The Mathematics of Reliability

Fred Baumgartner, CPBE, CBNT

Continuing Education

Webinars by SBE

ENNES EDUCATIONAL FOUNDATION TRUST

SBE University on-line. on-demand.

Society of Broadcast Engineers

www.sbe.org

SBE

St. Augustine

The good Christian should beware of mathematics and all those who make empty prophecies.
The danger already exists that the mathematicians have made a covenant with the devil to darken the spirit and to confine man to the bonds of hell.
– St. Augustine

YEAR = 365.25 Days = 8766 Hours = 525,960 Minutes

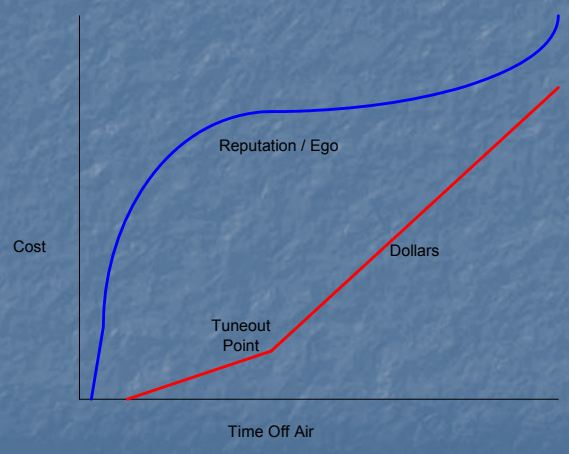
Reliability Is Measured In % Availability

Availability	9s	Non-availability	Days	Hours	Minutes
99%	2	1%	3.65	87.66	5259.6
99.9%	3	0.1%	.365	8.766	525.96
99.95%		0.05%	.182625	4.383	262.98
99.99%	4	0.01%	.0365	.8766	52.596
99.995%		0.005%	.0182625	.04383	26.298
99.999%	**5**	0.001%	.00365	.08766	**5.2596**
99.9995%		0.0005%	.0018265	.004383	2.6298
99.9999%	6	0.0001%	.000365	.008766	0.52596 (31 Seconds)

The Value of Availability is Fluid

- 30 Seconds of Super Bowl on Network = $2.4 Million
- 30 Seconds of 3:00 AM on an LPTV in Rice Lake =
  -$0.01

The Value of Availability is Fluid



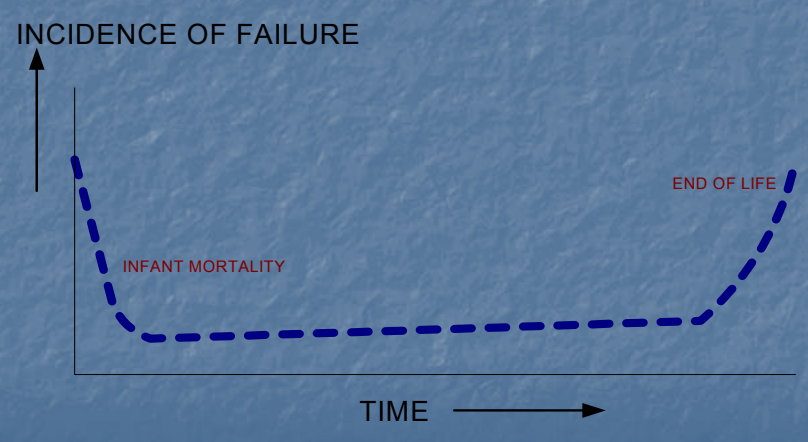
Availability is:

$$\frac{MTTR}{MTBF_{(+MTTR)}} \times 100 = \%\ Unavailability$$

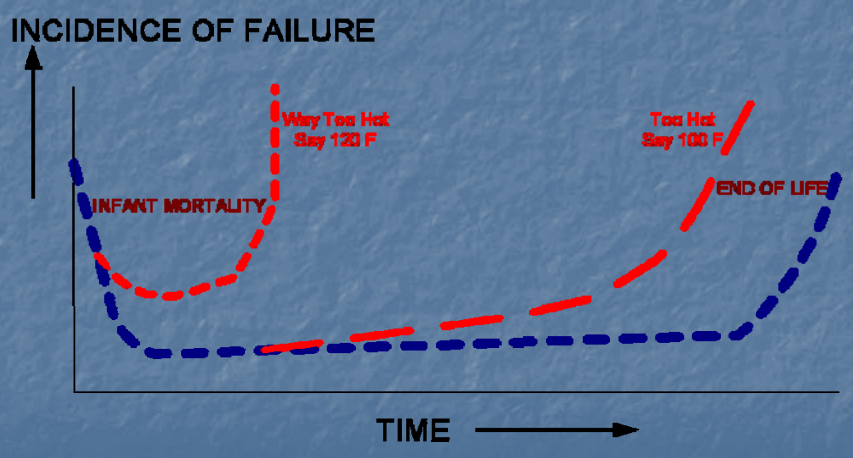
100 - % Unavailability = % Availability

Example: $\frac{1\ Hr\ MTTR}{100\ Hr\ MTBF}$ = 1% Unavail = 99% Avail

MTBF – The Bathtub Curve



MTBF – The Hot Bathtub



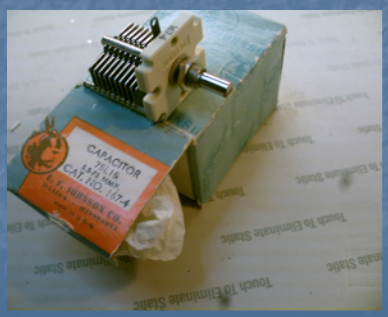
MTBF – Component Life at Temperature

2,000 Hour Useful Life at 85 C (185 F)

2,000 Hours is 83 Days

MTBF – Component Life with Time

Born 1922
Estimated Useful Life 18 Months
2005, 0.257 Volts into 10 MOhms



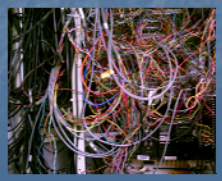
Born 1947
Estimate Useful Life = Unlimited
2005, 5.4-78 uF (5.5-75 uF rated)

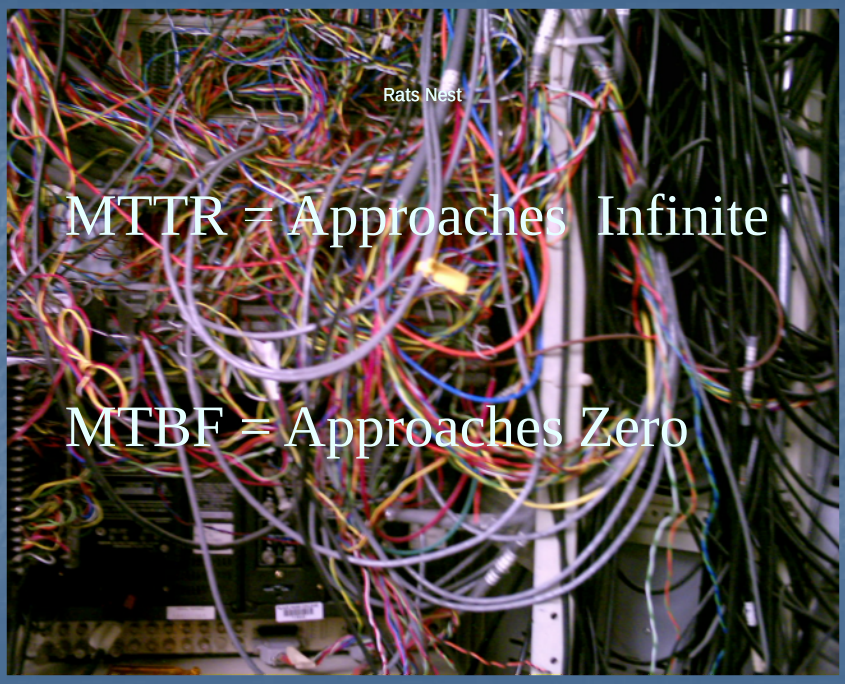
MTBF – Component Life, Who Knows?

