Availability and Reliability Theory

and the Expectations Behind the Numbers

Legendary Reliability®

Purpose

Provide an understanding of reliability and availability which enables IT decision makers to make sound management decisions.

Agenda

- Introduction of the NCPI Science Center
- Availability Science Theory and Application
- Probabilistic Analysis Methodologies
- Learning from the real world

NCPI Science Center

Mission:

To advance the state of knowledge about the design and operation of Network-Critical Physical Infrastructure (NCPI) in both the industry and user communities. To provide techniques, guidelines, and tools to empower users to make the most effective planning decisions regarding their NCPI investments, maximizing availability and agility while reducing TCO.

Availability / Reliability Theories and Application

Using numbers to make sound decisions

Legendary Reliability®

99.999%
FIVE NINE

Get 99.999% reliability.

99.999% - Når oppetid er kritisk

APC
Legendary Reliability®

A few myths and misconceptions

- MTBF is the average number of hours a system will operate
- More parts = less reliability
- Field MTBF values can be compared if everyone defines “load drop” as a failure

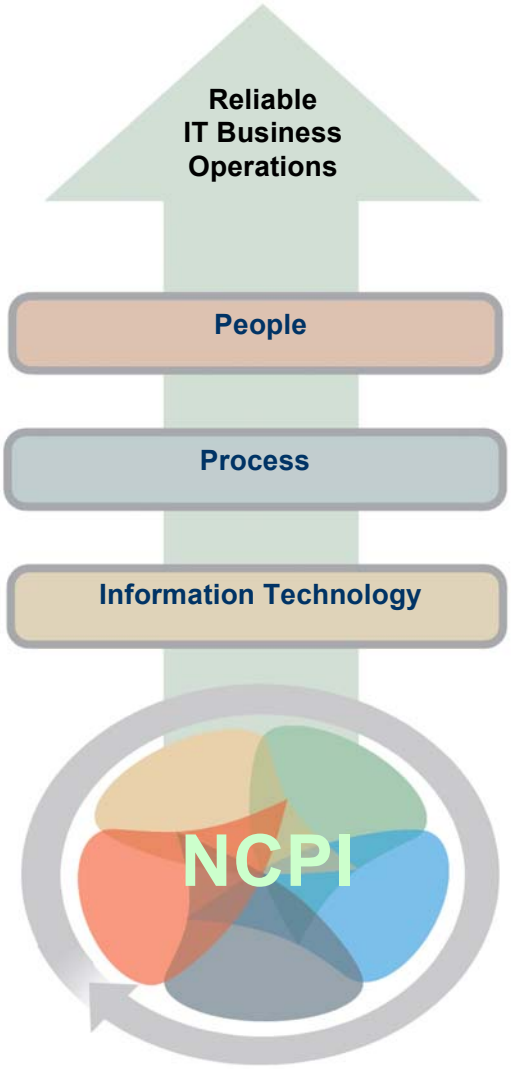
Why use *Availability Analysis*?

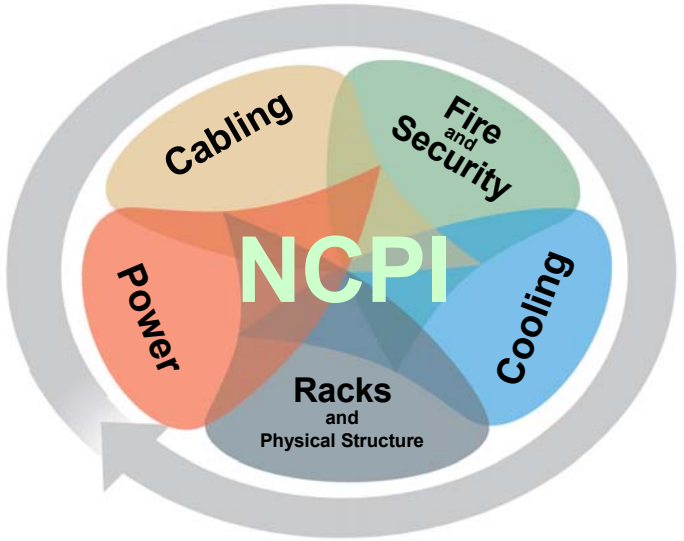
- Illustrate the strengths and weaknesses of one architecture over another.
- Answer how and where dollars should be allocated to increase availability.
- Most useful for systems that expect significant downtime from outages, or planned downtime.
- Most applicable industries: Oil refineries and certain manufacturing industries, mining.

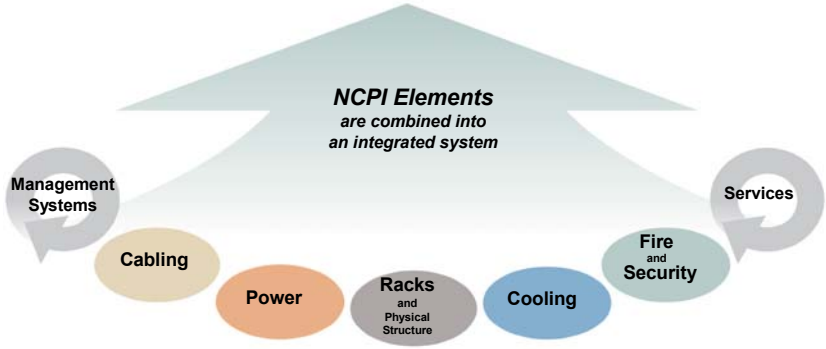
Why use *Reliability Analysis*?

