15-424/624/824: Logical Foundations of Cyber-Physical Systems

Course Syllabus

André Platzer

aplatzer@andrew

Computer Science Department, Carnegie Mellon University

Cyber-physical systems (CPSs) combine cyber effects (computation and/or communication) with physical effects (motion or other physical processes modeled by differential equations). Cars, aircraft, and robots are prime examples, because they move physically in space in a way that is determined by discrete computerized control algorithms. Designing these algorithms to control CPSs is challenging due to their tight coupling with physical behavior. At the same time, it is vital that these algorithms be correct, since we rely on CPSs for safety-critical tasks like keeping aircraft from colliding. In this course we will strive to answer the fundamental question posed by Jeannette Wing:

> "How can we provide people with cyber-physical systems they can bet their lives on?"

The cornerstone of our course design are hybrid programs (HPs), which capture relevant dynamical aspects of CPSs in a simple programming language with a simple semantics. One important aspect of HPs is that they directly allow the programmer to refer to real-valued variables representing real quantities and specify their dynamics as part of the HP.

This course will give you the required skills to formally analyze the CPSs that are all around us – from power plants to pacemakers and everything in between – so that when you contribute to the design of a CPS, you are able to understand important safety-critical aspects and feel confident designing and analyzing system models. It will provide an excellent foundation for students who seek industry positions and for students interested in pursuing research.

Contents

1 Course Information

Home https://lfcps.org/course/lfcps.html

Lectures Tue/Thu 11:50-1:10

Recitations Fri 10:10-11:30

Credit 12 units

Prerequisites As elaborated in Section 5, the course assumes prior exposure to basic computer programming, differentiation, and mathematical reasoning:

    1. 15-122 Principles of Imperative Computation (**or** equivalent), **and**

2. 21-120 Differential and Integral Calculus (**or** equivalent)

Textbook You are expected to follow the accompanying textbook (or its free electronic version), which also comes with videos that enable you to review lectures:
André Platzer. *Logical Foundations of Cyber-Physical Systems*. Springer, 2018.
DOI 10.1007/978-3-319-63588-0

Grading 5% Homework, 29% Labs, 22% Final project, 22% Midterms I+II, 22% Quiz. Your best dozen quizzes throughout the semester will determine your quiz score. Absent exceptional circumstances (such as unusually large discrepancies of exam and homework scores), grade assignment is based on total score percentages:

total score:	$\geq$90%	$\geq$80%	$\geq$70%	$\geq$60%	<60%
grade:	A	B	C	D	R

Quiz Learning by doing is a crucial element of understanding. Quizzes after nearly every lecture give you an opportunity to practice and identify what to review again. The purpose of this quiz is to give you feedback on how well you have achieved a selection of some of the learning goals of this chapter. By observing which ones you are unsure about, you can identify which material you should review again. Since you ultimately need a solid understanding of all aspects of cyber-physical systems, this helps you stay up to speed before you proceed to later chapters. The quizzes are open book and due in the week of the corresponding lecture.

Homework Weekly, usually Thursdays, consisting of theory assignments and labs.

Midterms in class, closed internet, closed book, one double-sided sheet of hand-written notes permitted. The dates of Midterm Exams I+II are on course web page.

Grand Prix During exam week for presenting final course project for feedback and possible awards to a panel of experts. The date is listed on course web page.

Diderot discussion board, quiz, homework submission, and grade information

Tools we will make ample use of the hybrid systems verification tool KeYmaera X
http://keymaeraX.org/

Key topics Cyber-Physical Systems · Dynamic Logic · Models and Controls · Axiomatics · Differential Equations Reasoning · Hybrid Games · Formal Verification

The 15-424 course counts as a Logics/Languages elective in the Computer Science curriculum. The course 15-824 fulfills the Programming Languages star requirement.

Please carefully read the entire syllabus to make yourself familiar with the contents and expectations and policies in this course. It is also your go-to reference later.

Pandemic Provisions

The course staff is monitoring the progress of the pandemic. If you are unable to come back to campus or otherwise have scheduling conflicts, the course has a does-not-meet section to enable you to take this course based on its extensive electronic resources. This will require your initiative to succeed.

