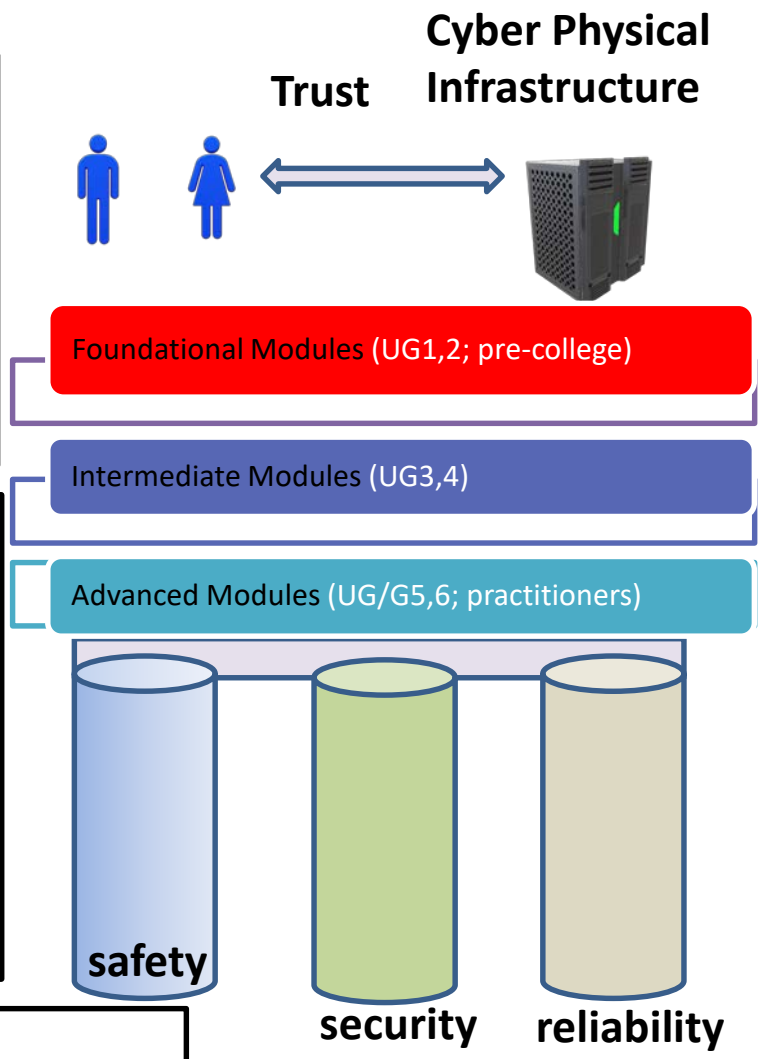
Cyber-Training: Pilot: Modular experiential learning for secure, safe, and reliable AI (MELSSRAI)

Challenges:

- How to promote trust between Cyber Infrastructure (CI) users and AI algorithms
- Delicate balance between improving secure and reliability and algorithmic performance.

Solution:

- Identify underlining reasons for AI mishaps
- Develop experiential learning modules to rapidly upskill CI users
- Assessing robustness of ML applications in CPS security



Scientific Impact:

- Model security, safety, and reliability (SSR) as pillars that support trust in AI
- Promote secure AI use by instilling trust as a core value.
- Understanding trade-off between security, safety and performance

Broader Impact and Broader Participation:

- Current and future CI users better understand what AI can and cannot do.
- Outreach through workshops at conferences
- Translation of education to the assessment of ML applications in security of CPS and human in the loop CPS

Investigators: A. Fong (PI), A. Gupta (Co-PI), S. Carr (Co-PI), and S. Bhattacharjee (Co-PI)

Grant #: 2017289

Contacts: alvis.fong@wmich.edu steve.carr@wmich.edu shameek.Bhattacharjee@wmich.edu ajay.gupta@wmich.edu