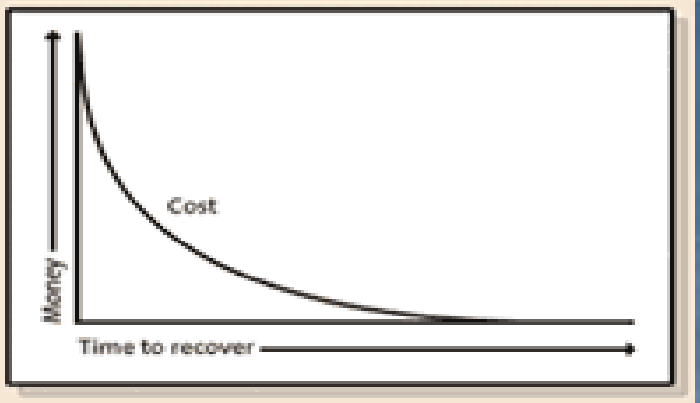
It is generally the plan followed by Information System to recover an IT processing facility or by business units to recover an operational facility. The plan must be consistent with, and support the overall plan of the organization

DEVELOPING RECOVERY STRATEGIES (DRS)

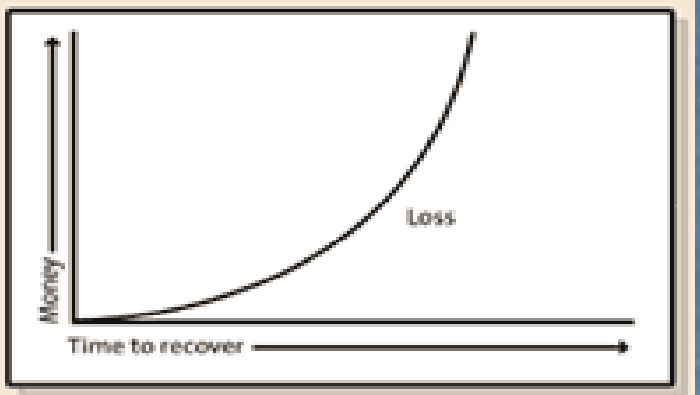
The next phase in the continuity plan development is to identify the various recovery strategies and select the most appropriate strategy for recovering from a disaster.

RECOVERY STRATEGY

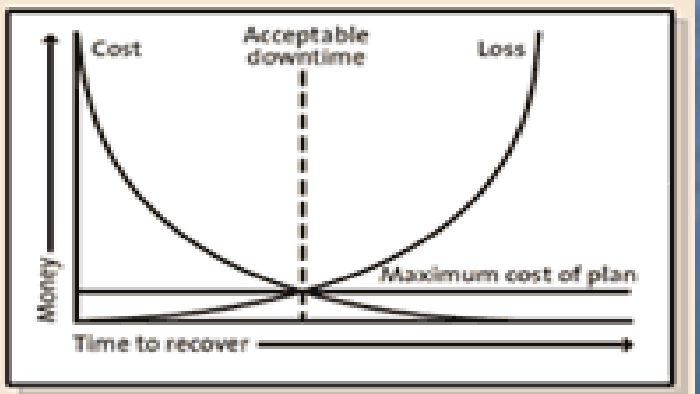
- The criticality of the business process and the applications supporting the processes.
- Cost
- Time required to recover
- Security



Cost of Recovery



Loss due to unavailability of entity.

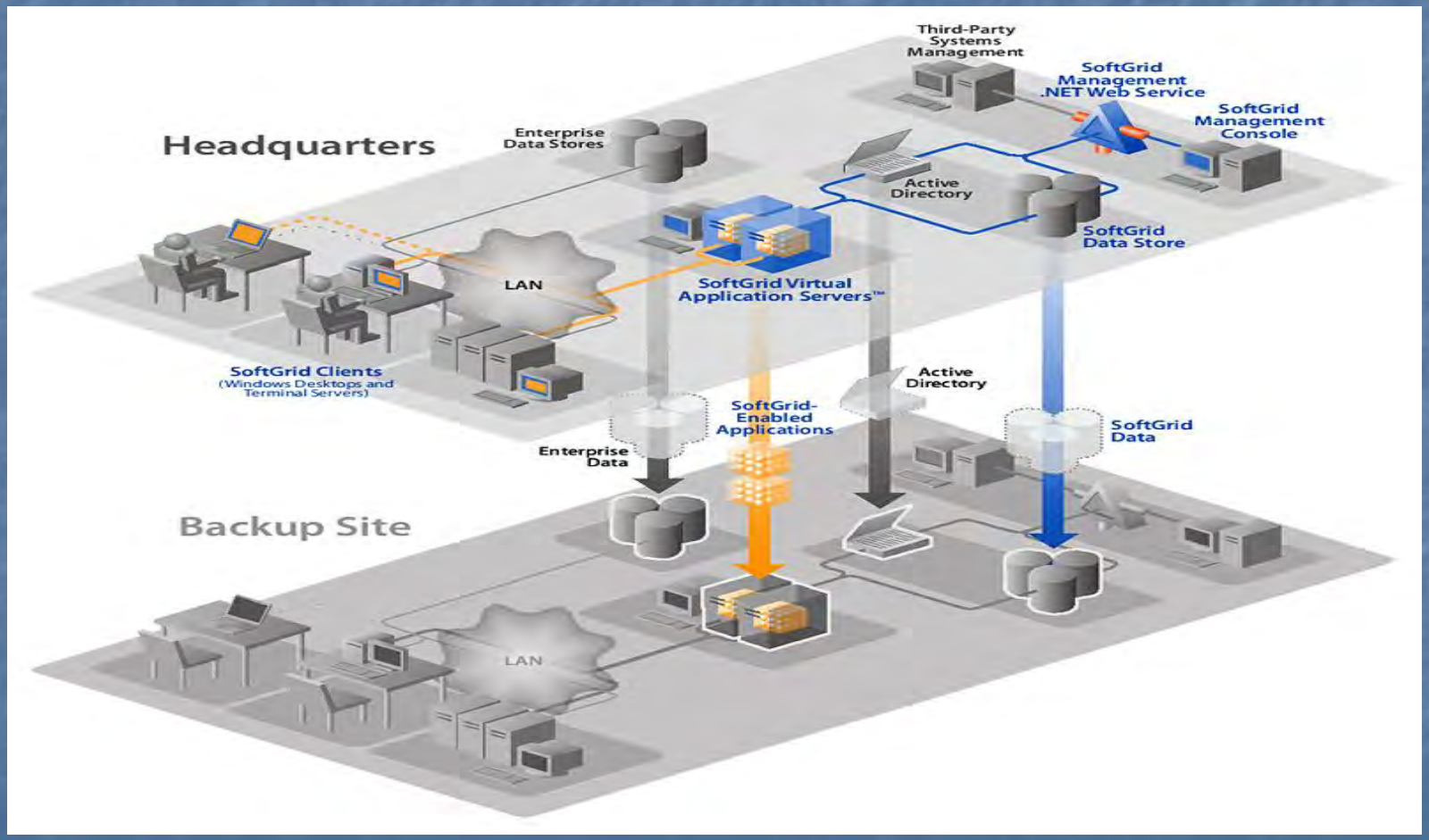


Maximum justfiable cost of plan.

RECOVERY STRATEGY

- Hot sites.
- Warm sites.
- Cold sites.
- Reciprocal arrangements with other companies.

HOT SITES


Third-Party Systems Management
SoftGrid Management .NET Web Service
SoftGrid Management Console
Headquarters
Enterprise Data Stores
Active Directory
SoftGrid Data Store
LAN
SoftGrid Virtual Application Servers™
SoftGrid Clients
(Windows Desktops and Terminal Servers)
Active Directory
SoftGrid-Enabled Applications
SoftGrid Data
Enterprise Data
Backup Site
LAN

WARM SITES

These are partially configured, usually with network connections and selected peripheral equipment, but without the main computer.

COLD SITES

They have only the basic environment to operate an information processing facility. The cold site is ready to receive equipment, but does not offer any components at the site in advance of the need.

RECIPROCAL AGREEMENTS

They are between two or more organizations with similar equipment or applications. Under the agreement, participants promise to provide computer time to each other when an emergency arises.

COMPONENTS OF AN EFFECTIVE BUSINESS CONTINUITY PLAN

TELECOMMUNICATION NETWORK

Thresholds of outage for each telecommunications capability should be identified.

ALTERNATIVES

- Providing multiple paths between routers
- Fiber optic ring
- Dial Up
- Wireless connection

FAULT TOLERANT SERVERS

Fault-tolerant servers provide for fail-safe redundancy through mirrored images of the primary server. Using this approach also may entail distributed processing of a server load, a concept referred to as load balancing or clustering.

RAID

RAID provides performance improvements and fault-tolerant capabilities via hardware software solutions, onto which a series of multiple disks are written to, improve performance.

Business Continuity vs Disaster Recovery

The sole purpose of **Business Continuity** is to maintain a minimum level of service while restoring the organization to business as usual

Disaster recovery is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster

Business Continuity is PROACTIVE; its focus is to avoid or mitigate the impact of a risk

Disaster Recovery is REACTIVE; its focus is to pick up the pieces and to restore the organization to business as usual after a risk occurs

Disaster Recovery is an integral part of a Business Continuity plan

Risk- Types

A few Risk Types :

- Aircraft accident
- Drought
- Electrical failure
- Epidemic
- Fire
- Flood
- Hacked database
- Heat
- Hurricane
- Internet failure
- Intranet failure
- IT/MIS
- Loss of key personnel
- Rail accident
- Stock value
- Tornado
- Traffic accident
- Wildfire

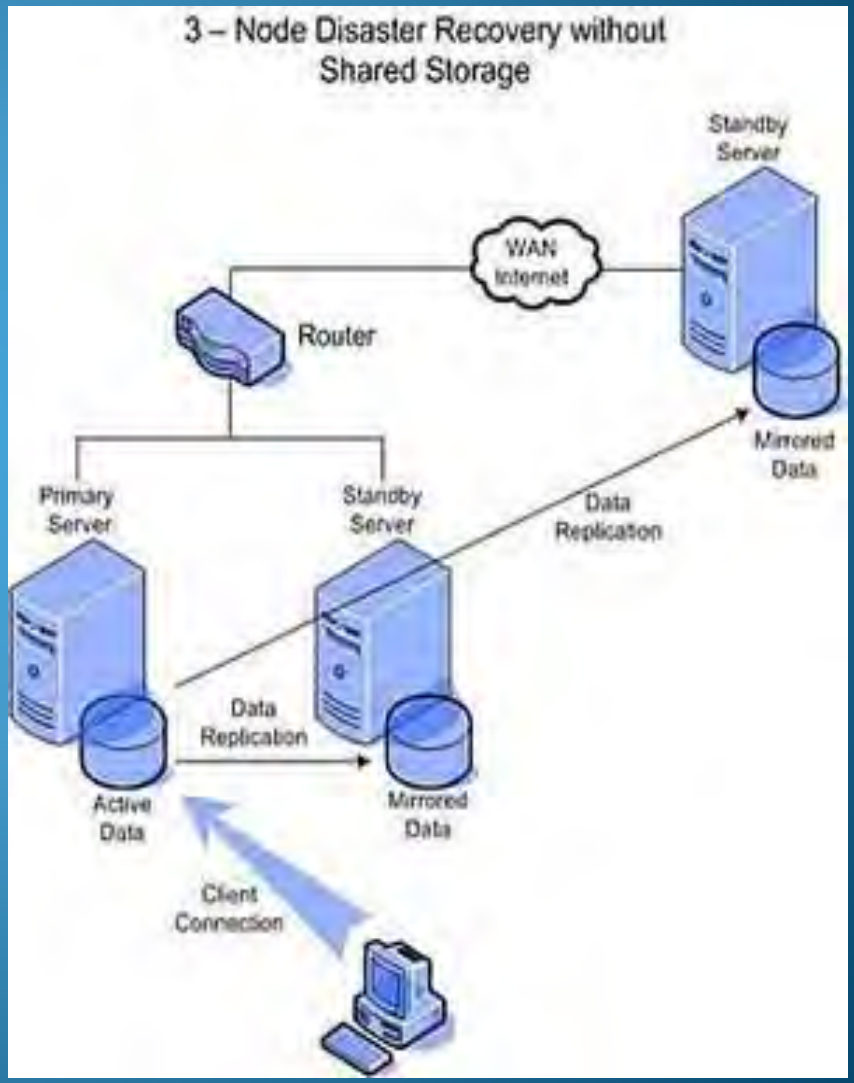
Not all risks present the same danger to an organization

Risks are rated based on

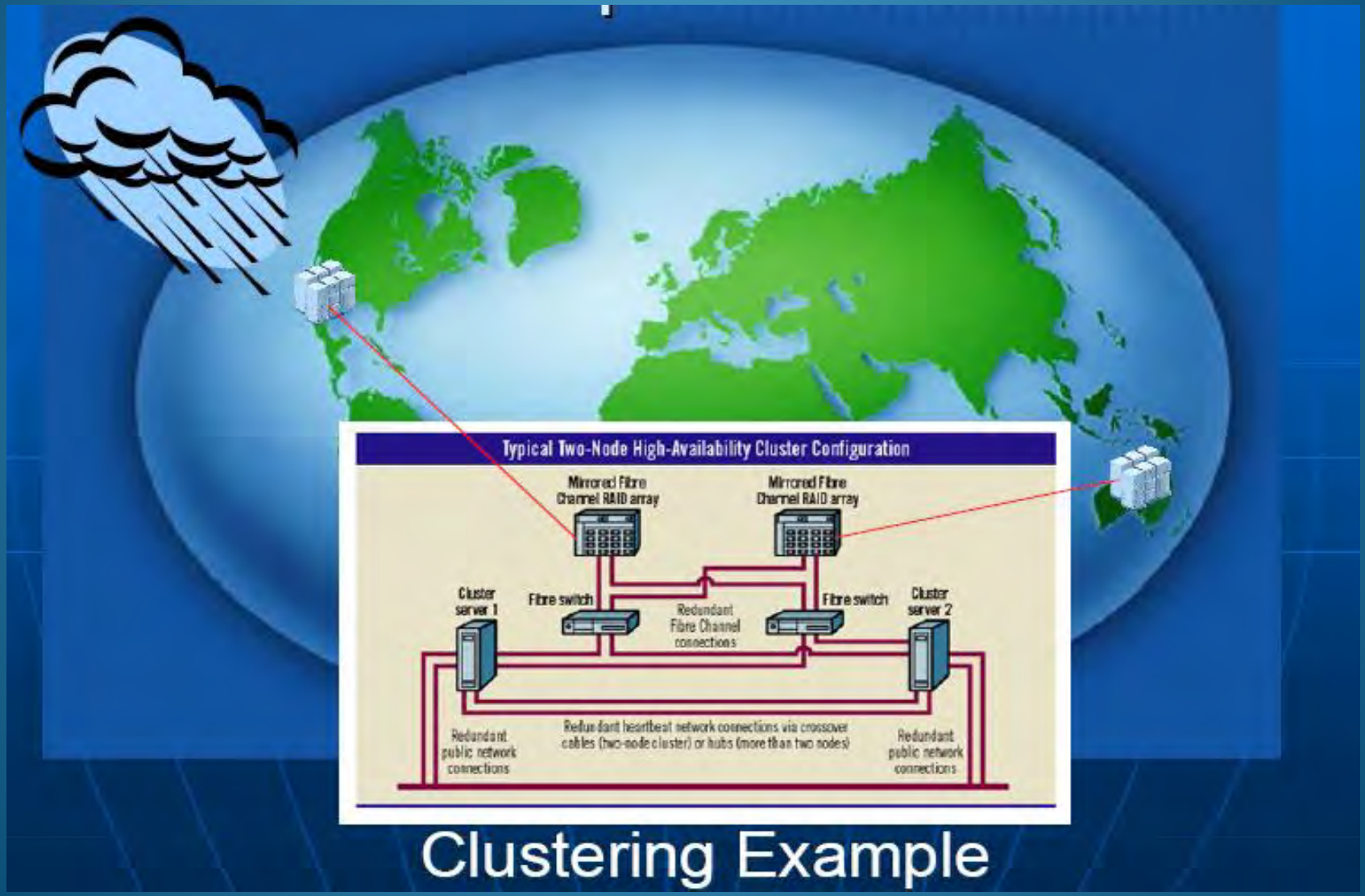
- Probability of occurrence
- Impact on the organization

Disaster Recovery Solution - Redundant Network in Software System

- The two network infrastructures, primary and Disaster should be divided into distinctive zones.
- The primary network should have installed proper attacking detection mechanisms such as intrusion prevention systems in order to monitor, alarm and activate the overlay network in situations of extreme attacks.
- Both Primary and Disaster should use replication and redundancy mechanisms that will enable the protection of data. Backup schemas and mirroring mechanisms should be designed to provide data availability at all times.
- Both Primary and Disaster should use different access network and different public IP to prevent attacks



Disaster Recovery Solution
- Redundant Architecture in Software System



TESTING

- Pre-testing
- Testing
- Post – testing
- Paper test
- Full Operational Test

Outline (Thoughts and excerpts from past classes)

- Risk
  - Probabilistic Risk Assessment (PRA)
  - Business Continuity
- **Hardware**
  - Comments on High Reliability without Redundancy
  - 1553 Busses
  - XTMR Tool
  - X-38 System Integration and Test Facility (SITF)
  - Stratus and the Stock Exchange of India
  - Commercial Aircraft
- Software: Associated Technologies
  - COCOMO
  - Nano Technology
  - Error Tolerant Computing
  - CMMI
  - FT in UPC (Universal Product Codes)
  - FEMA
  - SIL – Safety Integrity Level
- FT In Our Daily Life
  - Automobiles
  - Health Care Systems
  - Warranty: Product Lifespan
- What I've Learned

Common Sense Approach to High Reliability

- Redundancy is the key the Fault Tolerance which should lead to high reliability
- As we saw in the first lecture, adding redundancy to a poor system will not lead to higher reliability
- There is nothing wrong with a well designed single string system as evidenced by the single computer used in the Apollo Program vehicles
  - It was expensive which was the argument for the redundant based computer system used in the Shuttle
- Good engineering practices, inspection of all incoming parts for high quality components, traceable documentation of the design and all errors/faults, prototyping/simulation/testing of the highest degree, astute Software Engineering, adequate project funding, sensible schedules, supportive management → all leads to high reliability that will only be enhanced by fault tolerant techniques
- You can't make a silk purse out of a sow's ear - you cannot make a good quality product using bad quality materials

The Fault Tolerant Design of the C&DH System of the ISS (1553 Busses in ISS)

Albert Corazzato

CENG 5334

Spring 2002

Hardware FT: MIL-STD-1553 Bus

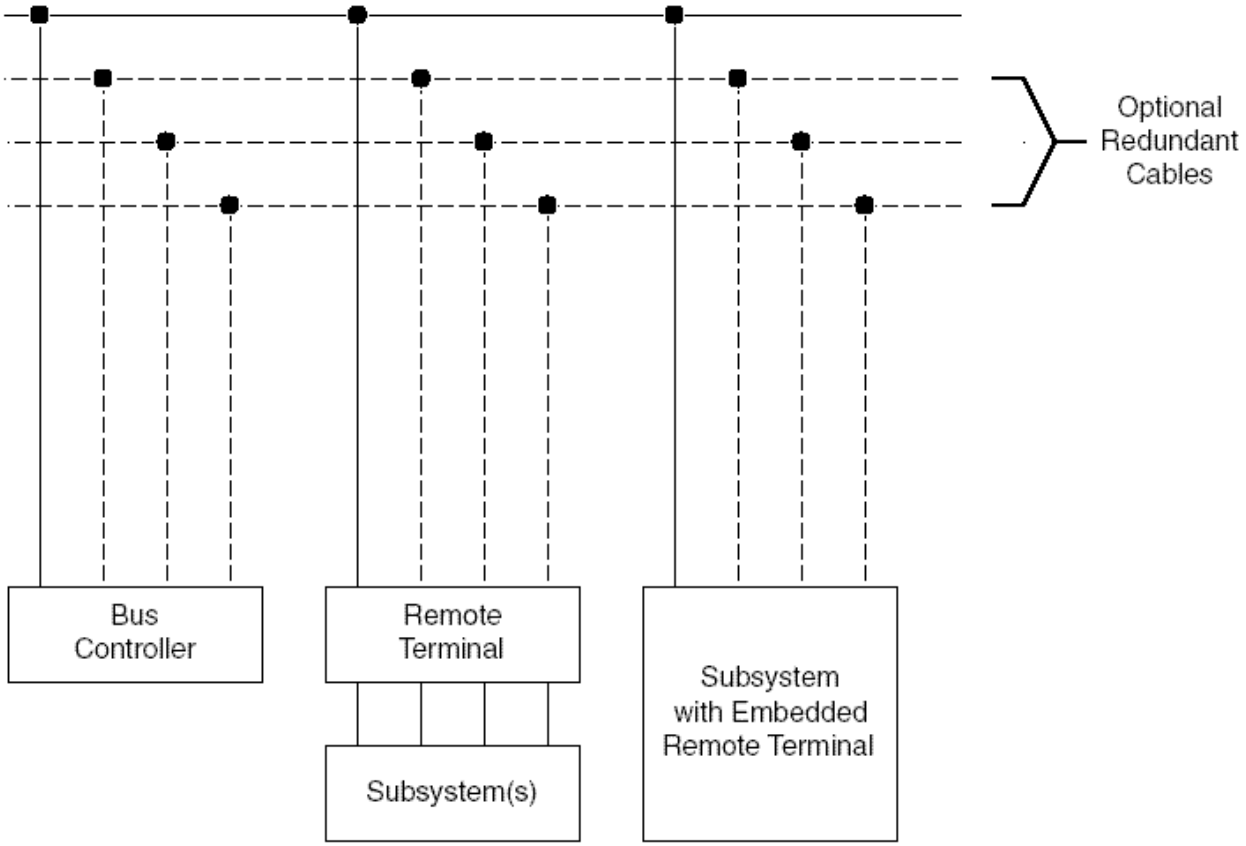
- Digital, TDM (time division multiplexing), serial data bus
- Multiplexed data bus used in commercial/military aerospace applications
- Utilizes transformer coupled buses for copper
- Fiber optic cable is today's means of implementation (MIL-STD-1773)
- Proven design
- Not limited to aerospace (factories, London Underground)

