

Reliability, Redundancy, and Resiliency

- Review of probability theory
- Component reliability
- Confidence
- Redundancy
- Reliability diagrams
- Intercorrelated Failures
- System resiliency
- Resiliency in fixed fleets



Review of Probability

- Probability that A occurs

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

- Probability that A does not occur

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

- Sum of all probable outcomes

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



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

$$P(A) \cup P(B) = 1 - P(\bar{A})P(\bar{B})$$

$$= 1 - [1 - P(A)][1 - P(B)]$$

$$= P(A) + P(B) - P(A)P(B)$$



Expected Value Theory

- Probability of an outcome does not determine value of the outcome
- Combine probabilities and values to determine expected value of outcome

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



Expected Value Example

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

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

- Assume \$10,000,000 jackpot

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

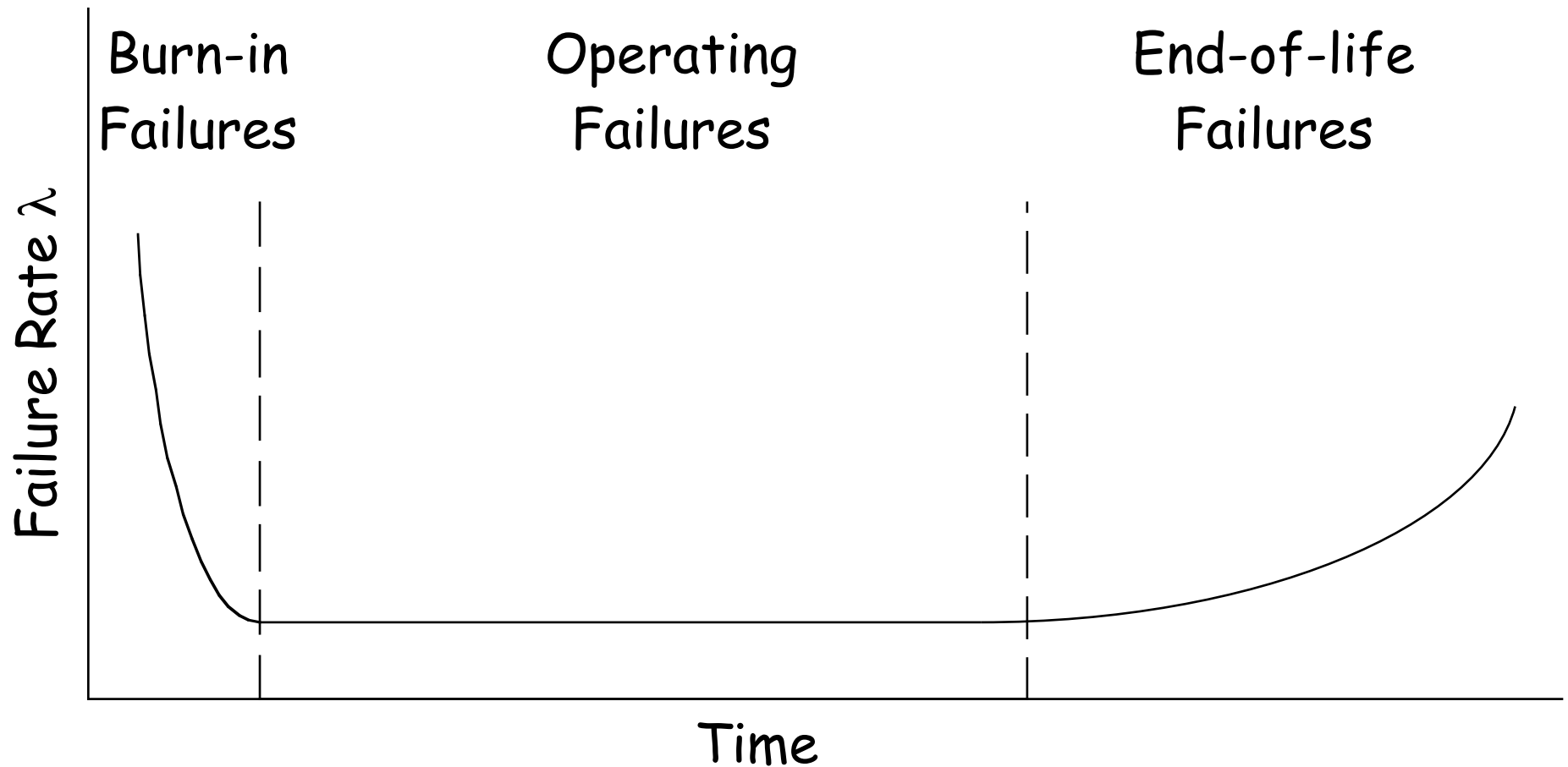


Utility Theory

- 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 -
$$EV = (.998)(-\$1000) + (.002)(\$999,000) = \$1000$$
risk adverse



