# Reliability, Redundancy, and Resiliency

- Review of probability theory

- Component reliability

- Confidence

- Redundancy

- Reliability diagrams

- Intercorrelated Failures

- System resiliency

- Resiliency in fixed fleets

UNIVERSITY OF
MARYLAND

**Reliability, Redundancy, and Resiliency**
**ENAE 791 - Launch and Entry Vehicle Design**

# Review of Probability

- Probability that A occurs

$$0 \leq P(A) \leq 1$$

- Probability that A does not occur

$$P(\overline{A})$$

- Sum of all probable outcomes

$$P(A) + P(\overline{A}) = 1$$

# Review of Probability

- Probability of both A and B occurring

$$P(A) \cap P(B) = P(A)P(B)$$

- Probability of either A or B occurring
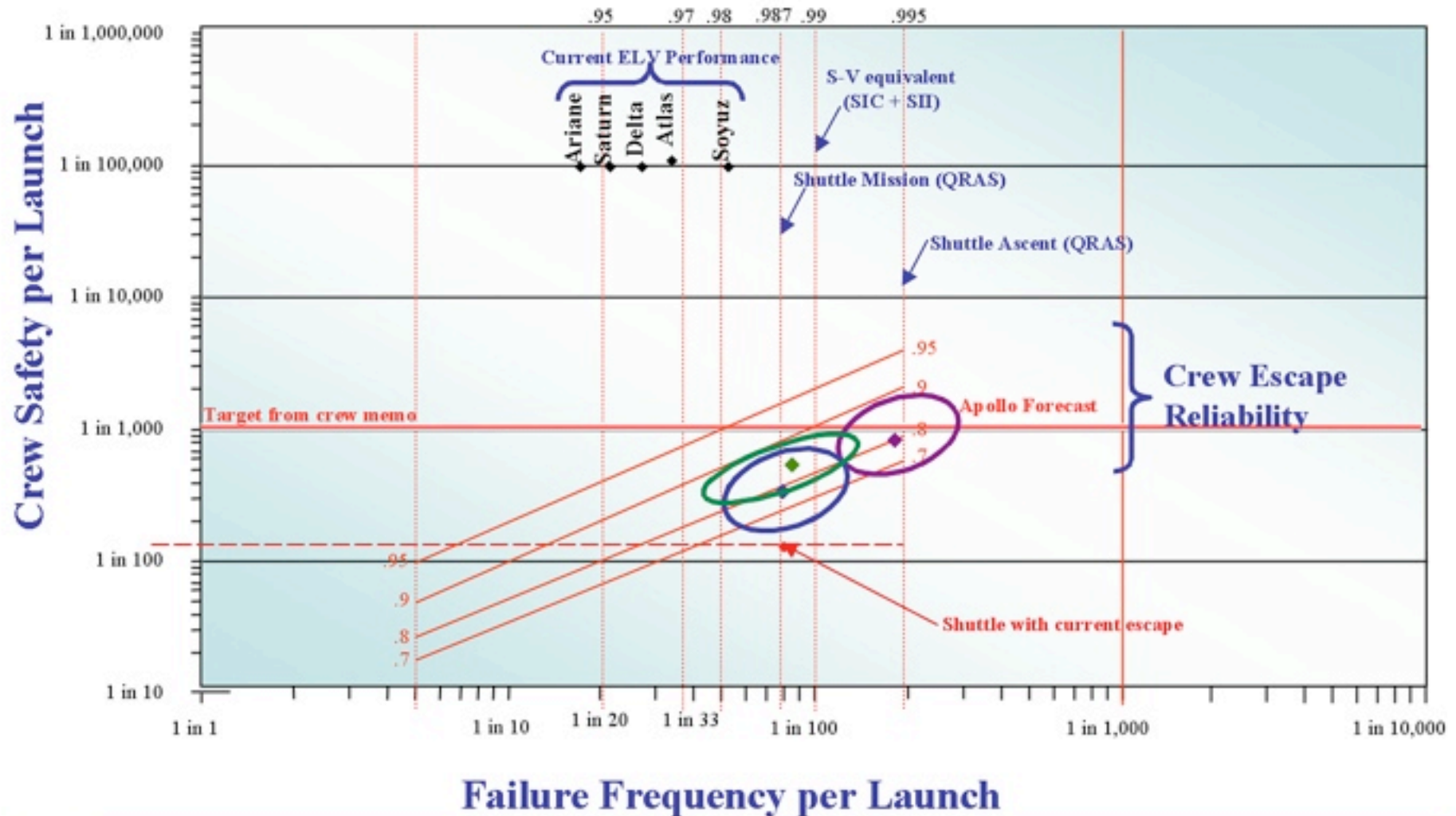
$$P(A) \cup P(B) = 1 - P(\overline{A})P(\overline{B})$$
$$= 1 - [1 - P(A)][1 - P(B)]$$
$$= P(A) + P(B) - P(A)P(B)$$

**Reliability, Redundancy, and Resiliency**
**ENAE 791 - Launch and Entry Vehicle Design**

# Baseline Results

## Results in the reliability / safety space



**Failure Frequency per Launch**

# Simple Overview of Abort Reliability

$$P_{survival} = P_{launch} \cup P_{abort}$$

$$P_{survival} = 1 - \left( \bar{P}_{launch} \cap \bar{P}_{abort} \right)$$

$$P_{survival} = 1 - \left[ (1 - P_{launch})(1 - P_{abort}) \right]$$

$$P_{abort} = 1 - \frac{1 - P_{survival}}{1 - P_{launch}}$$

$$P_{survival} = 0.999; \ P_{launch} = 0.97$$

$$P_{abort} = 1 - \frac{1 - 0.999}{1 - 0.97} = 0.9667$$

# Expected Value Theory

- Probability of an outcome does not determine value of the outcome

- Combine probabilities and values to determine expected value of outcome

$$EV = P(A)U(A) + P(\overline{A})U(\overline{A})$$

UNIVERSITY OF
MARYLAND

**Reliability, Redundancy, and Resiliency**
**ENAE 791 - Launch and Entry Vehicle Design**

# Expected Value Example

- Maryland State Lottery - pick six numbers out of 49 (any order)

$$P(win) = 1 \Big/ \frac{49!}{6!43!} = 1/13,983,816$$

- Assume $10,000,000 jackpot

$$EV = (7.151 \times 10^{-8})(10^7) + (1)(-1) = -\$0.39$$

# Utility Theory

- Numerical rating from expected value calculations does not fully quantify utility

- Lottery example previously: utility of (highly unlikely) win exceeds negative utility of small investment: *risk proverse*

- Imagine lottery where $1000 buys 1:500 chance at $1M -
  $$EV=(.998)(-\$1000)+(.002)(\$.999M)=\$1000$$
  *risk adverse*

