Resiliency Threats to Critical Infrastructures

Andy Snow, PhD
School if Information & Telecommunication Systems
Ohio University
asnow@ohio.edu

Outline

A. **Telecom & Network Infrastructure Risk**
B. **Telecommunications Infrastructure**
C. **RAM (Reliability, Availability, Maintainability) and Resiliency**

Outline

A. Telecom & Network Infrastructure Risk

B. Telecommunications Infrastructure

C. Reliability, Availability, Maintainability (RAM) and Resiliency

A. Telecom & Network Infrastructure 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”
  - Overestimate the chance of good outcomes
  - Underestimate the chance of bad outcomes
- Which is more likely?
  1. Winning the “Big Lotto”
  2. Getting hit by lightning
  3. Being killed by a large asteroid over an 80-year lifetime

Human Perceptions of Risk

- Perceptions of "Rare Events"
  - Overestimate the chance of good outcomes
  - Underestimate the chance of bad outcomes
- Which is more likely?
  1. Winning the "Big Lotto"
  2. Getting hit by lightning

  About 1 in 5 Million

  3. Being killed by a large asteroid over an 80-year lifetime (about 1 chance in 1 Million)*

*A. Snow and D. Straub, "Collateral damage from anticipated or real disasters: skewed perceptions of system and business continuity risk?", IEEE Engineering Management Conference (IEMC2005), 2005, pp. 740-744.

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
  - Spend too little – too much risk
  - Spend too much – waste of money
- There is an elusive equilibrium point

We Focus 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

But Things Go Wrong!

- Central Office facility in Louisiana
- Generators at ground level outside building
- 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
  - Tsunami protection: a 10 meter wall

Fukushima Nuclear Accident (Continued)

- Design vulnerabilities?
  - Nuclear plant requires AC Power for cooling
  - Tsunami wall 10 meters high, in a country where in the last 100 years numerous > 10 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

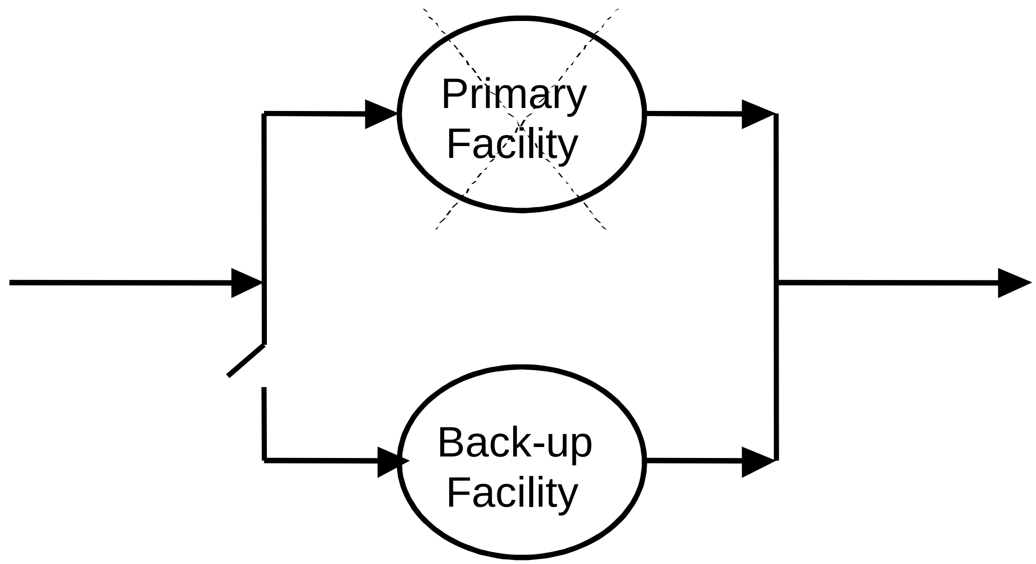
Sequence of Events: Fukushima Nuclear Accident

1. Large land based and ocean floor earthquake
   - AC transmission lines fall
   - Twelve 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 10 meter tsunami wall !!!!

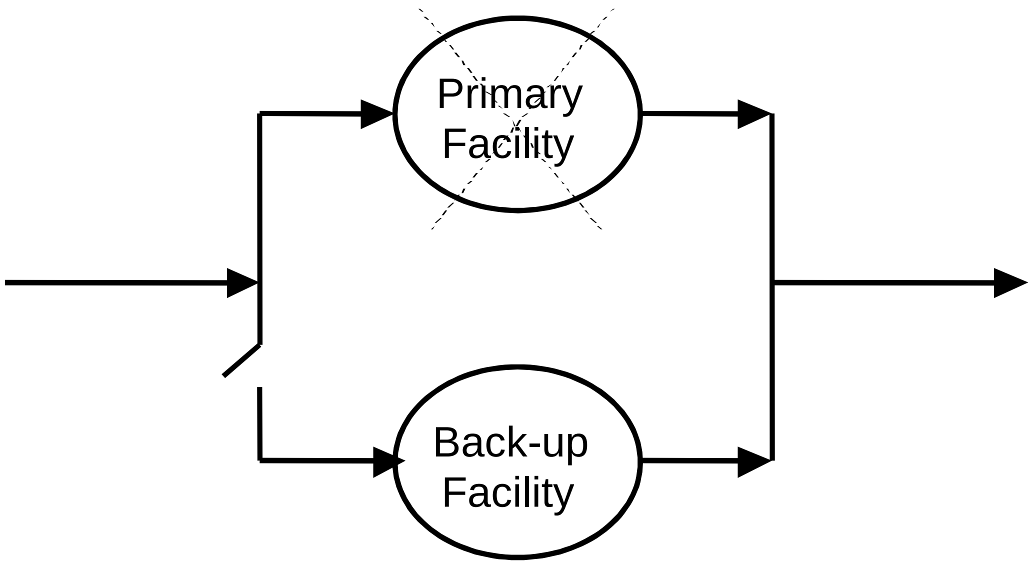
9-11 Effect
Geographic Dispersal of Human and ITC Assets

Pre 9-11 IT Redundancy



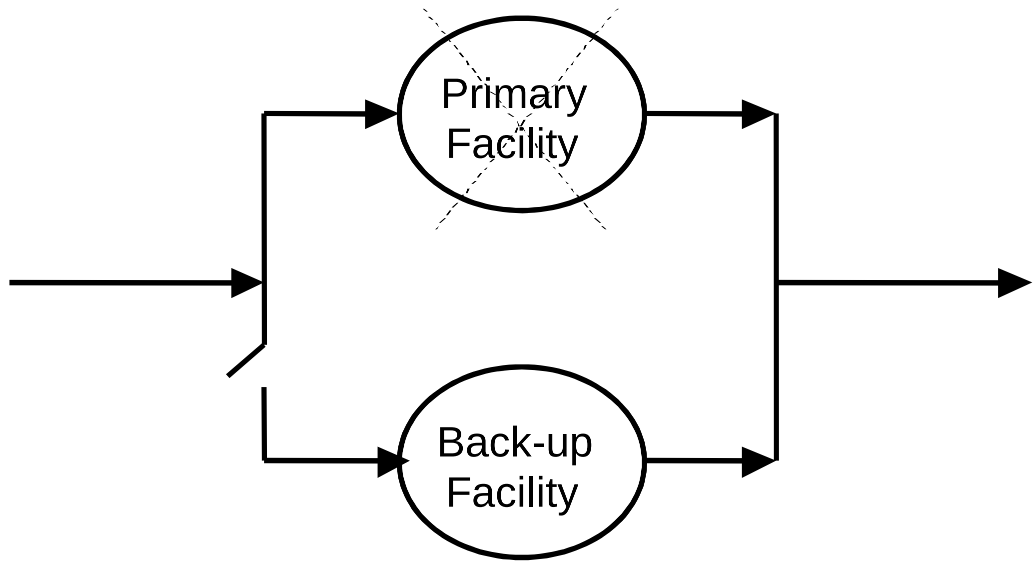
Scenario	Single IT Facility Reliability	Redundant IT Facility Reliability
1	0.90	0.9900
2	0.95	0.9975
3	0.99	0.9999

Key Assumptions



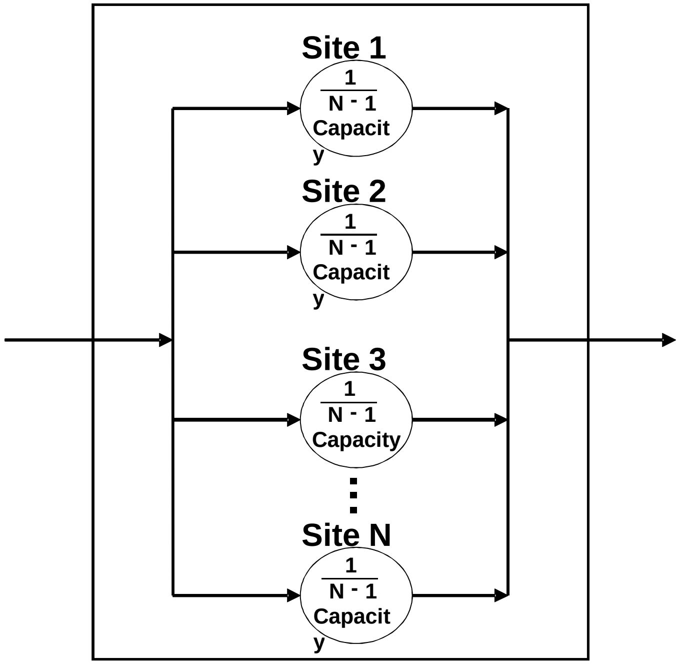
1. Failures are independent
2. Switchover capability is perfect

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.

Challenges in Ensuring Resilient Critical Infrastructure

- Communication Infrastructure Convergence
- Communication Industry Sector Consolidations
- Intra- and Inter - Sector Dependence
- High Resiliency = = $$$$
- Assessing Risk is difficult
- Vulnerability Dilemma: Secrecy vs. Sunshine

Convergence, Consolidation and Interdependence

- The outages of yester-year affected voice, data <u>OR</u> video
- The outages of today and tomorrow affect all three.
  - Technological convergence
  - Telecom mergers and acquisitions
- Inter-sector dependence
  - Geographic overlay of telecom, natural gas, electricity, and water?
  - Telecom needs power…..power needs telecom
  - SCADA separate from IT?

