V&V FOR HIGH-DEPENDABILITY SYSTEMS – INTRO TO FORMAL METHODS

CIS 4930/6930 Sections 29EH/043E
Class Periods: MWF 5, 11:45-12:35
Location: CSE E221
Academic Term: Fall 2019

Instructor:
Steve Thebaut
smt@cise.ufl.edu
352-294-6672
Office Hours: M/W/F 10:00-11:00 AM or by appointment, CSE 330
Website: www.cise.ufl.edu/class/cen6070/special_topics_fa19.html (available mid-August)

Teaching Assistant: TBD

Course Catalog Description:
Credits: 3, Variable content provides an opportunity for in-depth study of topics not offered elsewhere and of topics of current significance.

Course Objectives: CIS 4930/6930, V&V for High-Dependability Systems – Intro to Formal Methods, is a small-enrollment, class-participation-driven seminar course intended to provide students with the "flavor" of Formal Methods. It is *not* a programming course or a practicum in mainstream software development.

> ***The term "formal methods" refers to various mathematical techniques that offer a rigorous approach to the development of high-quality software and are useful in the safety critical field.***

Topics include software reliability and dependability, relevant aspects of symbolic logic, formal (mathematical) program specification, axiomatic and function-theoretic verification, theory of computation, model checking, industrial tools for Formal Methods, and technology transfer to industry. Most topics are surveyed at a high level in the required textbook, "Concise Guide to Formal Methods: Theory, Fundamentals and Industry Applications" by Gerard O'Regan. Students will also read several historically significant papers from the literature related to some of the topics covered, and will lead and/or participate in group discussions of them. Class attendance and active participation is of paramount importance and, together with an in-class comprehensive closed-notes/closed-book exam, will be primary factors in determining final course grades.

The course will employ a "flipped learning" model whereby students will explore selected topics *outside the classroom* via assigned textbook/paper readings, the review of instructor provided self-study lecture notes, and working problem sets that may introduce course material *not* covered in the readings or lecture notes. *In the classroom,* the instructor will introduce and provide a brief overview of each course topic, answer questions related to previously assigned lecture notes, readings, and problem sets, elucidate critical concepts, etc., and oversee/facilitate focused group activities such as paper discussions, fishbowl conversations, and problem solving sessions. The success of this learning model requires diligent individual preparation for class, consistent class attendance, and active engagement in small group activities.

Prerequisites: CIS 4930 – COP 3503 or instructor permission; CIS 6930 – CIS 3020 (Advanced Programming Fundamentals for CIS Majors) and COT 3100 (Applications of Discrete Structures).

You should already be familiar with individual and team-based software development/programming using a high-level language (C, C++, Java, etc.), and have a basic knowledge of algorithms, data structures, and discrete math.

In addition, the non-programming, reading, writing and in-class group activity-intensive nature of this course is such that students should already be comfortable with English, using the technical terms necessary for computer scientists/engineers, and communicating effectively with others in small, diverse groups. Therefore, it may be

inadvisable for some students whose first or native language is not English to take this course *during their first semester at UF.*

Finally, depending on one's career goals and previous development/programming experience, it may be inadvisable to take this course in lieu of courses that provide vocational experience in mainstream software development/programming (e.g., agile development of web-based business applications). Please discuss with the instructor before the end of the *drop/add* course registration period if you think this might apply to you, or if you have any concerns about the prerequisites listed above.

Materials and Supply Fees: $47.13

Professional Component (ABET): **N/A**

Relation to Program Outcomes (ABET): **N/A**

Required Textbook:
Concise Guide to Formal Methods: Theory, Fundamentals and Industry Applications
Gerald O'Regan
2017
978-3-319-64020-4

A copy of the text will be placed on reserve in Marston Science Library when available. A Canvas course shell will be available via E-Learning to track attendance, submit assignments, and access scores/course grades.

Recommended Materials: N/A

Course Schedule/Topics (tentative): The following topics will be covered in the order given. Chapter numbers refer to the O'Regan text; ''LNO'' = Lecture Notes Only.

