USC Viterbi
School of Engineering

CSCI 699
Topics in Formal Reasoning for Cyber-Physical Systems

Units: 4

Term—Day—Time: Fall-Tuesday-

Instructor: Jyo Deshmukh
Office: SAL 340
Office Hours: 11-12am Tuesday
Contact Info: jdeshmuk@usc.edu, phone number (cell: 512-203-7083), Skype: jyotirmoy.deshmukh, Email replies within 24 hours.

Teaching Assistant:
Office:
Office Hours:
Contact Info: Email, phone number (office, cell), Skype, etc.

IT Help: Group to contact for technological services, if applicable.
Hours of Service:
Contact Info: Email, phone number (office, cell), Skype, etc.

Course Description

Modern automobiles, medical devices, avionics systems, complex robots, smart energy and infrastructure systems are all examples of cyber-physical systems (CPS). Such systems are characterized by two main aspects: (1) physical components (e.g. electrical, electronic, mechanical, hydraulic mechanisms), and (2) software that is used to control the behavior of the physical components. Increasingly, such CPS applications are seeking to become autonomous with the help of artificial intelligence components trained using machine learning algorithms. In such a setting, an important question is how we reason about the correctness, safety, reliability and security of such systems. In this seminar course, we will explore the key literature in this area including the latest research results.

Learning Objectives

1. Gain basic familiarity with formal techniques for reasoning about correctness of CPS applications.
2. Understand verification approaches based on automatic techniques like model checking as well as less automated deductive methods.
3. Learn how system specifications are expressed using real-time temporal logics.
4. Learn about requirement-based testing approaches.
5. Learn about CPS applications that use AI-based components such as neural networks.
6. Learn how to critically read a technical research paper in this topic.

Prerequisite(s): CSCI 170, 270 (preferred)
Co-Requisite(s): none
Concurrent Enrollment: none
Recommended Preparation: Basic introduction to automata theory, formal verification (preferred)

Course Notes

Course Structure: The course will explore the topics indicated in the course description through a series of assigned readings in the form of papers and book chapters. The course is divided into three atomic topics. The reading list and description of the atoms is included later in this document. For each atom, the instructor will present the basic background material. Each class will be in the format of a discussion. For lectures giving introduction to background material, the instructor will lead the discussion. For student-led discussion classes, one student will be designated as a discussion leader and one student as a scribe. The leader will be tasked on moderating the discussion and the scribe will be tasked with summarizing the discussion. The discussion summary will be posted to the course web-page.

Course project/paper: Students will have a choice to do a project with a working demonstration or a technical paper with a new idea. Students will have the choice of working in groups of 2, or to work solo. The course project can explore building prototypes of algorithms discussed in one of the assigned papers or a related paper. Technical papers that students choose to write can either be a comprehensive survey or can propose a new technical idea.

Technological Proficiency and Hardware/Software Required

No specific hardware/software proficiency required. Ability to read advanced mathematical and research papers required.

Required Readings and Supplementary Materials

All reading material will be posted on the course web-page at the beginning of the course. The following is a list of papers that we will use:

Atom A. Basics of CPS Verification

A1. Ranjit Jhala, Rupak Majumdar: Software model checking. ACM Comput. Surv. 41(4): 21:1-21:54 (2009)
A2. X. Chen, E. Abraham, S. Sankaranarayanan, Taylor model Flowpipe construction for non-linear hybrid systems. In IEEE Real-Time Systems Symposium, 2012.

A3. C. Le Guernic, A. Girard, Reachability analysis of hybrid systems using support functions. In International Conference on Computer Aided Verification, 2009.
A4. A. Donzé, O. Maler, Systematic simulation using sensitivity analysis. In Hybrid Systems: Computation and Control, 2007.
A5. S. Prajna, A. Jadbabaie, Safety verification of hybrid systems using barrier certificates. In Hybrid Systems: Computation and Control, 2004.
A6. S. Gao, S. Kong, E. M. Clarke, Satisfiability modulo ODEs. In Formal Methods in Computer-Aided Design (FMCAD), 2013

Atom B. Basics of Temporal Logic-based Testing/Verification
B1. J. Kapinski, J. Deshmukh, X. Jin, H. Ito, K. Butts, Simulation-based Approaches for Verification of Embedded Control Systems, *IEEE Control Systems*, *36*(6), 45-64, 2016.
B2. G. Fainekos, G. Pappas, Robustness of temporal logic specifications for continuous-time signals. *Theoretical Computer Science*, 2009.
B3. A. Donzé, O. Maler, Robust satisfaction of temporal logic over real-valued signals. In International Conference on Formal Modeling and Analysis of Timed Systems, 2010.
B4. T. Wongpiromsarn, U. Topcu, and A. Lamperski, Automata theory meets barrier certificates: Temporal logic verification of nonlinear systems, *IEEE Transactions on Automatic Control* 2016.
B5. M. Kwiatkowska, G. Norman, and D. Parker, Stochastic model checking, *International School on Formal Methods for the Design of Computer, Communication and Software Systems*.

Atom C. Reasoning about CPS models with AI components
C1. G. Katz, C. Barrett, D. Dill, K. Julian, M. Kochenderfer, Reluplex: An efficient SMT solver for verifying deep neural networks. In *International Conference on Computer Aided Verification* 2017.
C2. M. Alshiekh, R. Bloem, R. Ehlers, B. Könighofer, S. Niekum, U. Topcu, Safe reinforcement learning via shielding, AAAI 2017.
C3. S. Ghosh, F. Berkenkamp, G. Ranade, S. Qadeer, S., A. Kapoor, Verifying Controllers Against Adversarial Examples with Bayesian Optimization, ICRA 2018.
C4. C. E. Tuncali, G. Fainekos, H. Ito, J. Kapinski, Simulation-based Adversarial Test Generation for Autonomous Vehicles with Machine Learning Components, Intelligent Vehicles Symposium 2018

The following books can be used as supplementary reading material:
1. [HR] Logic in Computer Science, by M. Huth and M. Ryan, Cambridge University Press.
2. [BK] Principles of Model Checking by Christel Baier and Joost-Pieter Katoen, MIT Press.
3. [Alur] Principles of Cyber-Physical Systems by Rajeev Alur, MIT Press.