High Resiliency Levels = = $$$$

– Who Pays??
– Regulatory Regime: Unregulated vs. Price Cap vs. Rate-of-Return (RoR)
– Competitive vs. Noncompetitive markets
– Service Provider Economic Equilibrium Points
  - Economies of Scale vs. Vulnerability Creation
  - Proactive vs. Reactive Restoration Strategies
  - Geography: Urban vs Rural

Assessing Risk is Difficult

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

Vulnerability Dilemma: Secrecy vs. Sunshine

- Market correction of vulnerabilities vs. Exposing CIP to exploitation
- Known vs. Unknown vulnerabilities
- Customer knowledge of service provider vulnerabilities?
- Data sharing
  - National, Regional, State, County, Municipal
- Tracking outages as a bellwether for Resiliency deficits
  - Establishing measures and reporting thresholds
- Tracking frequency, size, duration of events

Infrastructure Protection and Risk

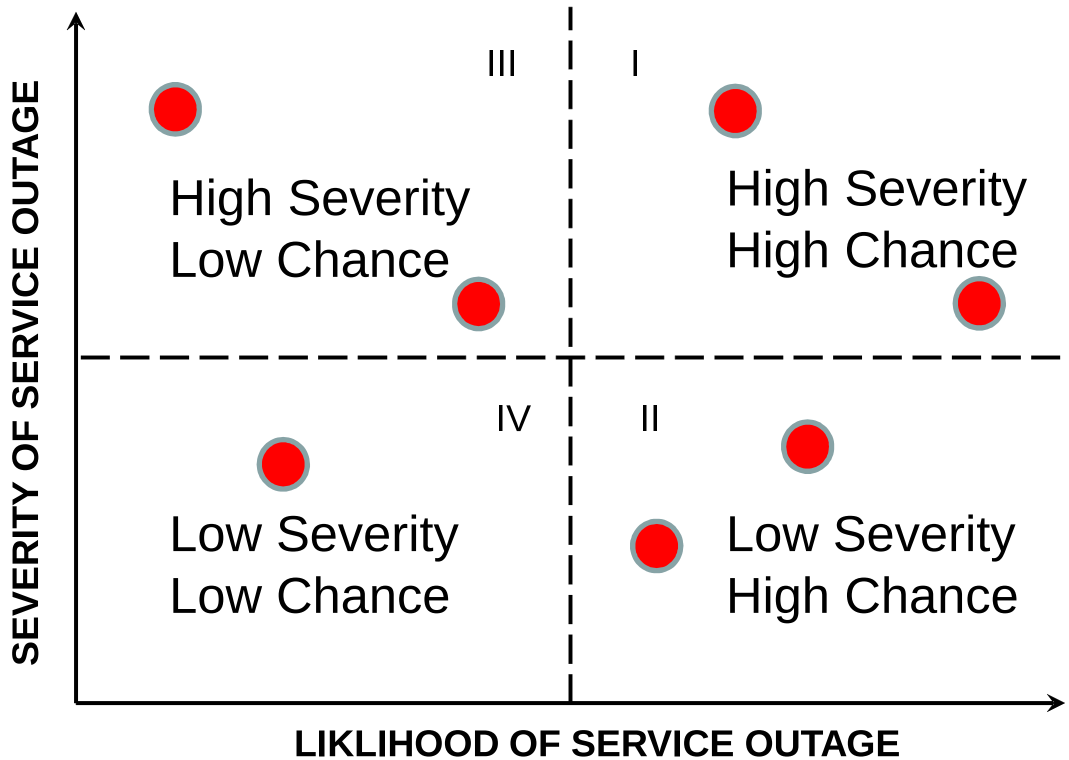
- Outages
- Severity
- Likelihood
- Fault Prevention, Tolerance, Removal and Forecasting

Infrastructure Protection and Risk

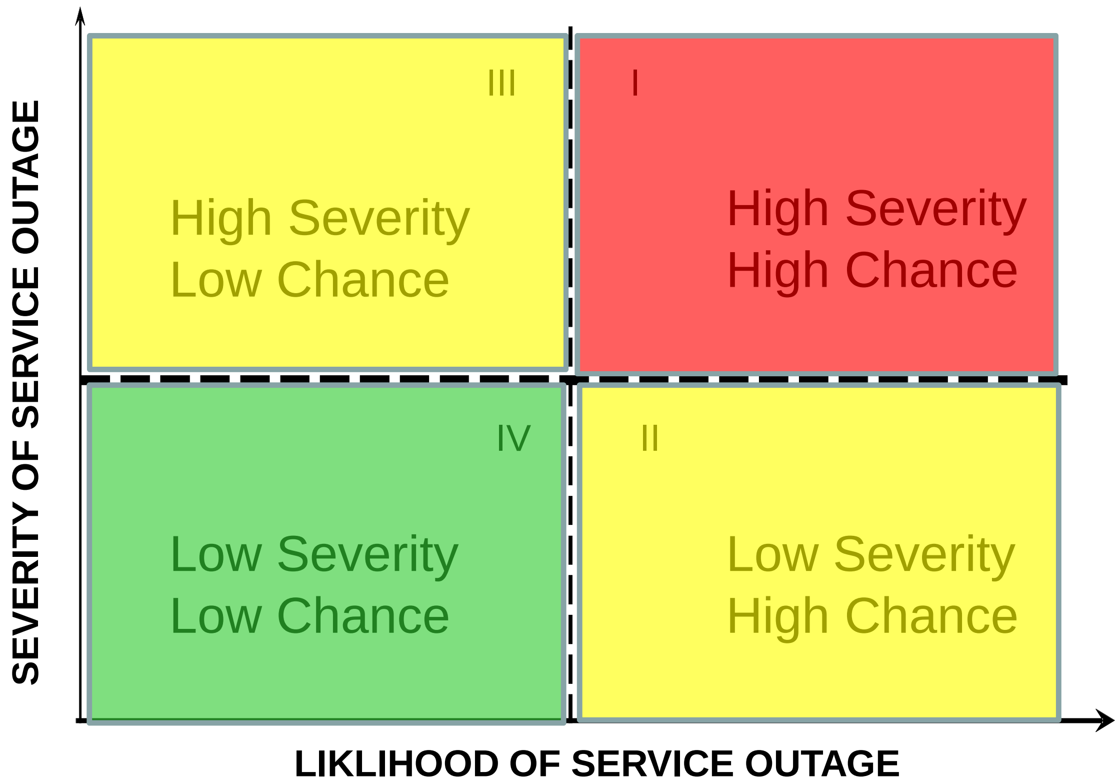
- Outages
- Severity
- Likelihood
- Fault Prevention, Tolerance, Removal and Forecasting

RISK

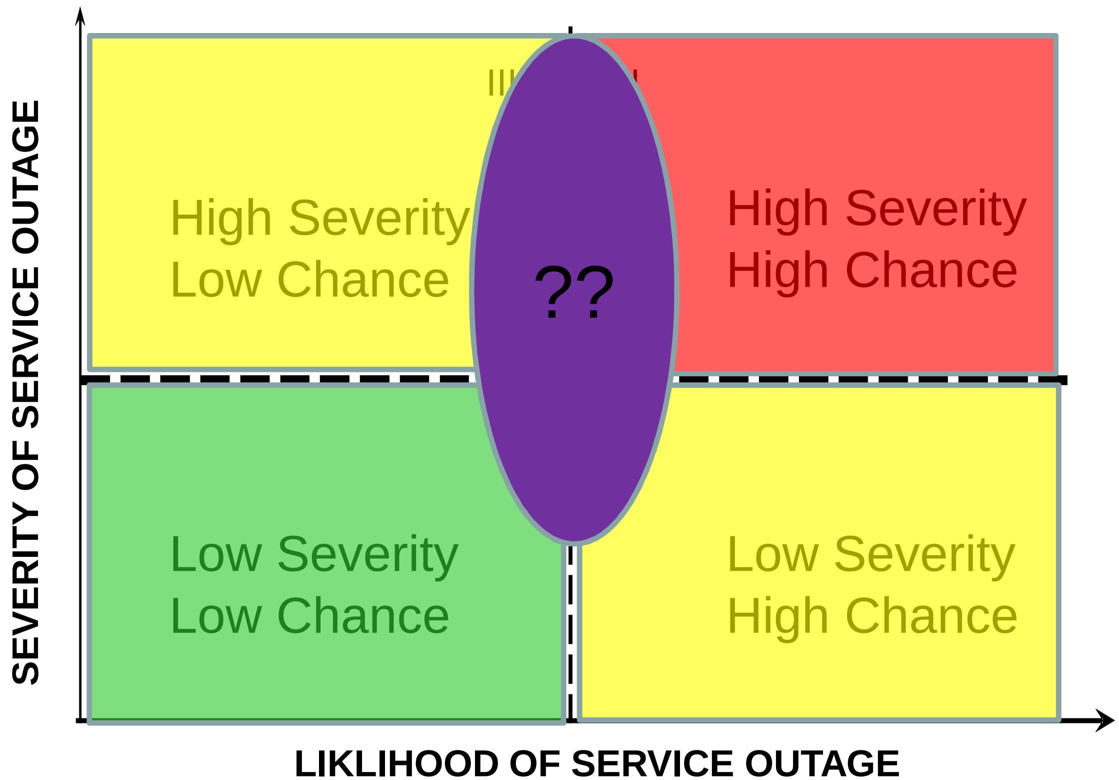
Risk – ID & Map Vulnerabilities



Risk


III
I
High Severity
Low Chance
High Severity
High Chance
IV
II
Low Severity
Low Chance
Low Severity
High Chance
SEVERITY OF SERVICE OUTAGE
LIKLIHOOD OF SERVICE OUTAGE

