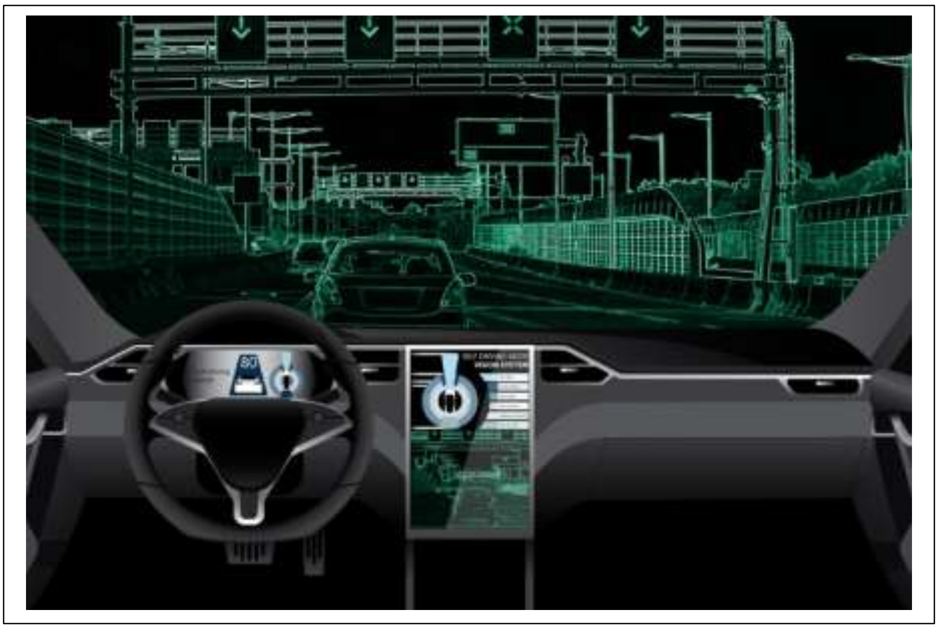
TECHNISCHE UNIVERSITÄT DRESDEN

HS SS-2019

Prof. Dr. Frank J. Furrer

Engineering Trustworthy Cyber-Physical Systems



© Shutterstock_746309743 (used with permission)

Summary

Cyber-physical systems are computer-controlled systems which interact with the physical environment, some of them in an autonomous way. Typical examples include autonomous cars, an autopilot in an airplane, or cooperating robots in a manufacturing line. Because of their impact on their real-world environment, cyber-physical systems must be built in such a way that they cannot harm or damage people or property: There behavior must be ***trustworthy***. Engineering trustworthy cyber-physical systems has become a specific, interesting engineering discipline – to which this Hauptseminar offers a gentle entry.

Context

A long time ago, computers were just processing data, such as keeping accounts or managing inventory. Then they slowly started interacting with the physical world in the form of embedded computers, such as controlling a combustion engine. Today, embedded computers controlling all sorts of cyber-physical systems are pervasive – we find them everywhere. From small devices, such as a heart pacemaker to large applications, such as an autonomous container ship, they have taken over control.

At the heart of a cyber-physical system is ***software***. The software receives information about the environment from ***sensors*** (temperature, wheel rotation rate, camera, radar, gyroscope, etc.) and acts on the physical environment through ***actuators*** (motors, pumps, valves, etc.). The software comprises a number of interacting control algorithms, many of them closed-loop, feedback algorithms. Some of these algorithms are based on self-learning (machine learning) e.g., the video pattern recognition.

Controlling cyber-physical systems by software carries some ***risks***: A failure, fault or error – either in the software or in the execution hardware platform – can have grave consequences, such as accidents, crashes, or casualties. In today's environment, also malicious interactions, such as hacking, malware, infiltration, etc. can inhibit the correct operation and also lead to dangerous consequences.

Developing software for cyber-physical systems is a demanding challenge. The engineering of trustworthy cyber-physical systems has become a sophisticated engineering discipline of its own. At the center of this discipline is the insight, that the ***quality of service properties*** (such as safety, security, availability, integrity, etc.) have higher priority than the functional requirements and must consistently be planned, designed and consequently implemented and maintained.

In this Hauptseminar, we focus on the two properties ***safety*** and ***security***.

Seminar Work

This seminar will work on the central theme: *How can we plan, design, implement and verify trustworthy cyber-physical systems*?

Each participant chooses one of the three fields:

F1: How can we plan, design, implement, and verify ***safety*** in a cyber-physical system?

F2: How can we plan, design, implement, and verify ***security*** in a cyber-physical system?

F3: Which are possible ***societal*** risks of untrustworthy cyber-physical systems?

The Hauptseminar has three seminar days (see separate work program, dates below):

- An introduction day: ***Engineering Trustworthy Cyber-Physical Systems*** will be introduced in a lecture by Professor Dr. Frank J. Furrer, and the parts of the Hauptseminar (Paper, presentation) will be defined;

- Then follows individual, guided research in the selected area and authoring of a scientific paper. Feedback from peer reviewers;
- A first seminar day: The participants will present their results and receive feedback from the audience;
- Improvement of the paper and the presentation, based on the peer feedback (Prof. Dr. F.J. Furrer will review and comment on all the papers);
- A second seminar day: The participants will present their improved results and receive feedback from the audience,
- Delivery of the final paper.

Learning Outcome

The participants will learn: (a) to do focused research in a specific area ("Engineering Trustworthy Cyber-Physical Systems"), (b) to author a scientific paper, (c) to improve their LATex expertise, (d) to experience the peer-review process and (e) to hold convincing presentations, and (f) to benefit from a considerable broadening of their perspective in the field of technology, software, and applications.

Seminar language is English. Three seminar days will be held and 3 ECTS credits are awarded for successful participation.

The audience is limited to 7 active participants. Please register in advance (jExam).

Mandatory Reading

(1) ***Introductory Text***:
Poul Heegaard, Erwin Schoitsch (Editors): *Combining Safety and Security Engineering for Trustworthy Cyber-Physical Systems*. ERCIM News, Nr. 102, July 2015. Free pdf-Donwload from: https://ercim-news.ercim.eu/en102/special/combining-safety-and-security-engineering-for-trustworthy-cyber-physical-systems [last accessed 6.1.2019]

(2) For the topic: ***Safety***:
The National Academies Press (NAP), Washington DC, 2012. TRB Special Report 308: *The Safety Challenge and Promise of Automotive Electronics*: Insights from Unintended Acceleration. ISBN 978-0-309-25297-3. Free pdf-Downlad from: https://www.nap.edu/catalog/13342/trb-special-report-308-the-safety-challenge-and-promise-of-automotive-electronics [last accessed 6.1.2019]

(3) For the topic ***Security***:
Bruce Schneier: **Click Here to Kill Everybody – *Security and Survival in a Hyper-connected World***. Norton & Company, USA, 2018. ISBN 978-0-393-60888-5. € 17.69 (www.amazon.de)

Seminar Schedule:

Kick-Off Meeting (Introduction): Wednesday, **April 17, 2019** / 11:10 – 12:40 in APB/INF 2101

Seminar Day 1: Wednesday, **June 19, 2019** / 09:20 – 10:50 & 11:10 – 12:40 in APB/INF 2101

Seminar Day 2: Wednesday, **July 10, 2019** / 09:20 – 10:50 & 11:10 – 12:40 in APB/INF 2101

More information can be found on the HS-Website:
https://st.inf.tu-dresden.de/teaching/hs