For everyone's safety, you are required to follow CMU's and CDC's best practice guidance when attending lecture or recitation in person. You are required to wear facial coverings / masks at all times in class, regardless of vaccination status.

2 Learning Objectives

The learning objectives of Logical Foundations of Cyber-Physical Systems are organized along the dimensions: *modeling and control*, *computational thinking* [2], and *CPS skills*.

2.1 Modeling and Control

In the area of *modeling and control*, successful students will
  – **understand the core principles behind CPS.** A solid understanding of these core principles is important for anyone who wants to integrate cyber and physical components to solve problems that no part could solve alone.
  – **develop models and controls.** In order to understand, design, and analyze CPS, it is important to be able to develop models for the various relevant aspects of a CPS design and to design controllers for the intended functionalities based on appropriate specifications, including modeling with differential equations.
  – **identify the relevant dynamical aspects.** It is important to be able to identify which types of phenomena of a CPS have a relevant influence for the purpose of understanding a particular property of a particular system. These allow us to judge, for example, where it is important to manage adversarial effects, or where a nondeterministic model is sufficient.

2.2 Computational Thinking

In the area of *computational thinking*, successful students should be able to
  – **identify safety specifications and critical properties.** In order to develop correct CPS designs, it is important to identify what "correctness" means, how a design may fail to be correct, and how to make it correct.
  – **understand abstraction in system designs.** The power of abstraction is essential for the modular organization of CPS, and for the ability to reason about separate parts of a system independently. Because of the overwhelming practical challenges and numerous levels of detail, abstraction is even more critical than it already is in conventional software design.
  – **express pre- and post-conditions and invariants for CPS models.** Pre- and post-conditions allow us to capture under which circumstance it is safe to

run a CPS or a part of a CPS design, and what safety entails. They allow us to achieve what abstraction and hierarchies achieve at the system level: decompose correctness of a full CPS into correctness of smaller pieces. Invariants achieve a similar decomposition by establishing which relations of variables remain true no matter how long and how often the CPS runs.

– **use design-by-invariant.** In order to develop correct CPS designs, invariants are an important structuring principle guiding what the control has to maintain in order to preserve the invariant. This guidance simplifies the design process, because it applies locally at the level of individual localized control decisions that preserve invariants without explicitly having to take system-level closed-loop properties into account.

– **reason rigorously about CPS models.** Reasoning is required to ensure correctness and find flaws in a CPS design. Both informal reasoning and formal reasoning in a logic are important objectives for being able to establish correctness, which, for CPS, includes also rigorous reasoning about properties of differential equations.

– **verify CPS models of appropriate scale.** This course is not limited to covering the science of how to prove CPSs, but you will gain practical experience through appropriately scoped projects in the theorem prover KeYmaera X. This experience will help you learn how to best select the most interesting questions in formal verification and validation. Formal verification is not only critical but, given the right abstractions, quite feasible in high-level CPS control designs.

– **use formal methods tools for CPS.** Formal verification at nontrivial scale becomes more feasible with a good command of formal verification tools. While a full coverage of all aspects of, say, an aircraft is out of reach for this course, you will be exploring a series of safe designs for increasingly challenging tasks of a robot controller. You also have the opportunity to explore your favorite projects in the final course project.

2.3 CPS Skills

In the area of *CPS skills*, successful students will be able to

– **understand the semantics of a CPS model.** What may be easy in a classical isolated program becomes very demanding when that program interfaces with effects in the physical world. A full treatment of, e.g., the semantics of stochastic CPS effects is better placed in a specialized course. But understanding the meaning of a CPS model with fewer dynamical aspects and knowing how it will execute is fundamental to reasoning.

– **develop an intuition for operational effects.** Intuition for the joint operational effect of a CPS is crucial, e.g., about what the effect of a particular discrete computer control algorithm on a continuous plant will be.

– **understand opportunities and challenges in CPS and verification.** While the beneficial prospects of CPS for society are substantial, it is crucial to also develop an understanding of their inherent challenges and of approaches for minimizing the impact of potential safety hazards. Likewise, it is important to understand

the ways in which formal verification can best help improve the safety of system designs.

