Tutorial: “Statistical Methods for System Dependability: Reliability, Availability, Maintainability and Resiliency”

NexComm 2016
International Associatioin of Research and Industrial Academia (IARIA)

Drs. Andy Snow* and Gary Weckman**
(asnow@ohio.edu & weckmang@ohio.edu)

***School of Information & Telecommunication Systems**
**** Department of Industrial & Systems Engineering**
Ohio University

Outline

A. **ICT Infrastructure Risk**
B. **Examples of ICT Network Infrastructure**
C. **RAM-R: Reliability, Availability, Maintainability and Resiliency**
D. **Protection Level Assessment & Forecasting**

Outline

A. ***ICT Infrastructure Risk***
B. **Examples of ICT Network Infrastructure**
C. **RAM-R: Reliability, Availability, Maintainability and Resiliency**
D. **Protection Level Assessment & Forecasting**

A. Infrstructure Risk

- Human Perceptions of Risk
- Threats (natural and manmade)
- Vulnerabilities
- Faults Taxonomy
- Service Outages
- Single Points of Failure
- Over-Concentration
- Risk as a *f(Severity, Likelihood)*
- Protection through fault prevention, tolerance, removal, and forecasting
- Best Practices

Human Perceptions of Risk

- Perceptions of “Rare Events”
- Users Demand Dependable Systems
- Dependable Systems are Expensive

Some Fun with Probability

- Which is more likely?
  1. Winning the “Big Lotto”
  2. Getting hit by lightning
  3. Being eviscerated/evaporated by a large asteroid over an 80-year lifetime

Some Fun with Probability

- Pick one:
    1. Winning the "Big Lotto"
    2. Getting hit by lightning
- *The chances are about the same*
- *One you have to pay for – the other is free*

Some Fun with Probability

3. Being eviscerated/evaporated by a large asteroid over an 80-year lifetime

– *Based upon empirical data, the chances are about 1 in a million**

*A. Snow and D. Straub, "Collateral damage from anticipated or real disasters: skewed perceptions of system and business continuity risk?",

Probability and People

- It is human nature that we perceive “good” events to be more likely and “bad” events to be less likely
- Until a bad event happens, that is

We Expect *Dependability* attributes from our Critical Infrastructure

- Reliability
- Maintainability
- Availability
- Resiliency[1]
- Data Confidentiality
- Data Integrity

[1]This perspective replaces "Safety" with "Resiliency". Attributes were first suggested in A. Avizienis, et al, "Basic Concepts & Taxonomy of Dependable & Secure Computing", *IEEE Transactions on Dependable & Secure Computing*, 2004

We Expect *Dependability* from our Critical Infrastructure

- Reliability
  - We expect our systems to fail very infrequently
- Maintainability
  - When systems do fail, we expect very quick recovery
- Availability
  - Knowing systems occasionally fail and take finite time to fix, we still expect the services to be ready for use when we need it

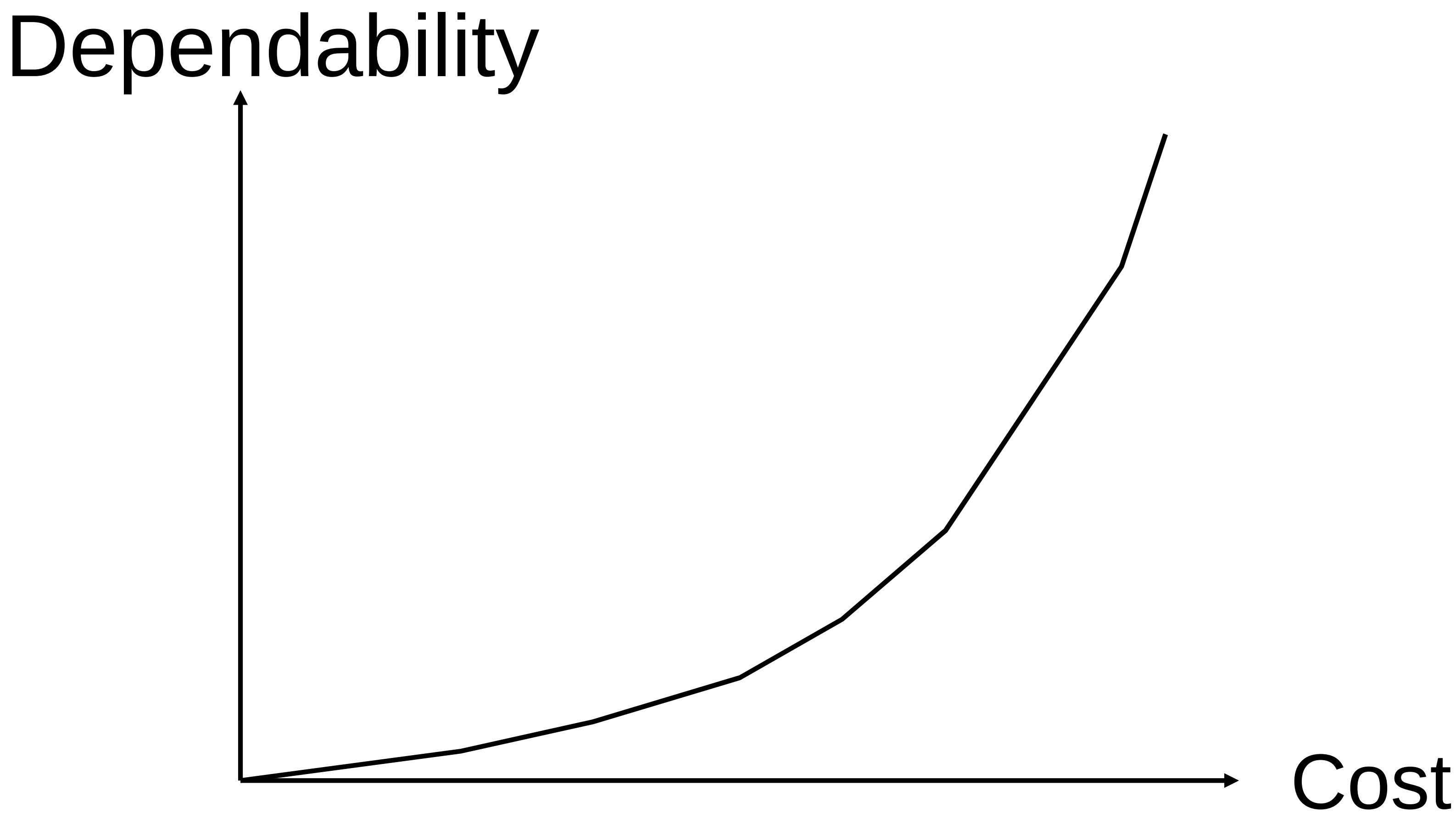
We Expect *Dependability* from our Critical Infrastructure (Continued)

- Resiliency
  - We expect our infrastructure not to fail cataclysmically
  - When major disturbances occur, we still expect organizational missions and critical societal services to still be serviced
- Data Confidentiality
  - We expect data to be accessed only by those who are authorized
- Data Integrity
  - We expect data to be deleted or modified only by those authorized

Are our Expectations Reasonable?

- Our expectations for dependable ICT systems are high
- So is the cost
- If you demand high dependability…………

Don’t Forget Your Wallet



Focus is often on More Reliable and Maintainable Components

- How to make things more <u>reliable</u>
  - Avoid single points of failure (e.g. over concentration to achieve economies of scale?)
  - Diversity
    - Redundant in-line equipment spares
    - Redundant transmission paths
    - Redundant power sources
- How to make things more <u>maintainable</u>
  - Minimize fault detection, isolation, repair/replacement, and test time
  - Spares, test equipment, alarms, staffing levels, training, best practices, transportation, minimize travel time
- What it takes --- lots orf capital and operational costs

Paradox

- We are fickle
- When ICT works, no one wants to spend $$ for unlikely events
- When an unlikely event occurs
  - We wish we had spent more
- Our perceptions of risk before and after catastrophes are key to societal behavior when it comes to ICT dependability

But Things Go Wrong!

- Central Office facility in Louisiana
  - Generators at ground level outside building
  - Rectifiers and Batteries installed in the basement
  - Flat land 20 miles from coast a few feet above sea level
  - Hurricane at high tide results in flood
  - Commercial AC lost, Generators inundated, basement flooded
  - Facility looses power, communications down
  - Fault tolerant architecture defeated by improper deployment

Fukushima Nuclear Accident

- Nuclear reactor cooling design required AC power
- Power Redundancy
  - Two sources of commercial power
  - Backup generators
  - Contingency plan if generators fail? Fly in portable generators
- Risks?
  - Power plant on coast a few meters above sea-level
  - Tsunamis: a 5 meter wall

Fukushima Nuclear Accident (Continued)

- Design vulnerabilities?
  - Nuclear plant requires AC Power for cooling
  - Tsunami wall 5 meters high, in a country where in the last 100 years numerous > 5 meter tsunamis occurred
  - Remarkably, backup generators at ground level (not on roofs !!!)
- Where do tsunamis come from?
  - Ocean floor earthquakes
- What can a severe land-based earthquake do?
  - Make man-made things fall, such as AC power lines

Sequence of Events: Fukushima Nuclear Accident

1. Large land based and ocean floor earthquake
   – AC transmission lines fall
   – Ten meter tsunami hits Fukushima
2. Backup Generators
   – Startup successfully, then
   – Flooded by tsunami coming over wall
3. Portable generators
   – Flown in
   – Junction box vault flooded
4. Nuclear reactors overheat, go critical, and explode

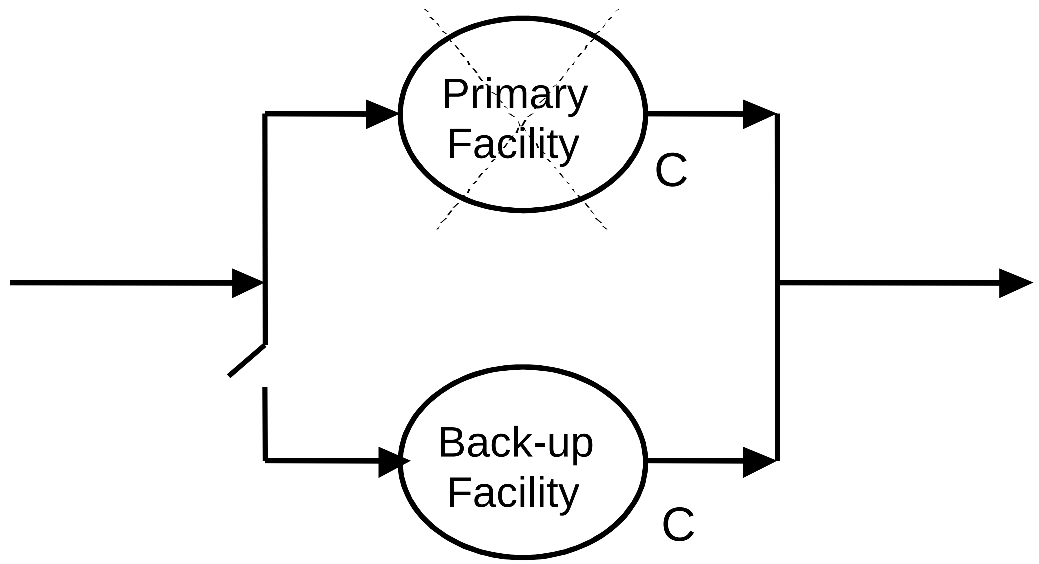
For 40 years, people walked by AC generators at ground level and a 5 meter tsunami wall !!!!

Assessing Risk is Difficult

- Severity
  - Economic impact
  - Geographic impact
  - Safety impact
- Likelihood
  - Vulnerabilities
  - Means and Capabilities
  - Motivations

9-11 Effect
Geographic Dispersal of Human and ITC Assets

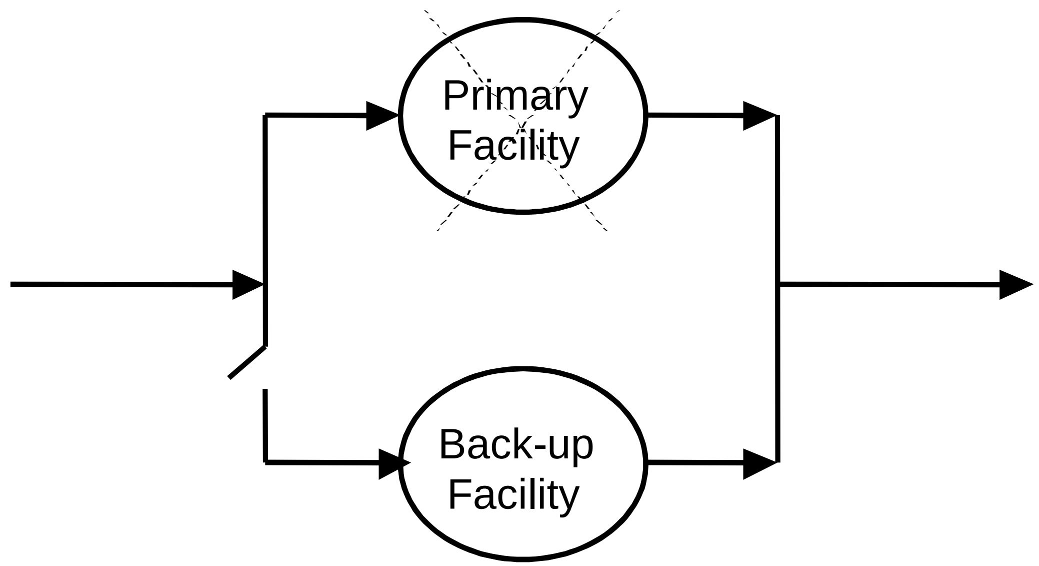
Pre 9-11 IT Redundancy



Cost~2C

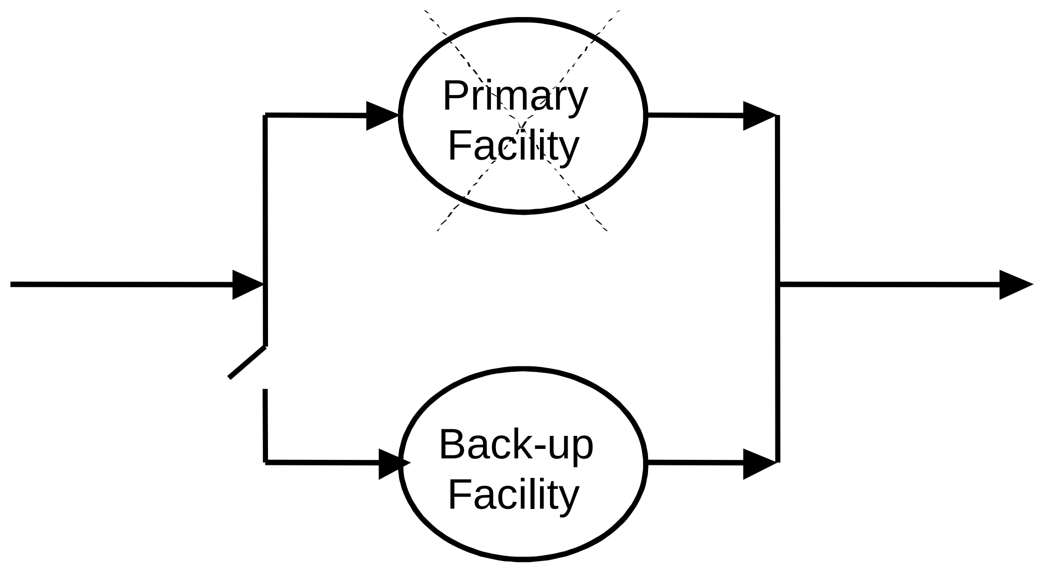
Scenario	Single IT Facility Reliability	Redundant IT Facility Reliability
1	0.90	0.9900
2	0.95	0.9950
3	0.99	0.9999

Key Assumptions



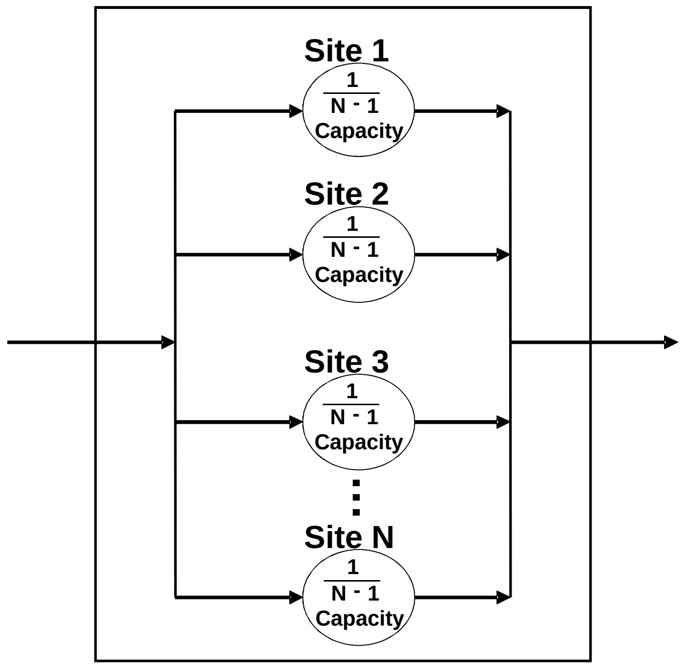
1. Failures are independent
2. Switchover capability is perfect

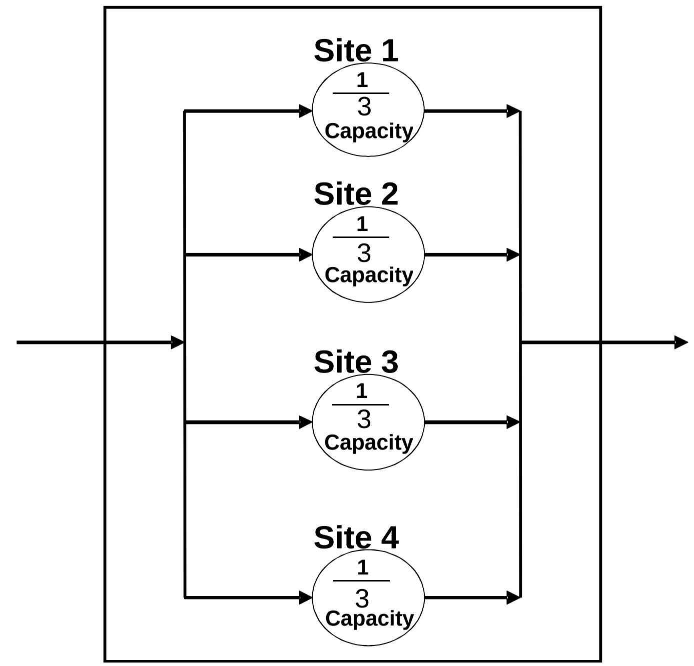
9-11: Some Organizations Violated These Assumptions



1. Failures not independent
   - Primary in WTC1
   - Backup in WTC1 or WTC2
2. Switchover capability disrupted
   - People injured or killed in WTC expected to staff backup facility elsewhere
   - Transportation and access problems

Post 9-11 IT Redundancy Perspectives





- No concentrations of people or systems to one large site
- Geographically dispersed human and IT infrastructure
- Geographic dispersal requires highly dependable networks
- Architecture possible with cloud computing !!

Geographic Dispersal

- A. Snow, D. Straub, R. Baskerville, C. Stucke, “The survivability principle: it-enabled dispersal of organizational capital”, in Enterprise Information Systems Assurance and System Security: Managerial and Technical Issues, Chapter 11, Idea Group Publishing, Hershey, PA, 2006.
- Cloud computing enables such approaches!!

Assessing Risk is Difficult

- Severity
  - Safety impact
  - Economic impact
  - Geographic impact
- Likelihood
  - Vulnerabilities
  - Means and Capabilities
  - Motivations

Infrastructure Protection and Risk

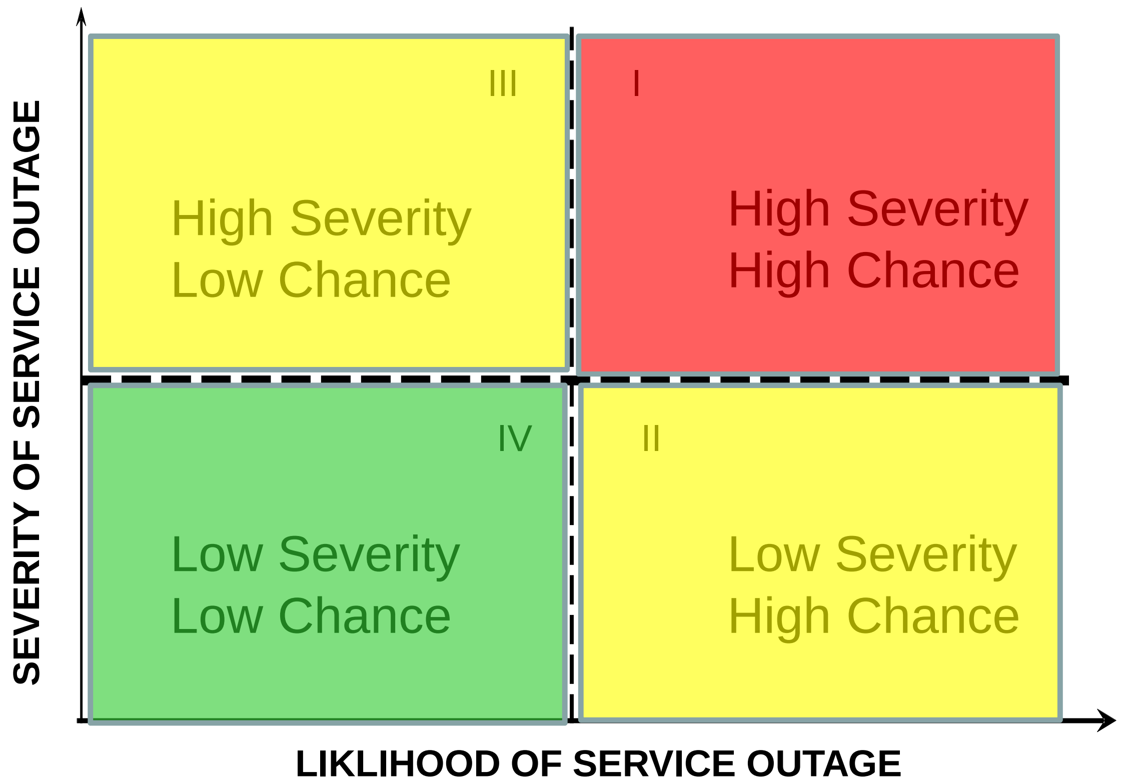
- Outages
- Severity
- Likelihood
- Fault Prevention, Tolerance, Removal and Forecasting

Infrastructure Protection and Risk

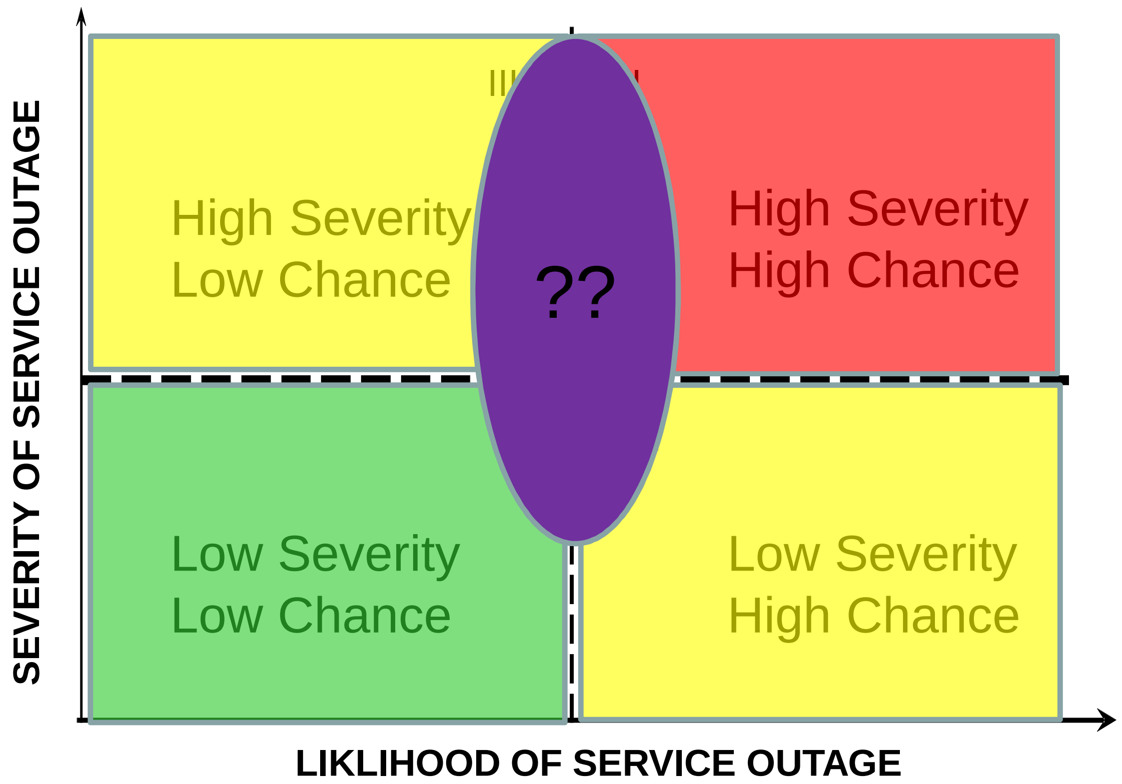
- Outages
- Severity
- Likelihood
- Fault Prevention, Tolerance, Removal and Forecasting

} RISK

Risk/Likelihood



Risk


High Severity
Low Chance
??
High Severity
High Chance
Low Severity
Low Chance
Low Severity
High Chance
SEVERITY OF SERVICE OUTAGE
LIKLIHOOD OF SERVICE OUTAGE

Vulnerabilities and Threats

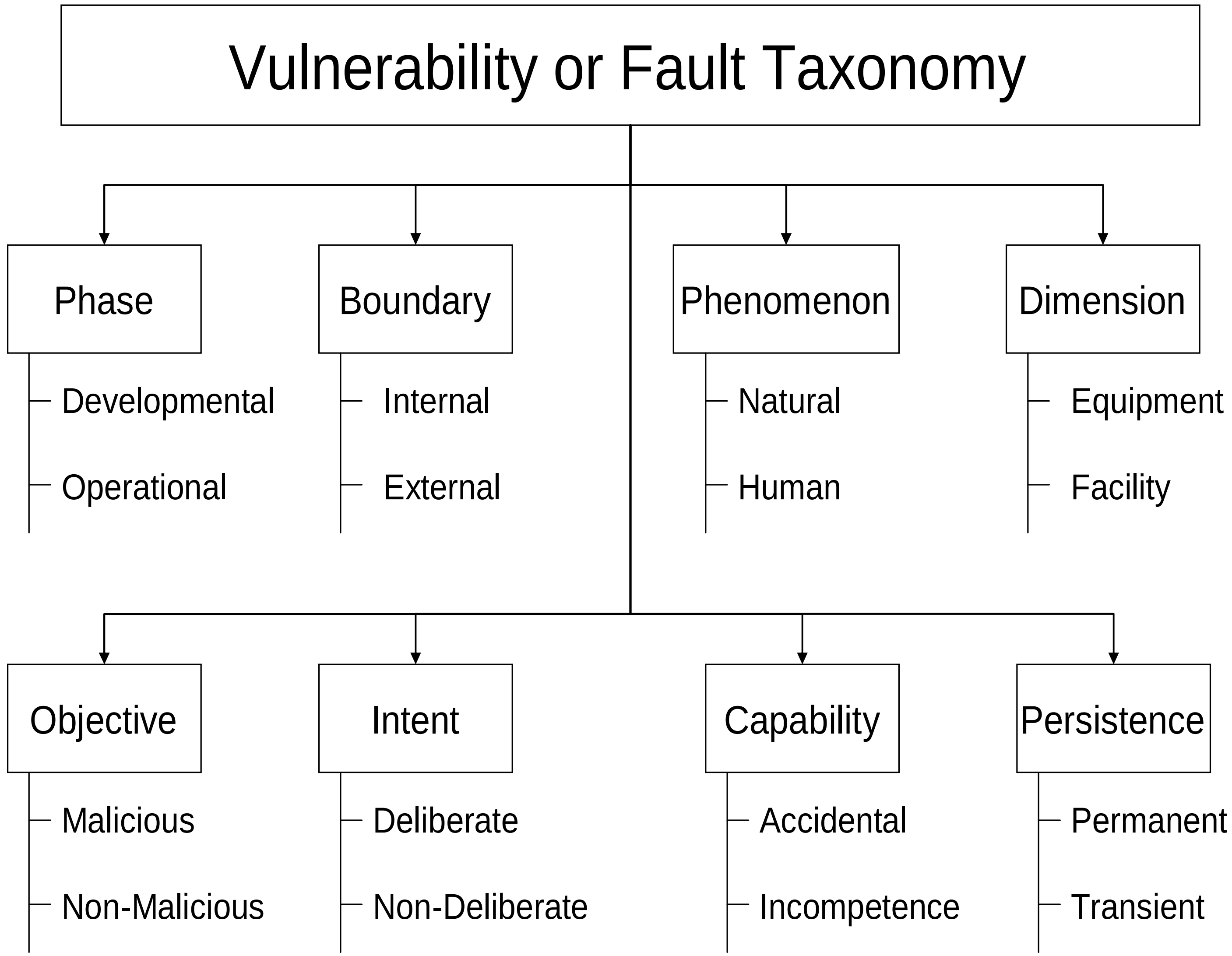
- *Vulnerability* is a weakness or a state of susceptibility which opens up the infrastructure to a possible outage due to attack or circumstance.
- The cause of a triggered vulnerability, or error state, is a system *fault*.
- The potential for a vulnerability to be exploited or triggered into a disruptive event is a *threat*.
- Vulnerabilities, or faults, can be exploited intentionally or triggered unintentionally

Proactive Fault Management

- Fault Prevention by using design, implementation, and operations rules such as standards and *industry best practices*
- Fault Tolerance techniques are employed, wherein equipment/process failures do not result in service outages because of fast switchover to equipment/process redundancy
- Fault Removal through identifying faults introduced during design, implementation or operations and taking remediation action.
- Fault Forecasting where the telecommunication system fault behavior is monitored from a quantitative and qualitative perspective and the impact on service continuity assessed.

