University of Idaho

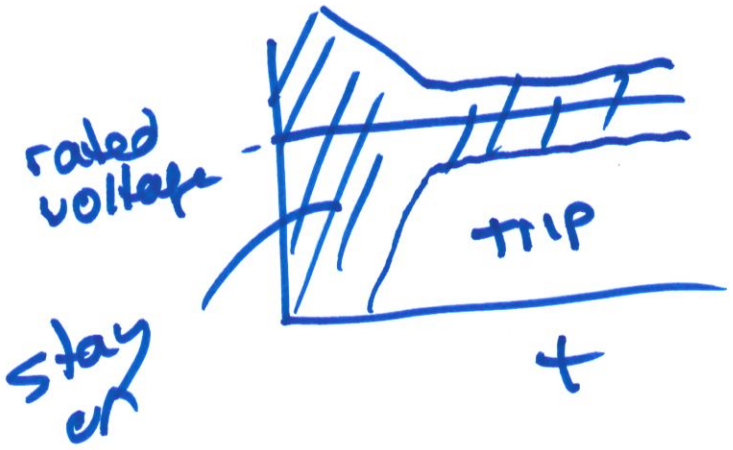
ECE 444 / ECE 544 / CS 444 / CS 544 Supervisory Control and Critical Infrastructure Systems

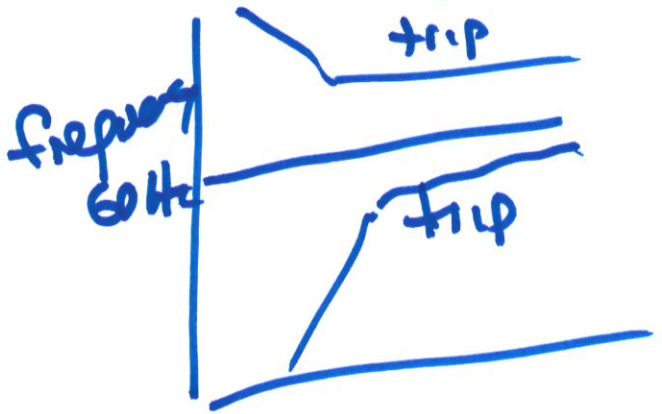
Session 10

L10 1/9

- short circuit faults on 500kV transmission - due to forest fire (Blue Cut fire)

- PV inverter
  - → one of vendors was following the then current IEEE 1547 standard for generators on dist. systems





L10 2/9

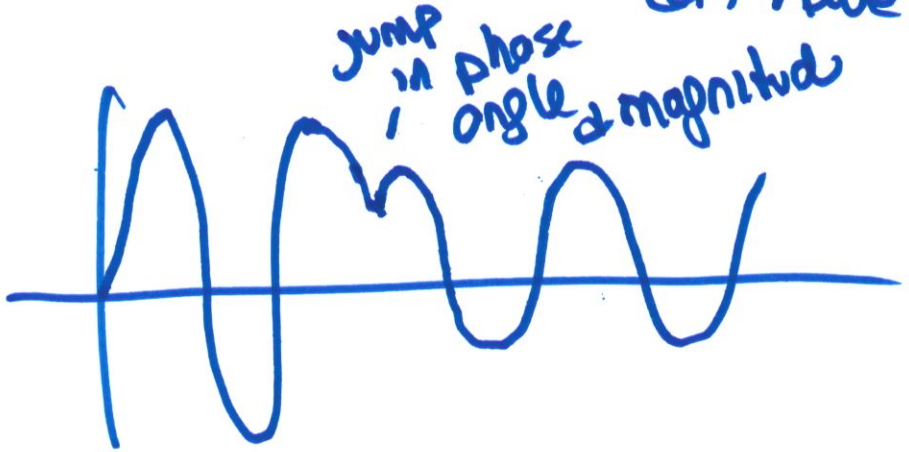
measure frequency?