3 Programming Language

With a suitably generalized programming language, the behavior of a CPS can be described by a program. This course develops the programming language of *hybrid programs* (HPs) to capture relevant dynamical aspects of cyber-physical systems in a simple programming language with a simple semantics. The most distinctive features of HPs are that they prominently feature *differential equations* and *nondeterminism*. HPs support differential equations as continuous models of the physical system dynamics so that you can directly write down a differential equation in the middle of a program to describe the behavior of physics. Nondeterminism is another feature required for the adequacy of CPS models, e.g. for capturing choices in the system execution or uncertainty about the environment. When describing a robot controller, for example, we cannot know for sure what decisions other agents in the environment reach and need to be prepared to handle multiple choices in the execution. The course leverages *differential dynamic logic* (dL) as a specification and verification language for rigorous reasoning about hybrid programs that makes program properties explicit and localizes reasoning about their correctness.

4 Course Project for the CPS V&V Grand Prix

The final course project gives you an opportunity for you to creatively use what you've learned throughout the course and dive deeply into a CPS problem of your choosing. It is your big chance to achieve fame, glory, and prizes at the CPS Verification and Validation final project competition (CPS V&V Grand Prix). What you attempt for your project is completely up to you. There are only two requirements: (1) We want your project to be challenging (you should learn something relevant to the themes of this class) and (2) we want your project to be fun (you should be excited to work on it)!

The course project consists of the following:

1. A *white paper* in which you set up some preliminary ideas regarding the topic, scope, and challenges of your project. Think of it as an elevator pitch for your idea.

2. The *project proposal* is a fleshed-out version of your white paper, giving you a chance to report on what you have already achieved in your research / implementation / proofs. The proposal also details your specific plans and technical challenges going forward. More substantiative results in your project proposal enable more informed feedback.

3. A *term paper* and project deliverables (such as models, proofs, implementations) describing your project outcomes in sufficient depth for us to assess your work.

4. A *final project presentation* in the CPS V&V Grand Prix.

Even if the white paper and proposal are worth less points than the final course project, there is a strong correlation of good performance on the white paper and proposal with good performance on the eventual project. You should, thus, do your best to have compelling white papers and proposals, because this gives you a stronger basis and increases the quality of the feedback you can get on how to approach the final project. On all submissions related to your course project, you should include your name and email address to make sure feedback can reach you. Otherwise you risk receiving no feedback and/or that feedback about your project reaches other people.

By submitting any part of your final course project, you agree to its information being stored, including on portable devices, and the final project to be shared publicly on the course web page, which will maximize the feedback and appreciation you can get for your hard work. You also ascertain that you are responsible for respecting relevant copyright etc. and have cited requisite related work.

5 FAQ

This section elaborates the expected background and purpose of this course.

5.1 Who Should Take This Course?

You should definitely take this logic course if
  – you ever want to program robots that operate near humans so that you need to understand how to do that safely, or
  – you ever want to develop computer control systems for cars, or
  – you ever want to write programs that control aircraft or drones, or
  – you ever want to help computers control power plants or the smart grid, or
  – you want to do embedded systems or cyber-physical systems, or
  – you are interested in learning how computation interfaces with the real world, or
  – you are simply fascinated by combining mathematics and computer science, or
  – you want to see logic matter in reality.

5.2 What are Students Expected to Know Before This Course?

The formal requirements for the course are listed in Section 1. The course assumes prior exposure to basic computer programming such as 15-122 and that you have seen basic differentiation as in 21-120. The course covers the basic required mathematical and logical background of cyber-physical systems but you will be expected to follow the companion textbook [1] as needed.

If you are afraid of programming or afraid of mathematics, then you will find this course more challenging. The course is specifically designed *not* to require particularly advanced background, but you should feel comfortable picking the required concepts up as we go. We will explain what you need to know in the course and provide pointers to reading material. Coming into this course, you should definitely already know what a

derivative is and be comfortable using derivatives in mathematical arguments. Throughout the course you need to develop an intuitive understanding of differential equations for modeling common physical processes. We will frequently need this ordinary differential equation system (ODE)

$$x' = v, v' = a \tag{1}$$

which can be understood as saying that the time-derivative of x is v, and the time-derivative of v is a. In other words, this differential equation means that the derivative of the position x is the velocity v, and the derivative of the velocity v is the acceleration a. Understanding ODE (1) will suffice for the first part of the course. As the course progresses, we will learn how to do elegant reasoning about even ODEs whose solutions are nasty, which provides a good opportunity to reinforce your understanding of ODEs.