Threats and Vulnerabilities

- Natural Threats
  - Water damage
  - Fire damage
  - Wind damage
  - Power Loss
  - Earthquake damage
  - Volcanic eruption damage
- Human Threats
  - Introducing or triggering vulnerabilities
  - Exploiting vulnerabilities (hackers/crackers, malware introduction)
  - Physical Vandalism
  - Terrorism and Acts of War
- Fault Taxonomy


Vulnerability or Fault Taxonomy
Phase
Developmental
Operational
Boundary
Internal
External
Phenomenon
Natural
Human
Dimension
Equipment
Facility
Objective
Malicious
Non-Malicious
Intent
Deliberate
Non-Deliberate
Capability
Accidental
Incompetence
Persistence
Permanent
Transient

Reference

- A. Avizienis, et al, “Basic Concepts & Taxonomy of Dependable & Secure Computing”, *IEEE Transactions on Dependable & Secure Computing*, 2004.

Case Study – Danger Index

- **Snow, Weckman & Hoag, "Understanding Danger to Critical Telecom Infrastructure: A Risky Business",** ***International Conference on Networks 2009 (ICN09),*** **IEEE Communications Society Press, March 2009.**

Danger

- Malicious acts aimed directly against humans, or indirectly at their critical infrastructures is a real and present danger
- However, most compromises to ICT critical infrastructure are often accidental and non-malicious
- How can we quantify the danger??
  - Not easily

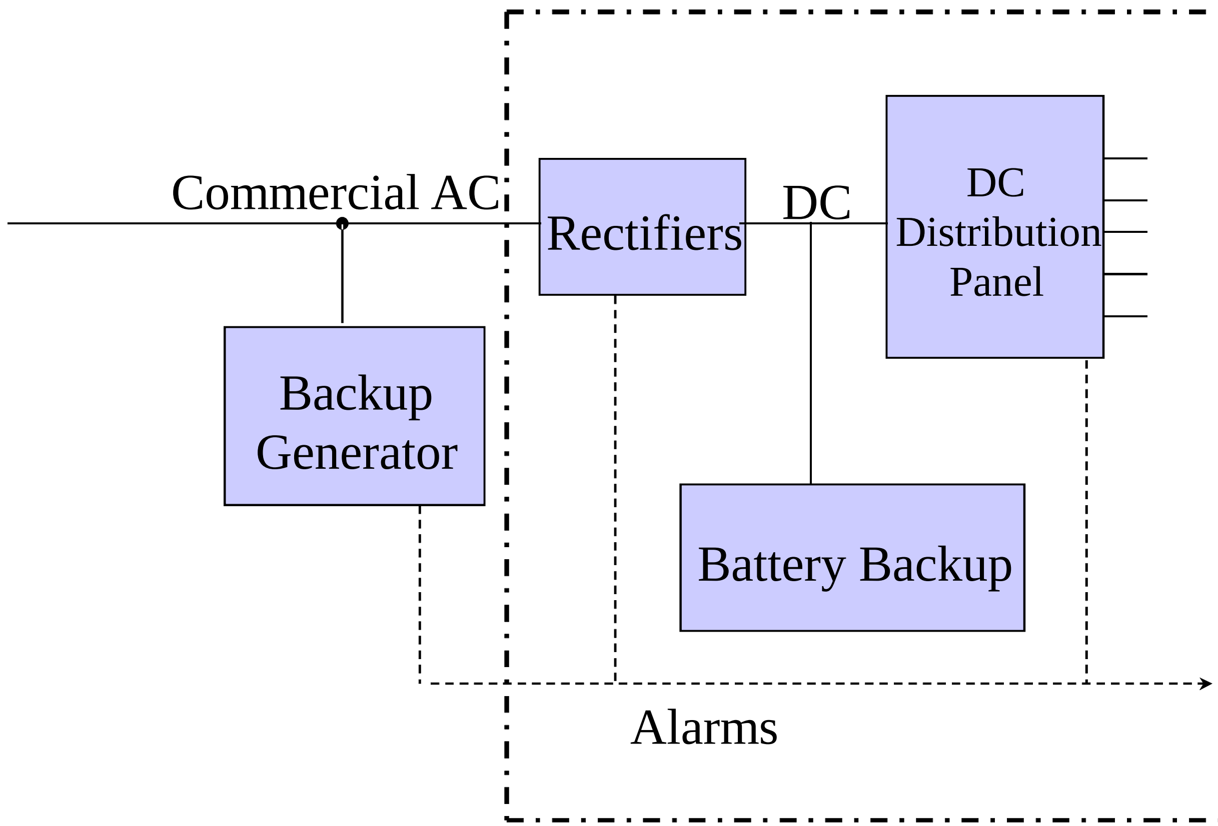
September 11, 2001

- A large telecommunications outage resulted from the collapse of the world trade centers
  - Over 4,000,000 data circuits disrupted
  - Over 400,000 local switch lines out
- Pathology of the event
  - Towers collapsed
  - Some physical damage to adjacent TCOM building
  - Water pipes burst, and in turn disrupted TCOM facility power and power backup facilities
- What was the a priori probability of such an event and ensuing sequence?
  - P = Pr{ Successful hijack} x Pr{ Building Collapse} x Pr{ Water Damage}
  - Infinitesimal??

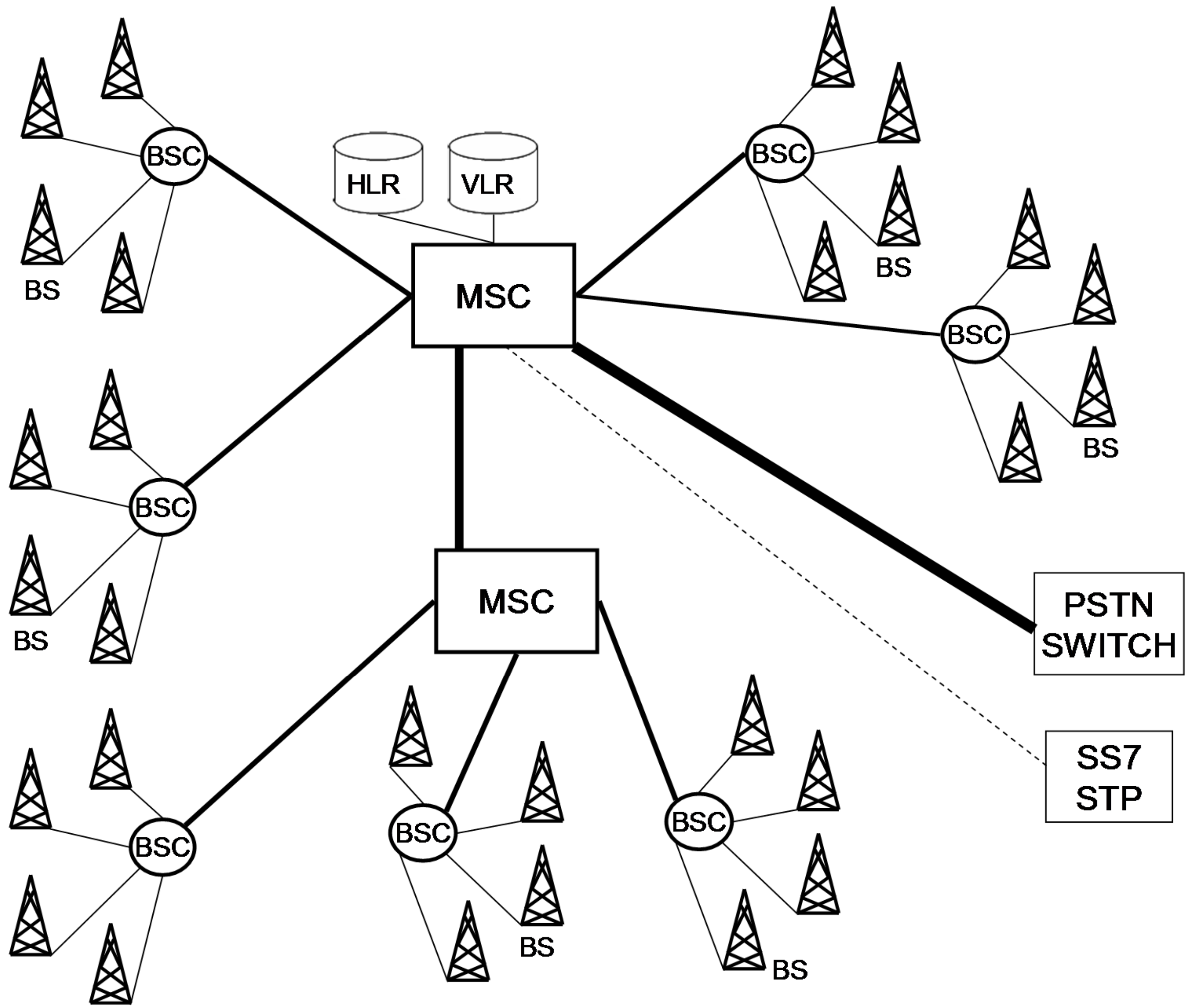
Probabilities

- Risk assessments requiring “probabilities” have little utility for rare events
- Why? Can’t rationally assess probability
- Such probabilistic analysis attempts may also diminish focus of the root cause of the outage, and may detract from remediating vulnerabilities
- In the 9-11 case the issue was one of TCOM “over-concentration” or creation of a large SPF

Typical TCOM Power



PCS Architecture



B. Telecommunications Infrastructure

- Wireline architecture and vulnerabilities
- Wireless architecture and vulnerabilities
- Cable architecture and vulnerabilities

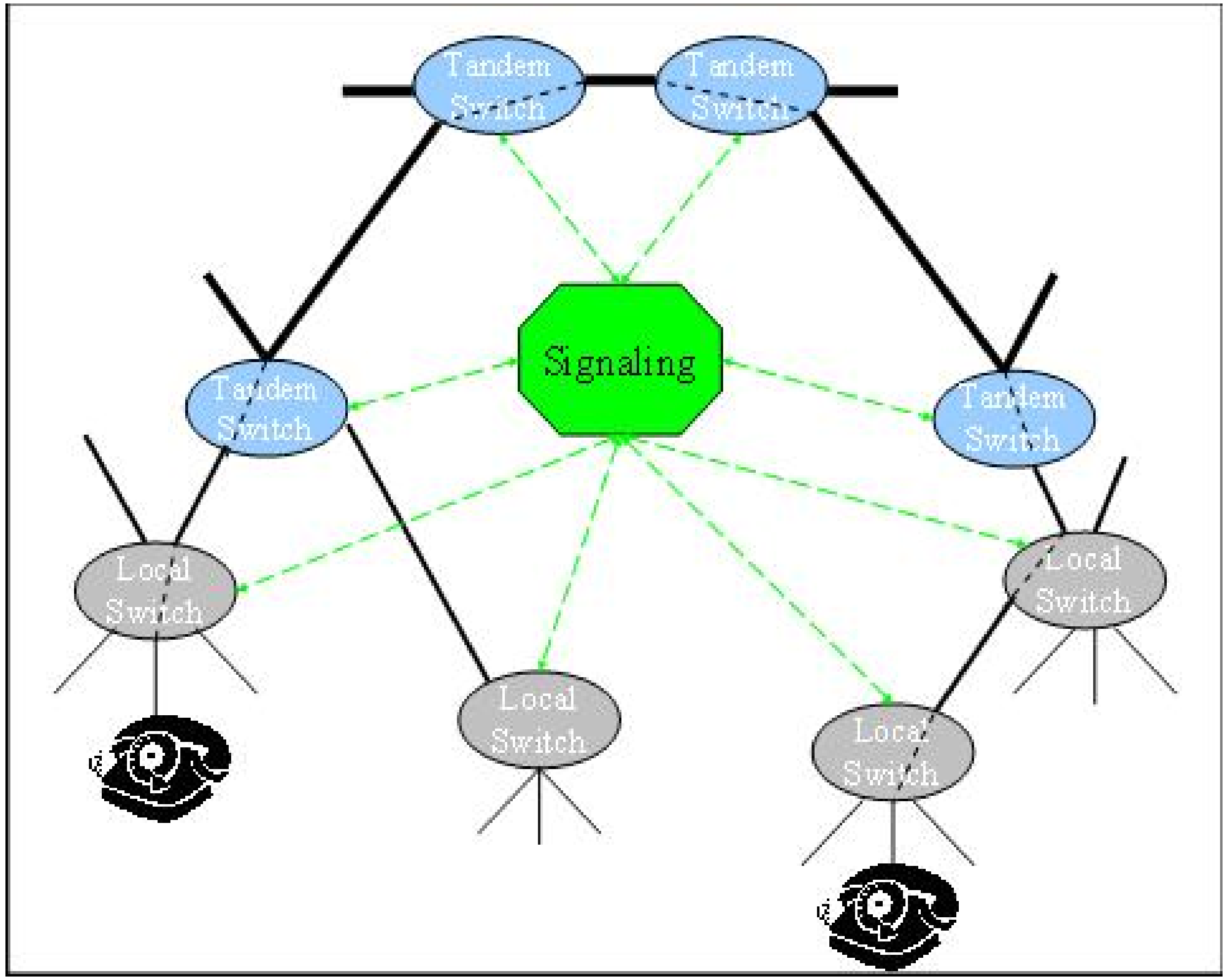
Outline

A. **ICT Infrastructure Risk**
B. ***Examples of ICT Network Infrastructure***
C. **RAM-R: Reliability, Availability, Maintainability and Resiliency**
D. **Protection Level Assessment & Forecasting**

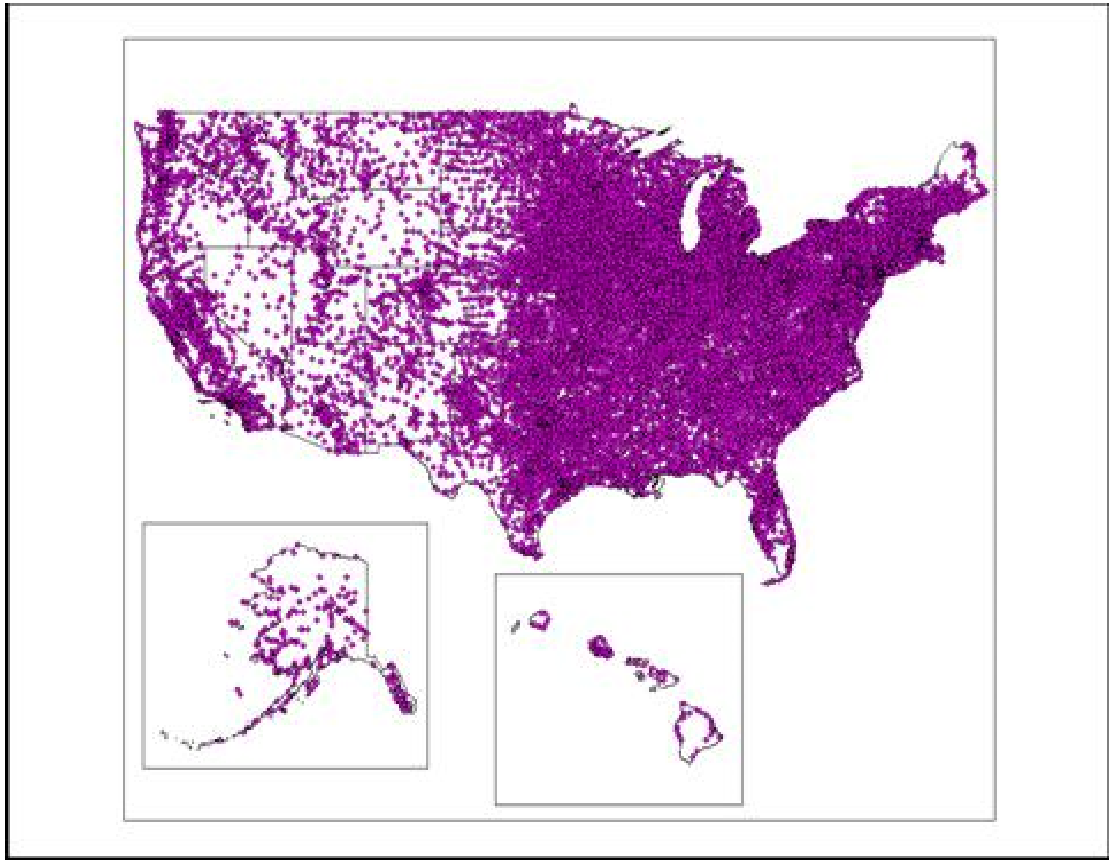
Public Switched Telephone Network

- Architecture
- Local and Tandem Switching
- Transmission
- Signaling & SS7
- Power
- Vulnerabilities

PSTN End to End Connections

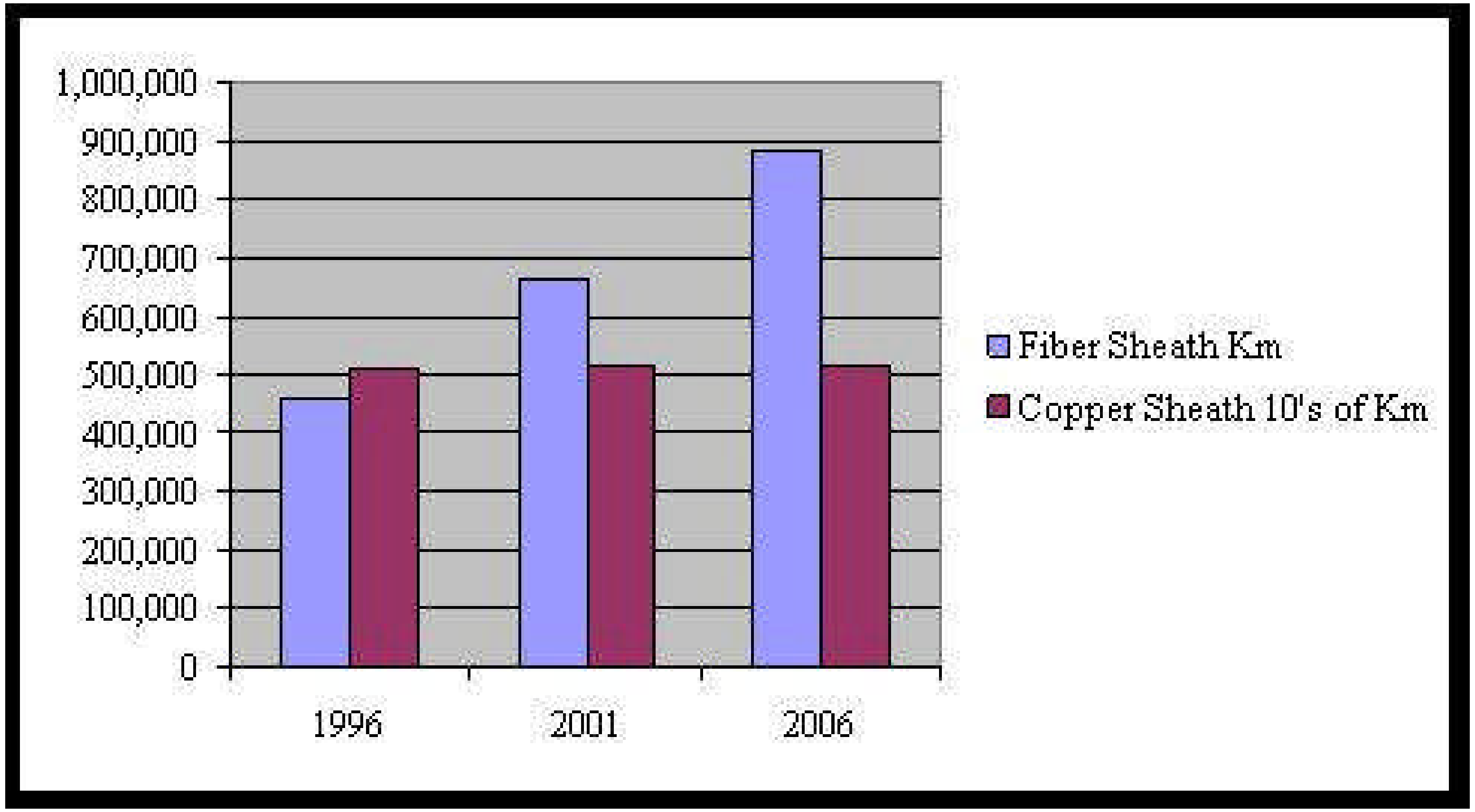


Switching Infrastructure Dispersal/Concentration



Retrieved from Wikipedia November 7, 2007.
http://en.wikipedia.org/wiki/Image:Central_Office_Locations.png

US Growth in Fiber



Transmission Vulnerabilities

- Fiber cuts with non-protected transmission systems
- Fiber over Bridges
- Fiber transmission failures inside carrier facilities
- Digital Cross Connect Systems
- Local Loop Cable Failures

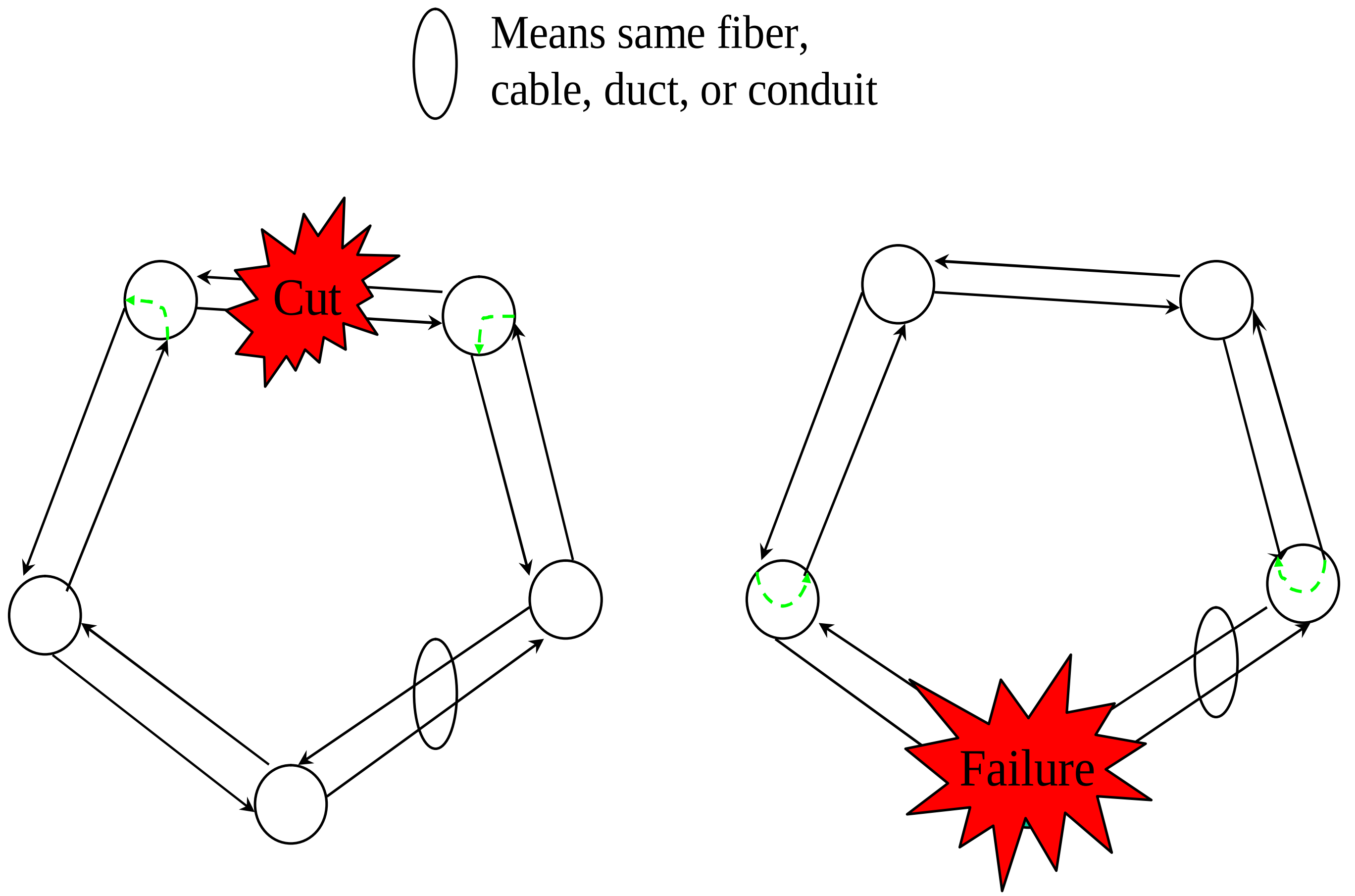
Transmission Vulnerabilities

- Fiber cuts with non-protected transmission systems:
  - No backup path/circuits deployed.
  - Often done for economic reasons
  - In urban areas where duct space is at a premium
  - In rural areas where large distances are involved.
- Fiber over Bridges:
  - Fiber is vulnerable when it traverses bridges to overcome physical obstacles such as water or canyons
  - There have been reported instances of fires damaging cables at these points

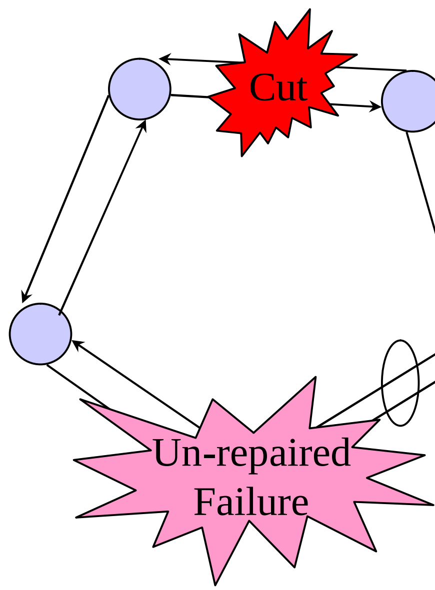
Transmission Vulnerabilities

- Fiber transmission failures inside carrier facilities:
  - Studies have demonstrated that the majority of fiber transmission problems actually occur inside carrier facilities
  - Caused by installation, and maintenance activities.
- Digital Cross Connect Systems:
  - Although hot standby protected equipment, DACSs have failed taking down primary and alternate transmission paths.
  - These devices represent large impact SPFs.
- Local Loop Cable Failures:
  - In some instances, construction has severed multipair cable, or cable sheaths have become flooded
  - Require long duration splicing or replacement

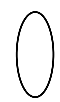
Proper SONET Ring Operation



Improper Operation of SONET Rings

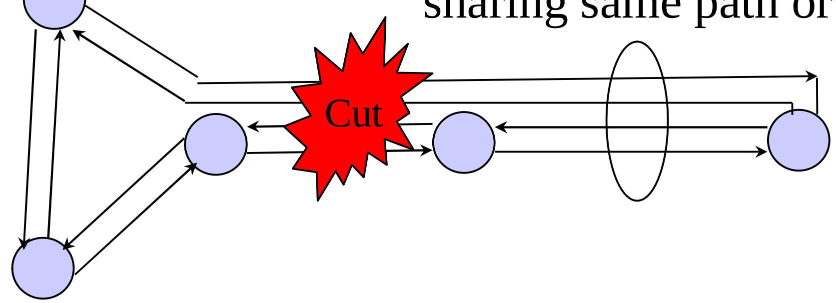


<u>Improper Maintenance:</u>
Node’s previous failure, and subsequent fiber cut prior to spare on hand

