UNIVERSITÀ DI PISA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

Dottorato di Ricerca in Ingegneria dell'Informazione

Doctoral Course

"Verification and Validation of User Interface Software in Safety-Critical Systems"

Prof. Paolo Masci

NASA Langley Research Center (NASA LaRC) and Analytical Mechanics Associates (AMA)

E-mail address: paolo.masci@ama-inc.com; paolo.m.masci@nasa.gov

Short Abstract: Safety-critical systems, including those with a high degree of autonomy, provide user interfaces that allow human operators to control and monitor the system. Software modules typically define the functionalities of the user interface, including control safety functions. To gain confidence that the system can fulfil its expected mission goals, it is therefore important that user interface software is designed to make the system easy to use and at the same time capable of correcting foreseeable mistakes that can be committed by the operator.

This 20-hour course will provide PhD students with knowledge and skills on advanced methods and tools for rigorous verification and validation of user interface software in safety-critical systems. Examples from the avionics and medical domain will be used through the course to ground the discussion on concrete cases and actual systems.

The learning outcomes are: (i) understanding of the design challenges with user interface software in safety-critical systems; (ii) understanding of analysis methods and use-related safety requirements; (iii) understanding of verification and validation techniques based on formal (mathematical) methods; (iv) practical experience with toolkits routinely used at NASA Langley for the verification and validation of safety-critical systems, including the PVS theorem prover [3], the VSCode-PVS integrated development environment [4,5], and the DAA-Displays toolkit [6].

While the focus of this course is on safety-critical systems, the presented techniques are in fact generally applicable to any software-intensive interactive system, to catch latent design anomalies early in the development process, before important design decisions are made that could be expensive to correct at later stages of the development process.

Course Contents in brief:

- Design challenges in user Interface software in safety-critical systems
- Hazard analysis methods for software intensive safety-critical systems
- Formal methods technologies for V&V of user interface software
- Practical modeling and analysis experience with methods and tools routinely used at NASA Langley for the verification and validation of safety-critical systems

Total # of hours of lecture: 20 hours

References:

[1] “Assistive Detect and Avoid for Pilots in the Cockpit”, VA Carreño, P Masci, M Consiglio IEEE/AIAA 41st Digital Avionics Systems Conference (DASC), 2022

[2] “Usability Engineering Recommendations for Next-Gen Integrated Interoperable Medical Devices” P Masci, S Weininger, AAMI BIT, vol 55(4), 2022

[3] https://pvs.csl.sri.com/

[4] “An Integrated Development Environment for the Prototype Verification System”, P Masci and C Muñoz, Electronic Proceedings in Theoretical Computer Science (EPTCS), Vol. 310, pp. 35-49, 2019

[5] “Proof Mate: an Interactive Proof Helper for PVS”, P Masci and A Dutle, NASA Formal Methods Symposium, Lecture Notes in Computer Science, Springer, 2022

[6] “A Graphical Toolkit for the Validation of Requirements for Detect and Avoid Systems”, P Masci and CA Muñoz, Proceedings of the 14th International Conference on Tests and Proofs, Lecture Notes in Computer Science, Vol. 12165, pp. 155-166, 2020

CV of the Teacher

Paolo Masci is a Research Scientist (Associate Principal) with Analytical Mechanics Associates (AMA) at NASA Langley Research Center (NASA LaRC). He received his PhD in Information Engineering from the University of Pisa, Italy, in 2008. His expertise is on modeling and verification of human-machine interfaces in safety-critical systems. At NASA LaRC, Paolo is working on topics related to Urban Air Mobility (UAM) and Advanced Air Mobility (AAM) within the ATM-X project, in particular formal analysis of traffic alerting logic and resolution guidance, fast-time simulation of UAM/AAM flight scenarios, and rapid prototyping of assistive detect-and-avoid applications for pilots in the cockpit. Prior to joining NASA LaRC, Paolo developed his career in various universities and research institutions, including the University of Pisa (Italy), Queen Mary University of London (UK), and University of Minho (Portugal). Since 2010, he has been working in close collaboration with medical device manufacturers, hospitals, and medical device regulatory authorities, to carry out applied research on medical devices, e.g., see his publications on infusion pump software research carried out in collaboration with the FDA Center for Devices and Radiological Health.

Final Exam: Project Assignment

Room and Schedule

Room: *Aula Riunioni del Dipartimento di Ingegneria dell’Informazione, Via G. Caruso 16, Pisa – Ground Floor*

Schedule:

22/07/2024: 9:00-13:00

23/07/2024: 9:00-13:00

24/07/2024: 9:00-13:00

25/07/2024: 9:00-13:00

26/07/2024: 9:00-13:00