Security and Privacy-Aware Cyber-Physical Systems

Challenges:

- How to build an ideal resilient CPS?
  - architecture, build blocks and capabilities, design requirements (technical. legal, social)
- What solutions will be accepted by practitioners?
- Who/what is liable when such a system fails due to security and privacy attacks?

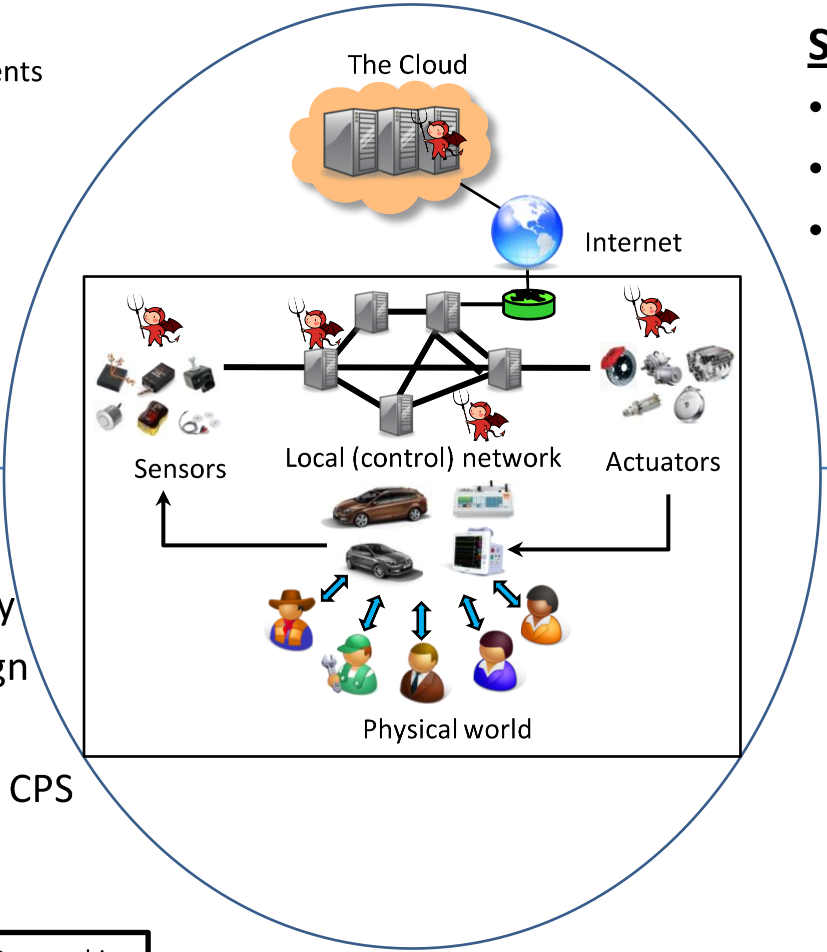
Solution:

- Platform support for security
- Security-aware control design
- Differential privacy in CPS
- Privacy-related tradeoffs for CPS
- Human-in-the-loop security assurance

Supported by NSF CNS-1505799 and Intel-NSF Partnership for Cyber-Physical Systems Security and Privacy

Lead institution: University of Pennsylvania

Lead PI: Insup Lee, lee@cis.upenn.edu



Scientific Impact:

- Foundational understanding
- New resilience techniques
- Case studies from different CPS domains (transportation, medical) to ensure that results are generally applicable

Broader Impact:

- Safer and more trustworthy CPS and IoT systems
- Clarification of legal consequences
- Joint law/engineering workforce training