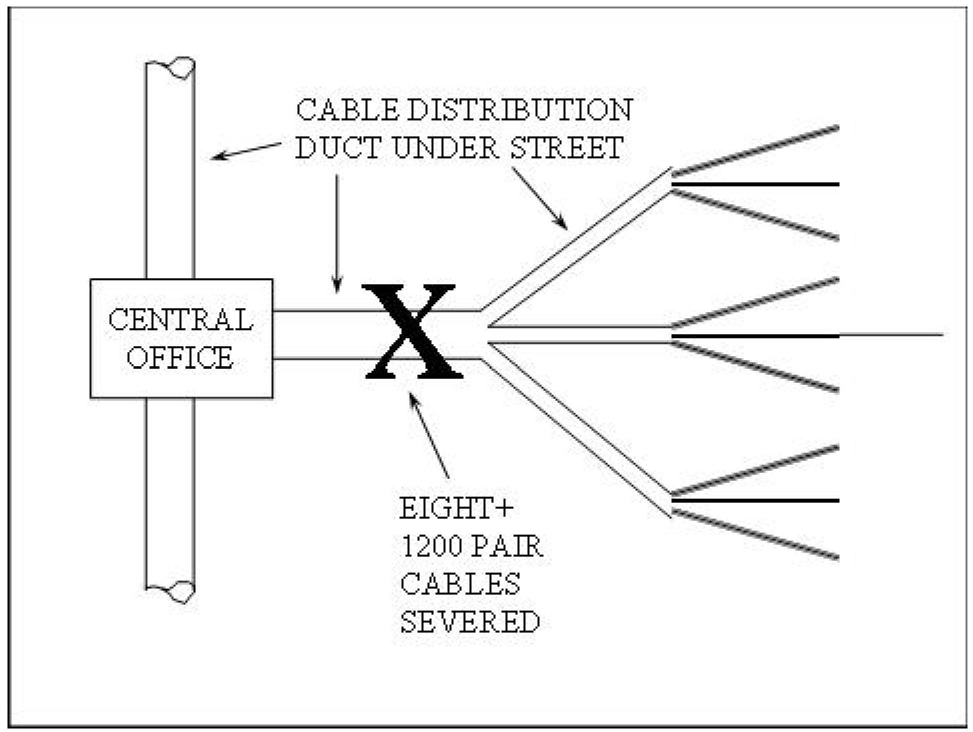


Means same fiber,
cable, duct, or conduit

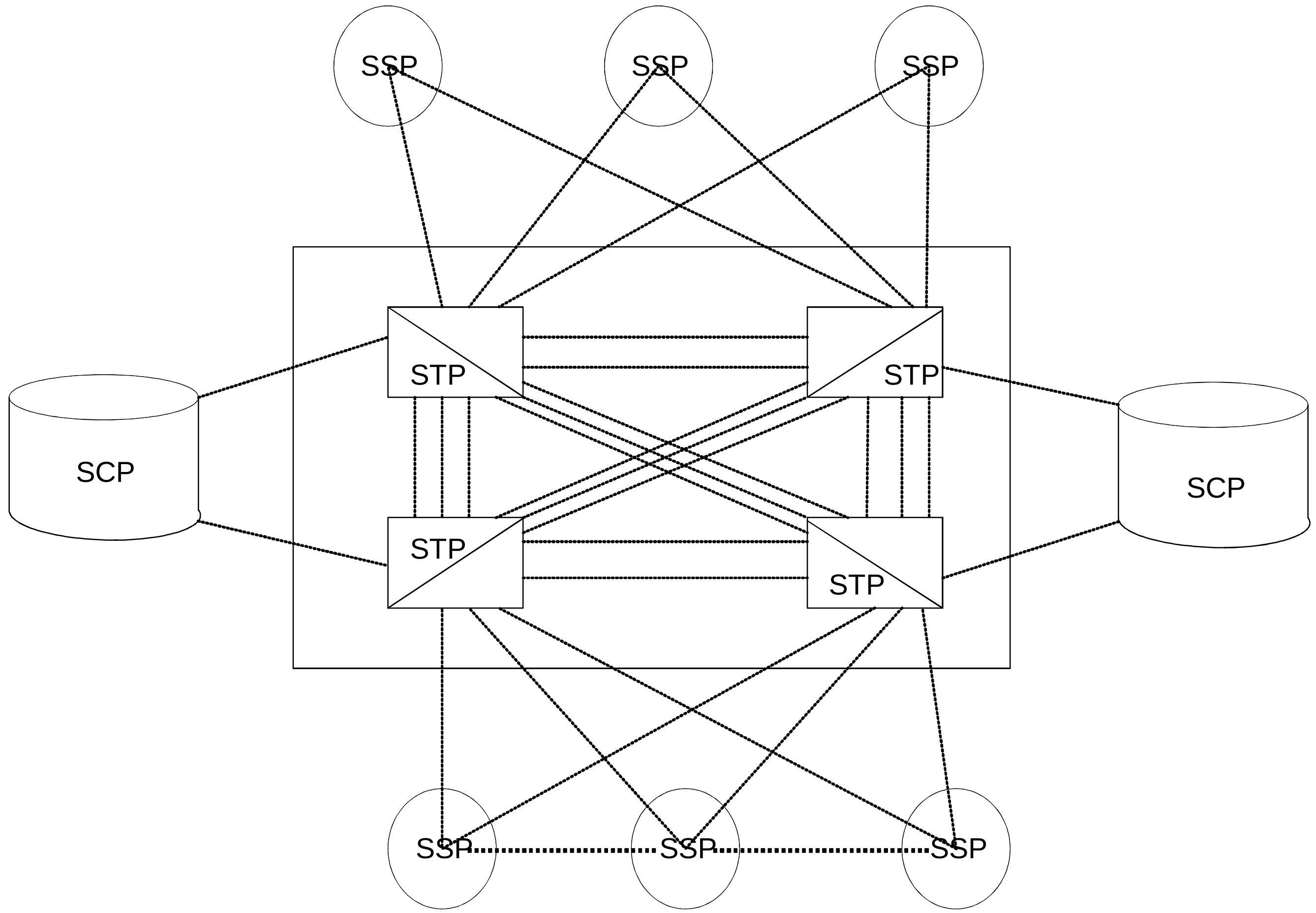
<u>Improper Deployment:</u>
“Collapsed” or “Folded” Ring sharing same path or conduit



Outside Plant Vulnerable Near Central Offices



SS7 Architecture



------- A, B, or C, or F Transmission Link

SSP: Signaling Service Point (Local or Tandem Switch)

STP: Signal Transfer Point (packet Switch Router)

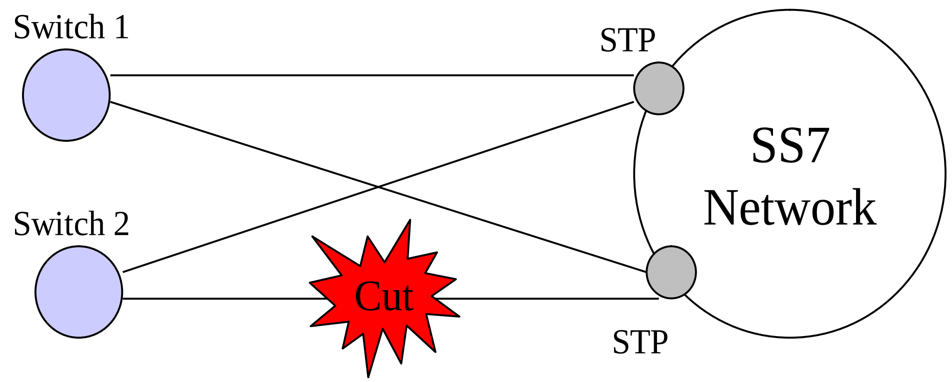
SCP: Service Control Point

SS7 Vulnerabilities

- <u>Lack of A-link path diversity</u>: Links share a portion or a complete path
- <u>Lack of A-link transmission facility diversity</u>: A-links share the same high speed digital circuit
- <u>Lack of A-link power diversity</u>: A-links are separate transmission facilities, but share the same power circuit
- <u>Lack of timing redundancy</u>: A-links are digital circuits that require external timing. This should be accomplished by redundant timing sources.
- <u>Commingling SS7 link transmission with voice trunks and/or alarm circuits</u>: It is not always possible to allocate trunks, alarms and A-links to separate transmission facilities.

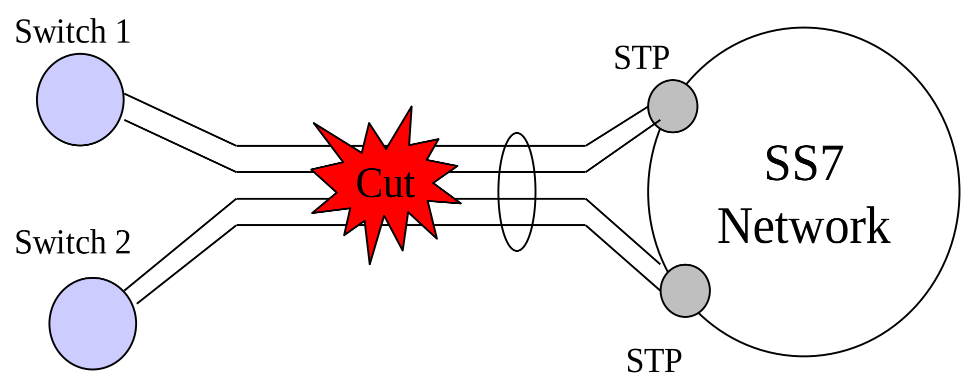
SS7 A-Links

Proper Deployment

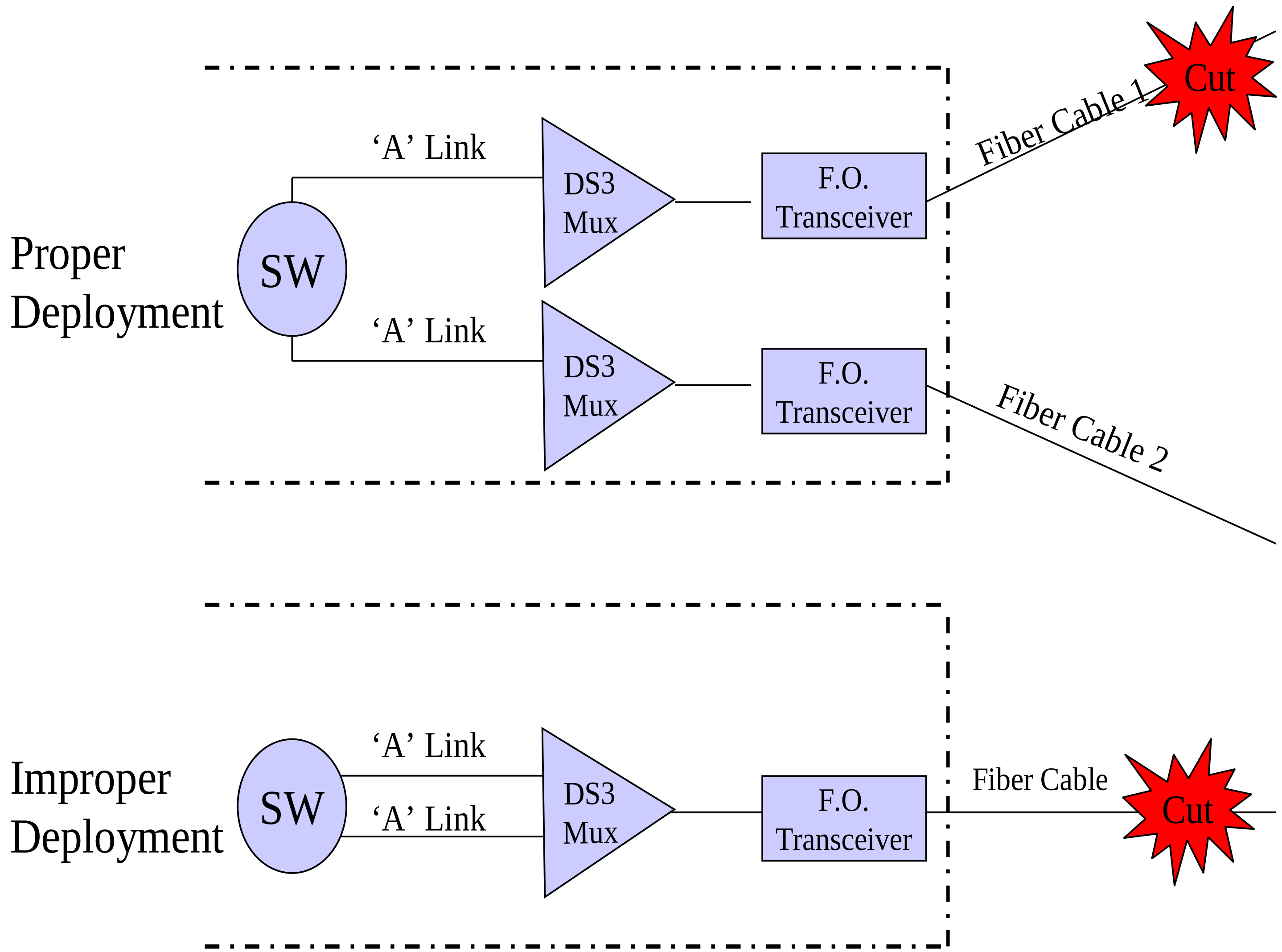


Means same fiber, cable, duct, or conduit

Improper Deployment

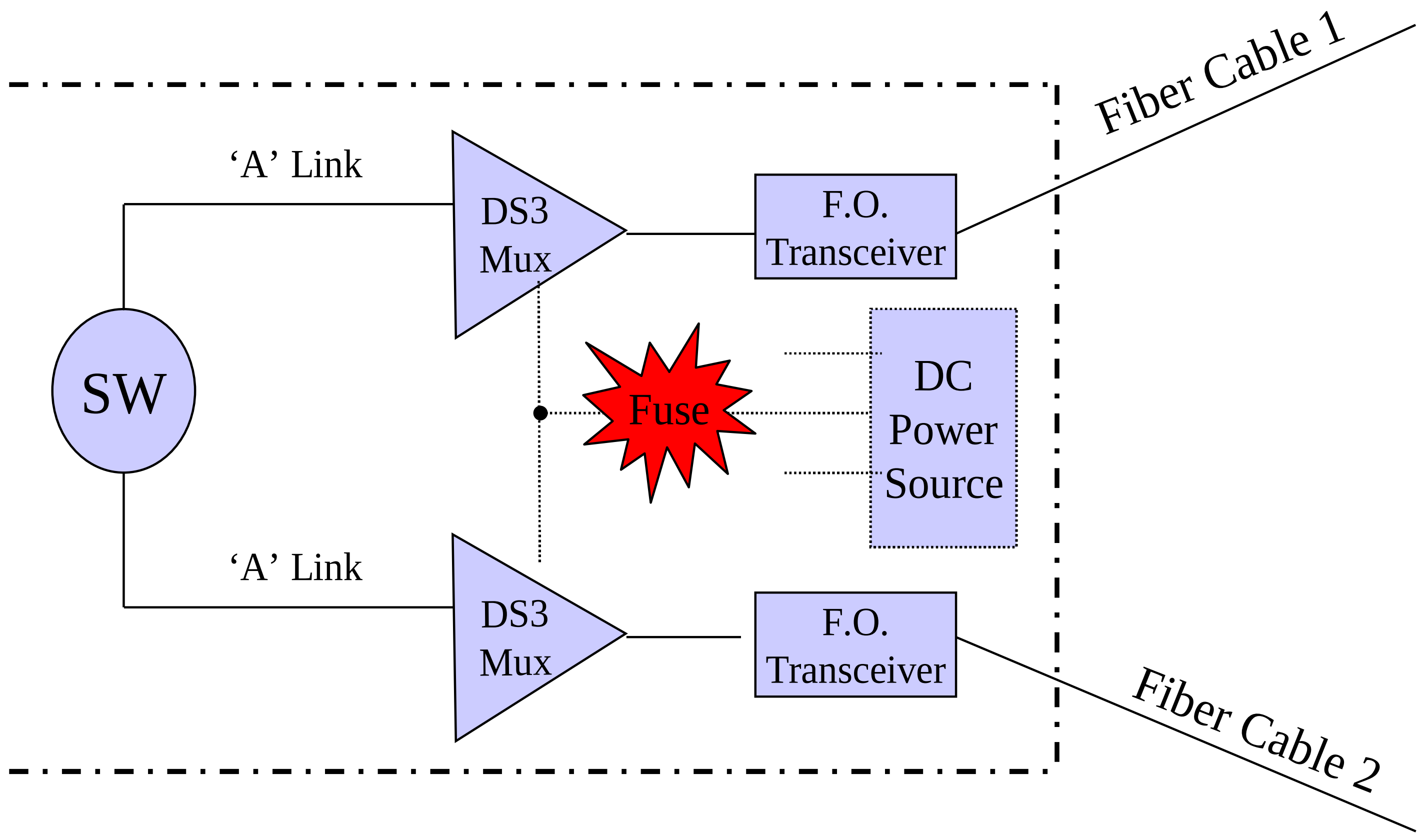


SS7 A-Links



Proper Deployment
SW
'A' Link
'A' Link
DS3 Mux
DS3 Mux
F.O. Transceiver
F.O. Transceiver
Fiber Cable 1
Cut
Fiber Cable 2
Improper Deployment
SW
'A' Link
'A' Link
DS3 Mux
F.O. Transceiver
Fiber Cable
Cut

SS7 A-Links



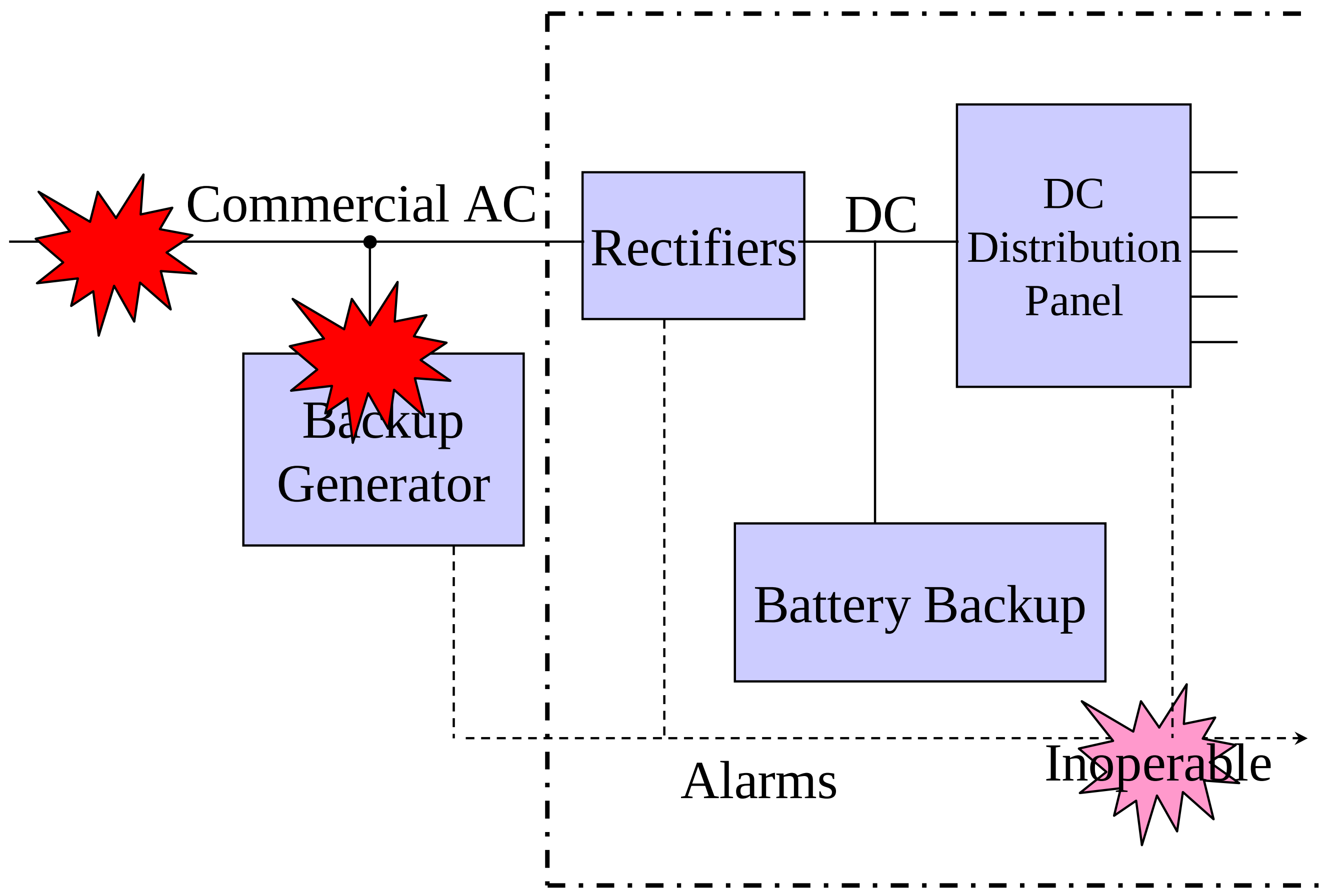
Fiber Cable 1
'A' Link
DS3
Mux
F.O.
Transceiver
SW
Fuse
DC
Power
Source
'A' Link
DS3
Mux
F.O.
Transceiver
Fiber Cable 2

Power Architecture & Vulnerabilities

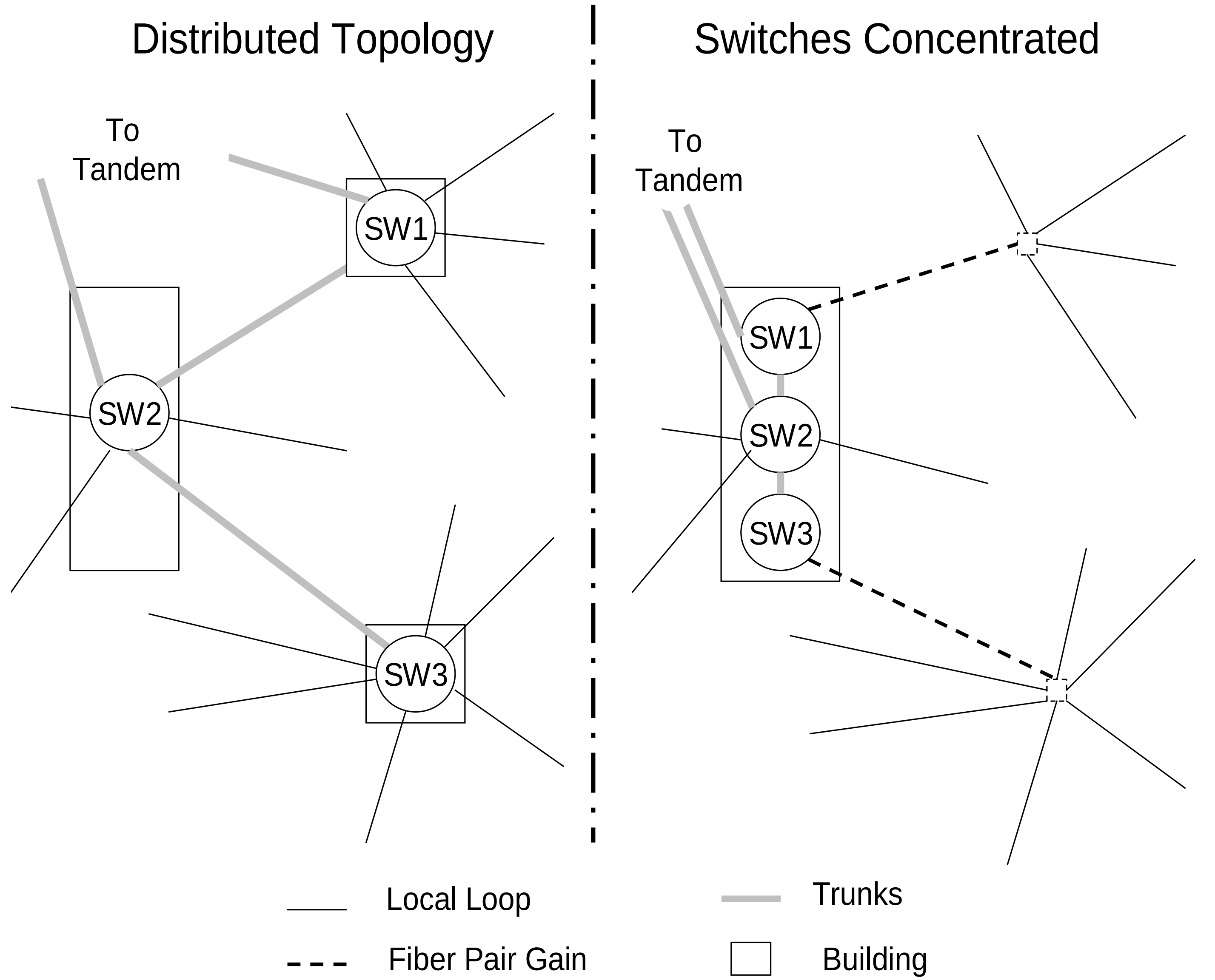
- Redundant Power
  - Commercial AC
  - AC Generator
  - Batteries

Inoperative Alarms

- Loss of commercial power
- Damaged generator
- Untested or inoperable alarms prior to loss and damage
- Batteries Deplete



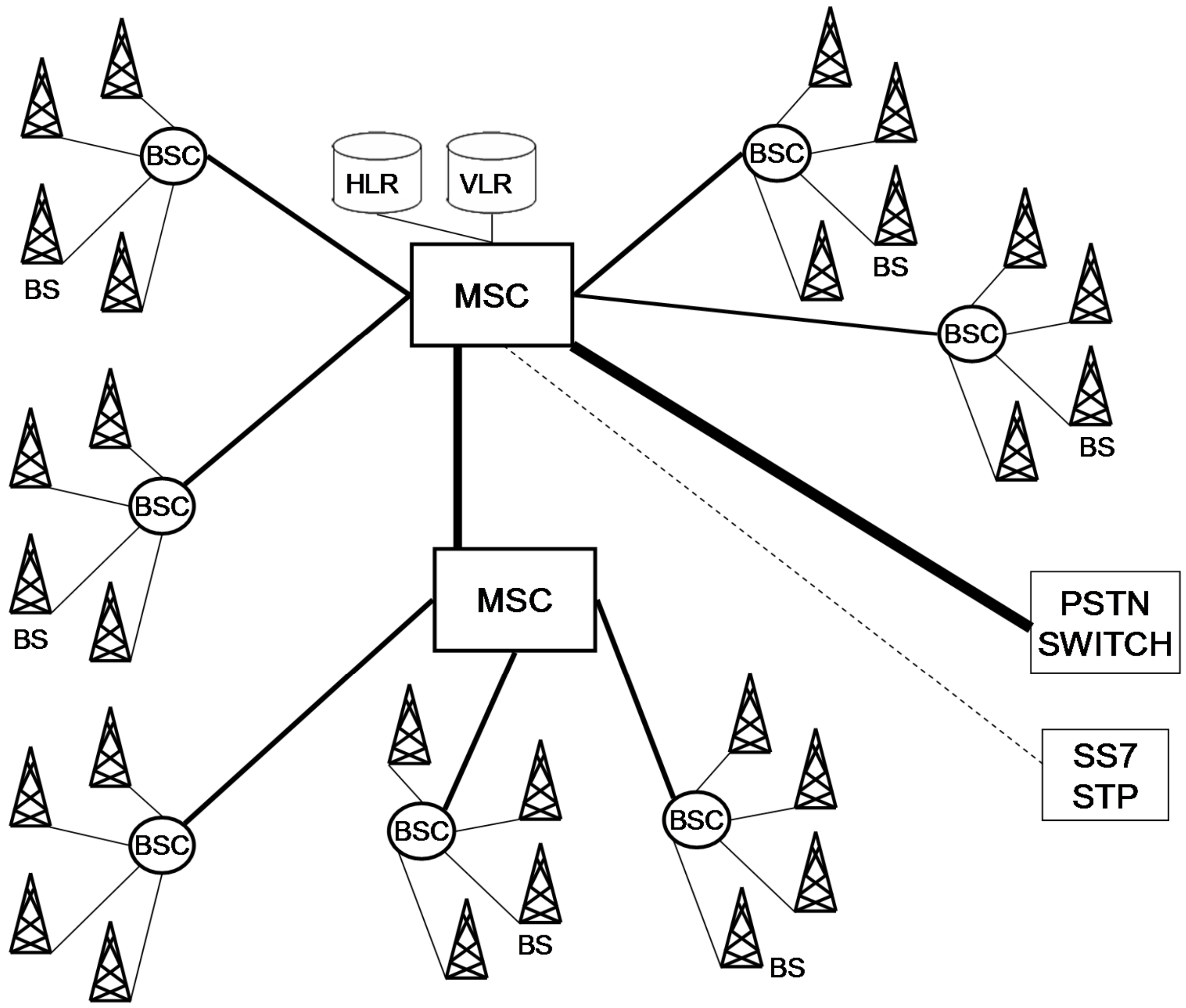
Economy of Scale Over-Concentration Vulnerabilities



Wireless Personal Communication Systems

- Architecture
- Mobile Switching Center
- Base Station Controllers
- Base Stations
- Inter-Component Transmission
- Vulnerabilities

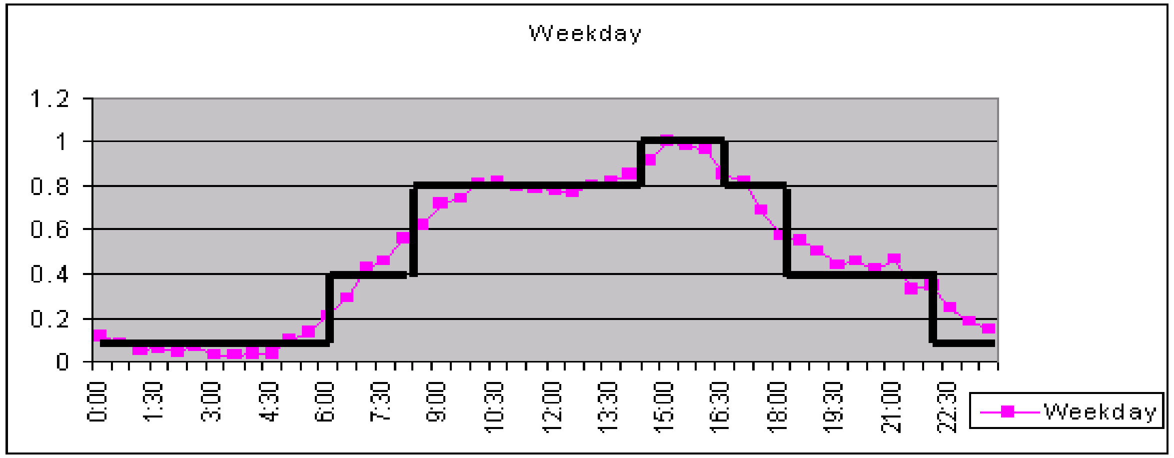
PCS Architecture

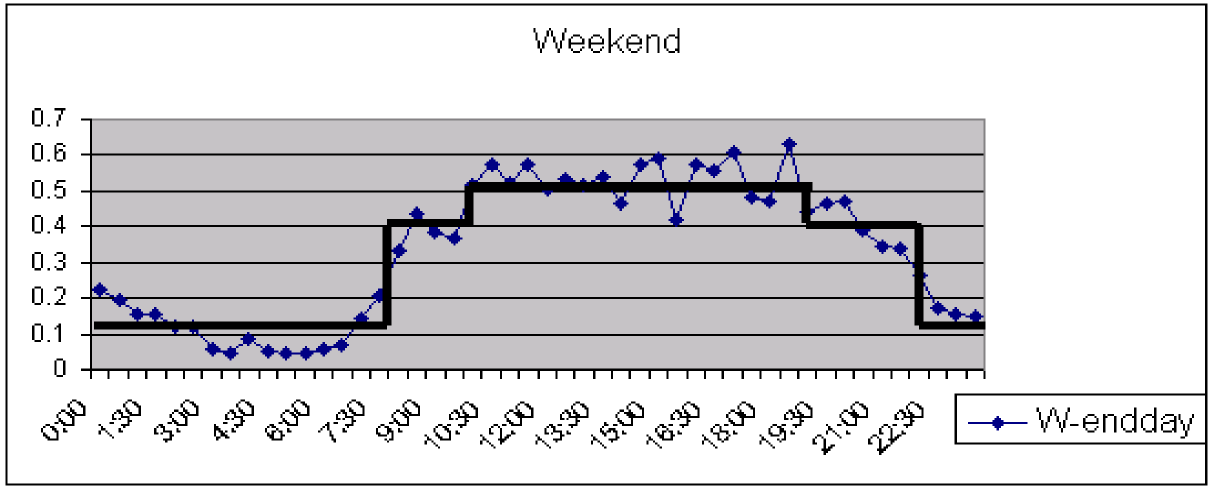


PCS Component Failure Impact
Wireless Infrastructure Building Block (WIB)

