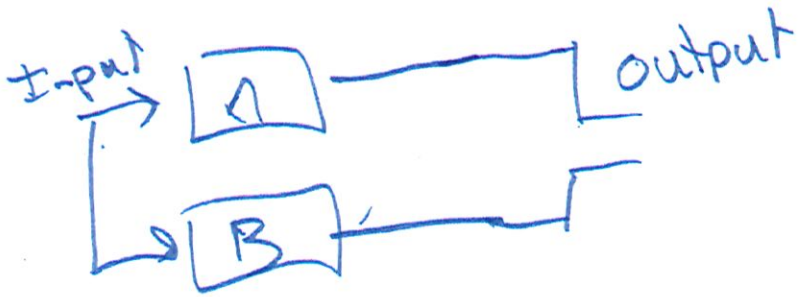
University of Idaho

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

Session 19

L9 4/12 ~~L18 9/10~~

Adding redundancy

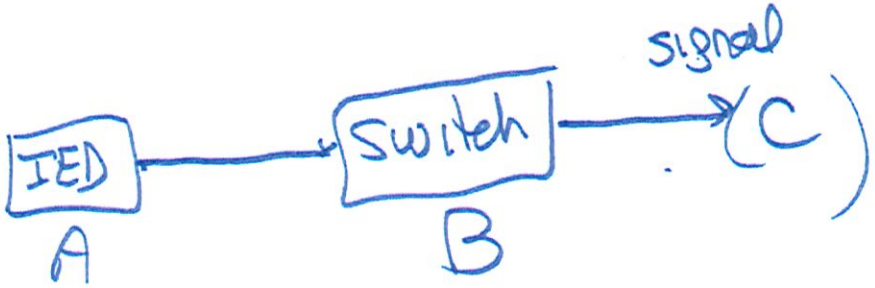


$q_A = 300 \times 10^{-6}$

$q_B = 150 \times 10^{-6}$

~~$C = q_A + q_B = 450 \times 10^{-6}$~~

L19 2/12 ~~L18 8/10~~



$$q_C = q_A \cdot q_B$$

$$q_A = 2000 \times 10^{-6}$$

$$q_B = 1000 \times 10^{-6}$$

$$q_C = q_A + q_B$$

$$= \cancel{2 \times 10^{-6}}$$

$$3000 \times 10^{-6}$$

Six Line Substation Example from Lecture 17

CS&ECE 444/544

Lecture 18

- With RTU for now

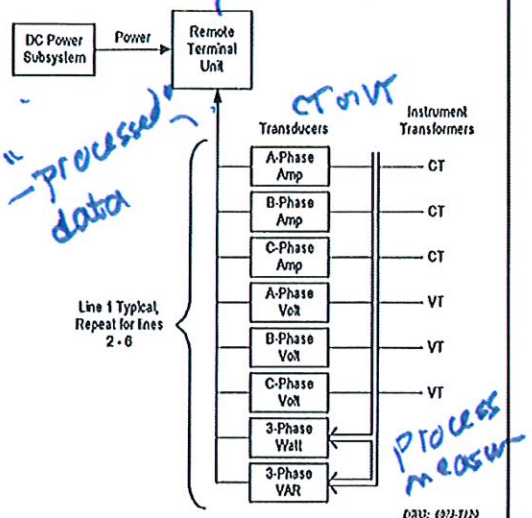


Figure from: G.W. Scheer, "Answering Substation Automation Questions Through Fault Tree Analysis," *4th Annual Substation Automation Conference, 1998*

Supervisory Control & Critical Infrastructures

5

Fault Tree for Not Acquiring Data from Line 1

CS&ECE 444/544

Lecture 18

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

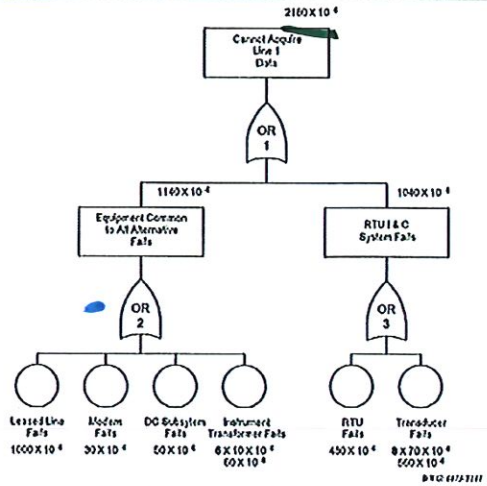


Figure from: G.W. Scheer, "Answering Substation Automation Questions Through Fault Tree Analysis," *4th Annual Substation Automation Conference, 1998*

