University of Idaho

ECE 444 / ECE 544 / CS 444 / CS 544 Supervisory Control and Critical Infrastructure Systems

Session 18

Midterm Exam

- Take home exam
  - 72 hours
- Available friday March 22
  - finish by end of day April 1
  - choose which 3 day period
    - Email me day & time you want to start
- mix of short answer & some calculations
  - 544 students - additional problems

CS&ECE 444/544

Lecture 18

Performance Measures

- Communication network level

-Speed → how many MB/s

→ Latency

data - security - loss or interruption of data flow

+ (lost packet/frames)

- errors in data

- cyber security

CS&ECE 444/544

Lecture 18

Failures

- Failures of communication
  - » Impact of single point failure
  - » Risks and rewards of adding more components

- disrupt the networks → the outcome of the process

2 communication devices

- switchs
- IEDs
- conductors

- cost
- Timing - planned shutdown
- increase possibility of configuration errors
- increases attack surface

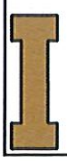
Industrial Process Performance Expectations

- Need quantifiable measures of performance
  - » Based on proper outcome of the process
- Engineering design has measurable performance expectations based on physics.
- Especially systems or components where failures effect human safety
- Does a failure in communication device leave no option for safe failure mode
- Updating equipment in process environment not trivial

Fault Tree Analysis

- Look at the steps in the process
  - » For example, tripping a circuit breaker upon detection of a fault
- Look at the components involved
  - » And the communication paths
- Look at failure modes of that equipment
  - » And probability of failure
  - » Can go a step further and look at effects of failures

consequences



L18 3/10

Failure rates for components?

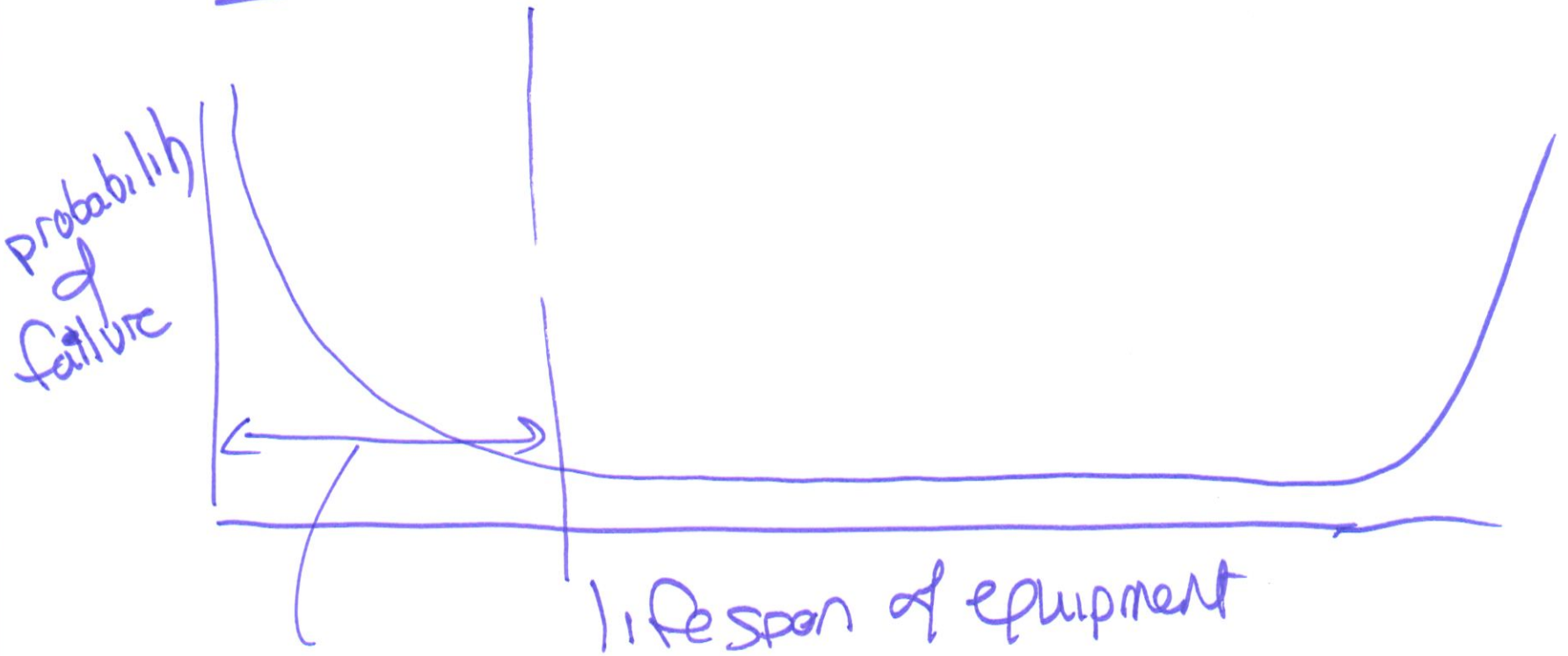
How is this determined?