5.3 What Time Commitment Does This Course Need to Succeed?

The course is a 12 unit course and includes lectures, recitations and quizzes. Assignments alternate between labs where you model and formally verify systems in a theorem prover and written assignments which exercise the underlying logical and mathematical theory. Before you submit your final robot (called *Veribot*), you will also submit a *Betabot*, which is a beta-version of your robot controller that you conjecture to be safe and submit for feedback. Unlike your final robot submission (the Veribot), your Betabot does not yet need to be verified, but should provide your best-thought-out conjecture in order to give you a head-start on your Veribot. Keep in mind that most CPS designs are more challenging than it appears at first glance. You should, thus, start your assignments early. The more thorough your early designs are, the better and more informative our feedback to you can be. So be sure to give your Betabot and Veribot sufficient attention.

How much time you need to complete this course depends on how easily the material comes to you. The course will certainly be challenging and require your full attention. It will not be challenging because of sheer volume of things that we demand you do. Instead, the challenges will be of a more conceptual nature. Your final safety arguments for a CPS design may be easy, but it takes time to develop a safe design in the first place and then build a safety argument for it. We structure the labs and assignments in a way that carefully builds things up layer by layer, so that you will learn about cyber-physical systems with a well-structured gradual approach. You will gradually learn about one layer of CPS challenges at a time and we will proceed to the next challenges once we have mastered the previous ones. The course's active learning quizzes also give you an opportunity to practice, learn from the feedback, and identify what to review again.

This is an interdisciplinary course. Every student will come in with substantial background in some but certainly not all areas. The course gives you time to play catchup on the background, including simple physics, differential equations, and logic, but you should expect to spend enough time getting up to speed and read up on the background.

5.4 How To Take This Course

Since not all material is covered in full in lecture, and reading presents a complementary way of internalizing material at your own pace, you are strongly encouraged to subsequently read the corresponding textbook chapters. Some students also learn better when first going through the textbook chapter at their own pace before the lecture.

Staying up to speed can be a challenge in any course, especially for remote students. The course quizzes that you complete after lecture give you an opportunity for active learning to practice the material and identify what you should review again before moving on. Only a function of your best quizzes count for your grade, so you do not need to worry if you miss one. At the same time, the course topics build on one another, so you should do your best to catch up, because later topics require a strong understanding of earlier topics. While the quizzes give you some flexibility, you should submit them early because recitations can then prioritize concepts that are more effective for your learning.

6 Schedule

The tentative schedule of lectures follows the chapters of the textbook [1] with some adaptations for semester timing reasons or to follow student interest:

1. Cyber-Physical Systems: Introduction
2. Differential Equations & Domains
3. Choice & Control
4. Safety & Contracts
5. Dynamical Systems & Dynamic Axioms
6. Truth & Proof
7. Control Loops & Invariants
8. Events & Responses
9. Reactions & Delays
10. Differential Equations & Differential Invariants
11. Differential Equations & Proofs
12. Ghosts & Differential Ghosts
13. Differential Invariants & Proof Theory
14. Hybrid Systems & Games
15. Winning Strategies & Regions
16. Winning & Proving Hybrid Games
17. Game Proofs & Separations
18. Axioms & Uniform Substitutions
19. Verified Models & Verified Runtime Validation
20. Virtual Substitution & Real Equations
21. Virtual Substitution & Real Arithmetic

7 Take Care of Yourself

Cyber-physical systems are crucially important for our society, but so are you! When you are facing CPS challenges or any others, please keep in mind that you can only help our society design better and safer systems if you also watch out for yourself. Do take some time to relax, which often helps you approach questions with a fresh perspective next morning.

All of us benefit from support during times of struggle. You are not alone. There are many helpful resources available on campus and an important part of the college experience is learning how to ask for help. You should ask sooner rather than later.