# Component Reliability

Burn-in
Failures

Operating
Failures

End-of-life
Failures
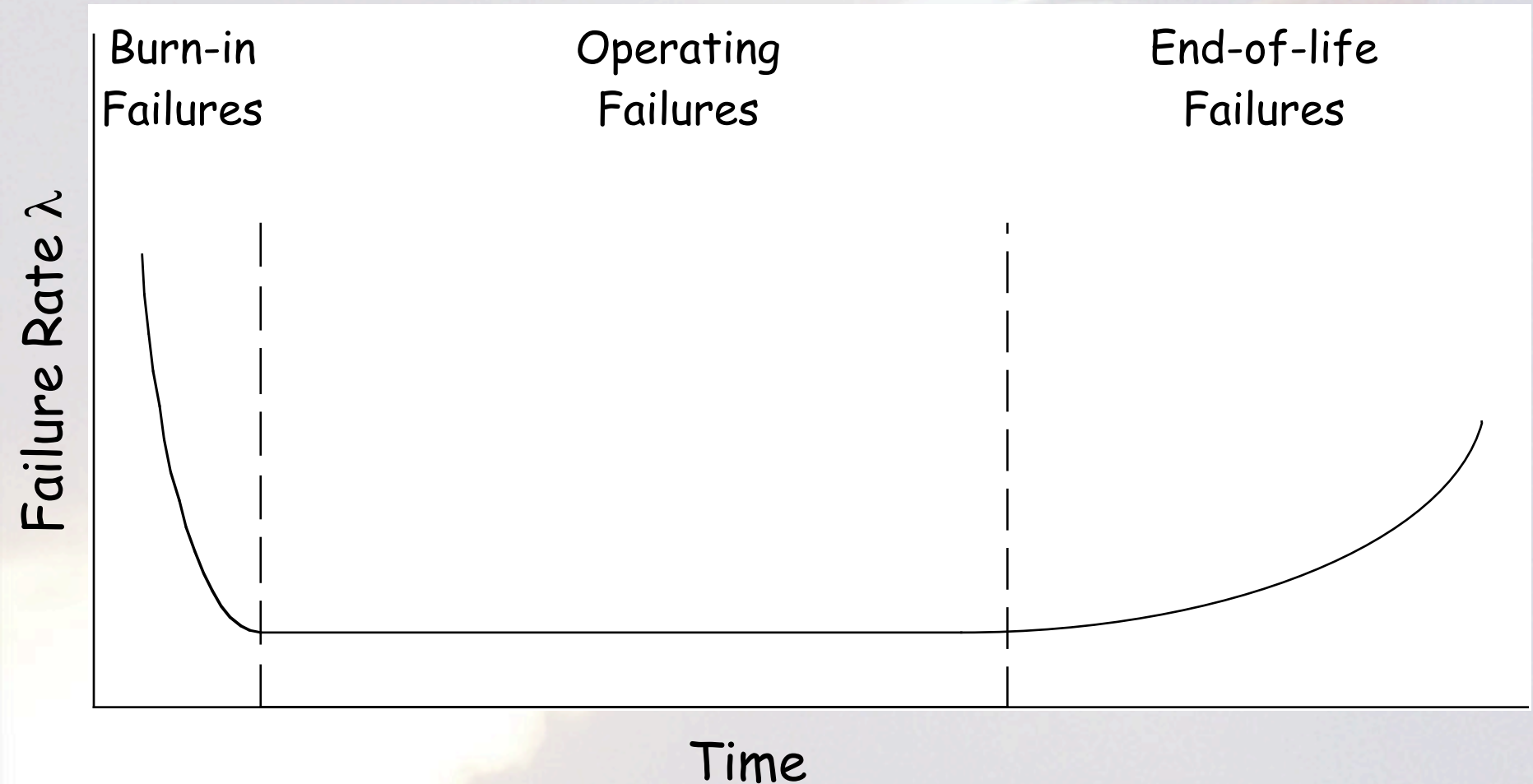
Failure Rate λ

Time

# Reliability Analysis

- Failure rate is defined as fraction of currently operating units failing per unit time

$$\lambda(t) = -\frac{1}{R(t)}\frac{d}{dt}R(t)$$

- The trend of operating units with time is then

$$\int_0^t \lambda(\tau)\,d\tau = -\int_1^{R(t)} \frac{dR(\tau)}{R(\tau)}$$

# Reliability Analysis (continued)

- Evaluation of the definite integrals gives

$$\int_0^t \lambda(\tau)\, d\tau = -\ln\left[R(t)\right]$$

- Assuming that $\lambda$ is constant over the operating lifetime,

$$R(t) = \exp\left[-\int_0^t \lambda(\tau)d\tau\right] = e^{-\lambda t}$$

- At $t = 1/\lambda$, $1/e$ of the original units are still operating (defined as mean time between failures)

# Reliability Analysis (continued)

- Frequently assess component reliability based on reciprocal of failure rate $\lambda$ :

$$R(t) = e^{-\frac{t}{MTBF}}$$

where MTBF=mean time between failures

- For a mission duration of N hours, estimate of component reliability becomes

$$R(mission) = e^{-\frac{N}{MTBF}}$$

UNIVERSITY OF
MARYLAND

**Reliability, Redundancy, and Resiliency**
**ENAE 791 - Launch and Entry Vehicle Design**

# Verifying a Reliability Estimate

- Given a unit reliability of R, what is the probability P of testing it 20 times without a failure?

- What is the probability Q that you will see one or more failures?

  – R=.99  -  P=.8179  -  Q=.1821

  – R=.95  -  P=.3584  -  Q=.6416

  – R=.90  -  P=.1216  -  Q=.8784

# Confidence

- The confidence C in a test result is equal to the probability that you should have seen worse results than you did
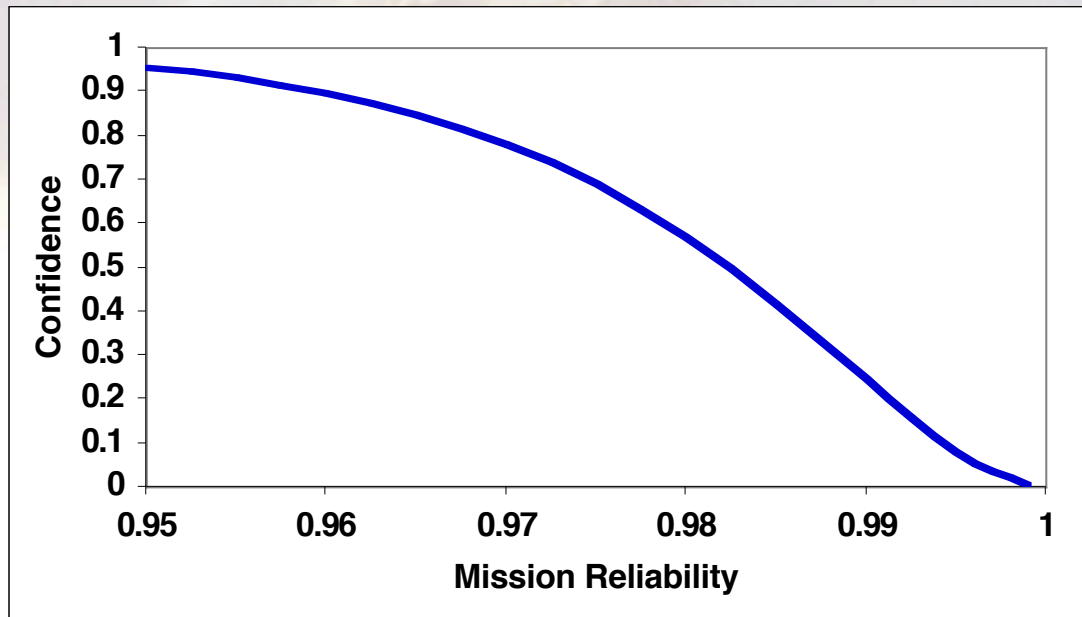
  P(observed and better outcomes) + C = 1

# Example of Confidence

- 100 vehicle flights with 1 failure

- Assume a reliability value of R

$$R^{100} + 100R^{99}(1 - R) + C = 1$$

- Trade off reliability with confidence values

UNIVERSITY OF
MARYLAND

**Reliability, Redundancy, and Resiliency**
**ENAE 791 - Launch and Entry Vehicle Design**

# Definition of Redundancy

- Probability of k out of n units working = (number of combinations of k out of n) x P(k units work) x P(n-k units fail)

$$P\binom{k}{n} = \frac{n!}{k!(n-k)!}P^k(1-P)^{n-k}$$

# Redundancy Example

3 parallel computers, each has reliability of 95%:

- Probability all three work

$$P(3) = P^3 = (.95)^3 = .8574$$

- Probability exactly two work

$$P(2) = 3P^2(1 - P) = 3(.95)^2(.05) = .1354$$

- Probability exactly one works

$$P(1) = 3P(1 - P)^2 = 3(.95)(.05)^2 = .0071$$

- Probability that none work

$$P(0) = (1 - P)^3 = (.05)^3 = .0001$$

# Redundancy Example

3 parallel computers, each has reliability of 95%:

- Probability all three work

$$P(3) = .8574$$

- Probability at least two work

$$P(3) + P(2) = .8574 + .1354 = .9928$$

- Probability at least one works
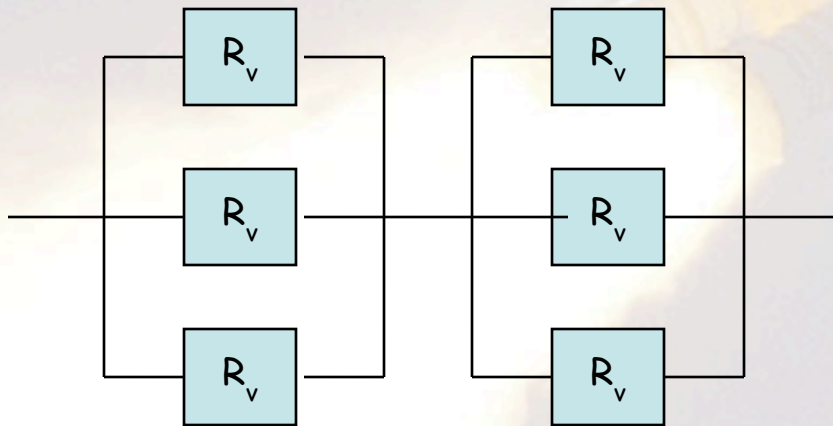
$$P(3) + P(2) + P(1) = .9928 + .0071 = .9999$$

- Probability that none work

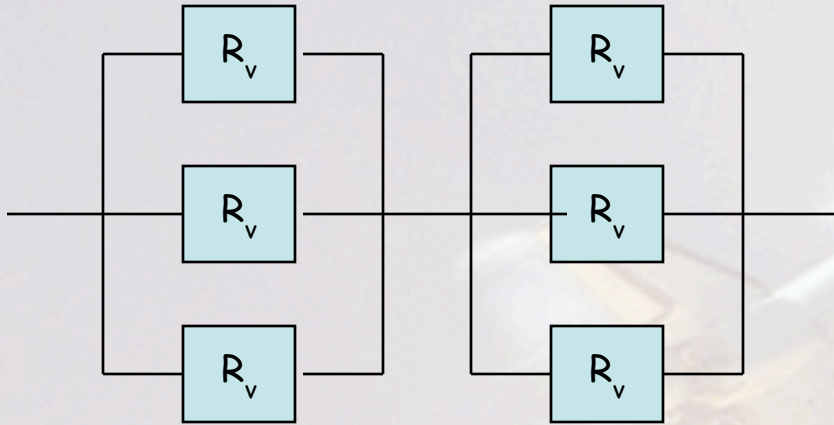$$P(0) = (1 - P)^3 = (.05)^3 = .0001$$

# Reliability Diagrams

- Example of Apollo Lunar Module ascent engine

- Three valves in each of oxidizer and fuel lines

- One in each set of three must work

- $R_v=0.9 \rightarrow R_{system}=.998$

$$R_{system} = \left[1 - (1 - R_v)^3\right]^2$$

# Reliability Diagrams (how not to…)

$$R_{system} = \left[ 1 - (1 - R_v)^3 \right]^2$$

$R_v = 0.9 \rightarrow R_{system} = .998$

$$R_{system} = \left[ 1 - (1 - R_v^2)^3 \right]$$
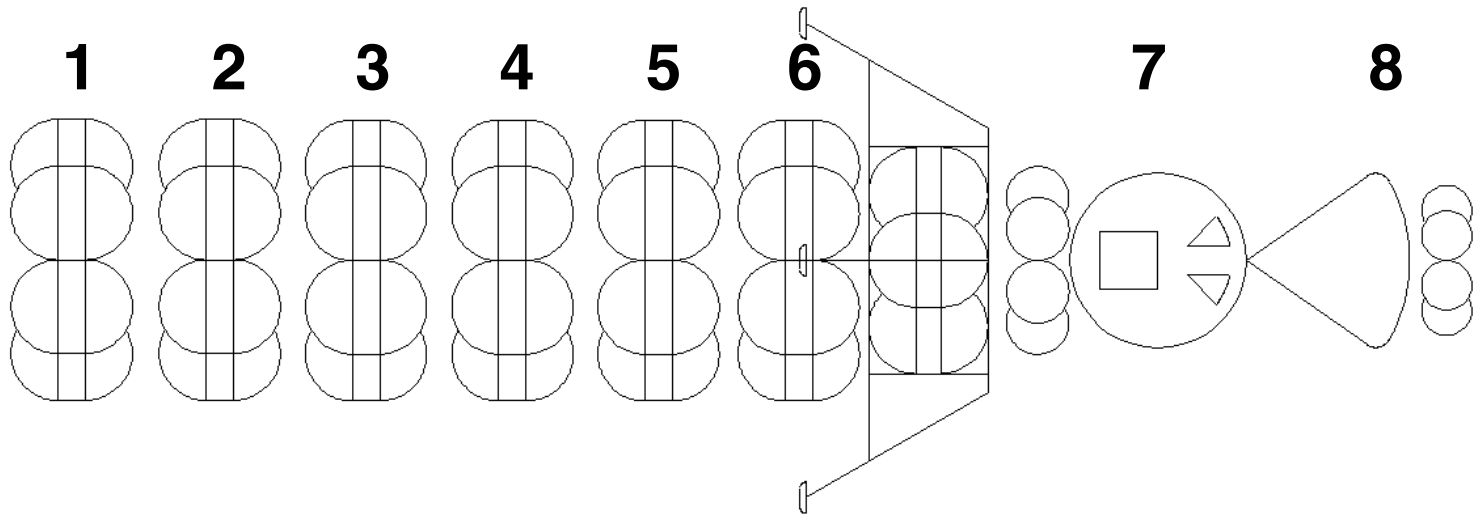
$R_v = 0.9 \rightarrow R_{system} = .993$