Component Reliability



Component 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

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



Component Reliability Analysis (continued)

- Evaluation of the definite integrals gives

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

- Assuming that λ 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)



Component Reliability Analysis (continued)

- Frequently assess component reliability based on reciprocal of failure rate λ :

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

where MTBF=mean time between failures

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

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



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
- $P(\text{observed and better outcomes}) + C = 1$



Confidence Example - Saturn V

- NASA MSFC initially set requirement that Saturn V should demonstrate 95% reliability at 80% confidence prior to manned operations

$$0.95^n + 0.80 = 1 \implies n = 31.4$$

- NASA actually flew 13 Saturn Vs without a failure - actual reliability at 80% confidence was

$$R^{13} + 0.80 = 1 \implies R = 88.4\%$$



Example of Confidence - Space Shuttle

- 113 vehicle flights with 2 failures
- Assume a reliability value of R
- Confidence if no failures had occurred

$$R^{113} + C_0 = 1$$

- Confidence if one failure had occurred

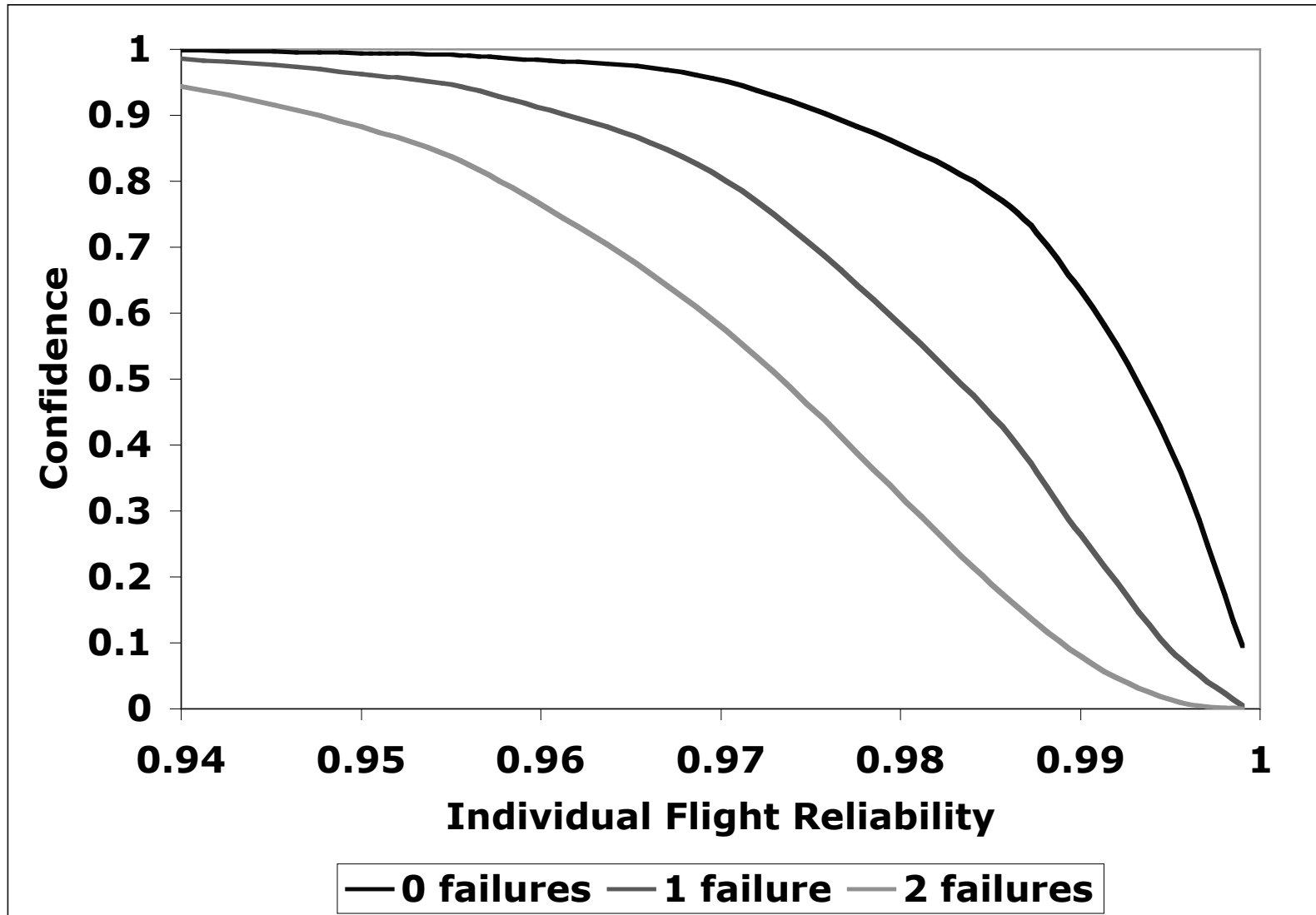
$$R^{113} + 113R^{112}(1 - R) + C_1 = 1$$