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

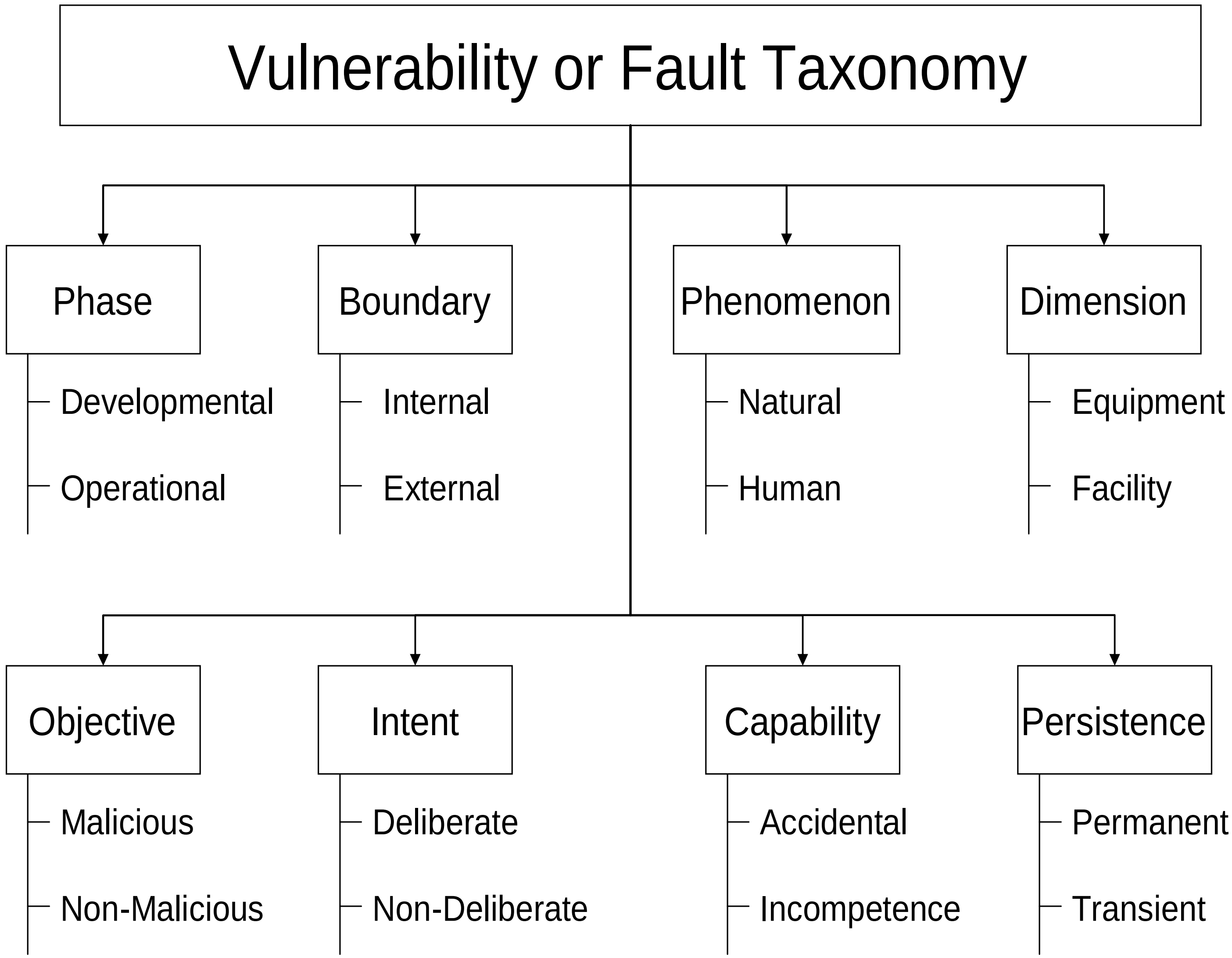
- *Vulnerability* is a weakness or a state of susceptibility which opens up the infrastructure to a possible outage due to attack or circumstance.
- The cause of a vulnerability, or error state, is a system *fault*.
- The potential for a vulnerability to be exploited or triggered into a disruptive event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

Telecommunication Infrastructure 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.

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

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??

Some Conclusions about Vulnerability

- Vulnerability highly situational, facility by facility

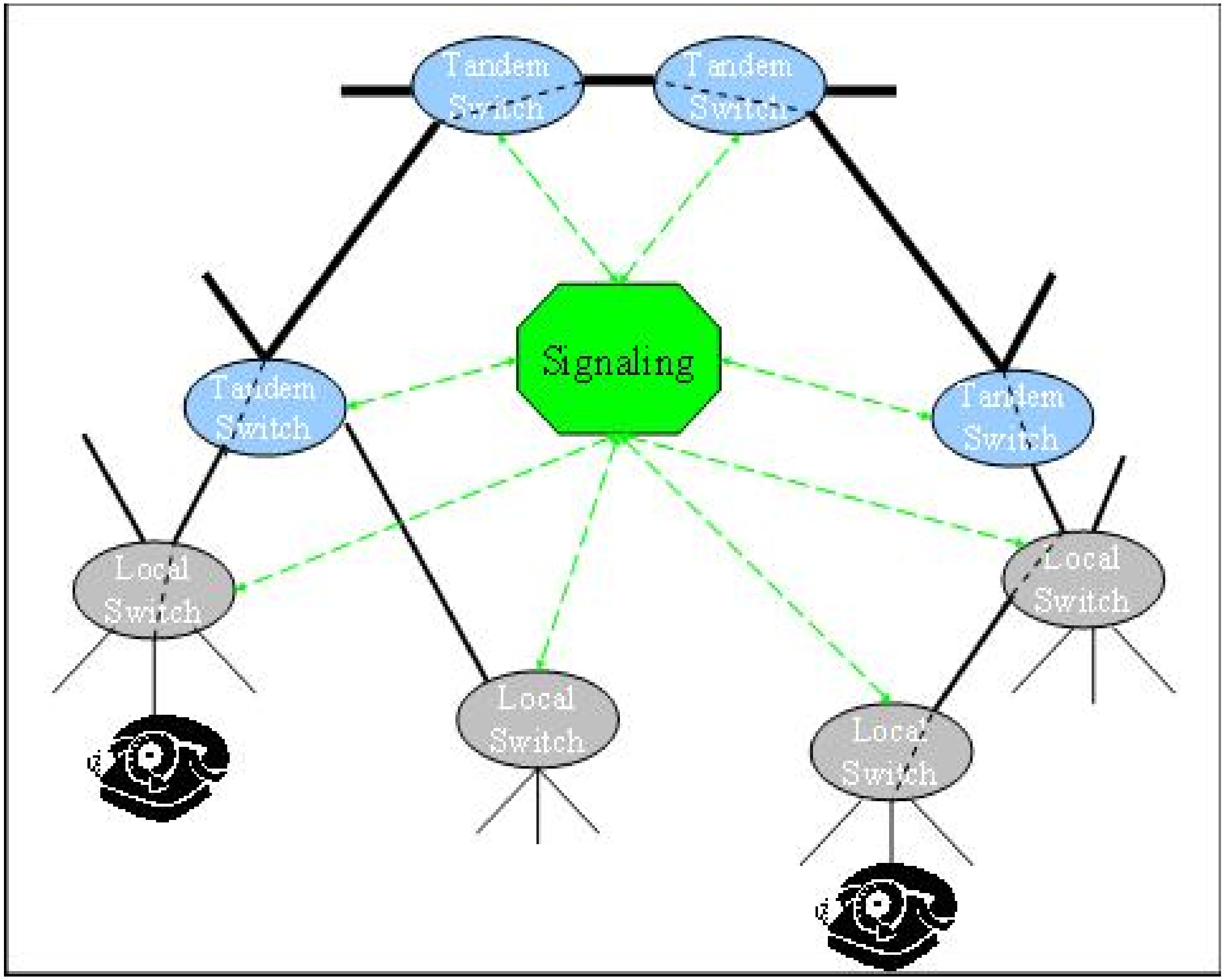
Outline

A. **Telecom & Network Infrastructure Risk**
B. ***Telecommunications Infrastructure***
C. **RAMS and Resiliency**

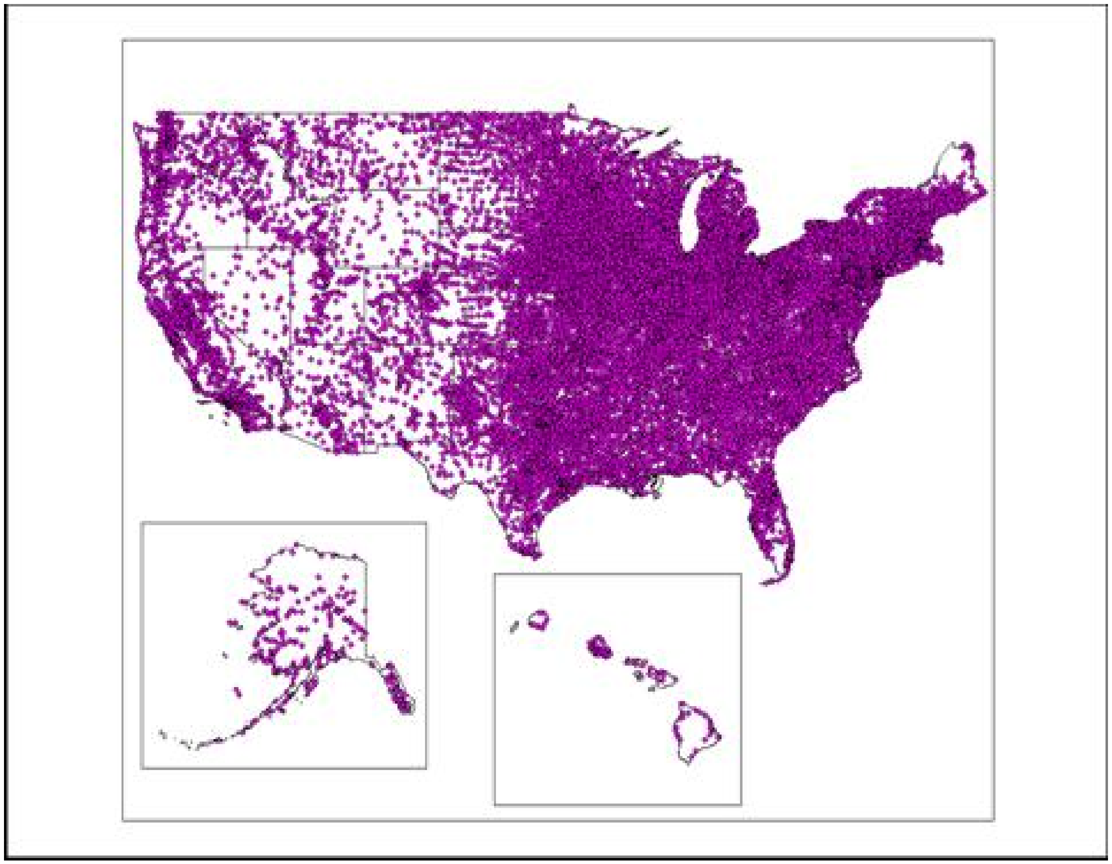
B. Telecommunications Infrastructure

- Wireline architecture and vulnerabilities
- Wireless architecture and vulnerabilities