Should you find yourself or a friend in serious trouble, take it seriously: your classes can wait. For emergencies call UPMC's re:solve Crisis Network at 1-888-796-8226. Counseling and Psychological Services (CaPS) is here to help: call 412-268-2922 and visit their website at http://www.cmu.edu/counseling/.

Also consider reaching out to a friend, faculty or family member you trust for help getting connected to the support that can help.

8 Policies

8.1 Course Culture

This course is open to anyone who is excited about cyber-physical systems and wants to learn all they need to become proficient in the subject matter. With its cross-disciplinary appeal, this course attracts students from different majors, different backgrounds, and different prior experiences, who all bring valuable and unique perspectives to the interdisciplinary aspects of cyber-physical systems. Listening to the contributions and opinions of your fellow students provides a huge opportunity for you to learn how others approach and overcome the challenges of the world.

We desire an open and inclusive course culture, where diversity in all its aspects is embraced. Everybody is different, everybody is special, and it is our collective responsibility to ensure that everybody is welcome in this course. If you experience or observe behavior that makes you feel unsafe, unwelcome, or discriminated against, please let the instructors know so they can help.

8.2 Quizzes for Active Learning

Learning by doing is a crucial element of understanding material. The purpose of the course quizzes is to support your learning by giving you an opportunity to practice and get feedback on how well you have achieved a selection of some of the learning goals of this course. By observing which ones you are unsure about, you can identify which material you should review again. Since you ultimately need a solid understanding of all aspects of cyber-physical systems, this helps you stay up to speed before you proceed.

If you cannot find the answer to a question during a quiz, you can look at the textbook chapter again. Subsequently, however, you should carefully review any material you were

missing and incorporate a summary into your study notes. This helps you remember without having to look it up when you need it next time.

The most profound impact of your learning stems from the ways of thinking that you internalize so deeply that you can produce them on the fly without having to look anything up. Concepts that become part of your thinking will enable you to autonomously detect situations where they apply, instead of needing to rely on your manager to tell you which concept to apply in order to solve which problem.

While quizzes feature carefully paced introductory questions, they are also designed to challenge your understanding. This gives you an opportunity to think through some of the more subtle aspects of cyber-physical systems at your own pace before you face similar challenges in application contexts where they may become overwhelming. By solving a sequence of such separate challenges, you become better at understanding nuances and will internalize the way of thinking that is required to solve them. A few of the quiz questions give you an opportunity to synthesize multiple individual concepts to solve a small joint challenge. These questions exercise synthetic knowledge and enable you to form conceptual bridges between individual skills to identify what you need where.

For example, some of the quiz questions ask you to check your thinking on certain simple subskills, which are useful to acquire early to avoid confusions. Other quiz questions may make you wonder how long differential equations evolve and what exactly a safety property of a hybrid system means. These are fundamental questions about cyber-physical system models that you can answer using their semantics. Yet other quiz questions ask you to put all your acquired skills together to design simple CPS controllers or criticize their designs before facing the challenges of real applications. Discovering a problem in your thinking in the small context of a quiz question is a great learning experience and prevents you from the major downstream effects of carrying a conceptual misunderstanding forward into later parts of the course.

The quizzes feature active learning activities and are designed to lay an important foundation for your understanding right away. You are expected to have achieved a solid understanding of important core elements of this course by the time you reach a solid quiz overall score. In order to get there, it is in your best interest to work on every quiz as early as possible. However, the quizzes also feature some difficult questions. Since only your best quiz scores ultimately count for your grade, you already achieve a score on every quiz and can work toward securing even better quiz scores on later quizzes. Over time, you will learn which topics you understand particularly well and will find questions easier that initially appeared difficult.

The quizzes are genuine active learning quizzes. Even from a grade percentage perspective you can think of the quizzes as an exam stretched out throughout the semester. If you achieve a good quiz score, then you should have a solid understanding of this course. The converse implication does *not* hold. If you find the quizzes challenging, then that does *not* mean that you will receive a suboptimal grade. Rather, it means that you have been alerted to nuances in the understanding right away that you should double check now before the course moves on. Every foundation you lay early helps you better achieve such mastery of the material later on. This is reflected in the fact that only a function of your best quizzes ultimately counts toward your grade.