Supervisory Control & Critical Infrastructures

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

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*

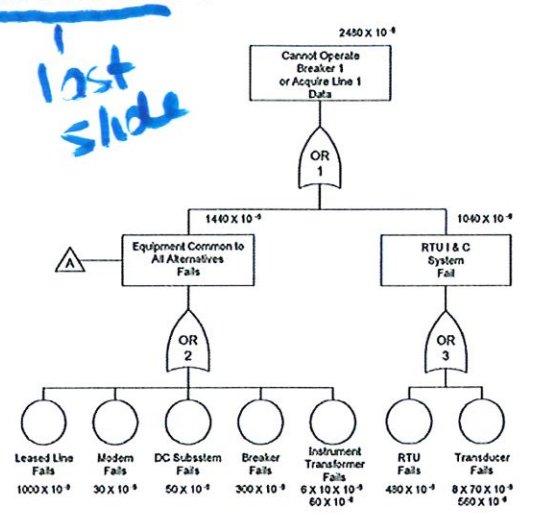


Figure 3: Fault Tree for RTU-Based I&C System in Six-Line Substation

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*

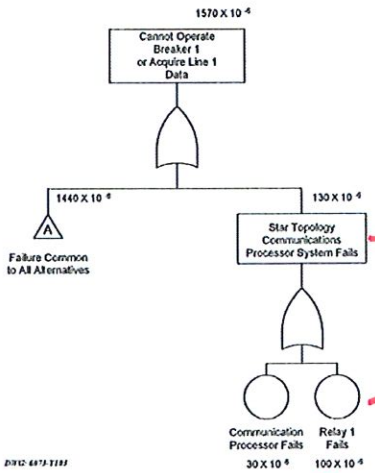


Figure 4: Fault Tree for Relay and Communications Processor Star I&C System in a Six-Line Substation

