NEW COURSE
Fall 2018
ENEE 769H (3 credits)- Advanced Topics in Controls: Formal Methods for Cyber-Physical Systems

Instructor: Professor John S. Baras (baras@isr.umd.edu)
Mon, Wed, 5:00 – 6:15 pm, Location: TBD

Purpose

Cyber-physical systems (CPS) are systems in which computational (cyber) processes interact closely with physical dynamical processes. The design and verification of such systems requires a good understanding of formal mathematical methods that are found in both computer science and the traditional engineering disciplines. These formal methods are used to model, verify, and design complex embedded systems in which the interaction of computational and physical processes must be approached in a holistic manner. This course introduces first/second graduate students to the formal methods used in the verification and design of cyber-physical systems with applications drawn from several areas: robotics, manufacturing, healthcare, autonomous vehicles, smart grids, security and privacy, communication networks, social networks.

Overview

Computing and communication capabilities are embedded in all types of objects and structures in the physical environment. Applications with enormous societal impact and economic benefit are and will be created by harnessing these capabilities across both space and time. Such systems that bridge the cyber-world of computing and communications with the physical world are referred to as *cyber-physical systems*. Cyber-physical systems (CPS) are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core. This intimate coupling between the cyber and physical is manifested from the nano-world to large-scale wide-area systems of systems. The Internet transformed how humans interact and communicate with one another, revolutionized how and where information is accessed, and even changed how people buy and sell products. Similarly, CPS is transforming how humans interact with and control the physical world around us. Examples of CPS include medical devices and systems, aerospace systems, transportation vehicles and intelligent highways, defense systems, robotic systems, process control, factory automation, building and environmental control and smart spaces. CPS interact with the physical world, and must operate dependably, safely, securely, and efficiently and in real-time. Most CPS are actually networked systems, and this fact introduces new challenges.

CPS can be considered to be a confluence of embedded systems, real-time systems, distributed sensor systems and controls. The promise of CPS is *pushed* by several recent trends: the proliferation of low-cost and increased-capability sensors of increasingly smaller form factor; the availability of low-cost, low-power, high-capacity, small form-factor computing devices; the wireless communication revolution; abundant communications bandwidth on-demand; continuing improvements in energy capacity, alternative energy sources and energy harvesting. The need for CPS technologies is also being *pulled* by cyber-physical system vendors in sectors like aerospace, building and environmental control, critical infrastructure, process control, smart grids, factory automation, and healthcare, who are increasingly finding that the technology base to build large-scale safety-critical CPS correctly, affordably, flexibly and on schedule is seriously lacking.

CPS bring together the discrete and powerful logic of computing to monitor and control the continuous dynamics of physical and engineered systems. The precision of computing must interface with the uncertainty and the noise in the physical environment. The lack of perfect synchrony across time and space must be dealt with. The failures of components in both the cyber and physical domains must be tolerated or contained. Security and privacy requirements must be enforced. System dynamics across multiple time-scales must be addressed. Scale and increasing complexity must be tamed. These needs call for the creation of innovative scientific foundations and engineering principles. Trial-and-error approaches to build computing-centric engineered systems must be replaced by rigorous methods, certified systems, and powerful tools. Analyses and mathematics must replace inefficient and testing-intensive techniques. Unexpected accidents and failures must fade, and robust system design must become an established domain. New sensors and sensor fusion technologies must be developed. Smaller and more powerful actuators must become available.

The confluence of the underlying CPS technologies enables new opportunities and poses new research challenges. CPS will be composed of interconnected clusters of processing elements and large-scale wired and wireless networks that connect a variety of smart sensors and actuators. The coupling between the cyber and physical contexts will be driven by new demands and applications. Innovative solutions will address unprecedented security and privacy needs. New spatio-temporal constraints must be satisfied. Novel interactions among communications, computing and control must be understood, modeled and analyzed. CPS will also interface with many nontechnical users. Integration and influence across administrative boundaries will be possible. The innovation and development of CPS requires computer scientists and network professionals to work with experts in various engineering disciplines including control engineering, signal processing, civil engineering, mechanical engineering and biology. This, in turn, will revolutionize how universities educate engineers and scientists. The size, composition and competencies of industry teams that design, develop and deploy CPS will also change dramatically. The global competitiveness of national economies that become technology leaders in CPS will improve significantly.

Topics to be Covered

The following broad areas will be covered:
CPS Composition, Robustness Safety and Security of CPS, Modeling and Control of Hybrid Systems, Computational Abstractions, Architectures, Real-Time Embedded Systems Abstractions, Sensor and Mobile Networks, Model-Based Development of CPS, Verification Validation and Certification of CPS.

The following is a more detailed list of topics that will be covered, organized in groups (parts):

Part – 1: Modeling CPS:

Dynamical Systems
Automata and Timed Automata
Hybrid Systems
Uncertain Systems

Networked Systems
Graphical Models
Petri Nets

Part – 1: Formal Methods from Computer Science:

Propositional and Predicate Logic
Floyd-Hoare logic, Communicating Processes
CTL, LTL and MTL Model Checking
Constraint Programming and Constraint Based Reasoning
SAT and SMT Solvers
Black-box testing
Compositionality and Composability

Part – 2: Formal Methods from Control Theory:

Feedback Control and Stability
Risk Sensitive and Robust Control
Optimization Methods
Game Theoretic Methods
Lyapunov and Inverse Lyapunov Methods
Control of Hybrid Systems
Reachability Analysis

Part – 3: CPS Validation and Verification:

Requirements Engineering, Safety-Reliability-Security
Spatio-temporal constraints
Symbolic and Numerical Model Checkers for Timed and Hybrid Systems
Integration of Logic and Optimization
Integration of Reachability Analysis with MTL Methods
Communicating Extended Finite State Machines
Distributed Timed Petri Nets
Model-Checking methods and Tools
Contracts
Formal Theorem Proving Methods
AI and Learning Methods
Safe Learning
Trusted Autonomy

Part – 4: Applications:

Model-Based Systems Engineering for CPS
Software Tools and Integrated Tool-Suites
Autonomous UAVs
Autonomous Cars
Traffic Control (Urban, Highway, Air)
Robotic Systems and Human-Robot Teams
Power-grid systems

Healthcare Systems (devices, instruments, hospitals)
Manufacturing Systems

Structure and Organization of the Course

Course will be based on recent (last five years) papers, tutorials and reviews on the subject matter, which will be distributed. Lectures will be given by the Instructor, and few distinguished guest lecturers. The grade will be based on a Take Home Mid-term Exam, a Take-Home Final Exam, and a Final Term Paper, that each student (taking the course for credit) will prepare with guidance from the instructor.

Prerequisites

Introductory Signals and Systems (at the level of ENEE 425), Control Systems (at the level of ENEE 460), Optimization (at the level of ENEE469O), Stability (at the level of ENEE 460), recommended. Linear Algebra and associated algorithms required (at the level of MATH 461). Introductory Discrete Mathematics and Logic recommended (at the level of CMSC 250). Working knowledge of MATLAB, C++ or JAVA required.