- Answer how and where dollars should be allocated to increase reliability – may be different than availability answer
- Value appears the same throughout the organization
- Most useful for systems with highest $ risk in first outage cycle
- Most applicable industries: Data center applications, chip fabrications

4 Layers of Business Process Availability







APC
Legendary Reliability®

Key Terminology

- **Reliability – The probability that an entity experiences no failures under given conditions for a given time interval**
- **Availability – The probability that an entity is operating under given conditions at a given instant of time**
  - Availability categories: steady state / inherent, achieved, operational
- **Mean Time Between Failure (MTBF) – The average operating time between failures. MTBF ≅ MTTF when MTBF >> MTTR**
  - At time = MTBF; 63% of population has failed
- **Mean Time To Recover (MTTR) – The average time to restore or recover**
- **Failure Rate (λ) – The inverse of MTBF or** $\frac{1}{MTBF}$ (Exponential Distribution only)
- **Recovery Rate (μ) – The inverse of MTTR or** $\frac{1}{MTTR}$ (Exponential Distribution only)

Source: Reliability Engineering Handbook

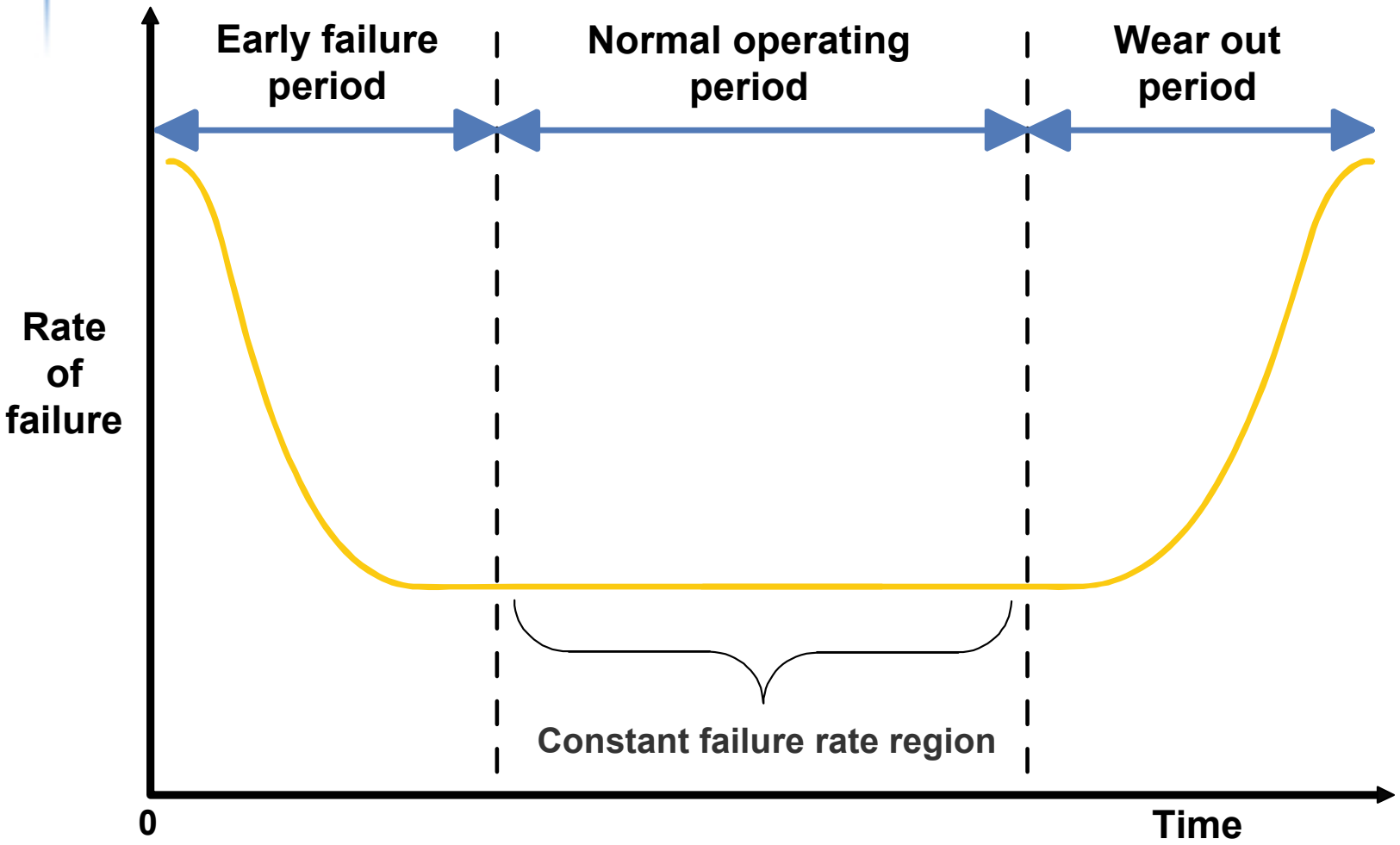
MTBF – Real "Life" Example

- 500,000 25-year-old humans in the sample population
- Data is collected on failures (deaths) for this population over the year
- Operational life of the population is
  500,000 x 1 year = 500,000 people years
- Throughout the year, 625 people failed (died)
- The failure rate is
  625 failures / 500,000 people years = 0.125% / year
- MTBF is the inverse of failure rate or 1 / 0.00125 = 800 years

Even though 25-year-old humans have high MTBF values, their life expectancy (service life) is much shorter and does not correlate.