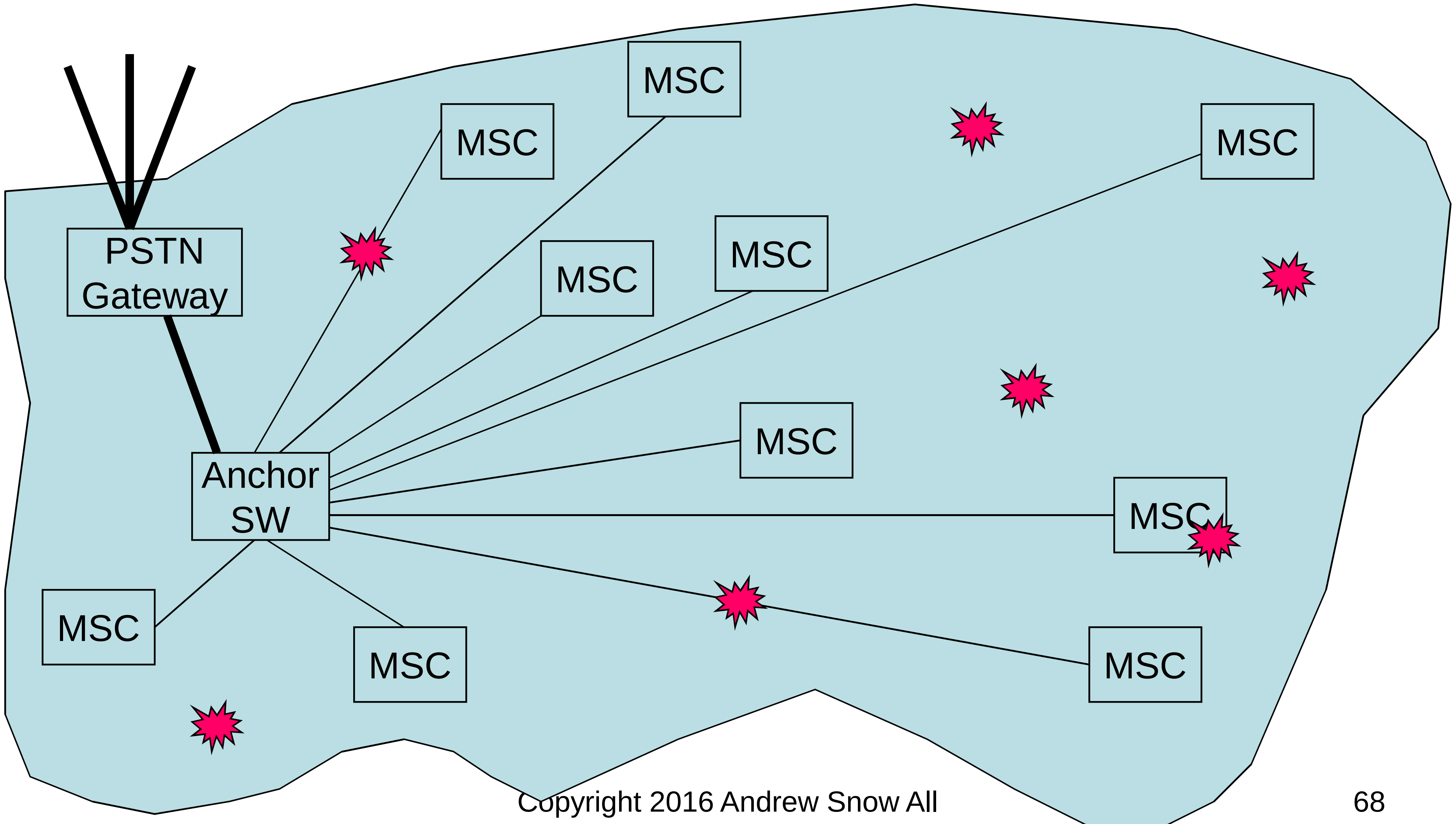
Components	Users Potentially Affected
Database	100,000
Mobile Switching Center	100,000
Base Station Controller	20,000
Links between MSC and BSC	20,000
Base Station	2,000
Links between BSC and BS	2,000

Outages at Different Times of Day Impact Different Numbers of People



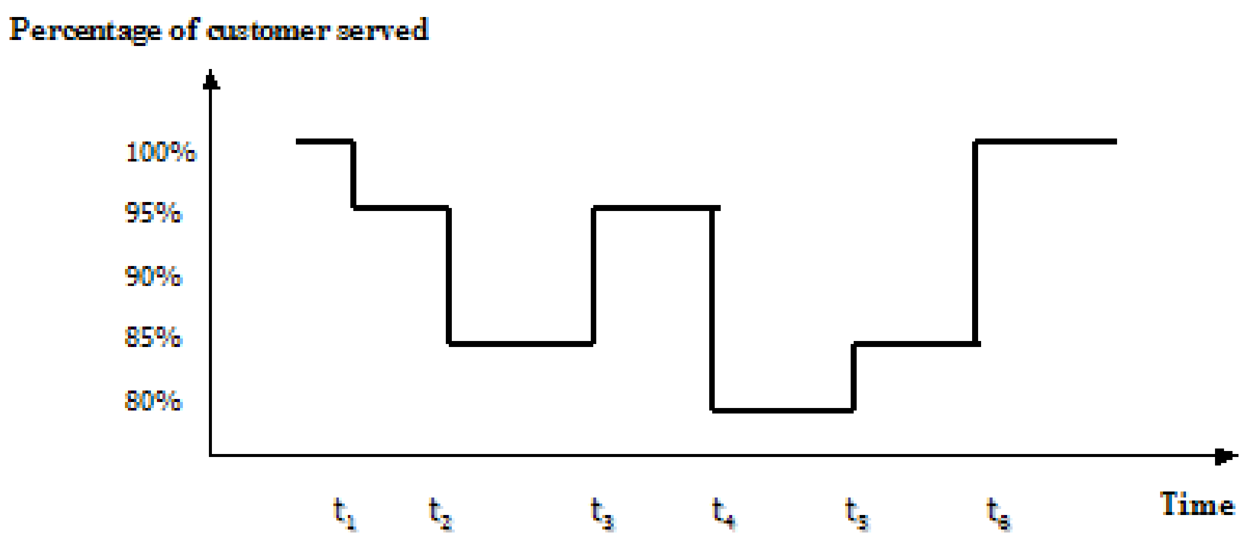


Concurrent Outages are a Challenge for Network Operators



Episodic Outage Events

- Episodes defined as events when either
  - A Single outage occurs, or
  - Multiple concurrent outages are ongoing



Distribution of Multi-outage Episodes over One Year

No. Outages in Epoch	Number of WIB				
	2 (200K)	**4 (400K)**	**6 (600K)**	**8 (800K)**	**10 (1 M)**
1	105	191	254	304	342
2	4	18	38	54	77
3	0	2	7	14	21
4	0	0	1	3	5
5	0	0	0	0	1
6	0	0	0	0	0
7	0	0	0	0	0

,

Andy Snow, Yachuan Chen, Gary Weckman, "The Impact of Multi-Outage Episodes on Large-Scale Wireless Voice Networks, "The International Journal on Networks and Services, vol 5, no 3&4,pages: 174 – 188, 2012, IARIA.

Outline

A. **ICT Infrastructure Risk**
B. **ICT Network Infrastructure**
C. ***RAM-R: Reliability, Availability, Maintainability and Resiliency***
D. **Protection Level Assessment & Forecasting**

RAMS

- Reliability – *f(MTTF)*
- Maintainability – *f(MTTR)*
- Availability – *f(MTTF, MTTR)*
- Resiliency -- *f(MTTF, MTTR, Severity)*
- Rresiliency Metrics and Thresholds
- User vs System Administrator Perspectives

Reliability

- *Reliability* is the chance equipment or a service will operate as intended in its environment for a specified period of time.
- A function of the mean time to failure (MTTF) of the equipment or service.
- Reliability deals with:
  - "How often can we expect this equipment/service to not fail", or,
  - "What is the expected lifetime of the equipment/service"?

Mean Time To Failure (MTTF)

- How do we get it?
  - If equipment/service has been fielded, the MTTF is the arithmetic mean of the observed times to fail.
  - If it not yet fielded, it is the predicted lifetime.
- There is a very simple way to calculate the reliability, if arrivals are a Poisson process (i.i.d and exponentially distributed:

$$R = e^{-\lambda \cdot t} \qquad \lambda = \frac{1}{MTTF}$$

- *R* is the reliability, or the chance the service/component will be operational for time *t*. Lamda known as the failure rate, or reciprocal of the MTTF.
- If lamda is constant, exponentially distributed arrival assumption is conservative.

Reliability Example

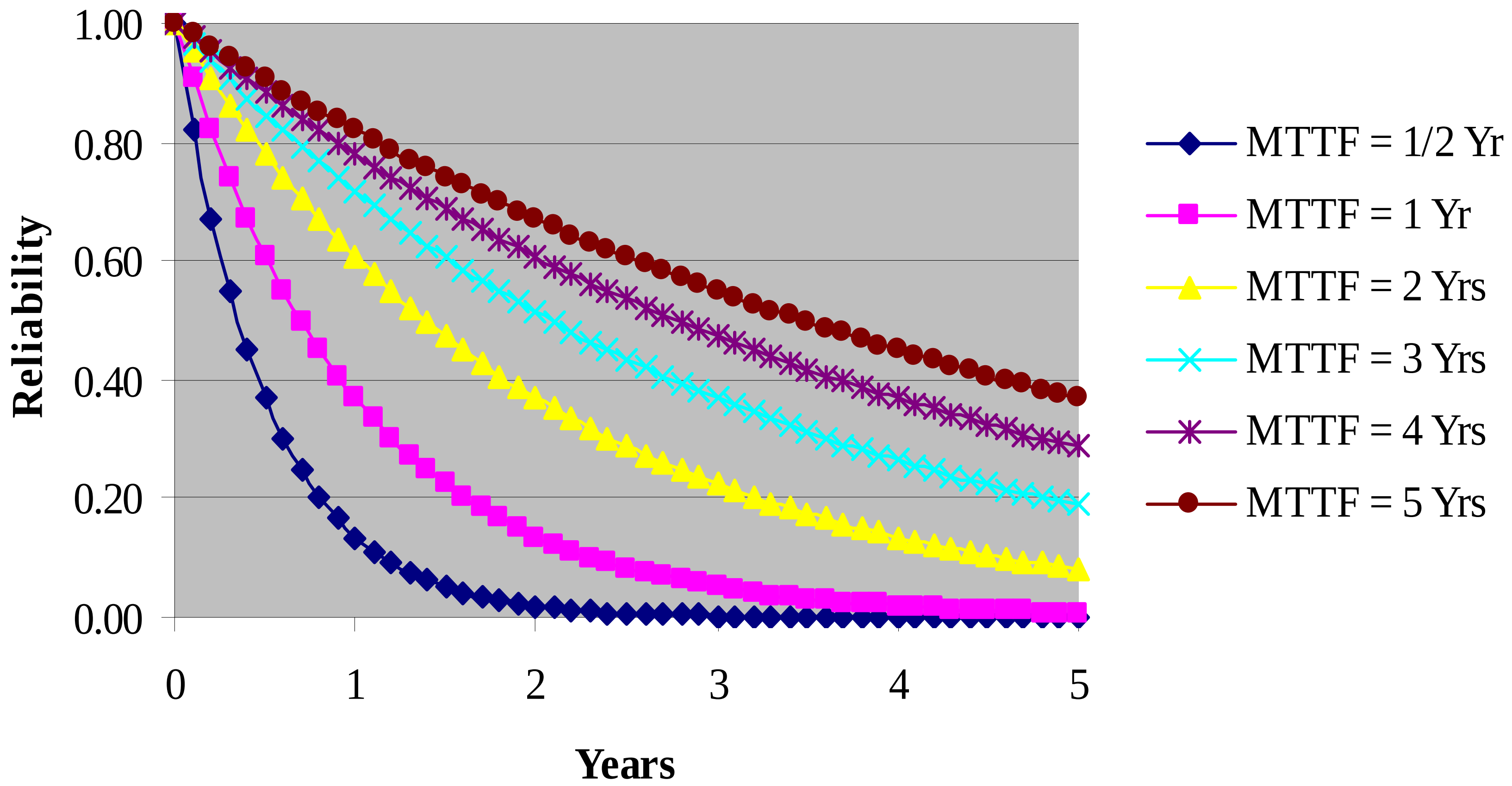
- What is the chance a switch with an MTTF of 5 years will operate without failure for 5 years? 1 year? 1 week?

$$R_{5-Yrs} = e^{-\lambda \cdot t} = e^{-t/MTTF} = e^{-5/5} = e^{-1} = 0.368$$

$$R_{1-Yr} = e^{-\lambda \cdot t} = e^{-t/MTTF} = e^{-1/5} = e^{-0.2} = 0.818$$

$$R_{1-Wk} = e^{-\lambda \cdot t} = e^{-t/MTTF} = e^{-(1/52)/5} = e^{-0.00385} = 0.996$$

Reliability Curves



Maintainability

- *Equipment or Service Maintainability* is the chance a piece of failed equipment will be fixed/replaced in its environment by a specified period of time.
- It is a function of the mean time to repair (MTTR), the inverse of "service rate", and for exponential repair (a conservative assumption):

$$M = 1 - e^{-\mu \cdot t} \qquad u = \frac{1}{MTTR}$$

- Basically equipment reliability deals with
  - "How fast can we expect to repair/replace this equipment", or
  - The "expected repair time".
- The restore time includes the total elapsed time:
  - To realize there is an outage, isolate, travel to, repair, test service/component, and put the service/component back into service.

Maintainability Example

- A DS3 digital circuit has an MTTR of 12 minutes. What is the chance the DS3 will be recovered for use in 1 minute?

$$M_{1-Min} = 1 - e^{-\mu \cdot t} = 1 - e^{-t/MTTR} = 1 - e^{-1/12} = e^{-0.0833} = 0.08$$

Availability

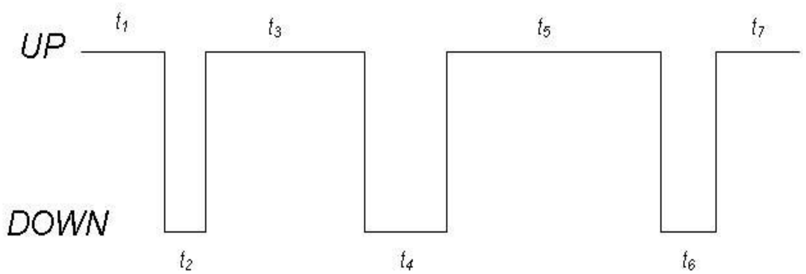
- Availability is an attribute for either a service or a piece of equipment. Availability has two definitions:
  - The chance the equipment or service is “UP” when needed (Instantaneous Availability), and
  - The fraction of time equipment or service is “UP” over a time interval (Interval or Average Availability).
- Interval availability is the most commonly encountered.
- Unavailability is the fraction of time the service is “Down” over a time interval $U = 1 - A$

Availability (Continued)

- Over some time interval, availability can be retrospectively calculated from the total uptime experienced over the interval:
- Availability can also be calculated for a prospective view from the MTTF and MTTR of the equipment or service:
- So availability is a measure of *how often an item/service fails,* and when it does *how long does it take to fix*.
- An availability profile can be shown. The times *between* failure is equal to the time to failure and the time to repair/restore, leading to:

$$A = \frac{UPTIME}{INTERVAL\_TIME}$$

$$A = \frac{MTTF}{MTTF + MTTR}$$



$$MTBF = MTTF + MTTR$$

Availability Example

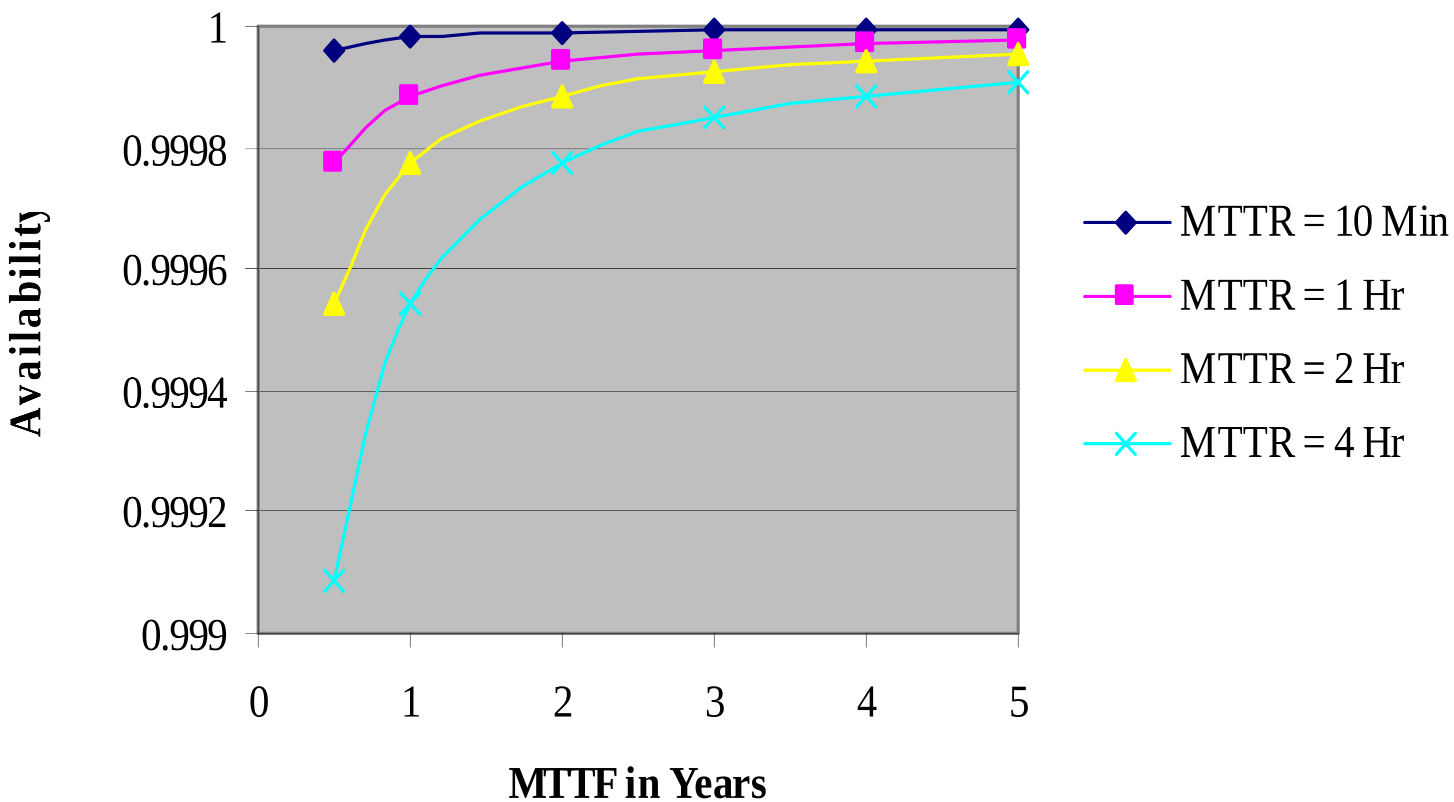
- A telecommunications service has an MTTF of 620 hours and an MTTR of 30 minutes.
  - What is the availability of the service?
  - How many hours per quarter can we expect the service to be down?

$$A = \frac{MTTF}{MTTF + MTTR} = \frac{620}{620.5} = 0.99919$$

$$U = 1 - A = 0.00081$$

$$Down\_Time = 0.00081 \cdot 24hrs \cdot 30day \cdot 3months = 1.74Hours$$

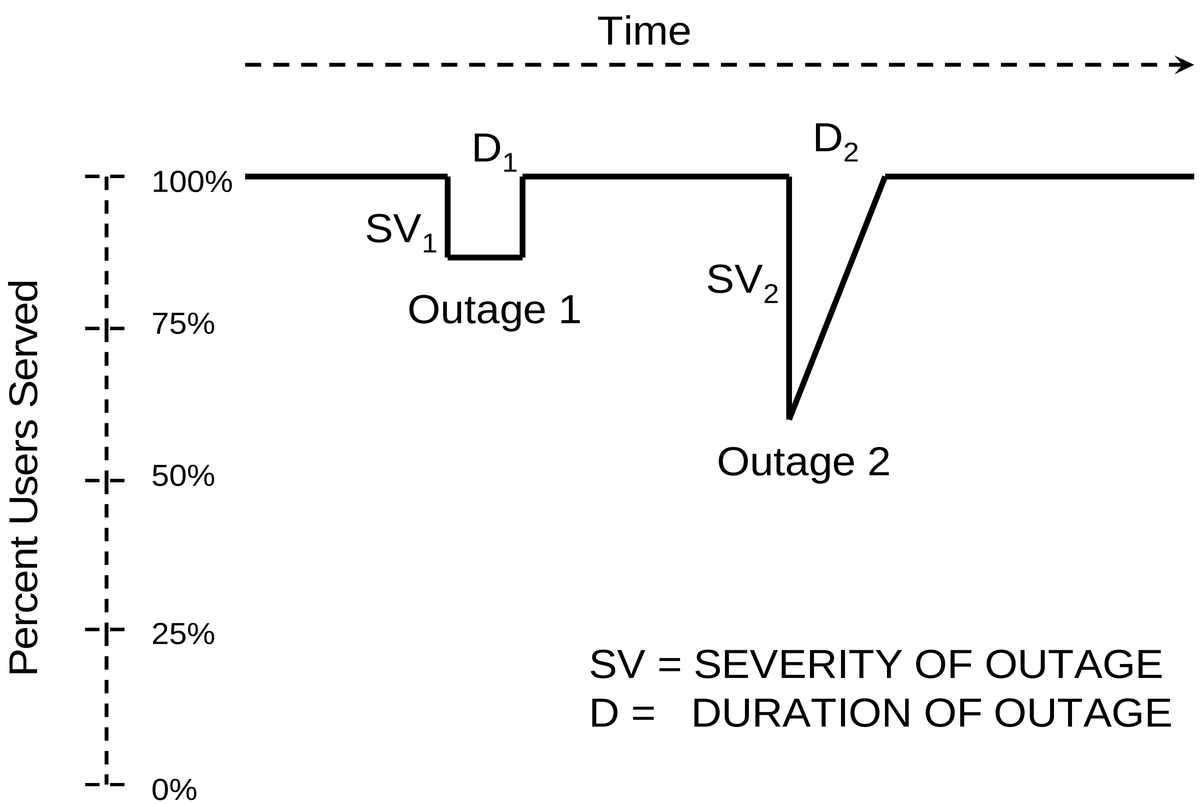
Availability Curves



Resiliency

- There are shortcomings with assessing a large ICT infrastructure by only RAM perspectives.
- First, the infrastructure often offers many different services over wide geographic areas.
- Second, large ICT infrastructures are rarely <u>completely</u> “up” or “down”.
- They are often “partially down” or “mostly up”
- Rare for an infrastructure serving hundreds of thousands or millions of users not to have some small portion of subscribers out at any one time.
- Resiliency describes the degree that the ICT system can service users when experiencing service outages

Outage Profiles



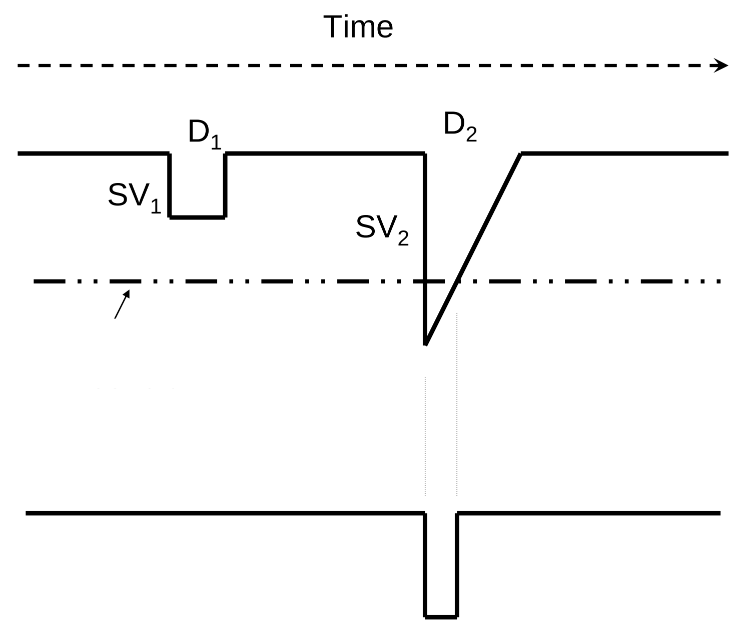
Outage 1: Failure and complete recovery. E.g. Switch failure

Outage 2: Failure and graceful Recovery. E.g. Fiber cut with rerouting

Resiliency Thresholds

- One way to measure resiliency is to set a severity threshold and observe the fraction of time the infrastructure is in a resilient state.
- Why set a threshold? At any instant in an ICT system there are bound to be a small number of users without service.
- Resiliency deficits are not small event phenomena.
- We can define resiliency as the fraction of time the infrastructure is in a resilient state, MTTRD is mean time to resiliency deficit (RD) and MTTRD is mean time to restore the resiliency deficit D.

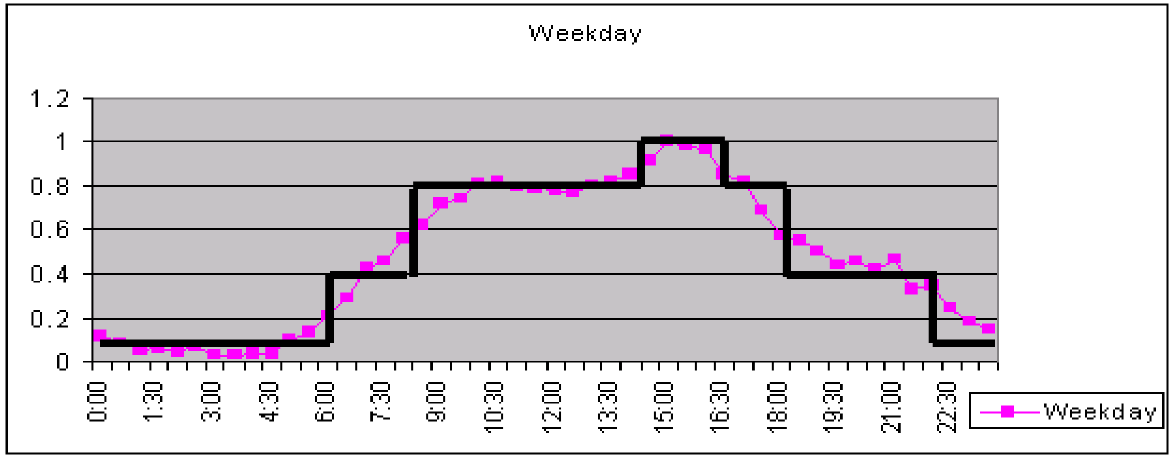
$$S = \frac{MTTRD}{MTTRD + MTTRD}$$

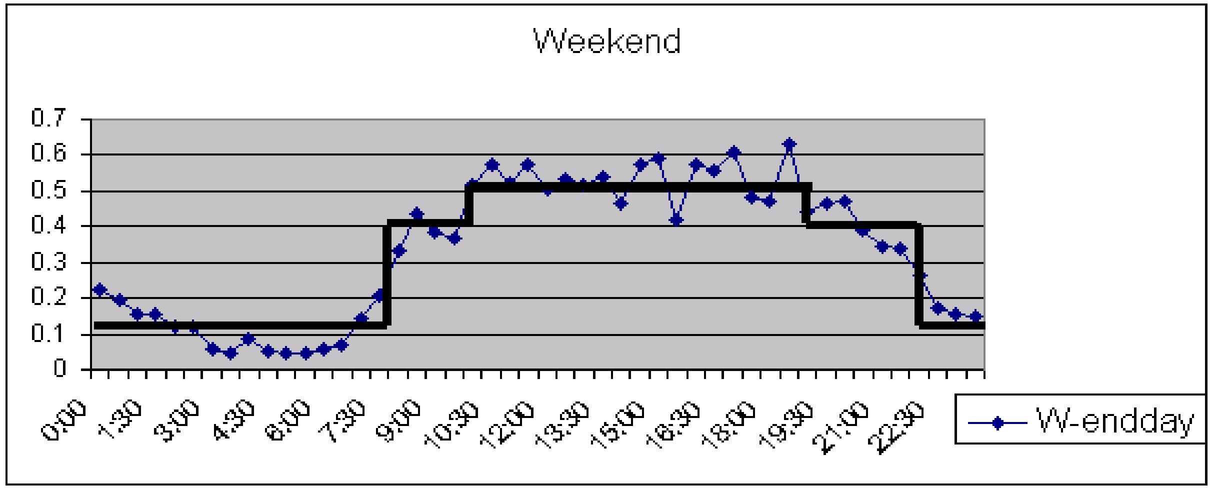


Severity

- The measure of severity can be expressed a number of ways, some of which are:
  - Percentage or fraction of users potentially or actually affected
  - Number of users potentially or actually affected
  - Percentage or fraction of offered or actual demand served
  - Offered or actual demand served
- The distinction between “potentially” and “actually” affected is important.
- If a 100,000 switch were to fail and be out from 3:30 to 4:00 am, there are 100,000 users *potentially* affected. However, if only 5% of the lines are in use at that time of the morning, 5,000 users are *actually* affected.