UNIVERSITY OF MARYLAND

**Reliability, Redundancy, and Resiliency**
**ENAE 791 - Launch and Entry Vehicle Design**

# Earth Departure Configuration

**8 launches and 7 dockings required to start mission**



**Assume $P_{launch}=0.97$ and $P_{dock}=0.99$**

$P_{no\ failures}= P_{launch}^8 P_{dock}^7 = 0.73$

$P_{all\ boost\ modules}= P_{launch}^6 P_{dock}^5 = 0.792$

$P_{all\ boost\ modules}= P_{no\ failures} + P_{1\ failure} =$

$0.792+6(1-P_{launch})P_{launch}^6 P_{dock}^5 = 0.792+0.143 = 0.935$

# Spares - The Big Picture

- **Have to get 6 functional boost modules for each of 10 missions**

- **Have to get functional lunar vehicle and crew module for each mission**

- **Assume composite reliability =0.97(0.99)=0.96**
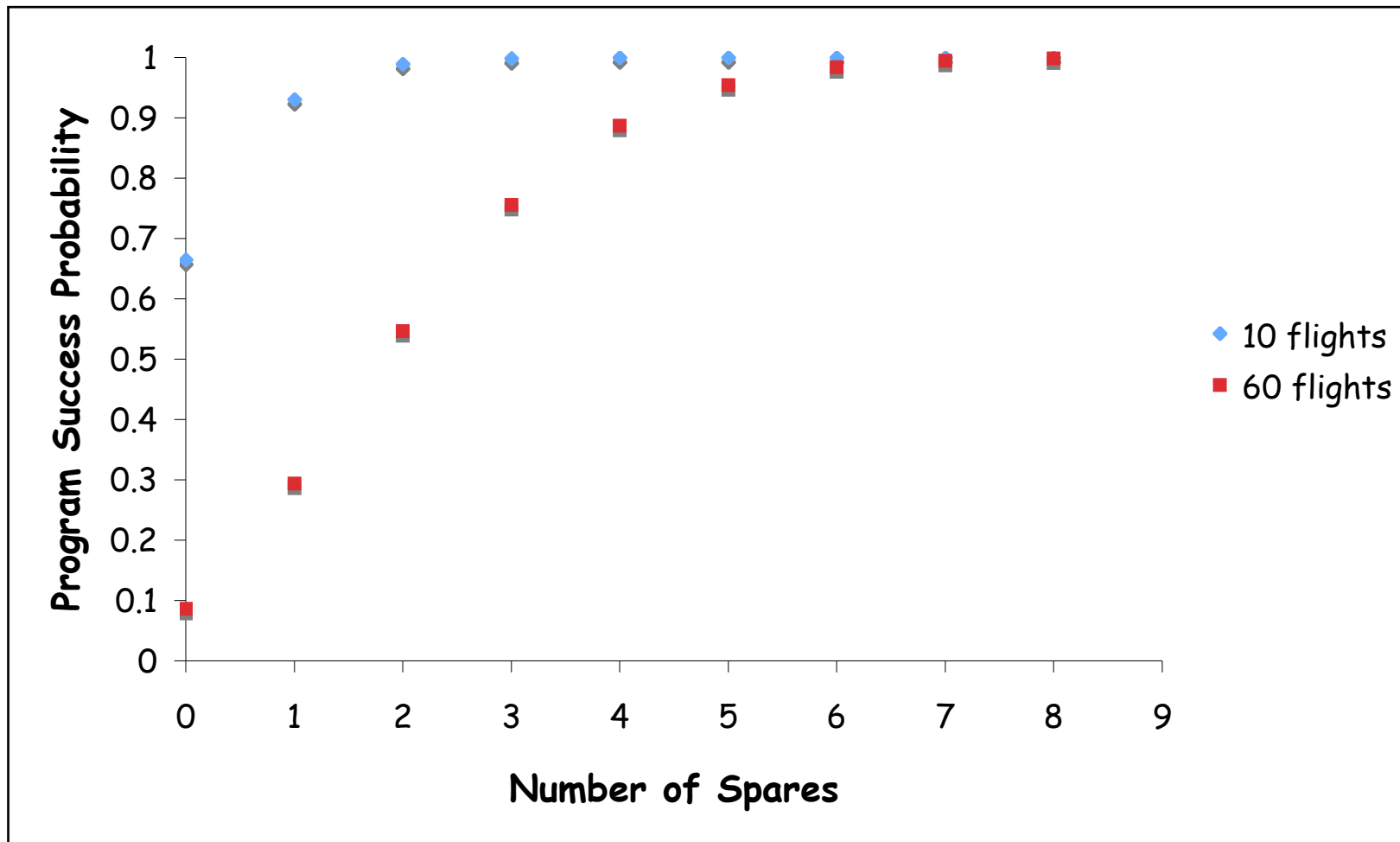
$$P(n \mid n) = p^n$$

$$P(n \mid n+1) = n(p^{n-1})(1-p)(p)$$

$$P(n \mid n+2) = \frac{n(n-1)}{2}(p^{n-2})(1-p)^2(p)$$

$$P(n \mid n+m) = \frac{n!}{(n-m)!m!}(p^{n-m})(1-p)^m(p)$$

**Space Systems Laboratory – University of Maryland**

# Effect of Fleet Spares on Program

# Spares Strategy Selection

- **VSE approach:**
  - **2 launches and 1 dock: $P=(0.97)^2(0.99)=0.931$**
  - **Program reliability over 10 missions: $0.931^{10}=0.492$**

- **Goal: meet VSE program reliability**
  - **1 lander and 1 CEV spare - p=0.9308 each**
  - **2 boost module spares - p=0.5464**
  - **Program reliability: $(0.9308)^2(0.5464)=0.473$**

- **Alternate goal: 85% program reliability**
  - **2 lander, 2 CEV, 4 BM spares: $(0.9893)^2(0.8871)=0.868$**
  - **1 lander, 1 CEV, 6 BM spares: $(0.9308)^2(0.9838)=0.852$**

# Intercorrelated Failures

- Some failures in redundant systems are common to all units

  - Software failures

  - "Daisy-chain" failures

  - Design defects

- Following a failure, there is a probability f that the failure causes a total system failure

UNIVERSITY OF
MARYLAND

**Reliability, Redundancy, and Resiliency**
**ENAE 791 - Launch and Entry Vehicle Design**

# Intercorrelated Failure Example

3 parallel computers, each has reliability of 95%, and a 30% intercorrelated failure rate:

- Probability all three work

$$P(3) = P^3 = (.95)^3 = .8574$$

- Probability exactly two work (one failure)

$$P(2) = 3P^2(1 - P) = 3(.95)^2(.05) = .1354$$

  – Probability the failure is benign (system works)

  $$P\left(2_{safely}\right) = .7(.1354) = .0948$$

  – Probability of intercorrelated failure (system dies)

  $$P\left(2_{system\ failure}\right) = .3(.1354) = .0406$$

# Intercorrelated Failure Example

(continued from previous slide)

- Probability exactly one works (2 failures)

$$P(1) = 3P(1 - P)^2 = 3(.95)(.05)^2 = .0071$$

 – Probability that both failures are benign

$$P\left(1_{safely}\right) = .7^2(.0071) = .0035$$

 – Probability that a failure is intercorrelated

$$P\left(1_{system\ failure}\right) = \left(1 - .7^2\right)(.0071) = .0036$$

# Redundancy Example with Intercorrelation

3 parallel computers, each has reliability of 95%, and a 30% intercorrelated failure rate:

- Probability all three work

$$P(3) = .8574$$

- Probability at least two work
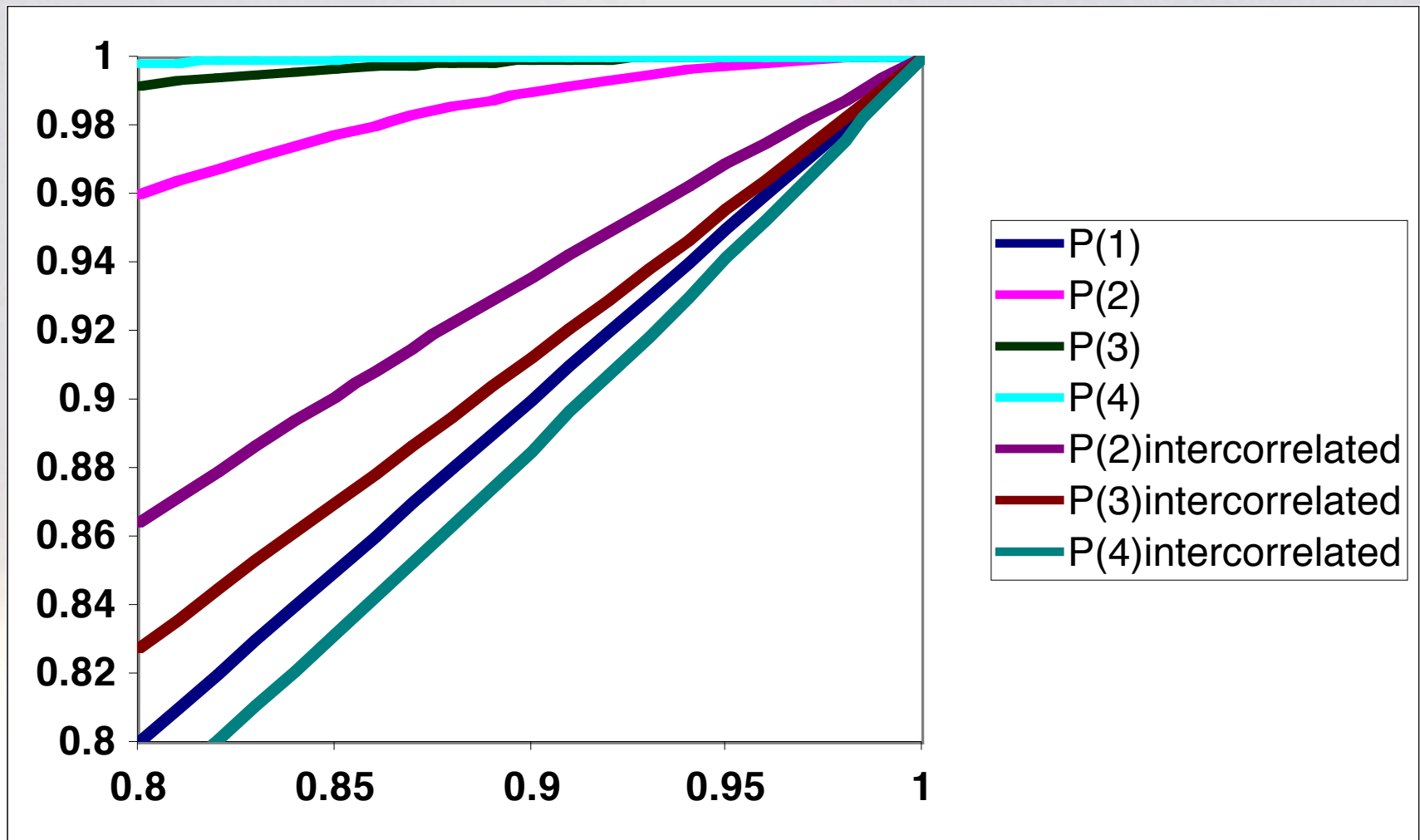
$$= .8574 + .0948 = .9522 \quad (was\ .9928)$$

- Probability at least one works

$$= .9522 + .0035 = .9557 \quad (was\ .9999)$$

# System Reliability with 30% Intercorrelation

# Probabilistic Risk Assessment

- Identification and delineation of the combinations of events that, if they occur, could lead to an accident (or other undesired event)

- Estimation of the chance of occurrence for each combination

- Estimation of the consequences associated with each combination.
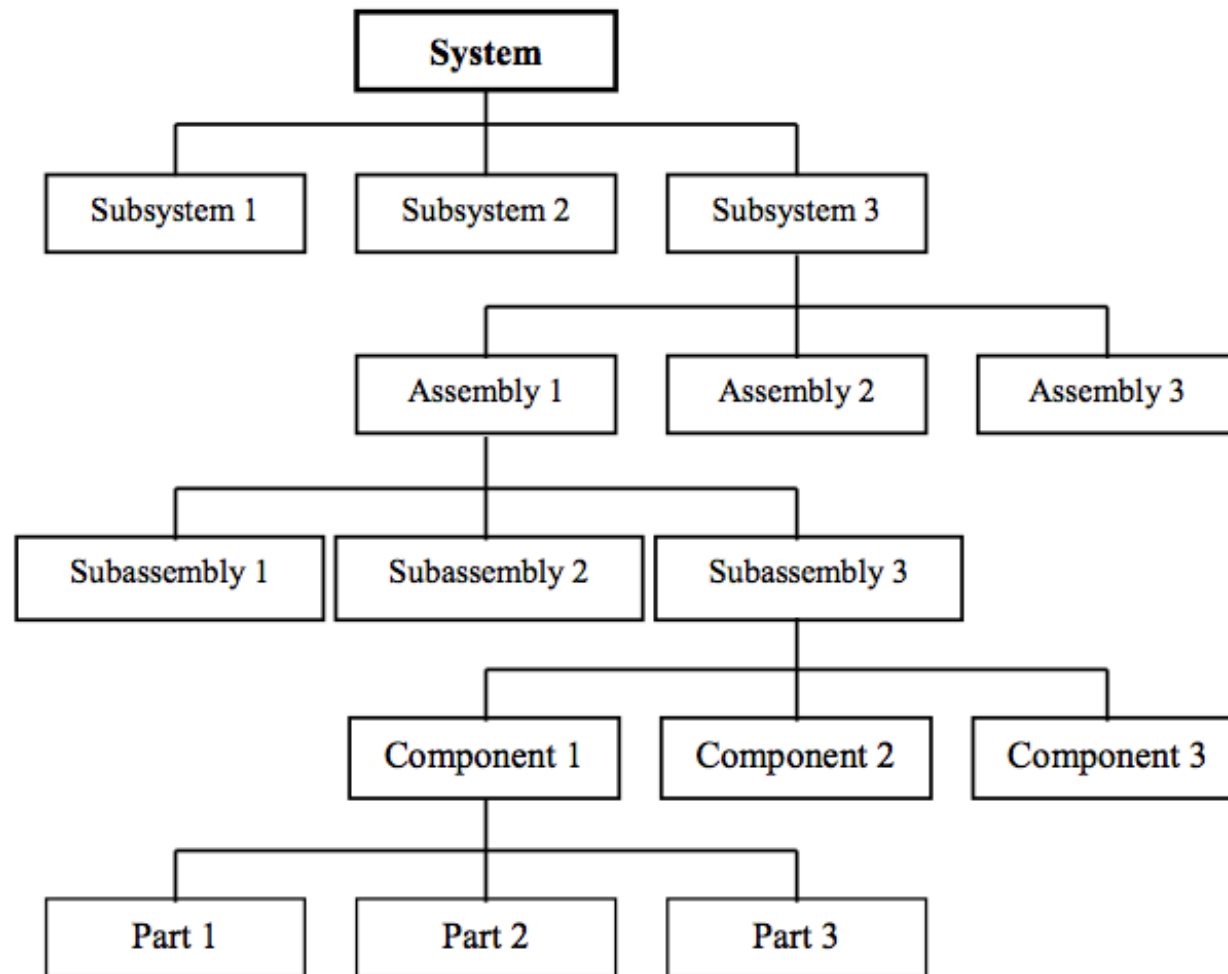
# PRA Process Flowchart
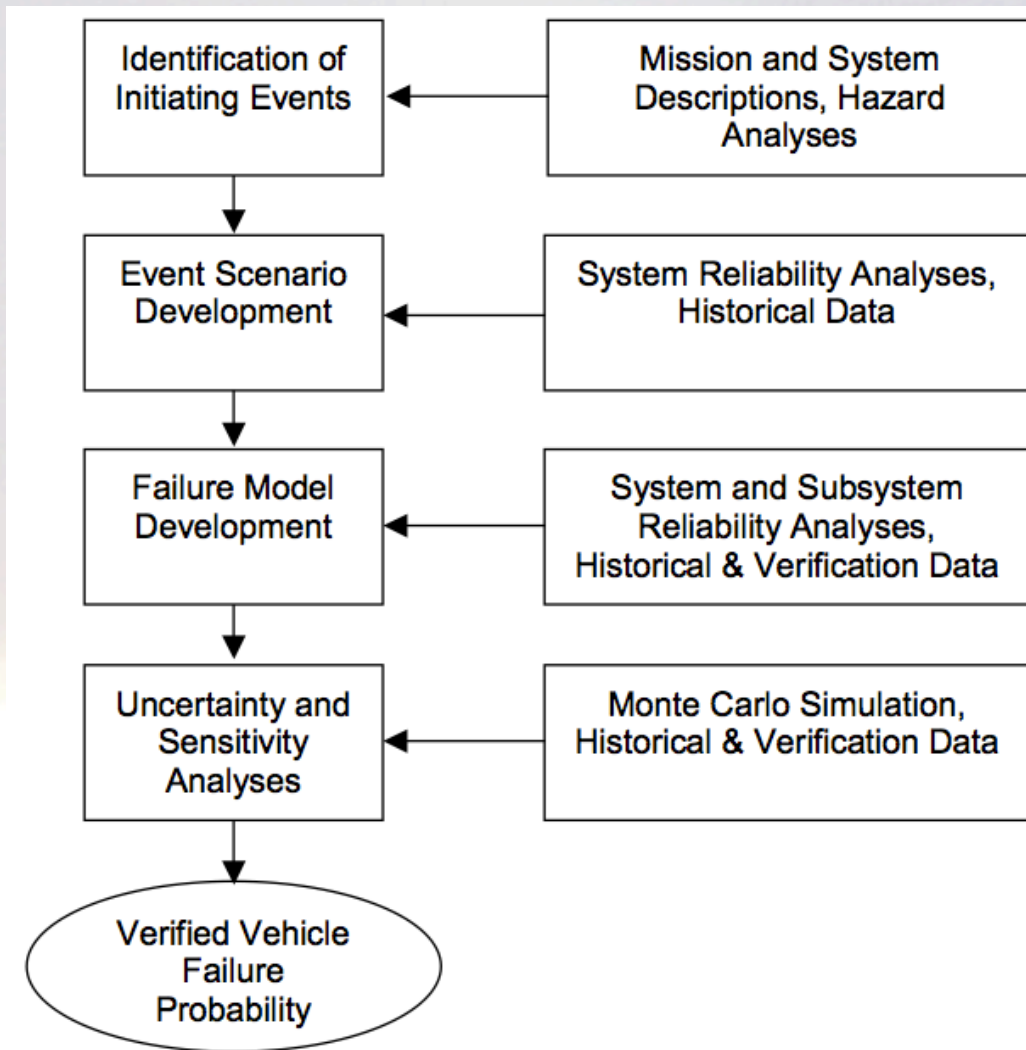


