Introduction to Electric Vehicles Software Design and Analysis

Spring Semester 2016

Master and Bachelor (Junior, 3rd Year) Combined Course

Associate Prof. Eun-Young Kang

Prerequisites

- This course is suited to undergraduate and master students who have some basic knowledge of or are interested in: real-time systems design and analysis, computer architecture, model-checking and Eclipse.

Course Description: Purpose & Application Areas

- Safety-critical vehicle systems. In contrast to general purpose systems, such a high assurance system development tends to place a stronger emphasis on rigorous requirements and specifications, V&V.
- Formal verification techniques, e.g., various forms of machine-checkable languages to demonstrate that a system satisfies its specification.

- The goal of this course is to:

+ Learn techniques to ensure reliable design and verification of these systems, in particular automotive systems.

+ E.g., ISO 26262 -- adaptation of the functional safety standard IEC61508 for automotive electric/electronic (E/E) systems and defines functional safety for automotive equipment applicable through the lifecycle of automotive E/E safety-related systems.

- *“Functional safety features form an integral part of each automotive product development phase, ranging from the specification, to design, implementation, integration, V&V, and production release. The standard ISO 26262 is an adaptation of the Functional Safety standard IEC 61508* for Automotive Electric/Electronic Systems.’’ [Wikipedia]*

- *IEC 61508 **is an international standard of rules applied in industry.** *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems* **(**E/E/PE, **or** E/E/PES**).**

- Concept of functional safety features, which form an integral part of each automotive product development phase, ranging from specification to design, implementation, integration, and V&V.

1. Study a collection of techniques currently used in industry to design and certify safety-critical vehicle systems;

2. Design and analyze realistic high-assurance automotive products, and investigate the extent to which formal V&V techniques can be incorporated into the development;

Objectives

- You will be able to demonstrate the following knowledge and skills:

1. Explain basic definitions related to safety-critical vehicle (SCV) systems;

2. Give an overview of the development process for SCV systems;

3. Explain and apply a methodology for writing requirements for SCV systems;

4. Use tools for formal architecture and behavior specification relevant to SCV systems;

5. Understand concepts and context relevant to SCV systems such as traceability, designing for testing, V&V, safety architectures, etc.;

6. Be familiar with concepts related to system certification, regulation, and application of safety standards;

7. Learning on-the-fly.

- **Course Topics**

1. Development process and life-cycle of SCV systems;
2. Definitions related to automotive systems safety;
3. Requirements and V&V of SCV systems;
4. Architecture Description Language, EAST-ADL, for automotive systems;
5. Formal architectural specifications, behavioral specifications, and interface specifications;
6. Definition of Non-functional operational properties that supports system analysis.

- **Course Materials**

All lectures and materials are in English. This course is based on concepts from model-based development and component-based development. The course slides will be accessible to registered students during the lectures via FTP, and will incorporate the following:

1. Modeling of requirements and V&V information;
2. Feature modeling for software system product lines;
3. Structural and behavioral modeling of functions;
4. Non-function operational properties and environment modeling, and analysis.

- **Additional Literatures**

Architecture Description Languages from Wikipedia:
http://en.wikipedia.org/wiki/Architecture_Description_Languages

EAST-ADL an Architecture Description Language, Validation and Verification Aspects: http://www.east-adl.info/index.html

MetaEdt+ : http://www.metacase.com/products.html

Verifying Functional Behaviors of Automotive Products in EAST-ADL using UPPAAL-PORT – Eun-Young Kang, Pierre-Yves Schobbens, and Paul Pettersson

An ADL centric approach for the formal design of real-time systems - Sébastien Faucou , Anne-Marie Déplanche, Yvon Trinquet (RTSt -IRCCyN, France)

Grade Allocation Scheme

- Individual Term Report (50%), Team Projects (40%), Participation (10%)

Grading System

- This course includes both individual assignments and team projects. Individual term reports must be completed "individually" (not in collaboration with other students).

- No paper exams: Term project presentation + individual reports/assignments are considered “Exams” so do not miss submitting reports and yourself during the team presentation.

- For team projects, each student is expected to make a unique and substantial contribution to the assigned project.

- Expectations for the project must be clarified by constructing a written system model that will summarize scope of the project, expected artifacts along with format and correctness of artifacts to be delivered, as well as the role and responsibilities of individual team members.

Others

- Lab course will start between the 5th and 6th lectures.

- Use of cell phones in class, for talking, texting or reading/writing email is prohibited. If you wish to leave your cell phone on in “Silent” mode because of an ongoing emergency situation that you may need to respond to, please speak to me at the start of class to let me know.

- You feel that your learning will be hindered by not having access to your laptop for note-taking or other legitimate purposes, speak to me in advance. Otherwise keep your laptop turned off and stowed away during class.

- Brief introduction of EAST-ADL architectural Language
- Examples of design and analysis
- Enjoy simulation and see you in person in the next class!