Outages at Different Times of Day Impact Different Numbers of People





User vs. System Administrator Perspectives

- User Perspective – High End-to-End Reliability and Availability
  - Focus is individual
- SysAdmin Perspective – High System Availability and Survivability
  - Focus is on large outages and large customers

Minimizing Severity of Outages

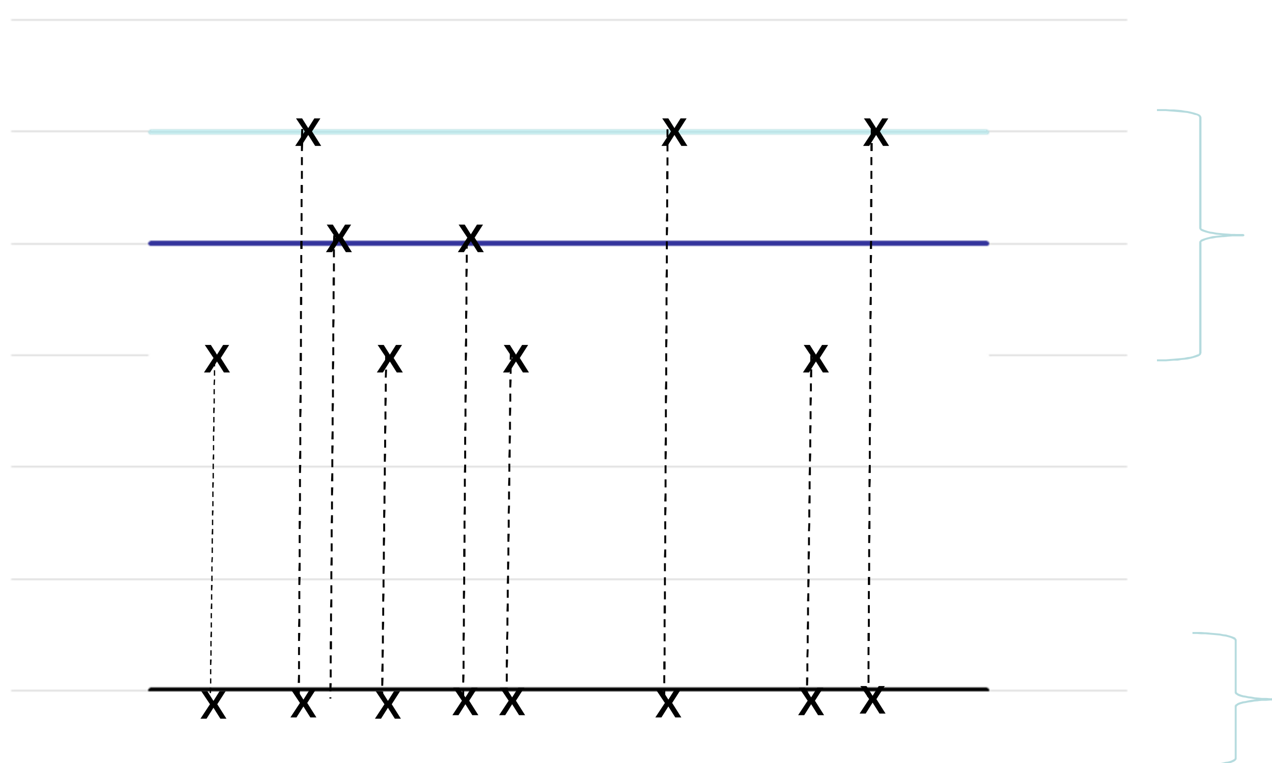
- It is not always possible to completely avoid failures that lead to outages. Proactive steps can be taken to minimize their size and duration.
  - Avoiding single points of failure that can affect large numbers of users,
  - Having recovery assets optimally deployed to minimize the duration of outages.
- This can be accomplished by:
  - Ensuring there is not too much over-concentration of assets in single buildings or complexes
  - Properly deploying and operating fault tolerant ICT architectures
    - Equipment/power fault tolerance
    - Physically and logical diverse transmission systems/paths
  - Ensuring there is adequate trained staff and dispersal of maintenance capabilities and assets

9 -11 TCOM Collateral Damage

- The telecommunications facility adjacent to the World Trade Center towers is an example of over-concentration,
  - 4,000,000 data circuits originating, terminating, or passing through that facility, which experienced catastrophic failure with the onset of water/structural damage.
  - Such “Mega-SPFs” ought to be avoided. If they cannot, significant contingency plans/capabilities should exist.

Examples of Statistical Reliability Analysis

Superposed Point Processes



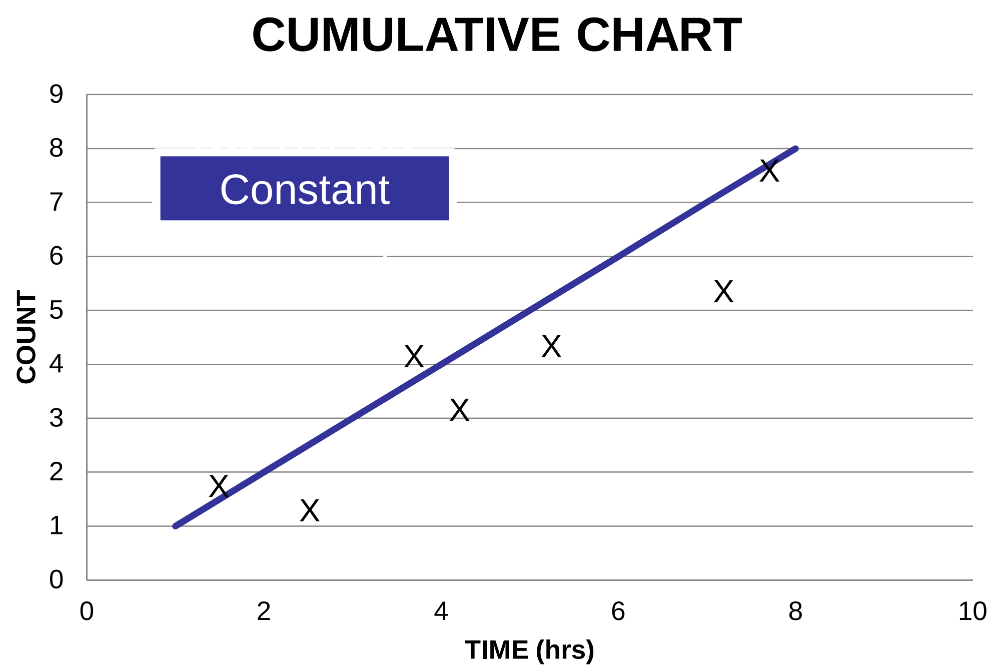
Individual processes
like Equipment, Caus
Services, etc.

Superposed process

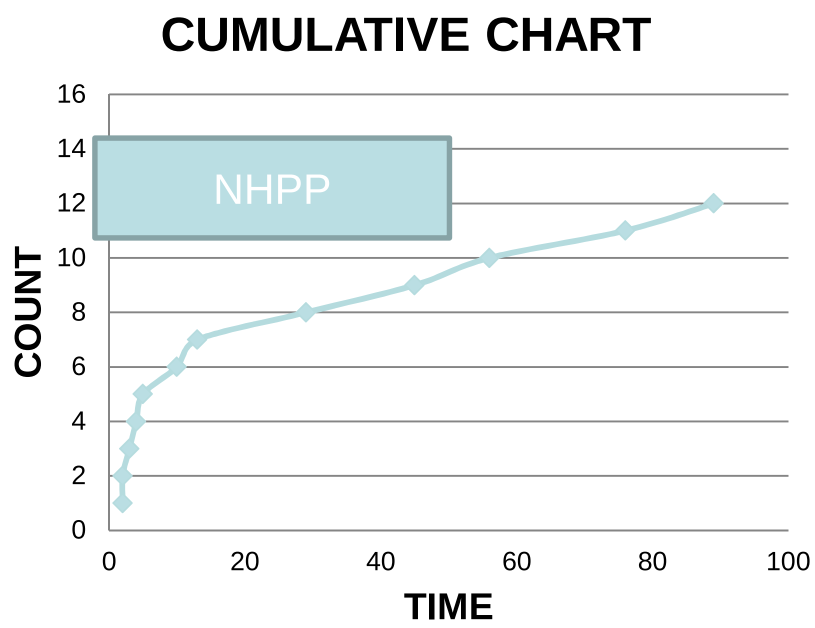
Classification of Failure/Outage Event Processes

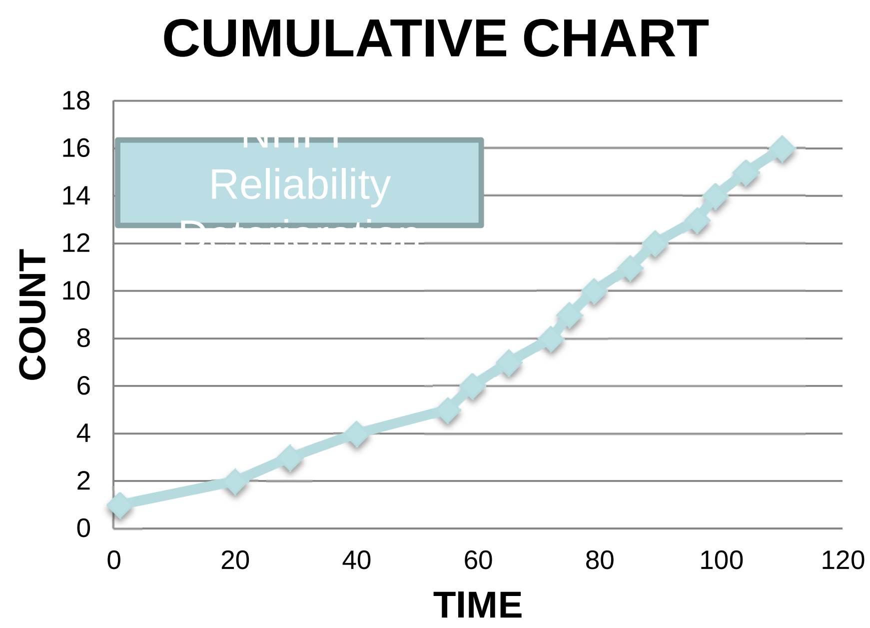
- HPP: HOMOGENOUS POISSON PROCESS
  - Stationary process; No trend; Poisson arrival
  - Time to Fail (ttf) i.i.d and exponential distribution
  - $R = e^{-\lambda t}$
  - Cumulative Count $\Omega(t) = \lambda t$ (constant failure)
- RP: RENEWAL PROCESS
  - Stationary process; No trend: (constant failure)
  - i.i.d but some other distribution such as Gamma, Weibull
- NHPP: NON-HOMOGENOUS POISSON PROCESS
  - Non-stationary process; Improving/Decreasing monotonic trend
    - Power Law

Hypothetical HPP

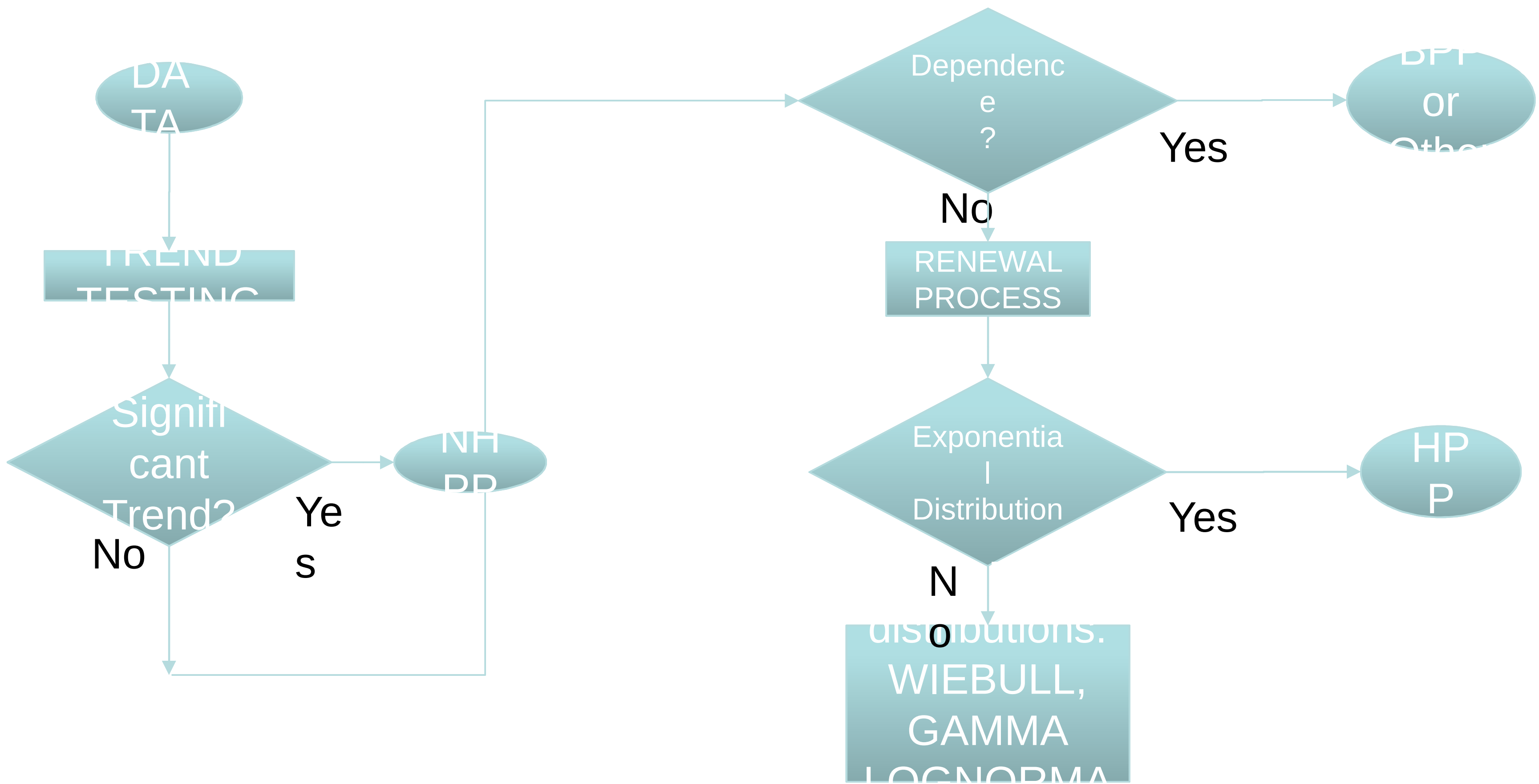


Hypothetical NHPP





Process Classification (HPP-RP-NHPP)



Hypothesis Testing

- Time Series of Event Trends (Event = Outage)
  - Laplace Test
  - Lewis-Robinson Test
  - Military Handbook Test
- Time Event Dependence
  - Correlation tests

Hypothesis Testing

- LAPLACE
  - Null H_0: There is no trend
  - Alternative H_a: The process is a NHPP
- Lewis-Robinson
  - Null H_0: The process is a RP
  - Alternative H_a: The process is a NHPP
- Military Handbook Test
  - Null H_0: The process is a HPP
  - Alternative H_a: The process is a NHPP
- Dependence Test
  - Null H_0: The process is classified as a BPP or other
  - Alternative H_a: The process is classified as an RP

Trend??

Independence?

Proposed Methods for Reliability

- Visual Trend Assessment
- Analytic Test of Trends (Laplace, Lewis Robinson, MilHbk tests)
- Independence of events (significance of first autocorrelation coefficient)
- Uniform distribution over time tests (Chi-Squared)

Analytical Tests for Sub-Processes

- LAPLACE

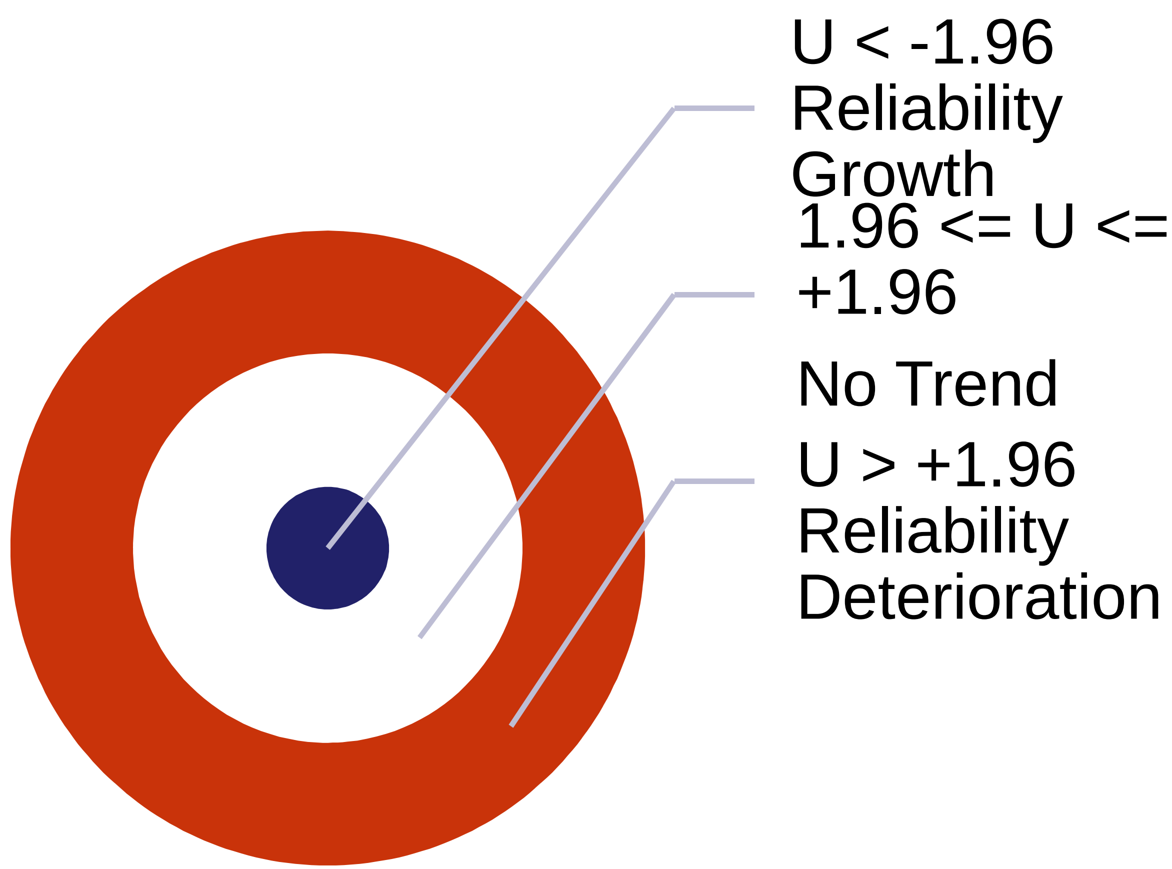
  $$U_L = \frac{(MEAN\ (ti) - T/2)}{(T * \sqrt{\ }(1/(12 * n))}$$

  - *T = 14 years; n = Count*

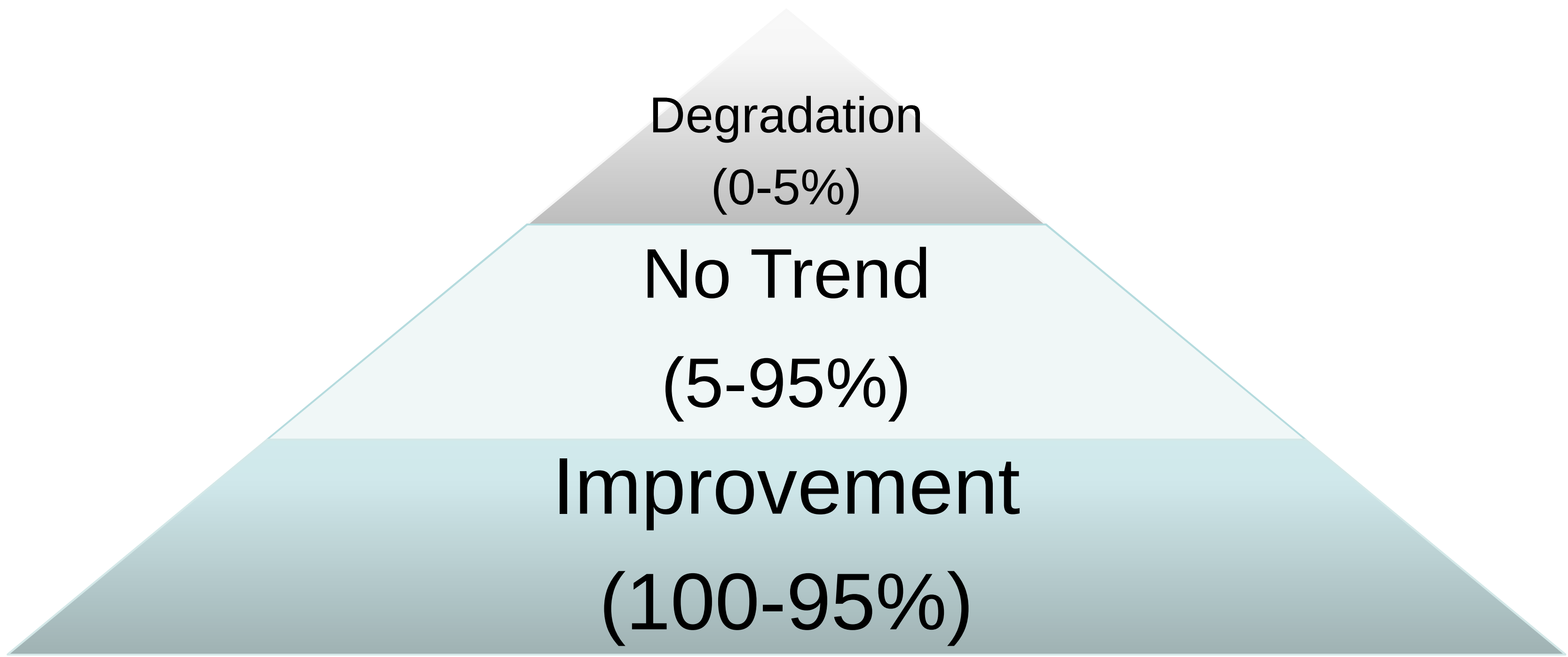
- LEWIS-ROBINSON TEST
  - $U_{LR} = U_L/CV$
  - CV = Coefficient of variation (VAR/MEAN)

- MILITARY HANDBOOK TEST
  - $\chi^2_{2n} = 2 * \Sigma \ln(T/t_i)$

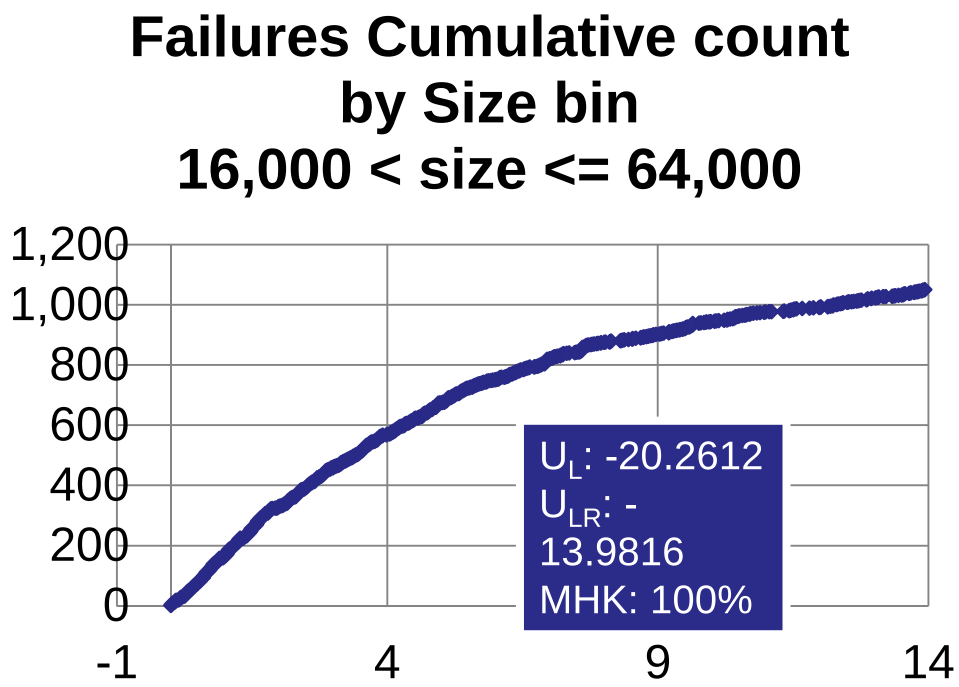
Hypothesis Testing U-SCORE Critical values

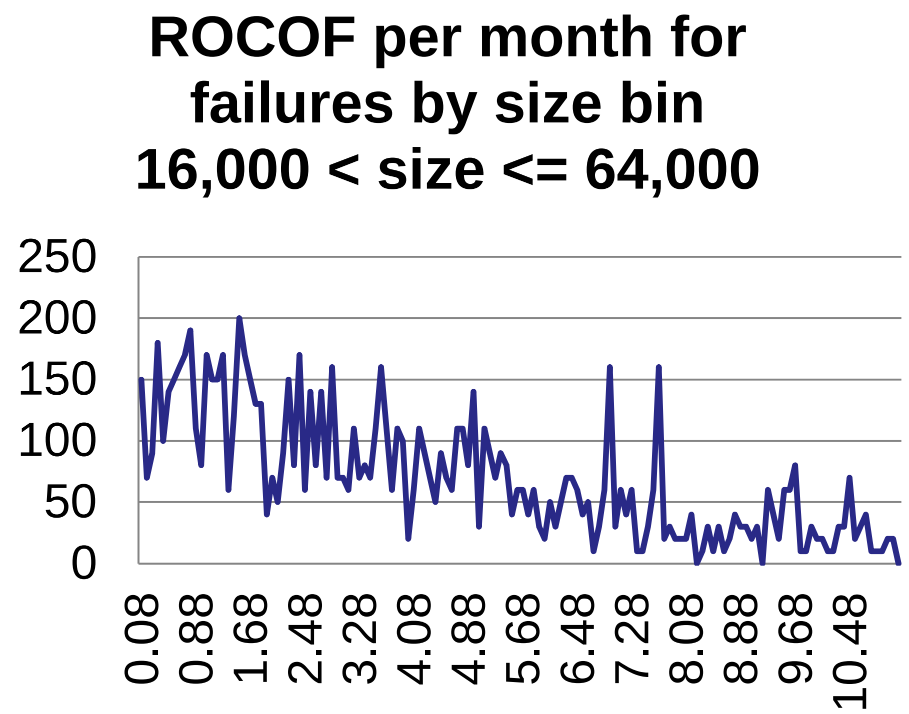


MilHbk Trend Test Hypothesis (Chi-Square Percentile values)