PSTN End to End Connections

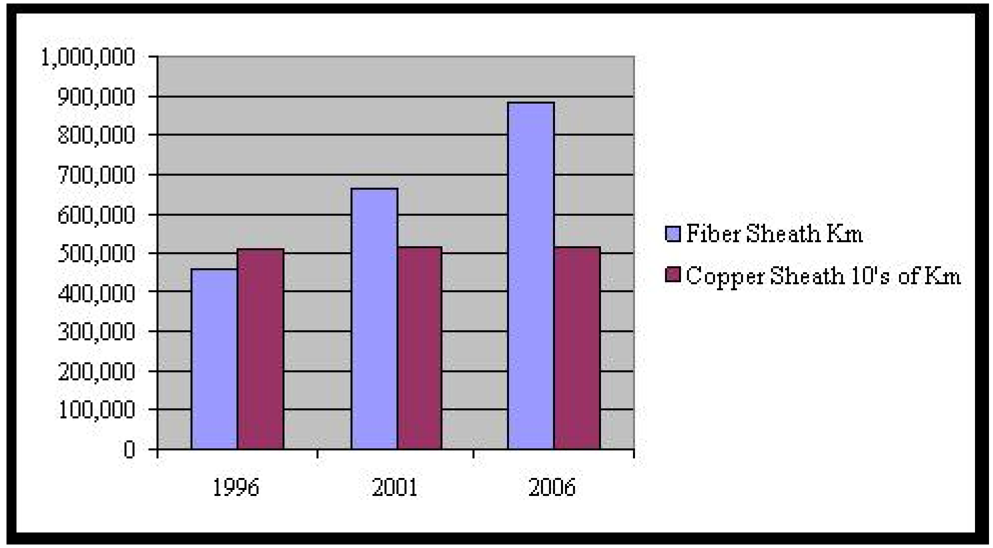


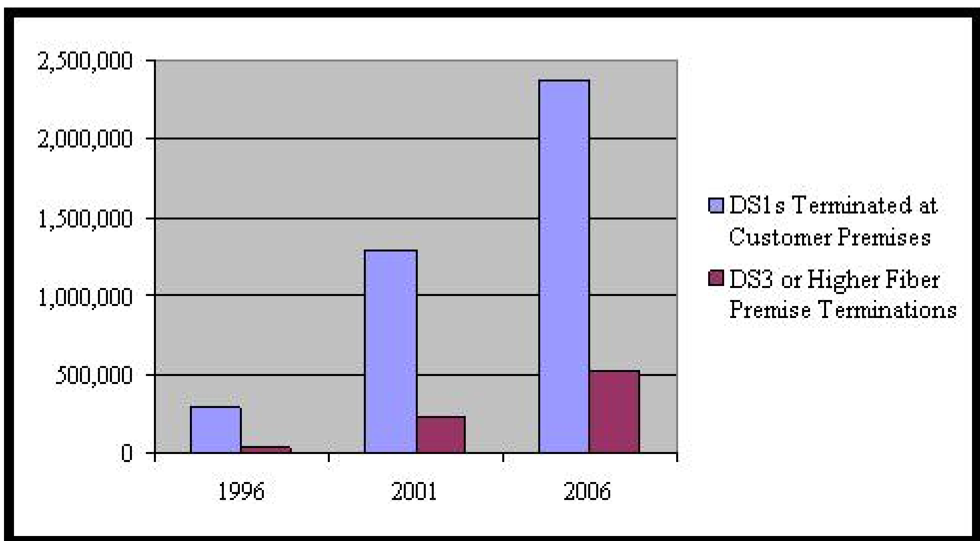
Switching Infrastructure Dispersal/Concentration



Retrieved from Wikipedia
http://en.wikipedia.org/wiki/Image:Central_Office_Locations.png

US Growth in Fiber & High Speed Digital Circuits to Customer Premises





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

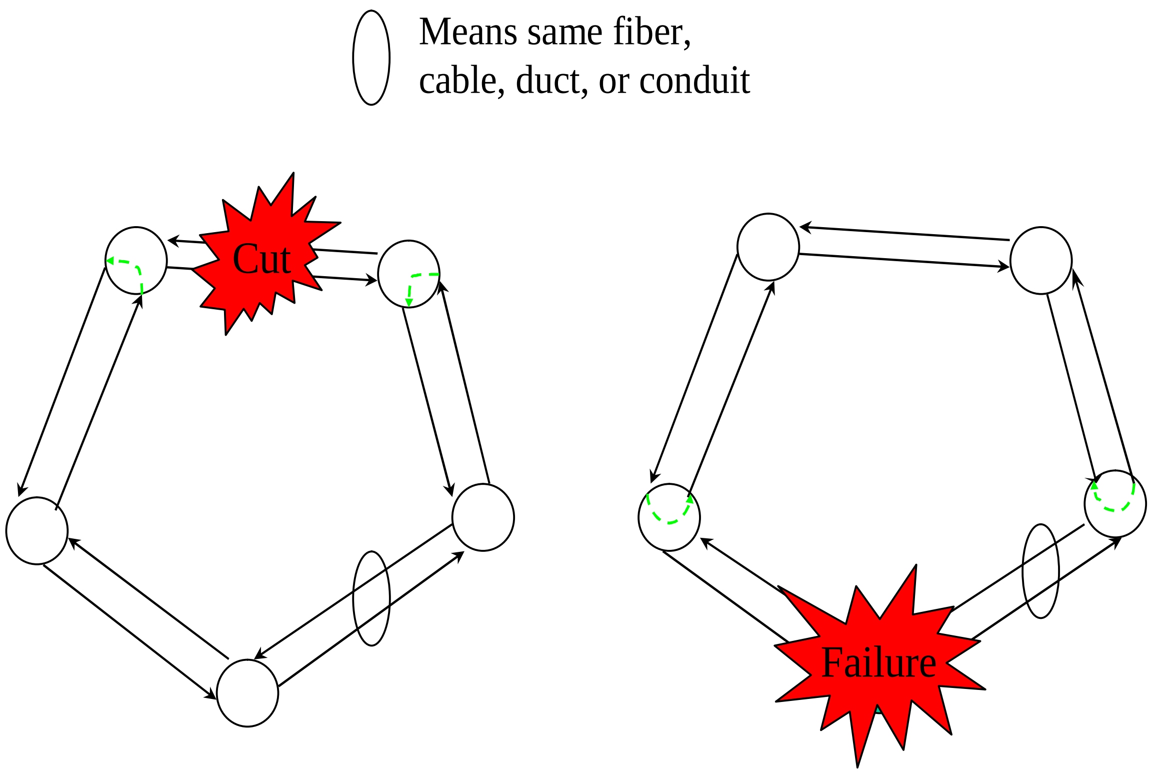
Transmission Vulnerabilities

- 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 and auto/truck accidents damaging cables at these points

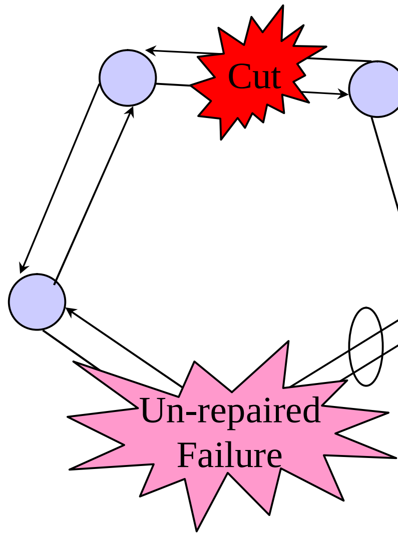
Transmission Vulnerabilities

- Fiber transmission failures inside carrier facilities:
  - Studies by FCC staff and other researchers 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.

Proper SONET Ring Operation



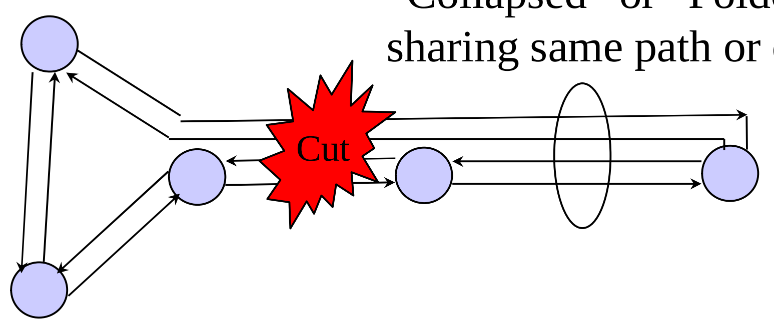
Improper Operation of SONET Rings



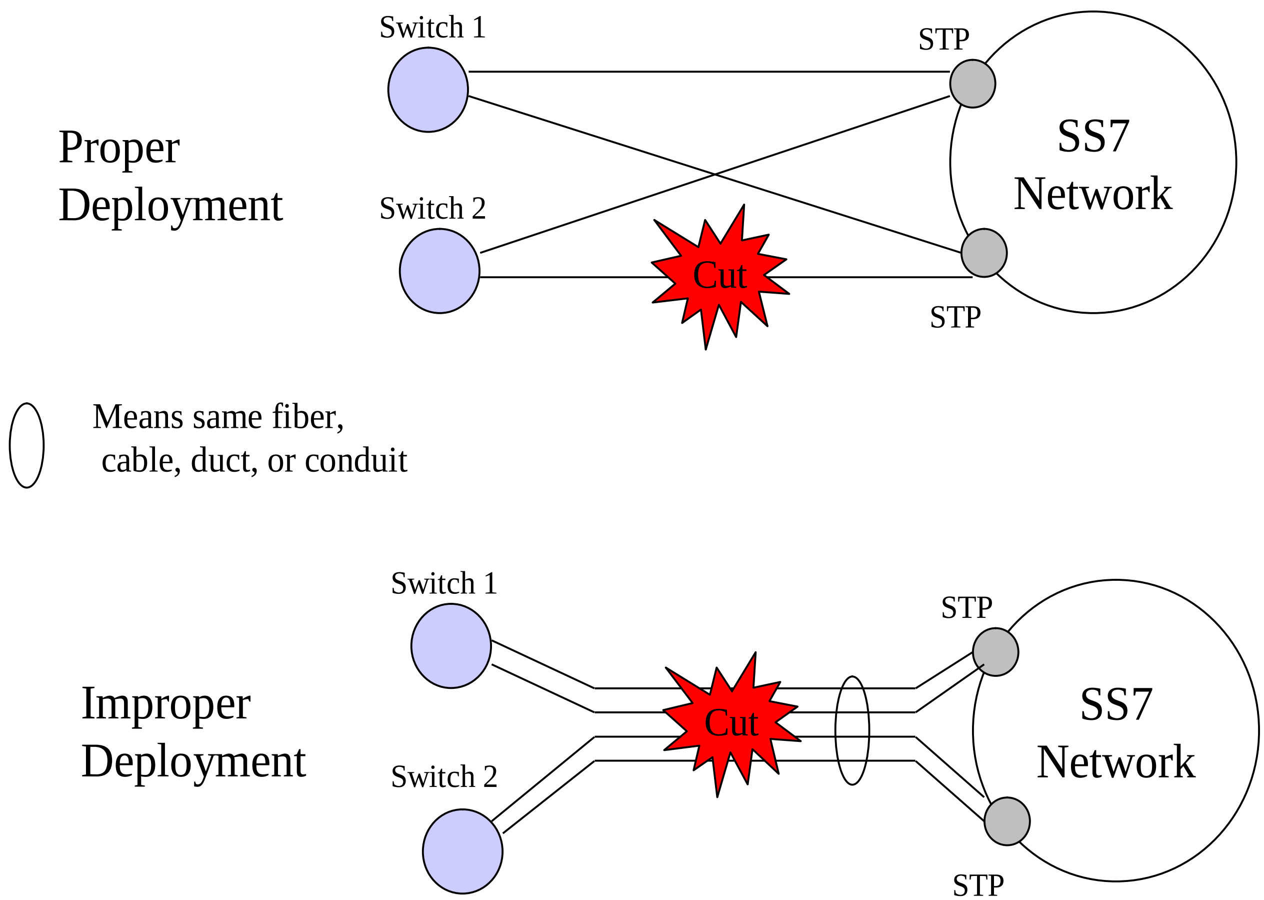
Improper Maintenance:
Node's previous failure, and subsequent fiber cut prior to spare on hand