Born, 2001
Estimated Life, Indefinite
Actual Life, 1 Year 3 Months
(400 Others did Better)
Stress, 40%
(8 Amps on 20 Amp Circuit)
Reason for failure:
Undetermined; I think 1 turn to few
Cost of failure: $50,000 +
MTTR ~ 30 Minutes

MTBF Summary

- Highly Dependent on Workmanship
- Everything is the sum of the component weaknesses – Heat is #1
- Stress moves the Bathtub Curve
- Stress is most often heat, but can be:
  - Moisture
  - Bio
  - Power Supply
  - NEVER UNDERESTIMATE HUMAN ERROR





MTTR

- ALWAYS more important than MTBF
- A ZERO MTTR makes any MTBF irrelevant.
- MTTR is 100% Architecture and Process

"We are ready for an unforeseen event that may or may not occur."

–Al Gore, VP

MTTR Factors

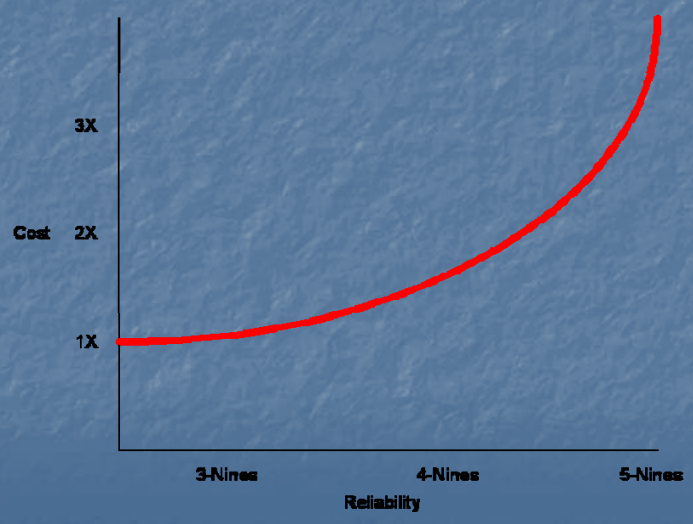
- Notification Time
- Access Time
- Diagnostic Time
- Replacement or Reroute Time
- Configuration Time

Nt + At + Dt + Rt + Ct = MTTR

MTTR Scenario Extremes

- Call in service
- Drive, Walk Time
- Diagnostic Time
  - Training
  - Experience
- Get Parts
  - Shelf or Ship
- Install
- Configure
  - Tools to auto config
- Switch to *useful* hot backup

Cost of Low MTTR



Estimating MTBF

- Power, Phone, Gas, Water… ~ 5,000 Hrs
- Things with Tubes and Motors ~ 10,000 – 25,000 Hrs
- Things with reasonable complexity ~ 50,000 Hrs
- Low power, simple things ~ 100,000 Hrs
- Passive components ~ 1,000,000 Hrs

Estimating MTTR

- Power, Phone, Gas, Water… ~ 5,000 Hrs
  - 5 Nines
- Things with Tubes and Motors ~ 10,000 – 25,000 Hrs
  - 4 Nines
- Things with reasonable complexity ~ 50,000 Hrs
  - 4-5 Nines
- Low power, simple things ~ 100,000 Hrs
  - 6-9 Nines
- Passive components ~ 1,000,000 Hrs
  - 9-10 Nines

Summary of MTTR and MTBF

- While MTBF is easier to comprehend, It's impact on availability is not paramount
- MTBF is about Genes and Lifestyle
- MTTR is a function of:
  - Process
  - Supplies
  - Staffing Access
  - Information (M&C)

Availability is:

$$\frac{\text{MTTR}}{\text{MTBF}} \times 100 = \%\ \text{Unavailability}$$

100 - % Unavailability = % Availability

Example: $\frac{\text{1 Hr MTTR}}{\text{100 Hr MTBF}}$ = 1% Unavail = 99% Avail

Availability Makes No Distinction

- Long but Rare
  - Usually what we think of
  - Some write these off as Acts of God
- Short and Often
  - Is a lost bit an outage?
  - Usually some threshold above:
    - Some BER
    - Loss of revenue
    - Perception

99.99% Reliability is

- 1 Day MTTR in 27.7 Years
- 52 Minutes off in a Year
- 1 Second Glitch Every 2.7 Hours

Reliability Is Measured In % Availability

Availability	9s	Non-availability	Days	Hours	Minutes
99%	2	1%	3.65	87.66	5259.6
99.9%	3	0.1%	.365	8.766	525.96
99.95%		0.05%	.182625	4.383	262.98
99.99%	4	0.01%	.0365	.8766	52.596
99.995%		0.005%	.0182625	.04383	26.298
99.999%	**5**	0.001%	.00365	.08766	**5.2596**
99.9995%		0.0005%	.0018265	.004383	2.6298
99.9999%	6	0.0001%	.000365	.008766	0.52596 (31 Seconds)

Requirements for High Availability

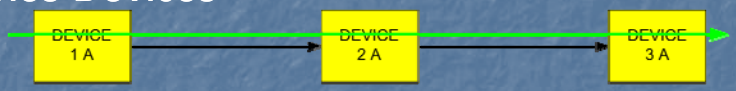
- Architecture
  - SPOF (Single Point of Failure) = Bad
  - Redundant Designs = Good
- Increase MTBF
  - Healthy Environment = Good
  - Preventive Maintenance = Good
  - EOL gear = Bad
- Reduce MTTR
  - Critical Spares on hand = Good
  - Repair services on hand = Good
  - Too few $ and available good techs = Bad

We can do this with this simple formula

Richard Hamming on the Right
Copyright McGill University 1948

Design – Architectural Options

Series Devices



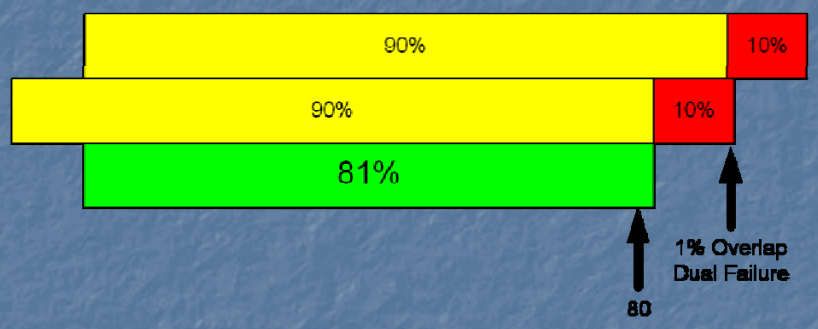
A x A x A... = Total Availability

99% x 99% x 99% (Availability)

.99 x .99 x .99 = .970299

Thus 97.03% Availability

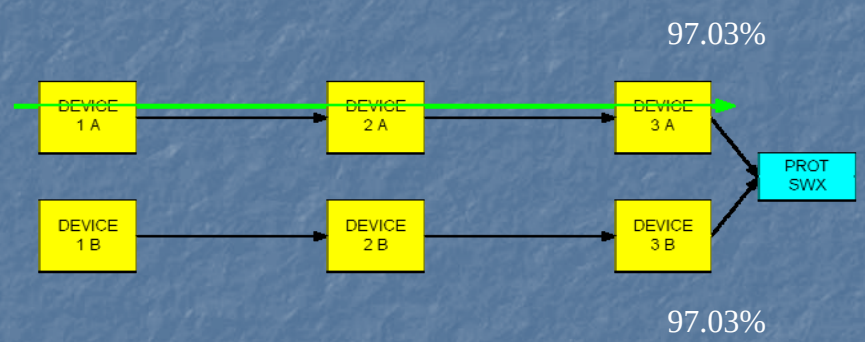
Series Paths – Venn Diagram



Two devices available 50% of the time

work together 25% of the time… not 0%

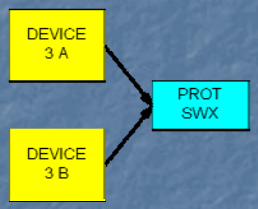
Dual Series Paths



Redundant Path Design

Parallel Devices

U x U... = Total Unavailability



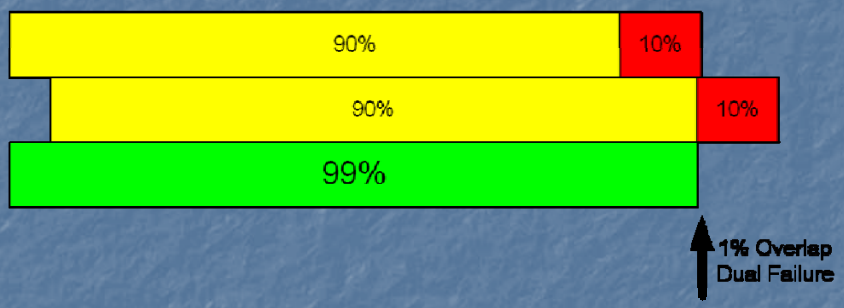
99% ‖ 99% = ? (Availability)