FAA, "Guide to Reusable Launch and Reentry Vehicle Reliability Analysis" April 2005

Reliability, Redundancy, and Resiliency
ENAE 791 - Launch and Entry Vehicle Design

# System Breakdown Chart



FAA, "Guide to Reusable Launch and Reentry Vehicle Reliability Analysis" April 2005

# Failure Modes and Effects Analysis

**FAILURE MODES, EFFECTS, AND CRITICALITY ANALYSIS WORKSHEET**

System: Upper Stage Propulsion System

Mission: Satellite Delivery to GEO

Phase: Orbital Insertion

Ref. Drawing: GTYD-1002B008

Sheet 1 of 20

Prepared by: John Smith

Reviewed by: Janet Jones

Approved by: Sharon Jackson

Date: January 2, 2004

| ID | Item | Failure Modes | Failure Causes | Failure Effects | Risk Assessment | | | Detection Methods and Controls |
|----|------|---------------|----------------|-----------------|------|------|------|--------------------------------|
| | | | | | Sev. | Prob. | Risk | |
| 2.0 | Combustion Chamber | a. Coolant loss<br>b. Seal failure | a. Manufact. process problem<br>b. Cyclic fatigue | a. Reduced performance, burn-through, possible crash and injury to involved public<br>b. Reduced performance | a.II<br>b.III | a.C<br>b.D | a.6<br>b.14 | a. Inspect welds<br>b. Seal redundancy |

FAA, "Guide to Reusable Launch and Reentry Vehicle Reliability Analysis" April 2005
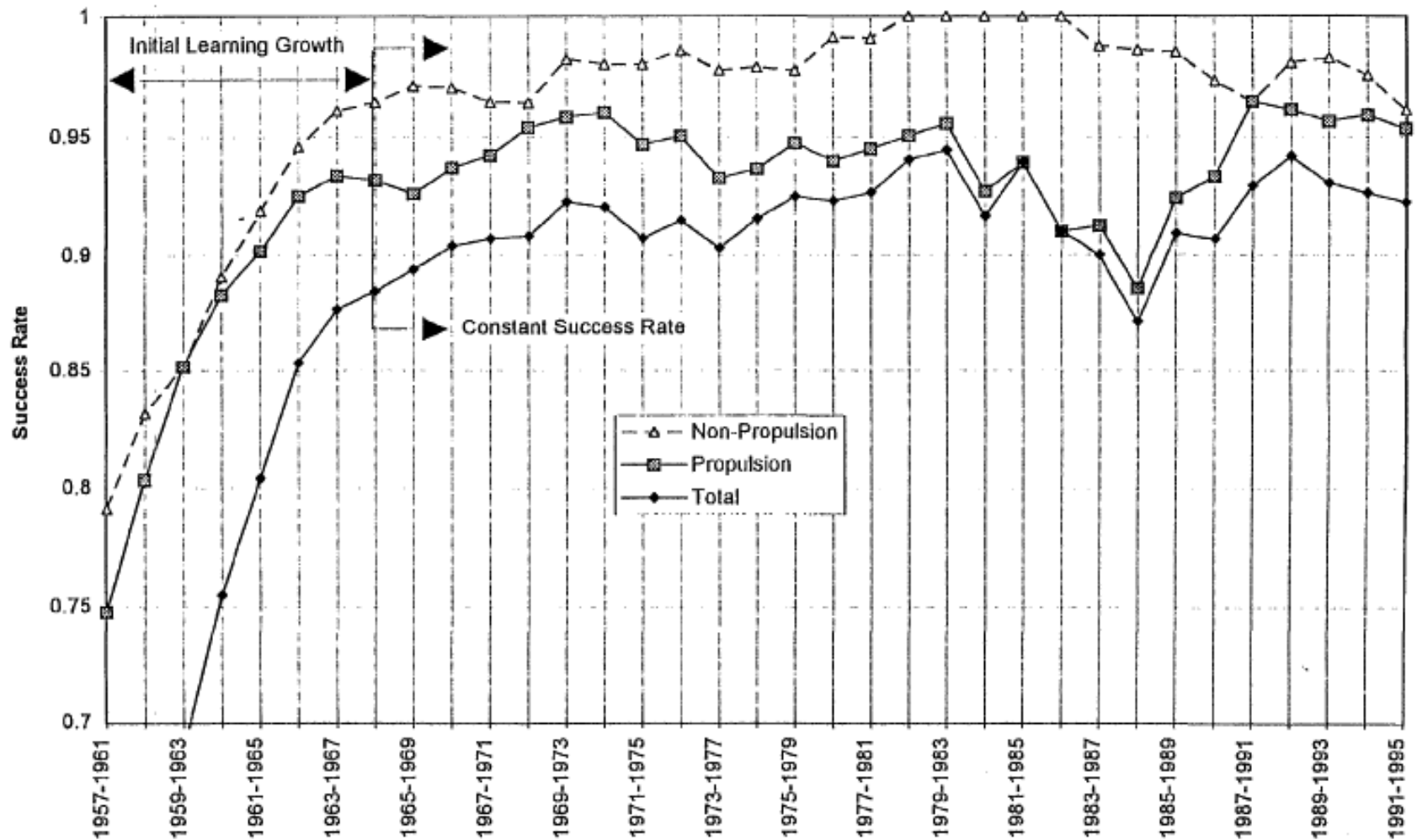
# Fault Tree Analysis
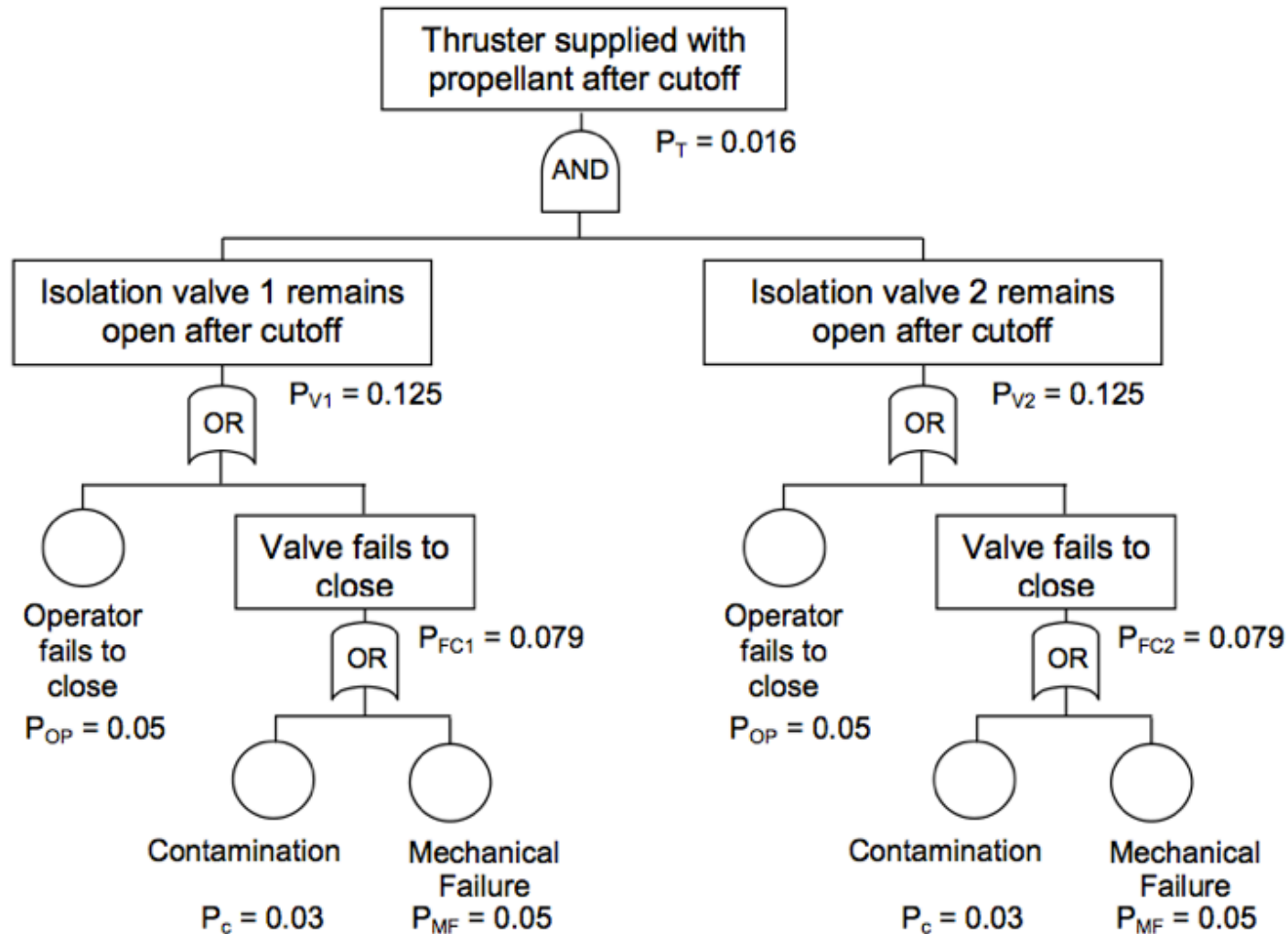
UNIVERSITY OF
MARYLAND