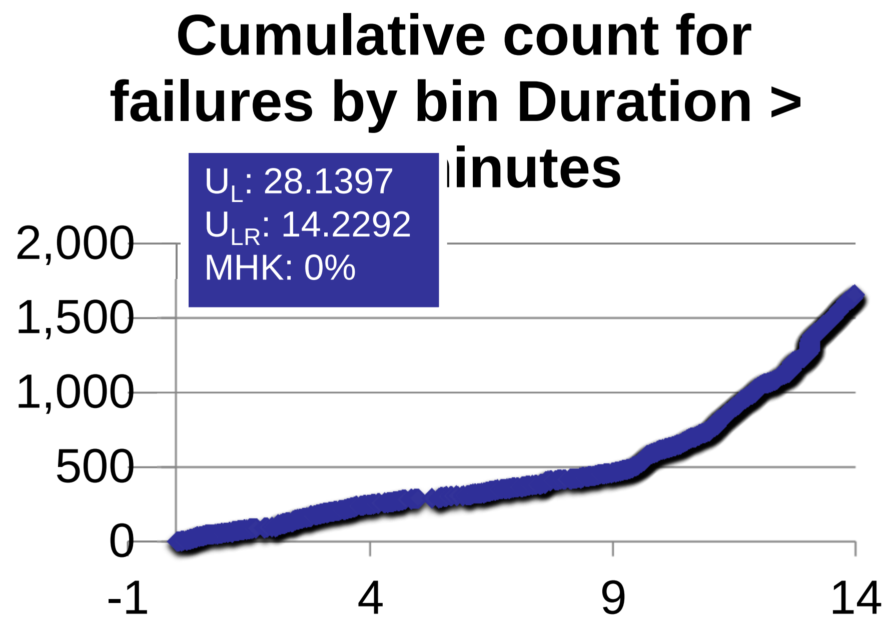


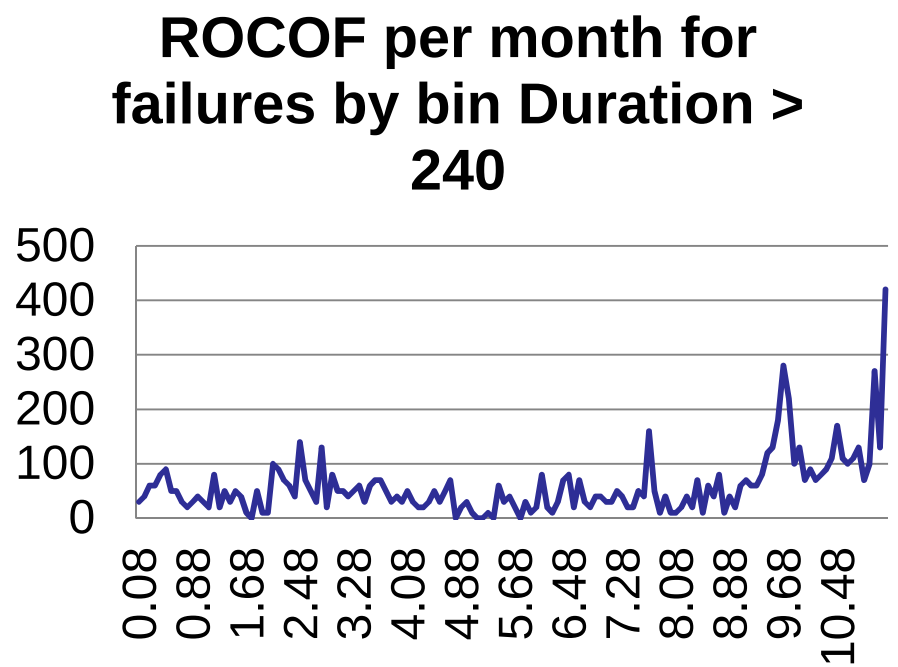
Reliability Growth Sample Result





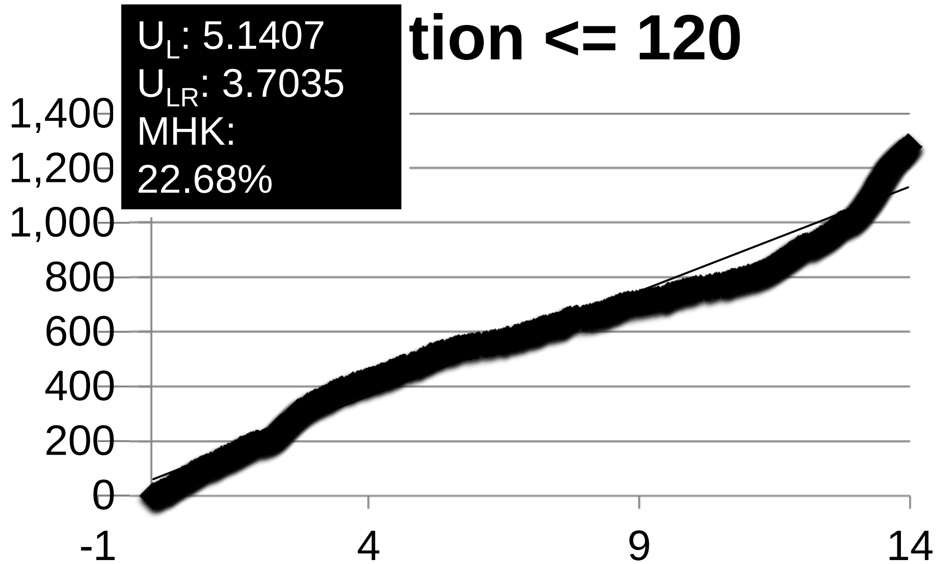
Reliability Deterioration Sample Result



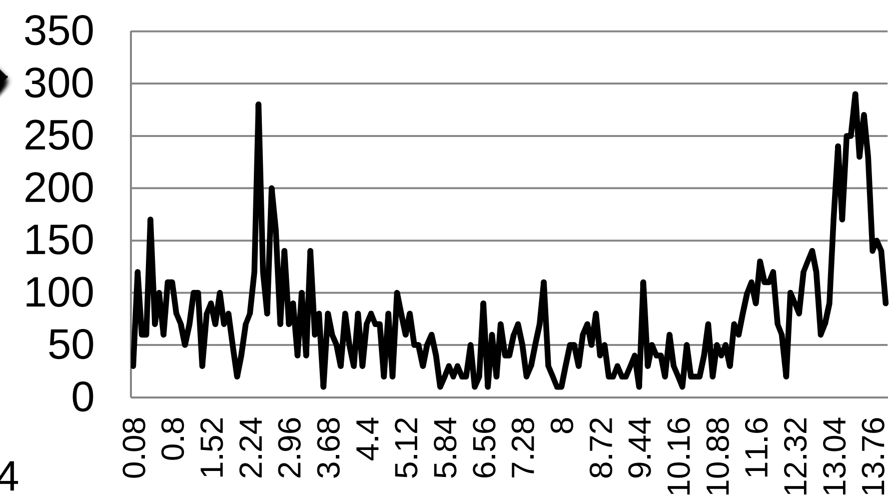


Constant Reliability Sample Result

Failures Cumulative count by duration bin 60 ... tion <= 120



ROCOF per month for failures by duration bin 60 < duration <= 120



Outline

A. **ICT Infrastructure Risk**
B. **ICT Network Infrastructure**
C. **RAM-R: Reliability, Availability, Maintainability and Resiliency**
D. ***Protection Level Assessment & Forecasting***

Empirical CIP Assessment

- Industry Best Practices & Standards
- Reviewing Disaster Recovery Plans for Rational Reactive/Proactive Balance
- Outage Data Collection and Analysis

Industry Best Practices & Standards

- Industry best practices deal with the architecture, design, installation, operations and maintenance activities
- Deviations from best practices should never be accidental, as an inadvertent or unknown deviation represents a latent vulnerability that can be triggered or exploited.
- In the U.S. Wireline best practices were initially developed as a Network Reliability & Interoperability Council (NRIC) initiative. [1]
- The scope of best practices has been expanded to cover the major network types and there are over 700 common best practices.
- A website can be queried by network type, industry role, and keyword:

[1] NRIC is a federal advisory council to the Federal Communications Commission, which has been continuously re-chartered since 1992.

NRIC Industry Best Practices

- Network Type
  - Cable
  - Internet/Data
  - Satellite
  - Wireless
  - Wireline
- Industry Role
  - Service Provider
  - Network Operator
  - Equipment Supplier
  - Property Manager
  - Government

www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm

Prevention vs. Reaction

- Preventing outages requires both capital and operational expenses.
  - Capital expenditures for such items as backup AC generators, batteries, redundant transmission paths, etc. can be very large.
  - Capital expenses to remove some vulnerabilities might be cost prohibitive, wherein the risk is deemed as *acceptable*.
- Users might not be aware that the service provider has a vulnerability that they do not plan to remediate.
- Regulator and the service provider might have significant disagreements as to what is an acceptable risk.
  - For instance, duct space in metropolitan areas might present significant constraints to offering true path diversity of fiber cables.
  - Or rural local switches might present considerable challenges for designers to offer two separate SS7 access links.

Prevention vs. Reaction

- Disaster recovery plans are geared toward *reacting* to outages rather than preventing them.
  - It is very important not to overlook the importance of fault removal plans.
- There must be an adequate balance between:
  - Preventing outages and reacting to outages once they have occurred.
  - This is a delicate economic equilibrium point which service providers struggle with.
  - Customers should be aware of this balance and competing perspectives

Prevention vs. Reaction

- Preventing outages requires both capital and operational expenses.
  - Capital expenditures for such items as backup AC generators, batteries, redundant transmission paths, etc. can be very large.
  - Capital expenses to remove some vulnerabilities might be cost prohibitive, wherein the risk is deemed as *acceptable*.
- Users might not be aware that the service provider has a vulnerability that they do not plan to remediate.
- Service providers might have significant disagreements as to what is an acceptable risk.
- Disaster recovery plans are geared toward *reacting* to outages rather than preventing them.
  - It is very important not to overlook the importance of fault removal plans.
- There must be an adequate balance between preventing outages and reacting to outages once they have occurred. This is a delicate economic equilibrium point which service providers struggle with.

Outage Data Collection and Analysis

- Outage data is the bellwether of infrastructure vulnerability.
- The faults which manifest themselves because of vulnerabilities are an indicator of the reliability and survivability of critical ICT infrastructure.
- Important to track reliability and survivability in order to asses whether the protection level is increasing, constant, or decreasing.
- Root Cause Analysis (RCA) is instrumental in improvements
  - Trigger
  - Direct
  - Root

Assessment Case Studies

- Case 1: Wireless Survivability Infrastructure Improvement Assessment with ANN
- Case 2: Chances of Violating SLA by Monte Carlo Simulation
- Case 3: TCOM Power Outage Assessment by Poisson Regression & RCA
- Case 4: SS7 Outages Assessment by Poisson Regression & RCA

Case 1: Wireless Survivability Infrastructure Improvement Assessment with ANN

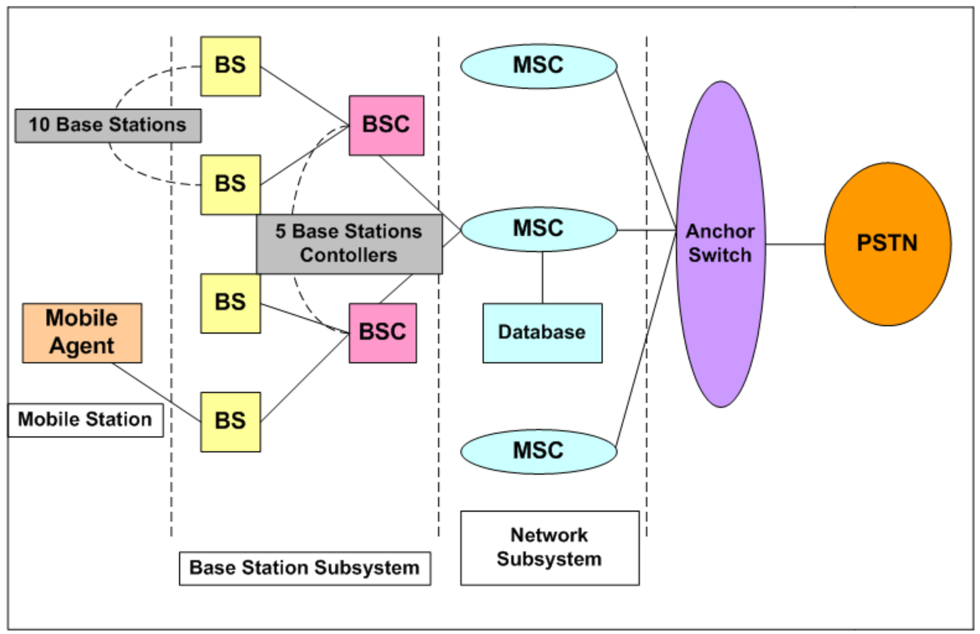
"Evaluating Network Survivability Using Artificial Neural Networks" by Gary R. Weckman, Andrew P. Snow and Preeti Rastogi

"Assessing Dependability Of Wireless Networks Using Neural Networks" by A. Snow, P. Rastogi, and G. Weckman

Introduction

- Critical infrastructures such as network systems must exhibit resiliency in the face of major network disturbances
- This research uses computer simulation and artificial intelligence to introduce a new approach in assessing network survivability
  - A discrete time event simulation is used to model survivability
  - The simulation results are in turn used to train an artificial neural network (NN)
- Survivability: defined over a timeframe of interest in two ways:
  - Fraction of network user demand capable of being satisfied
  - Number of outages experienced by the wireless network exceeding a particular threshold

Wireless Infrastructure Block (WIB)



- MSC: Mobile Switching Center
- PSTN: Public Switching Telecommunication Network Signaling
- SS7: System Numbering 7

WIB Characteristics

Components	Quantity in Each WIB
Database	1
Mobile Switching Center	1
Base Station Controller	5
Links between MSC and BSC	5
Base Station	50
Links between BSC and BS	50

Components	Customers Affected
Database	100,000
Mobile Switching Center	100,000
Base Station Controller	20,000
Links between MSC and BSC	20,000
Base Station	2,000
Links between BSC and BS	2,000

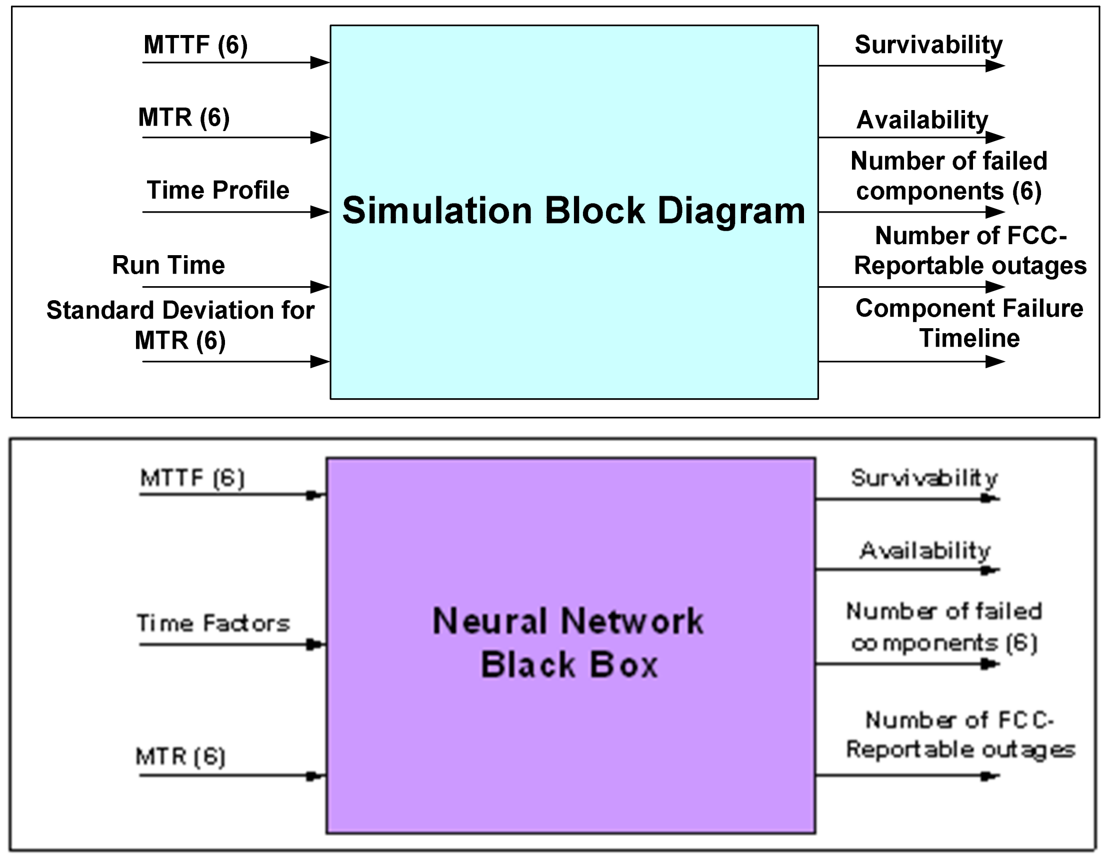
Reliability and Maintainability Growth, Constancy, and Deterioration Scenarios

Maintainability Growth, Constancy, Deterioration

Reliability Growth, Constancy, Deterioration

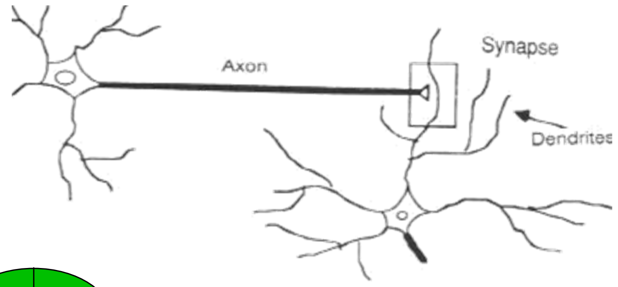
	MG	MC	MD
RG			
RC			
RD			

Simulation and Neural Network Model

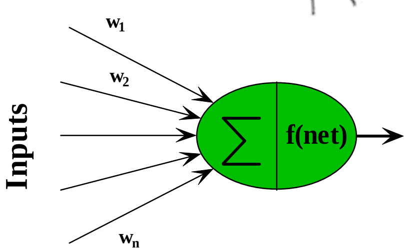


Biological Analogy

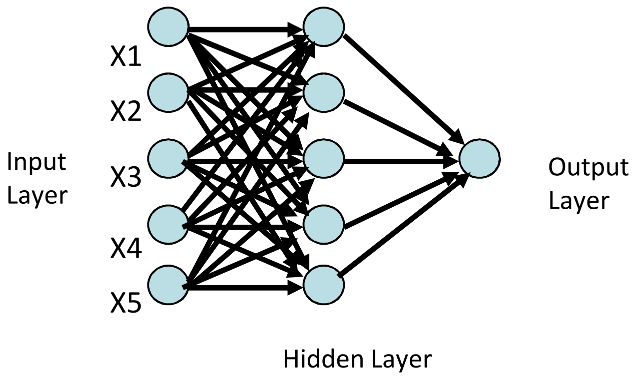
- Brain Neuron



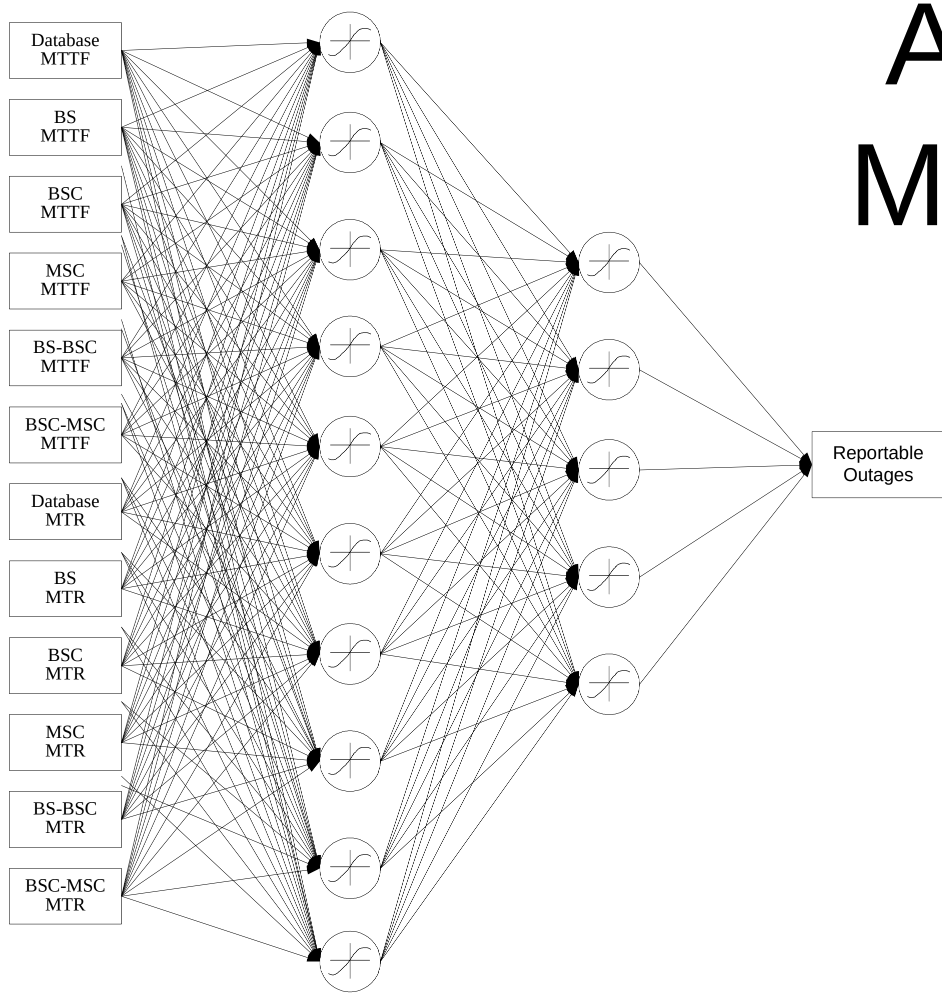
- Artificial neuron



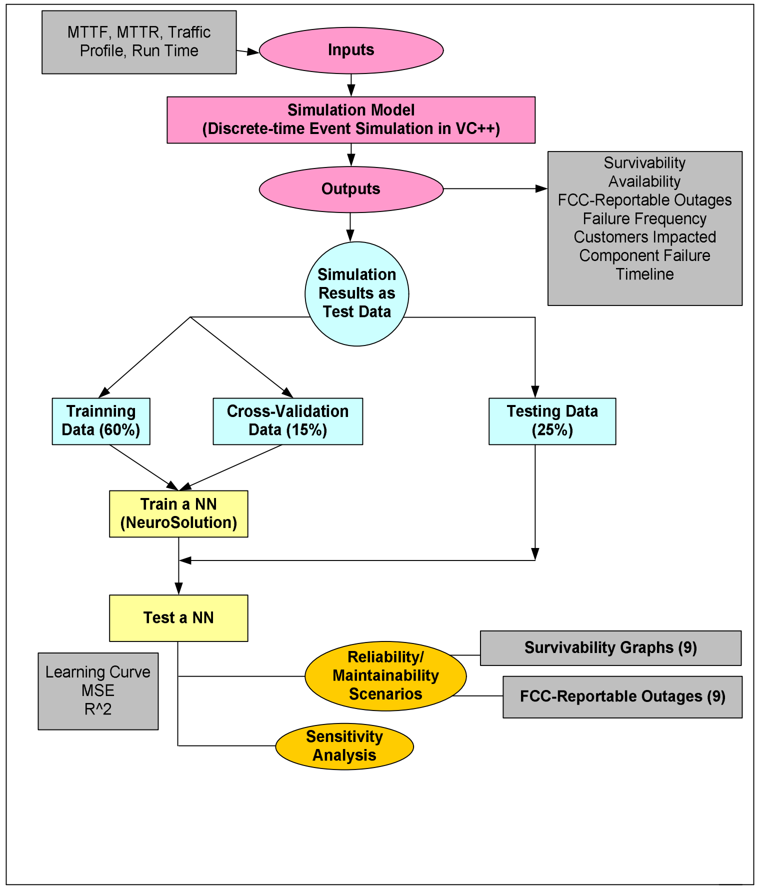
- Set of processing elements (PEs) and connections (weights) with adjustable strengths



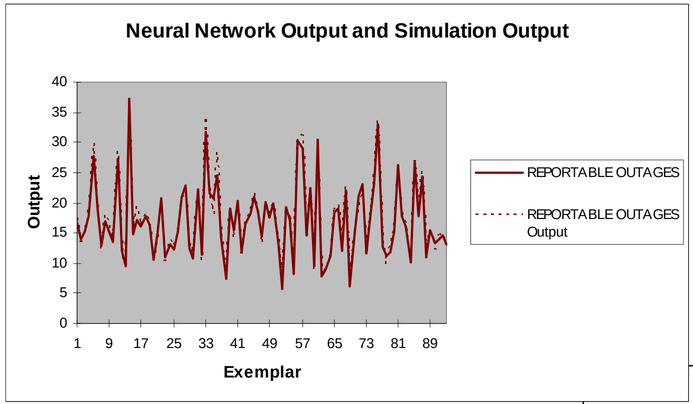
ANN Model

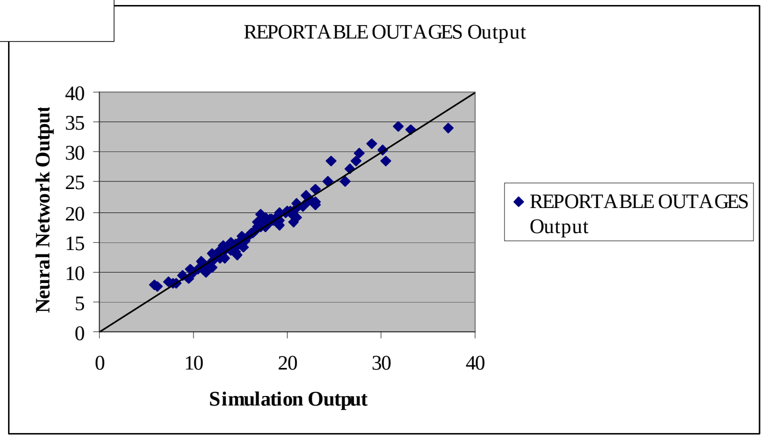

Database
MTTF
BS
MTTF
BSC
MTTF
MSC
MTTF
BS-BSC
MTTF
BSC-MSC
MTTF
Database
MTR
BS
MTR
BSC
MTR
MSC
MTR
BS-BSC
MTR
BSC-MSC
MTR
Reportable
Outages

Research Methodology



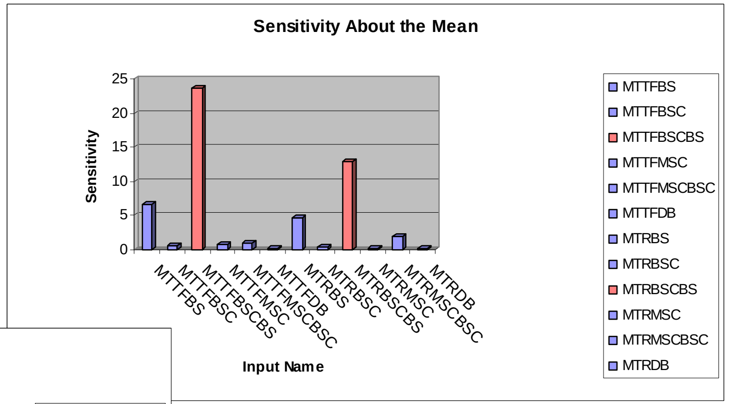
Simulation Vs Neural Network Outputs for FCC-Reportable Outages



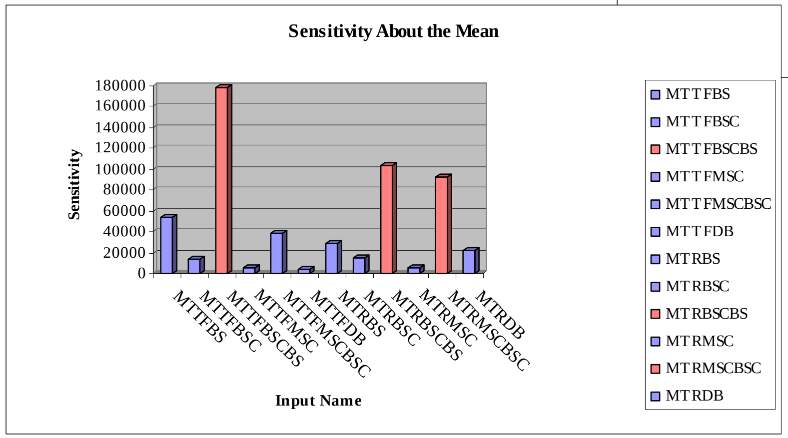


Sensitivity Analysis

FCC-Reportable Outages

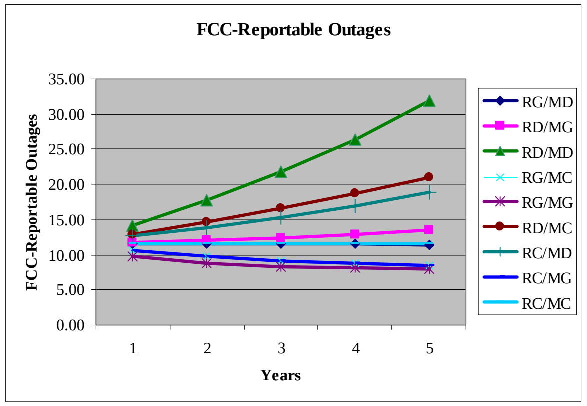


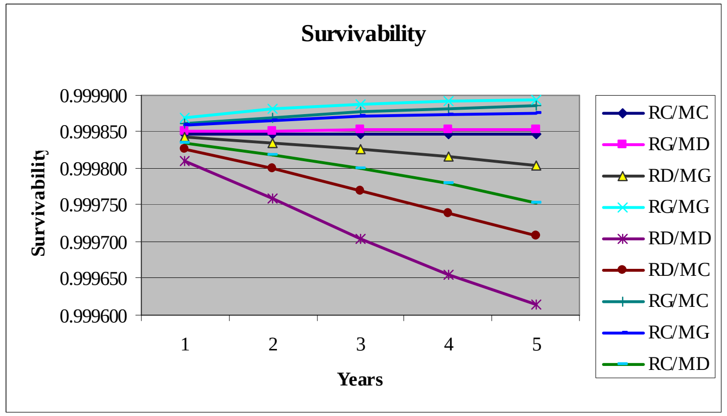
Survivability



COMPOUNDED IMPACT ON GROWTH AND DETERIORATION

Years	Compounded Growth (%)	Compounded Deterioration (%)
1	10	10
2	21	19
3	33.1	27.1
4	46.4	34.4
5	61.1	40.9





Conclusions (Continued)

- Reliability and/or maintainability:
  - Deterioration below nominal values affects wireless network dependability more than growth
  - Growth beyond nominal values does not improve survivability performance much
  - Cost/performance ratio plays an important role in deciding R/M improvement strategies.
- Scenario RG/MG gives the lowest value for FCC-Reportable outages, lost line hours and WIB downtime (high survivability)
  - Cost is high for marginal survivability improvement
- Scenario RD/MD indicates massive decreases in survivability
  - Fighting deterioration is more important than achieving growth.

Conclusions

- FCC-Reportable outages and survivability, reliability deterioration below the nominal values cannot be compensated by maintainability growth, whereas maintainability deterioration can be compensated by reliability growth.
- Benefits of an ANN model
  - wireless carrier can find out the expected number of threshold exceedances for a given set of component MTTF and MTTR values
  - Sensitivity analysis tells us the most important components

Conclusions

- Results indicate neural networks can be used to examine a wide range of reliability, maintainability, and traffic scenarios to investigate wireless network survivability, availability, and number of FCC-Reportable outages
- Not only is NN a more efficient modeling method to study these issues, but additional insights can be readily observed
- Limitations of study:
  - Only one wireless infrastructure building block (WIB) and does not include the entire wireless network integrated with PSTN
  - Modeling for 3G+ generation, however topology/hierarchy has similarities with 4G
  - Optimization is completed without the involvement of a cost function and hence economic considerations are not entertained.