1% x 1% = .01% (Unavailability)

.01 x .01 = .0001

Thus 99.99% Availability

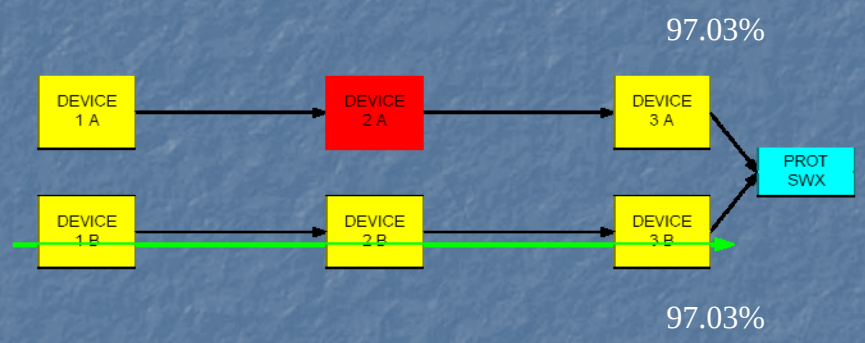
Parallel Paths -- Venn Diagram



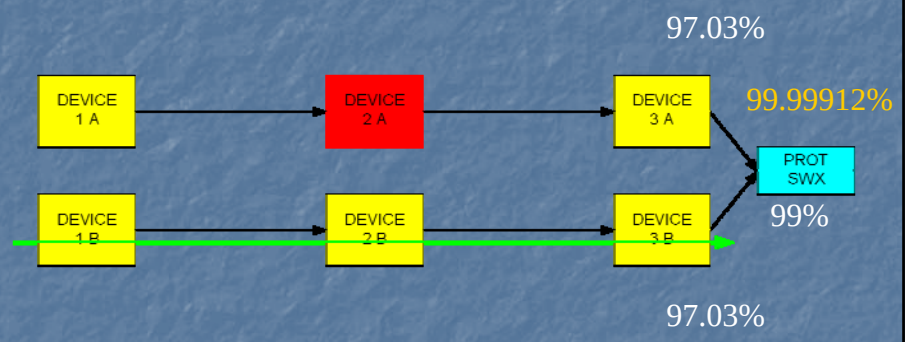
Two devices available 50% of the time

work together 75% of the time… not 100%

Failure To Redundant Path

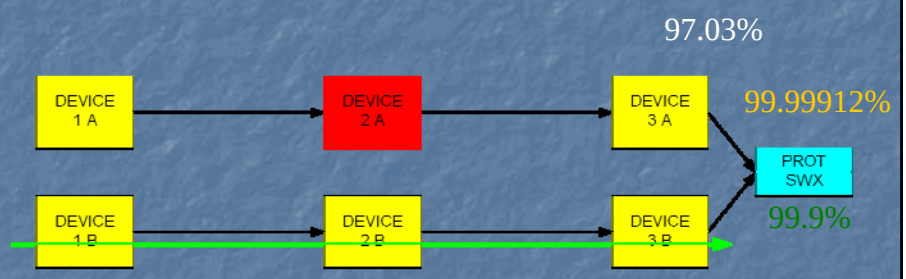


Failure To Redundant Path



99.99912% x 99% = **98.999128%**

Failure To Redundant Path



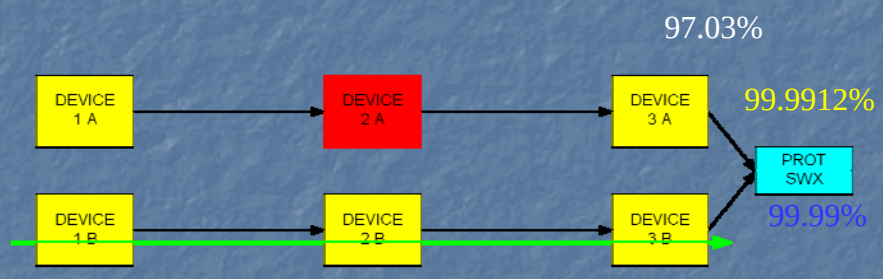
Protect SWX 10 x more reliable

97.03%

99.99912% x 99% = **98.999128%**

99.99912% x 99.9% = **99.89912%**

Failure To Redundant Path



Protect SWX 100 x more reliable

97.03%

99.99912% x 99% = **98.999128%**

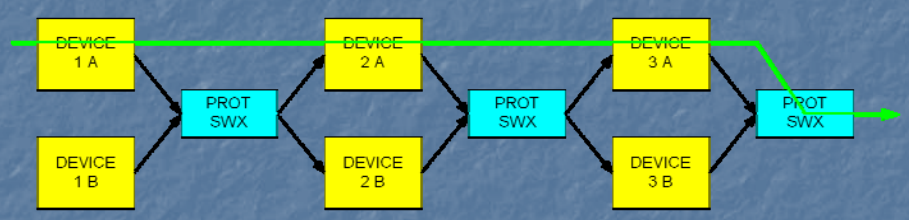
99.9912% x 99.9% = **99.8912%**

99.9912% x 99.99% = **99.9812%**

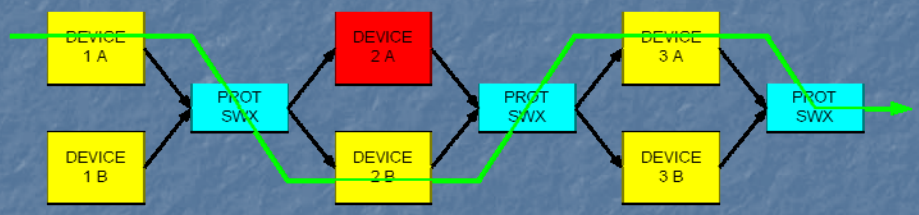
Put Your Money in the Protection Switch

- Often; the Prot Switch is made out of the same flesh and blood… not high reliability or mil spec.
- Often, there are no redundant power supplies or internal redundancy
- Often these are not tested… known to be good.
- *Don't let the facts muddle a good theory.*

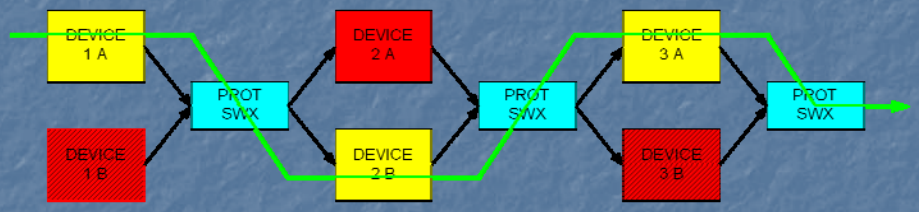
Series Parallel Architecture



Series Parallel Architecture Fault

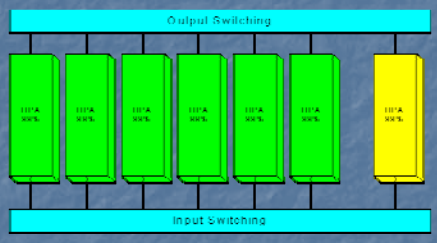


Do You Know Where Your Dead Devices Are?

