Center for ENERGY
A University Center within the Swanson School of Engineering

LEAdERS

Fault Tolerance and Healing

Alexis Kwasinski, Ph.D.

R. K. Mellon Faculty Fellow in Energy

University of Pittsburgh, Swanson School of Engineering

University of Pittsburgh

PITT | SWANSON ENGINEERING
ELECTRICAL & COMPUTER

Overview

- How to evaluate fault tolerance and healing capability?
  - Availability vs. reliability
  - Resiliency
- Fault tolerance techniques
  - Redundancy
  - Diversity
  - Distributed functions
  - Modularity
  - Storage
- Conclusions

Fault Tolerance and Healing

- **Fault tolerance is the ability of a system to maintain operation when one or more of its components fail.**
- **Fault tolerant systems should avoid single point of failures**

- **Healing is the ability of the system to regain operation of failed components**
- **Healing process is related to hardware design and to organizational process (logistics, spare parts practices).**

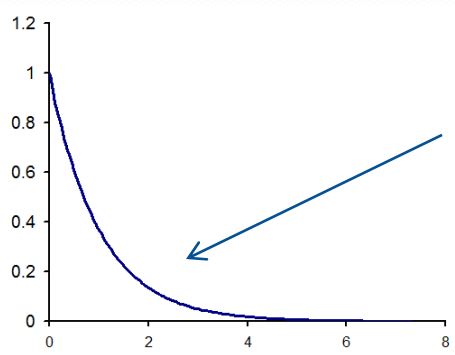
- **How can fault tolerance and healing measured? Is there a concept that allows to evaluate them in an integrated way?**
- **Fault tolerant systems should avoid single point of failures**

Reliability

Can reliability be a measurement of fault tolerance?

- Reliability, *R*, is defined as the probability that an entity will operate without a failure for a stated period of time under specified conditions.
- For electronic components the most common way of mathematically defining reliability is

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



Sooner or later everything fails

- Reliability is often characterized based on the mean time to failure (MTTF): It is the expected operating time to (first) failure. Mathematically, it is the inverse of the failure rate λ.

Fault tolerance and healing

Fault tolerance and healing metrics

- Fault tolerance is a system concept…. Implicitly it is acknowledged that there will be failures but the system will still be able to operate with some level of failures.
- Healing implies repairs.
- Hence, reliability is a concept that does not seems to adjust well to represent fault tolerance and healing.

- **Availability:**
- **It is a concept that applies to systems.**
- **It recognizes that the system can still operate when one or more components are in a failed condition.**
- **It explicitly considers that components can be repaired.**

Availability

Availability as a measure for fault tolerance and healing

$$\text{Availability} = \frac{\text{Expected time operating “normally”}}{\text{Total time (“normal” operation + off-line time)}}$$

- System components can be repaired. So, in addition to a failure rate λ we can define a repair rate μ that is the analogous concept to that of the failure rate but applied to repairs.
- The repair rate is influenced by hardware and managerial attributes of the system.
- Availability is calculated over an infinite number of failure and repair cycles

Resilience

Is there a relationship between resilience and availability?

- What is resilience?

  From US Presidential Policy Directive 21, resiliency is "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions."
- Hence, a measure of resilience would consider "up times" to measure withstanding capabilities (influenced by fault tolerance attributes) and rapid recovery characteristics (dependent on healing properties). Thus, resilience can be measured as:

$$\text{Resiliency} = \frac{\text{Up Time}}{\text{Up Time} + \text{Down Time}}$$

- While availability is evaluated as an average behavior over many failure and repair cycles, resilience can be computed over one cycle.
- Fault tolerance and healing are attributes related to resilience

