CPS AI

Building the Future of Cyber-Physical Super-Intelligence

Challenge Domains

- **Robustness and Reliability**
  - Security issues: Model poisoning, attacks, adversarial manipulation
  - Safety issues: Responsiveness, quality, coverage
- **SWAP**
  - Low resource models
  - Efficient execution
- **Holistic view:** Design of the Device/Edge/Cloud continuum for AI
- **Complex trade-off space:** Complex relations between model size, quality, and security
  - Small models may be more predictable and more economically viable
  - Large models are more feature-full
- Issues in **AI regulation for CPS**
  - Academics took the lead in the network neutrality debate. We should have a voice into AI regulation
- **Special purpose** (foundation) models
- **Human Interfaces** for intelligent CPS-Human Systems
  - AI and privacy
  - AI and usability
  - AI and interpretability/explainability
- **AI in CPS deign** → lifecycle perspective on CPS

Unique CPS Angle (page 1 of 2)

How is CPS changing the AI conversation

- **Dynamics:** The operating environment is a lot more dynamic
- **Adaptation:** Adaptation to the environment dynamics and applications is needed at a different level
  - Closed loop design to adapt while preserving assurances
  - A closed-loop
- **SWAP issues**
  - Interaction between resource issues and the system
- **Data issues**
  - How to handle challenges arising from insufficient data
  - How to compute risk and manage risk when the system had insufficient data to train
  - Simulation of the physical world
  - Digital twins, world models
- **Scale and Heterogeneity:** CPS applications are very heterogeneous so we need better ways to scale across different applications.
  - Foundation models that scale with the number of modalities not applications
  - What can be generalized across models
- **Depth:** Continuity between system 1 and system 2 models for the physical world (a knowledge versus reasoning trade-offs).
- **Holistic interactive complexity:** The importance of environment/perception/understanding:
  - Example: Resource limits affecting functionality, physics help counter threats

Unique CPS Angle (page 2 of 2)

- **Distributed multi-agent AI** in CPS:
  - Frameworks for safer multimodal multiagent systems that operate on the physical environment
  - Time is another dimension that they need to worry about
- **Neural network architecture** for CPS
  - Real-time architectures for AI. Physically inspired neural networks (PINNs). Rethinking the design of neural networks from a CPS perspective.
  - Post-training robustification: Changes between training and testing to help reliability.
  - Model design to provide assurances within specified input bounds
- **Software assurances:** Coding agents have gotten a lot better at low-level control tasks. It is changing the way people are designing systems but offers new robustness risks. How to make it robust?
- **Model/Data Gap:** CPS is about interaction often based on models with a gap to reality. AI in contrast is black box but closer to environment complexity. How to bridge the two? Neurosymbolic AI
- **Human to formal specification gap:** How to do a “formal specification” (instead of a natural language specification) as a new model “prompt” to express intent. How to bridge the gap between formal and information specification.
  - Create better interfaces to capture semantics or correct gaps
  - Is action consistent with the prompt
- Information theory + control + AI challenge. Since AI works on data.

Community Engagement and Infrastructure Support

- How to blend across communities (AI + CPS + stakeholders)?
- Stakeholder engagement: Example, AI for emergency management.
  - Engage AI community
  - Engage with stakeholder community to help understand the human angle in AI use
  - Engage with first responder community to understand how to integrate AI and user needs.
  - Bring these communities to our events
    - Example: AI for physical systems (robotics for search and rescue).
  - Workshops for bringing communities together
- Need for infrastructure to support AI-driven CPS research
  - How to facilitate data collection?
  - How to facilitate world simulation?
  - Need CPS community testbeds that allow running end-to-end CPS experiments in real-world physical settings (e.g., ARL Graces Quarters in defense, but for the broader community)
  - Linking with existing infrastructure programs
  - Facilitate end-to-end testing
    - Community scale effort (clusters tied together for training/testing/twinning)
  - What would the infrastructure look like for CPS AI?
    - Multi-tier architecture (device/edge/cloud continuum)
- Standard benchmarking for CPS applications
  - Database of examples
  - Leaderboard