8.3 Evaluation Criteria

The most important criterion is always correctness. Buggy code is useless, and is likely to get a low score, because the corresponding CPSs are likely to do serious damage. Elegance and clear structure is beneficial if not necessary for achieving correctness. A secondary criterion is the performance of your robot controller in terms of reaching its goal and interacting with its environment.

Grading for written assignments is based on the correctness of the answer and the presentation of your reasoning. Strive for clarity and conciseness, but show how you arrived at the answer. Stating an answer without explanation does not count as an answer. If you cannot solve a problem, explaining your approach and why you failed is encouraged. Such answers will be given partial credit.

8.4 Due Dates and Late Submissions

Labs and written assignments will be submitted electronically via Diderot. **Labs have two different due dates**, the Betabots and the Veribots. Quizzes are due as indicated after their corresponding lectures.

Submitting assignments on time lets the instructional team provide feedback in a more timely and efficient manner. Assignments and especially labs build on each other, so timely submissions are crucial to your progress in the class. However, sometimes life happens. If you submit a lab or homework assignment late after it is due, 10% will be docked of the possible score per late day. For reasons of course logistics and to enable quick-turnaround feedback, *no late submissions or any extensions of any kind are possible for the final project!* You are strongly discouraged from submitting Betabots late, because you risk getting late feedback for your Veribot.

This course gives you a lot of flexibility so that you can manage health issues etc. Try to stay up to date, because it will otherwise get increasingly difficult to catch up.

Additional extensions, e.g., due to family or medical emergencies, should be requested on your behalf by your academic advisor or the Office of Student Affairs.

Written assignments, quizzes and exams must be done alone. Labs 0 and 1 must be done individually. Later labs can be done *individually or in pairs*. You must choose a partner by the respective due date of the Betabot. If you have difficulty finding a partner, or if problems in your working relationship arise during the semester, please get in touch with the instructor as soon as possible.

Exams are of special significance. For reasons of course logistics, make-up exams are generally not possible. In exceptional medical emergencies during an exam, go seek medical care immediately and immediately notify the instructor by email. Keep documentation of your health care in case your advisor or the Office of Student Affairs wants to check in with you. In these rare circumstances an oral exam may be used to expedite the process. If you experience technical difficulties during an exam, save your work and notify the course instructor immediately, attaching a copy of your exam so far.

8.5 Laptops and Phones in Lecture

As research on learning shows, unexpected noises and movement automatically divert and capture people's attention, which means you are affecting everyone's learning experience if your phone, laptop, etc. makes noise or is visually distracting during class.

Therefore, please silence all mobile devices during class and stow them away. You are welcome to use tablets or laptops for note-taking only, but if possible, please use laptops only in the back of the classroom so as not to distract others.

Research also shows that concepts are best internalized when actively working with the material and taking notes. You have a full textbook available [1], but you are strongly encouraged to write summaries of the most important material in your own words.

8.6 Collaboration and Academic Integrity

Academic Integrity is a core CMU value, and as a member of the CMU community, it is important that the work you turn in for this class is wholly your own. As your instructor, I will strive to ensure that you develop the necessary knowledge and skills to meet the learning objectives for this class, just as it is your task to put in the effort to complete the work, acquire the requisite background, and ask for help if you need it.

You are expected to comply with the University Policy on Academic Integrity, which will be applied rigorously. Please read this policy carefully to understand the penalties associated with academic dishonesty at Carnegie Mellon.

The value of your degree depends on the academic integrity of yourself and your peers in each of your classes. It is expected that, unless otherwise instructed, the work you submit as your own is your own work and not someone else's work or a collaboration between yourself and other(s). It is also expected that, unless otherwise instructed, you cannot share your work or any assignments, labs, quizzes, or exams with anyone else.

In this class, cheating/copying/plagiarism means copying all or part of a program or homework, model, or proof etc. from another student or unauthorized source such as the Internet, knowingly giving such information to another student, or giving or receiving unauthorized information during an examination. In general, *each solution you submit (assignment, lab, model, proof, quiz or exam) must be your own work.* Some labs expressly indicate that they can be done by a single student or by a pair of students, at your discretion. But all written assignments, quizzes, and exams must be your own. In the event that you use information by another person in your solution, you must clearly cite the source of this information (and receive prior permission if unsure whether this is permitted). It is considered cheating to compare or discuss complete or partial solutions.