Means same fiber, cable, duct, or conduit

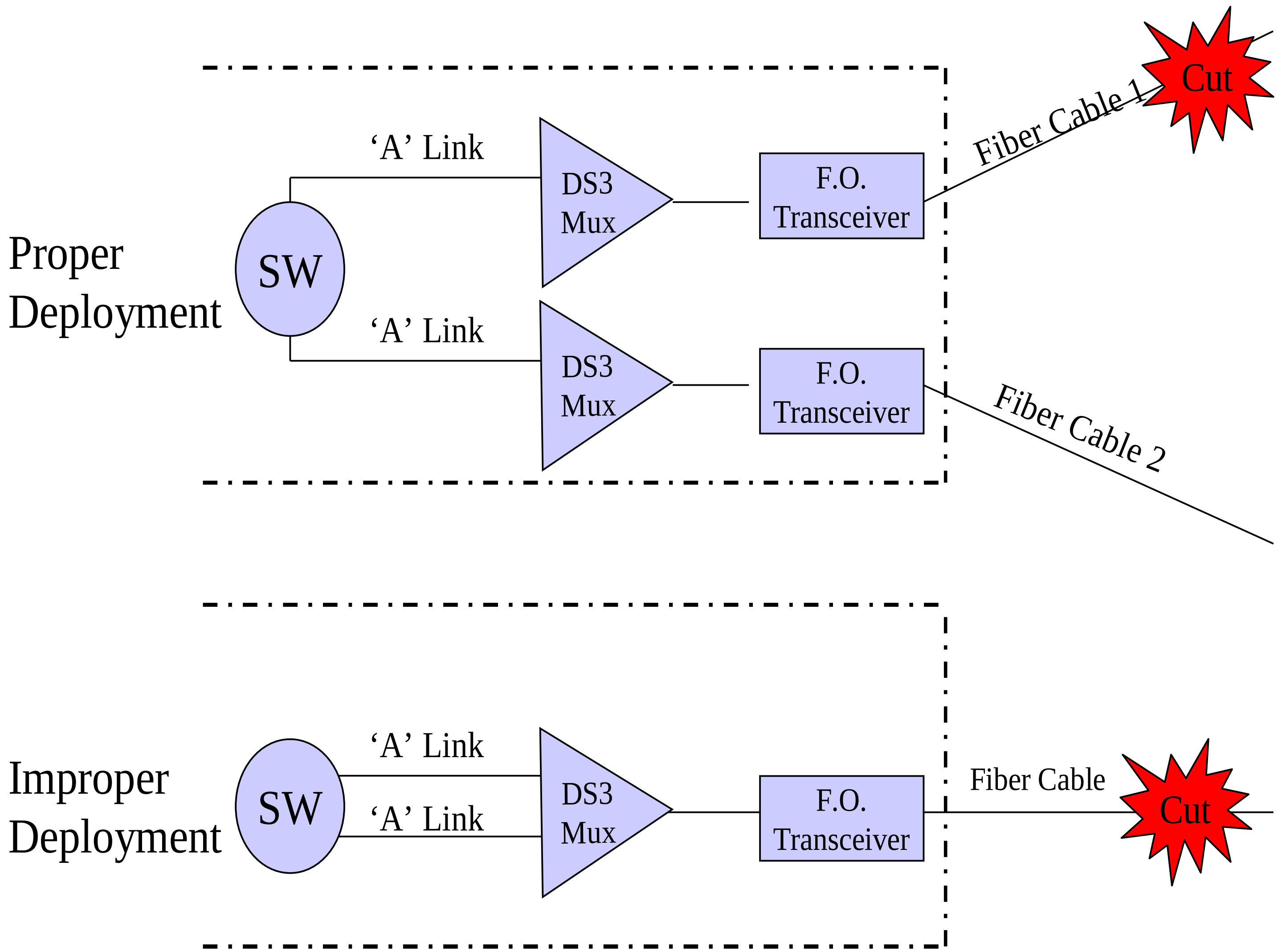
Improper Deployment:
"Collapsed" or "Folded" Ring sharing same path or conduit



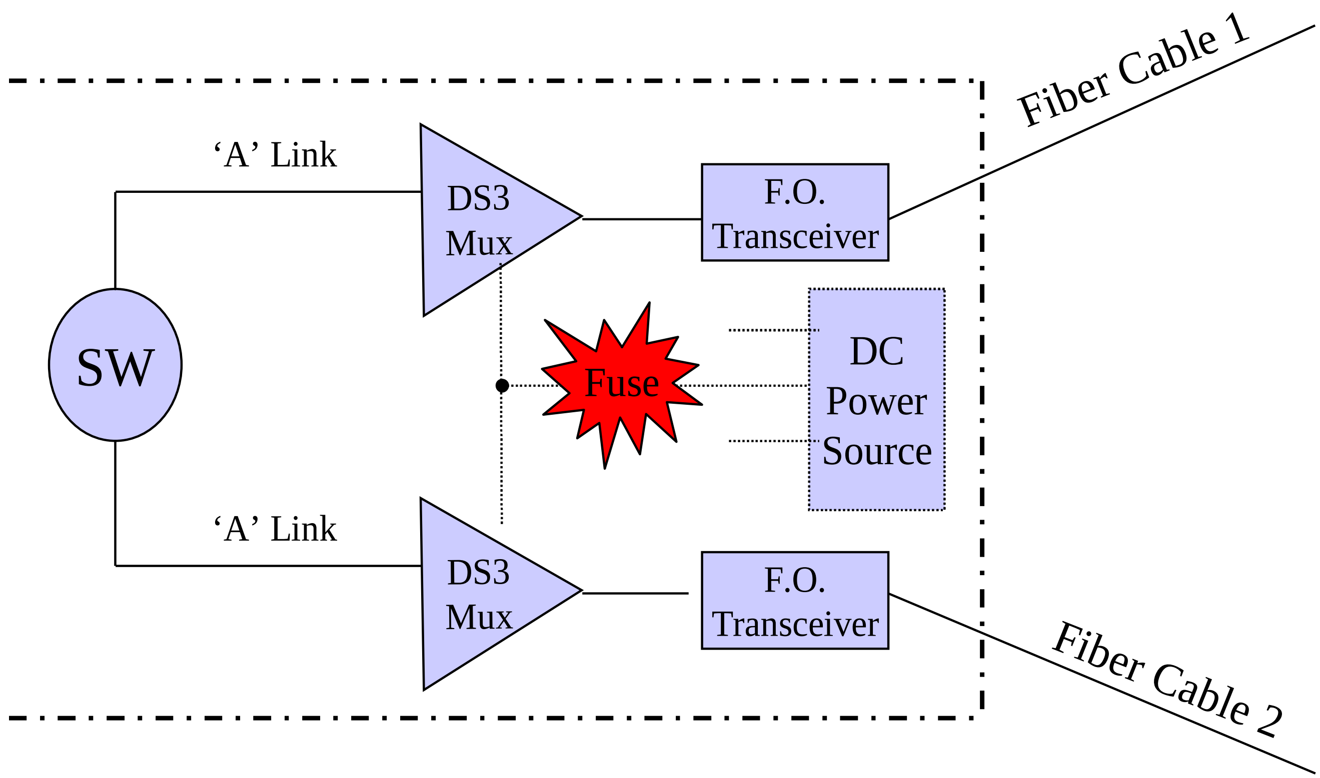
SS7 A-Links


Switch 1
STP
Proper
Deployment
SS7
Network
Switch 2
Cut
STP
Means same fiber,
cable, duct, or conduit
Switch 1
STP
Improper
Deployment
SS7
Network
Cut
Switch 2
STP

SS7 A-Links


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

SS7 A-Links



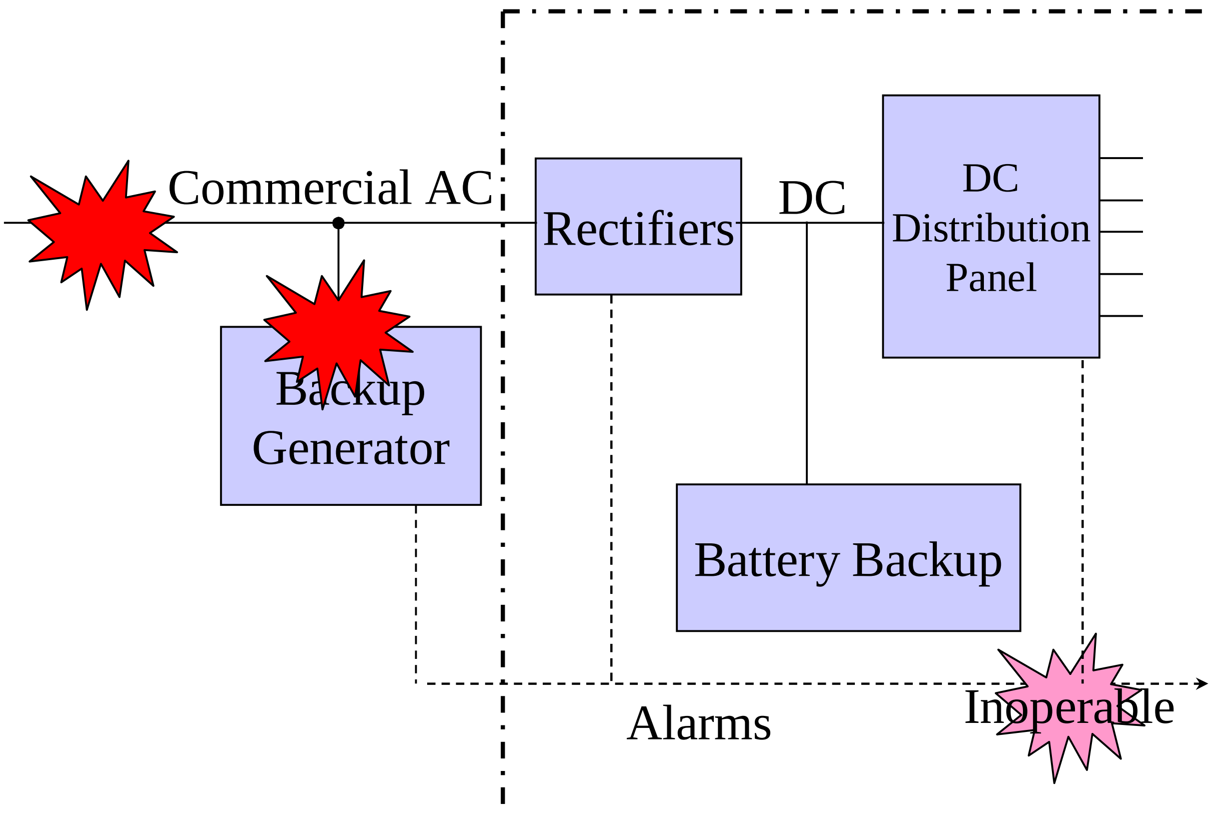
'A' Link
DS3
Mux
F.O.
Transceiver
Fiber Cable 1
SW
Fuse
DC
Power
Source
'A' Link
DS3
Mux
F.O.
Transceiver
Fiber Cable 2

