

**AERE 407/507 (COMS 407/507)****Applied Formal Methods**

3 credits

<b>Instructor:</b>	Prof. Kristin Yvonne Rozier Assistant Professor of Aerospace Engineering,
<b>Office:</b>	Howe Hall 2335
<b>Office Phone:</b>	515-294-6956
<b>E-mail:</b>	kyrozier@iastate.edu
<b>Office Hours:</b>	TR 12:40pm–1:55pm, or by appointment.
<b>Guest Lecturer:</b>	Rohit Dureja Guest Lecturer,
<b>Office:</b>	Howe Hall 2234
<b>E-mail:</b>	dureja@iastate.edu
<b>Office Hours:</b>	by appointment
<b>Department Office:</b>	AER-E, Howe Hall 1200
<b>Department Office Phone:</b>	515-294-5666
<b>Lecture:</b>	TR 11:00am–12:15pm, Room 2220 Howe Hall
<b>Course website:</b>	<a href="http://temporallogic.org/courses/AppliedFormalMethods/">http://temporallogic.org/courses/AppliedFormalMethods/</a>

**Prerequisites:**

- One of the following: AERE 361, or COMS 311 (required for COMS students), or an equivalent course + instructor permission.

**Course Goals and Learning Outcomes:**

In this course you will be introduced to the fundamentals of formal methods, a set of mathematically rigorous techniques for the formal specification, validation, and verification of safety-critical systems. We will explore the tools, techniques, and applications of formal methods with an emphasis on real-world use-cases such as enabling autonomous operation. Students will build experience in writing mathematically analyzable specifications from English operational concepts for real systems, such as aircraft and spacecraft. We will examine the latest research to gain an understanding of the current state of the art, including the capabilities and limitations of formal methods in the design, verification, and system health management of today's complex systems.

**Learner Objectives**

In this course you will gain hands on experience with formal methods tools and techniques. Through assignments, classroom discussions, homeworks, and projects you will have the opportunity to learn to:

- Specify system requirements formally in Linear Temporal Logic (LTL).

- Specify systems as formal models.
- Apply model checking to system models and LTL specifications to determine if the models satisfy the specifications.
- Use tools popular in industrial verification labs, including explicit and symbolic model checkers, and theorem provers.
- Evaluate real-world systems to determine appropriate formal methods to use in their analysis.
- Evaluate system requirements, including determining if they are safety or liveness, and performing basic specification debugging.
- Analyze and draw conclusions about real-world systems regarding formal properties.
- Explain the principles underlying formal methods for different types of system analysis (e.g. design time versus runtime), the capabilities, and the limitations.
- Develop an understanding of the current state of the art and how to find formal methods tools for real-world use cases.

## Reading Materials

- Reading materials will be handed out in class. If you cannot attend a class, contact the professor for a copy of the reading materials. *There is no required textbook for this class.*
- **Optional Textbook:** *Practical Formal Methods Using Temporal Logic* by Michael Fisher. Wiley & Sons, 2011. [[https://www.amazon.com/Introduction-Practical-Formal-Methods-Temporal-ebook/dp/B005E8AID2/ref=sr\\_1\\_1?ie=UTF8&qid=1483648485&sr=8-1&keywords=practical+formal+methods+using+temporal+logic](https://www.amazon.com/Introduction-Practical-Formal-Methods-Temporal-ebook/dp/B005E8AID2/ref=sr_1_1?ie=UTF8&qid=1483648485&sr=8-1&keywords=practical+formal+methods+using+temporal+logic)]
  - *Use this for:*
    - \* good background on LTL: well-formed formulas, semantics, encoding English sentences, expressivity, normal forms, relationship to automata
    - \* reactive system properties: safety, liveness, fairness
    - \* specification and modeling of real systems
    - \* deciding the truth of a temporal formula; related proof techniques including explicit model checking
    - \* thorough chapter on Spin, including how to run it from the command line and a good Promela tutorial
    - \* review of classical and propositional logic
    - \* extensions including synthesizing software from specifications
  - *Be cautious that:*
    - \* LTL is instead called PTL in this book; that is non-standard