(1) Software Engineering (Ch 1)
(2) Reliability and Dependability (Ch 2)
(3) Overview of Formal Methods (Ch 3)
(4) Propositional and Predicate Logic (Ch 6)
(5) Advanced Topics in Logic (Ch 7)
(6) Z Formal Specification Language (Ch 8)
(7) Dijkstra, Hoare and Parnas (Ch 12)
(8) Mills Function-Theoretic Verification (LNO)
(9) Reasoning about Loops (LNO)
(10) Model Checking (Ch 14)
(11) The Nature of Theorem Proving (Ch 15)
(12) Industrial Tools for Formal Methods (Ch 17)
(13) Technology Transfer to Industry (Ch 18)
(14) The Future of Formal Methods (Ch 19)

In addition, student fishbowl discussions of two or three safety-critical system accidents/failures that resulted in the loss of life will take place in class during the 2nd and 3rd days of the "drop/add" (class enrollment change) period: Friday, Aug. 23 and Monday, Aug. 26. (Note that while class attendance is not required during the drop/add period, it is strongly encouraged, and familiarity with the systems/accidents discussed will be assessed during a comprehensive final exam in December.) Pointers to reading/review material concerning the systems/accidents to be discussed will be posted on Canvas by Monday, Aug. 19.

Attendance Policy, Class Expectations, and Make-Up Policy:
The University recognizes the right of the individual professor to make attendance mandatory. Following the initial Fall '19 drop/add period, registered CIS 4930/6930 students who do not have a documented medical excuse are generally expected to attend each and every class. Do not schedule elective activities (family gatherings, interview trips, weddings, divorces, vacations, etc.) that conflict with class or the final exam. Unexcused absences will count against you through the last class meeting, as will arriving late or leaving early for unexcused reasons as this can be a significant distraction for others. IT IS ESPECIALLY IMPORTANT THAT YOU BE PRESENT AND PUNCTUAL FOR SCHEDULED ACTIVITIES SUCH AS GROUP DISCUSSIONS, FISHBOWL CONVERSATIONS, PROBLEM SOLVING SESSIONS, TERM PROJECT PRESENTATIONS, ETC.

In general, excused absences must be in compliance with university policies (see:

https://catalog.ufl.edu/ugrad/current/regulations/info/attendance.aspx
or
https://gradcatalog.ufl.edu/content.php?catoid=10&navoid=2020#attendance)

and require appropriate documentation. However, you are allowed **2 absences** in CIS 4930/6930 during the semester due to sickness, accident, or other reasons beyond your control WITHOUT PROVIDING ACCEPTABLE DOCUMENTATION. (For example, "not feeling well enough" to come to class but "not feeling ill enough" to visit the Student Health Center, etc., to seek consultation/treatment.) Additional absences will only be excused with acceptable documentation.

Missing Class Due to Job Interviews: Job interviews are important and necessary. However, students should make a serious effort to schedule (or attempt to re-schedule already scheduled) interviews for days/times that do NOT conflict with class -- ESPECIALLY classes for which there are scheduled group activities. Given that a *conscientious effort* has been made to avoid such conflicts, a reasonable number of absences will be excused.

Make-Ups: If missing a class or the final exam is unavoidable (e.g., due to sickness, accident, or other reasons beyond your control), your absence may be excused and a suitable make-up activity may be made available to you. However, there is usually no practical way to "make-up" a missed in-class ***group activity***. Thus, if your absence meets the criteria for being excused described above, it will not affect your class attendance score, but any missed group activity will be dropped from the "participation" portion of your final grade, while the weight of the final exam portion of your grade will be increased by the same amount. *Again, this policy only applies if your absence meets the criteria for being excused.*

Absence from Final Exam: Note that depending on the circumstances, it may NOT be possible to make-up a final exam (missed for reasons beyond your control) before the end of the term. In such cases, a course grade of "I" (incomplete) may be assigned to be replaced after a (possibly oral) make-up exam has been administered the following semester..

Grading Policy/Evaluation of Grades: Course grades will be based solely on (1) required class attendance + participation/engagement in group learning activities, and (2) a 2-part, in-class comprehensive closed-notes/closed-book exam (tentatively scheduled for Monday, Dec. 2 and Wednesday, Dec. 4). There will be *no* "mid-term" exam.