→ use zero crossing of voltage - average over number of cycles

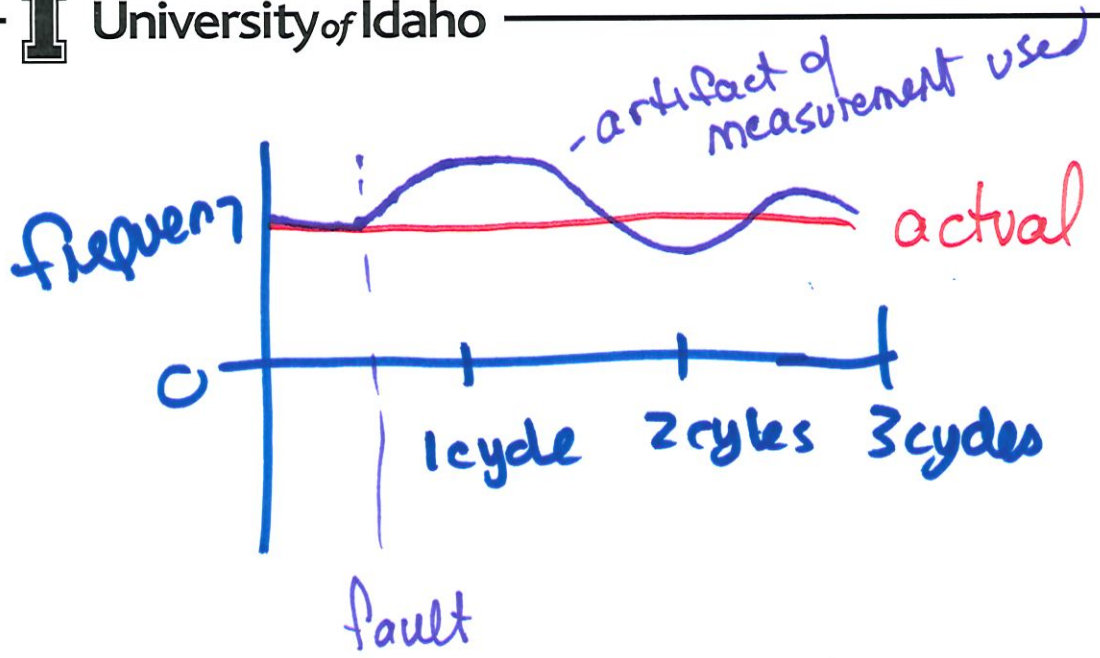
→ phase locked loop (PLL)
Proportional/Integral controller

↳ inverter manufacturers used as part of converter control - protect power electronic devices