MIL-STD-1553 Bus (cont'd)

Data Bus Architecture

- One Bus Controller (BC) per physical bus
  - The BC is the sole controller of the bus
  - It initiates all transmissions on the bus
  - Can have multiple buses per BC
- Each bus can have 1-31 Remote Terminals (RT)
- Each bus has two separate channels (dual redundancy)
  - Each channel is on a separate wire

MIL-STD-1553 Bus (cont'd)



Typical Data Bus Architecture

MIL-STD-1553 Bus (cont'd)

Data Bus Architecture (cont'd)

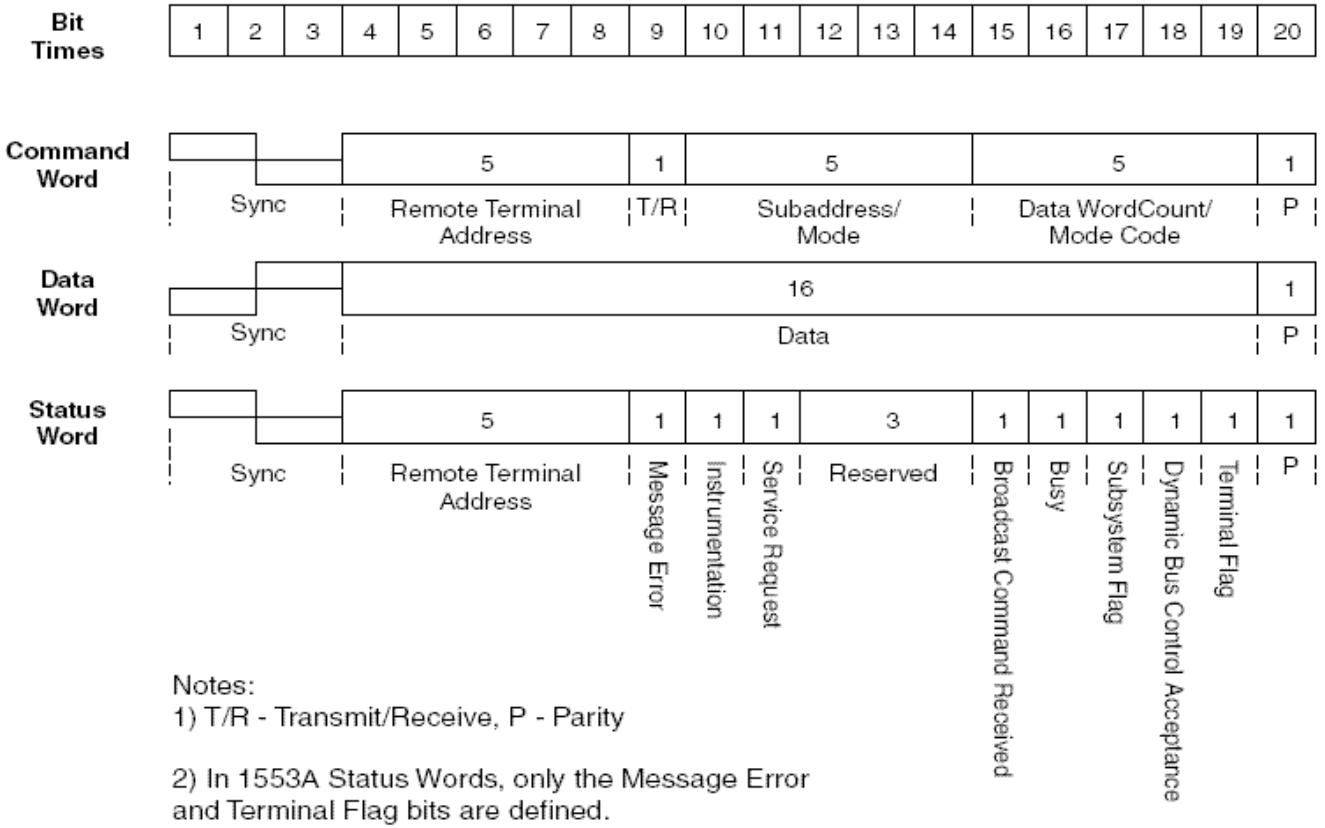
- Information flows across bus in messages comprised of three types of words
  - Command word
  - Data word
  - Status word

MIL-STD-1553 Bus (cont'd)

Data Bus Word Formats

- Data coding uses a bi-phase Manchester II scheme
  - Bi-polar coded signal
  - Most appropriate for transformer-coupled buses
- Command/Data/Status Words
  - 20 bits wide (3 sync, 16 data, 1 parity)
- Single bit odd parity
  - Sufficient when used w/Manchester II encoding and a word sync field
  - CRC or Checksums can provide additional error checking if needed

MIL-STD-1553 Bus (cont'd)

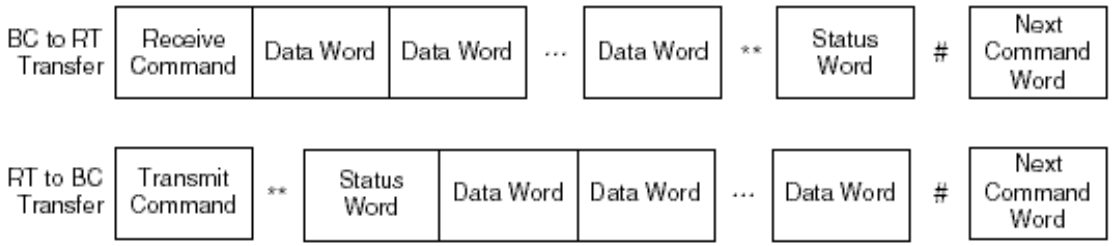


Notes:
1) T/R - Transmit/Receive, P - Parity

2) In 1553A Status Words, only the Message Error and Terminal Flag bits are defined.

Word Formats

MIL-STD-1553 Bus (cont'd)



Typical Message Transfer Formats

XTMRTool

- The Xilinx TMRTool is a graphical application that automates the implementation of TMR for FPGA designs.
- TMRTool allows Xilinx FPGA designers to focus on designing mission logic rather than on the TMR scheme.
- TMRTool reduces design errors and makes short work of a incorporating TMR into a design, a task that normally took weeks.

History behind TMRTool

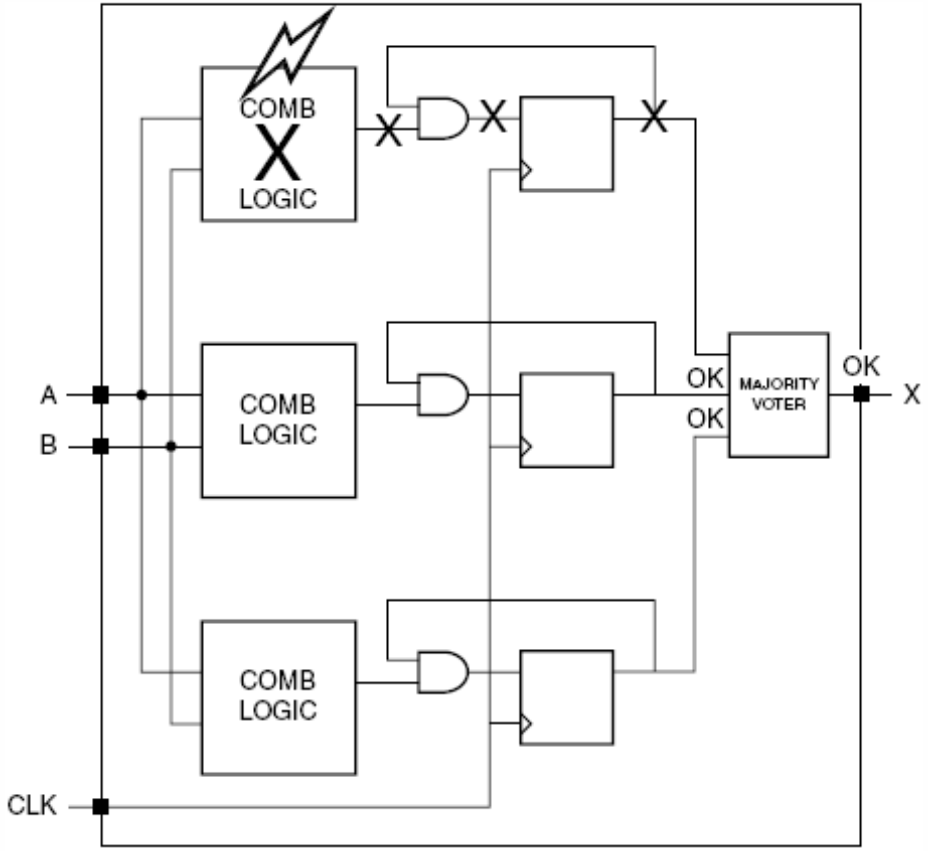
XTMRTool

- Designs in high-radiation environments can experience radiation-induced Single-Event Effects. These can manifest themselves in the following ways, none of which can cause physical damage to the Xilinx FPGAs:
  - Single-Event Transients (SETs) that cause voltage pulses on routing resources
  - Single-Event Upsets (SEUs) that flip bits in the configuration memory or in user registers
  - Single-Event Functional Interrupts (SEFIs) that disable user designs
- The “Xilinx Triple Module Redundancy” (XTMR) approach for design triplication was devised by Xilinx in cooperation with Sandia National Labs and others.

Traditional TMR vs. TMRTool

XTMRTool

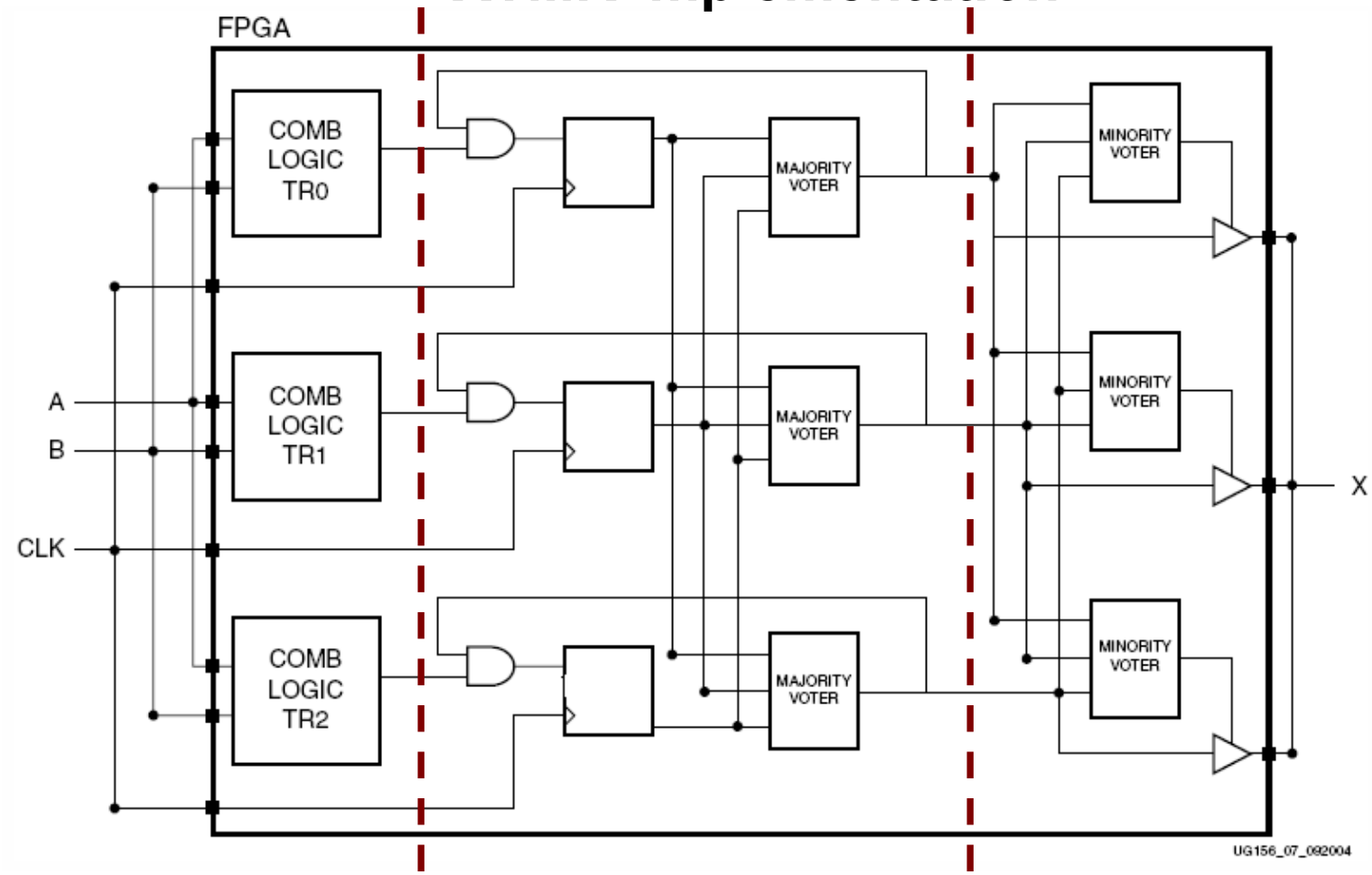
- Basic drawbacks to traditional TMR
  - Traditional TMR leaves designs vulnerable to SEUs in the voting circuitry and does not protect against SETs.
  - Traditional TMR does not provide a way of re-synchronizing state logic after configuration scrubbing. After an SEU in a traditional TMR state machine is corrected through scrubbing, the state machines must be reset to resynchronize.



TMRTool

XTMRTool

XTMR Implementation



TMRTool (cont.)

XTMRTool

- Inputs and throughput logic
  - XTMR starts by triplicating all inputs, throughput (combinational) logic and routing.
  - In effect, the redundant XTMR design domains begin and end on the printed circuit board (PCB), where they are not affected by radiation. All inputs, outputs, and voters are triplicated, which eliminates these resources as single points of failure. This feature immunizes designs from upsets in the voting circuitry and Single-Event Transients.

Traditional TMR vs. TMRTool (cont.)

XTMRTool

- Feedback logic
  - XTMR ensures constant synchronization between redundant state machines by inserting majority voters on all feedback paths. As a result, the feedback logic for each state machine is a function of the current state of all three state machines.
  - If an SEU upsets a state machine, the state machine will resynchronize with its redundant partners after the upset is corrected through scrubbing. **State logic can operate uninterrupted in the presence of SEUs and SETs, a major advantage of the XTMR approach.**

Traditional TMR vs. TMRTool (cont.)

XTMRTool

- Outputs
  - XTMR protects voting logic from SEUs by triplicating the voters.
  - Also, redundant domains converge on the printed circuit board, which is SEU immune.

Requirement Specifications for TMRTool

XTMRTool

- The original agreement with Sandia specifies the following requirements:
  - The tool should not place any special demands on the design description methodology.
  - The tool should offer a “push-button” flow for implementing the XTMR algorithm on an entire design with little user input.
  - The tool should provide designers with the option of excluding certain design elements from the XTMR algorithm.
  - The tool should allow designers to specify their own TMR approach.

TMRTool Features

XTMRTool

- TMRTool features and benefits include the following:
  - Automatic implementation of XTMR for any Xilinx FPGA design
  - Provides complete SEU and SET immunity
  - Supports all design entry methods, HDLs and synthesis tools
  - Automatic design triplication and voter insertion
  - Allows easy integration of custom-built TMR modules
  - Provides designers with complete control over how and what portions of their designs are triplicated.
  - Vastly increased designer productivity through reduced errors and fast XTMR implementation
  - And many more . . . (www.xilinx.com)

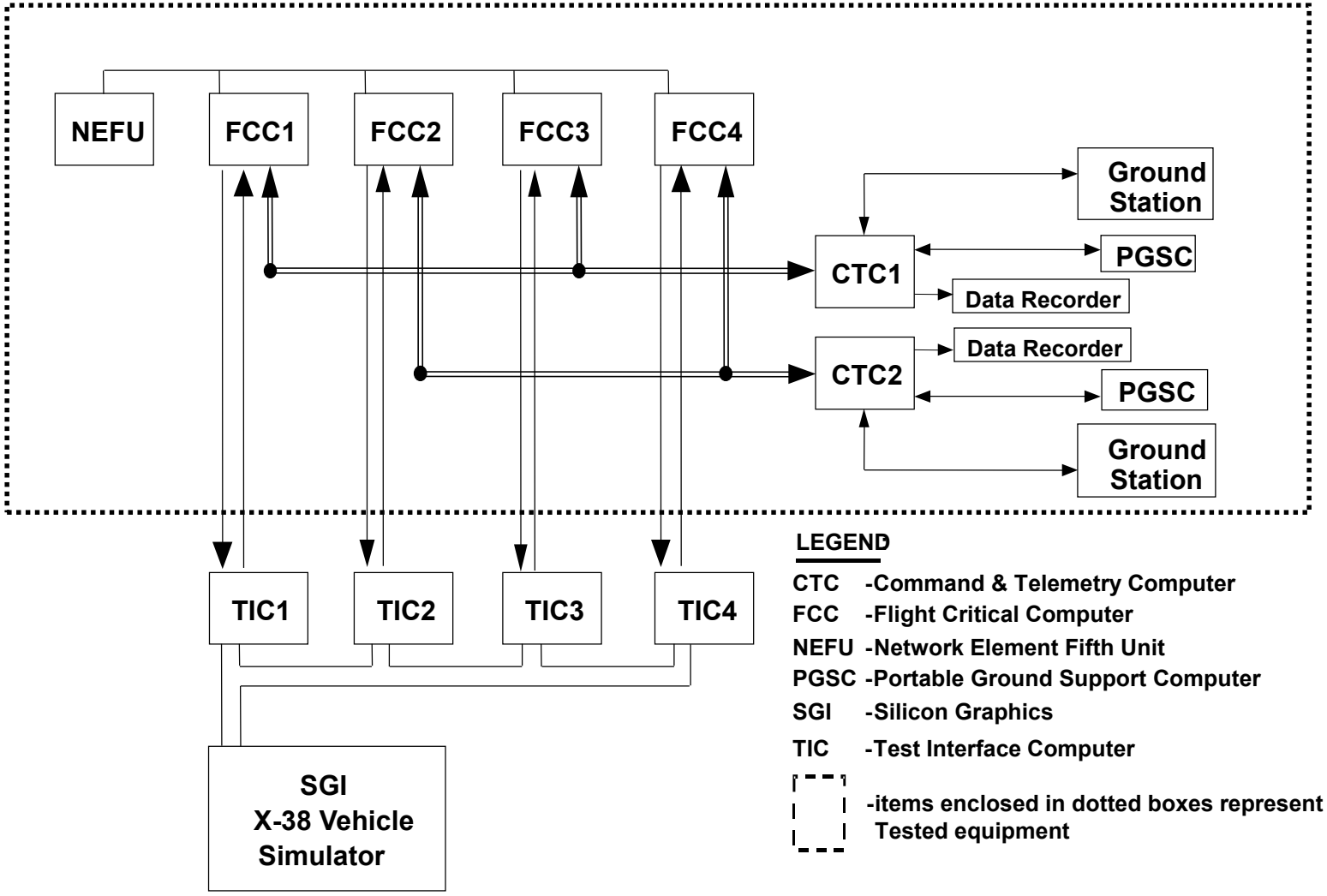
X-38 System Integration and Test Facility (SITF)

- Objectives
  - Test and simulation system supporting verification and validation of X-38 flight and ground software.
  - An environment that for all intensive purposes the flight software is flying a real vehicle.
  - Emulation of all flight equivalent hardware interfaces to send effector commands to and receive sensor data from the simulated vehicle.

SITF Objectives (Cont.)

- Process hardware in the loop simulation within the flight computer timing constraints, i.e. 50hz, 10hz and 1hz processing frames.
- Provide vehicle subsystem fault simulation and propagation to test the flight computer response to vehicle subsystem faults.
- Provide a foundation for the X38 hardware integration test facility and for the training of ground controllers.

SITF High Level Architecture



I/O Interfaces between the Flight Critical Computers and the Test Interface Computers

- 160 discrete outputs per string.
- 10 analog outputs per string.
- 1 Mil-Std-1553 dual redundant serial bus per string
- 1 RS-422 (clock and data) interface per string.
- 1 RS-232 interface per string.
- 1 532 word per frame PCM sensor data stream per string.