The nominal grading break-down is as follows:

- Class attendance + participation/engagement in group learning activities: 50%
- Comprehensive exam: 50%

Evaluating ("grading") the *quality* of class participation/engagement is inherently subjective, but I will provide sample rubrics from various sources that will identify the specific participatory behaviors that one should aspire to. Obviously, evidence of having completed the assigned readings or other preparation activities in advance together with thoughtful, critical in-class discussion is paramount in this regard!

Grade requirements for graduation: Graduate students must have an overall GPA of 3.0 (B average) or better. (Note: a B- average is equivalent to a GPA of 2.67, and therefore does NOT satisfy this requirement.) Undergraduate students must have an overall GPA and an upper-division GPA of 2.0 (C average) or better. (Note: a C- average is equivalent to a GPA of 1.67, and therefore does NOT satisfy this requirement.)

More information on UF grading policy may be found at:

http://gradcatalog.ufl.edu/content.php?catoid=10&navoid=2020#grades
or
https://catalog.ufl.edu/ugrad/current/regulations/info/grades.aspx

Fishbowl Group Discussion Format: Various forms of "fishbowl discussions/conversations" will be employed in this class. In a fishbowl activity, a small group of students is chosen to discuss and/or demonstrate their knowledge and understanding of a topic, provide logical arguments for a position concerning a topic, etc. The rest of the class watches, listens, evaluates the arguments being presented, and reflects on new insights provided by the discussion. The presenter/observer roles change on a regular basis.

> *The fishbowl is a method to organize presentations and group discussions that offers the benefits of small group discussions – most notably, a spontaneous, conversational approach to discussing issues – within large group settings. This is done by arranging the room so that the speakers are seated in the center of the room with other participants sitting around them in a circle watching their conversation 'in the fishbowl.'*
>
> *- https://www.unicef.org/knowledge-exchange/files/Fishbowl_production.pdf*

We will discuss the use of this approach in CIS 4930/6930 during the first week of classes.

Students Requiring Accommodations:
Students with disabilities requesting accommodations should first register with the Disability Resource Center (352-392-8565, https://www.dso.ufl.edu/drc) by providing appropriate documentation. Once registered, students will receive an accommodation letter which must be presented to the instructor when requesting accommodation. Students with disabilities should follow this procedure as early as possible in the semester.

Course Evaluation:
Students are expected to provide professional and respectful feedback on the quality of instruction in this course by completing course evaluations online via GatorEvals. Guidance on how to give feedback in a professional and respectful manner is available at https://gatorevals.aa.ufl.edu/students/. Students will be notified when the evaluation period opens, and can complete evaluations through the email they receive from GatorEvals, in their Canvas course menu under GatorEvals, or via https://ufl.bluera.com/ufl/. Summaries of course evaluation results are available to students at https://gatorevals.aa.ufl.edu/public-results/.

University Honesty Policy:
UF students are bound by The Honor Pledge which states, "We, the members of the University of Florida community, pledge to hold ourselves and our peers to the highest standards of honor and integrity by abiding by the Honor Code. On all work submitted for credit by students at the University of Florida, the following pledge is either required or implied: "On my honor, I have neither given nor received unauthorized aid in doing this assignment." The Honor Code (https://sccr.dso.ufl.edu/policies/student-honor-code-student-conduct-code/) specifies a number of behaviors that are in violation of this code and the possible sanctions. Furthermore, you are obligated to report any condition that facilitates academic misconduct to appropriate personnel. If you have any questions or concerns, please consult with the instructor or TAs in this class.

Commitment to a Safe and Inclusive Learning Environment:
The Herbert Wertheim College of Engineering values broad diversity within our community and is committed to individual and group empowerment, inclusion, and the elimination of discrimination. It is expected that every person in this class will treat one another with dignity and respect regardless of gender, sexuality, disability, age, socioeconomic status, ethnicity, race, and culture.