It is *not* considered cheating to clarify vague points in the labs, assignments, or lecture material, or to give help or receive help in *general use* of the computer systems or tools such as KeYmaera X, or other facilities. It is permitted and encouraged to share general advice on how to use KeYmaera X or general discussions about course assignments. Any assistance, though, must be limited to discussion of the *problems in general*, and cannot be about the solutions of the assignments. You must also refrain from looking at other students' models and proofs while you are getting or receiving help for these tools.

It is an academic integrity violation due to *unauthorized assistance to share assignments, labs, exams, quizzes, models or proofs between different iterations of the course*. Do not post any material concerning this course publicly, e.g. to GitHub or BitBucket and remember to keep all repositories private at all times. The sole exception to this no-share policy is your final course project, which is your own self-defined project that you will be very proud of and are encouraged to share to show others what you can do.

When you are having difficulties designing safe controllers or conducting a safety analysis for them, keep in mind that this is quite a universal challenge. A good strategy to overcome such obstacles is to consider simplified scenarios with simplifying assumptions first. Correctness is crucial, and a correct safety result for a simpler safe controller is more valuable than a more general and more complex controller that fails to be analyzable.

8.7 Exams

Any communication with anyone other than course staff during the exams of this course constitutes an academic integrity violation. Resolution of exam conflicts must be requested within one week of release of the schedule of the respective exam. For reasons of course logistics, makeup exams cannot necessarily be given. In exceptional medical emergencies during an exam, go seek medical care immediately and immediately notify the instructor by email. Keep documentation of your health care in case your advisor or the Office of Student Affairs wants to check in with you. In these rare circumstances an oral exam may be used to expedite the process.

8.8 Accommodation

CMU makes every effort to provide accessible facilities and programs for individuals with disabilities. If you have a disability and require accommodations, contact the Office of Disability Resources at access@andrew.cmu.edu. Please let the instructors know early in the semester so that your needs may be appropriately met. Special accommodation for exams must be requested at least 2 weeks before each exam.

8.9 Recording

No student may record any classroom activity without express written consent from the instructor. If you have (or think you may have) a disability such that you need to record or tape classroom activities, you should contact the Office of Disability Resources to request an appropriate accommodation.

Any recordings of class sessions are solely for educational use by students enrolled in the course and, due to regulations under the **Family Educational Rights and Privacy Act (FERPA)**, must **not** be shared with anyone else under any circumstance.

8.10 Opt-Out Option for Research Study

Cyber-Physical Systems is a novel but very important area of science and engineering that is a challenge in research and in education. This new area requires entirely new

teaching material and principles. We plan to study and evaluate the effectiveness of teaching strategies and techniques for the Logical Foundations of Cyber-Physical Systems course for improving the quality of the teaching as well as possible dissemination of material about the course to other universities and the general public.

Unless you opt out, we plan to study the homework you are already submitting for grading purposes also for the purpose of this research study. Our study will involve both automated and manual inspection of homework submissions using means such as simulation and/or checking of proofs. The study will be performed on an anonymized version of your homework submissions and the final study will only be performed after you have received your grade in this course.

Your participation is voluntary. If you do not want your homework submission to be included in the study, *you can opt out* by emailing my assistant `chasek@cs.cmu.edu` with an email with subject `Opt-out 15424` and a short declaration that you would like to opt out from the study. Your decision to opt-out will not result in any penalty.

8.11 Re-grading

Most of our grading effort focuses on feedback to you. If we have made a mistake in any part of your grade assignment, however, you can submit your assignments for re-grading within two weeks after the assignment has been returned. You will receive a new grade after review, which, of course, may be higher or lower than your previous score, depending on where we have made a mistake in grading.

8.12 Communication Support

Communication Support of the Student Academic Success Center (SASC) offers free one-on-one communication consulting as well as group workshops to support strong written, oral, and visual communication in texts. This may help you write more compelling project proposals and term papers and succeed with a convincing presentation in the CPS V&V Grand Prix.