- Confidence if two failures occurred

$$R^{113} + 113R^{112}(1 - R) + \frac{(113)(112)}{2}R^{111}(1 - R)^2 + C_2 = 1$$



Shuttle Reliability and Confidence



Definition of Redundancy

- Probability of k out of n units working =
(number of permutations of k out of n) ×
 $P(k \text{ units work}) \times P(n-k \text{ units fail})$

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



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

$$P(3) + P(2) + P(1) = .9928 + .0071 = .9999$$

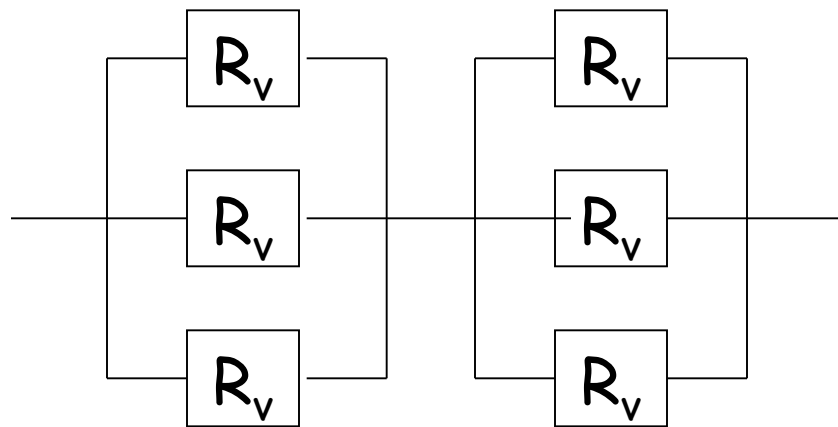
- Probability that none work

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



Reliability Diagrams

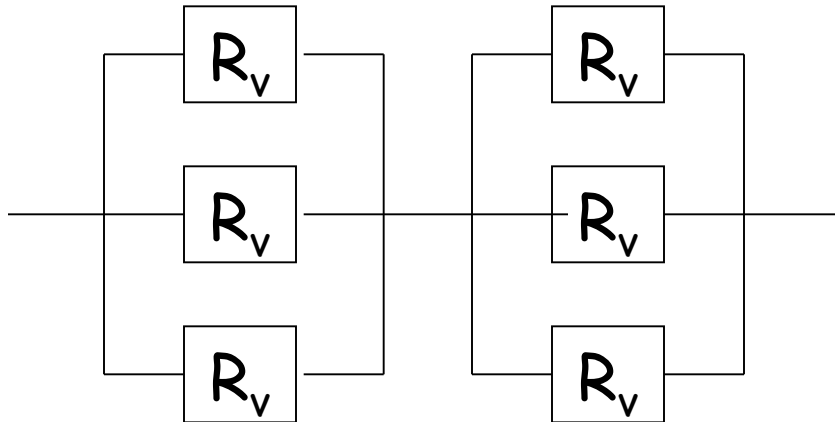
- Example of Apollo Lunar Module ascent engine
- Three valves in each of oxidizer and fuel lines
- One in each set of three must work
- $R_v=0.9 \rightarrow R_{system}=0.998$



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

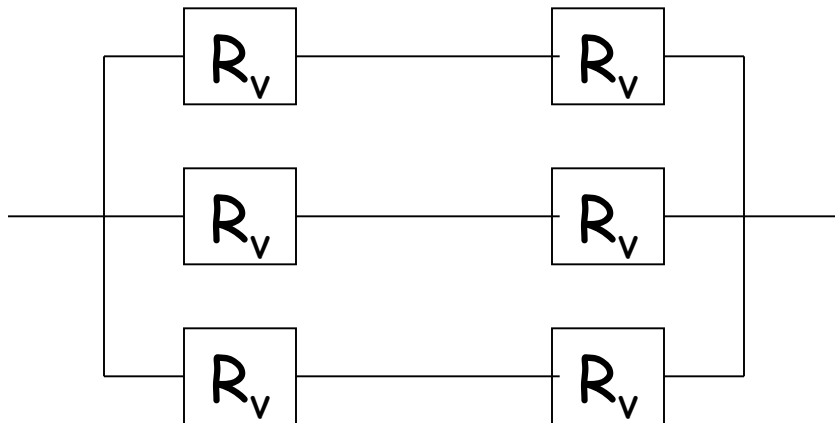


Reliability Diagrams (how not to...)