Case 2: Chances of Violating SLA by Monte Carlo Simulation

- Snow, A. and Weckman G., *What are the chances of violating an availability SLA?,* International Conference on Networking 2008 (ICN08), April 2008.
- Gupta, V., Probability of SLA Violation for Semi-Markov Availability, Masters Thesis, Ohio University, March 2009.

What’s an SLA?

- Contractual agreement between a service provider and a customer buying a service
- Agreement stipulates some minimum QOS requirement
  – Latency, throughput, availability…..
- Can have incentives or disincentives:
  – Partial payback of service fees for not meeting QOS objectives in agreement

Who Cares About Availability?

- Who Cares About Availability?
  - End Users of systems/services
  - Providers of systems/services
- When a system/service is not available, customers could suffer:
  - Inconvenience
  - Lost revenue/profit
  - Decreased safety

Availability Distribution

- Availability is a function of MTTF and MTTR
- MTTF is the arithmetic mean of TTFs, which are random variables
- MTTR is the arithmetic mean of TTRs, which are random variables
- As availability is a function of MTTF and MTTR, its distribution is complex

What is the problem with a mean?

- As Availability is made up of means, it too is a mean
- The “Holy Grail” for Availability is often:
  - “Five Nines”, or
  - 0.99999 = 99.999%
  - Power System, T/E-3 digital link, etc.
- What is the problem with a mean?

More than One Way to Meet an Interval Availability Goal of 5-Nines

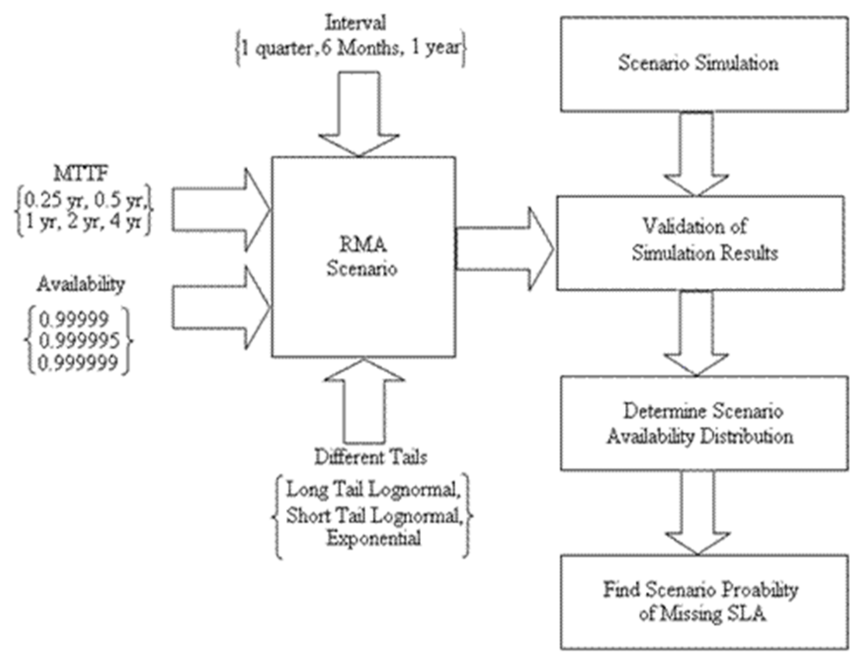
- For a given Availability goal, many combinations of *MTTF* & *MTTR* produce the same availability

AVAILABILITY	MTTF (Yr)	MTTR (Min)
0.99999	0.5	2.63
0.99999	1	5.26
0.99999	2	10.51
0.99999	3	15.77
0.99999	4	21.02
0.99999	5	26.28
0.99999	6	31.54
0.99999	7	36.79
0.99999	8	42.05

What we investigated

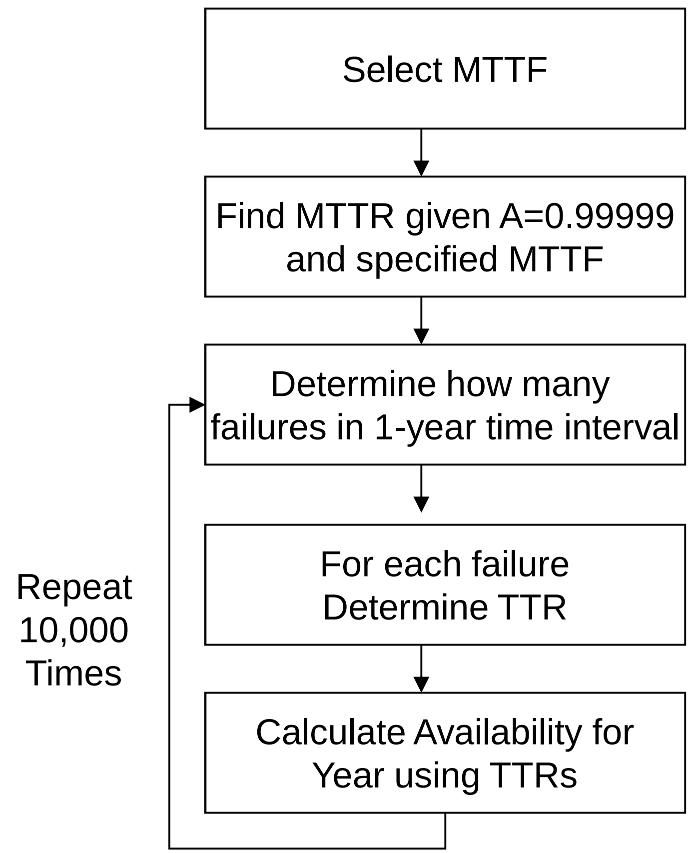
- Markov Availability
  - Exponential arrival of failures and independence of failures (HHP)
  - Exponential repair time
- Semi-Markov Availability
  - Exponential arrival of failures and independence of failures (HHP)
  - Nonexponential repair
    - Used Lognormal distribution (short and long tail)

Research Methodology



Gupta, V., Probability of SLA Violation for Semi-Markov Availability, Masters Thesis, Ohio University, March 2009.

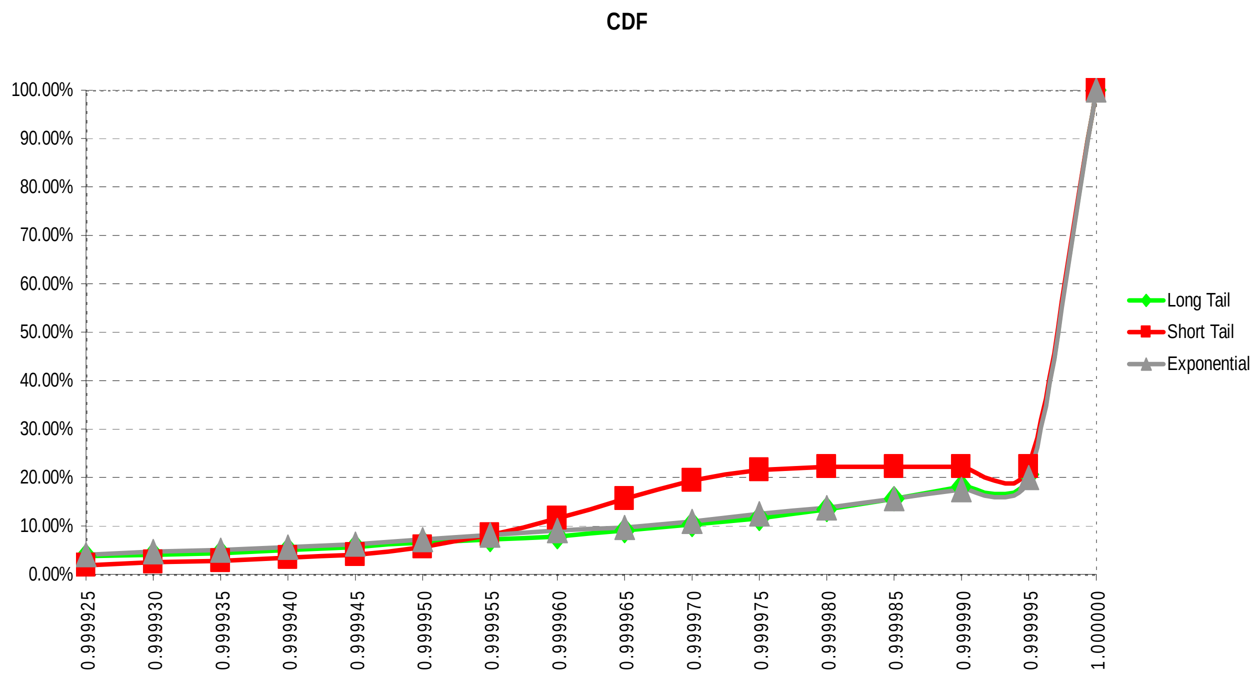
Monte Carlo Simulation Methodology



- Take a sample from Poisson Distribution to see how many failures in 1 year
- For each failure, determine TTR by taking a sample from EITHER exponential or lognormal repair distribution
- Calculate Availability based upon (Uptime)/(1-Year Interval)

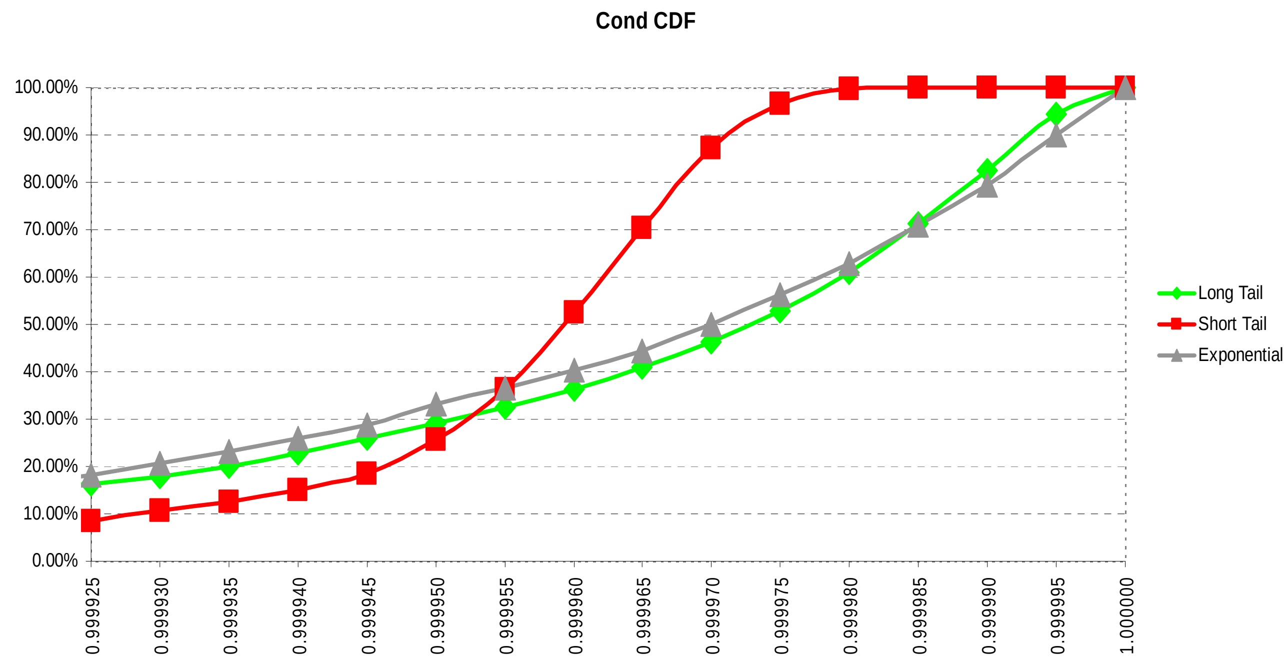
Cumulative Distribution Function

MTTF = 4 Yr; MTTR = 21.02 min; TI = 1 Yr

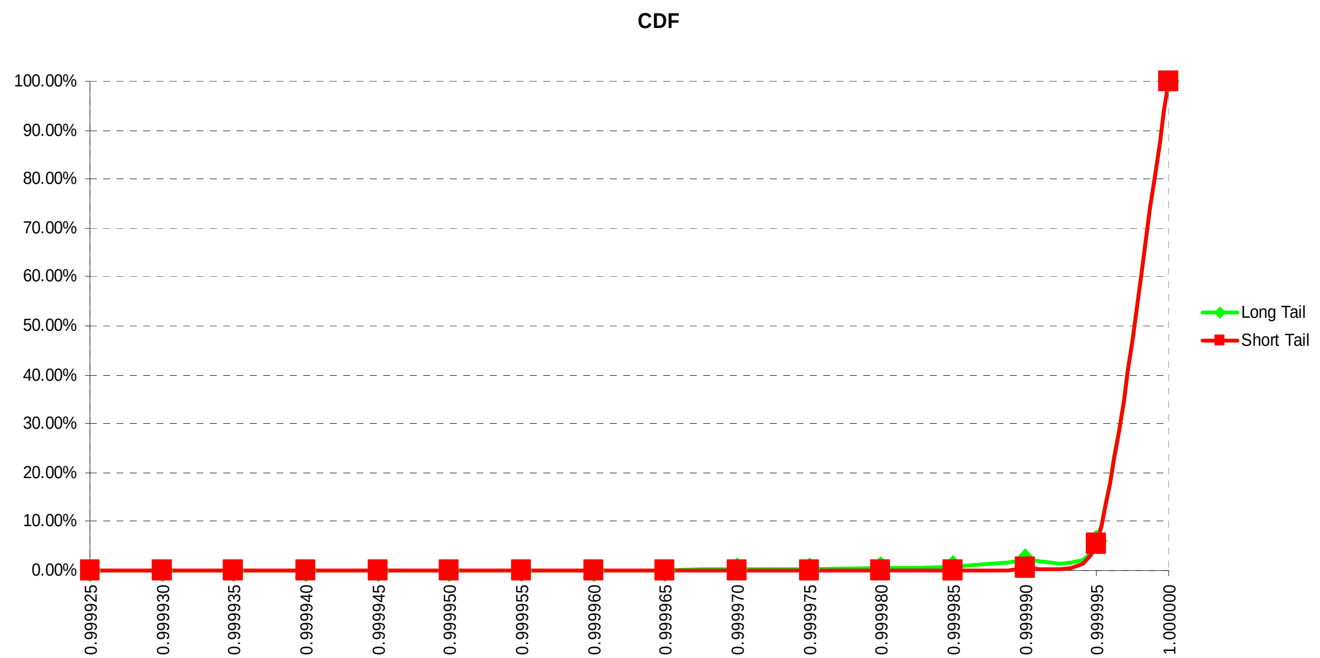


Conditional Cumulative Distribution Function

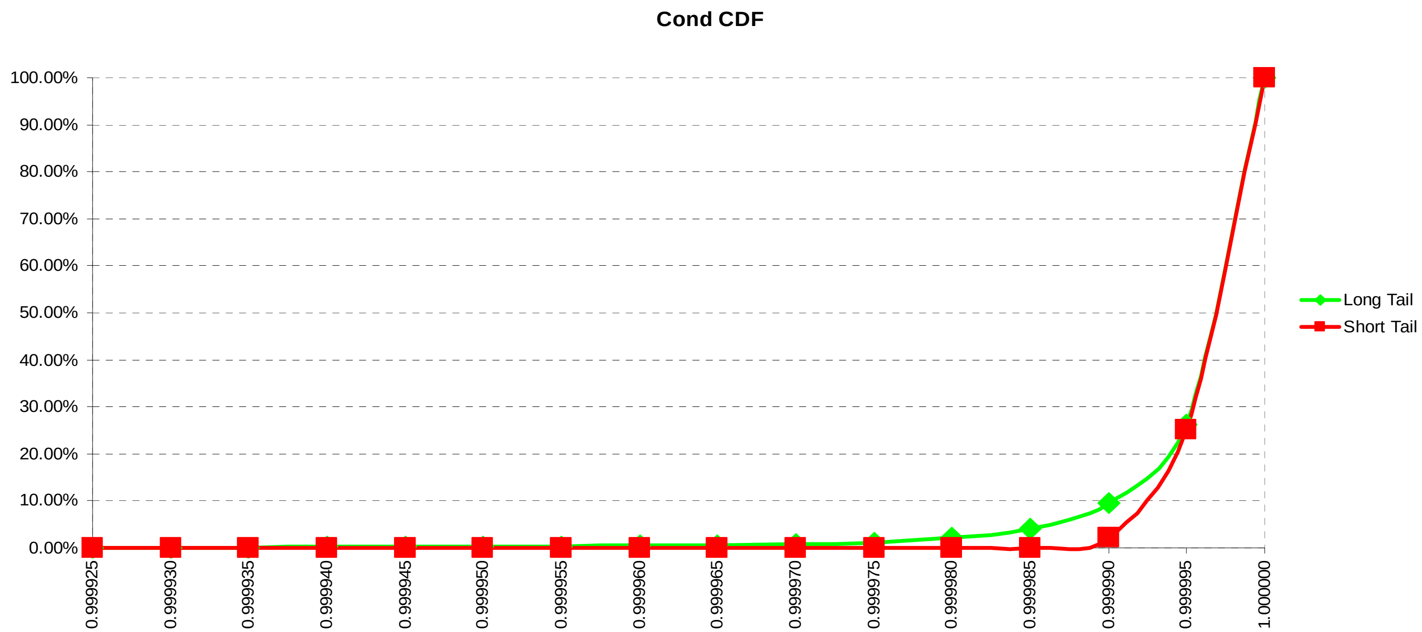
MTTF = 4 Yr; MTTR = 21.02 min; TI = 1 Yr



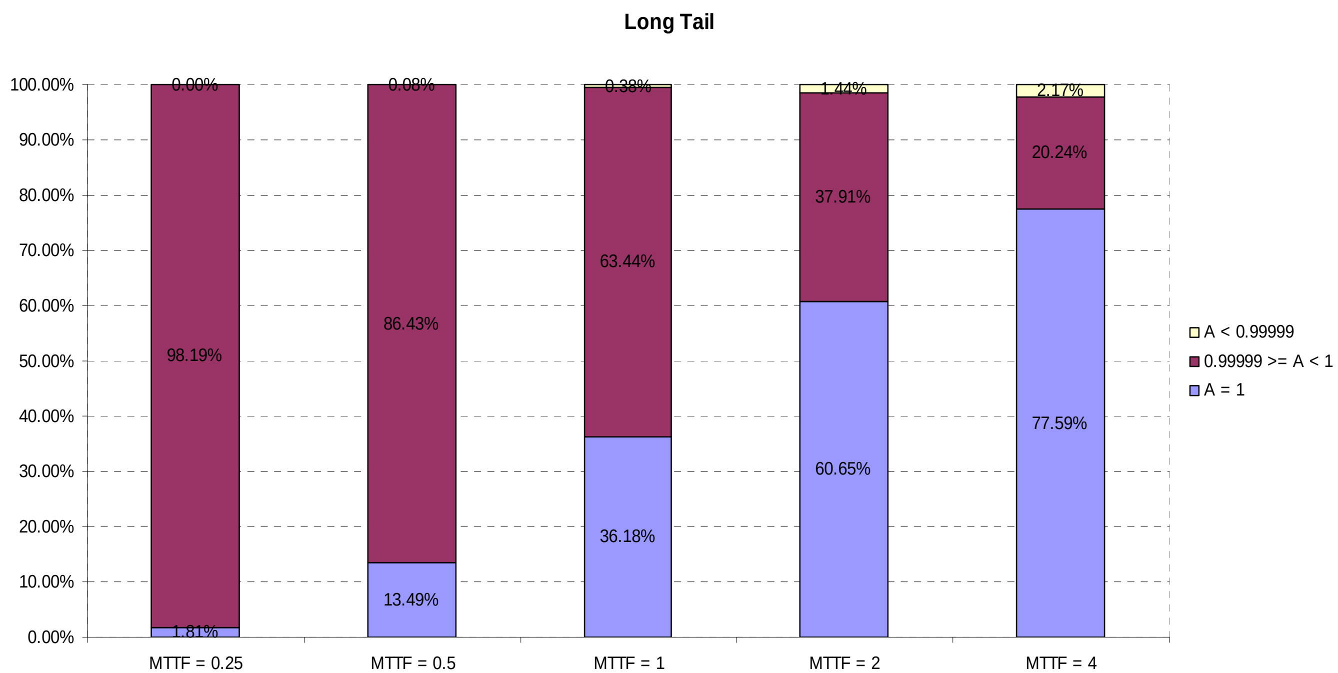
Cumulative Distribution Function MTTF = 4 Yr MTTR = 20.6 min; TI = 1 YR; A= 0.999999



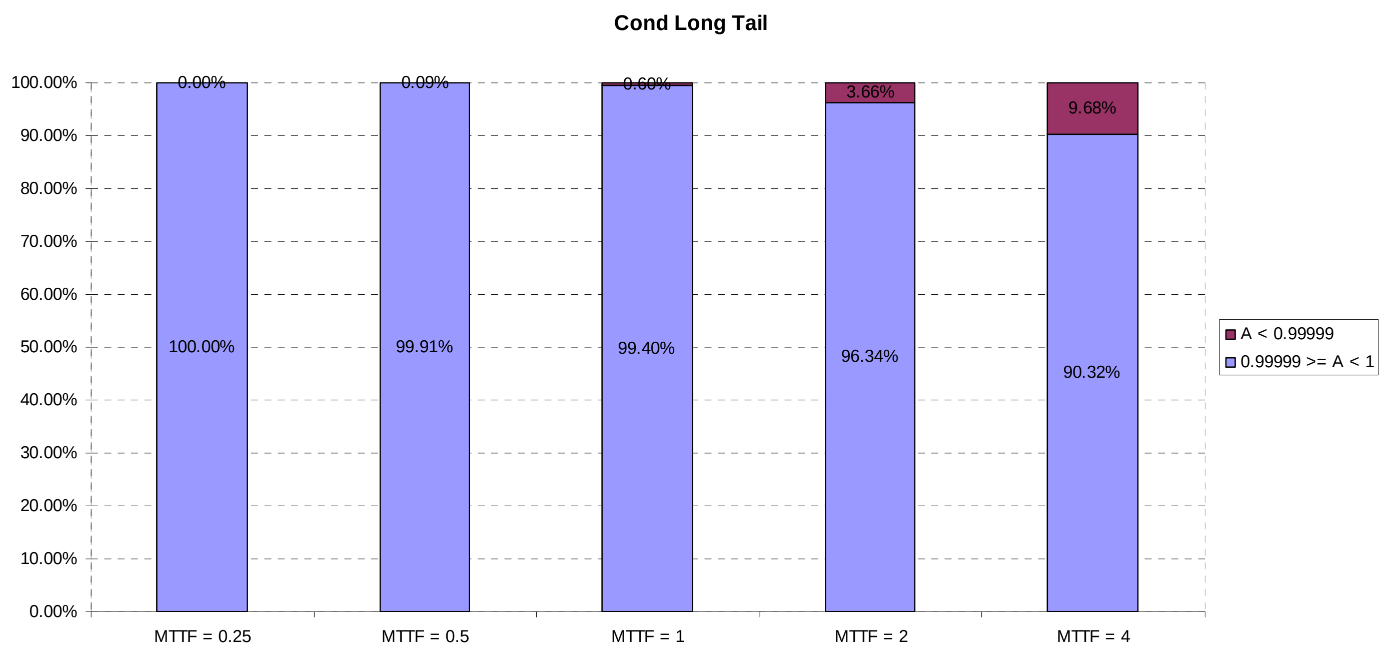
Conditional Cumulative Distribution Function
MTTF = 4 Yr; MTTR = 20.6 min;
TI = 1 YR; A= 0.999999



Long Tail Lognormal Distribution
TI = 1 YR; A = 0.99999



Conditional Long Tail Lognormal Distribution
TI = 1 YR; A = 0.999999



Some Conclusions

- Pr {SLA violation} for 5-nines is fairly insensitive to the long tail and short tail distributions studied
  - Largest difference found due to distribution about 5%
  - Exponential repair distribution pretty safe assumption
- High reliability scenarios depend upon no failures in interval to meet 5-nines SLA
  - If there is a failure in interval, SLA missed majority of time
- The shorter the interval, the less chance of violating 5-nines SLA, e.g. for MTTF 4 years:
  - Interval ¼ year: Pr {SLA violation} about 5%
  - Interval ½ year: Pr {SLA violation} about 9-12%
  - Interval 1 year: Pr {SLA violation} about 17-22%

Some Conclusions (Continued)

- Availability engineering margin
  - Engineered availability of 6-nines to meet a 5-nines objective
  - For the cases investigated drives Pr {SLA Violation} to 2% or less
  - Essentially removes distribution tail as a Pr {SLA Violation} factor
  - Even if there is a failure, maintenance ensures 5-nines objective met almost all the time
- When someone is selling/buying an Availability SLA, it is good to know
  - The availability engineering margin
  - How much the service provider is depending upon no failures[1]
  - Actual MTTR statistics

[1] Based upon statistics anonymously passed to author, recovery time for a DS3 circuit was reported to be about 3.5 hours

Case 3: TCOM Power Outage Assessment by Poisson Regression & RCA

- “Modeling Telecommunication Outages Due To Power Loss”, by Andrew P. Snow, Gary R. Weckman, and Kavitha Chayanam

- “Power Related Network Outages: Impact, Triggering Events, And Root Causes”, by A. Snow, K. Chatanyam, G. Weckman, and P. Campbell

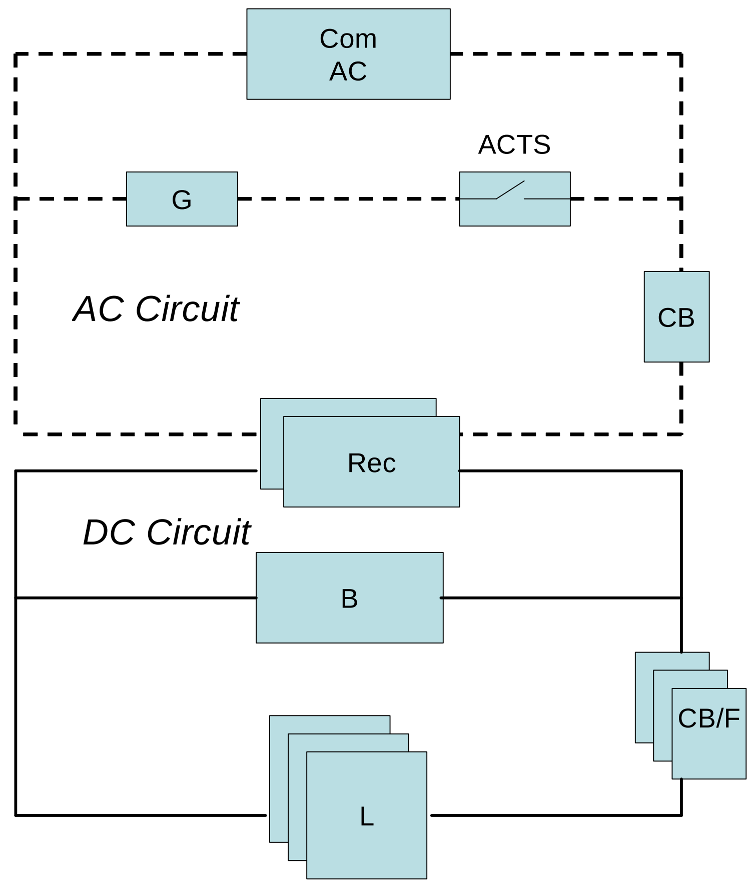
Introduction

- Management must include the ability to monitor the AC and DC power capabilities necessary to run the network.
- Large scale networks, communication facility power is often triply redundant
- In spite of significant redundancy, loss of power to communications equipment affects millions of telecommunications subscribers per Year
- This is an empirical study of 150 large-scale telecommunications outages reported by carriers to the Federal Communications Commission, occurring in the US over an 8 year period
  - Data includes the date/time of each outage, allowing time series reliability analysis

Overview

- Reasons of loss of power to communications equipment
- This study analyzes this special class of telecommunications outages over an 8-year period and is based on information found in outage reports to the FCC
  - Involve the failure of redundant power systems
  - Sequential events lead to complete power failure
- During the 8-year study period:
  - 1,557 FCC reportable outages This study considers:
  - Of these150 outages in which the service disruption was caused by loss of power to communications equipment and referred to as ‘Power outages’

Power Wiring Diagram



Com AC: Commercial AC
G: Generator
ACTS: AC Transfer Switch
CB: Main Circuit Breaker