APC
Legendary Reliability®

Bathtub Curve



APC Legendary Reliability®

Key Availability Equations

Availability – $$A = \frac{\mu}{(\mu+\lambda)} + \frac{\lambda}{(\mu+\lambda)} e^{-(\mu+\lambda)t}$$

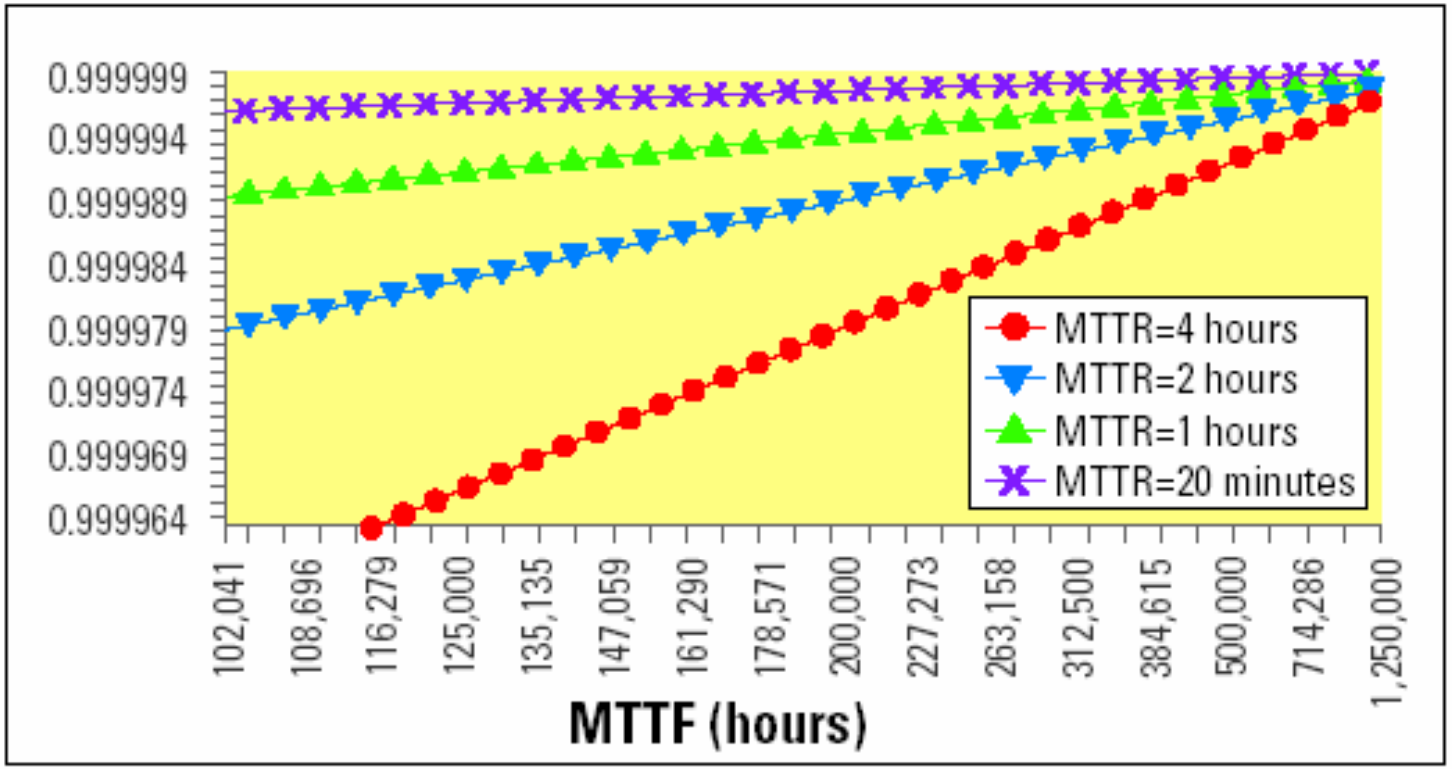
$$t = 0\,hrs \quad A = \frac{1}{(1+0.001)} + \frac{0.001}{(1+0.001)} e^{-(1+0.001)*0} = 1$$

Steady State Availability – $$A = \frac{\mu}{(\mu+\lambda)} \qquad A = \frac{MTBF}{(MTBF+MTTR)}$$

$$t = 1000\,hrs \quad A = \frac{1}{(1+0.001)} + \frac{0.001}{(1+0.001)} * 0 = 0.999 \qquad A = \frac{1000}{(1000+1)} = 0.999$$

APC Legendary Reliability®

Availability vs. Mean Time to Failure



APC
Legendary Reliability®

Key Reliability Equations

Reliability – $R = e^{-\lambda t}$

$ex.\quad MTBF = 1000\ hrs$

$t = 0\,hrs \quad R = e^{-0.001*0} = 1$

$t = 1000\,hrs \quad R = e^{-0.001*1000} = 0.368$

What makes calculated probabilities credible?

