University of Idaho

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

Session 31

L31 4/7

Operation Technology Systems

↳ controlling industrial processes

→ Power system operate

- Power plant/gen
- Paper mill
- oil refineries
- pipelines
- etc

Engineered systems → many built up over decades

- safety critical aspects

- consequences to misoperations
  - ↳ loss of life
  - damage to equipment
  - extended downtime

Communications added gradually over time

= simple serial connections and added complexity

- standardized protocols
  - ↳ originally more of a grass roots 61850 family

serial ↓ Ethernet in substation

Purdue Model - ICS specific

L0 (level 0): physical process

L1 - field devices - PLC, RTU, Relays

L2 Control system (distributed control) for a part of process or site

L3 - SCADA or similar - communication system/media

L4 - Enterprise/Business network

L5 - External Data Repository (Historian) -cloud computing

- Putting communications in should also have engineered approach
  - Recognize requirements/constraints of physical system/process
    - consequence
    - Importance of deterministic behavior - at process

IT/OT convergence

- Originally → use off the shelf IT equipment in OT applications and have IT team manage

- Evolved to - connect/bridge OT and IT systems

cyber - security
- security without impact process

- Engineering Cyber-security into the system
  - → Goals
    - Ensure that physical process operates + maintains safety
    - Boundaries between critical systems based on degree of consequence
      - → consequence based engineering
    - Data diodes - one way flow of info
    - Hardware solutions plus software

Having physical devices that are not connected to a network for safety critical applications that protect process.

---

consequence boundaries to isolate/divide networks