Rec: Rectifiers
B: Batteries
CB/F: DC Ckt Breakers/Fuses
L: Communication Load

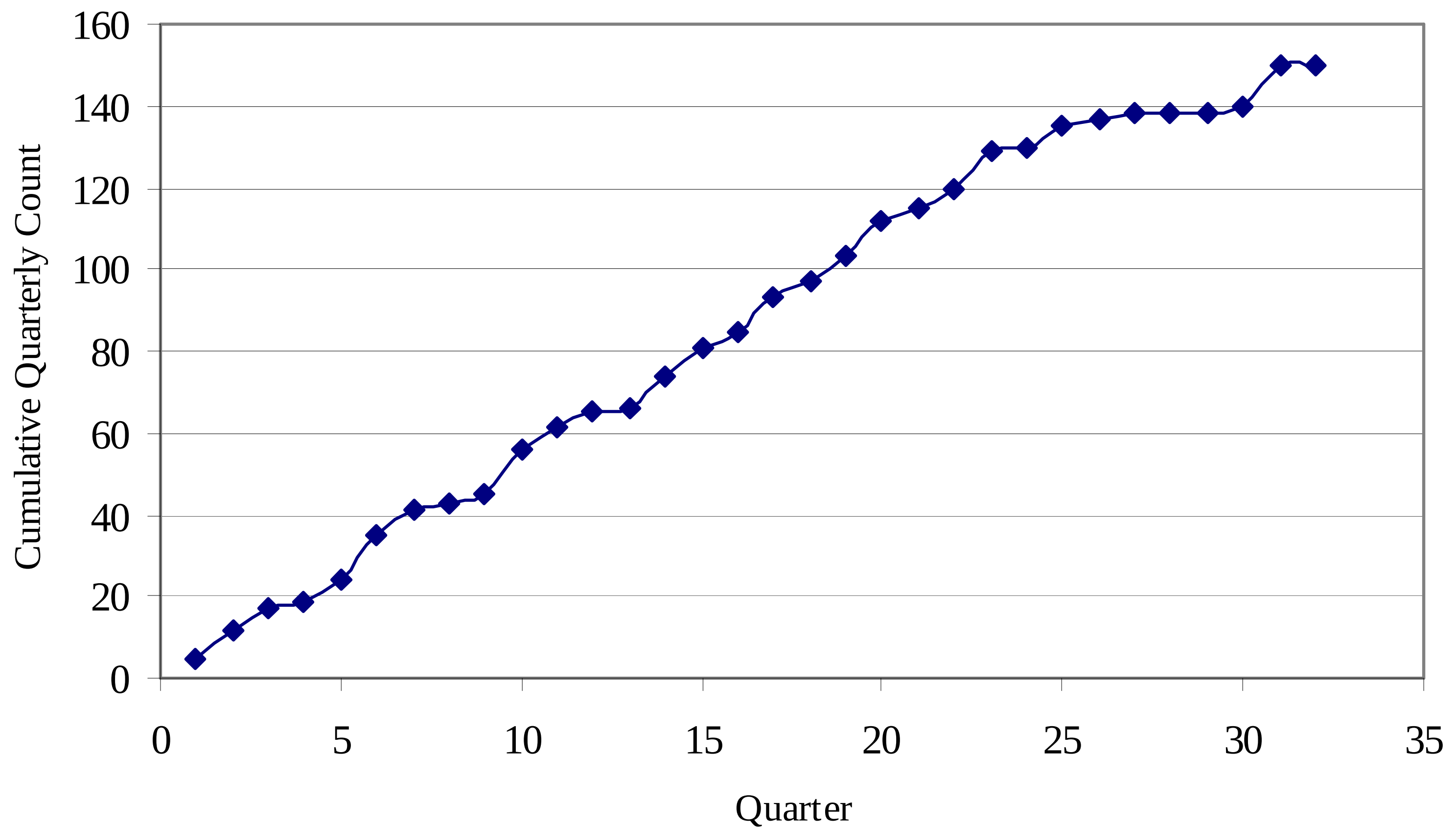
METHODOLOGY

- A nonhomogeneous Poisson process (NHPP) is often suggested as an appropriate model for a system whose failure rate varies over time
  - In the early years of development the term “learning curve” was used to explain the model’s concepts, rather than “reliability growth”. J. T. Duane presented his initial findings as a “Learning Curve approach to Reliability Monitoring”
  - Duane (1964) first introduced the power law model for decreasing failure point processes
- In addition to the power law, another technique for modeling reliability growth is by breakpoint analysis
  - Breakpoint reliability processes have previously shown up in large-scale telecommunications networks

Power Outage Count per Quarter for an Eight Year Study Period

Quarter	Count	Quarter	Count	Quarter	Count	Quarter	Count
1 (1st Q 96)	5	9 (1st Q 98)	2	17 (1st Q 00)	8	25 (1st Q 02)	5
2 (2nd Q 96)	7	10 (2nd Q 98)	11	18 (2nd Q 00)	4	26 (2nd Q 02)	2
3 (3rd Q 96)	5	11 (3rd Q 98)	5	19 (3rd Q 00)	6	27 (3rd Q 02)	1
4 (4th Q 96)	2	12 (4th Q 98)	4	20 (4th Q 00)	9	28 (4th Q 02)	0
5 (1st Q 97)	5	13 (1st Q 99)	1	21 (1st Q 01)	3	29 (1st Q 03)	0
6 (2nd Q 97)	11	14 (2nd Q 99)	8	22 (2nd Q 01)	5	30 (2nd Q 03)	2
7 (3rd Q 97)	6	15 (3rd Q 99)	7	23 (3rd Q 01)	9	31 (3rd Q 03)	10
8 (4th Q 97)	2	16 (4th Q 99)	4	24 (4th Q 01)	1	32 (4th Q 03)	0

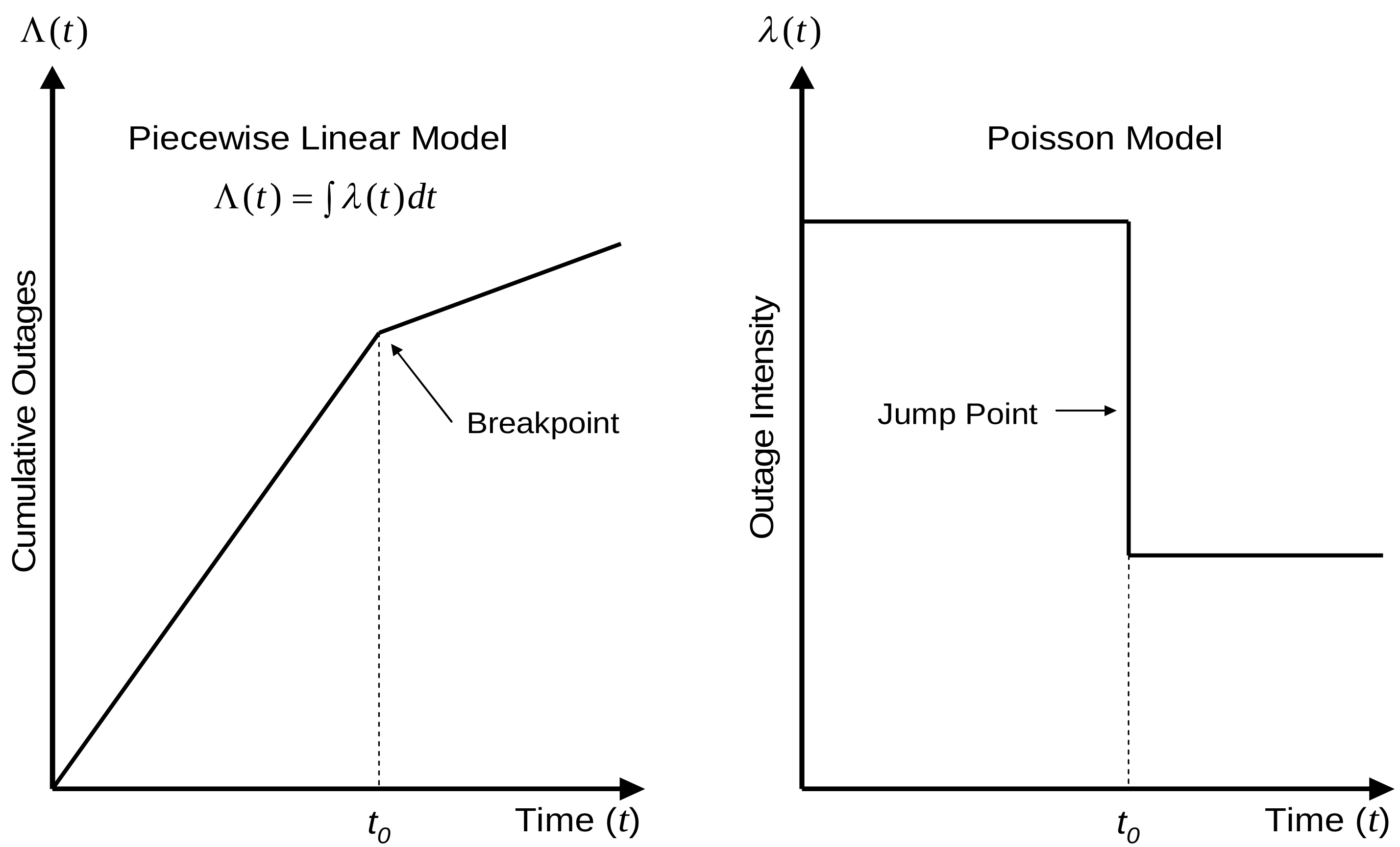
Power Outage Cumulative Quarterly Count



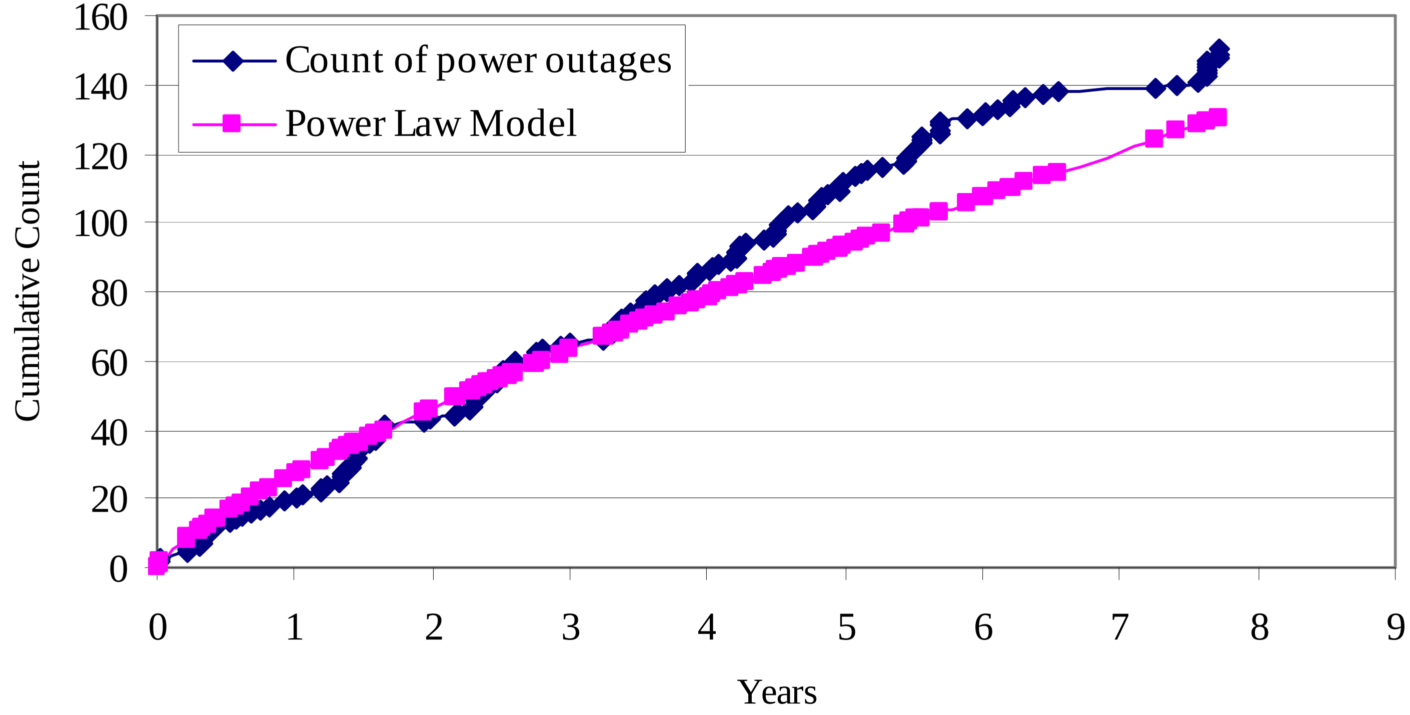
Power Law Model

- The Power Law Model is also called the Weibull Reliability Growth Model (Asher and Feingold, 1984)
- Commonly used infinite failure model, which shows monotonic increase or decay in events.
- This process is a NHPP

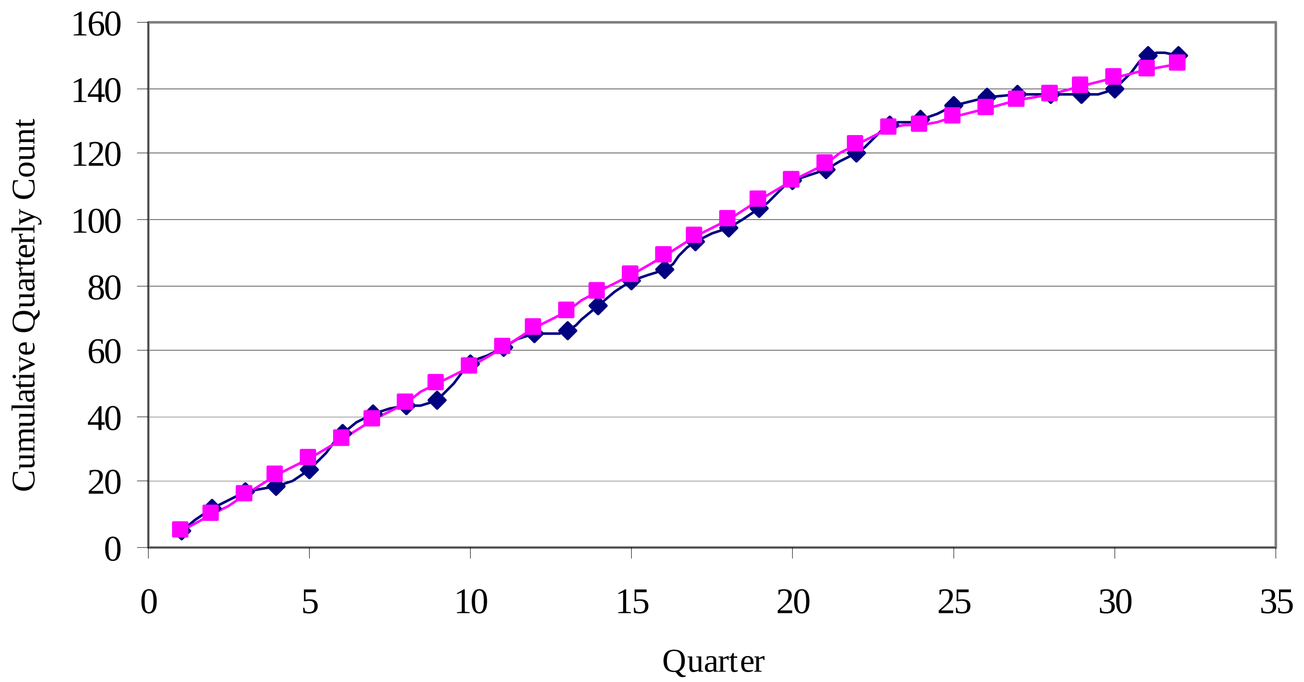
Piecewise Linear Model



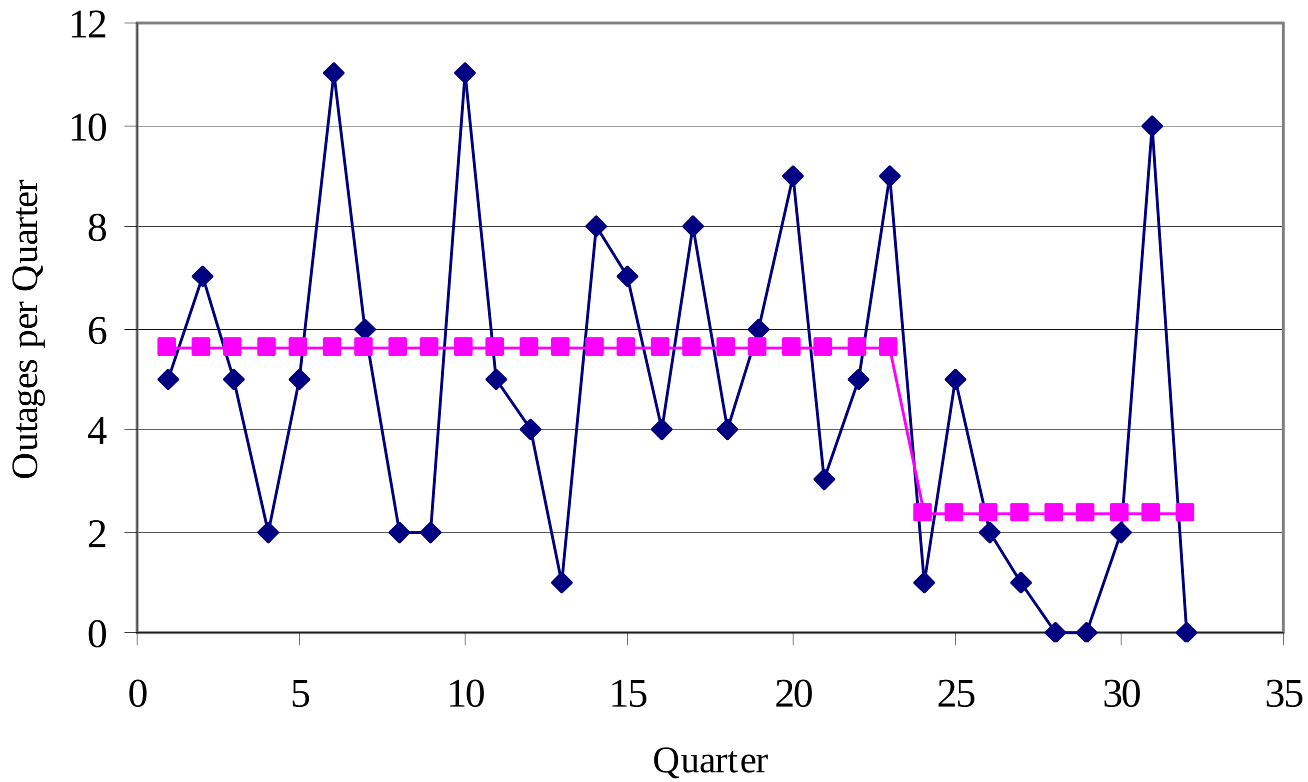
Comparison of Power Law Model and Cumulative Outage Data



Comparison of Piecewise Linear Model and Cumulative Outage Count



Comparison of Jump Point Model to Quarterly Outage Count



CONCLUSIONS

- Little evidence of a seasonal effect
  - Not unusual as every commercial power outage does not result in a telecommunications power outage because of backup power sources (generator and batteries)
  - hazards that take down commercial power occur throughout the year
- The Laplace Trend Test indicated strong statistical evidence of reliability growth
  - Reliability growth was not monotonic as evidenced by a poor fit to the power law model
  - Evidence for continuous improvement was lacking.
- Evidence for reliability growth occurring after 9-11 is strong
  - The piecewise linear model with a rate change jump point is the best reliability growth model found
  - Clearly indicates two distinct processes with constant reliability, yet improvement after the 9-11 attack.

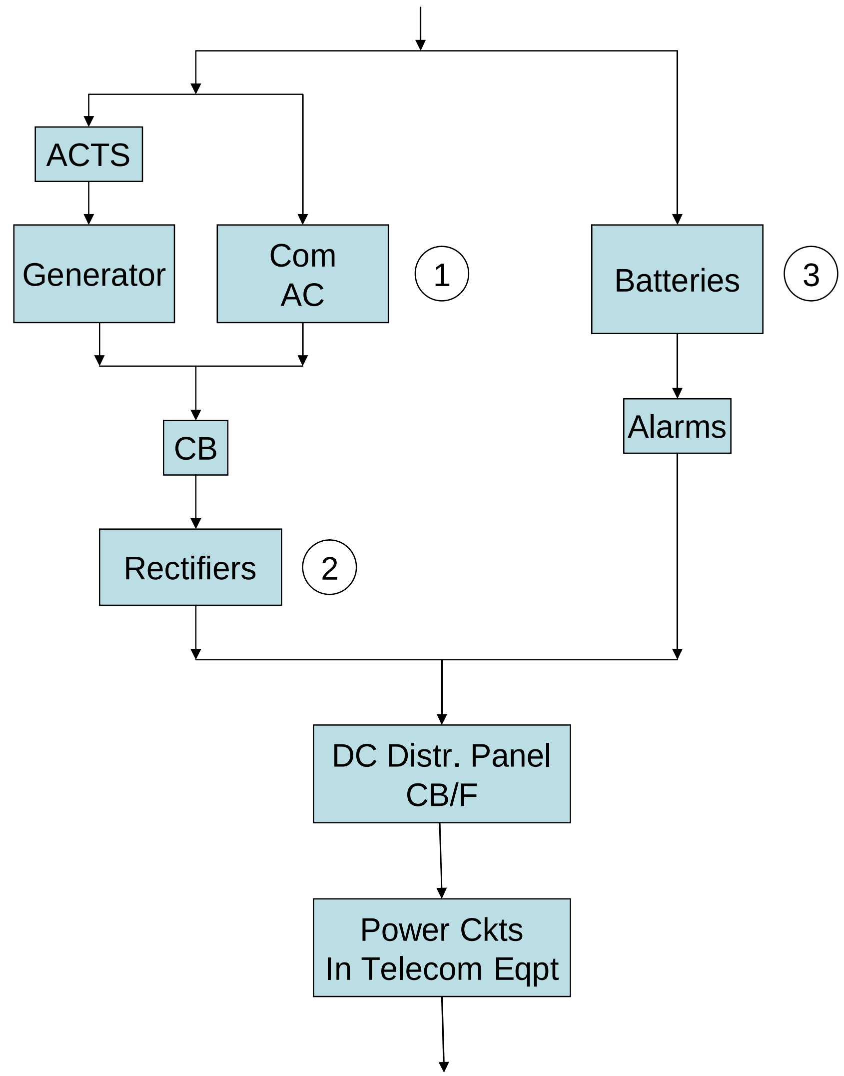
CONCLUSIONS

- It appears that 9-11 was episodic, with telecommunications carrier management and engineers focusing more closely on the reliability of critical infrastructures.
- At this point, it is not known what proportions of this improvement are due to improved engineering, operational, or maintenance processes
  - The abrupt improvement is highly suggestive of operational and maintenance efforts.
  - Perhaps 9-11 served as a wakeup call for service providers when it comes to business and service continuity? Time will tell.

OUTAGE CAUSES

- Trigger cause
  - event that initiates the sequence that finally resulted in the outage
- Direct cause
  - final event in the sequence of events that lead to the outage
- Root cause
  - gives an insight of why the outage occurred, and how to avoid such outages in the future
  - technique called Root Cause Analysis (RCA) [14].

Reliability Diagram with Failure Sequence



Root Cause Analyses: sample outages

Example 1: A lightning strike resulted in a commercial AC power surge, causing the rectifier AC circuit breakers to trip open. This means that AC from either the primary or backup source cannot be converted to DC. As a consequence, the batteries must supply power until the rectifiers are manually switched back on line. The alarm system does not work properly, and the NOC is not notified of the problem. After some time the batteries are exhausted and the communications equipment looses power, and an outage occurs.

- Trigger Cause: Lightning strike.
- Direct Cause: Battery Depletion.
- Root Cause: Maintenance -- Failure to test alarm system.

Root Cause Analyses: sample outages

Example 2: Torrential rains and flooding due to a tropical storm in Houston causes commercial AC power failure. The generators in the communication complexes are supplied with fuel from supply pumps that are located in the basement of the building. Due to the flooding, water entered the basement causing supply pump failure. Hence, the generators ran out of fuel, and the facility goes on battery power. After some time, the batteries stopped supplying power to the equipment thus resulting in an outage.

- Trigger Cause: Storms (Flooding).
- Direct Cause: Battery depletion.
- Root Cause: Engineering failure (The fuel pump system was placed in the basement in an area prone to flooding).

Root Cause Analyses: sample outages

Example 3: A wrench dropped by a maintenance worker landed on an exposed DC power bus which shorted out. Exposed power buses should be covered before maintenance activity starts. Maintenance personnel error can be reduced by providing sufficient training to personnel.

- Trigger Cause: Dropping a tool.
- Direct Cause: DC short circuit.
- Root Cause: Human error

Impact of Outages Studied
(Trigger and Root Causes)

Impact Category	Lost Customer Hours (LCH) In Thousands	Number of Outages
Low	LCH < 250	89
Medium	250 LCH < 1,000	30
High	1,000	31

Trigger Cause	Total Outages	Low Impact	Medium Impact	High Impact
Natural Disasters	14 %	8 %	16 %	29 %
Power Surges	18 %	23 %	10 %	13 %
Comm. AC Loss	38 %	39 %	37 %	35 %
Human Errors	30 %	30 %	37 %	23 %
Total	**100 %**	**100 %**	**100 %**	**100 %**

Root Cause	Total Outages	Low Impact	Medium Impact	High Impact
Engn. Error	2 %	4 %	3 %	35 %
Install. Error	23 %	27 %	27 %	10 %
Opns. Error	33 %	37 %	33 %	23 %
Maint. Error	27 %	26 %	37 %	23 %
Unforeseen	5 %	6 %	0.0 %	10 %
Total	**100%**	**100%**	**100%**	**100%**

Failing Power Component Associated with Root Cause

Component	Total Outages	Low Impact	Med. Impact	High Impact
Rectifiers	14%	9%	20%	23%
Batteries	13%	9%	23%	16%
Generators	18%	16%	13%	29%
AC Cir. Breakers	20%	23%	17%	16%
Comm. Equip.	12%	15%	10%	7%
DC Fuse/CB	10%	13%	8%	6%
Comm. AC	2%	3%	0%	0%
AC Trans Switch	3%	3%	3%	0%
Alarm Systems	7%	9%	3%	3%
Environ. Systems	1%	0%	3%	0%
Total	**100%**	**100%**	**100%**	**100%**

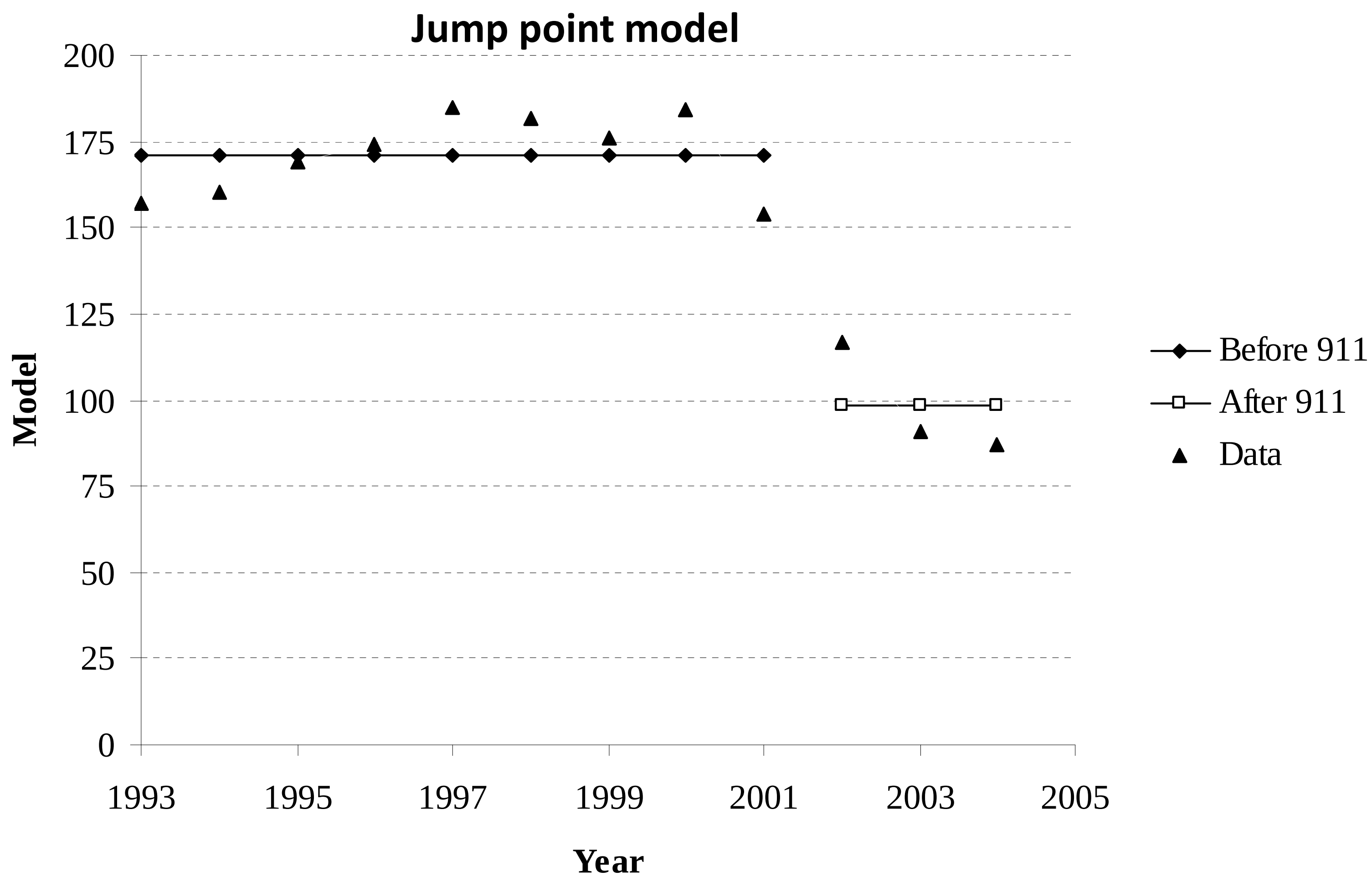
CONCLUSIONS

- The trigger, root cause, and equipment most associated with the root cause, have been examined by outage impact for telecommunications power outages over an eight year period
- This analysis has provided insights into these outages, and should be of interest to carriers, regulators, and Homeland Security
- There are two aspects of these results:
  - Proactive
    - Carrier industry adoption of NRIC Best Practices can go a long way to prevent such outages;
    - Following best practices could have prevented 75% of the outages.
    - The other 25% could not be determined from the reports.
  - Reactive
    - An emphasis on rectifier and generator recovery (e.g. spare parts, training, etc.) can help, as over half of high impact outages are due to problems with these components.

Case 4: SS7 Outages Assessment by Poisson Regression & RCA

"A Pre And Post 9-11 Analysis Of SS7 Outages In The Public Switched Telephone Network" by Garima Bajaj, Andrew P. Snow and Gary Weckman

Reliability Poisson model for all FCC-Large Scale Reportable Outages over 10 Years



Outline

A. **Telecom & Network Infrastructure Risk**
B. **Telecommunications Infrastructure**
C. **RAMS: Reliability, Availability, Maintainability and Survivability**
D. **Protection Level Assessment & Forecasting**

Thank You!!