- **Assumptions**
  - **Without assumptions the results mean nothing**
  - **I.e. Human error, spare parts on hand, constant failure rate**
- **Methods**
  - **Comparing two or more similar architectures is effective in evaluating the relative differences between them.**
    Helps to avoid the vender specific definitions of “failure”
    Helps mitigate the assumption of constant failure rate
  - **Confidence limits depend on the size of the population, you are studying**
    www.weibull.com/hotwire/issue4/relbasics4.htm
    Useful when calculating the availability or reliability of individual components. Data from Resistor batch much easier to gather then Data Center batch
- **Data**
  - **The results are only as good as the data**

APC Legendary Reliability®

What makes calculated probabilities credible?

- **Models**
  - The framework upon which the results are based.
  - Visually models can be represented using RBDs but ultimately models are the equations used to calculate availability or reliability
  - Equations used depend on the failure distribution of the components

Exponential Distribution **vs.** Weibull Distribution

Ex. Transformer **Ex. Capacitor (Polypropylene film)**

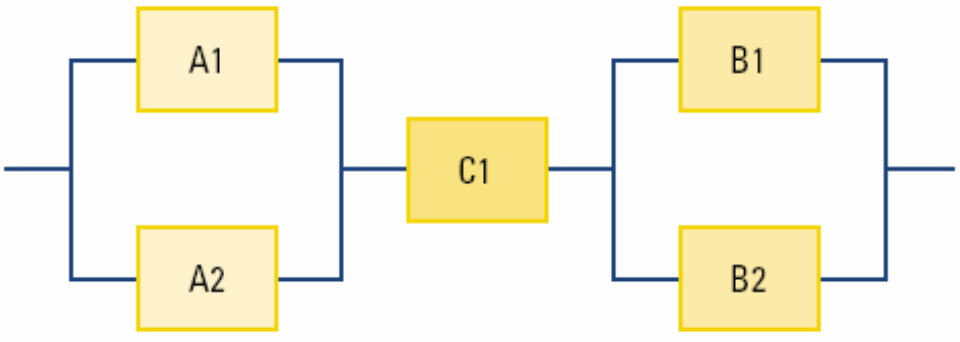
$$R(t) = e^{-\lambda t}$$

$$R(t) = \exp\left[-\left(\frac{t}{\theta}\right)^{\beta}\right]$$

$$\theta = Life\,At\ Name\ Plate\ Rating \times \left(\frac{Rated\ Cap\ Voltage}{UPS\ \ Applied\ Cap\ Voltage}\right)^{Vscale} \times 2^{\left(\frac{Rated\ Temp - Temp\ at\ steady\ state}{10}\right)}$$

APC Legendary Reliability®

Reliability Block Diagrams



Series/ Parallel Combination Model

$A_1 = A_2 = 0.99$

$B_1 = B_2 = 0.999$

$C_1 = 0.99999$

Availability calculations:

$A_A = 1 - [\ (1-A_1) * (1-A_2)\ ]$

$A_C = C_1$

$A_B = 1 - [\ (1-B_1) * (1-B_2)\ ]$

$A_{System} = A_A * A_B * A_C$

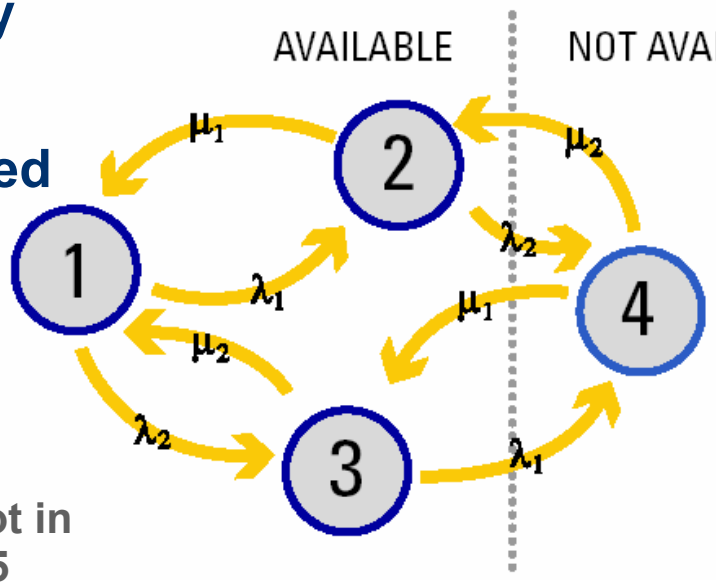
Assumptions:

- 5 repairpersons available
- Remaining components in operation during repair
- Components exhibit constant failure rate
- Human error has not been accounted for
- Independence of failures

APC Legendary Reliability®

Markov Chains

- Rewards are assigned based on the proportion of the data center that is operational
- Represents the state of the facility as a continuum
- Includes both normal and degraded states
- Combined with RBDs, this can represent a data center
  - Ex. If there are 20 sub-panels, power might be available in 19 of them, but not in the 20th. For this state, a reward of 0.95 would be assigned. If power were restored to the 20th sub-panel, then the reward would be 1.0.