TIC to Vehicle Simulator Interface – Reflective Memory

- Provides real-time interface between TIC's and SGI simulation computer.
- Memory is mirrored on all machines via fiber optic network.
- Latency of approximately 1 microsecond for a single 32 bit word.
- Interrupts upon writing to specific memory words and spinlocks are used for synchronization.

Test Interface Computer Executive Software

- VxWorks realtime OS.
- Multithreaded design for all I/O tasks.
- Synchronize TIC minor frames to FCC minor frames via MIL-STD-1553B message interrupts.
- Effector data transfers by initiated by timer interrupts.
- Sensor data transfers initiated by reflective memory interrupts.
- Status/Error/overrun reporting to SGI over Scramnet.

Vehcile Simulation Executive Software

- NASA/JSC ER Trick simulation environment for avionics simulation.
- NASA/JSC EG Shuttle Engineering Simulator for flight simulation.
- Simulation models interface via shared memory and semaphores.
- One CPU isolated for real time processing.
- Spinlocks used to synchronize with all four TIC's.
- Flexible data logging of all model and interface states

Testing methodologies

- FDIR testing by faulting simulated subsystems.
- Simulation software environment provides fault insertion in all simulation models and input file scritping capability for fault propagation.
- TIC's will emulate faults at hardware interfaces.
- Monitoring devices to test all hardware I/O interfaces.

Testing methodologies (Cont.)

- Up to two faulty FCP or ICP VxWorks software loads can be used to test how FTSS FDIR responds to faulty FCC’s.
- Explicit power control to all FCC's and CTC's to support dynamic redundancy testing.

INTRODUCTION

Stratus Computers and the National Stock Exchange of India (NSE)

- Companues: 1980: Stratus Computer, Inc. 1999: Stratus Technologies
- Business focus - Global provider of fault-tolerant computer servers, technologies, and services
- First application of hardware alone to provide fault tolerance
- Design: Duplicate hardware
- Provides greatly enhanced service capabilities, 24/7 availability of essential services and applications
- Recent achievements: fault-tolerant Intel based processors

Introduction (Cont'd)

National Stock Exchange of India (NSE)

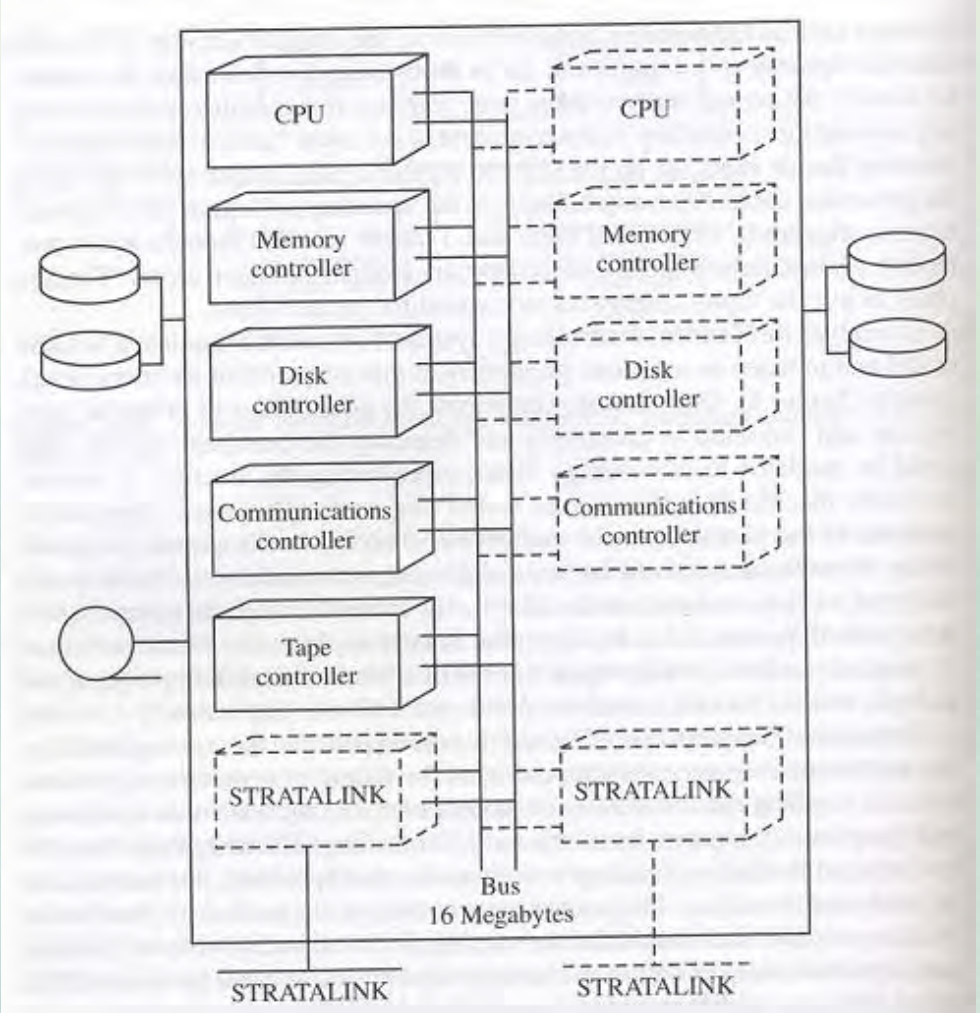
- Opened in 1994
- Largest Exchange in the country
- Challenge- to provide continuous, high performance trading services to NSE's members
- Runs trading operation on Stratus fault tolerant computers- Stratus Continuum server

- Two second system response time guarantee

Stratus System Architecture

- Up to 32 modules connected by Stratus intermodule bus (SIB)
  -StrataLINK
- StrataLINK- interconnect mechanism, used for system expansion
  - Restricts modules-geographic proximity of few miles
  - Two independent co-axial links
  - Links run at 1.4 Mbytes/second
- Stratus network- several systems connected using X.25 packet switched network or StrataLINK

Basic Stratus Architecture



Each module contains-

- Stratus backplane or midplane, StrataBUS
- One or more processor board pairs
- One or more memory board pairs
- Pairs of I/O controllers
- Power supplies
- Battery backup subsystem

The Basic Module Bus

- Boards of the module interface with the StrataBUS
- Logical slots- 6,10,20,32,40
- Arbitration scheme- function of bus slot number
- Partitioning of Slots- Even and Odd, different power subsystem
- Synchronous- clock signal -8 MHz
- Viewed as two independent buses- A and B
- Simultaneous interfacing with both buses

Monitoring of Bus by Memory Boards

- Parity signal- detection of bus failures
- Controller logic- detection within memory boards

Power Subsystem

- Battery Back-up system- works in two modes
  - Powers all boards
  - Powers only the memory boards
- Reaction to power failure- saves in main memory
- Power outage- Power entire module for 6 seconds
- Extended battery back-up mode

System Boards

- Synchronous operation
- Self checking and auto-isolating- duplicating logic, comparing, failed board indicated by an LED
- Power regulation
- Self-identifying –coded information, board type, revision level, board repair history
- Common interface conventions

- Major Boards operate in two ways-
  - Synchronous lockstep- both Self-Checking boards synchronized
  - Logically paired state-boards that interface with disks, tapes and the StrataLINK, not synchronized
- Interfacing to non-fault tolerant buses
  - Latches on logic interfacing to the bus
  - Conservative timing assumptions
  - Reflexive checking logic

- I/O processor boards use the P/Q bus
  - Duplicated address/data multiplexed bus
  - Both P and Q use parity for checking
  - Protects against any single-bit asynchronous glitch and/or a multi-bit failure
  - Uses loopback checking
  - Isn't impacted by electrical noise interference within the system with a white noise characteristic (uniform random over a very wide frequency range)

Immunity from certain failures

- Board failure - fault count, MTBF
- Power Supply Failure
- Operational Downtime
- Field Service - no preventive maintenance necessarily needed, self-diagnosing, self-identifying
- Hardware installation (hot backup)

Stratus Continuum Server in NSE

- Nerve center
- Ensures continuous availability connected to Stratus Customer Assistance Centers via Stratus Remote Service Network (RSN)
- Complete disaster recovery site consisting of Stratus systems
- No loss of data and performance degradation
- Continuous Availability - five nines (99.999%) and greater uptime
- Operational simplicity
- Compelling financial advantage

Stratus Computers in the NSE

- Advantages of Stratus with regard to NSE -
  - Continuous processing technology
  - Uptime of 99.999% of the Stratus server
  - Power supply failure in various Indian cities have no impact on transactions
  - Upgrading is easy
  - The CACs and RSNs ensure wide availability over the wide geographical area.
  - Power regulation function of boards overcomes voltage fluctuations
  - Lower overall cost per transaction

Fault Tolerance of Boeing 777 Computing Systems

Aircraft Statistics

- Boeing 777 Airplane
  - Design Phase started 1988
  - First Airframe delivered in 1995 to United Airlines
  - Capacity between 283 and 451 passengers
  - Range between 5,235 to 9,450 nautical miles
  - First airplane to qualify for ETOPS-180 certification

  - Length 209-242ft (63.7 – 73.9m)
  - Wingspan 200-212.5ft (60.9 – 64.8m)
  - Fuselage width 20.3 ft (6.19m)
  - Cruising speed: 0.84 Mach (560 mph, 905km/h)

How aircraft operates

- Fly-by-wire
- Pilots use conventional control stick & wheel, rudder pedals, and throttle controls
- Actuator Control Electronics (ACE) units use sensors on pilot controls to detect input
- ACE pass on pilot commands to Primary Flight Computer (PFC)
- PFC accepts pilot input, combines with other vehicle sensors, provides output to ACE
- ACE configure airfoil surfaces as commanded

PFC Redundancy

- Primary Flight Computers (PFCs) are triple-Triple Modular Redundant (TMR) design
- Each PFC contains three separate “lanes”
  - Two lanes are monitoring the “Command” lane
  - Either the “Monitor” or “Standby” lanes can inhibit the Command lane from issuing errant commands
- Each “Command” lane monitors the other two Command lane on the other bus, and has the ability (combined) to override the errant PFC

PFC Architecture

- Each PFC is made from three independent lanes.
  - Individual power supplies, microprocessors, and associate support / interface hardware is used for each lane
  - INTEL 80486, Motorola 6840, and AMD 29050 microprocessors
  - This division of hardware ensures a common fault will not render a single failure capable of rendering a PFC non-functional
  - All software is written using ADA, however each microcontroller requires a unique compiler to create the machine language the hardware operates on.

Fault Tolerant Characteristics

- The Primary Flight Computer and associated system architecture is a very reliable design for the 777 aircraft.
- The vehicle can operate nominally with a single lane failure in each PFC or the complete loss of a PFC or both.
- No single faults can cause an error without a failure indication.
- The triple-triple redundancy allows the system to meet functional integrity and functional availability requirements of 10^{-10} failures per flight hour.

Boeing 777 Primary Flight Computer System

- Launched in June 1995 to meet new regulations and market dynamics
- World's largest twinjet(powered by two engines) and has a capacity of over 300 passengers
- Over five million flights and 18 million flight hours
- First aircraft completely designed on a computer
- For the first time, eight major airlines had a role in the development of the aircraft
- Fully digital fly-by-wire controls, fully software-configurable avionics
- First use of a fiber optic avionics network on a commercial airliner

New technological aspects of Boeing 777

Challenge :

To meet the desire for more functionality with high reliability and easier maintainability

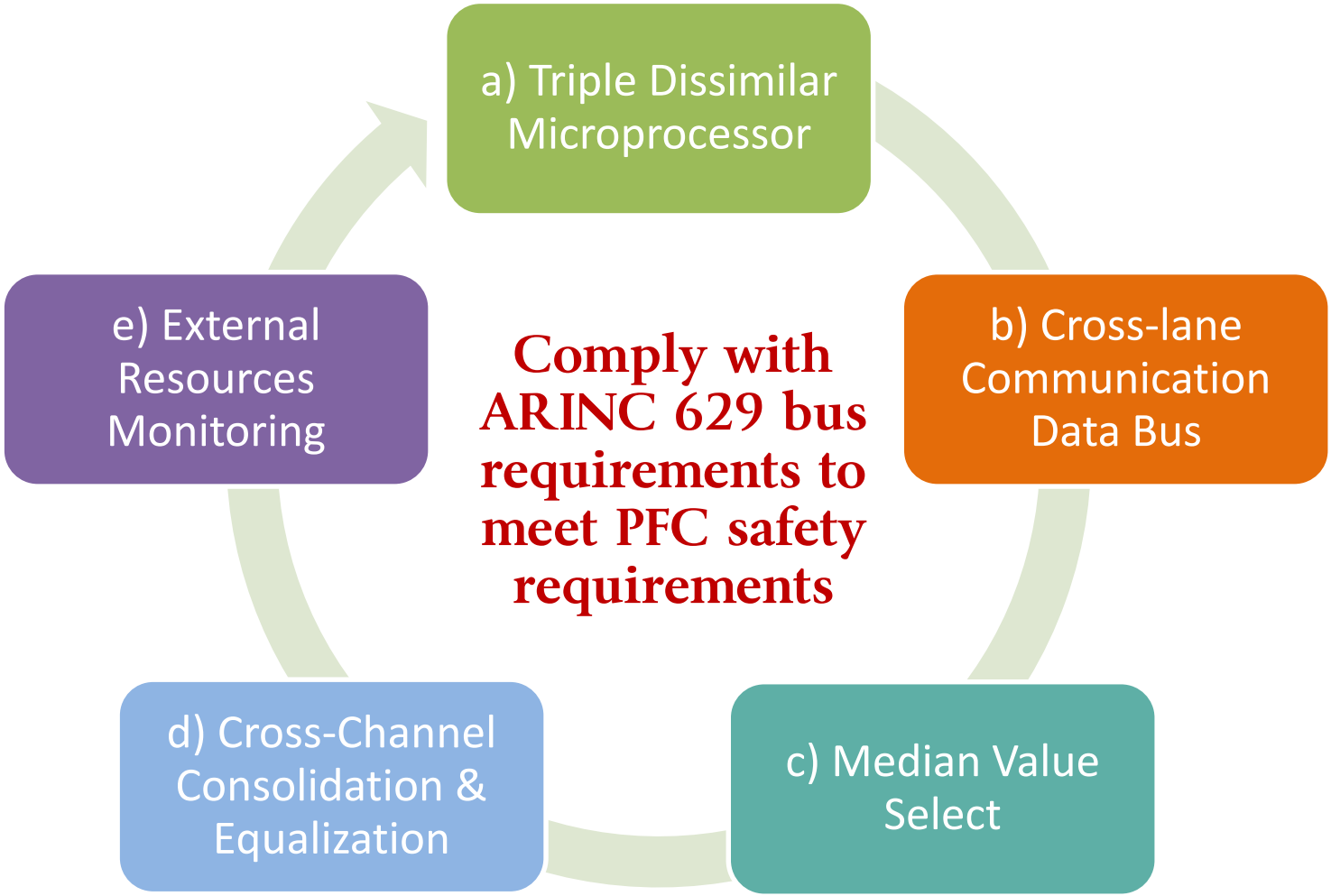
New Technologies:

- Fly-by-wire (FBW)
- ARINC 629 (DATAC) Bus
- Deferred Maintenance

Heart of FBW

Use of triple redundancy for all hardware resources: computing system, airplane electrical power, hydraulic power and communication path

PFC Hardware Resources Redundancy Management



Further scope for Fault Tolerance

The airliner has been involved in two hull-loss accidents, with no on-board fatalities, as of August 2012

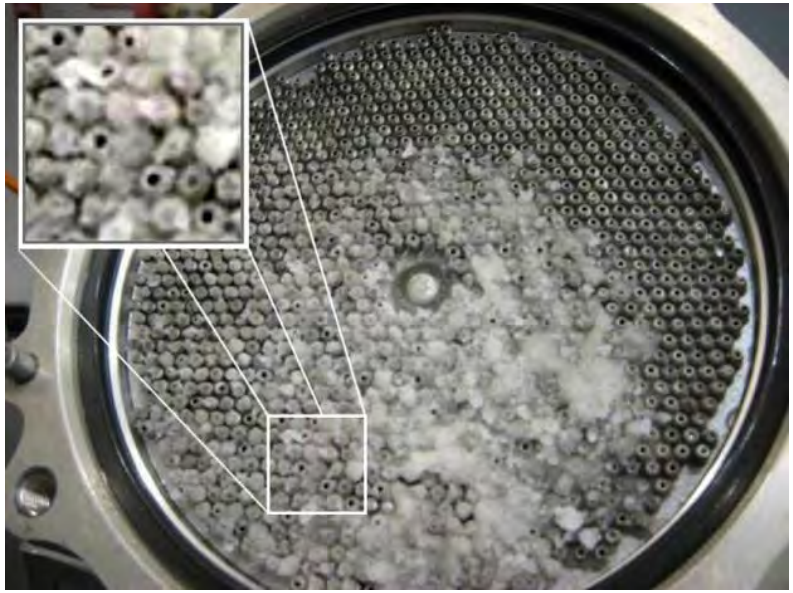
Date	Operator	Flight No.	No. Onboard	Injuries	Fatalities
20 January 1997	All Nippon Airways	Unknown	Unknown	0	0
29 July 1997	United Airlines	Unknown	289	0	0
14 October 2000	Saudi Arabian Airlines	Flight 115	112	0	0
31 January 2001	Emirates Airlines	Flight 069	123	0	0
20 April 2002	British Airways	Unknown	174	0	0
5 September 2001	British Airways	Flight 2019	26	0	1 (other accident)
23 June 2005	Japan Airlines	Unknown	Unknown	0	0
6 November 2005	American Airlines	Unknown	Unknown	0	0
1 August 2005	Malaysia Airlines	Flight 124	177	0	0
26 February 2007	United Airlines	Flight 955	205	0	0
27 July 2007	British Airways	Unknown	227	0	0
24 April 2009	Air Canada	Flight 031	227	11	0
17 January 2008	British Airways	Flight 38	152	47	0
25 April 2010	Emirates Airlines	Flight 530	364	20	0
20 July 2010	United Airlines	Flight 967	265	21	0
20 October 2010	Vietnam Airlines	Flight 147	Unknown	30	0

Further scope for Fault Tolerance

1) On 17th January 2008, Boeing 777-236ER aircraft crash landed just short of the runway at its destination

The accident was blamed on ice crystals from the fuel system clogging the fuel-oil heat exchanger.

BA Boeing 777 Heathrow crash evidence



Laboratory replication of ice crystals clogging the fuel-oil heat exchanger

Further scope for Fault Tolerance

2) In August 2005, Boeing 777-200 aircraft was involved in significant upset event while flying on autopilot
   - An anomaly existed in the component software hierarchy allowed inputs from a known faulty accelerometer
   - Pilots couldn't command an increase in engine thrust on approach to Heathrow Airport while flying over London
   - Anomaly not detected in the testing and certification process for the unit
   - Development of fault tolerant software can mask previous failures


BOEING

Aircraft Avionics Software Development with DO-178B Standards

- The science and technology of the electronic devices used in aeronautics and astronautics.
- Communication, Navigation, Monitoring, Weather Prediction, Collision Avoidance, Radar, Control Systems.

RTCA/DO-178B

- RTCA is the acronym for **R**adio **T**echnical **C**ommission for **A**eronautics.
- Document of Software Considerations in Airborne Systems and Equipment Certification.
- Developed by the Commercial Avionics Industry

Aircraft Avionics Background

- In Avionics industry the function and architecture of an embedded computer system (*i.e.*, Flight Control, Braking, Cockpit Display, etc.) are defined by system engineers.
- The associated control laws are developed by control engineers using some informal/semi-formal notation based on schema-blocks and/or state machines.
- Finally the embedded production software is specified textually and coded by hand in C and Ada by software engineers.

Background (continued)

- The avionics industry requires that safety-critical software be assessed according to strict certification authority guidelines before it may be used on any commercial airliner.

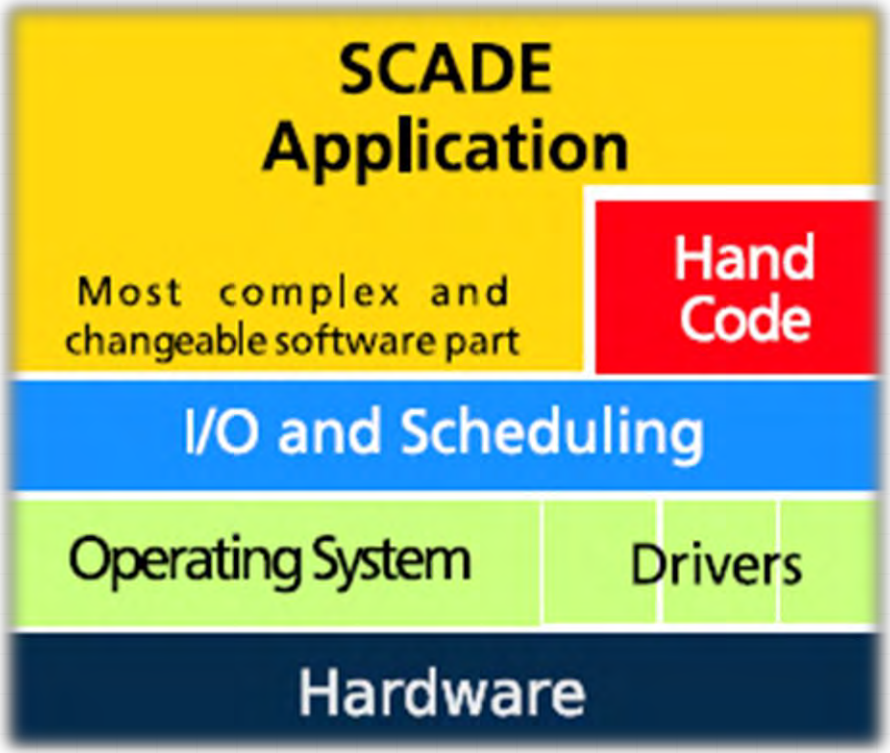
- ARP 4754 and DO-178B are guidelines used both by the companies developing airborne equipment and by the certification authorities.