L19 5/12

STAR

single point of failure

L18 6/12

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*

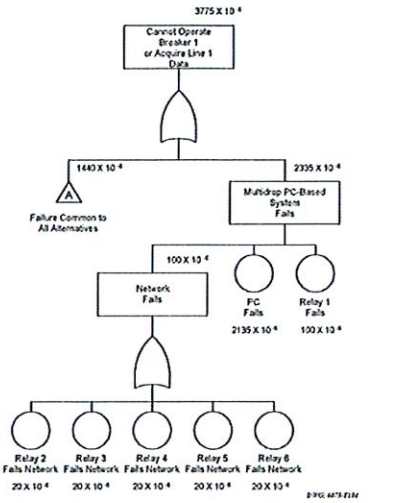


Figure 5: Fault Tree for a PC Multidrop Relay Network in a Six-Line Substation

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*

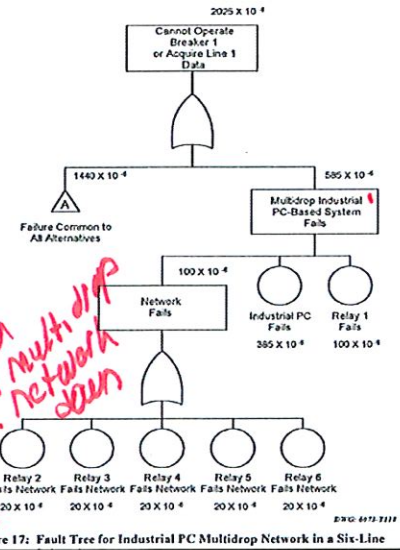
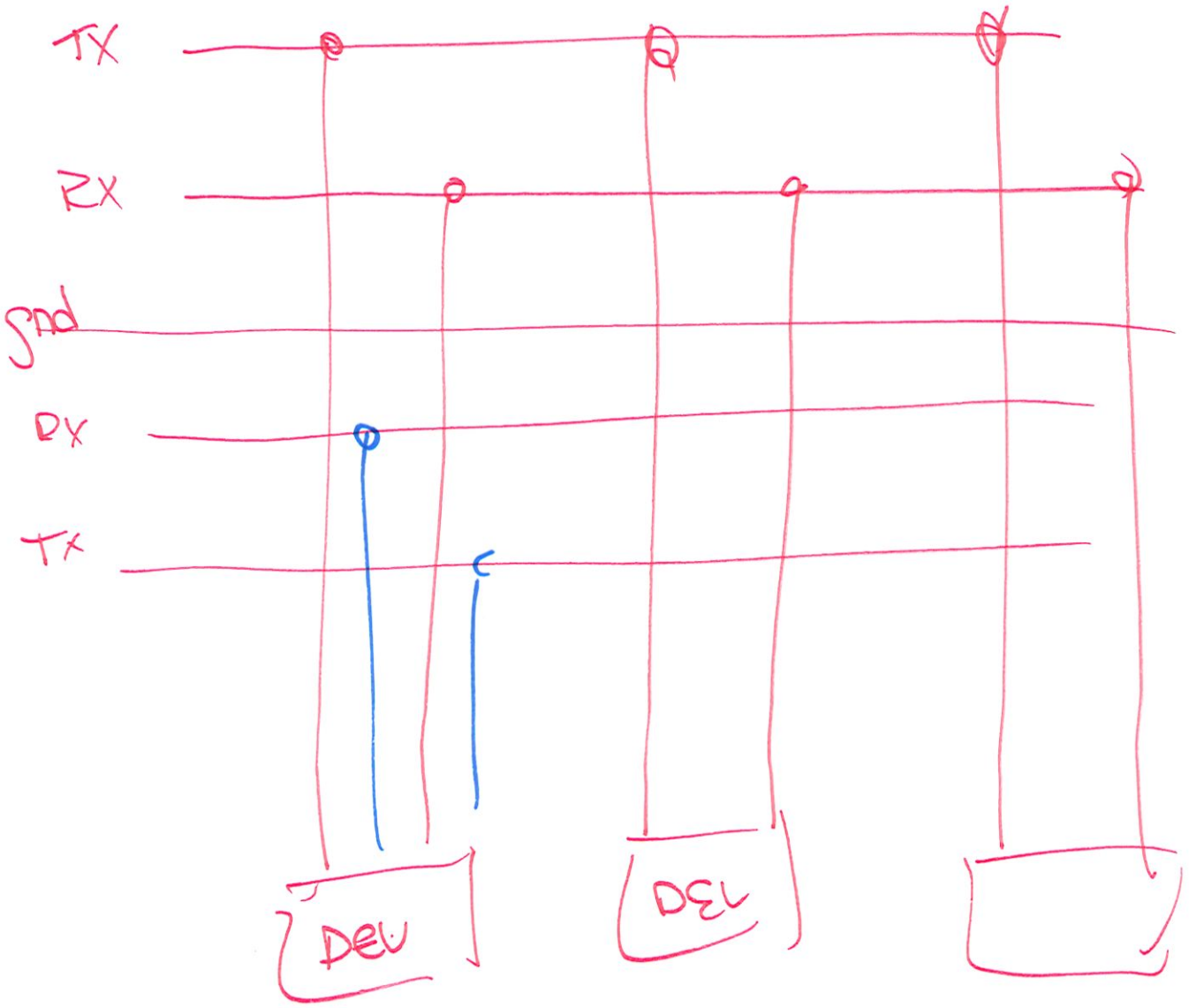


Figure 17: Fault Tree for Industrial PC Multidrop Network in a Six-Line

L19 7/12



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

Generalize for failure of any control action or communication

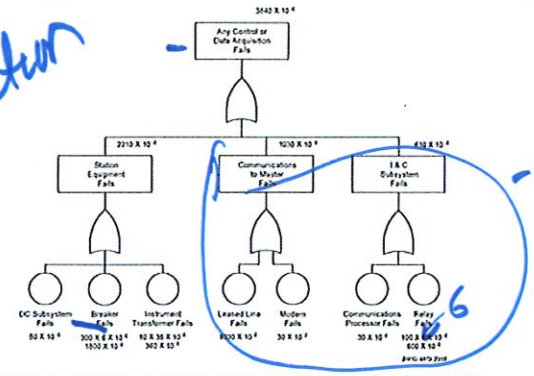


Figure 6: Fault Tree for Any Failure of Relay and Communications Processor Star I&C System in a Six-Line Substation

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

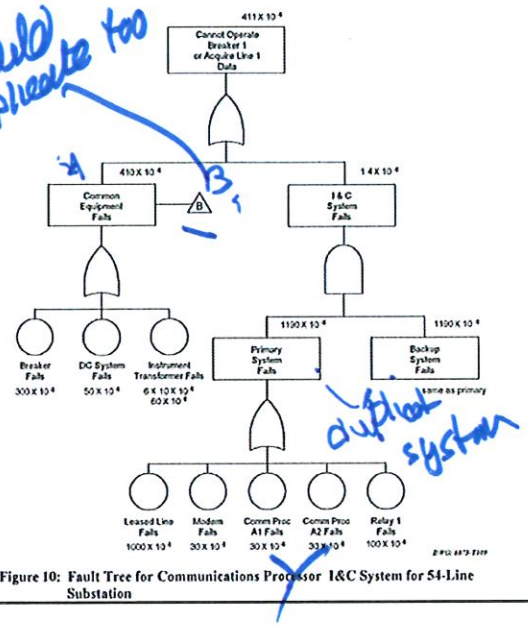
L19 9/12

Adding Redundancy

CS&ECE 444/544

could duplicate too

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



duplicate system

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

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

Comparing Ethernet Network Device Choices and Topologies

CS&ECE 444/544

Lecture 18

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 (RTU in past)	385
Ethernet switch	477
Ethernet router	577

