Model-based Development for High-Assurance Embedded Systems

Lecturers: John Hatcliff and Robby (Kansas State University)

Low cost embedded cyber-physical systems and ubiquitous networking has opened up a new world of connected devices in our homes and workplaces, and in safety critical contexts such as automobiles, medical care, and drone-based air vehicles. There are many different approaches to developing and assuring these systems, but not all take a rigorous approach and even fewer offer integrated frameworks for assurance.

In this lecture, we will introduce students to an integrated modeling and verification environment for high-assurance embedded systems. The modeling framework is based on the SAE standard Architecture and Analysis Definition Language (AADL). Students will enhance models from a building control systems and a simple medical device, generate component interfaces, develop component implementations and use an associated simulation environment to debug and assess the appropriateness of the design and implementation. Next, will use a code-level verification environment based on symbolic execution to illustrate how systems can be simulated and component implementations can be verified to conform to component contracts derived from system requirements.

An Overview of Malware Detection and Evasion Techniques

Lecturer: Axel Legay, INRIA

This tutorial presents and motivates various malware detection tools and illustrates their usage on a clear example. We demonstrate how statically-extracted syntactic signatures can be used for quickly detecting simple variants of malware. Since such signatures can easily be obfuscated, we also present dynamically-extracted behavioral signatures which are obtained by running the malware in an isolated environment known as a sandbox. However, some malware can use sandbox detection to detect that they run in such an environment and so avoid exhibiting their malicious behavior. To counteract sandbox detection, we present concolic execution that can explore several paths of a binary. We conclude by showing how opaque predicates and JIT can be used to hinder concolic execution.

	Tuesday, October 30	Wednesday, October 31	Thursday, November 1	Friday, November 2	Saturday, November 3
09:00		Meta-Modelling from a Practical Perspective	Model-based Development for High-Assurance Embedded Systems	Language-Driven Engineering	An Overview of Malware Detection and Evasion Techniques
10:30		*Coffee Break*	*Coffee Break*	*Coffee Break*	*Coffee Break*
11:00		Meta-Modelling from a Practical Perspective	Model-based Development for High-Assurance Embedded Systems	Language-Driven Engineering	An Overview of Malware Detection and Evasion Techniques
12:30	*Lunch Break*	*Lunch Break*	*Lunch Break*	*Lunch Break*	*Lunch Break*
14:30	Meta-Modelling from a Practical Perspective	Model-based Development for High-Assurance Embedded Systems	Model-based Development for High-Assurance Embedded Systems	An Overview of Malware Detection and Evasion Techniques	
16:30	*Coffee Break*	*Coffee Break*	*Coffee Break*	*Coffee Break*	
17:00 - 18:30	Soft Skills	Soft Skills	Soft Skills	Soft Skills	

STRESS 2018

5th International School on Tool-based Rigorous Engineering of Software Systems

30 October - November 3, 2018

Royal Apollonia Beach Hotel, Limassol, Cyprus

Associated with the **8th** International Symposium On Leveraging Applications of Formal Methods, Verification, and Validation (**ISoLA**)

http://santos.cs.ksu.edu/STRESS/2018/

Organizing Committee:

John Hatcliff, Kansas State University
Tiziana Margaria, LERO, The Irish Software Research Centre
Robby, Kansas State University
Bernhard Steffen, Technical University of Dortmund

The International School on Tool-based Rigorous Engineering of Software Systems (STRESS) series aims to provide top-quality lectures and innovative pedagogical material that provide young researchers with:

- instruction in existing and emerging formal methods and software engineering techniques that are tool-supported and process-oriented,
- insights into how software is developed in the real world, including emphasis on domains such as safety/mission-critical software and embedded systems where the development effort associated with tool-based formal methods promises greatest returns,
- case-studies and example domains in which formal methods have been successfully transitioned into actual development along with insights in how to bridge the gap between research tools and actual development processes, and
- additional pedagogical resources and personal contacts that they can explore for the purpose of increasing the impact of their research.

In addition to STRESS 2018, the ISoLA week offers a lot of opportunites besides the standard conference program, which addresses in particular also PhD students:

- The RERS challenge provides an ideal opportunity to check one's own verification competence. During the challenge you will meet world leading experts in tool-based software verification.http://www.rers-challenge.org
- The industrial day will give an impression of today's needs industry.