Software Tool: SCADE Suite®

- SCADE stands for **S**afety-**C**ritical **A**pplication **D**evelopment **E**nvironment.

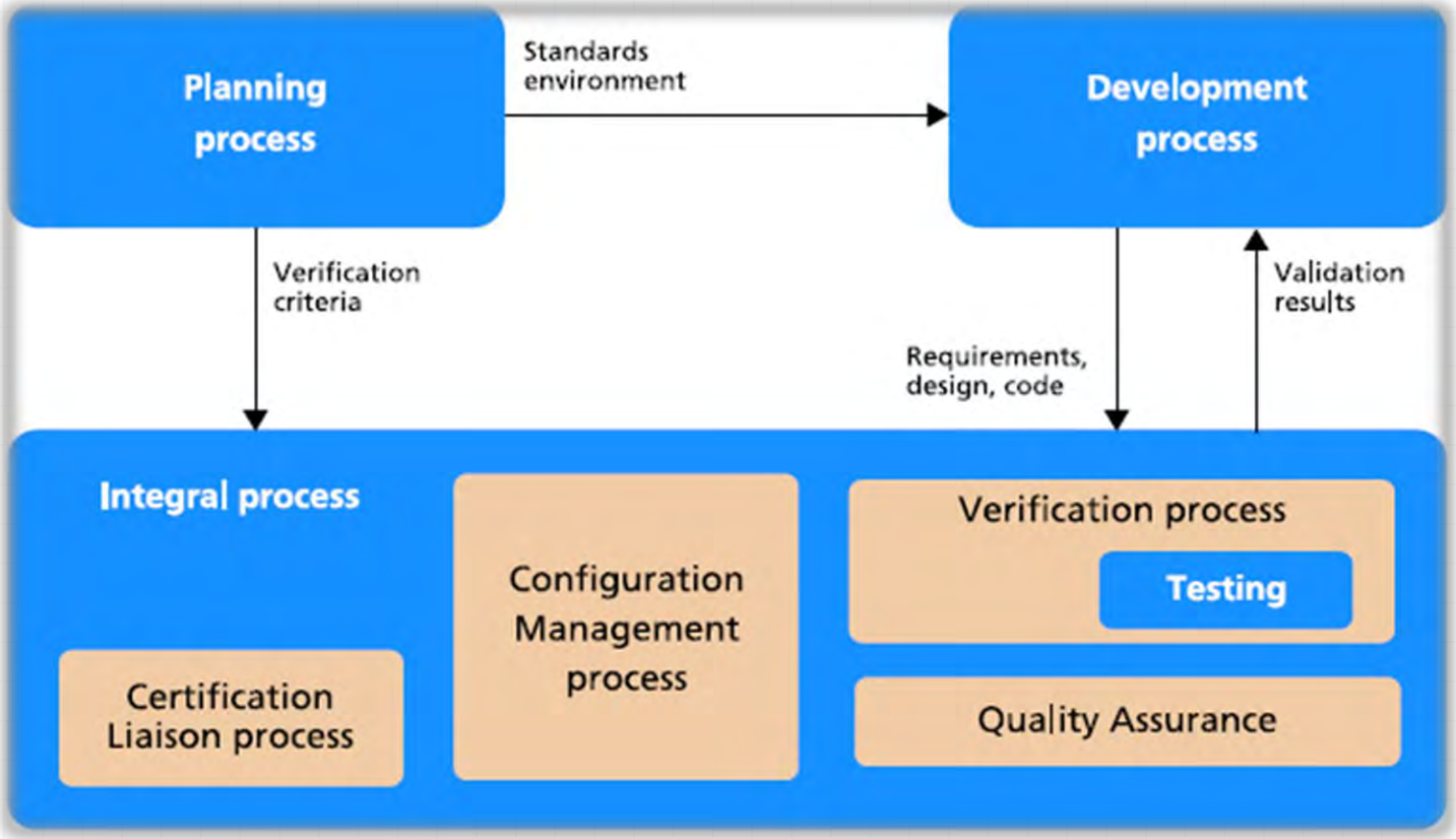
- SCADE Suite® is the unique **Integrated Development Environment** for critical applications spanning requirements management, model-based design, simulation, verification, qualified/certified code generation, and interoperability.

What does it do?



- Addresses the applicative part of control software.
- Is the most complex and changeable aspect of software, containing complex decision logic, filters, and control laws.
- It typically represents 60% to 80% of the software embedded in an airborne computer.

Life Cycle


Planning process
Standards environment
Development process
Verification criteria
Requirements, design, code
Validation results
Integral process
Configuration Management process
Verification process
Testing
Certification Liaison process
Quality Assurance

Avionics Software Development

- System and software engineers use software tools (e.g. SCADE®) to graphically design, verify, and automatically generate critical systems and software applications with high dependability requirements.
- Tools reduce software certification, coding, review and testing costs.
- Elimination of coding errors and low-level testing, fast and safe design changes are all possible throughout software life-cycle with the use of modern software tools.

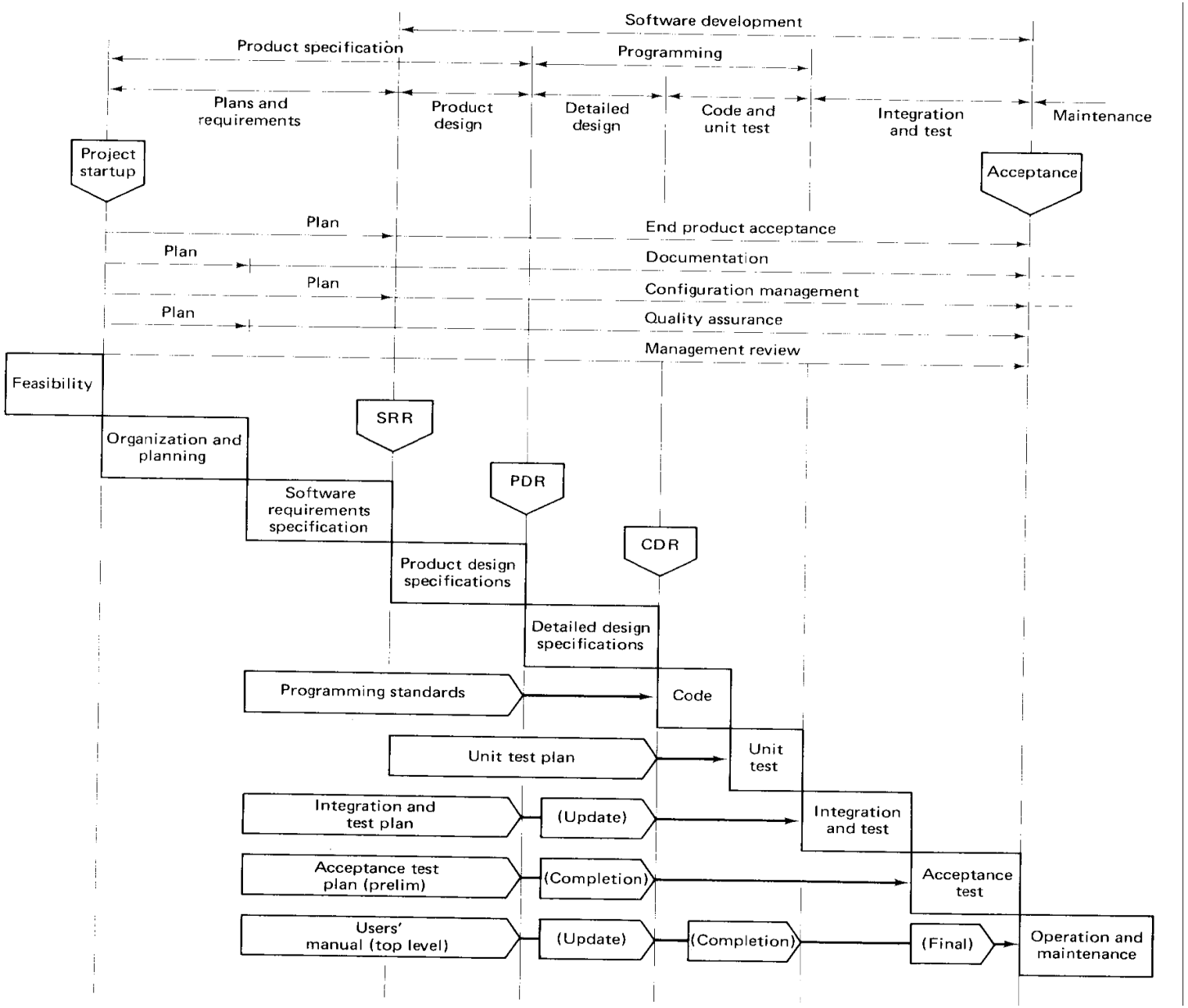
Outline (Thoughts and excerpts from past classes)

- Risk
  - Probabilistic Risk Assessment (PRA)
  - Business Continuity
- Hardware
  - Comments on High Reliability without Redundancy
  - 1553 Busses
  - XTMR Tool
  - X-38 System Integration and Test Facility (SITF)
  - Stratus and the Stock Exchange of India
  - Commercial Aircraft
- **Software: Associated Technologies**
  - COCOMO
  - Nano Technology
  - Error Tolerant Computing
  - CMMI
  - FT in UPC (Universal Product Codes)
  - FEMA
  - SIL – Safety Integrity Level
- FT In Our Daily Life
  - Automobiles
  - Health Care Systems
  - Warranty: Product Lifespan
- What I've Learned

COCOMO

- We’ve reviewed the goals of software engineering to produce high reliability software associated with the life-cycle of software.
- The quantitative life-cycle relationships are organized into a hierarchy of software cost-estimation models called COCOMO for COnstructive COst Model
- Basic model – development effort and cost as a function of the size of the software product in source instructions
- Intermediate model – software development effort as a function of the most significant software cost drivers besides size(complexity, required reliability, hardware attributes, personnel attributes, project attributes (schedule constraints, use of software tools)
- Detailed model – effects of these attributes on each individual life-cycle phase.

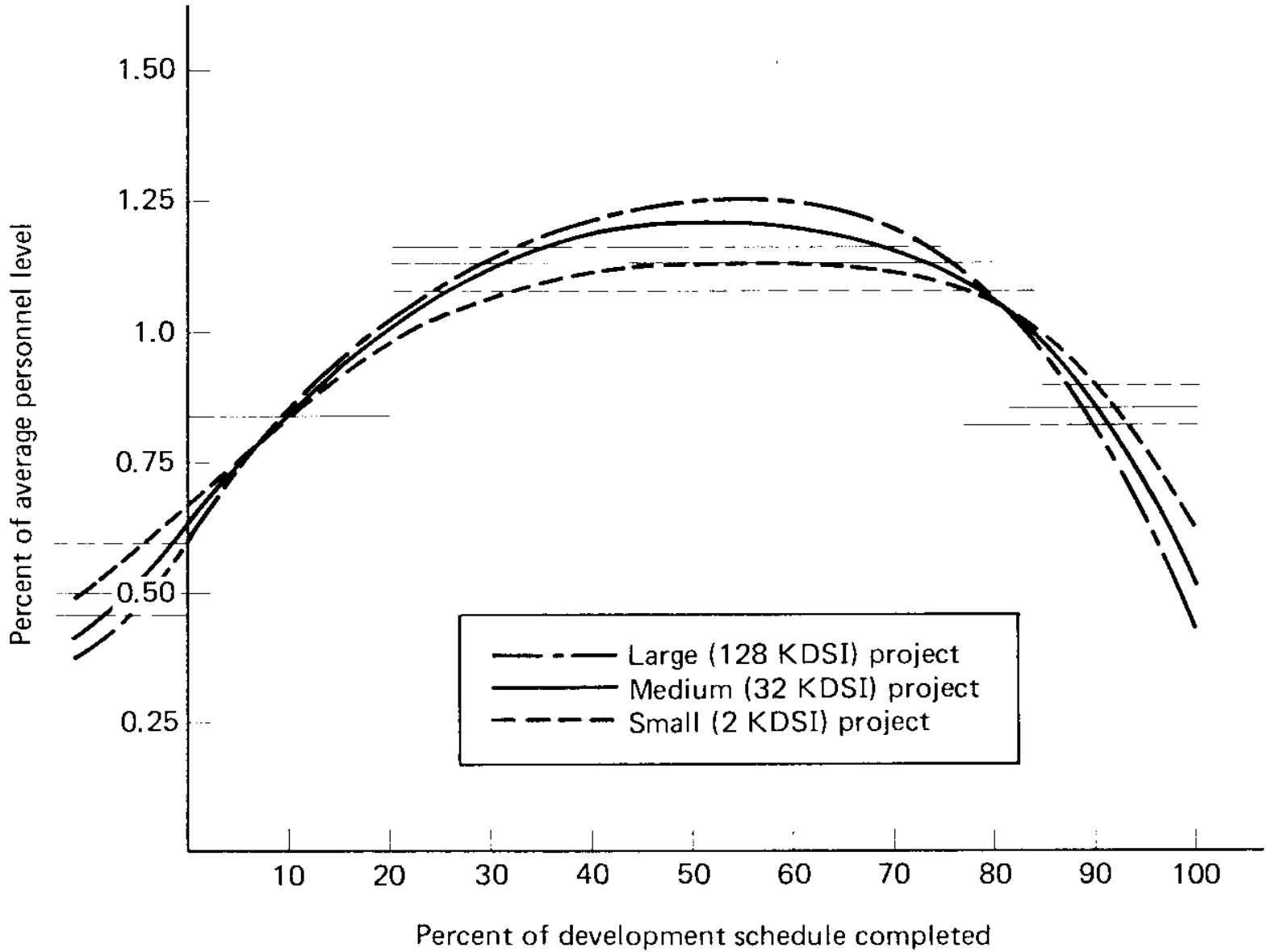
Software Project Phases



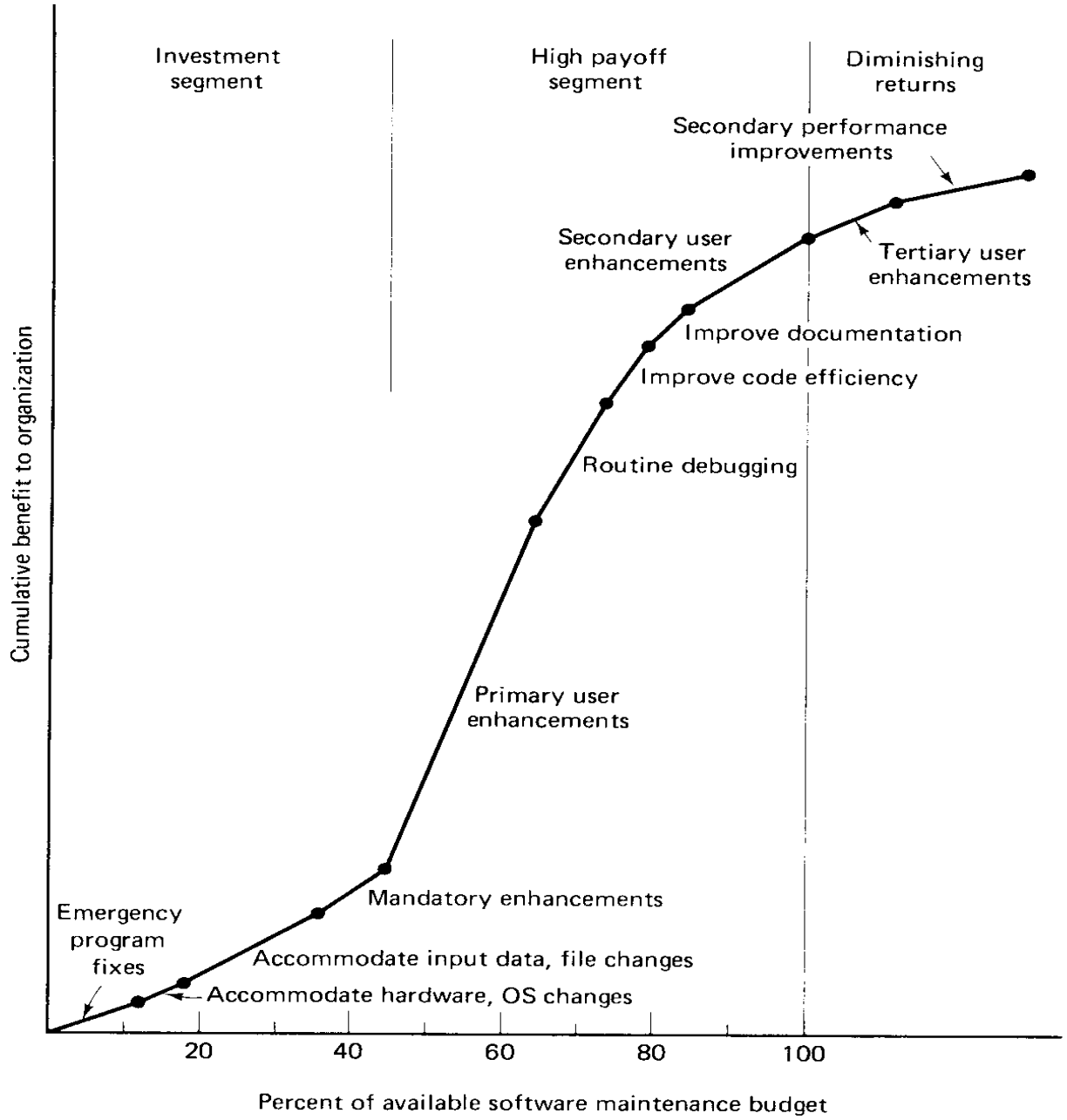
Basic Model

- Manmonths = $2.4(\text{KDSI})^{1.05}$ where KDSI = thousand delivered source instructions and a manmonth is a 152 hours of working time
- Development (months) = $2.5\ (\text{manmonths})^{0.38}$
- Knowing the number of manmonths and the development effort in months → the number of programmers = manmonths/development
- COCOMO models only applicable to programs larger than 2000 lines of code (big projects)

Basic Labor Distribution (Rayleigh Distribution)



Software Maintenance Production Function



Nanotechnology for FT in Computer Systems

- Nanotechnology is replacing deep submicron technology for device manufacturing for various reasons, among them reliability.
- Reliability in Nano-logic designs still is tied to reduction of defect tolerance through redundancy.
- Evaluation of tradeoffs in an NAND multiplexing.

The Submicron Tech Dilemma

- Semiconductor technology have led to impressive performance gains of VLSI circuits especially in microprocessors.
- However, smaller transistors, lower power voltages and higher operating frequencies have contributed to increased rates of occurrence of transient and intermittent faults.
- Semiconductor industry was approaching a new stage in the design and manufacturing of VLSI circuits mainly due to reliability issues.
- Fault-tolerance countermeasures have to be integrated into commercial-off-the-shelf (COTS) VLSI systems to ensure data integrity and to minimize the impact of transient and intermittent faults

The Submicron Tech Dilemma (cont'd)

- The supply voltage is scaled down to prevent reliability hazards such as oxide breakdown and hot carrier effects
- Reliability is a key factor in the design of any system. One of the factors that affect the reliability of submicron integrated circuits is electromigration.
- Electromigration: a phenomenon that describes the mass transport of metal ions in a conductor due to electron flow when under the influence of a strong electric field
- Eventually it causes the wire to break or to short circuit to another wire.

The Submicron Tech Dilemma (cont'd)

- Crosstalk is due to electromagnetic coupling between multiple lines running parallel to one another.
- Crosstalk: electromagnetic coupling between multiple lines running parallel to one another. It can cause noise pick-up on the adjacent quiet signal lines that may lead to false logic switching
- Proposed solution for higher reliability depends on the use of redundancy

Emergence of Nano Technology

- Chip Size
  - Device sizes are in the nanometer range
  - Entire VLSI processors can be accommodated into a small package.
  - Portability advantages. Example: smart phones.
  - Technological advances mean that manufacturers can now pack more features into a small, convenient package than ever before

Nanotechnology issues

- Dimension scaling of CMOS devices into the nanoscale realm imposes similar problems

Major issues:

- Transistor and interconnect parametric variations, leakage currents and power dissipation will cause a large number of functional faults, permanent and transient, in device and circuit operation.
- We are inevitably faced with the question of how to build reliable systems out of unreliable components (reliability??)