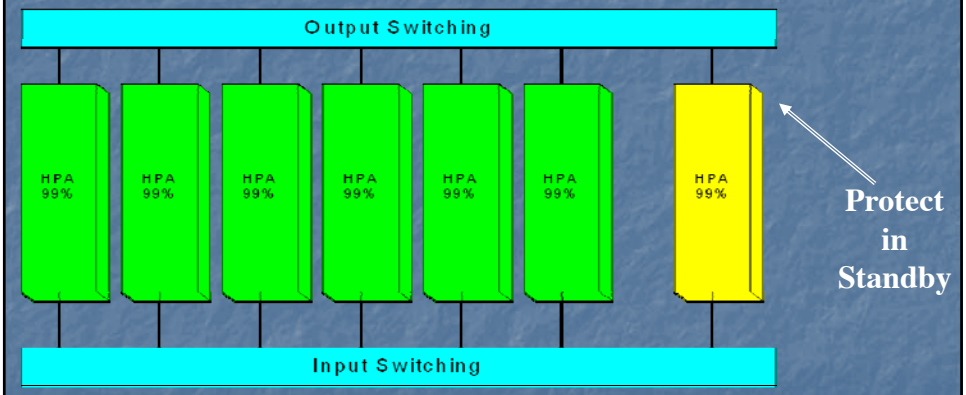


X:N designs

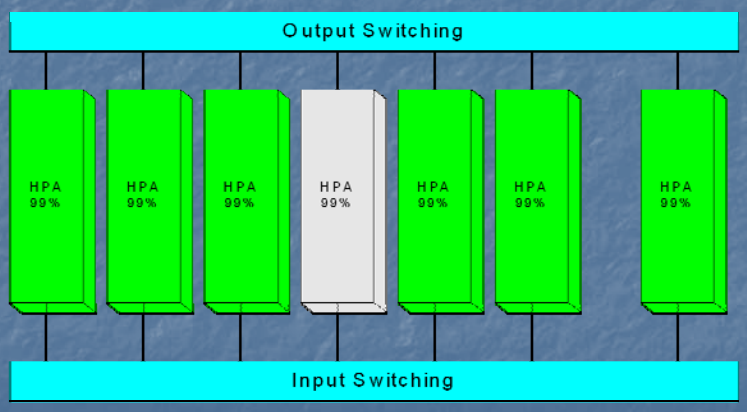
- Shares a Protection Device
- Elaborate switching required
- Protect Amp is only available when not in use elsewhere
  - Single Thread when Prot on line
- Configuration time



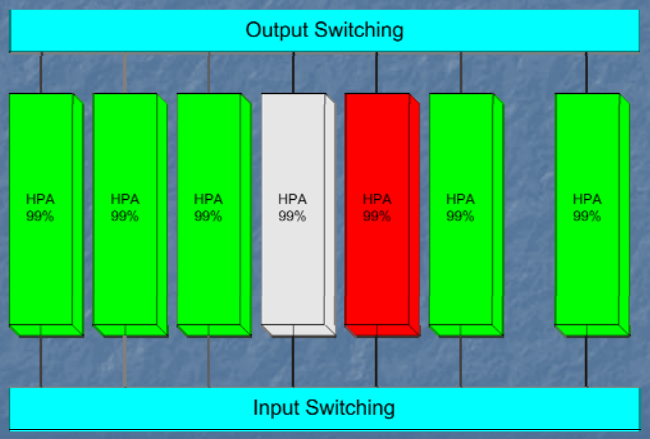
1:N say... 1:6 Design



1:N Fails over to Prot



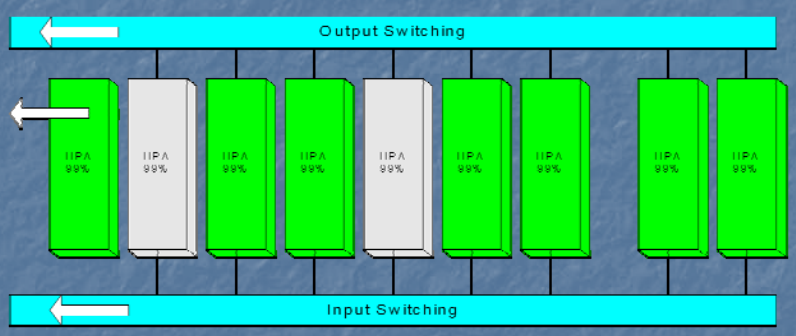
1:N Fails over to Prot... Survivors become unprotected



X:N Math....

- Subtract the "Prot Demand" from the Prot's Availability
  - 99% - 5% = 94%
    - (6 primary – 1 in use at 99% ea)
- Parallel the Prot with the desired Primary
  - 94% ‖ 99% = 99.94%
- Series the result with the Input / Output Availability
  - 99.99% X 99.99% = 99.98%
  - 99.94% X 99.98% = **99.92**%
    - Compare to 1:1
    - 99% ‖ 99% = 99.99%

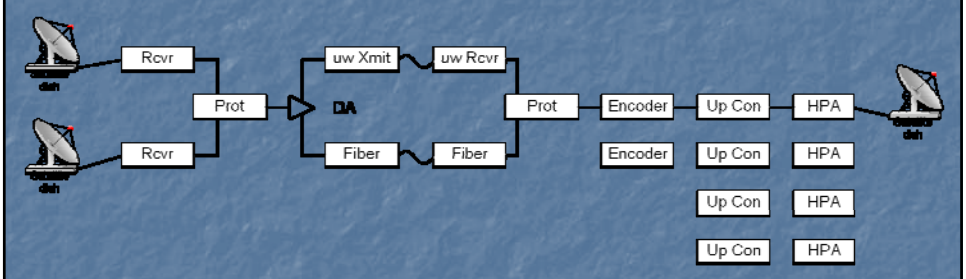
2:N say... 2:12 even better for units protected... *IF the common equipment is very reliable.*



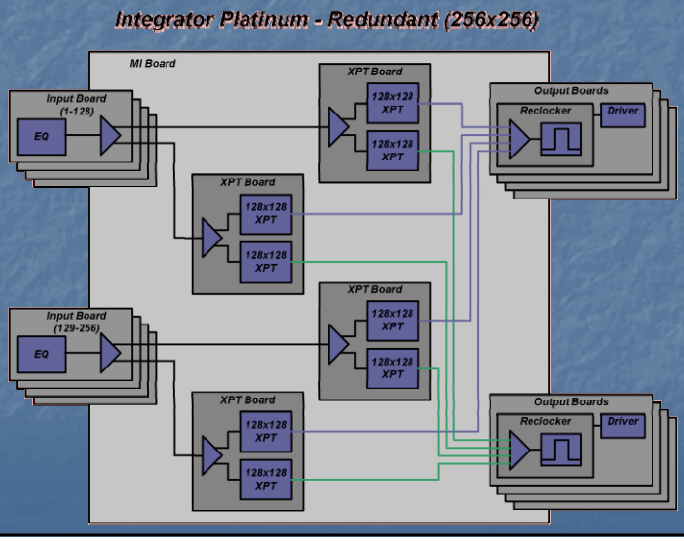
1:6 Vs 2:12

- 1:6 = 99.92%
- 2:12 = 99.94%
- But… a control or switch failure takes down all 12…
- Low Probability High Impact vs. High Probability Low Impact

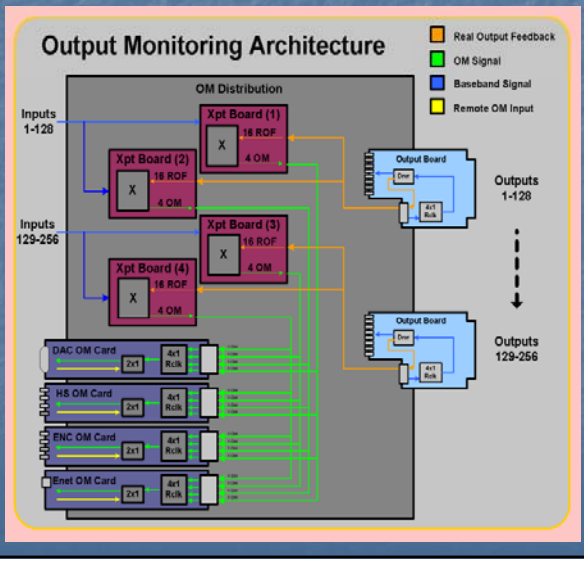
All Architectures are a Combination of Series and Parallel and X:N Configurations



Redundant Routers? – How *do* they do *that*?