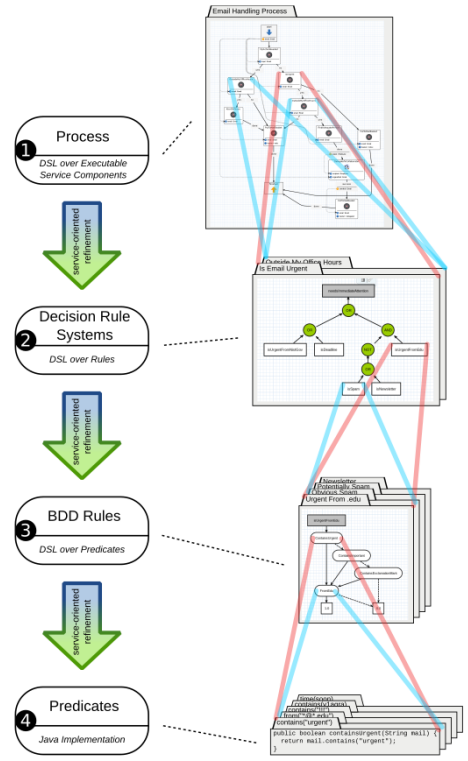
Finally, there is also a direct and tangible benefit for young scientists:

- The poster session gives PhD students the opportunity to give a 10 minutes sketch of their work, which they can later on elaborate on during the breaks. One page abstracts of selected contributions will be published in the ISoLA proceedings.
- Moreover, participating PhD student will be invited to contribute to the post conference proceedings published in Springer's CCIS series.

Language-Driven Engineering

Lecturers: Bernhard Steffen (Technical University of Dortmund), Tiziana Margaria (University of Limerick and LERO)

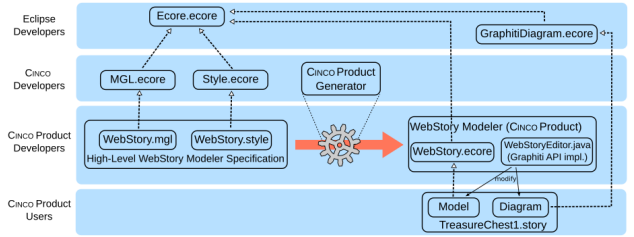
Language-Driven Engineering (LDE) is a new paradigm that aims at involving stakeholders, including the application experts, to participate in the system development and evolution process using dedicated Domains-Specific Languages (DSLs) tailored to match the stakeholders' mindsets. Technically, the interplay between the involved DSLs is realized in a service-oriented fashion. This eases product line and system evolution by allowing to introduce and exchange entire DSLs within corresponding Mindset-Supporting Integrated Development Environments (mIDEs). Participants of STRESS will be provided with a tangible LDE experience along the development and evolution of an email distribution system. The practical part will focus on the problem of profile-based email selection, where participants are invited to play with and adapt a variety of decision languages, e.g., to switch from a binary mindset to a "fuzzy" mindset. The practicality of the participants' solutions will be evaluated in a corresponding simulation environment.



Meta-Modelling from a Practical Perspective

Lecturers: Bernhard Steffen (Technical University of Dortmund), Tiziana Margaria (University of Limerick and LERO)

The practicality of LDE requires powerful means for the construction of Mindset-Supporting Integrated Development Environments (mIDEs). CINCO, the Meta Tooling Suite developed in Dortmund is designed exactly for this purpose. STRESS participants will be provided with hands-on experience with CINCO-based meta-model-driven engineering from three perspectives: (1) the perspective of a user of a CINCO product (an mIDE) by enhancing a basic "Web Story" application with additional features, (2) the perspective of an mIDE developer by enhancing the Web Story DSL, and (3) the perspective of a CINCO core developer by enhancing CINCO itself using CINCO.



In particular the third perspective is exciting because of its bootstrapping effect. As CINCO is available open source, participants are invited to continue their experimentation, and to cooperate as CINCO product users, CINCO product developers, or even as CINCO core developers.