Performance Measures

- Communication network level

Failures

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

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

Six Line Substation Example

- With RTU for now

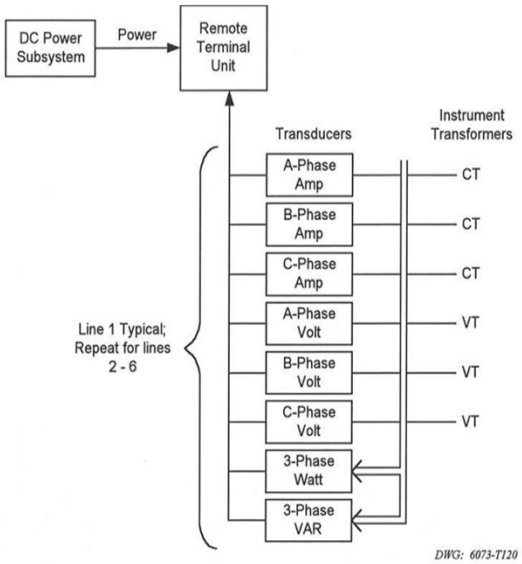


Figure from: G.W. Scheer, "Answering Substation Automation Questions Through Fault Tree Analysis," *4th Annual Substation Automation Conference, 1998*

Supervisory Control & Critical Infrastructures

5

Fault Tree for Not Acquiring Data from Line 1

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

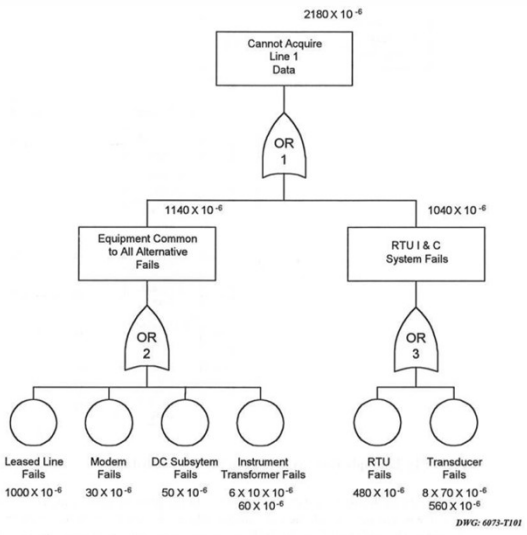


Figure 2: Fault Tree for RTU System in Six-Line Substation

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

Supervisory Control & Critical Infrastructures

6

Fault Tree for Cannot Operator Breaker 1 or Acquire Data from Line 1

- Equipment on left common to comparison cases
- Added the circuit breaker
- A in triangle is identifying equivalent circuit

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

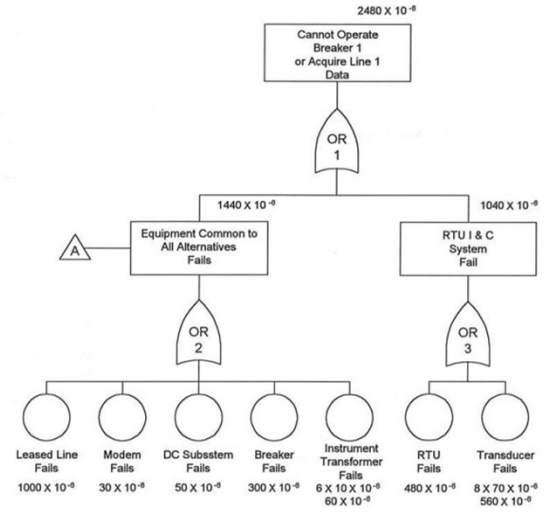
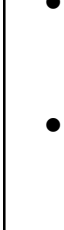


Figure 3: Fault Tree for RTU-Based I&C System in Six-Line Substation



Replace RTU with Communications Processor in Star Topology

- Communication Processor more reliable than RTU
- Lower overall unavailability score

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

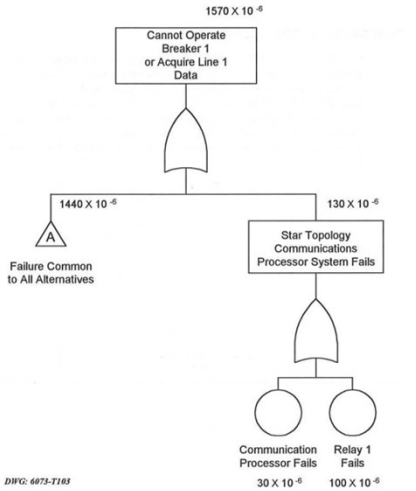


Figure 4: Fault Tree for Relay and Communications Processor Star I&C System in a Six-Line Substation

Replace RTU with PC Communicating with Relays in Multidrop Serial Network

- PC is single point of failure and is less reliable that communication processor or RTU
- Note the network failure path