Fault Tolerant countermeasures

- No matter how advanced are the systems, redundancy is still the main FT technique.
- Several fault-tolerant techniques based on redundancy have been investigated for nanocomputers recently:
- Reconfigurable architecture
- R-modular redundancy (R >3)
- NAND multiplexing

Fault Tolerant countermeasures

- Reliable computation with unreliable components can be termed as “probabilistic computation”
- R-modular redundancy and Reconfigurable architecture techniques have traditionally been used for microsystems where device failure rate is typically 10^{-7} to 10^{-6} . However, with these techniques alone, high fault-tolerance is hard to achieve for nanocomputers that are anticipated to have a device density of 10^{12} per chip

NAND Multiplexing

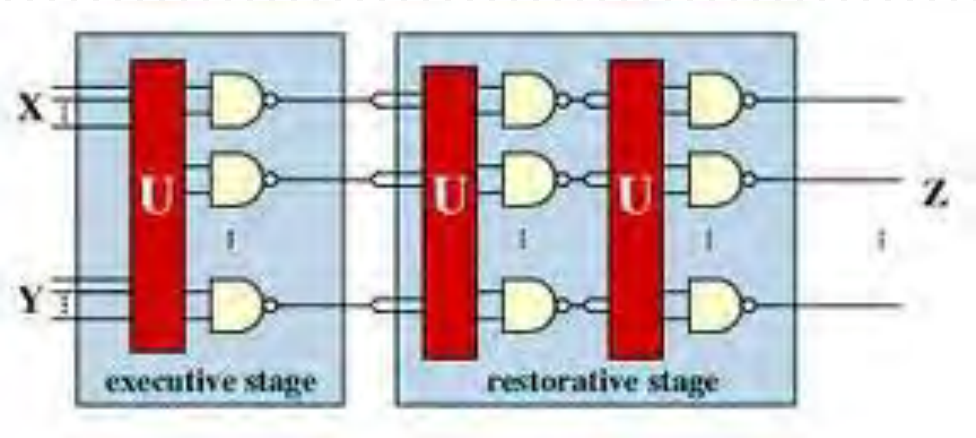
- Von Neumann proposed to build reliable computation from unreliable devices by using a redundancy technique called NAND multiplexing.
- Examples of potential future nanochips are used to illustrate how the NAND-multiplexing technique can lead to high system reliability in spite of large gate error probability while keeping the cost of redundancy moderate.
- In nanoelectronic systems, while permanent defects can be taken care of by reconfiguration, probabilistic computation schemes can incorporate another level of redundancy so that high tolerance of transient errors may be achieved

NAND multiplexing - if the failure probabilities of the gates are sufficiently small and failures are statistically independent, then computations may be done with a high probability of correctness

NAND Multiplexing

- A NAND multiplexing unit is comprised of a randomizing unit and copies of NAND gates which can fail (flipping the output bit value)
- The NAND multiplexing unit takes two bundles of wires as inputs and generates a bundle of wires as the output. Through a random permutation by the "randomizing unit," the inputs in one bundle are randomly paired with those from the other bundle to form input pairs to the duplicated NAND gates.
- In systems based on this construction, each signal is carried on a bundle of *N* wires instead of a single wire and every logic computation is done by *N* duplicated gates simultaneously.

NAND Multiplexing



The “executive” unit carries out logic computation
and the “restorative” unit (comprised of two NAND multiplexing units) restores the excitation level of the “executive” unit output bundle to its nominal level

NAND Multiplexing

- von Neumann stated that if ϵ is sufficiently small, computation by such constructions can always be done with arbitrarily high reliability by increasing the bundle size *N*
- However, at the system level two fundamental questions remain, which are:

1) How does the system behavior depend on the individual faulty components?
2) What are the mathematical frameworks to study such multiplexing schemes in general based on von Neumann's prototype?

NAND Multiplexing

- Han and Jonker have proposed a Markov chain-based model for a system architecture consisting of chains of parallel NAND multiplexing units. Their work have shown that:

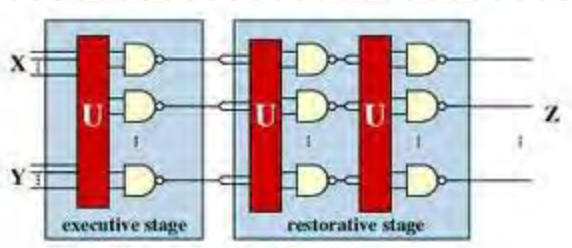
1) by retaining parallelism throughout the network, the redundancy needed to achieve high system reliability is significantly reduced

2) the Markov-chain model may be a powerful mathematical framework for the analysis of such multiplexing schemes

NAND Multiplexing

- Let us denote the number of excited wires in a bundle of size N by a random variable K and call K/N the bundle's excitation level. Assume that each wire in the bundle has a probability of Z to be excited. Obviously K follows a binomial distribution with parameters and as follows:

$$\mathbf{P}(K = k) = \binom{\mathbf{N}}{K} Z^k a^{N-k}$$



Conclusions

- For an extremely large N, the number of stimulated outputs of the executive stage is a stochastic variable normally distributed with an upper bound of 0.0107 for the probability of gate failure. If each gate fails independently then the threshold probability of each gate is 0.08856.
- For small N, the number of outputs of the executive stage is a binomial distribution.
- The system uses multiple stages of NAND multiplexing units, which can be modeled as a Markov chain.

Conclusions (continued)

- The most direct implication of this analysis is that the multistage NAND multiplexing architecture can be used to design fault tolerant nanoelectronic systems. One important observation is that all computation and interpretation of the results must be carried out in a probabilistic sense.
- As nanotechnology evolves, there are many promising candidates for the construction of the NAND gate and the multiplexing system, such as single electron transistors, quantum cellular automata and carbon nanotube transistors.
- In the end, reliability is simply a function of redundancy no matter what kind of technology is used.

Fault Tolerance and Stochastic (Probabilistic) Computing

- What is the future of fault tolerance with the advent of computers that will tolerate errors – Error Tolerant Computing?
- Two factors driving the replacement of deterministic computing with probabilistic outcomes
  - Transistor structures (scale chip dimensions of IC fabrication)
    - As transistor dimensions shrink the threshold voltage (on/off switching will vary from device to device (Moore's Law associated with high clock frequencies and low supply voltages)
    - This results in stochastic circuitry or error-resilient processor architectures that also consumes less power
  - Power Consumption
    - A concern for all electronic devices not just cell phones but overall power consumption in the United States (look at the Google's data centers around the US)
    - Power consumption is reduced by 'relaxed correctness' in processors. A good example is graphics processing that uses huge amounts of data. Allowing a reasonable number of pixel errors doesn't impact the quality of results but yet would reduce the amount of power used in making sure every pixel was 'correct'.
- Probabilistic Computing is definitely on the horizon
- Fault Tolerant Computing in light of allowable errors?

Capability Maturity Model Integration (CMMI)

- Originally developed as a tool for objectively assessing the ability of government contractors' *processes* to perform a contracted software project
- Organizations rated: Level 1 (low) to 5 (very high)
- Shooman credits the reduction in error rates for the Space Shuttle Software to IBM Federal Systems Division's rating of CMM level 5
- It allows organizations to address practices for process improvements that cover the product's life cycle from conception through delivery and maintenance

History of CMMI

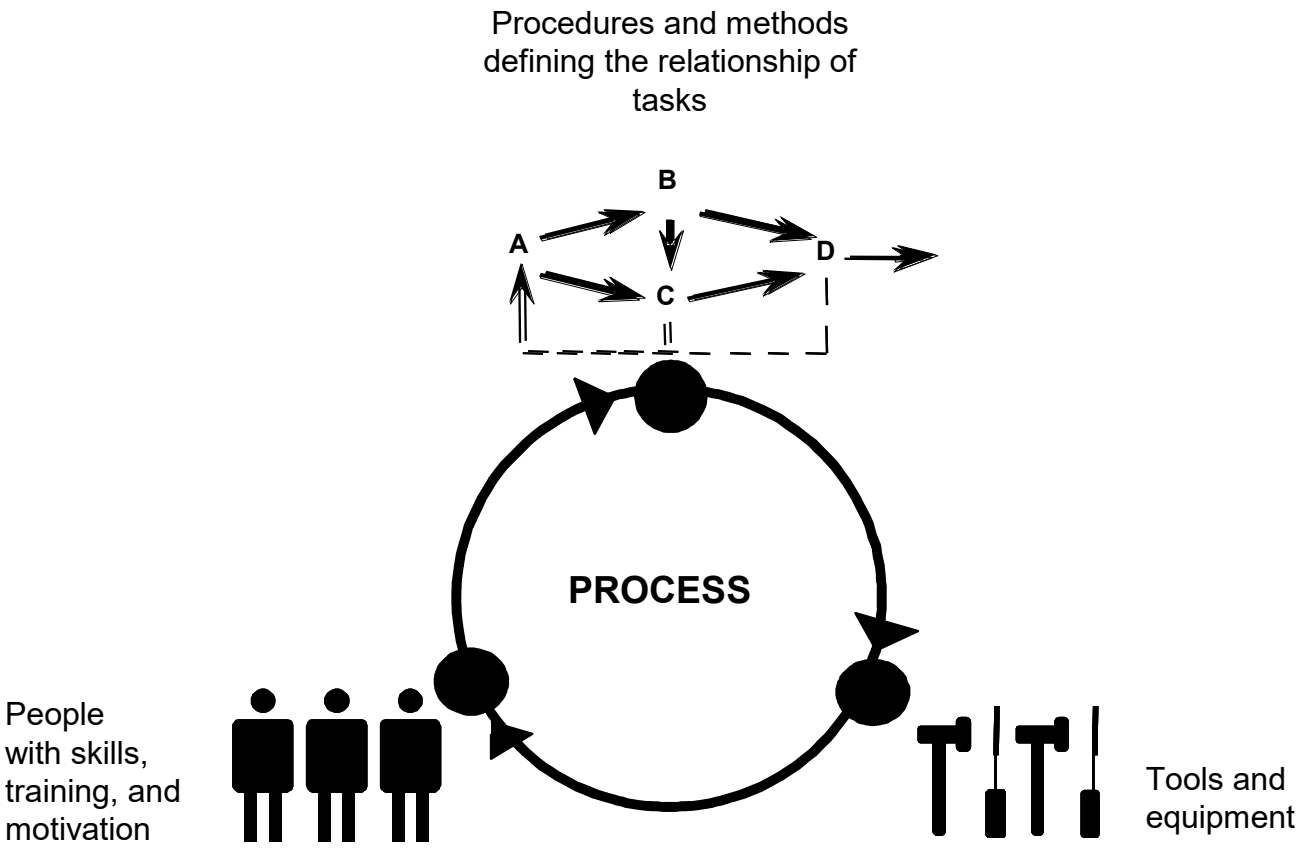


Figure 1: Three Critical Dimensions [3]

22 Process Areas

- Causal Analysis and Resolution (CAR)
- Configuration Management (CM)
- Decision Analysis and Resolution (DAR)
- Integrated Project Management +IPPD (IPM+IPPD)
- Measurement and Analysis (MA)
- Organizational Innovation and Deployment (OID)
- Organizational Process Definition +IPPD (OPD+IPPD)
- Organizational Process Focus (OPF)
- Organizational Process Performance (OPP)
- Organizational Training (OT)
- Product Integration (PI)
- Project Monitoring and Control (PMC)
- Project Planning (PP)
- Process and Product Quality Assurance (PPQA)
- Quantitative Project Management (QPM)
- Requirements Development (RD)
- Requirements Management (REQM)
- Risk Management (RSKM)
- Supplier Agreement Management (SAM)
- Technical Solution (TS)
- Validation (VAL)
- Verification (VER)

Maturity Level

- A defined evolutionary plateau for organizational process improvement.
- Matures an important subset of the organization's processes, preparing it to move to the next maturity level.
- Levels are measured by the achievement of the specific and generic goals associated with each predefined set of process areas.

Maturity Levels

- Level 1: Initial – processes are usually ad hoc and chaotic.
- Level 2: Managed – the projects of the organization have ensured that the requirements are managed and that processes are planned, performed, measured, and controlled.
- Level 3: Defined – processes are well characterized and understood, and are described in standards, procedures, tools, and methods.
- Level 4: Quantitatively Managed – the organization and projects establish quantitative objectives for quality and process performance and use them as criteria in managing processes.
- Level 5: Optimizing – an organization continually improves its processes based on a quantitative understanding of the common causes of variation inherent in processes.

Appraisal Method

Standard CMMI Appraisal Method for Process Improvement (SCAMPI)

- Class A – comprehensive assessment, interviews, documentation review, product inspection.
- Class B – some interviews, documentation review.
- Class C – documentation review.

UPC Bar Code Parity Bit Checking

- What is UPC?
  - UPC is Universal Product Code
  - It is a Bar Code that is widely used in the United States and Canada for tracking items
  - Split into two parts: a manufacture's code and a product code

Two Common Types of Bar Codes

- **UPC-A**
- A 12 decimal digit code
- Split into two sections, which are separated by a middle bit
- Each bar code consist of 30 bars

- **UPC-E**
- A six decimal digit code
- Used on smaller packages where the full 12 digit UPC-A code will not fit

Split of UPC Bar Codes

UPC Prefixes

- 0, 1, 6, 7, 8, or 9 are used for most products
- 2 is reserved for local use such as warehouse and in store products
- 3 is reserved for National Drug Code
- 4 is reserved for local use such as store and warehouse for loyalty cards or store coupons
- 5 is reserved for coupons

Understanding the Code (UPC-A)

- The code is SLLLLLLLMRRRRRRE
- The Check Bit is the 12th and final digit
- Each digit is seven bits with a total of 95 bits
- Start, Middle and End all include two bars
- Each number consists of two bars for a total of 30 bars

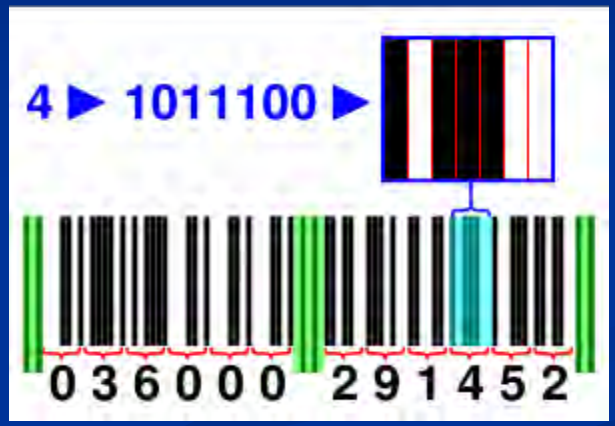
Understanding the Code (UPC-A)

Digit	Pattern	Digit	Pattern
0	0001101	5	0110001
1	0011001	6	0101111
2	0010011	7	0111011
3	0111101	8	0110111
4	0100011	9	0001011

Understanding the Code (UPC-A)

- In the UPC-A barcode each digit is represented by a seven digit sequence
- Zero indicate a space while Ones indicate a bar
- Numbers that occur after the middle bar are inverted

Examples of UPC-A Bar Codes



Parity Bit Checking (UPC-A) Step One

- Add all the odd numbering positions together and multiply the sum by 3
- Positions are

  1, 3, 5, 7, 9, 11

Parity Bit Checking (UPC-A) Step Two

- Add the values of all the even positions together
- Positions are 2, 4, 6, 8, 10

Parity Bit Checking (UPC-A) Step Three

- Take the results of steps one and two and add them together

Parity Bit Checking (UPC-A) Step Four

- Take the sum of step three
- The check digit is the number that when added to the sum makes it a multiple of ten
- The 12th digit, the check bit, is shown in the graphic as the number 2

SPACE SHUTTLE SAFETY AND RELIABILITY ANALYSIS

Qualitative vs. Quantitative Analysis

- What methods should be used for Reliability and Safety Analysis?
- Risk models initiated for Apollo Program.
- Quantitative analysis abandoned as program evolved
  - Predicted failure probabilities appeared inconsistent with test and unmanned flight experience
  - Predicted failure rates were high
- Decision to rely on qualitative analysis and processing controls
  - Design analysis to identify failure modes
  - Qualification of all Single Failure Points
  - Design review of all modifications since last design review
  - Review of test results
  - Review of all significant failures and corrective actions
  - Review of all unsolved problems

Qualitative vs Quantitative Analysis

- Shuttle Program
- Shuttle designed in 1970's
  - Extensive modifications since first flight
- First flight 12 April 1981
- 135 fights
- Last flight July 21, 2011
- First reusable spacecraft
  - Apollo qualitative approach continued
  - Traditional tools (life testing, reliability demonstration, maintainability analysis, etc) not deemed suitable for spacecraft
  - Decision to focus on engineering failure modes out rather than reliability predictions
  - "We don't play the numbers game"
- Dependency on design review, redundancy and rigorous processing controls

Safety & Reliability Specifications

- NSTS 5300.4 (1D-2) SRM&QA Provisions for the Space Shuttle Program
  - 1D201 System Safety: The contractor shall perform a qualitative hazard analysis to identify hazards and assure their resolution
  - ID301 Reliability Engineering: The contractor shall establish a system for the preparation, maintenance, and control of FMEAs and CILs
- NSTS 07700 Vol. X, Shuttle Flight and Ground System Specification
  - 3.5.1.1.1 Flight Vehicle Subsystem Reliability (Fail-Safe)
    - The redundancy requirements for all flight vehicle subsystems shall be established on an individual subsystem basis, but shall not be less than fail safe during all mission phases including intact aborts
    - Fail-Safe - The ability to sustain a failure and retain the capability to successfully terminate the mission (i.e. single failure tolerant)
      - Bring the crew back alive (flight systems)
      - Put the system into a safe configuration (ground systems)

FMEA-Failure Modes and Effects Analysis

- Failure Mode - Identification of all possible ways a component fail
  - Premature operation
  - Failure to operate at a prescribed time
  - Failure to cease operation as a prescribed time
  - Failure during operation
- Effects Analysis - Identifies the specific failure mode effects.
  - Includes the safety and mission success consequences on the subsystem, interfacing subsystem, mission, crew, vehicle
- Each hardware item is analyzed for each possible failure mode and for the worst case effect.
- The failure effects, causes, criticalities, etc., are individually assessed for each failure mode on each component.
- FMEAs are be prepared on all hardware… regardless of the probability of occurrence for each failure mode.

CIL-Critical Items List

- Derived from the FMEA. It documents failure modes which are deemed "critical" by program definition.
  - Failure could lead to loss of life/vehicle or mission
- Each item requires a retention rationale to "retain" the CI rather than eliminate through design
- Retention rationale mandates applicable tests and inspections during ground processing.
- Each CIL is formally presented to Program Management for approval

FMEA/CIL Benefits and Uses

- Design and Assurance Tools
  - Analyze design for compliance with requirements.
  - Identify Single Failure Points (SFPs).
  - Proactive tool initiated early in design.
  - FMEA is an inductive or "bottom-up" approach looking at components and systems.
  - Identifies areas for redundancy
- Risk Assessment/Management Tool
  - Identifies high risk items and provides management with rationale for decision making.
  - Documents the rationale behind design alternatives and mitigations of potential failures.
- Processing
  - Used to identify items which must be verified/checked out during ground processing.

FMEA/CIL Drawbacks

- Does not distinguish between high and low probability failures
- No overall risk focus
- Only identifies single independent failures
  - Common mode failures may be hidden
- Does not account for human error
- Expensive to perform-very labor intensive

Hazard Identification

- Items being designed are evaluated for any potentially hazardous situation that will influence or effect the function of the item.
- The potential hazards evaluation should include (but not be limited to):
  - Energy Sources - Chemical, Electrical, Mechanical, Kinetic…
  - Human Engineering - Human Capability, Human Hazards…
  - Contamination - Introduction of Contaminants to Surfaces, Orifices, Filters…
  - Interface Interaction - Compatibility Between Systems, Subsystems, GSE, Facilities, Software…
  - Natural Environment - Lightning, Radiation, Thermal, Pressure, Gravity, Humidity…
  - Induced Environment - Thermal, Vibration/Sound, Pressure…
  - Material Deformation - Degradation of Material by Corrosion, Ageing, Embrittlement, Oxidation…
  - Toxicants - Adverse Human Effects of Inhalants or Ingestion

Hazard Analysis/Hazard Report Description

- Hazard
  - The presence of a potential risk situation caused by an unsafe act or condition
- Hazard Analysis
  - Hazard Analyses identify hazards and their causes. Elimination or control of the causes is per the following hazard reduction precedence sequence.
    - Design
      - Elimination
      - Minimize through redundancy
    - Use of safety devices (i.e., parachute)
    - Use of warning devices
    - Use of special procedures to counter the hazardous condition.
  - Hazard analysis is a "top down" approach beginning with an undesired event and encompasses operational procedures, human error, and design

Hazard Report

- Hazard Report (HR)
  - Derived from the hazard analysis and lists the causes of hazards and the controls associated with those causes
  - Each hazard cause is assigned a likelihood and severity
  - The HR, like the CIL, provides the acceptance rationale as to why the hazard is acceptable to the program
  - Each hazard report with each cause is formally presented to Program Management for approval

Hazard Report Risk Matrix

Likelihood	Marginal	Critical	Catastrophic
Probable	***Accepted Risk***	***Accepted Risk***	***Unacceptable Risk***
Infrequent	***Accepted Risk***	***Accepted Risk***	***Accepted Risk***
Remote	Controlled Risk	***Accepted Risk***	***Accepted Risk***
Improbable	Controlled Risk	Controlled Risk	Controlled Risk

Severity

Hazard Report Definitions

- Likelihood
  - Probable: Expected to happen in the life of the program
  - Infrequent: Could happen in the life of the program. Controls have significant limitations or uncertainties
  - Remote: Could happen in the life of the program, but not expected. Controls have minor limitations or uncertainties
  - Improbable: Extremely remote possibility that it will happen in the life of the program. Strong controls in place
- Severity Level - The severity level is an assessment of the most severe effects of a hazard.
  - Catastrophic: Hazard could result in fatal injury to personnel and/or loss of major elements of the flight vehicle or ground facility
  - Critical: Hazard could result in serious injury and/or damage to flight or ground equipment that would cause mission abort or a significant program delay
  - Marginal: Hazard could result in a mishap of a minor nature inflicting first-aid injury to personnel and/or damage to flight or ground equipment that can be tolerated without mission abort or delay

Hazard Report Definitions

- Classification - Assign a classification to each hazard cause of controlled or accepted risk. Hazard cause with a classification of eliminated will not be included in the HR
  - Eliminated Hazard: A hazard that has been eliminated by completely removing the hazard causal factors
  - Controlled Hazard: The frequency of occurrence and/or severity level have been reduced by implementing the appropriate hazard reduction precedence sequence to comply with program requirements
  - Accepted Risk: A hazard for which the controls for one or more hazard causes fail to meet the hazard reduction precedence sequence and, therefore, have limitations or uncertainties such that the hazard could occur during the life of the program

Accepted Risk

- Risk – The qualitative chance of loss of personnel capability, loss of system, or damage to or loss of equipment or property.
  - Accepted risk – a hazard for which the controls (for one or more hazard causes) have limitations or uncertainties such that the hazard could occur during the life of the program.
- The following are examples of conditions that could be considered accepted risk hazards:
  - Critical Single Failure Points
  - Limited controls or controls that are subject to human error or interpretation
  - System designs or operations that do not meet industry or government standards.
  - Complex fluid system leaks
  - Safety detection and suppression devices which are not adequate
  - Uncontrollable random events which could occur even with established precautions and controls in place, such as weather or fires.

