Reliability of Physical Systems and Trustworthy Information

Anna Scaglione
**Information and Control**

**Industrial Automation**

- Electric Power Systems, Pipelines (Water, Fuel), Building Control, Manufacturing plants use Ethernet + Internet to gather information
- Hacking has not been a factor in their design
Examples of networked control

• Transportation Networks
  – Flow control (traffic lights, tolls) and myopic driver decisions
  – Feedback to the users $\rightarrow$ service latency

• Communication Networks
  – Resource allocation $\rightarrow$ decentralized
    – Internet, cellular, Wireless Local Area Networks
  – Feedback to the users $\rightarrow$ service latency

• Power Systems Networks
  – Resource allocation centralized at large (>100mW) and long term scales (15 min.)
  – Feedback to the users $\rightarrow$ black out
The scale of power lost in an event

- Cascading failures have a heavy tail distribution

The system has reserves for one large failure. We do not have good technology to island the system.
NERC Version 5 Critical Infrastructure Protection (CIP) Reliability Standards (ORDER NO. 791)

- Phases of a cyber-physical attacks:
  1. Target and position to breach network
  2. Leverage breach and expand reach
  3. Execute malicious commands & impair restoration

- NERC Rules to manage safely and isolate from external attacks “Electronic Security Perimeter”
  -- Could have prevented the recent Ukraine attack, diminishing spearfishing threat

- Conceived for the bulk power system....
Trend: Smart infrastructures

Placing intelligence in the edges:
• Greater situation awareness and control
• Attack surface larger