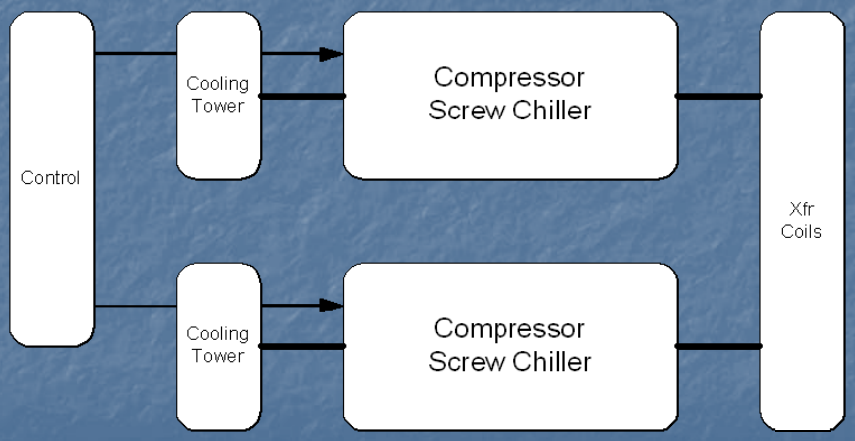
Output Monitoring Architecture



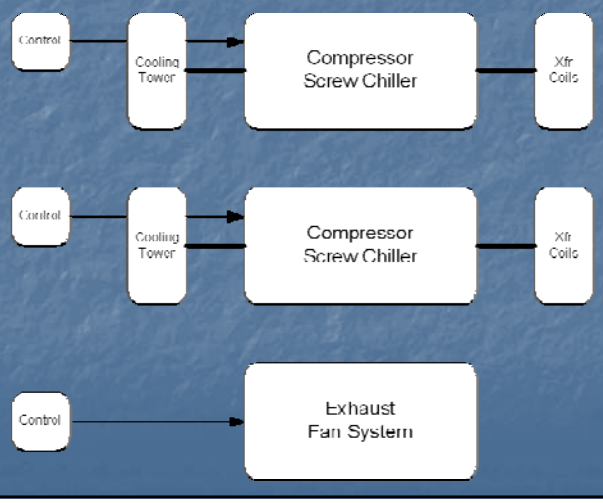
HVAC – Your most dangerous system

- Remember that heat thing?
- If a screw chiller takes 45-minutes to reset after a power bump…
- Controls cause most outages.
- Lead and Lag

HVAC – Standard "Dual System"



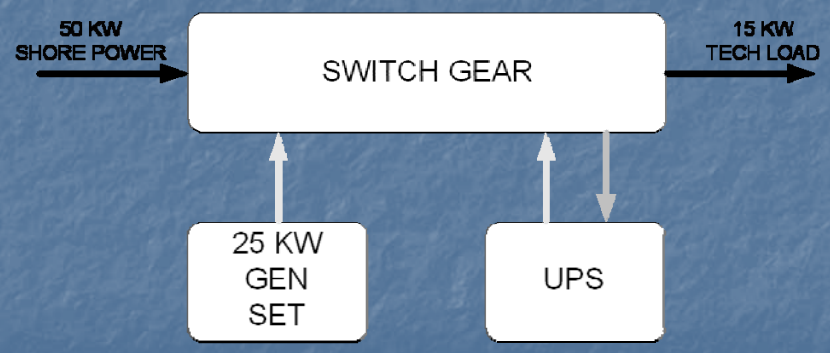
HVAC – "Autonomous System" w/"rainy day backup"



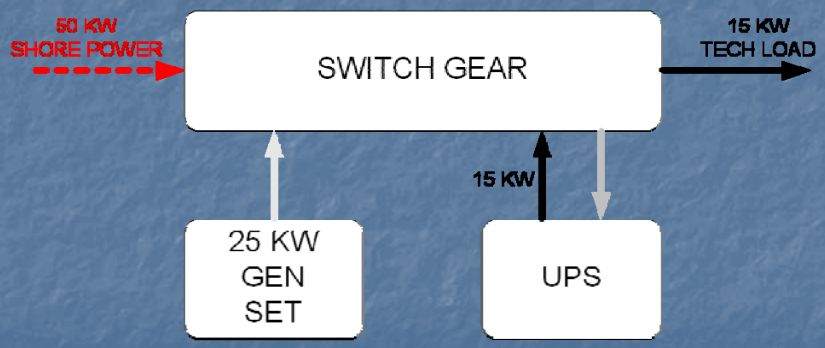
Power Systems – Your Second Most Dangerous System Or "Plant Switched OR Rack Switch"

- Plant Switched
  - Politically tough to fail-over test
  - Busses & Control often SPOF
  - Prone to Systematic failures
  - Scales poorly
- Rack Switched
  - Spreads risk
  - No SPOF
  - Not a lot of gear out there
  - Takes advantage of eq. redundant PS