Hazard Analysis Benefits and Uses

- Design and Assurance Tools
  - Analyze design for hazards
  - Proactive tool initiated early in design.
  - Hazard Analysis is deductive or Top Down approach
- Risk Assessment/Management Tool
  - Identifies hazards and provides management with rationale for decision making.
  - Documents the rationale behind design alternatives and mitigations of potential failures.
- Processing
  - Used to identify items which must be verified/checked out during ground processing.
- Flight
  - Used to identify in-flight contingency actions

FMEA/CIL/Hazard - Maintenance & Processing

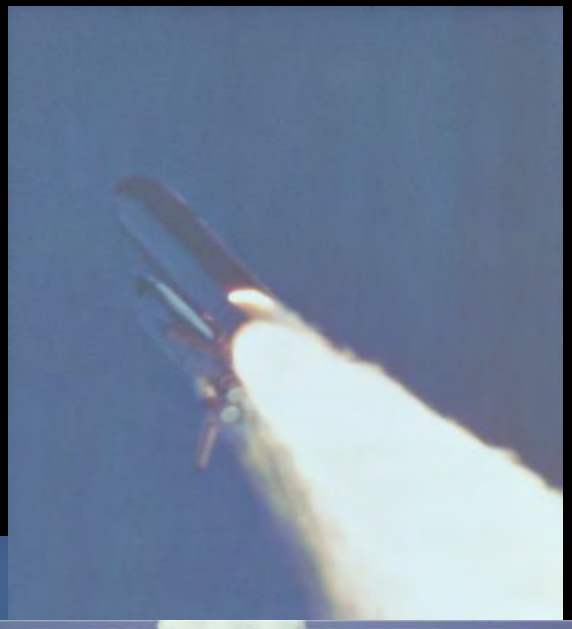
- FMEA/HA identifies risk associated with design (critical failure modes and hazards)
- CIL/HR identifies causes and maintenance requirements necessary to reduce risk of critical failure mode/hazard cause to an acceptable level
- Master Verification Plan (MVP) provides checkout verification requirements based on severity (criticality of failure mode) and likelihood (failure history)
- OMRSD specifies system maintenance requirements based on CIL's, HR's and MVP
- OMI provides detailed processing procedures for accomplishing OMRSD requirements
- Configuration Management verifies accomplishment of the OMRSD requirements

Summary

- Rigorous Process
  - Comprehensive analytical effort
  - Identified potential problem areas during design
  - Operational problem areas identified
  - Feedback process in place to address problems
  - Problems either eliminated, mitigated, or accepted as low risk
- FMEA/CA and HA good complementary processes
  - FMEA/CIL bottom up inductive process
  - HA top down deductive process
- But….
  - Limitations in understanding overall risk due to qualitative approach
  - Does not consider decision making process

Shuttle Accidents-Challenger

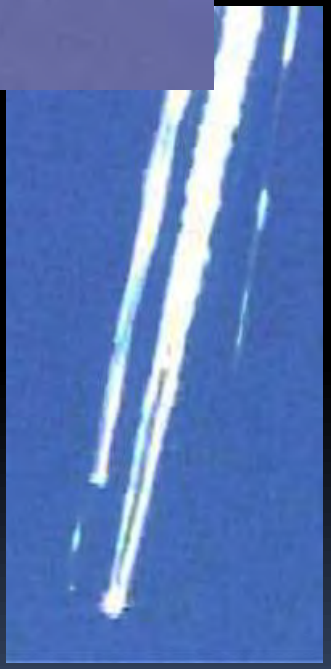
- Challenger January 28, 1986[3]
  - O-ring failure in Solid Rocket Booster
    - O-ring originally 1R, changed to 1 in Nov 1982
  - Faulty design unacceptably sensitive to temperature (temperature was 2° C, previous low temp was 13°C) and other factors
  - Flawed decision process
    - Persons making the launch decision were not aware of previous problems with O-ring



Pictures courtesy the NASA Johnson Space Center (NASA-JSC).

Shuttle Accidents-Columbia

- Columbia February 1, 2003[4]
  - Breach in left wing due to foam debris from External Tank bipod ramp
  - Foam loss experienced on more than 80% of flights
  - Management team did not understand significance of foam loss



AP Photo/via KXAS-TV

Common Issues on Accidents

- Flawed decision making
  - Significance of O-ring erosion on pre-Challenger flights
    - STS-51C O-ring erosion
  - Significance of External Tank foam shedding on Pre-Columbia flights
    - Debris strike seen on post launch video
    - Foam strikes on STS-27R (2 Dec 1988) not taken into account when foam loss observed during STS-107 ascent
    - No attempt made to inspect Obiter for damage by crew (damage to wing hidden by payload bay doors)
  - Believed that previous successes provided a safety margin[5]
    - Failure to understand probability of failure
- Dependence on qualitative analysis techniques
  - Miss the overall risk posture
  - Management estimate of Shuttle risk much, much less than engineer's estimate

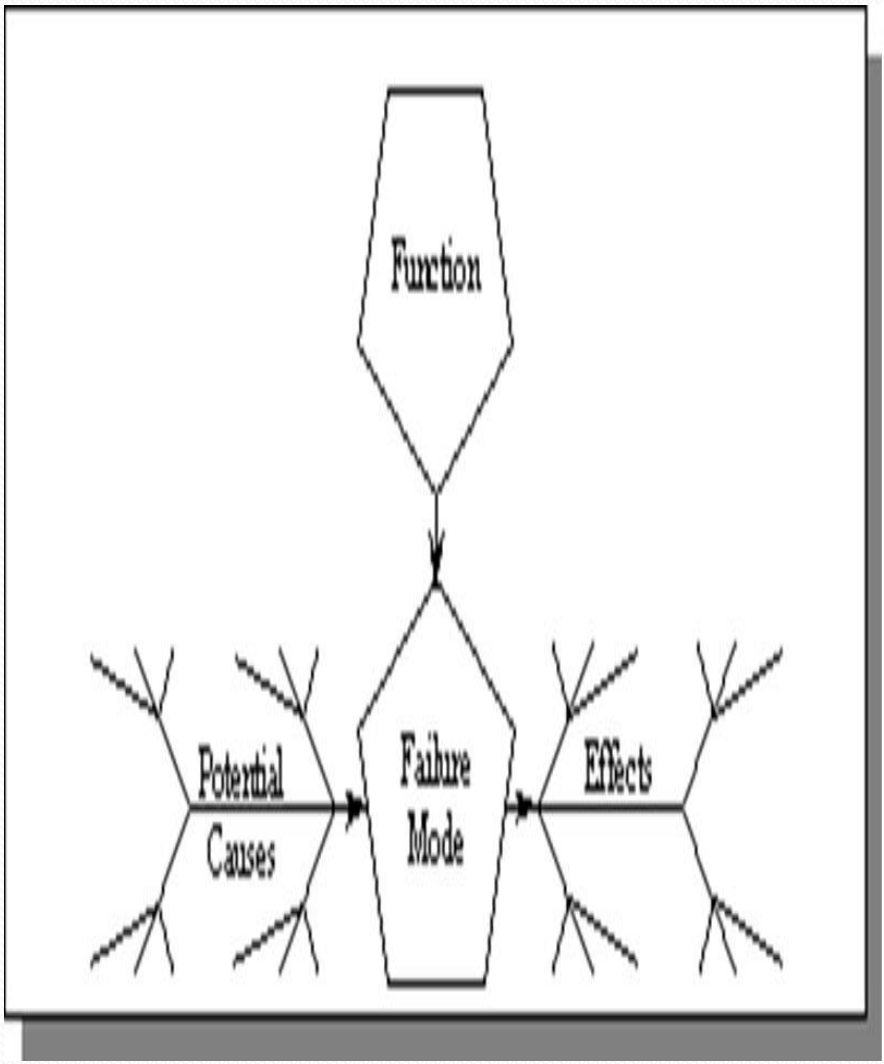
Future

- Continued utilization of FMEA/CIL and HA/HR methodology as primary risk baseline tools
- Good complementary processes but have limitations in assessing overall risk due to qualitative approach
- Utilization of PRA for problem investigation and decision making during flight operations incorporates a quantitative aspect lacking in FMEA/CIL & HA/HR
  - Mission Management Team
    - Meets daily during all Shuttle missions to consider and resolve in-flight problems
  - Repair-accept tradeoffs
    - Risk of no repair to tile on Orbiter vs risk of performing in space repair
    - Qualitative approach cannot answer the question

Automated FMEA (Failure Mode Effect Analysis)

What is FMEA?

- Failure Mode Effect Analysis : Analysis compile list of component failure modes and infer the effects of failure modes.
- System model: Analysis infer how local effect propagate through complex architecture and cause hazard effect at system level.



Problems in FMEA

- Time taken in developing a FEMA is more than modeling the design because it is a manual and laborious process
- Analysis is useful for mere delivery to costumer but not useful for product improvement
- Difficulty increases as complexity increases
- Automation can lead to simplification of FMEA

FMEA Characteristics

- Scope of FEMA
  - The scope is limited because of difficulties of efficiency and scalability of algorithms of automated FMEA.
  - It is widely used in manufacturing industries in various phases of the product life cycle and is now increasingly finding use in the service industry.
- Uses of FEMA
  - The outcome of an FMEA development is actions to prevent or reduce the severity or likelihood of failures, starting with the highest-priority ones. It may be used to evaluate risk management priorities for mitigating known threat vulnerabilities.
  - FMEA helps select remedial actions that reduce cumulative impacts of life-cycle consequences (risks) from a systems failure (fault).

A New Approach to FEMA

- Basis of Approach
  - Based on automating fault tree analysis
  - Built from engineering diagram which is about the component failures
- Features
  - The automated model is generic
  - The model provides the basis for analysis of the topology of a system.
  - The model provides a hierarchal dataflow which are used in many area of engineering design.

Analysis Steps

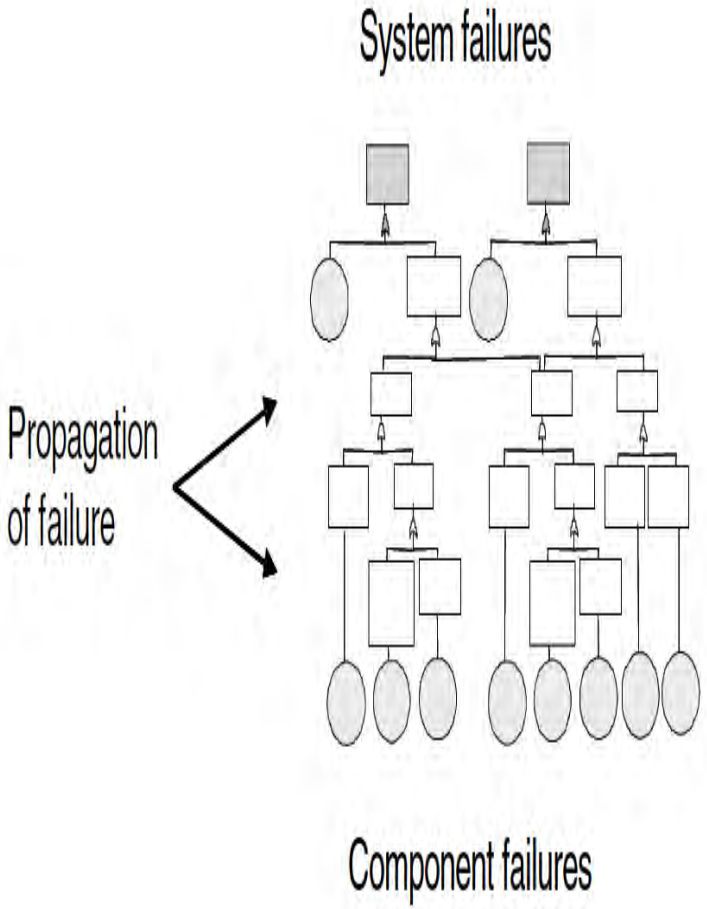
- Establishment of failure behavior of components in model as failure expressions
- These failure expressions represents the output failures due to malfunctions of components and deviations of component inputs.
- This creates structure of model. This automatically determines the basis of propagation of local failures through connections of models and causes of outputs failures of system.
- A global view of the system is obtained through the fault tree. This is constructed by travelling back from final elements to the system input and evaluating the failure expression of the components traversed.

Fault tree synthesis

- Shows how logical combination of component failures causes the output failures
- This fault tree synthesis is network of interconnected fault trees. This contains the logical relationship of components to system failures. A logical combination can share more than one branch or event, i.e. more than one system failure.

Block diagram

- System failure
- Leaf node: component failure
- Immediate system failure: failure propagation and progressive transformation of system failure



Automated Algorithm

- Transformation of network into table corresponding to
- Component System failure

Analysis from the table

- Each failure on each system
- Effect of failure of component on more than one system

Comparison with classical FMEA

- In classical approach only effect of single failures can be accessed
- In this automated FMEA effect of component on more than one system can be obtained
- Automated FEMA helps analysis not only to locate the problem in the design but also the fault tolerance level of the system.

Practical application

- FMEA is developed from MATLAB Simulink
- This is used for medium complexity of advanced steer by wire prototype system in Volvo cars. This system has hundreds of components and thousand of cut sets.
- FMEA is developed in just more than minutes.

Advantages of automated FMEA

- FMEA obtained records effects of four simultaneous component failure modes in minutes.
- Two component failure modes in few seconds
- When compared to other models which can take hours even for just a single components .

SIL RATINGS

* Why Have SIL Ratings? SAFETY INTEGRITY LEVEL
  * Deepwater Horizon Disaster – 11 dead
  * Bhopal Disaster – 2787 deaths
  * Texas City Plant explosion – 581 deaths
  * Murphy's Law – If something can go wrong, it will.

Current Regulations

* ISA – S84.01
* IEC 61508/61511

These are performance oriented regulations which are left up to the industry on how and when to follow (not enforced)

How to determine SIL Rating

* HAZOP team established
* Risk = Probability X Consequence
* Must be applied to entire system:
  * Hardware
  * Software
  * Equipment

SIL CLASSIFICATIONS

Safety Integrity Level	Risk Reduction Factor	Probability of Failure on Demand
SIL 4	100,000 to 10,000	10^{-5} to 10^{-4}
SIL 3	10,000 to 1,000	10^{-4} to 10^{-3}
SIL 2	1,000 to 100	10^{-3} to 10^{-2}
SIL 1	100 to 10	10^{-2} to 10^{-1}

The Future – Where are we heading?

* Government Involvement (enforcement)
* Certification Agency Creation
* More classifications and a better system resulting in a safer system design

Outline (Thoughts and excerpts from past classes)

- Risk
  - Probabilistic Risk Assessment (PRA)
  - Business Continuity
- Hardware
  - Comments on High Reliability without Redundancy
  - 1553 Busses
  - XTMR Tool
  - X-38 System Integration and Test Facility (SITF)
  - Stratus and the Stock Exchange of India
  - Commercial Aircraft
- Software: Associated Technologies
  - COCOMO
  - Nano Technology
  - Error Tolerant Computing
  - CMMI
  - FT in UPC (Universal Product Codes)
  - FEMA
  - SIL – Safety Integrity Level
- **FT In Our Daily Life**
  - Automobiles
  - Health Care Systems
  - Warranty: Product Lifespan
- What I've Learned

AUTOMOBILES: Synergy Between Mechanical Systems and Electronics

- ✓ Better fuel economy.
- ✓ Better vehicle performance in adverse conditions.
- ✓ Driver assisting functions
  - Anti-Lock Braking Systems (**ABS**)
  - Traction Control (**TCS**)
  - Electronic Stability Control (**ESP**)
  - Brake Assist (**BA**)
- ✓ Safety features
  - Collision Warning
  - Automatic Collision Avoidance Systems

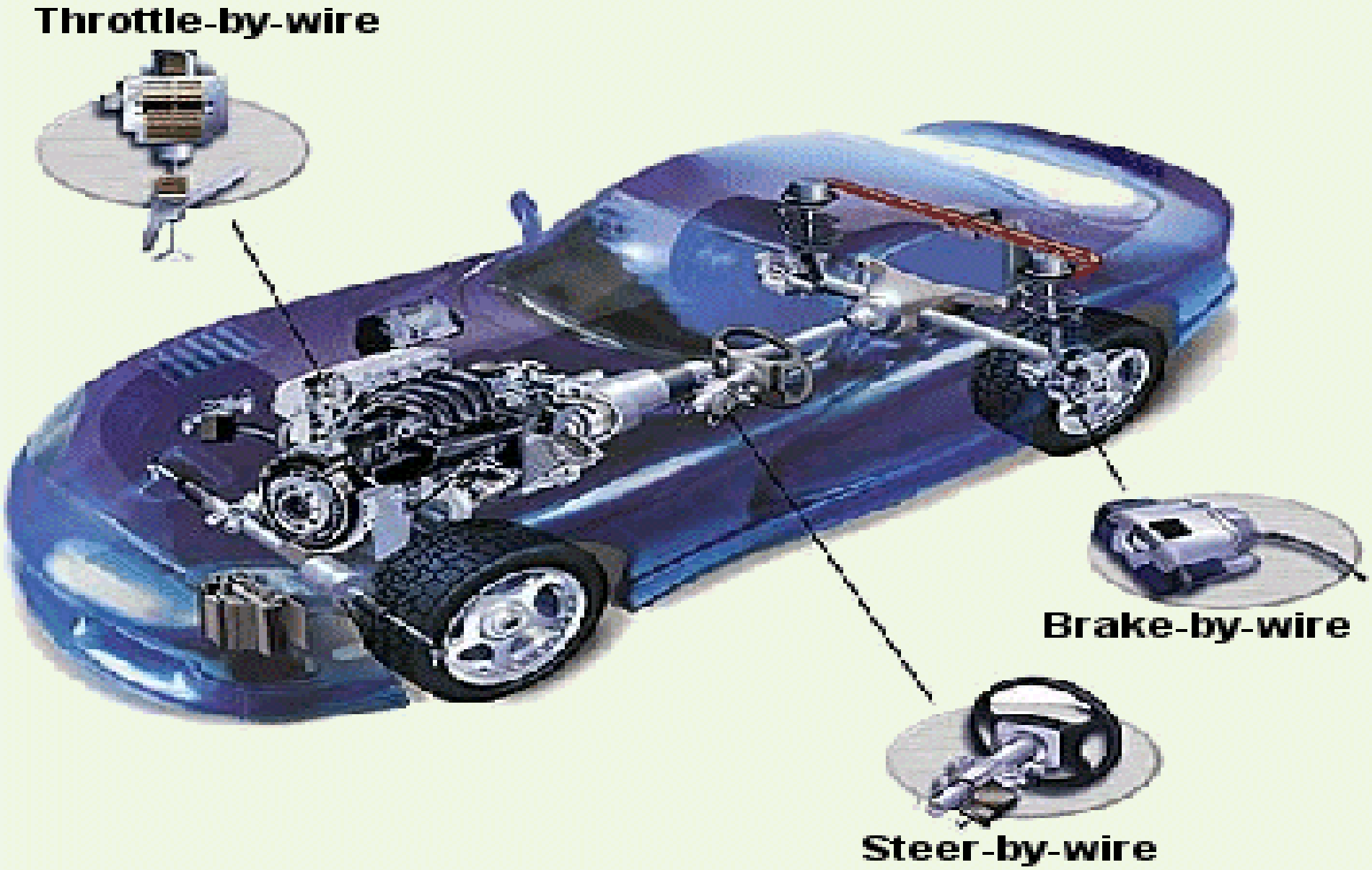
To design cars with better performance and higher level of safety, engineers must substitute mechanical interfaces (e.g., brake pedal) between the driver and the vehicle with electronic systems.

