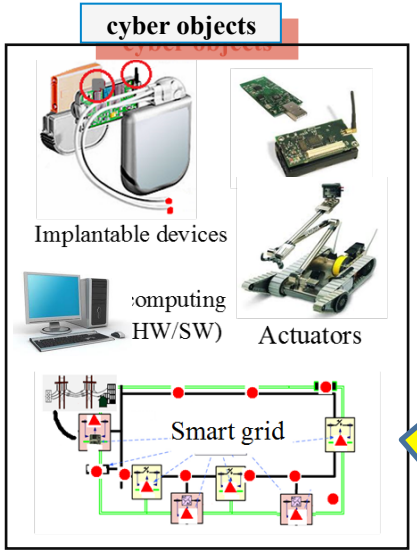
Cyber-Physical and Big Data Security: Training Workforce

THE UNIVERSITY OF ALABAMA

Cyber-physical Interaction Security; Big Data Security

Challenges:

- Lack of training on Security of cyber-physical systems (CPS).
- Difficult to teach Big Data security & privacy



Cyber → Physical:
Control Security
- Wireless charge attacks;
- Close-loop control attacks;
- Device coordination attack;
- Command misleading, etc.

Physical → Cyber:
Monitoring Security
- Sensor data attacks
- RFID tag attacks
- Memory reading attacks
- Log attacks (forensics)

Solutions:

- Use practical CPS examples to illustrate security (cases: IMD – implantable medical devices; Mobile Phones; Smart Grid, Industry Control, etc.)
- Explain how to secure big data analysis process (Machine Learning attacks & defenses).
- Interdisciplinary: Big data, Cybersecurity, Industry Control

Scientific Impacts:

- First development on Systematic Big data security education.
- Explains how to secure big data mining and learning.
- Covers major CPS security topics (control security, hardware security, etc.)

Broader Impacts:

- Trains next-generation cybersecurity workforce on big data and CPS security;
- Improves graduate students research capability;
- Used Virtual Reality based training approaches

PIs: Fei Hu (UA), Tommy Morris (UAH)
Contact: fei@eng.ua.edu