- can have temporary error



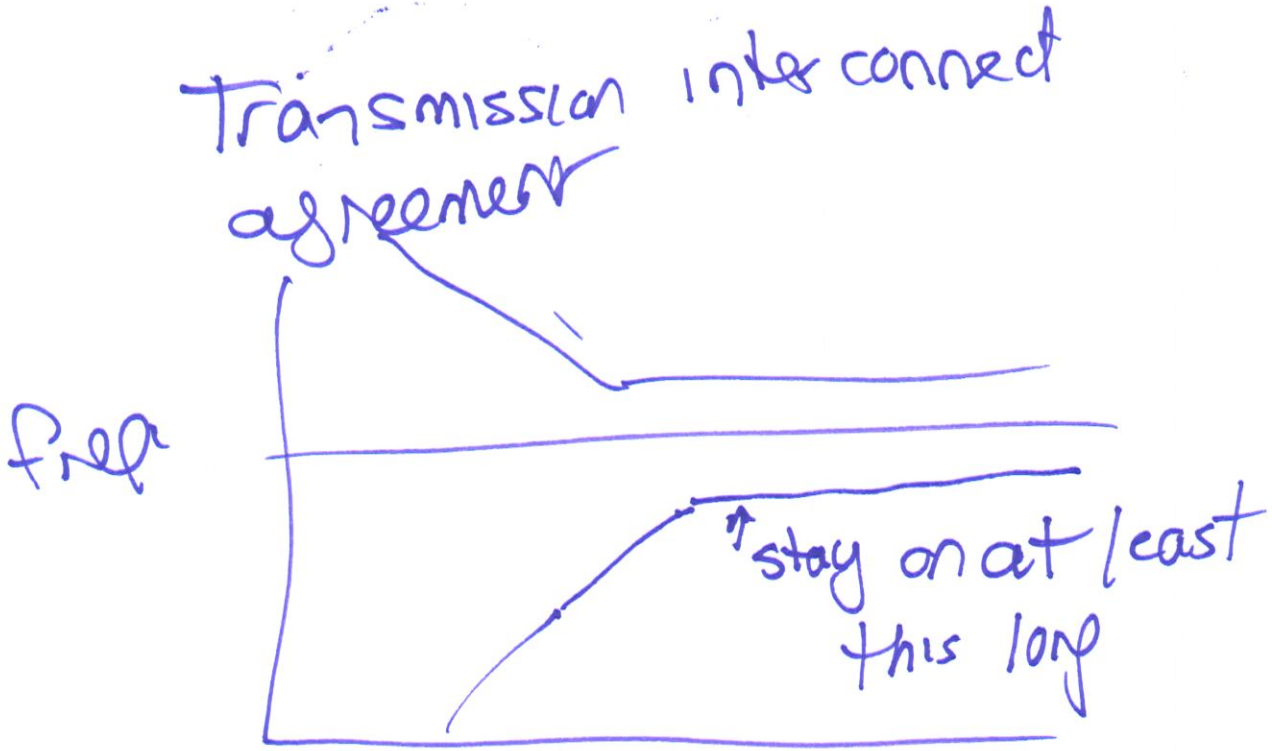
L10 3/9



Large number of PV inverters temporarily shutdown (cessation)

→ SCADA update rate was a second or so

L10 4/9


Transmission interconnect agreement
freq
stay on at least this long

L10 9/9

Power System vs. Communication System

- Power System – Analog system
  - limited, indirect control of flow on individual lines
  - simulation to plan control decisions
- Communication System
  - some analog
  - digital – packets of information
    - more tightly controlled – and predictable on some time scales

Communication in ICS

- Between what?
  - Inside substations
    - Between equipment
    - measurements to RTU (remote terminal unit)
  - substation to control center (typical)
  - substation to substation
  - substation to market operator
  - substation to equipment vendor
  - smart meters in building to utility
    - Energy use
    - demand response commands

} situational awareness (operators)

L10 6/9

Enterprise Technology

Networks (IT) information

- Characteristics - "Internet"
  - open network - connect through service provider
  - reboot for patches or unstable operation
- Performance expectations
  - expect high download capacity
  - varied upload
  - most applications can varied latency or dropped packets
  - users partially responsible for security

Operational Technology

- Performance expectations
  - Delivery of packets with high Reliability
  - Time critical delivery - failure to meet time is effectively lost data
- Characteristics
  - wide age range of equipment
    - legacy equipment (compatibility)

- Network segregated from Enterprise network } bridges between them

- Operational security
  - → Is it operating correctly
    - → Packets/data arriving with timing requirements
  - → Patching → rebooting
    - ↳ patch can't break something
      - → to test patches on replica equipment in a lab } evolving to digital twins support operation
- Real time - can't compromise by adding latency

Cybersecurity ← ICS are becoming a target

NERC - North American Electricity Reliability Corporation
- Regional reliability councils
- NERC CIP (critical infrastructure protection) rules

- some forms of security tools for Enterprise technology don't work for OT
  ⇒ Latency or lost packets

L10 9/9

Operational Technology-Characteristics

- Simplicity versus complexity
  - easy to make complex networks as capabilities grow
- Redundancy
  - no single point of failure
    - grown over time
  - documentation, verification, lease testing
  - cost trade off
- Security
  - (1) operational → is it online
  - (2) cybersecurity
    - and work in right

Data Transmission