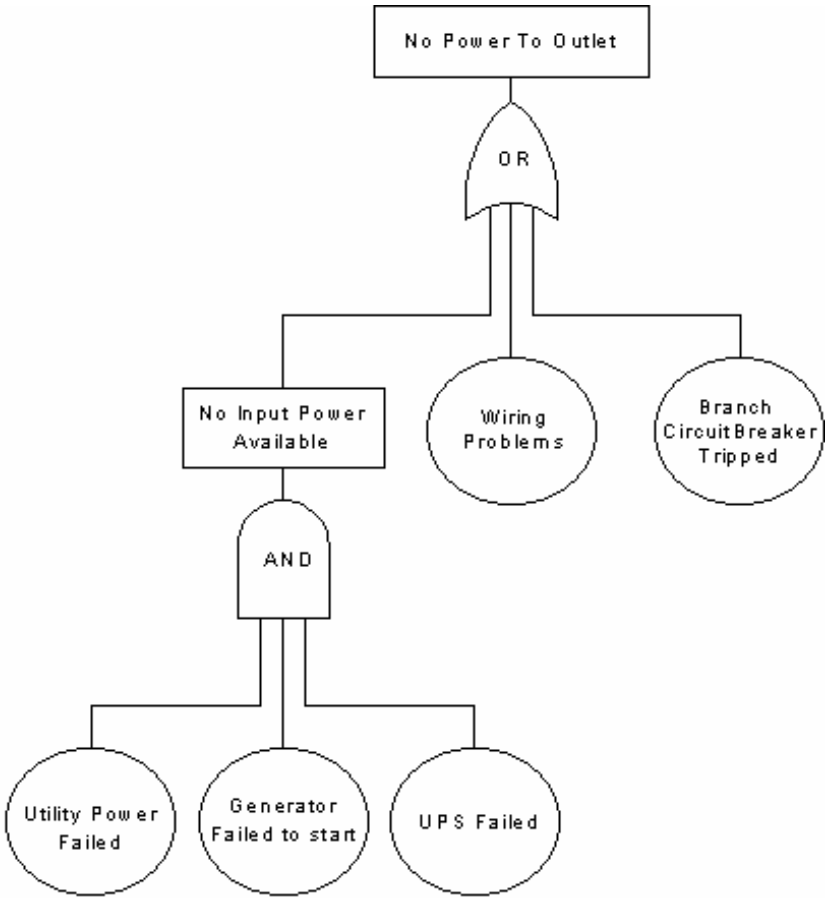


Markov of Simple Parallel System

APC Legendary Reliability®

Fault Trees

- Logical – easy to understand
- Composed mainly of Events, ANI gates, OR gates
- Everything leads to top failure event
- Analysis highly dependent on tree structure
- Cut set – a set of events that leads to the top event
- Minimal cut set – a set of events in which all must fail in order to reach top event



APC Legendary Reliability®

Probabilistic Analysis Methodologies

APC's Availability Methodology

- Used for comparing two or more electrical architectures, logic based on system success
- Detailed approach, from utility to load
- Combination of Reliability block diagrams and Markov chains.
- Reliability block diagrams are used to represent subsystems of the architecture.
  - For example, the PDU is in series with the UPS, so 2 series blocks would be drawn to illustrate this logic.
- Markov chains are then used to represent the Data Center state based on the number of sub-systems that are operational.

Where does the data come from?

- IEEE gold book– Power Systems Reliability
- Power Quality Magazine
- 3rd Party Vendor Data
- Reliability Analysis Center
- ASHRAE

3rd Party feedback of availability methodology

- **Ali Mosleh, Professor and Director of Reliability Engineering Program, University of Maryland**
  - "In my judgment the methodology is sound for the intended objective, namely a comparative analysis of two architectures.."

- **Joanne Bechta Dugan, Ph.D., Professor at University of Virginia**
  - "[I have] found the analysis credible and the methodology sound.. The combination of Reliability Block Diagrams (RBD) and Markov reward models (MRM) is an excellent choice that allows the flexibility and accuracy of the MRM to be combined with the simplicity of the RBD."

APC Legendary Reliability®

MTech's PRA Methodology

- Based on nuclear industry PRA
- Invasive data gathering, analysis can "stand alone", logic based on system failure
- Primarily uses Fault trees sometime combined with human factors
- Determine minimal cut sets from fault tree logical structure
- Calculate probability of each minimal cut set during mission
- Rank component contributions to failure
- Determine sensitivity of results to component failure rate