Power Architecture & Vulnerabilities

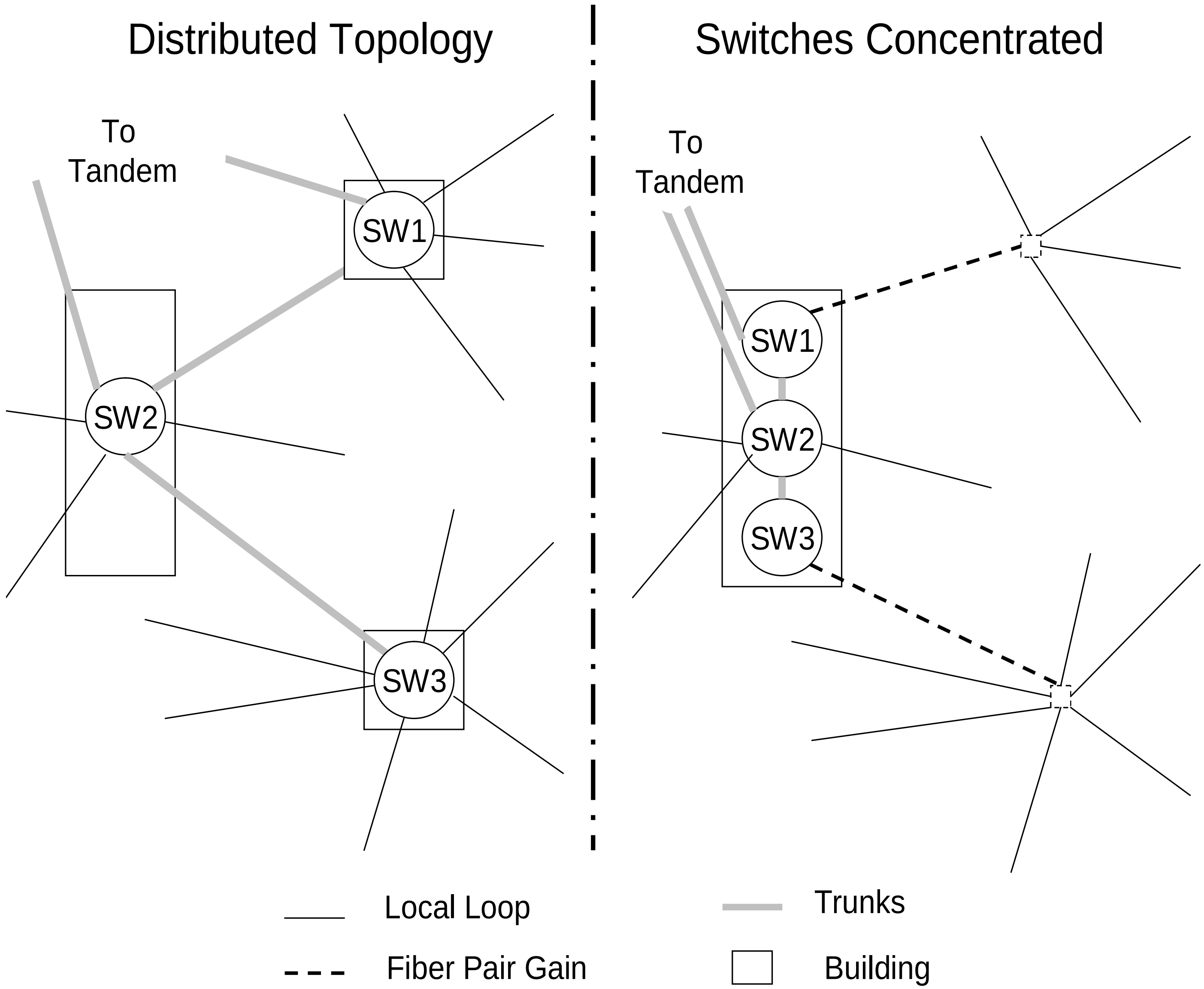
- Redundant Power
  - Commercial AC
  - AC Generator backup
  - Batteries for uninterruptible power systems (UPS)

Inoperative Alarms

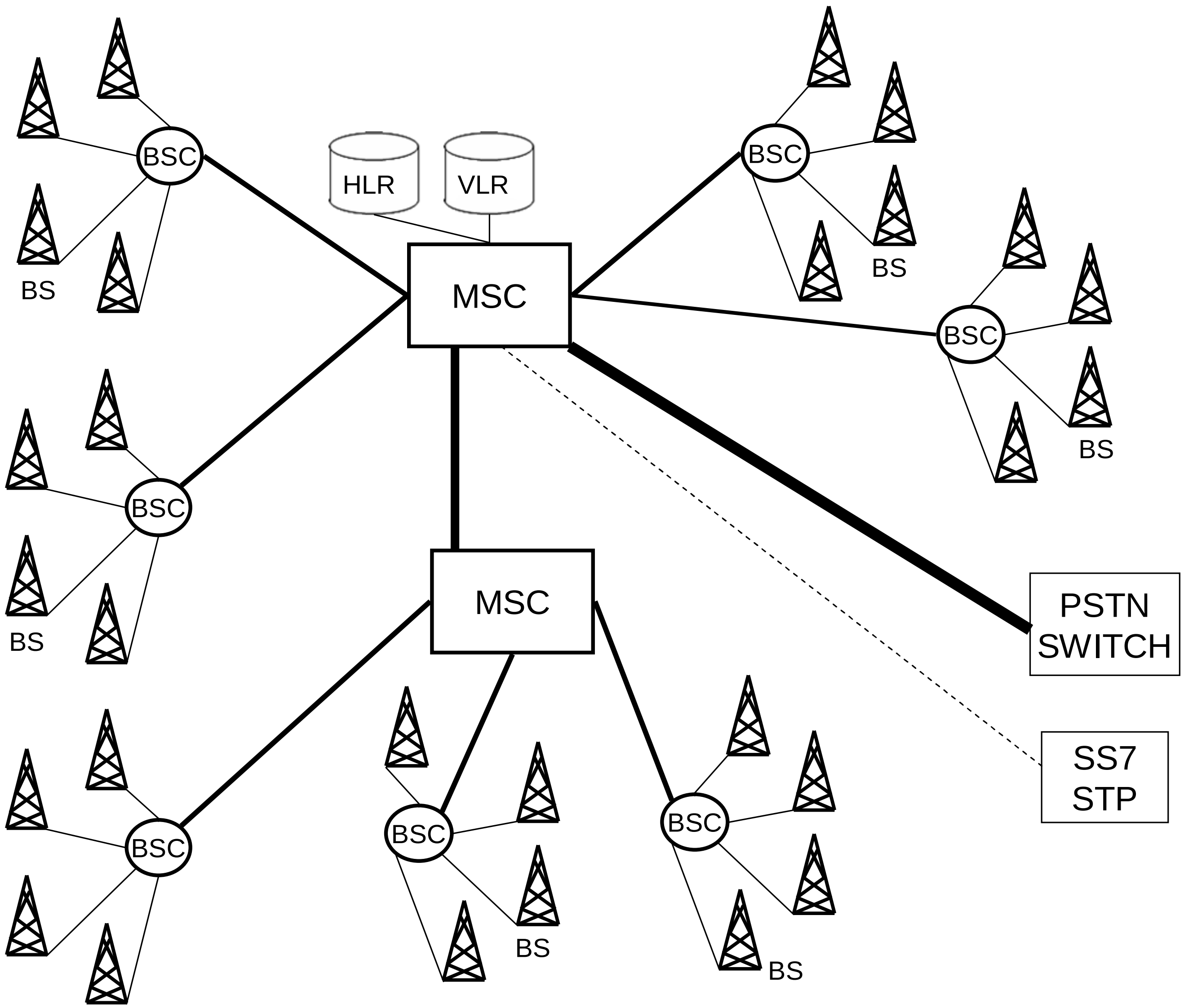
- Loss of commercial power
- Damaged generator
- Untested or inoperable alarms prior to loss and damage
- Batteries Deplete