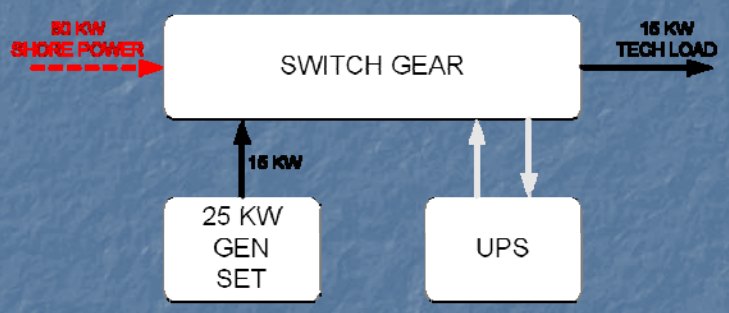
Primary Power – As The Day Begins



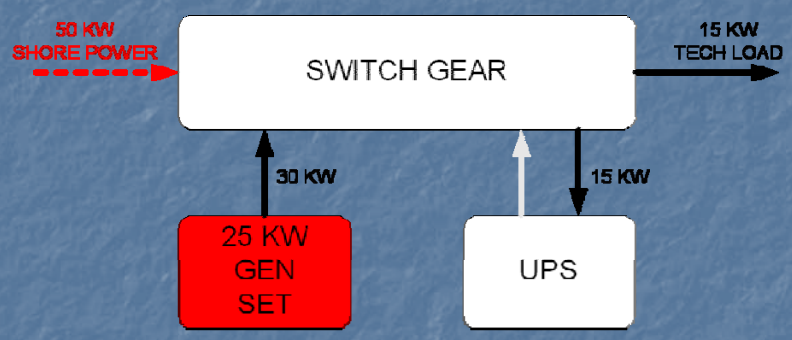
Primary Power – UPS Takes Over



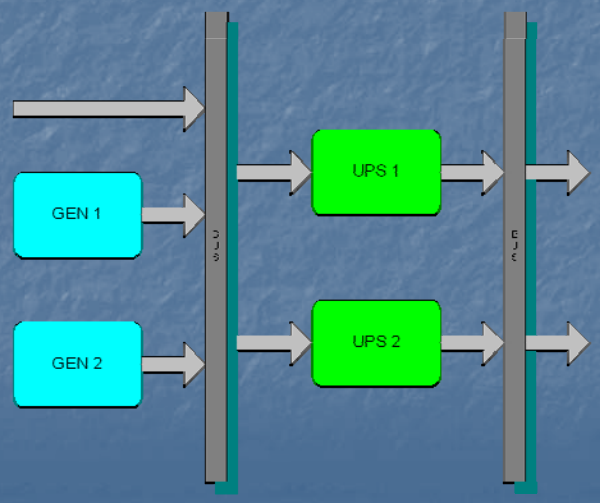
Primary Power – Generator Takes Over



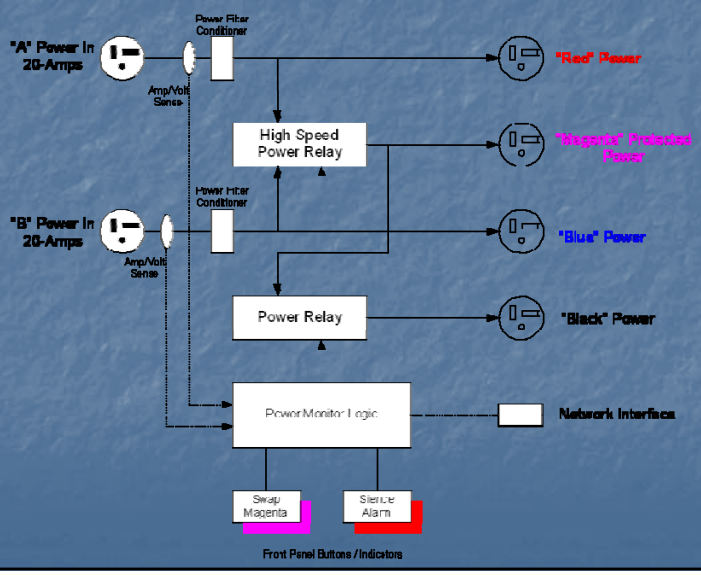
Primary Power – Boom



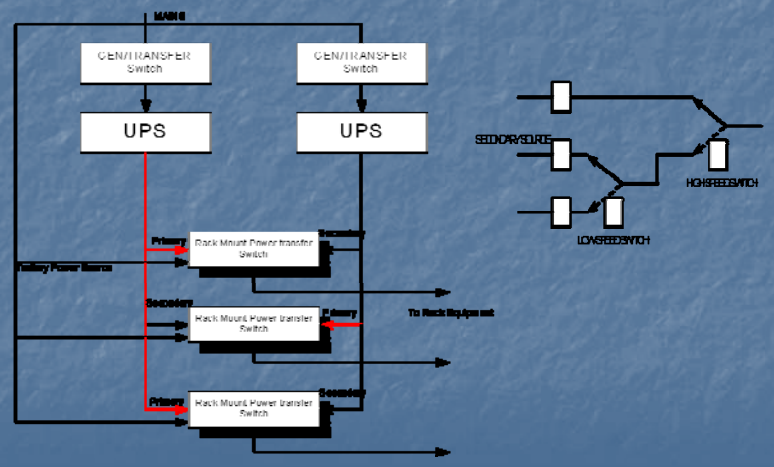
Standard "High Reliability" Power System



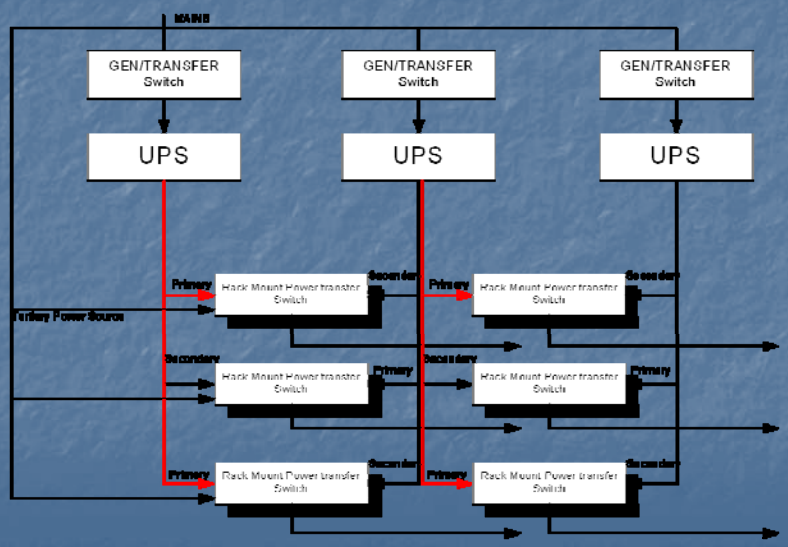
The Pri/Sec/Ter Switch



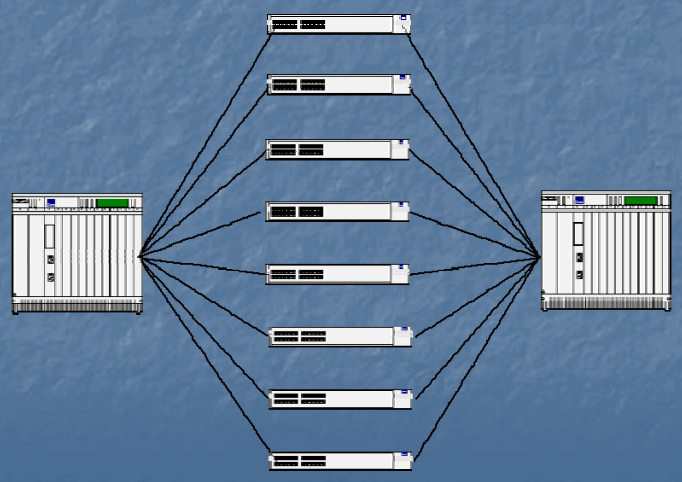
Pri/Sec/Ter – Rack Switched High Reliability / Minimum Risk Power System



Growing A Rack Switched System



Data Networks – Dual Homed Servers, Etc..

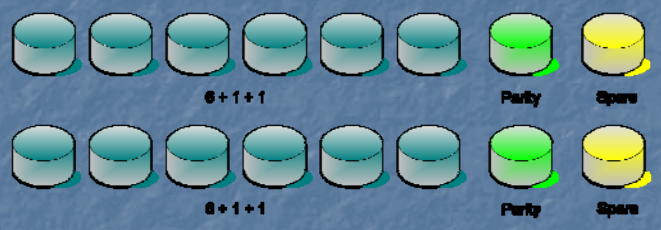


Raid-3 6+1+1

99% x 99% x 99% x 99% x 99% x 99 = 94.2%

94.2% ‖ 99% = 99.94%

Raid-31

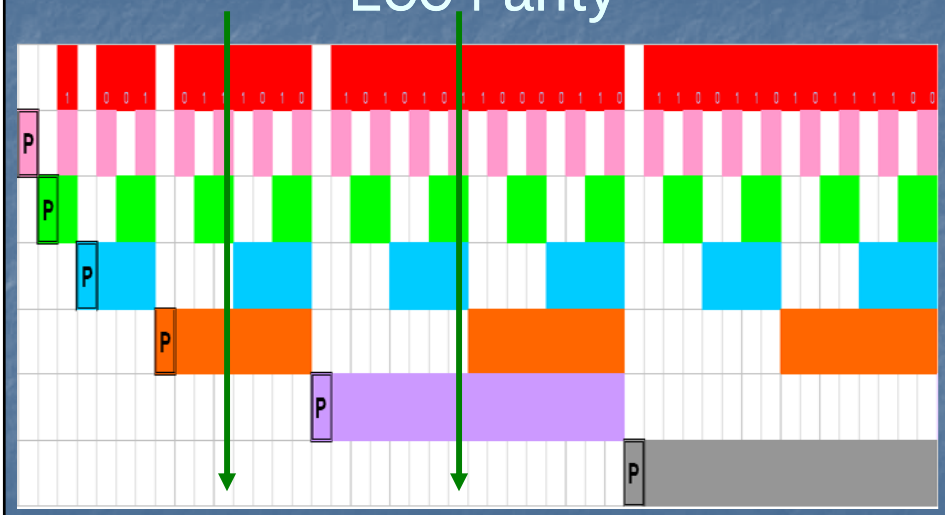


99.94% || 99.94% = 99.9997

JBOD... in ECC

99.94 || 99.94 = 99.999978

ECC Parity



I read your mail…

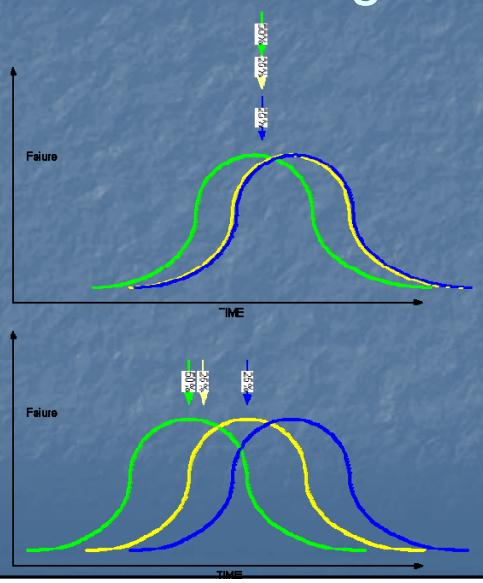
IT Stuff

- Software
  - Isolationist State
    - Production Network
    - Operational Network
    - Dirty Network
  - Protected State
    - Firewall
    - VPN
    - Virus protection
    - Rolling backups
    - Monitoring/Managed system
- Hardware
  - Redundant FC
  - Parallel Process
  - Raid
  - Distributed Processes