8.13 Extra Points for Proof Exploits: KeYmaera X Integrity

All feedback about how to improve the course material and KeYmaera X is always very welcome and is part of your participation grade. There is one form of feedback that is particularly helpful: feedback that concerns soundness.

Soundness is crucial and fundamental, but of special significance for the high stakes of cyber-physical systems. What good would a safety analysis of a broken cyber-physical system do if the analysis procedure itself is broken?

To reflect that, we are soliciting *Proof Exploits*. By which we mean proofs that exploit soundness-critical flaws in the lecture notes or soundness-critical bugs in KeYmaera X. Each new soundness-critical bug that you are the first person to report is worth 20 points of extra credit. For full credit you should also demonstrate with a proof exploit how that bug can be exploited to produce a proof of `false` or of `1=0`. A proof exploit is a formal proof on paper or a test case for KeYmaera X demonstrating how the flaw can

be exploited to exhibit a proof of `false`, which, since `false` is rarely true, cannot have a proof in any sound verification procedure.

Needless to say that this is not just a great way for you to earn extra credit but also a really solid preparation for questions scrutinizing what rules and axioms and proof attempts are sound and which ones aren't. This reflection is an invaluable skill when it comes down to analyzing CPSs.

We will award a special prize during the CPS V&V Grand Prix to the person achieving the most extra credit via proof exploits.

Hint: You are allowed to be *arbitrarily* creative in your proof exploits and do things that you are not ordinarily supposed to do in a verification tool.

8.14 Additional Course Requirements for 15-624

Being a master's-level course, the 15624 Logical Foundations of Cyber-Physical Systems course has additional course requirements. Students enrolled in 15624 are expected to read and follow the textbook chapters [1] carefully (for at least 10 of the chapters of your choosing). This additional course requirement is in your best interest in order to prepare you well for the topics discussed in this course and to make it easier for you to deliver a very compelling final course project. For some master's students, it might have been a while since you saw some basic concepts, so carefully going through the material again after it was developed in class will be valuable for your understanding.

For the proposal and term paper of the final course project, you are furthermore required to develop a thorough related work discussion. So please plan appropriate time for a literature search in your final course project. BibTeX is your friend for quality references if you write the paper using LaTeX.

8.15 Additional Course Requirements for 15-824

Being a PhD-level course, the 15824 Logical Foundations of Cyber-Physical Systems course has additional course requirements. The most important additional requirement is that students enrolled in 15824 are expected to deliver a final term paper that is of similar quality as a scientific publication, except that it reports about a shorter period of research than what a conference would expect. But your paper needs to deliver a crisp motivation, thorough related work discussion, a comprehensive presentation without unreasonable background knowledge assumptions etc. Basically, your term paper should be a research paper for a project that might be too small to be a real paper.

One way to understand this is that if you submit your term paper to a conference, then it should either be accepted or returned with "this is very interesting and promising and written well but more research would be needed." But it shouldn't come back with a review saying "reject because this paper isn't even written like a proper paper." Of course, if you end up publishing your term paper, that's even better!

As a PhD student, you need to learn how to read research papers related to CPS and/or logic. Over the course of the semester, you are expected to read at least half of the papers we point you to for further information. Feel free to follow your own interest.

8.16 Additional Course Requirements for Remote Students

The does-not-meet remote section of this course is online-only with prerecorded lecture videos, a textbook, and active learning quizzes to help you learn. But it still requires your discipline, devotion and organization to succeed. You are strongly encouraged to be very proactive about staying up to speed on the material covered in this course.

In the remote course, there are multiple avenues for regular and substantive interaction between instructors and students. Specifically, this course includes:

- Regular active learning quizzes (Section 8.2)
- Labs, assignments, and exams with feedback (Section 8.4 and 8.7)

You should pay close attention to course communication on Diderot, where you can also ask questions, as well as in office hours.

References

[1] André Platzer. *Logical Foundations of Cyber-Physical Systems.* Springer, Cham, 2018. URL: http://www.springer.com/978-3-319-63587-3, doi:10.1007/978-3-319-63588-0.

[2] Jeannette M. Wing. Computational thinking. *Commun. ACM*, 49(3):33–35, 2006. doi:10.1145/1118178.1118215.