APC Legendary Reliability®

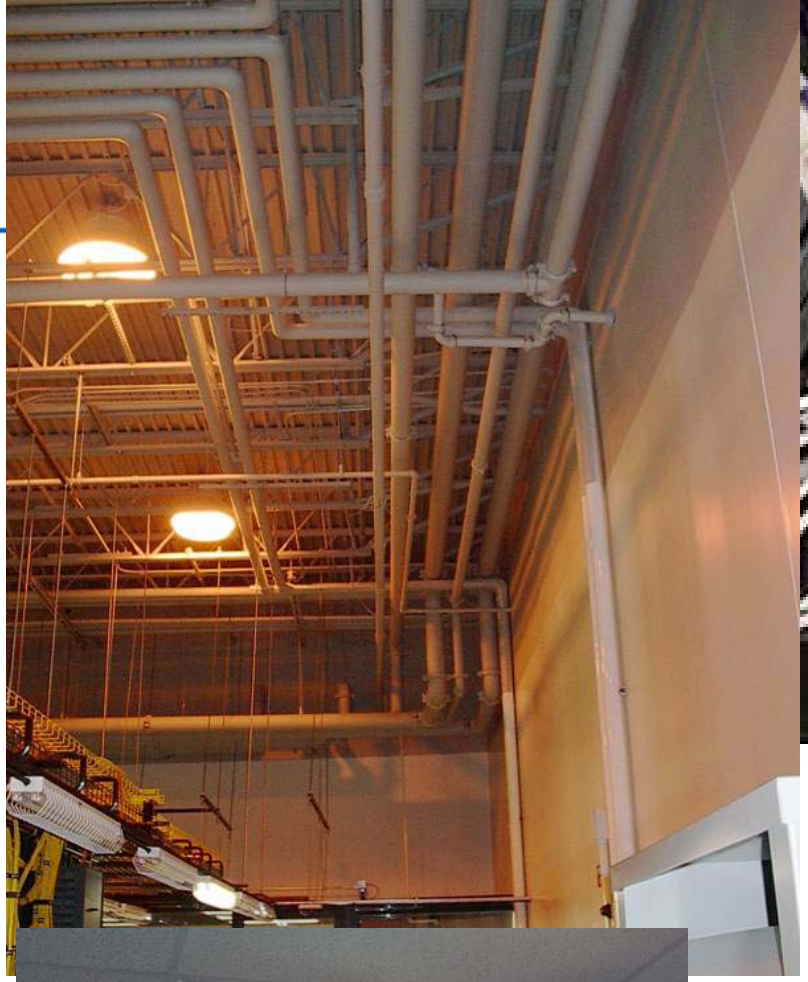
Where does the data come from?

- IEEE gold book– Power Systems Reliability
- Nuclear industry
- 3rd Party studies and data
- ASHRAE
- MTech database