Component Level Design

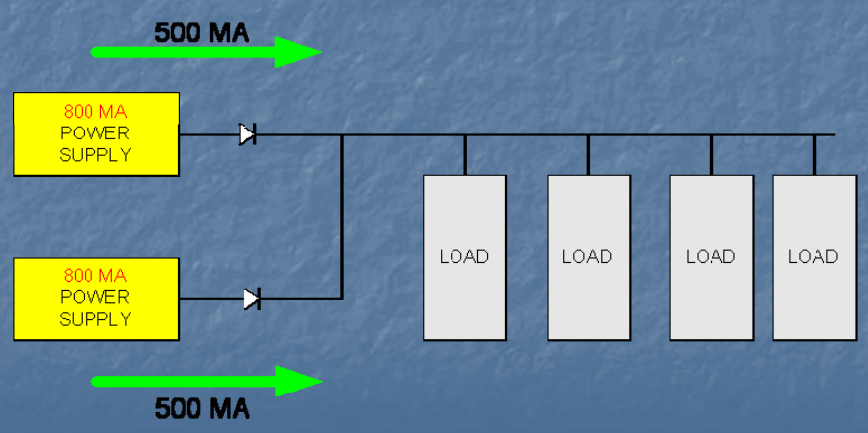
- Follows the same rules as systems
- Out of our control – most likely
- Schematics Anyone?
- Did we get what we think we bought?

Combining MTBF

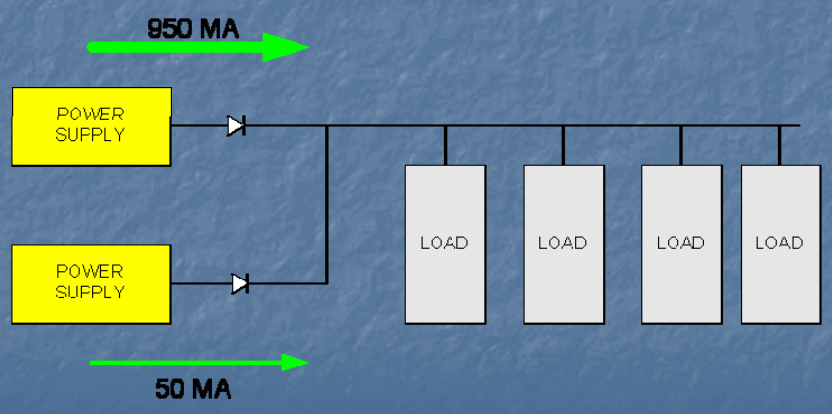


Calculate the collective Mean

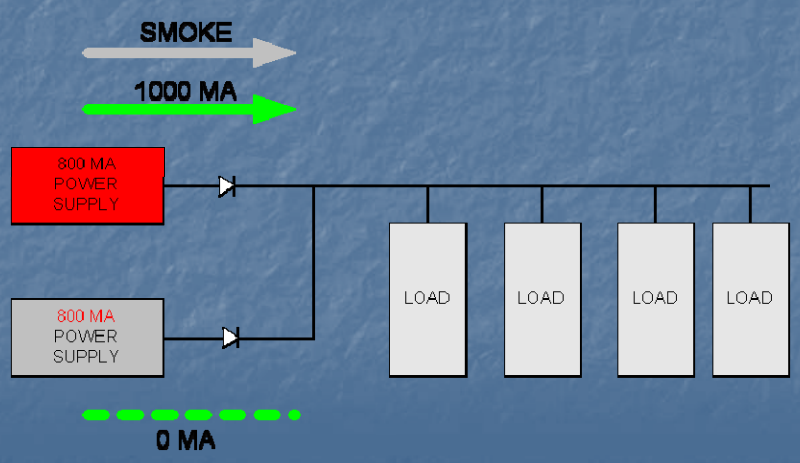
Redundant Frame Power Supplies
(Our Starting Example)



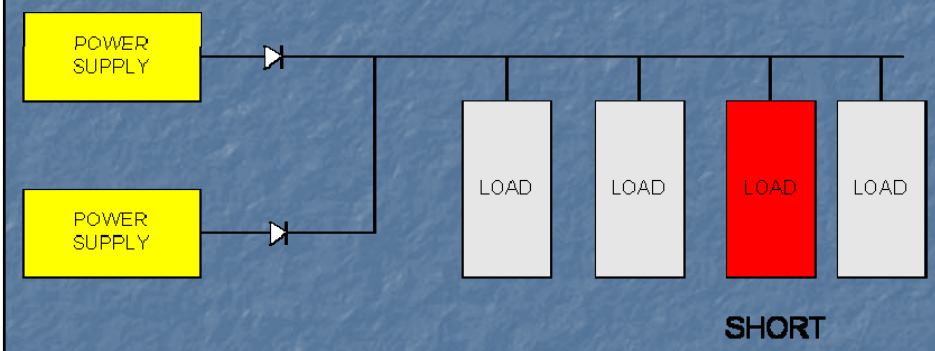
Redundant Frame Power Supplies
(Current Hogging)



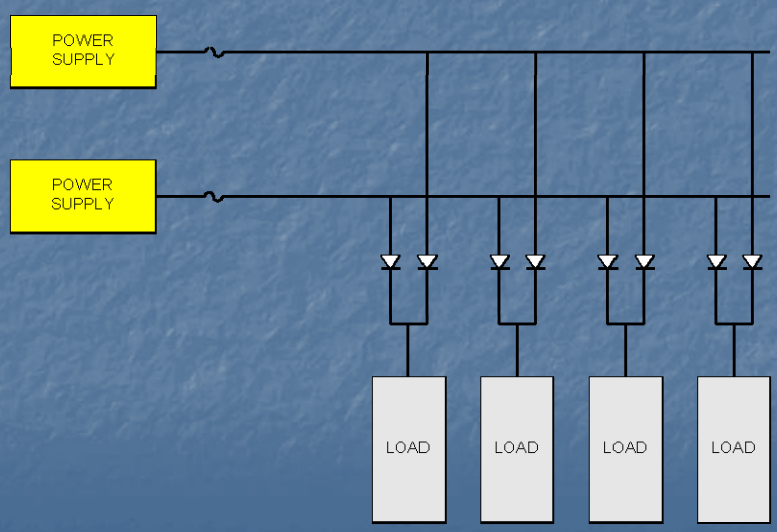
Redundant Frame Power Supplies
(Fault By Insufficient Capacity)



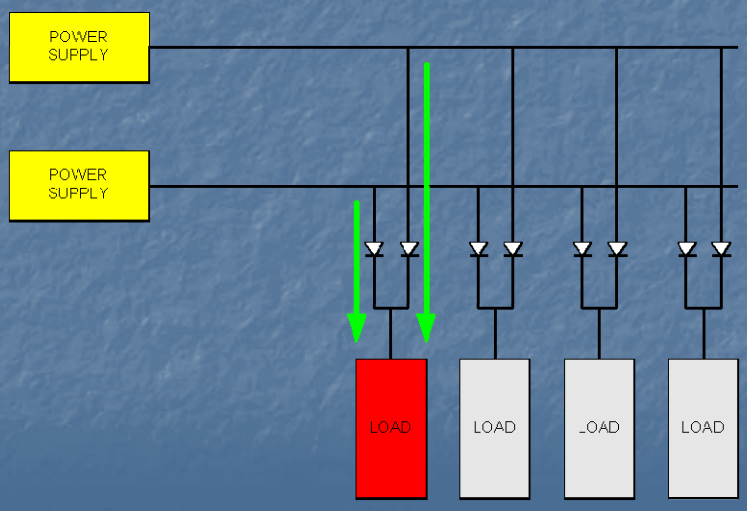
Redundant Frame Power Supplies
(Fault By Load)