**Reliability, Redundancy, and Resiliency**
**ENAE 791 - Launch and Entry Vehicle Design**

# U.S. Launch Reliability - 5 yr. rolling avgs.



A. G. Allred and D. R. Sauvageau, "Crew Survival and Intact
Abort using Solid Rocket Boosters" AIAA 96-3156, July, 1996

UNIVERSITY OF
MARYLAND

**Reliability, Redundancy, and Resiliency**
**ENAE 791 - Launch and Entry Vehicle Design**

# LV Subsystem Failures 1984-2004

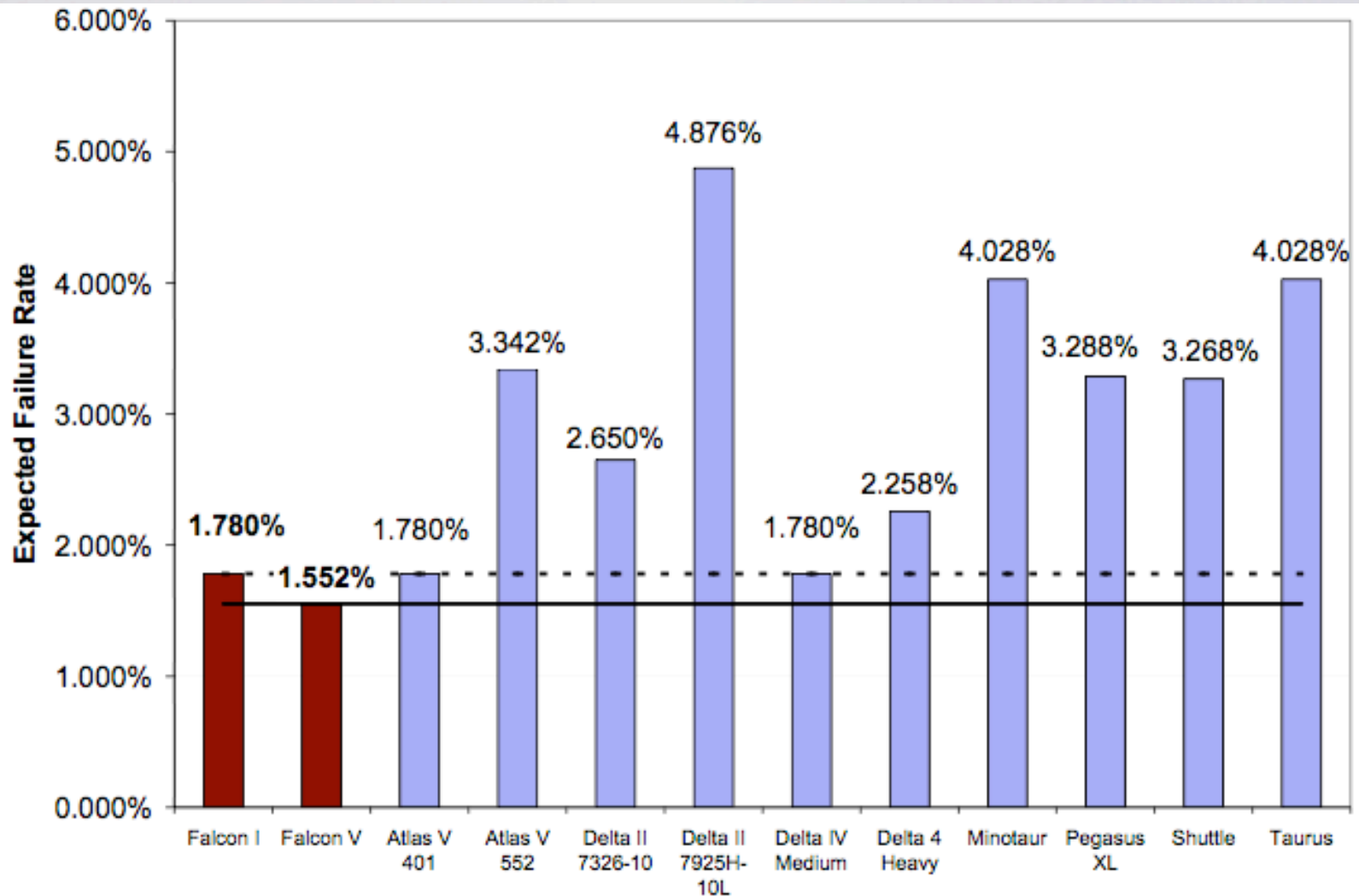| Failure Type | Failures | Total Events | Individual Percent Failure Rate |
|---|---|---|---|
| Liquid Propulsion (Start) | 3 | 1255 | 0.239% |
| Liquid Propulsion (In-flight) | 3 | 1255 | 0.239% |
| **Total Liquid Failure** | **6** | **1255** | **0.478%** |
| Solid Propulsion (Shell) | 4 | 1831 (all solids) | 0.218% |
| Solid Propulsion (TVC) | 3 | 571 (TVC only) | 0.525% |
| **Solid Propulsion with TVC (TVC and Shell Failure Modes)** | -- | -- | **0.743%** |
| Stage, Booster, and Payload Separations | 6 | 2577 | 0.233% |
| Fairing Separation | 1 | 357 | 0.280% |
| Small Solid Booster Separations | 1* | 1165 | 0.086% |
| Electrical | 2 | 470 | 0.426% |
| Avionics | 2 | 470 | 0.426% |
| Other | 1 | 470 | 0.213% |

*Did not result in total mission loss.