Learning from the real world

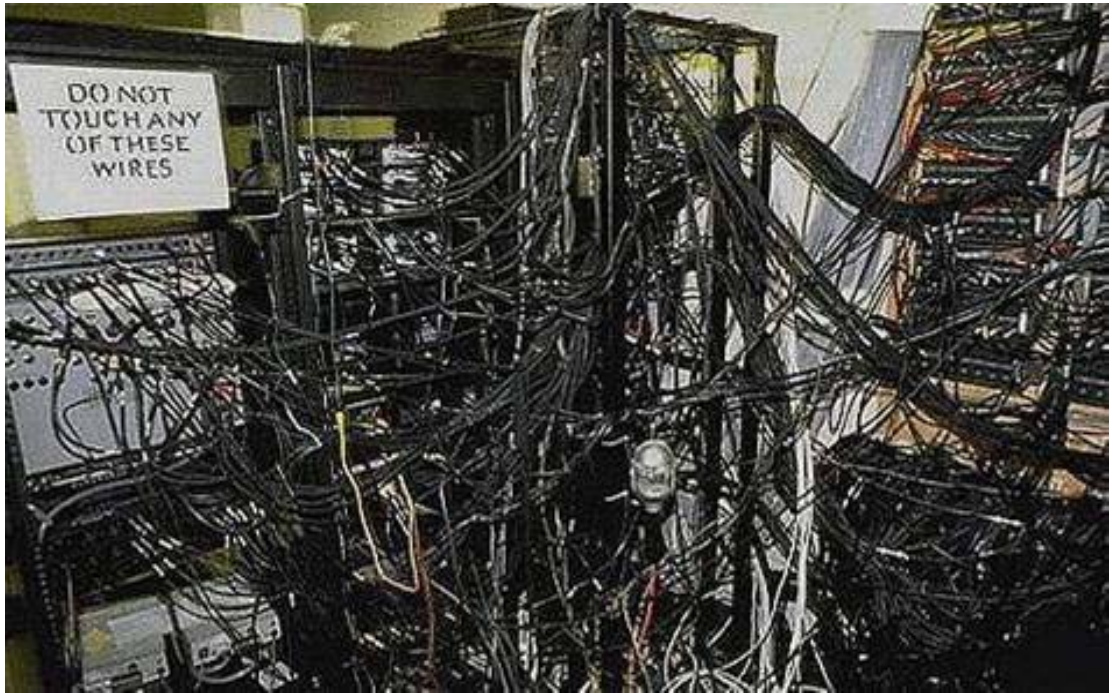
Real customer issues

Legendary Reliability®




EXIT

Source: Uptime Institute

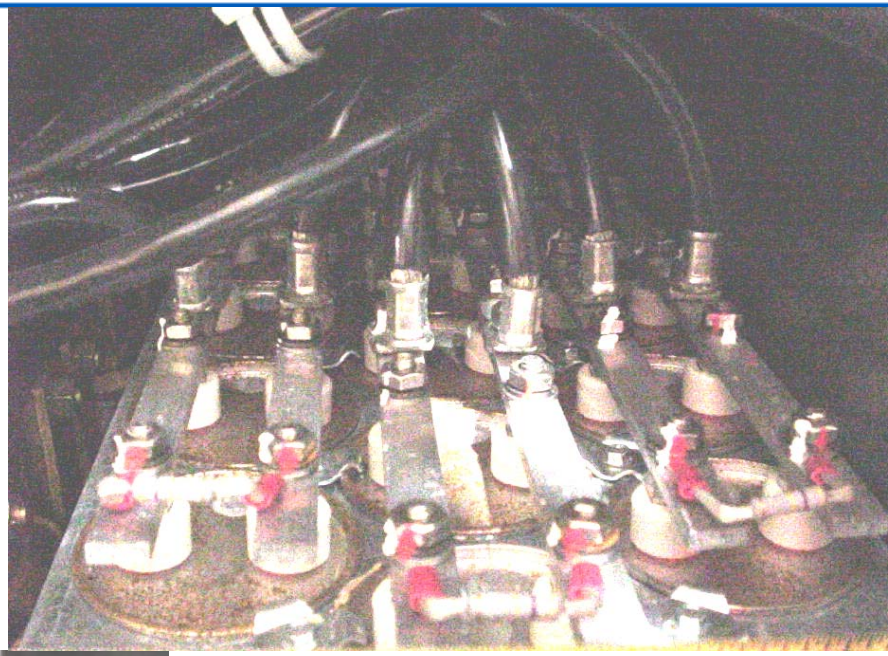


APC
Legendary Reliability®

Source: Uptime Institute

Capacitor Bank Designs

Failed cap – pressure interrupter opened



Rigid bus using threaded lugs

Flexible bus using fast-on connectors

APC Legendary Reliability®

Power Reactor	Event Number: 41226
Facility: KEWAUNEE Region: 3 State: **WI** Unit: [1] [ ] [ ] RX Type: [1] W-2-LP NRC Notified By: ETHAN TREPTOW HQ OPS Officer: JOHN MacKINNON	Notification Date: 11/26/2004 Notification Time: 03:22 [ET] Event Date: 11/26/2004 Event Time: 00:25 [CST] Last Update Date: 11/26/2004
Emergency Class: NON EMERGENCY 10 CFR Section: 50.72(b)(3)(v)(D) - ACCIDENT MITIGATION	Person (Organization): DAVE PASSEHL (R3)

Unit	SCRAM Code	RX CRIT	Initial PWR	Initial RX Mode	Current PWR	Current RX Mode
1	N	N	0	Intermediate Shutdown	0	Intermediate Shutdown

Event Text

SAFETY INJECTION ACCUMULATOR ISOLATION VALVES FOUND CLOSED AND THEIR BREAKERS LOCKED OFF.

"During plant startup following a Refueling Outage, the Reactor Coolant System was pressurized greater than 1000 psig with the Safety Injection Accumulator **Isolation Valves (SI-20A and SI-20B) closed and their breakers locked off. This is contrary to the plant Technical Specification requirement to open the valves and lock out their breakers prior to the Reactor Coolant System exceeding 1000 psig.** The Safety Injection Accumulators are required to inject into the Reactor Coolant System to mitigate the consequences to a LOCA. This is conservatively being reported under 10CFR50.72(b)(3)(v)(D) as "Any event or condition that at the time of discovery could have prevented the fulfillment of the safety function of structures or systems that are needed to mitigate the consequences of an accident."

"At the time of discovery, Reactor Coolant System pressure was approximately 1090 psig and Reactor Coolant System temperature was approximately 440 deg. Fahrenheit. Approximately three minutes after the condition was discovered, the SI Accumulator Isolation Valves were opened and their power breakers were locked out."

The STA discovered the problem while reviewing Technical Specification's and Plant Conditions.

The NRC Resident Inspector was notified of this event by the licensee.

Power Reactor	Event Number: 41353
Facility: INDIAN POINT Region: 1 State: **NY** Unit: [2] [3] [ ] RX Type: [2] W-4-LP,[3] W-4-LP NRC Notified By: BRIAN ROKES HQ OPS Officer: BILL HUFFMAN	Notification Date: 01/24/2005 Notification Time: 16:07 [ET] Event Date: 01/24/2005 Event Time: 10:00 [EST] Last Update Date: 01/24/2005
Emergency Class: NON EMERGENCY 10 CFR Section: 26.73 - FITNESS FOR DUTY	Person (Organization): WILLIAM COOK (R1)

Unit	SCRAM Code	RX CRIT	Initial PWR	Initial RX Mode	Current PWR	Current RX Mode
2	N	Y	100	Power Operation	100	Power Operation
3	N	Y	100	Power Operation	100	Power Operation

Event Text

FITNESS FOR DUTY REPORT

A non-licensed **plant employee was determined to be under the influence of alcohol** during a test conducted for cause. The employee's access to the plant has been terminated. Contact the Headquarters Operations Officer for additional details.

The licensee has notified the NRC Resident Inspector.

Power Reactor	Event Number: 41296
Facility: ROBINSON Region: 2 State: **SC** Unit: [2] [ ] [ ] RX Type: [2] W-3-LP NRC Notified By: BILL STOVER HQ OPS Officer: JOHN KNOKE	Notification Date: 12/27/2004 Notification Time: 01:02 [ET] Event Date: 12/27/2004 Event Time: 00:31 [EST] Last Update Date: 12/27/2004
Emergency Class: UNUSUAL EVENT 10 CFR Section: 50.72(a) (1) (i) - EMERGENCY DECLARED	Person (Organization): CAUDLE JULIAN (R2) PETER WILSON (IRD) MICHAEL JOHNSON (NRR) STEINDURF () AKERS (DHS)

Unit	SCRAM Code	RX CRIT	Initial PWR	Initial RX Mode	Current PWR	Current RX Mode
2	N	Y	100	Power Operation	100	Power Operation

Event Text

UNUSUAL EVENT DECLARED DUE TO FIRE INSIDE PROTECTED AREA LASTING GREATER THAN 10 MINUTES

Fire within the Protected Area lasting more than ten minutes. The Unusual Event was declared at 00:31 EST. **The fire was located in the small arms locker** in an out-building within the Protected Area. The fire was extinguished at 00:49 EST. Darlington County Fire Department responded."

