CPSS: Formal Methods, Safety and Security
Credits: 3
Course number: (Special Topics 6501/department equivalent)
Instructor: Lu Feng

Description
This is a core Cyber Physical Systems class. Cyber-physical systems (CPS) are smart systems that include co-engineered interacting networks of physical and computational components. Examples of CPS include medical devices, cars, and robots. Increasingly, such systems are everywhere. It becomes more and more important to assure the safety and security of CPS, since many CPS applications are safety-critical and life-critical. This course will give you the required skills to formally analyze the CPS that are all around us, so that when you contribute to the design of CPS, you are able to understand important safety-critical aspects and feel confident designing and analyzing CPS system models. It will provide an excellent foundation for students who seek industry positions and for students interested in pursuing research.

Prerequisites
This course has substantial elements of both mathematics and programming. You should have taken the following classes (or their equivalents): Discrete math, Probability, Linear Algebra, and Calculus.

Course Topics
Part I – Introduction to Formal Methods (This part will be following the textbook Principles of Cyber-Physical Systems; R. Alur, 2015, MIT Press.)
- Formal Specifications
  - Temporal Logics (LTL, CTL, STL, PCTL*)
  - Safety & Liveness Requirements
- Formal Modeling
  - Finite Transition Models
  - Timed Models
  - Hybrid and Dynamical Models
  - Probabilistic Models
- Formal Techniques
  - Formal Verification
  - Controller Synthesis
  - Runtime Monitoring

Part II – CPS Safety and Security Applications (This part will be based on state of the art research papers)
- Medical CPS
  - Safety: e.g., pacemaker verification, diabetes patient monitoring,
  - Security: e.g., attack on medical devices
- Automotive CPS
  - Safety: e.g., controller synthesis for autonomous driving
  - Security: e.g., attacks on automotive

Version updated on 3/25/19
- Smart cities & smart homes
  - Safety: e.g., runtime monitoring for smart city
  - Security: e.g., security and privacy of smart homes
- Human-in-the-loop CPS
  - Safety: e.g., verification and synthesis for human-UAV interactions
  - Security: e.g. man in the middle attacks
- Machine learning enabled CPS
  - Safety: e.g., falsification with Deep Learning enabled CPS
  - Security: e.g., adversarial machine learning

**Grading**
Overall course grades will be determined from: (percentages TBD)
- Homework
- Paper presentation and reviews
- Programming assignments
- Final project
- Quizzes and participation

**Project ideas**
- Potential programming assignments:
  - Drone collision avoidance (Matlab)
  - Road network generation for testing autonomous cars in Virtual Reality (Python and Unity3D)
- Students need to come up with their own ideas for the final course project.