Energy Infrastructure Cyber Security: Challenges and Opportunities

Moderator: Ravi K. Iyer (UIUC/ADSC)

Panelists:

Profs. HB Gooi (NTU), David Nicol UIUC/ADSC,

Nils Tippenhuauer (SUTD)

New Technologies

- **Cloud computing**
- Software defined networking
- **Intelligent HMI**
- Machine learning methods

Large Volume of Data

- **Sensors**
- IEDs, PMUs
- **Electric cars**

Smarter Grid Ecosystem

- **Cost effective**
- Trustworthy
- **Environment friendly**

SCADA Control

- Resiliency in presence of:
  - malicious attacks and accidental errors
  - volatility of energy sources e.g., solar and wind
- Smart applications, e.g., efficient state estimation, use of PMU data for control

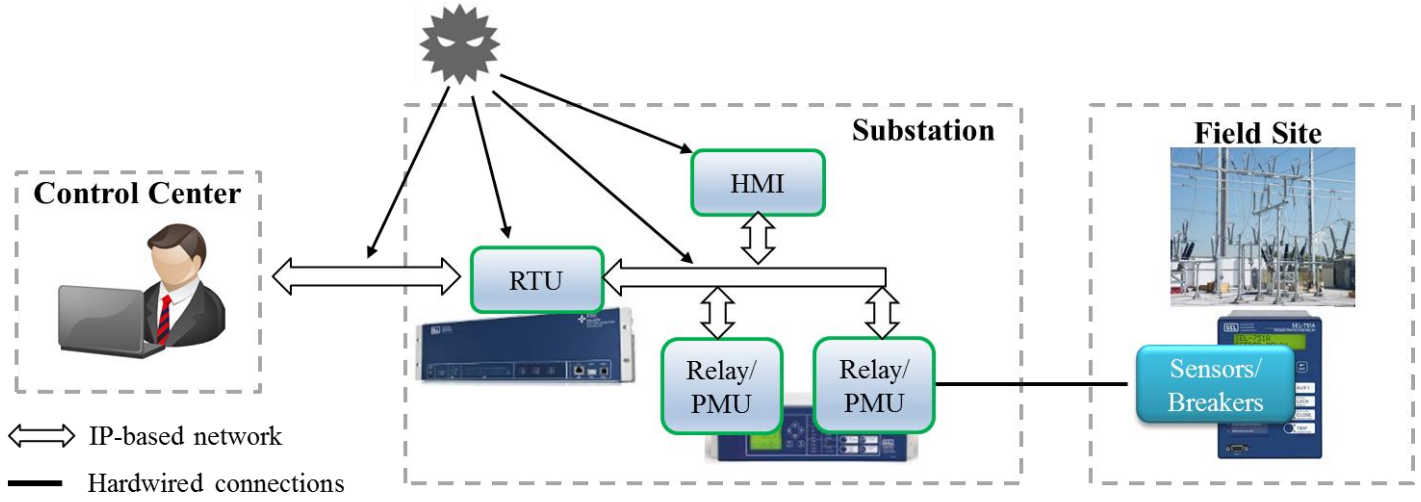
Assessment

- Methods and tools to support design and quantitative assessment of:
  - HW/SW architectures
  - devices, protocols, applications,
  - security and reliability of monitoring and protection mechanisms
- Model-based assessment
- Experiment-based assessment