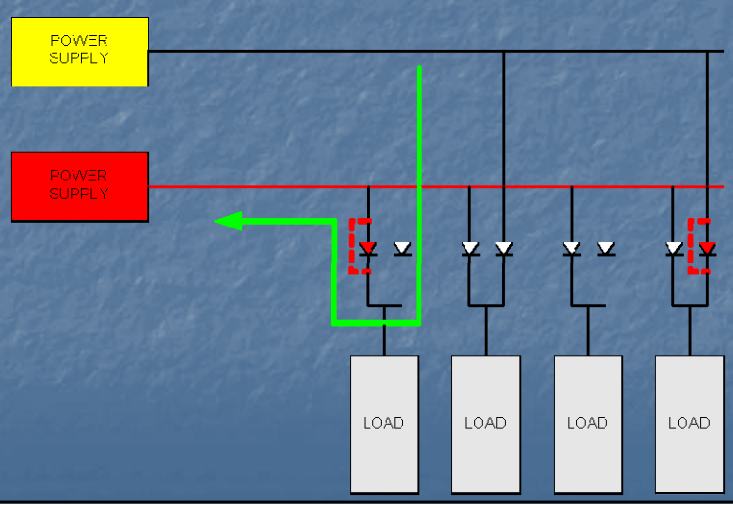
Redundant Frame Power Supplies
(Diode Steered and Source Fused)



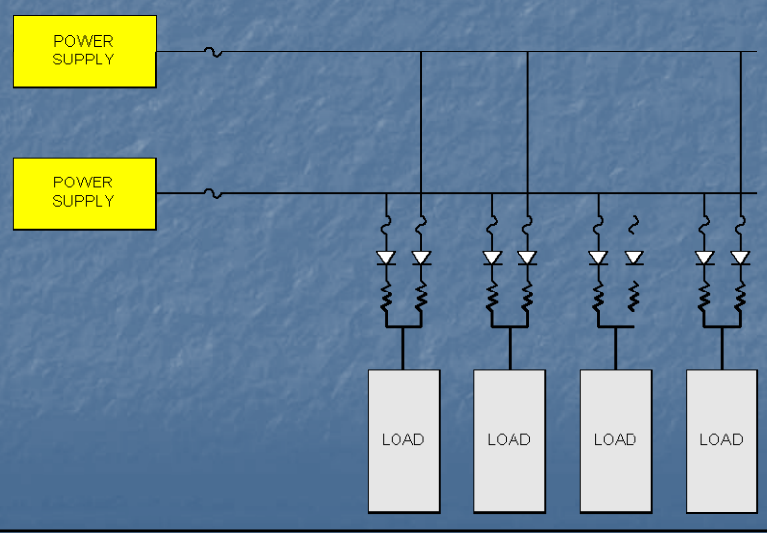
Redundant Frame Power Supplies Diode
(Fault By Unfused Load)



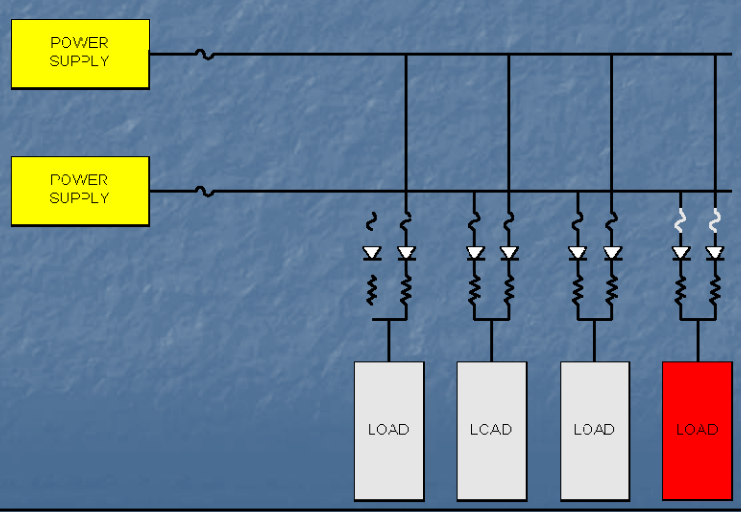
Redundant Frame Power Supplies
(Redundancy Lost to Diode)



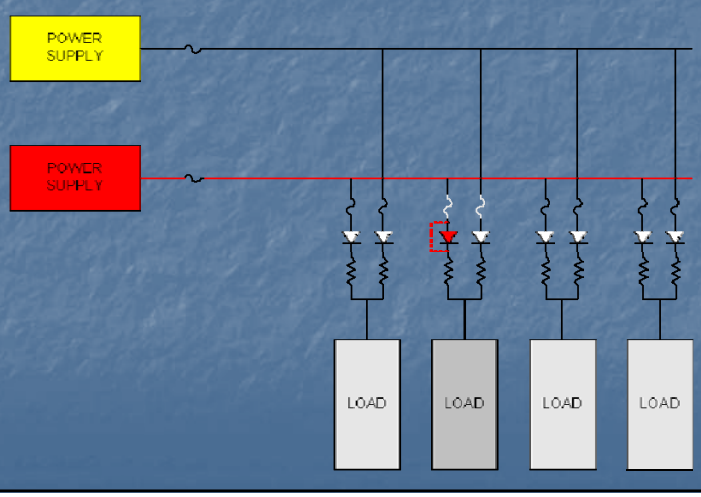
Redundant Frame Power Supplies
(with fuses, diodes, and load sharing)



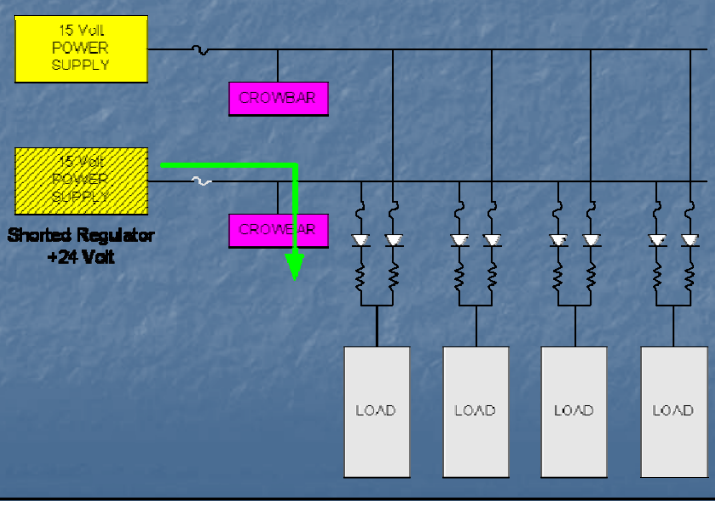
Redundant Frame Power Supplies
(Fault By Fused Load)



Redundant Frame Power Supplies
(The way it should be...)



Redundant Frame Power Supplies
(Death by Over-Voltage)



Beating the Cost

- So far… Redundancy for Reliability costs MORE than twice a single thread system.
- Minimize Protection Switch Points
- Concentrate on Critical Path
- Drive to X:N architectures

About Preventive Maintenance

- Guilt
- $
- 

- Thermal Imaging
- Current Mapping
- Parameter Logging/Tracking
- Replace old gear and components
- Clean, Lubricate
- Listen and Look
- Train and Practice
- Fail over Testing

What of Six Sigma?

- Data Driven Approach to reduce defects
- Motorola…
- Six Sigma = 3.4 defects per million
- Defect is anything outside of customer expectations
- BMPS – Business Process Management System
- Earn cool green, black and master's belts.

- **DMAIC**
  - Define
  - Measure
  - Analyze
  - Improve
  - Control
- **DMADV**
  - Define
  - Measure
  - Analyze
  - Design
  - Verify

NASA

The most reliable component is the one left out.

Jeff Bell – NASA

Take Away

- The point of diminishing returns for a protect switch is 2 orders of magnitude more reliable than everything else.
- Low MTTR is worth *LOTS* more than Low MTBF.
- You have an unstable system instead of a high reliability system if:
  - There is insufficient M&C
  - There is no fail-over testing
- Put your money in the critical paths
- ***This is what system engineering is…***

The Price of Nonconformance (PONC)

Board Shop	$49
Test	$89
Telephone Call	$279
Return	$744