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

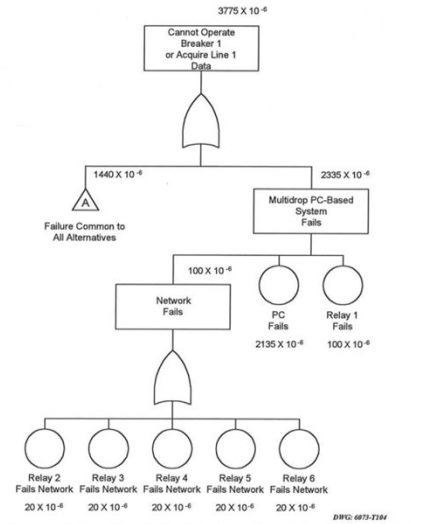


Figure 5: Fault Tree for a PC Multidrop Relay Network in a Six-Line Substation

Replace PC with Hardened Industrial PC

- PC is still single point of failure
- But now the PC is more reliable one

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

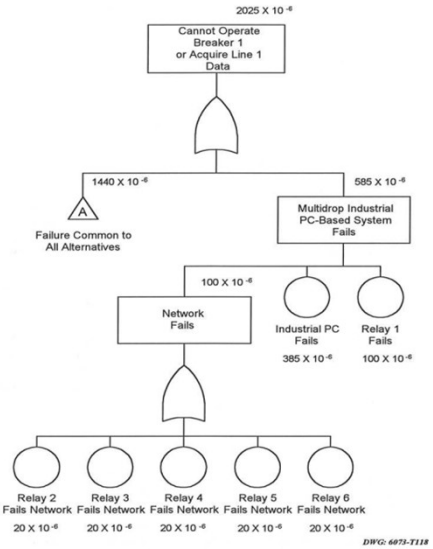


Figure 17: Fault Tree for Industrial PC Multidrop Network in a Six-Line

Can Use Fault Trees to Compare Hardware Options or Network Configurations

Table 2: Approximate Unavailabilities of Six-Line Substation Systems for Top Event *Cannot Sense or Operate Line 1*

System	I&C Unavailability	Total Unavailability
RTU-based	1040×10^{-6}	2480×10^{-6}
Communications processor star to relays	130×10^{-6}	1570×10^{-6}
PC star to relays	2235×10^{-6}	3675×10^{-6}
Industrial computer star to relays	485×10^{-6}	1925×10^{-6}
PC multidrop to relays	2335×10^{-6}	3775×10^{-6}
Industrial PC multidrop to relays	585×10^{-6}	2025×10^{-6}
PLC multidrop to relays	520×10^{-6}	1960×10^{-6}

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

11

Generalize for failure of any control action or communication

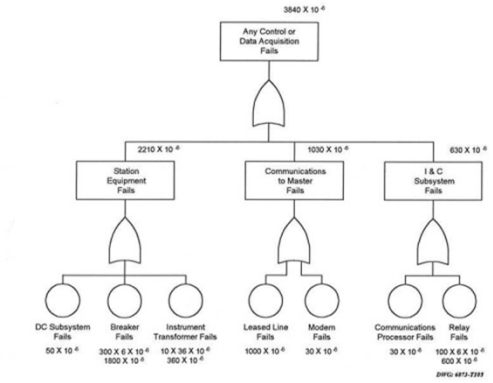


Figure 6: Fault Tree for Any Failure of Relay and Communications Processor Star I&C System in a Six-Line Substation

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

12

Adding Redundancy

- Also have redundancy in the dc power supply
- And the power system apparatus

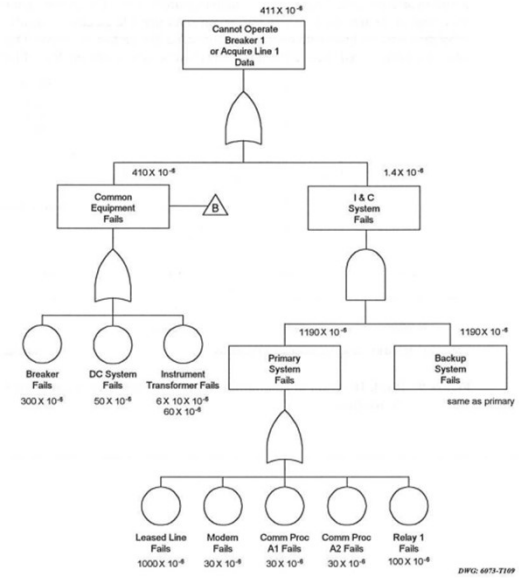


Figure 10: Fault Tree for Communications Processor I&C System for 54-Line Substation

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

13

Comparing Ethernet Network Device Choices and Topologies

Component	Unavailability (10^{-6})*
Communications Processor	30
Ethernet Hub	46
IED (protective relay)	55
IED Network Interface	285
Monitoring/metering IED	320
Industrial PC	385
SCADA Gateway	385
Ethernet switch	477
Ethernet router	577

*G.W. Scheer and D.J. Dolezilek, "Comparing the Reliability of Ethernet Network Topologies in Substation Control and Monitoring Networks," 2nd Annual Western Power Delivery Automation Conference, April 2000

14

Comparing Ethernet Network Device Choices and Topologies

Component	Unavailability (10^{-6})*
Communications Processor	30
Ethernet Hub	46
IED (protective relay)	55
IED Network Interface	285
Monitoring/metering IED	320
Industrial PC	385
SCADA Gateway	385
Ethernet switch	477
Ethernet router	577

*G.W. Scheer and D.J. Dolezilek, "Comparing the Reliability of Ethernet Network Topologies in Substation Control and Monitoring Networks," 2nd Annual Western Power Delivery Automation Conference, April 2000