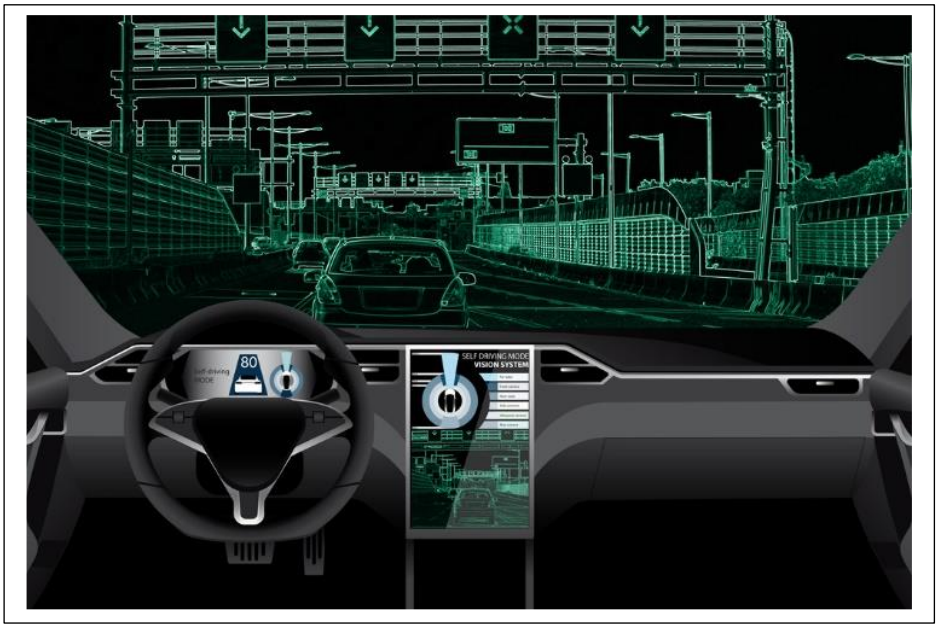
TECHNISCHE UNIVERSITÄT DRESDEN

HS SS-2022

Prof. Dr. Frank J. Furrer

Engineering Principles for Safety and Security of Cyber-Physical Systems



Summary

Cyber-physical systems are computer-controlled, networked systems that 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 the real-world environment, cyber-physical systems must be built so that they cannot harm or damage people, property, or the environment: Their behavior must be ***safe*** and ***secure***. Engineering safe and secure cyber-physical systems have become a specific, exciting, and essential 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, e.g., in the form of embedded computers controlling a combustion engine or as SCADA systems governing industrial plants. Today, computers controlling all sorts of cyber-physical systems are pervasive – we find them everywhere. They have taken over control from small devices like a heart pacemaker to large applications, such as an autonomous container ship.

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., an autonomous vehicle's video processing software.

Controlling cyber-physical systems by software carries some ***risks***: A failure, fault, error, or successful cyber-attack – 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 safe and secure 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.) must have higher priority than the functional requirements and must consistently be planned, designed, and consequently implemented and maintained.

This Hauptseminar focuses 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 safe and secure cyber-physical systems*?

Each participant chooses one of the two fields:

F1: Choose a documented ***safety accident*** involving a cyber-physical system (Note: Many such examples are documented on the Internet, e.g., search "`cyber-physical systems accident examples`");

F2: Choose a documented ***security incident*** involving a cyber-physical system (Note: Many such examples are documented on the Internet, e.g., search "`cyber-physical attacks 2020`");

The Hauptseminar has three seminar days:

- Hauptseminar Day 1: ***Engineering Principles for safe and secure Cyber-Physical Systems*** will be introduced in a lecture by Professor Dr.

Frank J. Furrer, and guidance for the paper and the presentation will be given;

- Then follows individual, guided research in the selected area **F1** or **F2** and authoring a scientific paper. Feedback from peer reviewers;
- Hauptseminar Day 2: 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);
- Hauptseminar Day 3: 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 Principles for Safety and Security of Cyber-Physical Systems"), (b) to author a scientific paper, (c) to experience the peer-review process, and (d) to hold convincing presentations, and (e) to benefit from a considerable broadening of their perspective in the field of technology, software, and applications.

The seminar language is English. Three seminar days will be held, and ***3 ECTS*** credits will be awarded for successful participation.

The audience is limited to 7 active participants. Please register in advance (jExam or directly to frank.j.furrer@bluewin.ch). **The closing date for registration is Monday, April 18, 2022.**

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-Download from: https://ercim-news.ercim.eu/en102/special/combining-safety-and-security-engineering-for-trustworthy-cyber-physical-systems [last accessed 16.03.2022]

(2) ***Safety and Security Principles***:

Frank J. Furrer: **Future-Proof Software-Systems – *A Sustainable Evolution Strategy***. Springer Vieweg Verlag, Wiesbaden, Germany, 2019. ISBN 978-3-658-19937-1

(3) 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-Download from: https://www.nap.edu/catalog/13342/trb-special-report-308-the-safety-challenge-and-promise-of-automotive-electronics [last accessed 16.03.2022]

(4) For the topic ***Security***:

Robert Radvanovsky, Jacob Brodsky: Handbook of SCADA/Control Systems Security. CRC Press (Taylor & Francis Group), Boca Raton, FL, USA. ISBN 978-1-4665-0227-7. Free pdf-Download from: http://www.icsdefender.ir/files/scadadefender-ir/books/ICS-SECURITY-NEW/Radvanovsky-%20Robert%20Handbook%20of%20SCADA_control%20systems%20security.pdf [last accessed 16.03.2022]

Seminar Schedule:

Hauptseminar Day 1 (Introduction): Friday, **April 22, 2022** / 09:20 – 10:50 in APB/INF 2101

Hauptseminar Day 2: Friday, **May 27, 2022** / 09:20 – 10:50 & 11:10 – 12:40 in APB/INF 2101

Hauptseminar Day 3: Friday, **July 1, 2022** / 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