If you feel like your performance in class is being impacted by discrimination or harassment of any kind, please contact your instructor or any of the following:
- Your academic advisor or Graduate Program Coordinator
- Robin Bielling, Director of Human Resources, 352-392-0903, rbielling@eng.ufl.edu
- Curtis Taylor, Associate Dean of Student Affairs, 352-392-2177, taylor@eng.ufl.edu
- Toshikazu Nishida, Associate Dean of Academic Affairs, 352-392-0943, nishida@eng.ufl.edu

Software Use:

All faculty, staff, and students of the University are required and expected to obey the laws and legal agreements governing software use. Failure to do so can lead to monetary damages and/or criminal penalties for the individual violator. Because such violations are also against University policies and rules, disciplinary action will be taken as appropriate. We, the members of the University of Florida community, pledge to uphold ourselves and our peers to the highest standards of honesty and integrity.

Student Privacy:
There are federal laws protecting your privacy with regards to grades earned in courses and on individual assignments. For more information, please see: https://registrar.ufl.edu/ferpa.html

Campus Resources:

Health and Wellness

U Matter, We Care:
Your well-being is important to the University of Florida. The U Matter, We Care initiative is committed to creating a culture of care on our campus by encouraging members of our community to look out for one another and to reach out for help if a member of our community is in need. If you or a friend is in distress, please contact umatter@ufl.edu so that the U Matter, We Care Team can reach out to the student in distress. A nighttime and weekend crisis counselor is available by phone at 352-392-1575. The U Matter, We Care Team can help connect students to the many other helping resources available including, but not limited to, Victim Advocates, Housing staff, and the Counseling and Wellness Center. Please remember that asking for help is a sign of strength. In case of emergency, call 9-1-1.

Counseling and Wellness Center: http://www.counseling.ufl.edu/cwc, and 392-1575; and the University Police Department: 392-1111 or 9-1-1 for emergencies.

Sexual Discrimination, Harassment, Assault, or Violence
If you or a friend has been subjected to sexual discrimination, sexual harassment, sexual assault, or violence contact the **Office of Title IX Compliance**, located at Yon Hall Room 427, 1908 Stadium Road, (352) 273-1094, title-ix@ufl.edu

Sexual Assault Recovery Services (SARS)
Student Health Care Center, 392-1161.

University Police Department at 392-1111 (or 9-1-1 for emergencies), or http://www.police.ufl.edu/.

Academic Resources

E-learning technical suppor*t*, 352-392-4357 (select option 2) or e-mail to Learning-support@ufl.edu. https://lss.at.ufl.edu/help.shtml.

Career Resource Center, Reitz Union, 392-1601. Career assistance and counseling. https://www.crc.ufl.edu/.

Library Support, http://cms.uflib.ufl.edu/ask. Various ways to receive assistance with respect to using the libraries or finding resources.

Teaching Center, Broward Hall, 392-2010 or 392-6420. General study skills and tutoring. https://teachingcenter.ufl.edu/.

Writing Studio, 302 Tigert Hall, 846-1138. Help brainstorming, formatting, and writing papers. https://writing.ufl.edu/writing-studio/.

Student Complaints Campus*:* https://www.dso.ufl.edu/documents/UF_Complaints_policy.pdf.

On-Line Students Complaints: http://www.distance.ufl.edu/student-complaint-process.

Course Feedback: Please provide the instructor with your feedback/recommendations about this course at any time during or after the semester in which you are enrolled. This may be done verbally (e.g., during a mid-term conference), in writing or via online evaluation, and will be greatly appreciated.

Instructor Biography: Steve Thebaut received the BA in Mathematics from Duke University in 1977, and the MS and PhD in Computer Science from Purdue University in 1979 and 1983, respectively. His research interests have included software requirements engineering, testing and verification, and software engineering technology transfer. He has received funding from the National Science Foundation, IBM, the Florida Department of Education, the Florida High Technology and Industry Council, the Sino-Software Research Center at Hong Kong University of Science and Technology (HKUST), the Software Engineering Research Center (SERC-an NSF I/UCRC), and the Software Engineering Institute (SEI) at Carnegie Mellon University, where he was an invited lecturer in the SEI production of "Software Project Management," a nationally distributed video-based continuing education course. He has been a course developer and consultant for IBM's IS&PG Technical Education program, and has served on the program committee of the Conference on Software Engineering Education. He was Associate Editor of the International Journal of Computer and Software Engineering from 1990-1996.