- \* LTL2BA is not the best tool; SPOT is far superior now: <https://spot.lrde.epita.fr/>
- \* URLs provided are outdated (no longer active or superseded by the state of the art)
- \* Spin chapter refers to outdated xspin (though only briefly)
- **Optional Textbook:** *Systems and Software Verification: Model-Checking Techniques and Tools* by B. Berard (Author), M. Bidoit (Author), A. Finkel (Author), F. Laroussinie (Author), A. Petit (Author), L. Petrucci (Author), P. Schnoebelen (Author), P. McKenzie (Translator). Springer, 2001. [[https://www.amazon.com/Systems-Software-Verification-Model-Checking-Techniques/dp/3642074782/ref=sr\\_1\\_1?ie=UTF8&qid=1483572091&sr=8-1&keywords=systems+and+software+verification](https://www.amazon.com/Systems-Software-Verification-Model-Checking-Techniques/dp/3642074782/ref=sr_1_1?ie=UTF8&qid=1483572091&sr=8-1&keywords=systems+and+software+verification)]
- *Use this for:*
  - \* supplemental material on temporal logics (LTL, CTL, CTL\*)
  - \* background on automata as system models
  - \* review of explicit and symbolic model checking
  - \* reachability, safety, liveness, deadlock-freeness, fairness
  - \* overview of modeling abstraction methods
  - \* out-of-date chapters on SPIN and SMV still have useful reviews of basic tool usage
  - \* ideas for related formal methods, including timed automata models, additional tools
- *Be cautious that:*
  - \* *This book is extremely out of date!*
  - \* LTL is the proper name for Linear Temporal Logic (book calls it PLTL)
  - \* comparisons of LTL vs CTL/CTL\* have been changed/been disproved
  - \* SMV version described is no longer available; current tool is nuXmv
  - \* Spin version described has been updated (xspin vs ispin)

## Class Sessions

Class sessions will include discussions of the readings, guest speakers from industry, small group activities, and lecture. Students are encouraged to participate actively in class sessions.

## Course Assignments

Course assignments will help you achieve the objectives of the course. Brief descriptions of the assignments follow. Detailed instructions will be provided when each assignment is given.

## Examinations

A midterm examination will be given during normal class hours, covering the material from readings and homeworks from the first half of the course.

A final project spanning the second half of the course will serve in place of a final exam. All students will be required to present the results of their final project to the class at the end

of the semester in lieu of a final exam. The project is determined by a proposal, submitted by the student or group of up to three students and approved by the professor. **For graduate students, the final project must include a research component.**

### **Homeworks and Projects**

All homework submitted should be typed and formatted. **Handwritten assignments will not be accepted.** Homeworks designate between problems that must be solved by all students, and problems that must be solved by graduate students. (Undergraduates may complete the harder graduate-only questions for extra credit.) You are strongly encouraged to use  $\text{\LaTeX}$  to typeset your assignments. All assignments should be completed in accordance with the Iowa State University Honor Code.

For the homework assignments, you may talk about the problems with fellow students and the instructor, but the write up must be yours. In particular when discussing with fellow students you must strictly follow the “empty hands policy.” You cannot leave a discussion meeting with any record of the discussion (hard copy or electronic). All scratch paper must be torn and thrown away and all boards erased. In your homework write-ups, you should also give credit to your collaborators for each problem.

For all homeworks, you are allowed to consult other books, papers, or physical published materials in the university library. **The internet is NOT considered a published material. You may not search for answers, post questions to internet forums, or discuss any assignments on the internet. Doing so will be considered a violation of the Honor Code.** You must reference ALL of the sources (references or people) that helped you in the assignment in an attached bibliography, citing the sources where appropriate.

Plagiarism is considered a violation of the Iowa State University Honor Code. All solutions should be written in your own words, even if the solutions exist in a publication that you reference.

### **Presentation**

Each member of the class will present a research paper in applied formal methods to the class during the second half of the semester. Students will sign up for presentation times. The professor must approve all papers selected. Students can choose their papers from a provided list of papers or from a list of relevant publication venues. Alternatively, students may feel free to propose a paper on applying formal methods from any source for approval.

Students will evaluate the presentations of others for credit. While the professor will read these evaluations, presentations will be graded by the professor alone.

### **Grading**

Grades will be assigned based on performance on homeworks, projects, presentations, a midterm exams, and a final project. The weight assigned to each component is as follows:

<b>Grade Component</b>	<b>Percentage</b>
Homeworks and Projects	30%
Midterm	25%
Research Paper Presentation	15%
Evaluation of Other Presentations	5%
Final Project	25%

Course grades will be assigned as follows; minimum totals for grades may be lowered, but they will not be raised:

	A:	94 to 100	A-:	90 to 93	
B+:	87 to 89	B:	84 to 86	B-:	80 to 83
C+:	77 to 79	C:	74 to 76	C-:	70 to 73
D+:	67 to 69	D:	60 to 66		
F:	0 to 59				

## Course Policies

### Participation and Attendance

You are expected to participate actively in class, including presenting solutions to assignments, and giving a presentation to the class on a selected research paper in the field. Class periods will consist of interactive activities combined with lectures to aid in learning the course materials.