These systems are common in the aerospace industry and are generically called **X-By-Wire/Fly-By-Wire** Systems

X-by-wire systems consist of:

- Brake pedal
- Throttle
- Gear selector
- Steering wheel

In automobiles all of the system processing is normally done by micro-controllers connected to electrical actuators.

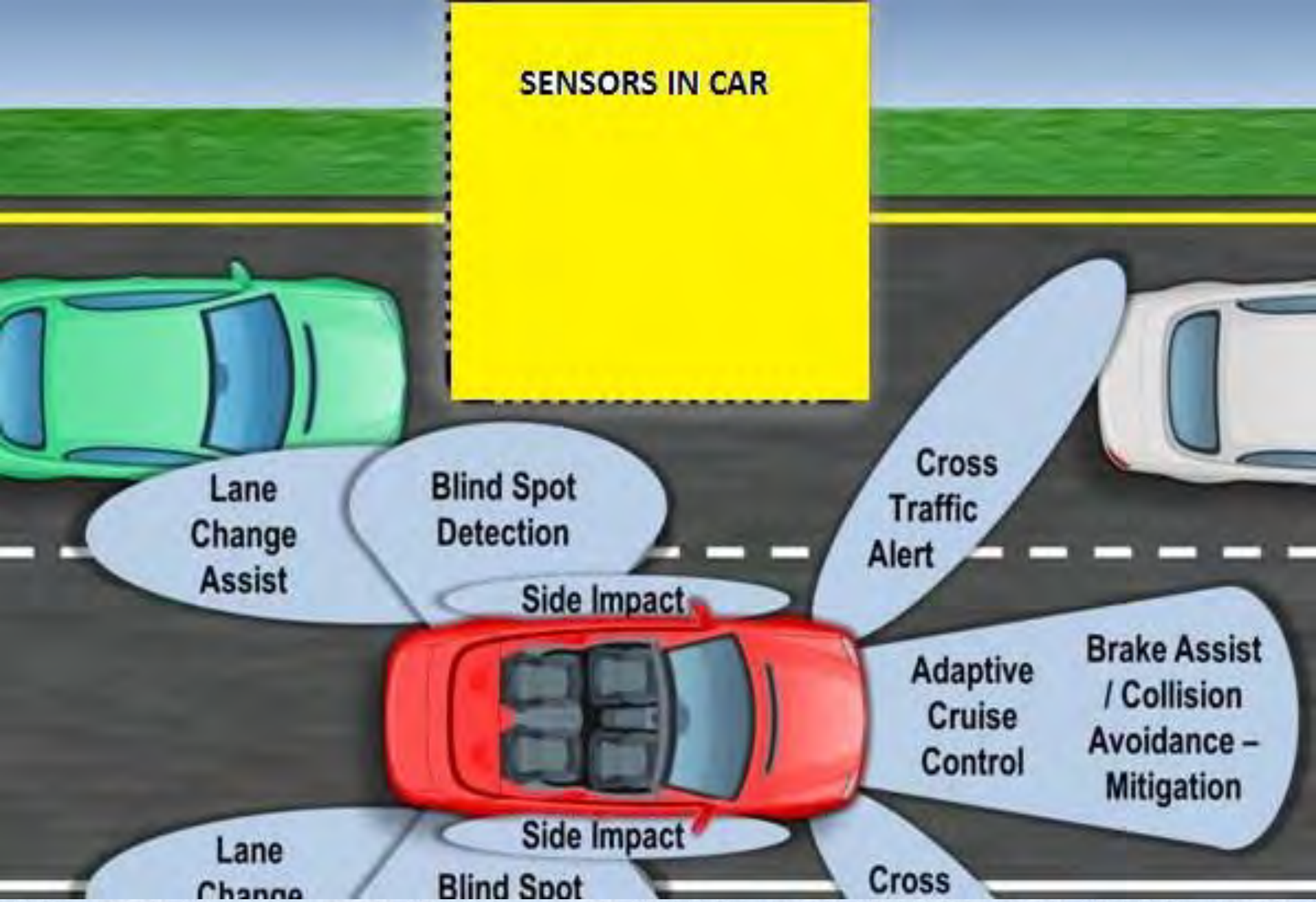

Throttle-by-wire
Brake-by-wire
Steer-by-wire

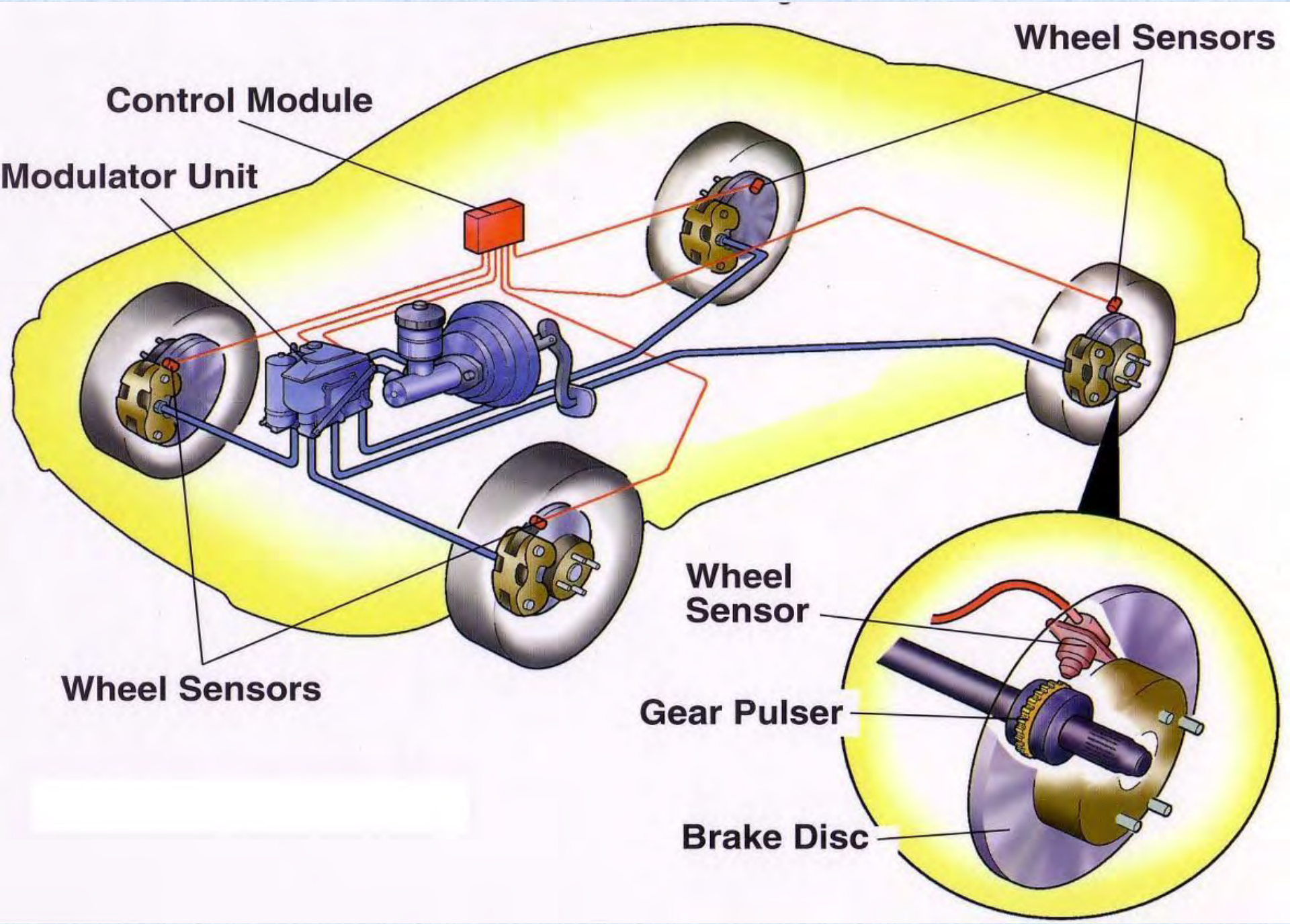
Mechanical Back-Ups

Throttle-By-Wire: A Throttle Spring System provides a reduced Engine Speed in the event of electronic Failure.

Electronic braking functions (ABS, TCS, ESP, BA): the brake system behaves like a conventional one providing a mechanical backup.

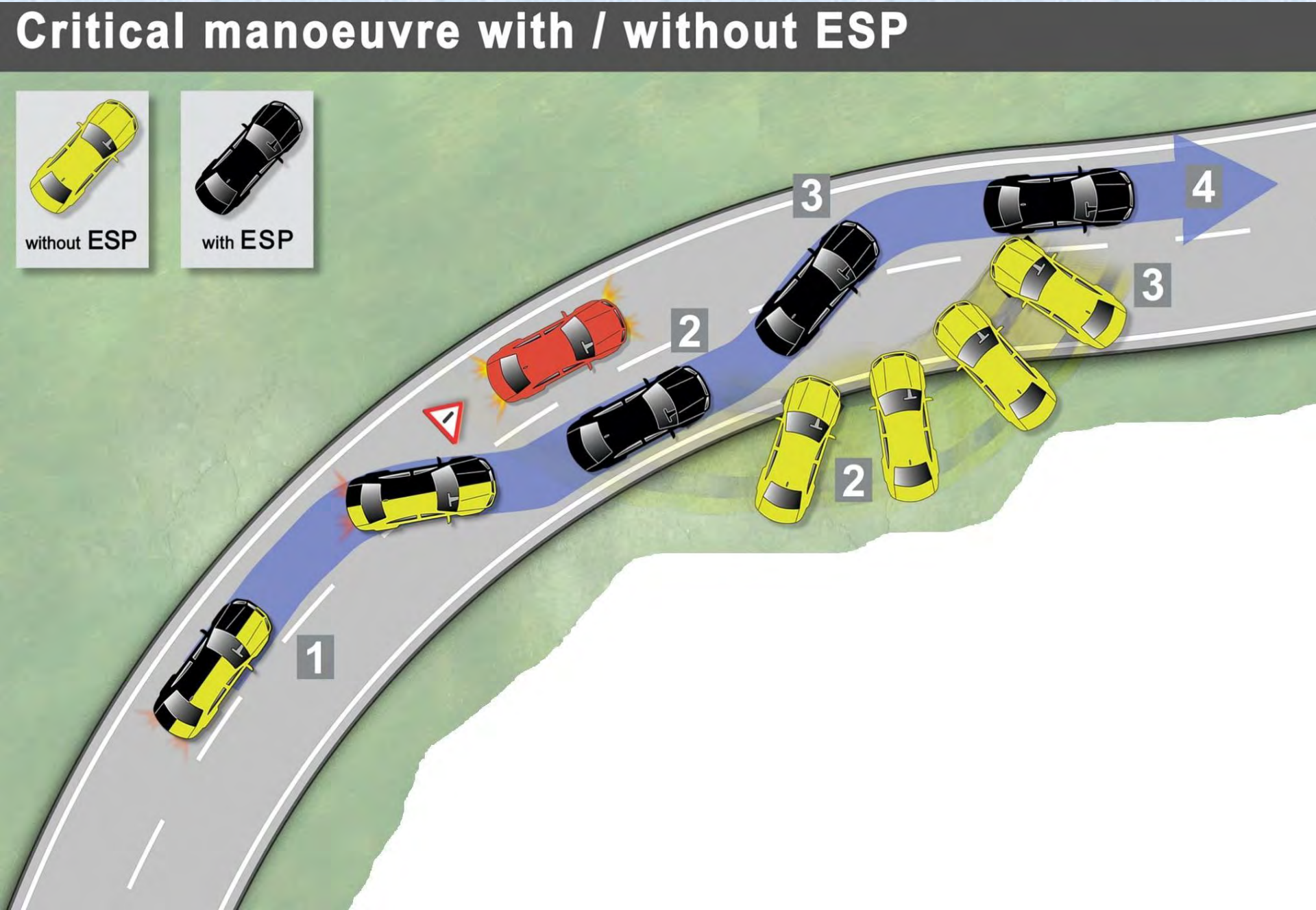
Mechanical backups relieve electronics of stringent fault-tolerance requirements.


SENSORS IN CAR
Lane Change Assist
Blind Spot Detection
Cross Traffic Alert
Side Impact
Adaptive Cruise Control
Brake Assist / Collision Avoidance – Mitigation
Side Impact
Lane
Blind Spot
Cross


Wheel Sensors
Control Module
Modulator Unit
Wheel Sensors
Wheel
Sensor
Gear Pulser
Brake Disc

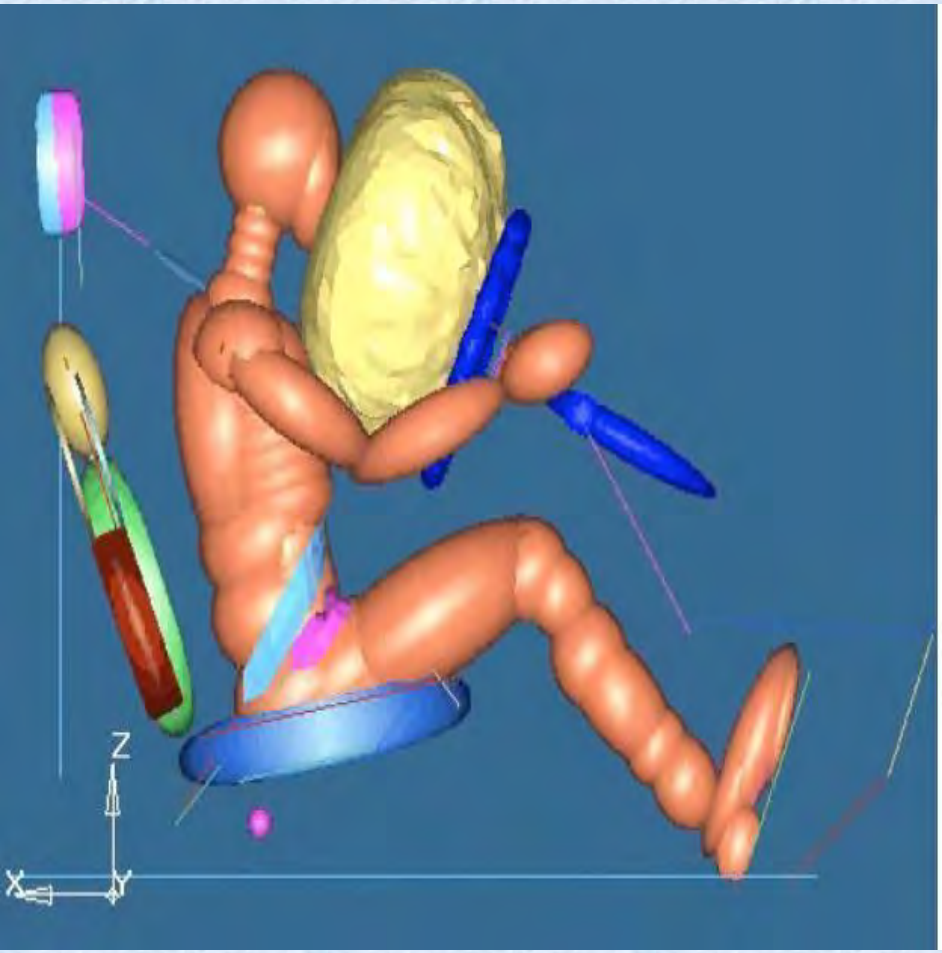

ABS warning light
60
mph
80
100
120
140
160
180
200
220
40
60
80
100
120
20
40
20
km/h
ABS

Electronic Stability Program (ESP) with ES Control

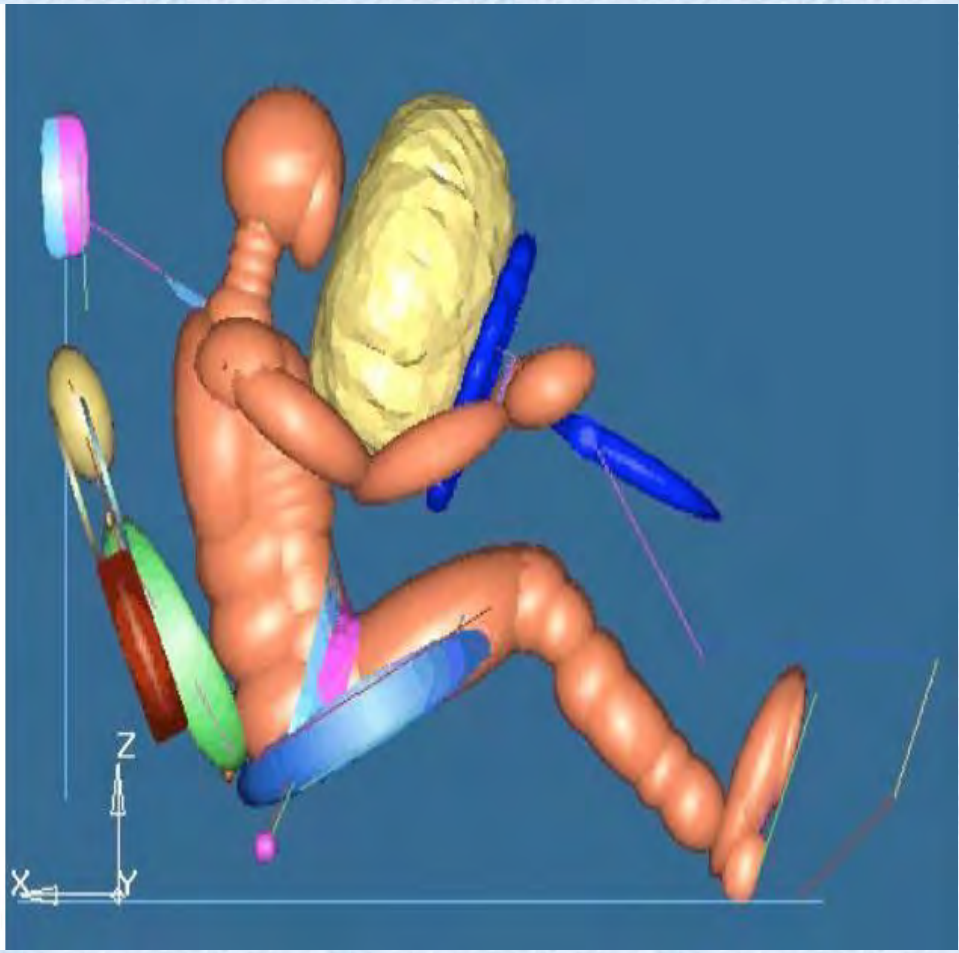


Counter Balance Motion (CBM) Seat

- Automatically adjusts.
- Movable Lumbar along with a seat motion that makes one feel “safe.”



Traditional Seat



CBM Seat

Fault Tolerant Design Approaches

Any form of fault-tolerance is based on redundancy.