Economy of Scale Over-Concentration Vulnerabilities



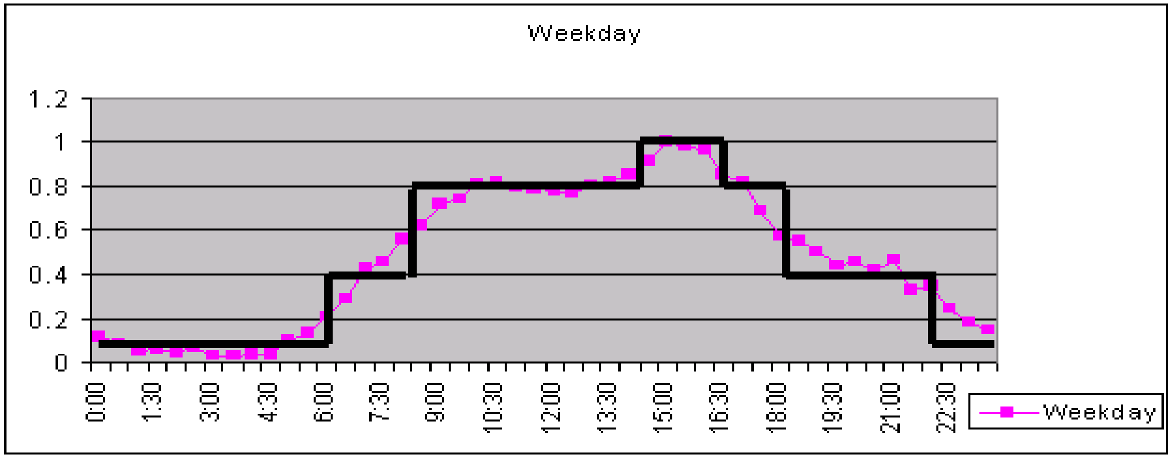
PCS Architecture

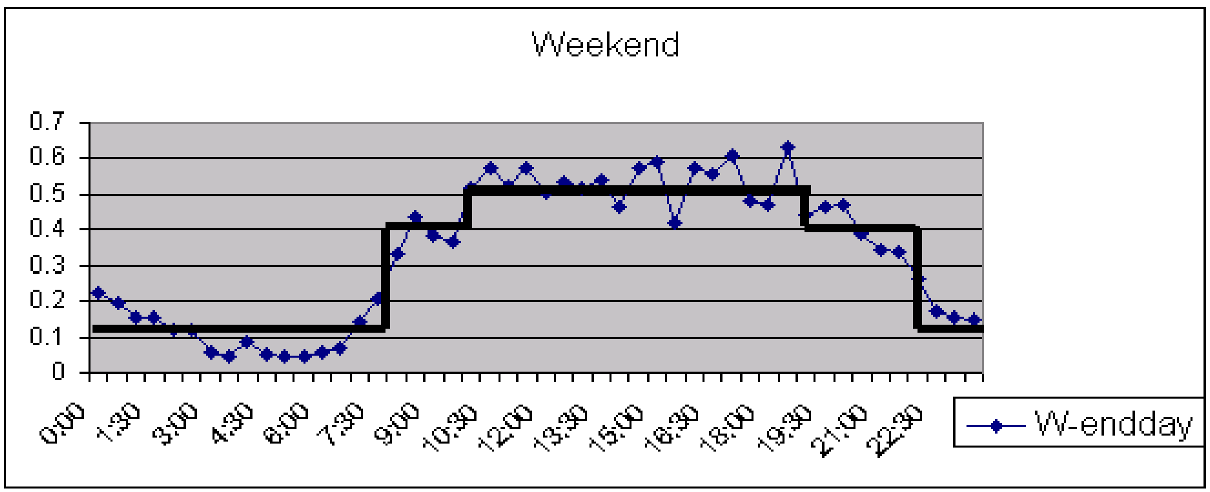


PCS Component Failure Impact

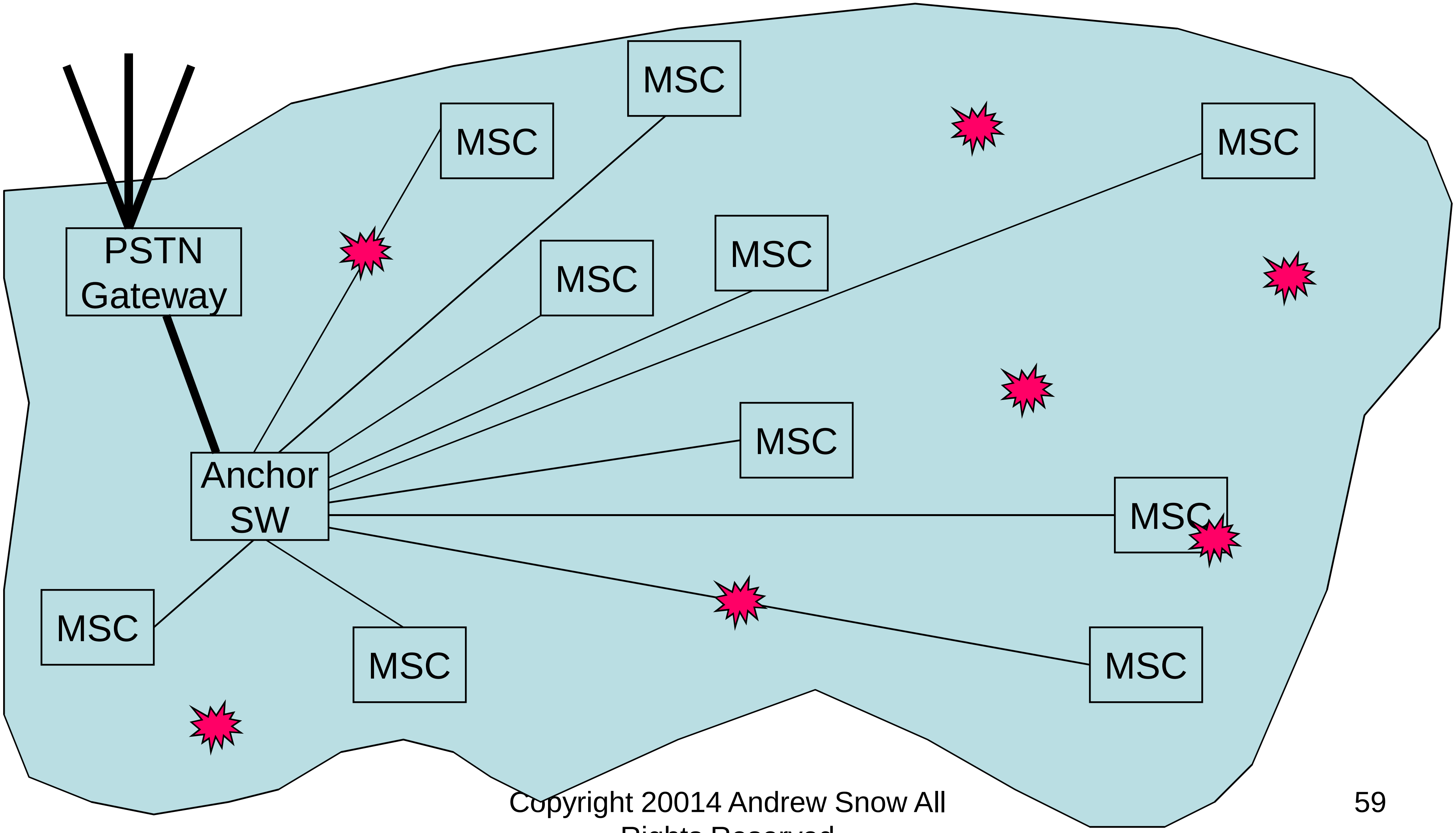
Components	Users Potentially Affected
Database	100,000
Mobile Switching Center	100,000
Base Station Controller	20,000
Links between MSC and BSC	20,000
Base Station	2,000
Links between BSC and BS	2,000