### Academic Integrity

Students are expected to uphold the Iowa State University policies for student conduct (<http://www.studentconduct.dso.iastate.edu>).

### Slip Days

Students have **two slip days** that may be used to delay the due date of any homework assignment for 24 hours during the first half of the semester. The use of a slip day must be explicitly stated at the top of the homework. Slip days may *not* be used for the second half of the semester, including the midterm, research paper presentation, or any assignments relating to the final project.

### Late Submission Policy

You are expected to submit assignments on the due dates. Assignments will only be accepted after the due date if arrangements are made with the instructor well in advance, or with proof of medical or other emergency.

### Electronic Devices

During class sessions, you may use laptop and tablet computers for work related to AERE 407/507 (COMS 407/507). Please silence cell phones during class and refrain from using cell phones or smart phones.

### Other Special Concerns

If you require special accommodations, you should notify the professor as soon as possible. In particular, you should contact the professor if an illness, religious practice, or disability might interfere with the successful completion of a course requirement.

---

## ISU Official Policies

---

### Respectful Communication

The classroom will be a place where everyone is treated with due respect. That includes accommodation of recipients choice of pronouns or titles. Your comments to others should be constructive and free from harassing statements. Strive to include everyone and select ideas and solutions on their merits, not based on prejudices and personalities. Mutual respect is expected inside and outside the classroom. Please contact the instructor if you have suggestions for improving the classroom environment.

## Academic Dishonesty

All acts of dishonesty in any work constitute academic misconduct. The Student Disciplinary Regulations will be followed in the event of academic misconduct. Depending on the act, a student could receive an F grade on the test/assignment, F grade for the course, and could be suspended or expelled from the University. Academic misconduct includes all acts of dishonesty in any academically-related matter and any knowing attempt to help another student commit an act of academic dishonesty that includes, but is not limited to (a) Obtaining unauthorized information, (b) Tendering of information, (c) Misrepresentation, and (d) Plagiarism, when performed in any type of academic or academically-related matter, exercise, or activity. See the Conduct Code at [www.policy.iastate.edu/policy/SDR](http://www.policy.iastate.edu/policy/SDR) for more details (See 4.2.1) and a full explanation of the Academic Misconduct policies.

## COVID-19 health and safety requirements

Students are responsible for abiding by the university's *COVID-19 health and safety expectations*.<sup>1</sup> All students attending this class in-person are required to follow university policy<sup>2</sup> regarding health, safety, and face coverings:

- wear a cloth face covering in all university classrooms, laboratories, studios, and other in-person instructional settings and learning spaces. Cloth face coverings are additionally required to be worn indoors in all university buildings, and outdoors when other people are or may be present where physical distancing of at least 6 feet from others is not possible. Students with a documented health or medical condition that prevents them from wearing a cloth face covering should consult with Student Accessibility Services in the Dean of Students Office.
- ensure that the cloth face covering completely covers the nose and mouth and fits snugly against the side of the face.
- practice physical distancing to the extent possible.
- assist in maintaining a clean and sanitary environment.
- not attend class if you are sick or experiencing symptoms of COVID-19.
- not attend class if you have been told to self-isolate or quarantine by a health official.
- follow the instructors guidance with respect to these requirements. Failure to comply constitutes disruptive classroom conduct. Faculty and teaching assistants have the authority to deny a non-compliant student entry into a classroom, laboratory, studio, conference room, office, or other learning space.

These requirements extend outside of scheduled class time, including coursework in laboratories, studios, and other learning spaces, and to field trips. These requirements may be revised by the university at any time during the semester.

In accordance with university policy, instructors may use a face shield while they are teaching as long as they are able to maintain 8 feet of physical distance between themselves

---

<sup>1</sup><https://www.dso.iastate.edu/guidance-for-supporting-community-expectations-during-covid-19-pandemic>

<sup>2</sup>

and students during the entire instructional period. Some form of face covering must be worn at all times in learning spaces regardless of the amount of physical distancing.

