Syllabus

This course is an introduction to high-assurance systems its application for the design and analysis of safe and secure cyber-physical systems. It serves as the foundation for further study in the field of high-assurance systems. In this course, high-assurance systems are computer-controlled systems that are designed and verified to meet stringent reliability, safety, security, and correctness standards that must reliably operate under normal and abnormal conditions, ensure safety, resist malicious attacks, adhere to requirements, and remain maintainable over time. Students will learn how to achieve high assurance through rigorous engineering practices, formal methods, verification techniques, and certification processes. They will learn how to enhance system security and justify the security implications of software and hardware system design and implementation. They will learn to use knowledge of operating system design principles to achieve safety and security goals. Students will learn to use formal methods to mathematically prove a cyber-physical system meets useful properties.

Instructor

Daniel G. Cole
605 Benedum Hall
dgcole@pitt.edu

Class time

TuTh 13:00--14:15
227 Benedum Hall

Office hours

TBD

Learning objectives

At the conclusion of this course, students should be able to do the following:

- explain basic operating principles of secure microkernels
- program and integrate secure microkernels into a cyber-physical system.
- define high-assurance specifications for cyber-physical systems.
- achieve high assurance through rigorous engineering practices, formal methods, verification techniques, and certification processes.
- enhance system safety and security to meet specifications
- use knowledge of operating system design principles to achieve safety and security goals.
- justify the security implications of software and hardware system design choices.
- use formal methods to mathematically prove a cyber-physical system meets useful properties.

Schedule

Week	Topic
1	Introduction to high-assurance systems
2	Microkernels
3	seL4 and HACMS
4	seL4 and CAmkES
5	Kry10 and KOS
6	Kry10 and KOS
7	Mathematical correctness of the microkernel
8	Introduction machine-checked proofs
9	Interactive proof assistants
10	Interactive proof assistants
11	Defining specifications for CPS
12	Formal verification of CPS properties
13	Certification of CPS systems
14	Rigorous digital engineering (HARDENS)
15	Final project or report

Insurance file

This is my system for reconsidering judgment grades. If an obvious error is made in grading your test or homework, I will correct it immediately. All appeals regarding severity and judgment *must be filed through a* **written appeal**. The appeal must include:

- A complete copy of the entire test or assignment, including grading rubrics.

- A cover page describing which problem(s) are in question and what the injustice is believed to be.
- How many points (a numerical value) you believe are owed to you.

Email the appeal to dgcole@pitt.edu as a **single PDF file** for one graded assignment.

This information will be saved in the insurance file until the end of the term. When I compute final grades, I will consider your insurance file. If the number of points in question is sufficient to improve your grade, I will evaluate your appeal and regrade. This process saves me time, and gives you a formal process for appealing grades.

Classroom Conduct

As soon-to-be engineers, students are expected to act professionally in class. Please observe the following guidelines for classroom and course conduct:

- Be in class on time. Showing up late means you miss important information and disturb the class.
- If you must leave class early, please let me know ahead of time.
- Keep talking to a minimum. It diverts your attention and those around you.
- If you must answer a phone call, please leave the class.
- No texting.
- No internet browsing.
- When you send me an email, please give your full name in a professional email with a salutation and closing.

Academic Policies

Academic Integrity

All students are expected to adhere to the standards of academic honesty. Any student engaged in cheating, plagiarism, or other acts of academic dishonesty would be subject to disciplinary action. Any student suspected of violating this obligation for any reason during the semester will be required to participate in the procedural process, initiated at the instructor level, as outlined in the University Academic Integrity Guidelines. This may include, but is not limited to the confiscation of the examination of any individual suspected of violating the University Policy.

To foster a high level of academic integrity, the MEMS Department has established a coordinated and uniform approach to dealing with violations of academic regulations against cheating and plagiarism. This approach involves disciplinary actions that increase in severity with number of instances a student has been found in violation of academic integrity.

AI policy

Artificial Intelligence (AI) tools, such as ChatGPT, GPT, DALL-E, Stable Diffusion, Midjourney, GitHub Copilot, and anything after, are not allowed to be used on quizzes, tests, and exams. AI may be used on other assignments unless stated otherwise.