- some vendors do accelerated aging testing
  - Thermal cycling
    - effects of heating on materials
  - vibration testing
- some organization have built databases of test data for components

- Mean time to failure (MTTF)
  - over a large set of devices
  - hopefully in years
- mean time between failures (MTBF)
- mean time to repair (MTTR)
  - for ICS comms systems → often replace

MTBF = MTTF + MTTR

MTTF - especially for IEC systems



System performance

unavailability (can't perform task)

$$q = \frac{MTTR}{MTBF} = \frac{MTTR}{MTTF + MTTR}$$

MTTF: decades (at least years)

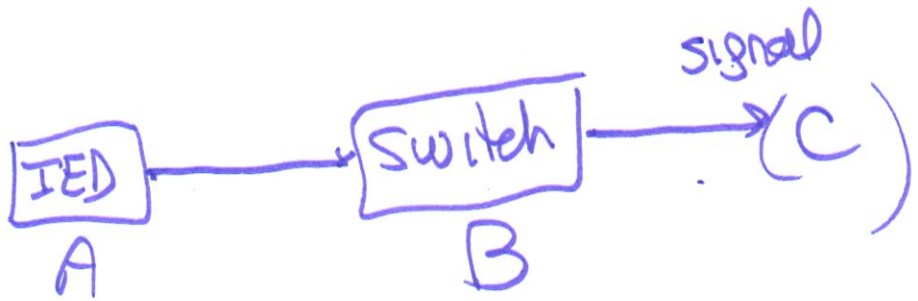
MTTR: hours to days

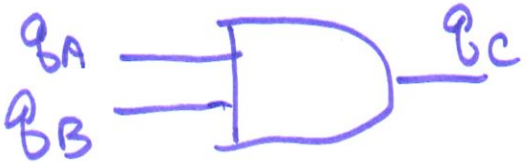
component & for system

q is small

availability $p = 1 - q$

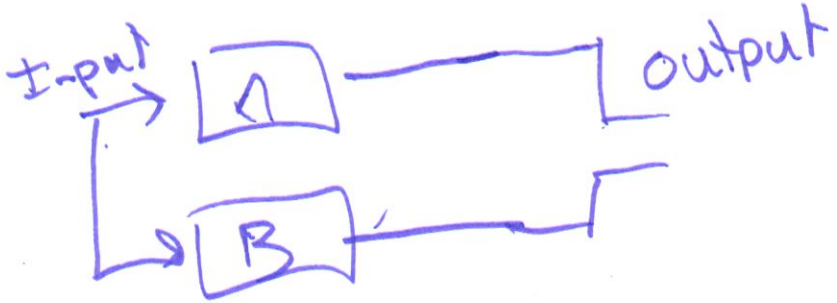
→ goal is often 0.99999 (five nines)





$$q_C = q_A \cdot q_B$$

Adding redundancy



L18/ 10/10

Six Line Substation Example from Lecture 17

- With RTU for now

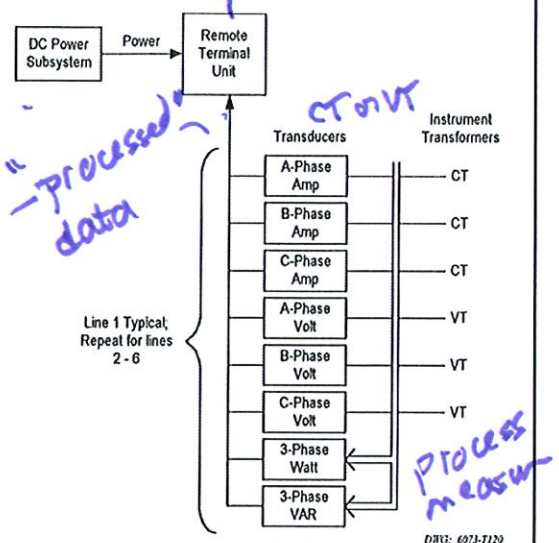


Figure from: G.W. Scheer, "Answering Substation Automation Questions Through Fault Tree Analysis," *4th Annual Substation Automation Conference, 1998*

Fault Tree for Not Acquiring Data from Line 1

- Equipment on left common to comparison cases
- This case has a RTU

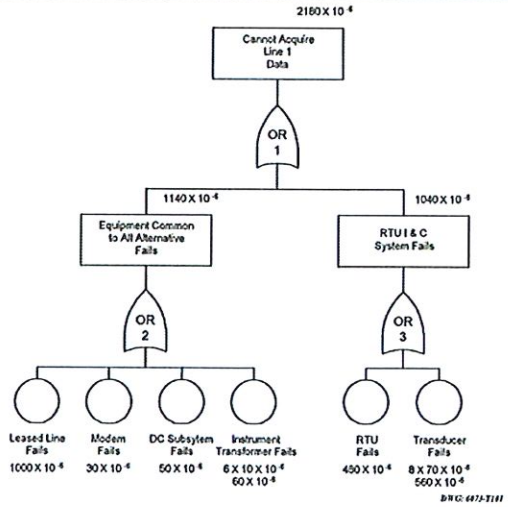


Figure from: G.W. Scheer, "Answering Substation Automation Questions Through Fault Tree Analysis," *4th Annual Substation Automation Conference, 1998*

Figure 2: Fault Tree for RTU System in Six-Line Substation