



# Department of Computer Science

Enhancing Safety of Cyber-Physical Systems in Real Time

Mengyu Liu  
University of Notre Dame

**Hosted by: Cong Shi**

**Date:** Monday, January 27, 2025  
**Coffee:** 2:15 PM – 2:30 PM  
**Time:** 2:30 PM – 3:30 PM (Eastern Time (US and Canada))  
**Location:** GITC 4402 (4<sup>th</sup> floor Seminar Lecture Hall)

**Zoom Link:** <https://njit-edu.zoom.us/j/91910475199?pwd=brP5NqF4HUvHASKLwrYXqQeabCS96w.1>

Meeting ID: 919 1047 5199  
Passcode: 449110

**Abstract:**

Cyber-Physical Systems (CPS) tightly couple computing and network components with physical processes via sensors and actuators. Typical applications of CPS include autonomous vehicles, drones, and industrial robots. Compared to conventional IT systems, challenges in CPS security are distinct in terms of not only serious consequences in case of security breaches (e.g., vehicle crash) but also new attack surfaces (e.g., transduction attacks on sensors). In this talk, Mengyu will present his recent works on how to enhance the safety of CPS in real-time scenarios.

**Bio:**

Mengyu is a final-year PhD student in the Department of Electrical Engineering and Computer Science at University of Notre Dame. Before that, he obtained his master degree at Syracuse University. He completed his bachelor in Computer Science at University of Toronto.

Mengyu's research addresses security, resilience and real-time efficiency for Cyber-Physical Systems, through techniques of machine learning, formal methods, control theory, and algorithm design, with applications to autonomous systems such as self-driving cars and drones. He has published over 15 research papers at highly reputable venues including RTSS, RTAS, EMSOFT, ICCPS, DAC, etc, various IEEE/ACM transactions, and book chapters. He has received the championship of ACM SIGBED Student Research Competition and the championship of ESWEEK Embedded System Software Competition.