Onsite security detected smoke and heard ammunition rounds discharging from a locked door small arms locker located in the Protected Area. Security reported the fire and onsite fire personnel responded. At 00:49 EST the fire was declared extinguished and a fire watch was set. No personnel were injured in this event. Darlington Fire Department was called and responded to the site, however, by the time they arrived the fire was put out and they, therefore, did not enter the Protected Area. Security believes this to be an isolated event with no evidence of malevolent actions.

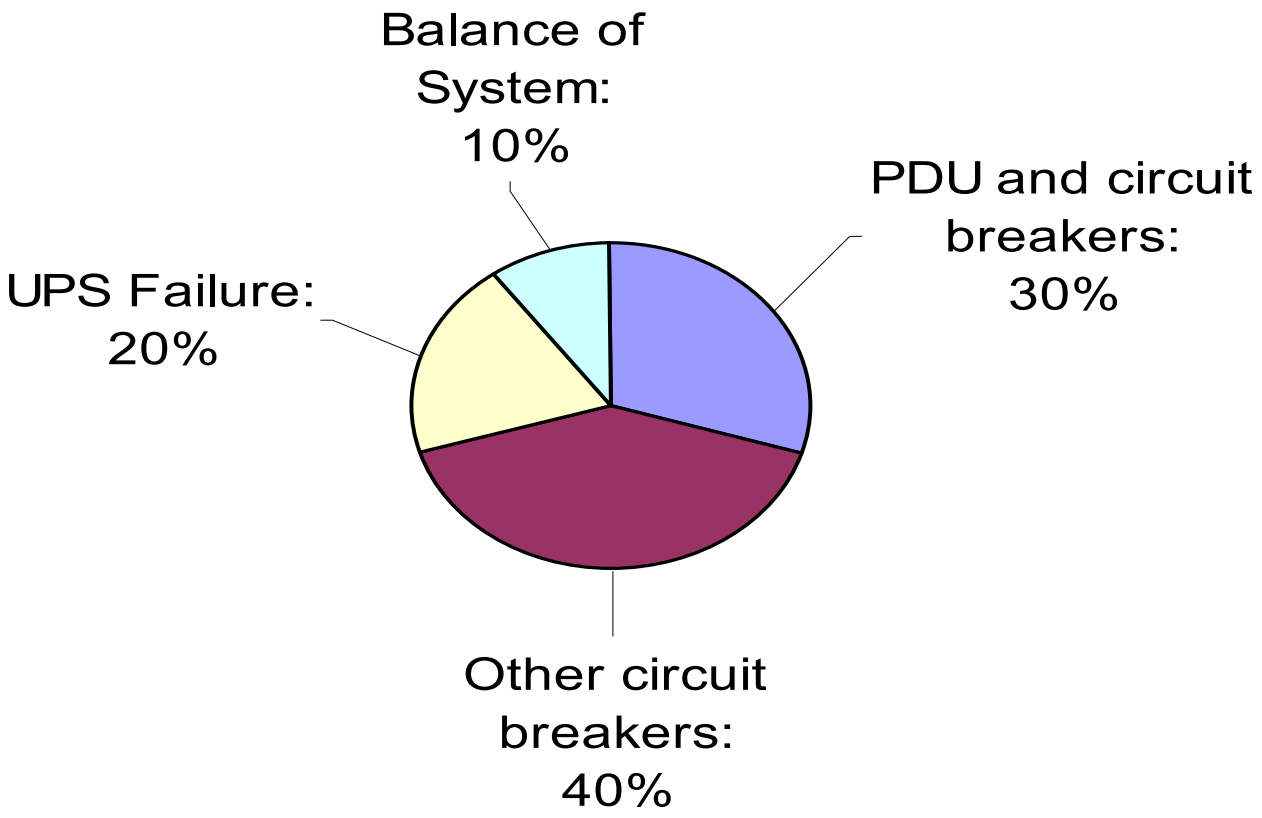
The Licensee notified state and local agencies and the NRC Resident Inspector.

* * * UPDATE ON 12/27/04 AT 02:03 EST FROM B. STOVER TO J. KNOKE * * *
At 01:30 on 12/27/04 the Licensee terminated the Unusual Event. The Licensee indicated the fire has been out for 41 minutes. All on site small arms lockers were inspected by security and no evidence of any damage or tampering was found. The LLEA was not called for this event, however, they did respond when the Darlington Fire Department responded. The LLEA did not enter the Protected Area. As a precautionary followup measure the Licensee requested the Darlington County Sheriff's office send an arson investigator to the scene.

The Licensee notified state and local agencies and the NRC Resident Inspector. Notified R2DO (Julian), NRR (Johnson), IRD (Wilson), FEMA (Steindurf), and DHS (Akers).

Where do failures occur?

Causes of failure in data center



Source: MTech

APC Legendary Reliability®

Questions?

Legendary Reliability®