Outages at Different Times of Day Impact Different Numbers of People

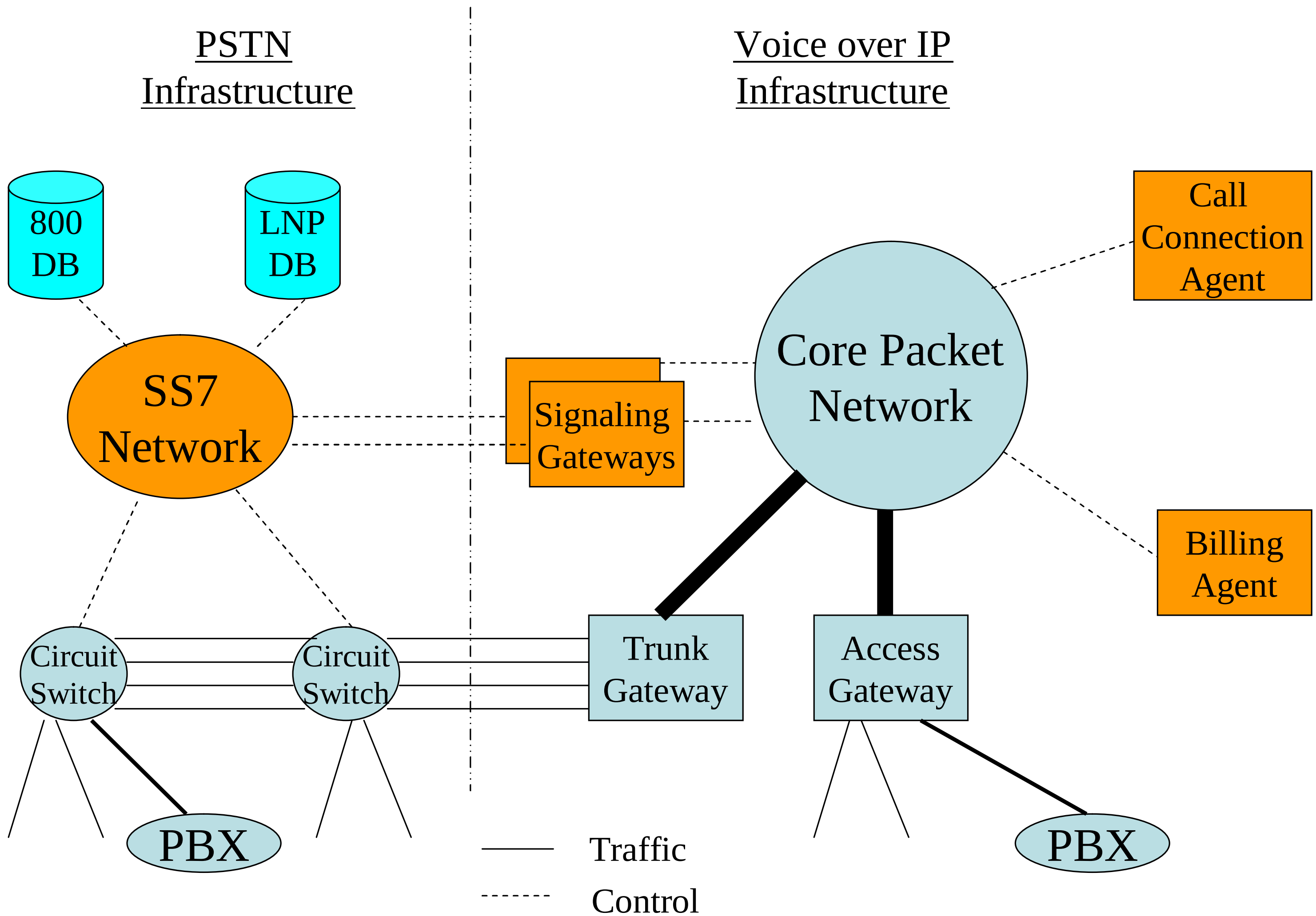




Concurrent Outages are a Challenge for Network Operators



Circuit to Packet Switch Interface



Outline

A. Telecom & Network Infrastructure Risk

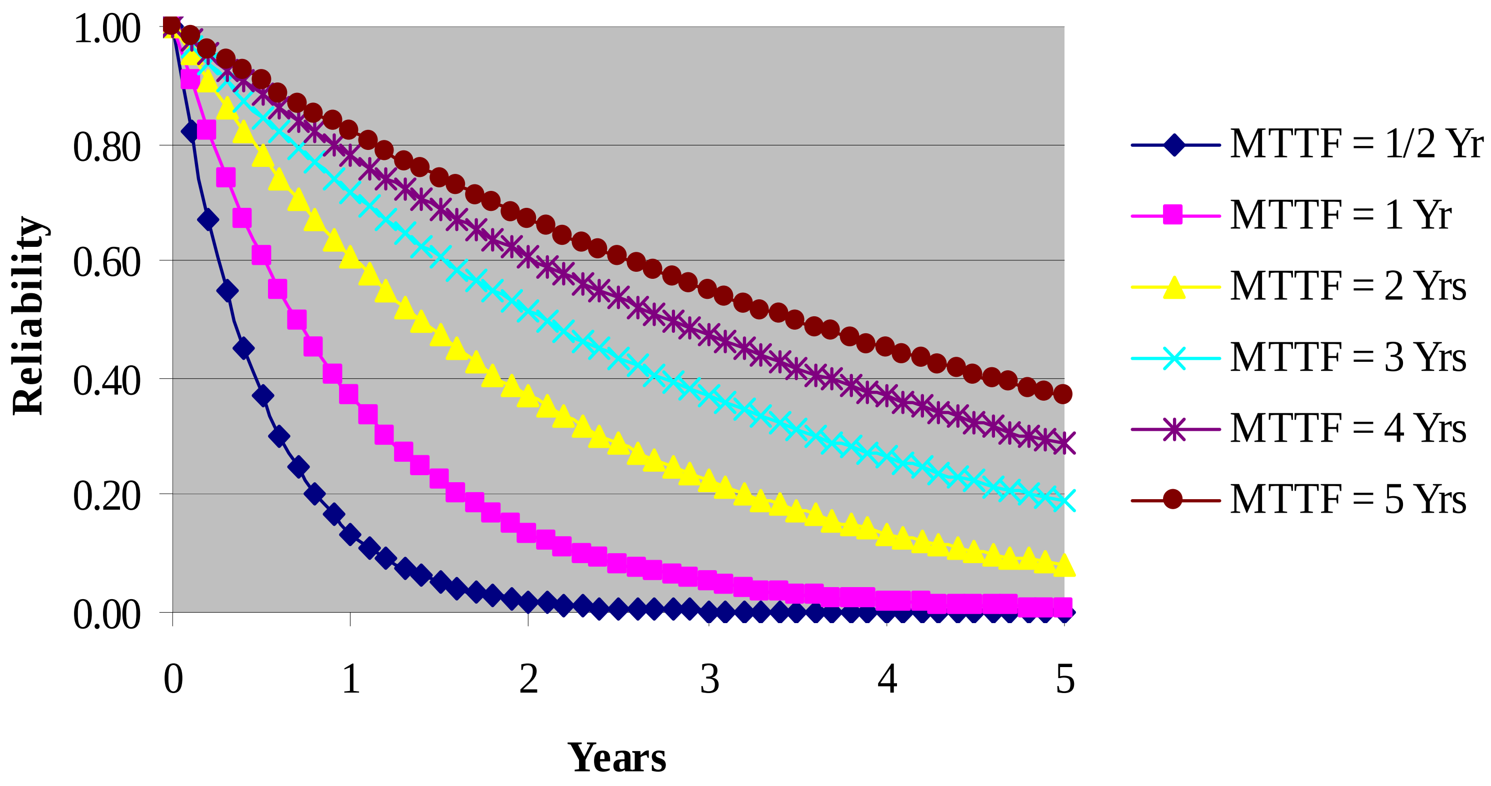
B. Telecommunications Infrastructure

C. RAMS and Resiliency

Dependability

- Reliability – *f(MTTF)*
- Maintainability – *f(MTTR)*
- Availability – *f(MTTF, MTTR)*
- Resiliency -- *f(MTTF, MTTR, Severity)*
- Resiliency Metrics and Thresholds

Reliability Curves



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)

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

Historical
Actual

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

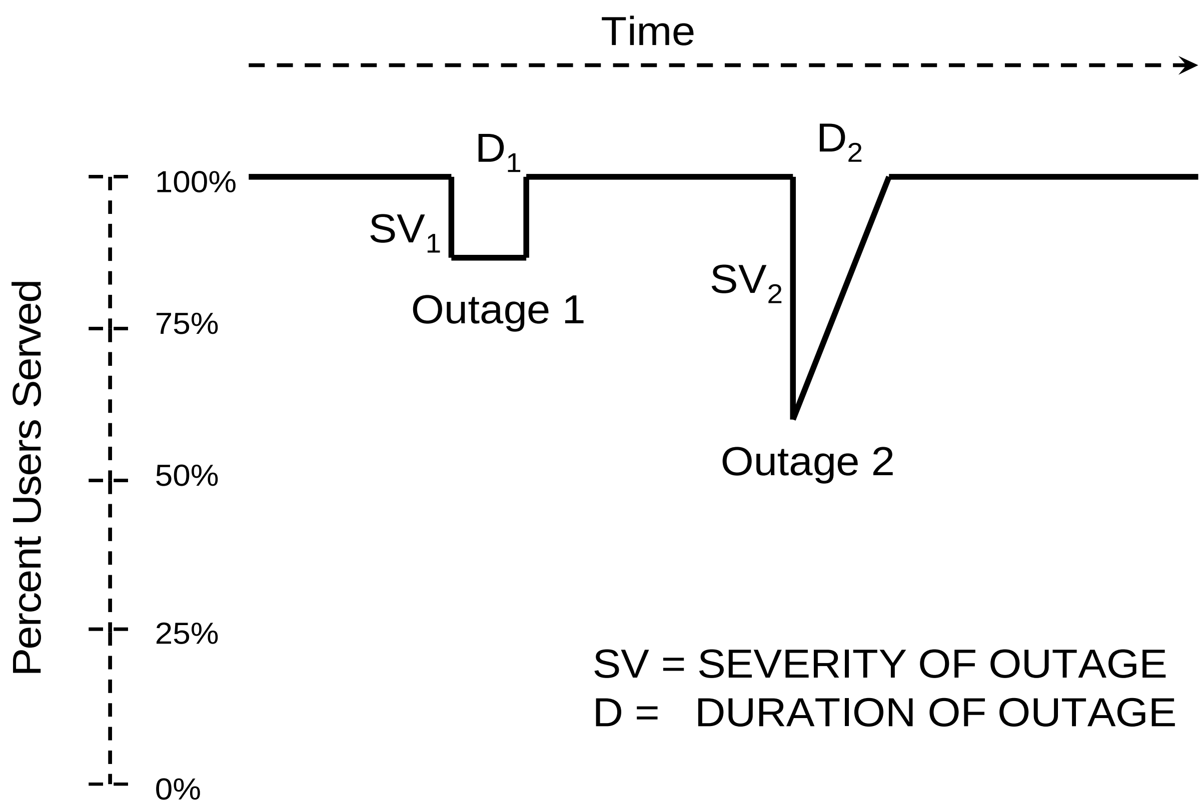
Point Estimate
Of RV

A ↑ MTTF ↑ MTTR ↓

Resiliency

- RAM isn't enough!
- Large telecommunication infrastructures are rarely completely "up" or "down".
- They are often "partially down" or "mostly up"
- Rare for an infrastructure serving hundreds of
- Resiliency describes the degree that the network can service users when experiencing service outages

Outage Profiles

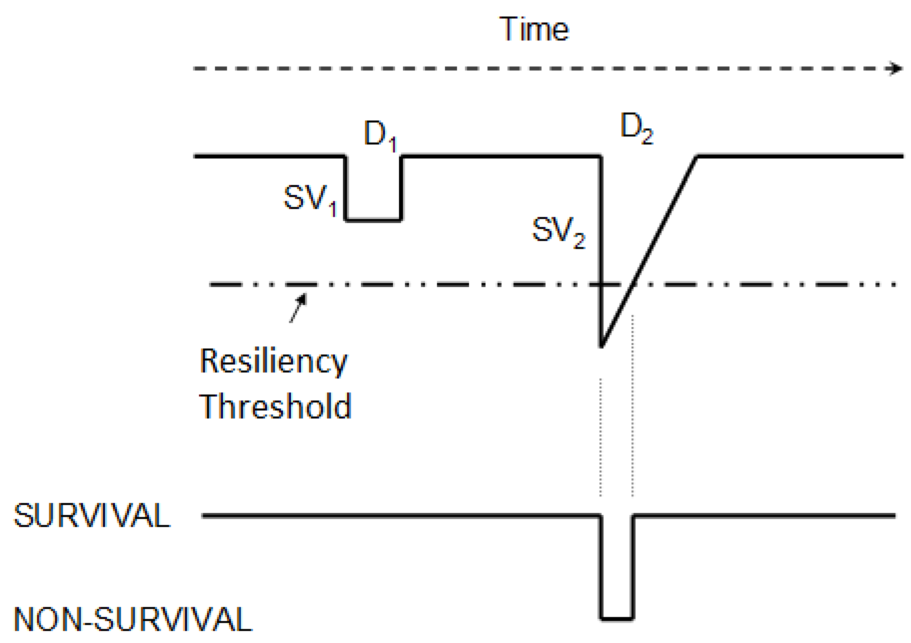


<u>Outage 1</u>: Failure and complete recovery. E.g. Switch failure

<u>Outage 2</u>: Failure and graceful Recovery. E.g. Fiber cut with rerouting

Resiliency Thresholds

- RESILIENCY deficits are not small event phenomena.
- Filter out the smaller outages with thresholds



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.

User & Carrier Perspectives

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

Minimizing Severity of Outages Makes Infrastructure More Resilient

- It is not always possible to completely avoid failures that lead to outages.
- Proactive steps can be taken to minimize their size and duration.
  - Avoid overconcentration and single points of failure that can affect large numbers of users (“Mega-SPF”)
  - Don’t defeat fault tolerance by improper deployment
  - Have recovery assets optimally deployed to minimize the duration of outages.
  - Track outages and their root causes
  - Identify vulnerabilities, assess risk, prioritize them and remove the high impact/probability ones

Thankyou.

Have a great conference!!