Futron Corporation, "Design Reliability Comparison for SpaceX Falcon Vehicles" Nov. 2004

UNIVERSITY OF MARYLAND

**Reliability, Redundancy, and Resiliency**
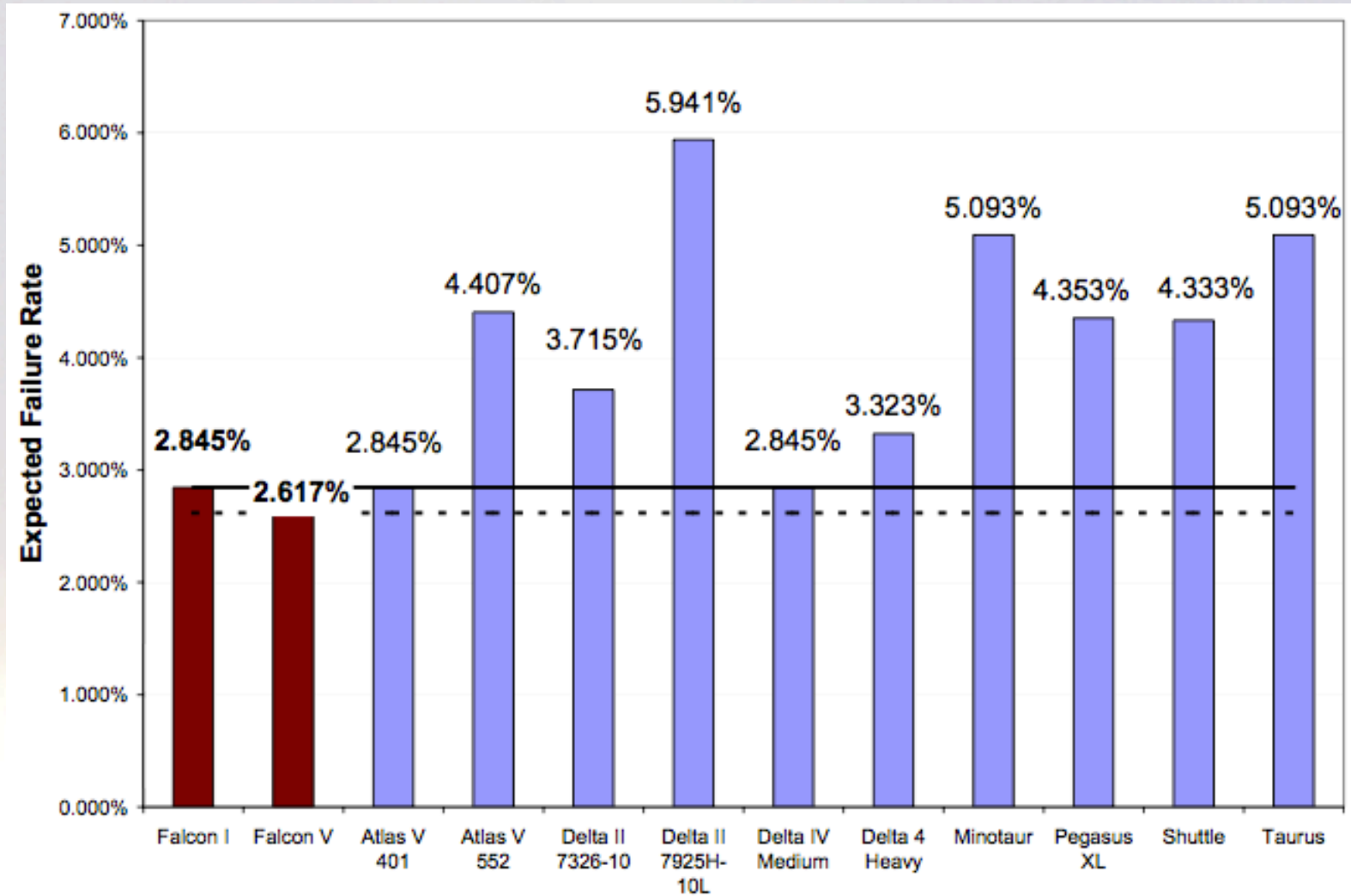**ENAE 791 - Launch and Entry Vehicle Design**

# Expected Failure Rates from Prop/Sep



Futron Corporation, "Design Reliability Comparison for SpaceX Falcon Vehicles" Nov. 2004

UNIVERSITY OF
MARYLAND

**Reliability, Redundancy, and Resiliency**
**ENAE 791 - Launch and Entry Vehicle Design**

# Failure Rates from All Causes



Futron Corporation, "Design Reliability Comparison for SpaceX Falcon Vehicles" Nov. 2004

UNIVERSITY OF
MARYLAND

**Reliability, Redundancy, and Resiliency**
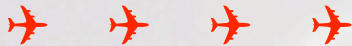**ENAE 791 - Launch and Entry Vehicle Design**

# Concept of System Resiliency

- Initial flight schedule

  ✈ ✈ ✈ ✈ ✈ ✈ ✈ ✈ ✈ ✈ ✈

- Hiatus period following a failure

  ✈ ✠ ✈ ✈ ✈ ✈ ✈

- Backlog of payloads not flown in hiatus

  ✈ ✈ ✈ ✈

- Surge to fly off backlog

  ✈ ✠ ✈✈ ✈✈ ✈✈ ✈✈ ✈

- Resilient if backlog is cleared before next failure occurs (on average)

# Resiliency Variables

r - nominal flight rate, flts/yr

d - down time following failure (yrs)

k - fraction of flights in backlog retained

S - surge flight rate/nominal flight rate

m - average/expected flights between failures

rd - number of missed flights

krd - number of flights in backlog

(S-1)r - backlog flight rate

# Definition of Resiliency

$$\frac{Srkd}{S-1} \leq m$$

- Example for Delta launch vehicle

- r = 12 flts/yr

- d = 0.5 yrs

- k = 0.8

- S = 1.5

- m = 30

- Srkd/(S-1) = 14.4 < 30 - system is resilient!

# Shuttle Resiliency (post-*Challenger*)

r = 9 flts/yr

d = 2.5 yrs

k = 0.8

S = .67 (6 flts/yr)

m = 25

✓ System has negative surge capacity due to reduction

in fleet size - cannot **ever** recover from hiatus without more extreme measures

# Modified Resiliency

k' - retention rate of all future payloads
(k'≤S for S<1)

- New governing equation for resiliency:

$$\frac{Srk'd}{S - k'} \leq m$$

- Implication for shuttle case:
- ✓ k<.417 to achieve modified resiliency

UNIVERSITY OF
MARYLAND

# Shuttle Resiliency (post-*Columbia*)

- r = 5 flts/yr

- d = 2 yrs

- S = .8 (4 flts/yr)

- m = 56 (average missions/failure)

- Modified resiliency requires k' ≤0.7 for all future payloads