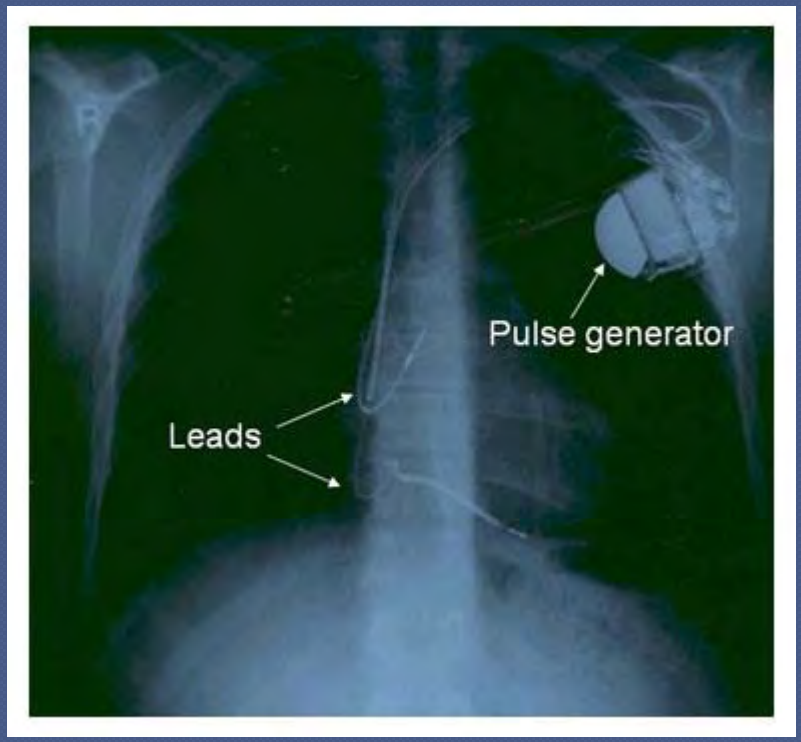
Types of redundancy:

- Spatial
- Temporal
- Information

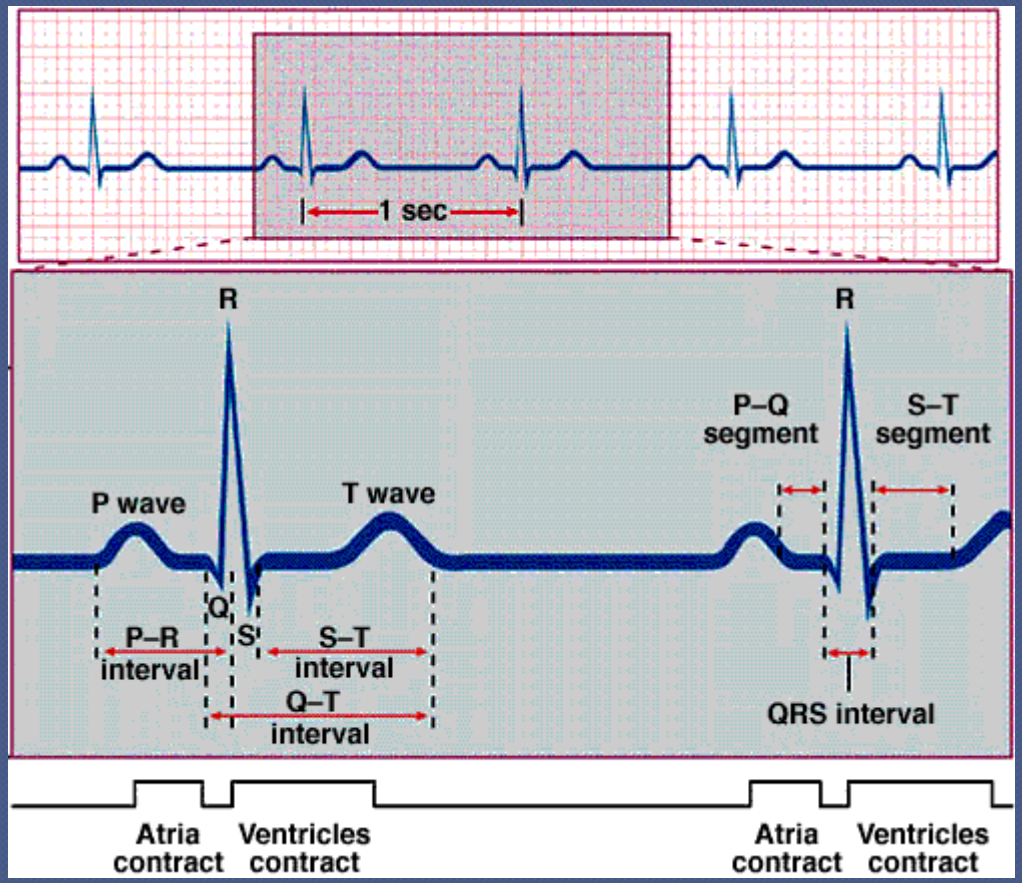
Redundancy alone does not guarantee fault-tolerance but is a logical start.

Fault Tolerance in Implantable Cardiac Devices

Inserted medical device containing a microprocessor, pulse generator and one to three leads for the purpose of maintaining normal heart rhythms.



Heart's Own Fault Tolerant System



Homeostasis:

Rhythmicity
Automaticity
Adaptive

Considerations & Constraints

Safety critical device, Class III (FDA)

Size

Cost → Favors simplex system

Power

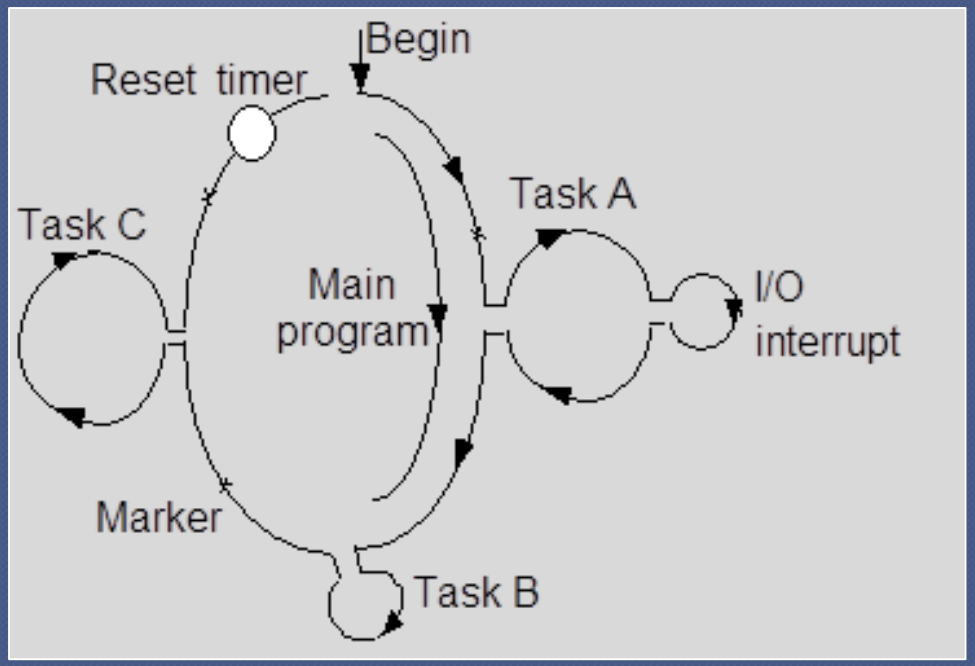
Complexity

Risk and reliability management depend on design and testing

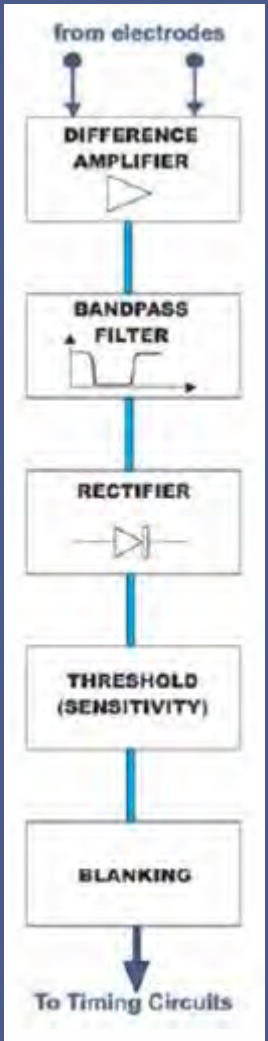
Fault Tolerance: Microprocessor

Watchdog Timer:
Waits for high priority interrupt signal to restart the system when a hardware or software fault fails to reset the timer.

Redundant components:
ROM/RAM module
Clock



Pulse Generator



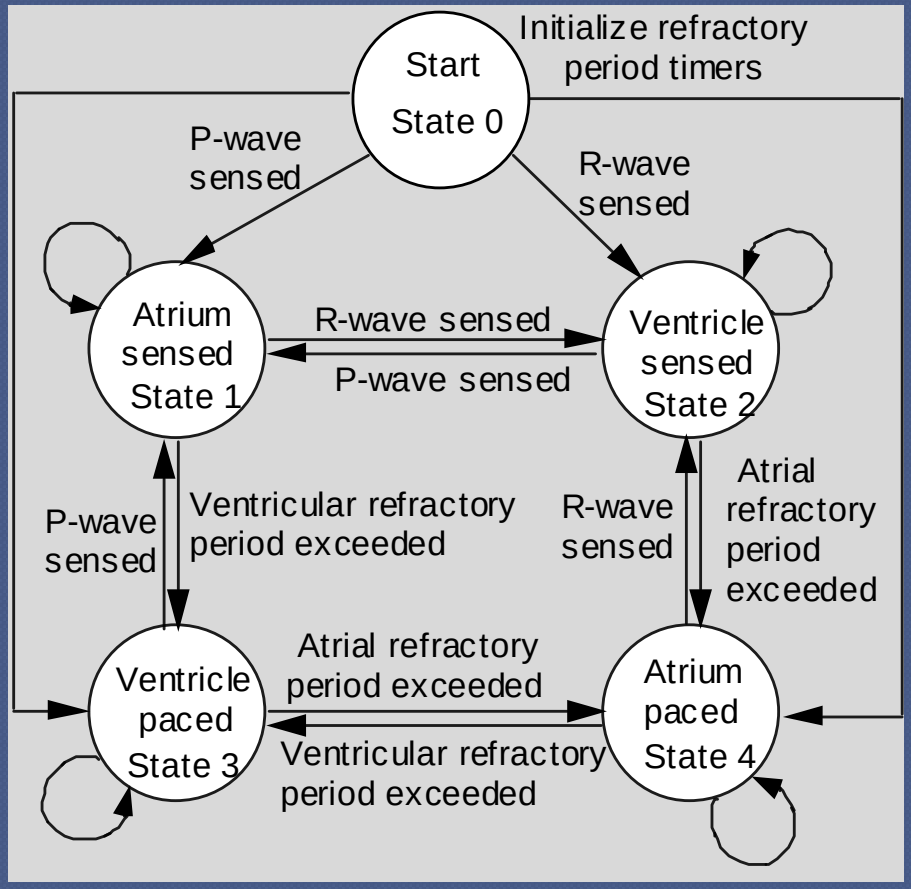
Sensing:

Front-end, single-event detection
Two or three leads
Amplifier/Filter (Wavelet analysis)
Comparator

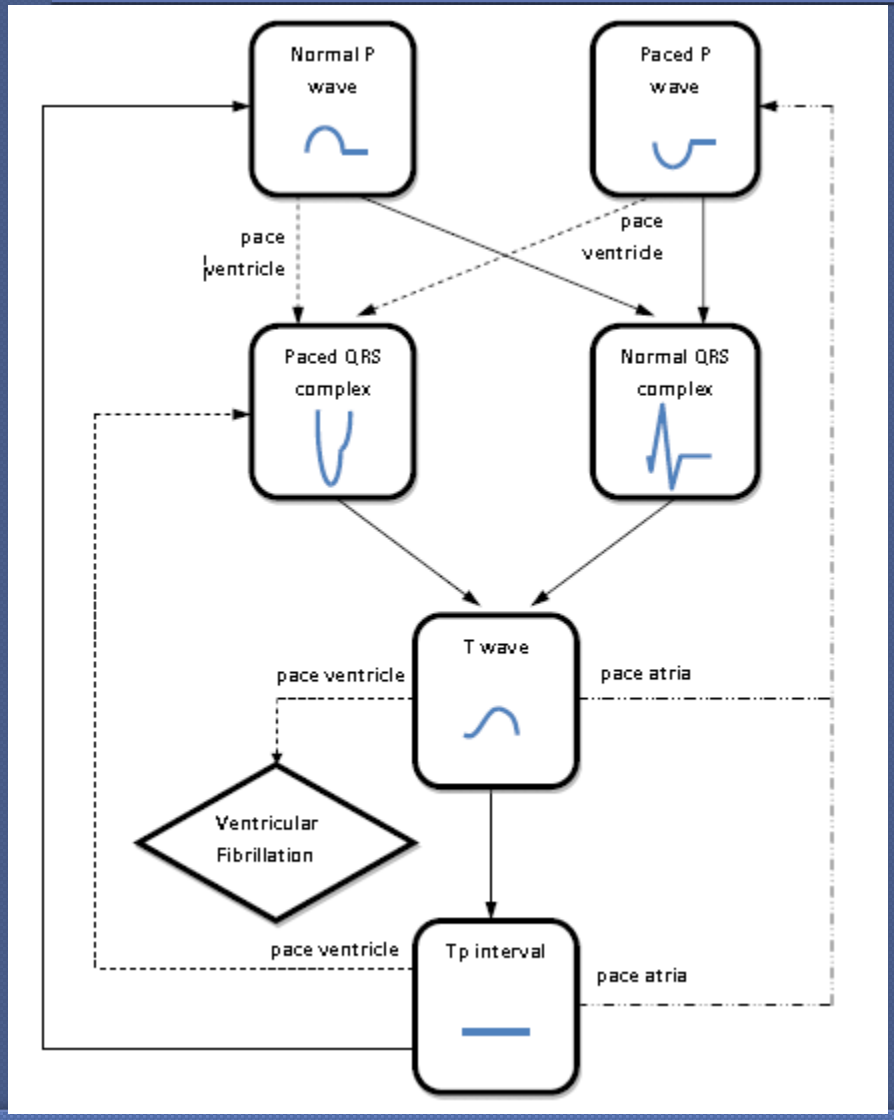
Fault Tolerance: Pulse Generator

Timing:

Timing circuits are redundant – series of counters that update the status of the state machine



Fault Tolerance: Pulse Generator



Pacing:

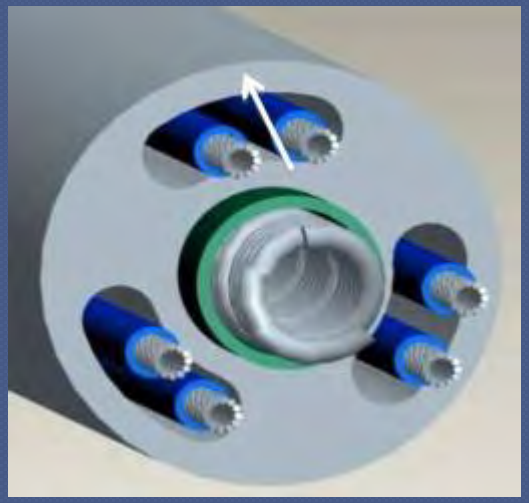
Dependent on input signals and control algorithms

"Shut-off" – non-committed state

Fault Tolerance: Leads

Traditionally an unreliable component – oxidation, oversensing, insulation breakdown

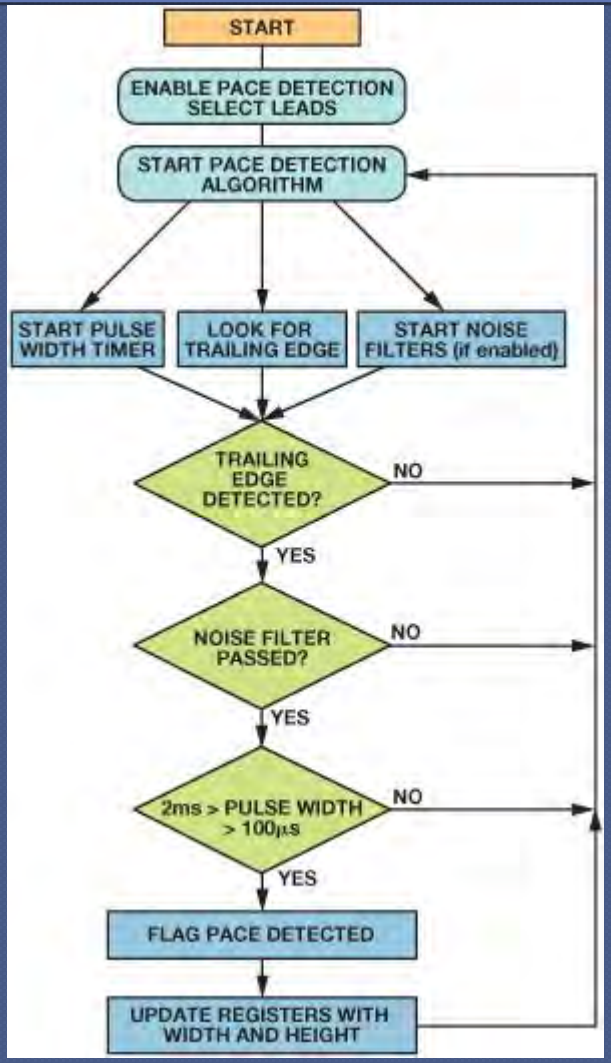
85% reliable for 5 years
72% reliable for 8 years



Riata coaxial lead

Riata lead failure analysis (2011)
25.7% leads with insulation defects
51.2% leads with abraded coating
Resulted in inappropriate shocks to 29.5% of the patients

Fault Tolerance: Software



Control algorithms:

Overlap timing cycles
Checkpointing – "safe" state
Error detection and restore

Additional Factors Affecting Reliability

Biological:
Infection
Rejection
Chemistry

Environment:
Radiation
Trauma

Human Error:
Placement
Monitoring
Patient Mngt.

Drug Interaction:
Blockers
Anti-arrhythmia

Product Lifespans and Warranty Insights

Stephen Emery

The Problem of Product Lifespans

- Factors that make it difficult to estimate product lifespan include:
  - Material variability
  - Customer usage
  - Usage conditions and environment
  - Innovative designs and materials

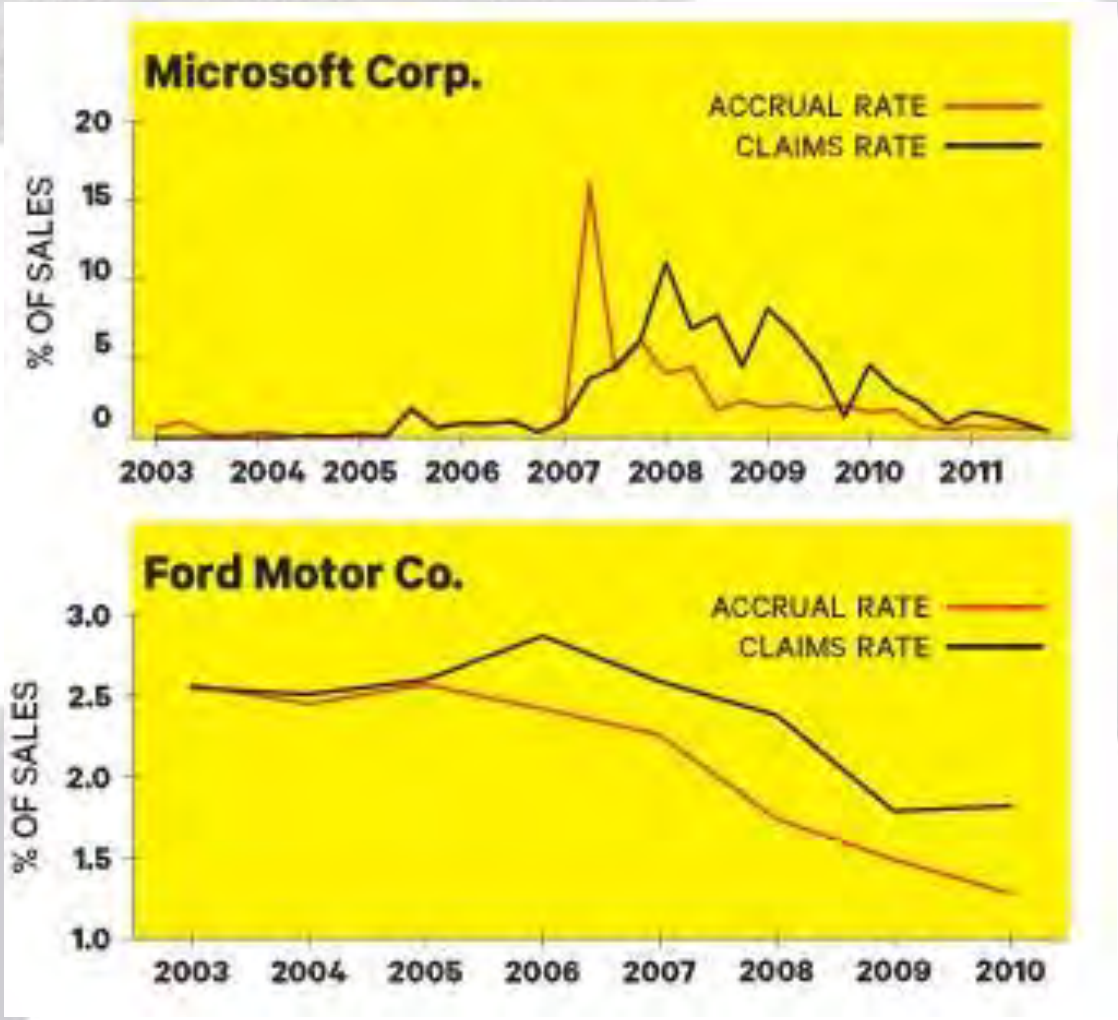
Over-Engineering

- Over-engineering makes products expensive and inefficient
- The amount of over-engineering that can be tolerated depends on the application
  - Aircraft
  - Racing Bicycles
- As over-engineering decreases, risk increases

The Warranty Market

- Companies don't like to talk about how much they send on warranties
- Since 2002, the SEC has required companies to report their warranty accrual and payment rates in their quarterly and yearly filings.
- Eric Arnum sorted through these documents and published the results on his website, *Warranty Week*.
- Basic warranties cost US manufacturers $24.7 Billion in 2011, and extended warranties resulted in and addition $30.2 Billion in payments

Ford Explorer vs. Xbox 360



Product Lifespan

- Specifying Minimum Lifespan
  - Ford guarantees all parts for 3 years and engines and transmissions for 6 years, so they design for 10 years.
- Determining Lifespan:
  - What is 10 years of use?
  - A test-to-failure yields one data point, and thousands are required to be statistically accurate.
  - These tests are prohibitively expensive

What I've Learned

- A study was conducted to ascertain the common factors associated with those that were highly successful NASA personnel (civil service rating)
- Correlation studies (how much did this factor contribute to career success) resulted in numerous factors
- Almost all of the factors of career success were expected, factors like years of experience, level of education, etc.
- One factor was orders of magnitude more important than all of the rest

Number of daily hours spent on the job, e.g., came in early/left late