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

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



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

$$R_v = 0.9 \rightarrow R_{system} = .993$$



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



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)

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

- Probability of intercorrelated failure (system dies)

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



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

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

- Probability that a failure is intercorrelated

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



Redundancy Example with Intercorrelation

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

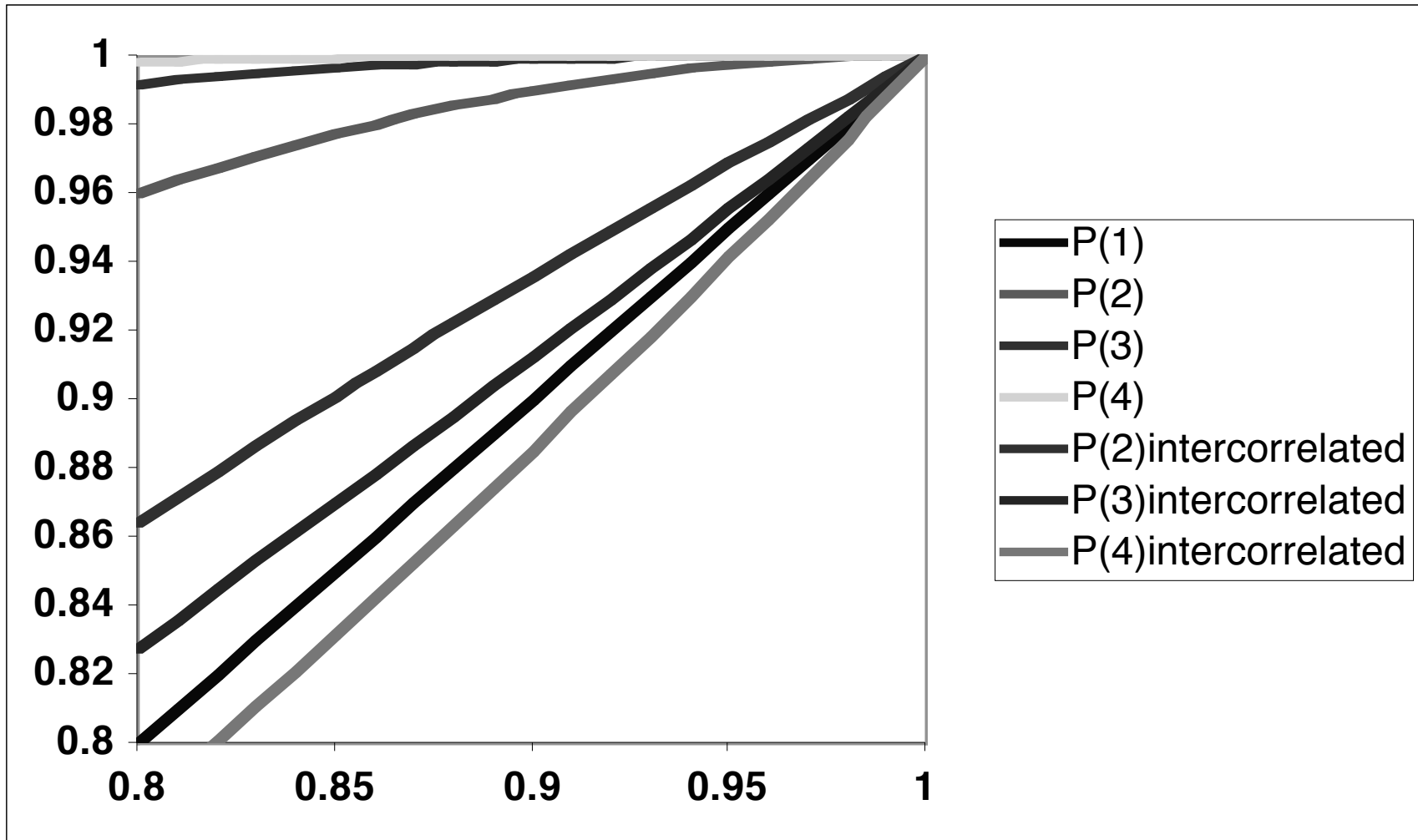
- Probability all three work

$$P(3) = .8574$$

- Probability at least two work
= $.8574 + .0948 = .9522$ (*was .9928*)
- Probability at least one works
= $.9522 + .0035 = .9557$ (*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.



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*)

$$r = 9 \text{ flts/yr}$$

$$d = 2.5 \text{ yrs}$$

$$k = 0.8$$

$$S = .67 \text{ (6 flts/yr)}$$

$$m = 25$$

➔ 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
($k' \leq S$ 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



Shuttle Resiliency (post-*Columbia*)

$$r = 5 \text{ flts/yr}$$

$$d = 2 \text{ yrs}$$

$$S = .8 \text{ (4 flts/yr)}$$

$$m = 56 \text{ (average missions/failure)}$$

➔ Modified resiliency requires $k' \leq 0.7$ for all future payloads