You should note that all large language models still have a tendency to make up incorrect facts and fake citations, code generation models have a tendency to produce inaccurate outputs, and image generation models can occasionally come up with highly offensive products. It is each student's responsibility to assess the validity and applicability of any AI output that is submitted. You will be responsible for any inaccurate, biased, offensive, or otherwise unethical content you submit regardless of whether it originally comes from you or AI. You bear the final responsibility.

When using AI, any such use must be appropriately acknowledged by an AI use statement. This statement should describe specifically how AI was used in the preparation of the assignment. Using AI without this statement will be evaluated as if it were plagiarism. The university's policy on plagiarism still applies to any uncited or improperly cited use of work by other human beings, or submission of work by other human beings as your own.

Different classes at Pitt may implement different AI policies, and it is the student's responsibility to conform to expectations for each course.

Violations of this policy will be considered academic misconduct.

Disability Services

If you have a disability for which you are or may be requesting an accommodation, you are encouraged to contact both your instructor and Disability Resources and Services (DRS), 140 William Pitt Union, (412) 648-7890, drsrecep@pitt.edu, (412) 228-5347 for P3 ASL users, as early as possible in the term. DRS will verify your disability and determine reasonable accommodations for this course.

Copyright Notice

These materials may be protected by copyright. United States copyright law, 17 USC section 101, et seq., in addition to University policy and procedures, prohibit unauthorized duplication or retransmission of course materials. See Library of Congress Copyright Office and the University Copyright Policy.

Statement on Classroom Recording

To ensure the free and open discussion of ideas, students may not record classroom lectures, discussion and/or activities without the advance written permission of the instructor, and any such recording properly approved in advance can be used solely for the student's own private use.

Synchronous online lectures may be recorded by the instructor if it is appropriate to do so. An announcement to that effect will be made before the recording starts.

Student Opinion of Teaching Surveys

Students in this class will be asked to complete a *Student Opinion of Teaching Survey..* . Surveys will be sent via Pitt email and appear on your CourseWeb landing page during the last three weeks of class meeting days. Your responses are anonymous. Please take time to thoughtfully respond, your feedback is important to me. Read more about Student Opinion of Teaching Surveys.

Religious Observance

The observance of religious holidays (activities observed by a religious group of which a student is a member) and cultural practices are an important reflection of diversity. As your instructor, I am committed to providing equivalent educational opportunities to students of all belief systems. At the beginning of the semester, you should review the course requirements to identify foreseeable conflicts with assignments, exams, or other required attendance. If at all possible, please contact me within the first two weeks of the semester to allow time for us to discuss and make fair and reasonable adjustments to the schedule and/or tasks.

Diversity and Inclusion

It is my intent that students from all diverse backgrounds and perspectives be well served by this course, that students' learning needs be addressed both in and out of class, and that the diversity that students bring to this class be viewed as a resource, strength and benefit. Please let me know ways to improve the effectiveness of the course for you personally or for other students or student groups.

If you feel like your performance in the class is being impacted by your experiences outside of class, please come and talk with me. I want to be a resource for you. If you prefer to speak with someone outside of the course, you might contact the University Counseling Center (412-648-7930).

The University of Pittsburgh does not tolerate any form of discrimination, harassment, or retaliation based on disability, race, color, religion, national origin, ancestry, genetic information, marital status, familial status, sex, age, sexual orientation, veteran status or gender identity or other factors as stated in the University's Title IX policy. The University is committed to taking prompt action to end a hostile environment that interferes with the University's mission. For more information about policies, procedures, and practices, see: https://www.diversity.pitt.edu/civil-rights-title-ix-compliance/policies-procedures-and-practices.

I ask that everyone in the class strive to help ensure that other members of this class can learn in a supportive and respectful environment. If there are instances of the aforementioned issues, please contact the Title IX Coordinator, by calling 412-648-7860, or e-mailing titleixcoordinator@pitt.edu. Reports can also be filed online: https://www.titleix.pitt.edu/civil-rights-title-ix-compliance/make-report. You may also choose to report this to a faculty/staff member; they are required to communicate this to the University's Office of Diversity and Inclusion. If you wish to maintain complete confidentiality, you may also contact the University Counseling Center (412-648-7930).

MEMS Department Email Dropbox

To provide a straightforward process for students to voice input and concerns, the MEMS Department has established the following email address: MEMS_confidential@pitt.edu. Messages will be received and acted upon in confidence by the MEMS Department Chair.