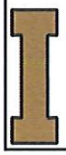
modern switches combine these

*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

L19 10/2

Substation Networking

- Most networks in substation use either
  - » BaseT: specialized copper, twisted pair
    - – 10baseT means 10 megabits/second transfer rate
    - – Copper cables are often cheaper
    - – Network connections cheaper
  - » BaseF: fiber-optic cable
    - – Galvanic isolation
    - – Immune for electromagnetic interference
    - – Not susceptible to ground loops
    - – Longer cable runs possible
    - – Requires specialized tools



Failure Modes: Inside Station

- Broadcast Data Storm
  - » A network interface on an IED can fail in a mode that corrupts network
  - » Failed interface can continuously broadcast messages
  - » Different network management devices respond differently
    - – Hub: passes the storm on
    - – Router: limits
    - – Unmanaged switch
    - – Managed switch
- Failures of network links
- Failures of switches /hubs - - -
- Protocols to manage situations

procedures to follow

Shared Hub Lan

CS&ECE 444/544

Lecture 19

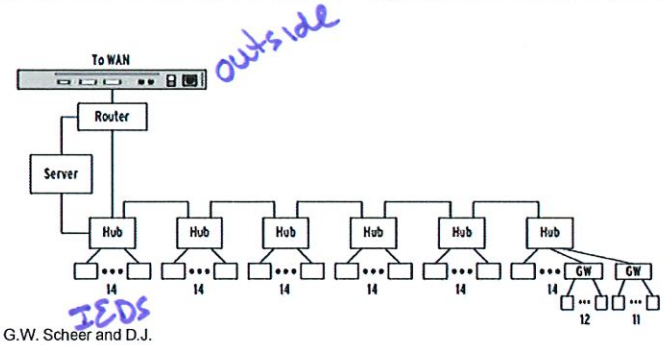


Figure from: G.W. Scheer and D.J. Dolezilek "Comparing the Reliability of Ethernet Network Topologies in Substation Control and Monitoring Networks," 2nd *Annual Western Power Delivery Automation Conference, 2000*

Shared Hub LAN Fault tree

CS&ECE 444/544

Lecture 19

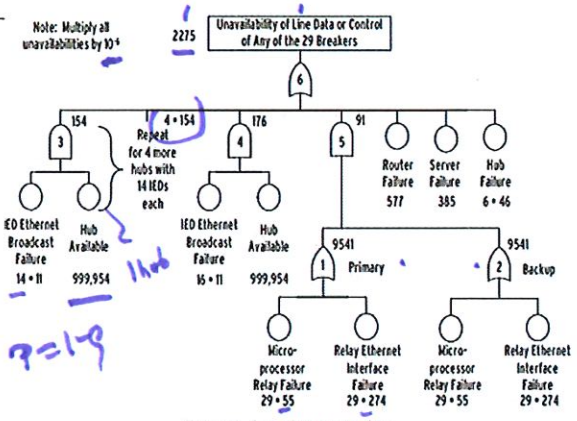


Figure 2: Shared Hub Fault Tree

Figure from: 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, 2000*

Switched LAN Fault tree

Figure from: 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, 2000*

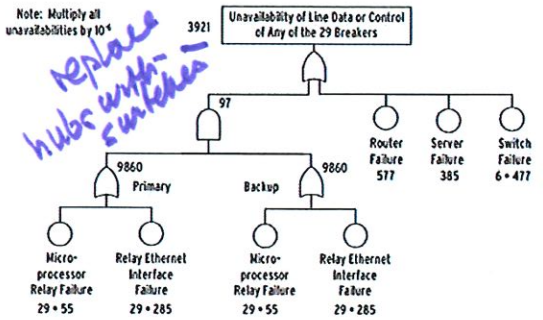


Figure 3: Switch Fault Tree

Unavailability = $3921*10^{-6}$

Availability = 99.6079%

- Switches not as reliable as hubs.
- But no data storms

Redundant Shared Hub Lan

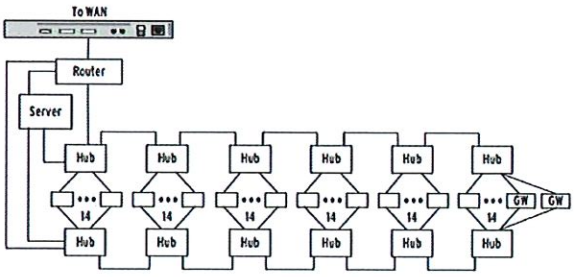


Figure from: G.W. Scheer and D.J. Dolezilek "Comparing the Reliability of Ethernet Network Topologies in Substation Control and Monitoring Networks," 2nd *Annual Western Power Delivery Automation Conference, 2000*