85th IFIP WG 10.4 Meeting
February 2-5, 2024 – Saint Simon's Island, Georgia, USA

Final Agenda

Thursday, Feb. 1

6:00-7:30pm   **Reception**
                                    King and Prince Hotel, Solarium

Technical Program

Trustworthy AI-Enabled Cyber-Physical Systems

Organizers: Homa Alemzadeh, Saman Zonouz
Location: King and Prince Hotel, Retreat Room (everything except lunches)

Friday, Feb. 2, 2024

7:15-8:00am	**Breakfast**
8:00-8:30am	**Welcome and Introductions**
	Marco Vieira, University of North Carolina at Charlotte
	Doug Blough, Georgia Tech
	Homa Alemzadeh, University of Virginia
	Saman Zonouz, Georgia Tech

Session 1 - ML/AI Verification in CPS

Session Chair: Marco Vieira, Scribe: Lishan Yang

8:30-9:15am	Neural Network Verification in Autonomous Cyber-Physical Systems
	Taylor Johnson, Vanderbilt University
9:15-10:00am	Assured Perception and Control of Autonomous Systems Using Formal Verification of Neural Networks
	Yasser Shoukry, UC Irvine
10:00-10:30am	Discussion
10:30-11:00am	**Coffee Break**

Session 2 - Safety and Security of ML-Enabled CPS

Session Chair: Domenico Cotroneo, Scribe: Carl Landwehr

11:00-11:45pm	Building Error-resilient and Attack-resilient ML-enabled CPS
	Karthik Pattabiraman, UBC
11:45-12:30pm	No-Regret Learning for Trustworthy Online Decision-Making
	Mahsa Ghasemi, Purdue
12:30-1:00pm	Discussion
1:00- 3:30pm	**Lunch (King and Prince, Solarium) and Break**
3:30- 4:00pm	**Coffee Break**

Session 3 - Trustworthy CPS and Educational Initiatives

Session Chair: Illir Gashi, Scribe: Rick Schlichting

4:00-4:15pm	Attacks and Defenses in Multi-robot Systems
	Cristina Nita-Rotaru, Northeastern University
4:15-4:30pm	Educational Efforts to Enhance Cybersecurity at William & Mary
	Evgenia Smirni, William & Mary
4:30-4:45pm	The Security of Engineered Systems
	Michael Bailey, Georgia Tech
4:45-5:15pm	Discussion

Saturday, Feb. 3, 2024

8:00-9:00am	**Breakfast**

Session 4 - Neurosymplic AI in CPS
Session Chair: Charles Weinstock, Scribe: Karthik Pattabiraman

9:00-9:45am	A Trip to the Neural Frontier: Neurosymbolic Sensor Fusion for Trustworthy CPS Luis Garcia, University of Utah
9:45-10:30am	Predictive Monitoring and Safety Shielding for AI-Enabled CPS Lu Feng, University of Virginia
10:30-11am	Discussion
11:00-11:30am	**Coffee Break**

Session 5 - Industry Panel
Session Chair: Lelio Di Martino, Scribe: Long Wang

11:30-12:30pm	Watch out for the Risky Actors: Assessing and Mitigating Risk in Dynamic Environments for Safe Driving Saurabh Jha, IBM
	Combating Digital Deception: Trustworthy AI in the Bot & Fraud Space Yi Han, F5
	Challenges of Using AI in Automotive CPS Ramon Serna Oliver, TTTech
12:30-1:00pm	Discussion
1:00- 3:30pm	**Lunch (King and Prince, Solarium) and Break**
3:30- 4:00pm	**Coffee Break**

Session 6 - Workshop Wrap-Up

4:00-5:00pm	Session chair reports, discussion, and workshop wrap-up

End Technical Program

Sunday, Feb. 4, 2024:

1:00pm   **Bus pick-up for excursion**
King and Prince, Lobby

7:00pm   **Dinner**
King and Prince, Solarium

Monday, Feb. 5, 2024:

8:00-8:30am   **Breakfast**

8:30–10:00am   Business meeting (members only)

10:00-10:30am   Break, hotel check-out

10:30am–12:30pm   Research reports

12:30pm   Meeting adjourns