Individuals & Enterprises

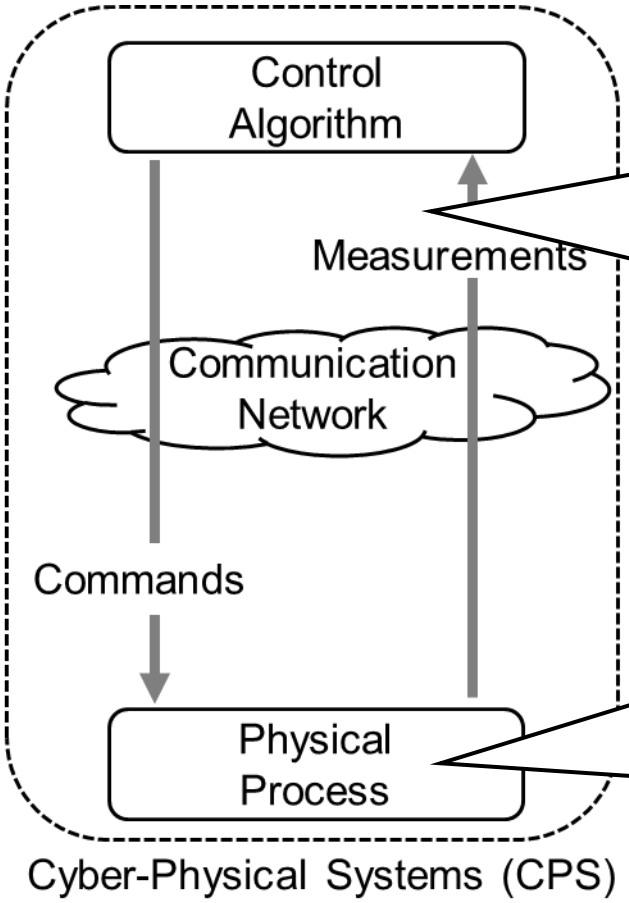
- **Human expertise**
- **Innovations**
- **Education**
- **Research**

Cyber-Physical Attack Models in the Power Grid



- **Remote penetration of isolated control networks**
  - E.g., sohisticated preparation used by attackers of Ukraine power grids
- **Initiated in Cyber Domain**
  - Monitor power flow on transmission lines
  - Identify target devices to attack
  - Compromise control fields in network packets
- **Manifested in Physical Domain**
  - E.g., Overloaded transmission lines to cause cascaded effect

Challenges in Detecting Cyber-Physical Attacks



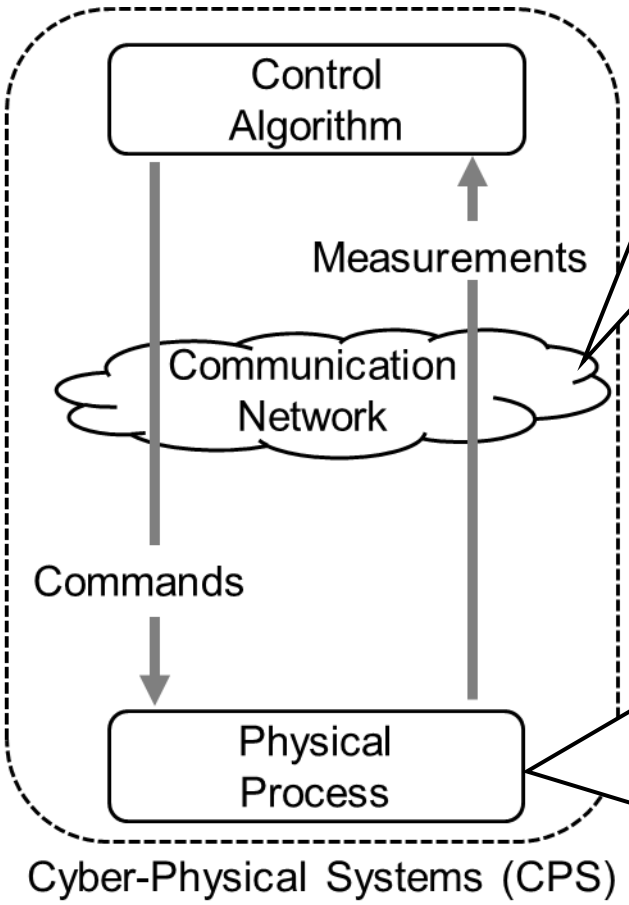
Challenge in cyber-domain

- Lack of encryption in communications
- Malicious commands in legitimate formats
- Inconsistency between states seen in cyber and physical domains
- Real-time constraints on control systems

Challenge in physical-domain

- Hard to distinguish attacks from incidental failures and human induced errors.
- Inadequate knowledge of the global system state.

Detecting Cyber-Physical Attacks: Continuous Monitoring, Learning plus Smart Analytics



Increase visibility in the cyber domain:

- Integrate network monitors (e.g., Bro) with CPS protocol (e.g., DNP3) analyzers
  - Monitor measurements, keep track of current state of the physical process
  - Extract commands' semantics from network packets

Estimate (ahead of time) the consequence of commands' execution

- Combine network monitoring with power flow analysis
  - Estimate the system state if commands are allowed to execute
- Adaptive power flow analysis algorithm:
  - Dynamically adjust the algorithm parameters, to balance detection accuracy and latency