Fault tolerance and healing

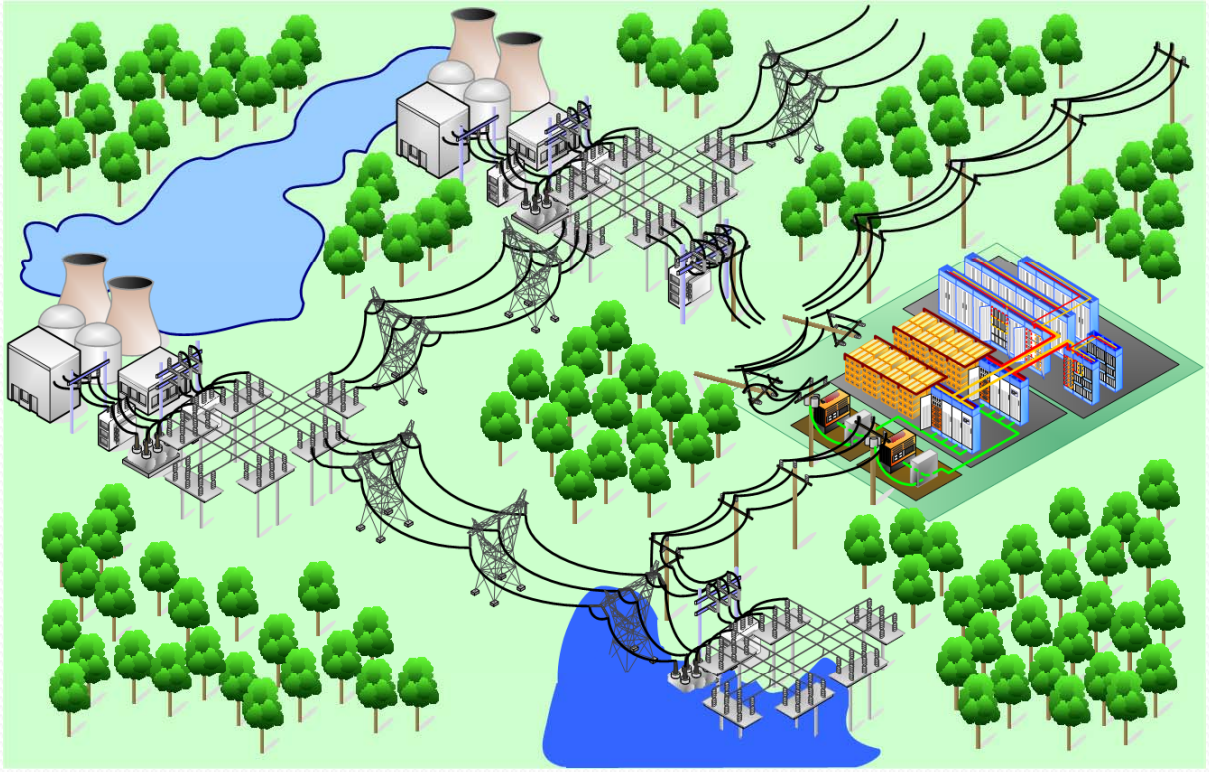
Ways of improving availability

- Modularity
- Redundancy (extra parallel operation of same components)
- Diversity
  - Functional: Use of different components for the same function.
  - Geographical: Use of different locations for a same function.
- Distributed functions
- Storage (to address internal and external cascading)
- **Tradeoffs:**
  - **Cost (additional components, idle capacity, etc.)**
  - **Complexity (influence human error potential)**
- **Effective use of these techniques requires an adequate design because availability will not improve by merely applying them.**

Redundancy and Diversity

Application level and perspectives

- From a grid perspective two power paths imply geographic diversity.
- From user perspective, two power paths is redundancy not diversity.

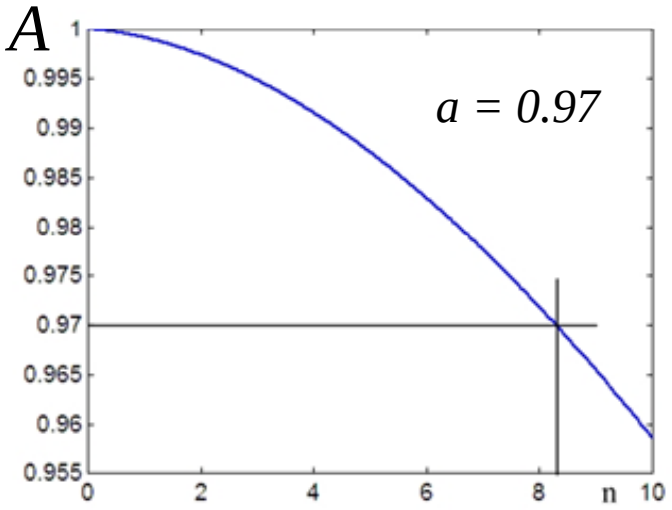


Redundancy

- The most common redundant configuration is $n + 1$ redundancy in which n elements of a system are needed for the system to operate, so one additional component is provided in case one of those n necessary elements fails.
  - n +1 redundant configuration. But more modules is not always better:

$$A=(n+1)a^n(1-a)+a^{n+1}$$

  - As n increases, idle capacity decreases



- Availability decreases when n increases to a point where $A < a$.
- Why? Because as n increases, chances of having two or more failed components at the same time increases.

Modularity and Distributed Functions

- **Modularity.**
- **Goals:**
  - **Simplify design**
  - **Enable scalable investments**
  - **Enable plug-and-play designs**
  - **Reduce replacement time (reduce healing time).**
- **Issues: too much modularity may increase system complexity**
- **Distributed functions**
- **Can be done based on software or hardware**
- **Issue: coordinated operation of the distributed parts of the system while avoiding single point of failures in communication links and limiting complexity.**

Fault tolerance and healing

Storage (buffers)

- Systems do not operate in a vacuum: by definition, systems need inputs to perform their intended functions.
  - Availability of inputs may depend on external systems. Hence, "our" system may depend on services provided by external systems.
  - Adequate fault tolerance design may address these dependences on external systems with the use of local storage. For example, batteries or other type of energy storage can be used in electric circuits to create fault tolerance to power grid outages.
  - The effect of storage is limited in time so calculations of required capacity is influenced by healing characteristics of the external system.

- Storage can be used as internal buffering interfaces in order to limit the propagation speed of cascading failures within the system.

Conclusions

- How to evaluate fault tolerance and healing capability?
  - A system approach is required. Availability seems to be a suitable metric. It is analogous to resiliency.
  - Fault tolerance and healing is not only influenced by hardware design… humans are an influencing factor, too
- Fault tolerance and healing techniques
  - Redundancy
  - Diversity
  - Distributed functions
  - Modularity
  - Storage
- Effective implementation of fault tolerance and healing technique requires adequate system planning, design and operation. Systems should not be considered isolated.