Faculty may refer matters of non-compliance to the Dean of Students Office for disciplinary action, which can include restrictions on access to, or use of, university facilities; removal from university housing; required transition to remote-only instruction; involuntary disenrollment from one or more in-person courses; and other such measures as necessary to promote the health and safety of campus.

It is important for students to recognize their responsibility in promoting the health and safety of the Iowa State University community, through actions both on- and off-campus. The university's faculty asks that you personally demonstrate a commitment to our Cyclones Care campaign.<sup>3</sup> Iowa State University's faculty support the Cyclones Care campaign and ask you personally to demonstrate a commitment to our campaign. Your dedication and contribution to the campaign will also protect your family, classmates, and friends, as well as their friends and families. Our best opportunity for a successful fall semester with in-person learning and extramural activities requires all of us to collaborate and fully participate in the Cyclones Care campaign.

### **Assistance with Communication**

The Center for Communication Excellence (CCE) of the Graduate College helps graduate students develop written and oral communication skills needed to successfully perform various academic tasks. To improve the quality of your papers and to practice your oral presentations, make one-on-one appointments with the CCE's specialized consultants. The CCE also offers a range of seminars and workshops on research writing, as well as facilitated peer review groups that provide constructive feedback. International students can additionally benefit from individualized English writing and English Speaking assistance. All forms of communication support offered by the are FREE! Make appointments and learn more from the homepage at <http://cce.grad-college.iastate.edu>.

### **Accessibility Statement**

Iowa State University is committed to assuring that all educational activities are free from discrimination and harassment based on disability status. Students requesting accommodations for a documented disability are required to work directly with staff in Student Accessibility Services (SAS) to establish eligibility and learn about related processes before accommodations will be identified. After eligibility is established, SAS staff will create and issue a Notification Letter for each course listing approved reasonable accommodations. This document will be made available to the student and instructor either electronically or in hard-copy every semester. Students and instructors are encouraged to review contents of the Notification Letters as early in the semester as possible to identify a specific, timely plan to deliver/receive the indicated accommodations. Reasonable accommodations are not retroactive in nature and are not intended to be an unfair advantage. Additional information or assistance is available online at [www.sas.dso.iastate.edu](http://www.sas.dso.iastate.edu), by contacting SAS staff via email at [accessibility@iastate.edu](mailto:accessibility@iastate.edu), or by calling 515-294-7220. Student Accessibility Services is a unit in the Dean of Students Office located at 1076 Student Services Building.

### **Religious Accommodations**

If an academic or work requirement conflicts with your religious practices and/or ob-

---

<sup>3</sup><https://www.care.iastate.edu/>

servances, you may request reasonable accommodations. Your request must be in writing, and your instructor will review the request. More information may be found at: <http://www.eoc.iastate.edu/discrimination/religious>.

### **Statement on Prerequisites**

It is the policy of the College of Engineering to require all students enrolled in this course to have satisfied all of the courses prerequisite requirements. If it is discovered that a student has not met any applicable prerequisite requirements, he/she will be required to immediately drop the course. The failure to drop the course will result in a final course grade of F, regardless of course performance. Students who discover they have improperly enrolled in a course without meeting the applicable prerequisite requirements are strongly encouraged to meet with advising staff to promptly drop the course and make alternative scheduling arrangements or discuss if an official waiver of the pre-requisite requirements may be applicable.

### **Statement on Dead Week**

This class follows the Iowa State University Dead Week policy as noted in section 10.6.4 of the faculty Handbook: <http://www.provost.iastate.edu/faculty-and-staff-resources/faculty-handbook>.

### **Harassment and Discrimination**

Iowa State University strives to maintain our campus as a place of work and study for faculty, staff, and students that is free of all forms of prohibited discrimination and harassment based upon race, ethnicity, sex (including sexual assault), pregnancy, color, religion, national origin, physical or mental disability, age, marital status, sexual orientation, gender identity, genetic information, or status as a U.S. veteran. Any student who has concerns about such behavior should contact his/her instructor, <http://new.dso.iastate.edu/sa/>, Student Assistance at 515-294-1020 or email [dso-sas@iastate.edu](mailto:dso-sas@iastate.edu), or the <http://www.hrs.iastate.edu/hrs/node/99> Office of Equal Opportunity and Compliance at 515-294-7612.

### **Contact Information**

If you are experiencing, or have experienced, a problem with any of the above issues, email [academicissues@iastate.edu](mailto:academicissues@iastate.edu).

*The contents of this document may be changed by the instructor during the semester.*