Description and Assessment of Assignments

Students will be expected to read the papers before class and submit a one-page review of the paper as homework. Every review should address the following 5 questions:
1. What is the main problem addressed by the paper?
2. What was done before, and how does this paper improve on it?
3. What is the one cool mathematical factoid or proof technique that was learned from this paper?
4. What part of the paper was difficult to understand?
5. What generalization or extension of the paper could be done?

Grading Breakdown

Category	Weight
Paper Reviews (15 papers @ 3% each)	45%
Participation and Scribing	25%
Final Project	30%

Grading Scale (Example)

Course final grades will be determined using the following scale

A 91-100
A- 86-90
B+ 81-85
B 75-80
C 60-75
F 59 and below

Assignment Rubrics

1. Reviews: Students will get credit for every review submitted. Reviews are expected to be turned in at the beginning of the class in which the paper will be discussed.
2. Participation: Students will be expected to participate in the class discussion. To ensure a minimum level of participation, we will have each student talk about their impression of the paper for up to five minutes. Once each student has had a chance to talk about the paper, the discussion leader will have the responsibility to sustain a discussion. The instructor will provide feedback to students about their participation as necessary.
3. Scribing: Each student will be tasked with being a scribe for at least one paper discussion. The paper summary should consist of no more than 5 slides, following the review template, with each slide dedicated to each question.
4. Project/Paper: Projects will be graded based on the depth of the research endeavor or the quality of the prototype tool. Survey papers will be graded based on their comprehensiveness. Technical papers will be graded based on their novelty and technical results. Students will be expected to present project proposals halfway through the course and give final presentations at the end of the course.

Assignment Submission Policy

1. Reviews are expected to be turned in at the beginning of every class on blackboard.
2. Proposal/Project Presentations are expected to be emailed to the instructor prior to the day of presentation.

Grading Timeline

Weekly.

Additional Policies

None.

Course Schedule: A Weekly Breakdown

	Topic	**Lead**
8/21	Admin, General Introduction	Deshmukh
8/28	Paper A1 Discussion	TBA
9/4	Invited Talk	TBA
9/11	Paper A2,A3 Discussion	TBA
9/18	Paper A4, A5, A6 Discussion	TBA
9/25	Introduction to Temporal Logic	TBA
10/2	Paper B1 Discussion	TBA
10/9	**Proposal Presentations**	TBA
10/16	Paper B2, B3 Discussion	TBA
10/23	Paper B4 Discussion	TBA
10/30	Paper B5 Discussion	TBA
11/6	Introduction to Autonomous CPS	TBA

11/13	Paper C1, C2 Discussion	Deshmukh
11/20	Paper C3, C4 Discussion	TBA
11/27	**Final Presentations**	TBA

Statement on Academic Conduct and Support Systems

Academic Conduct:

Plagiarism – presenting someone else's ideas as your own, either verbatim or recast in your own words – is a serious academic offense with serious consequences. Please familiarize yourself with the discussion of plagiarism in *SCampus* in Part B, Section 11, "Behavior Violating University Standards" policy.usc.edu/scampus-part-b. Other forms of academic dishonesty are equally unacceptable. See additional information in *SCampus* and university policies on scientific misconduct, http://policy.usc.edu/scientific-misconduct.

Support Systems:

Student Counseling Services (SCS) – (213) 740-7711 – 24/7 on call
Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention. engemannshc.usc.edu/counseling

National Suicide Prevention Lifeline – 1 (800) 273-8255
Provides free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week. www.suicidepreventionlifeline.org

Relationship and Sexual Violence Prevention Services (RSVP) – (213) 740-4900 – 24/7 on call
Free and confidential therapy services, workshops, and training for situations related to gender-based harm. engemannshc.usc.edu/rsvp

Sexual Assault Resource Center
For more information about how to get help or help a survivor, rights, reporting options, and additional resources, visit the website: sarc.usc.edu

Office of Equity and Diversity (OED)/Title IX Compliance – (213) 740-5086
Works with faculty, staff, visitors, applicants, and students around issues of protected class. equity.usc.edu

Bias Assessment Response and Support
Incidents of bias, hate crimes and microaggressions need to be reported allowing for appropriate investigation and response. studentaffairs.usc.edu/bias-assessment-response-support

The Office of Disability Services and Programs
Provides certification for students with disabilities and helps arrange relevant accommodations. dsp.usc.edu

Student Support and Advocacy – (213) 821-4710
Assists students and families in resolving complex issues adversely affecting their success as a student EX: personal, financial, and academic. studentaffairs.usc.edu/ssa

Diversity at USC
Information on events, programs and training, the Diversity Task Force (including representatives for each school), chronology, participation, and various resources for students. diversity.usc.edu

USC Emergency Information
Provides safety and other updates, including ways in which instruction will be continued if an officially declared emergency makes travel to campus infeasible. emergency.usc.edu

USC Department of Public Safety – UPC: (213) 740-4321 – HSC: (323) 442-1000 – 24-hour emergency or to report a crime.
Provides overall safety to USC community. dps.usc.edu