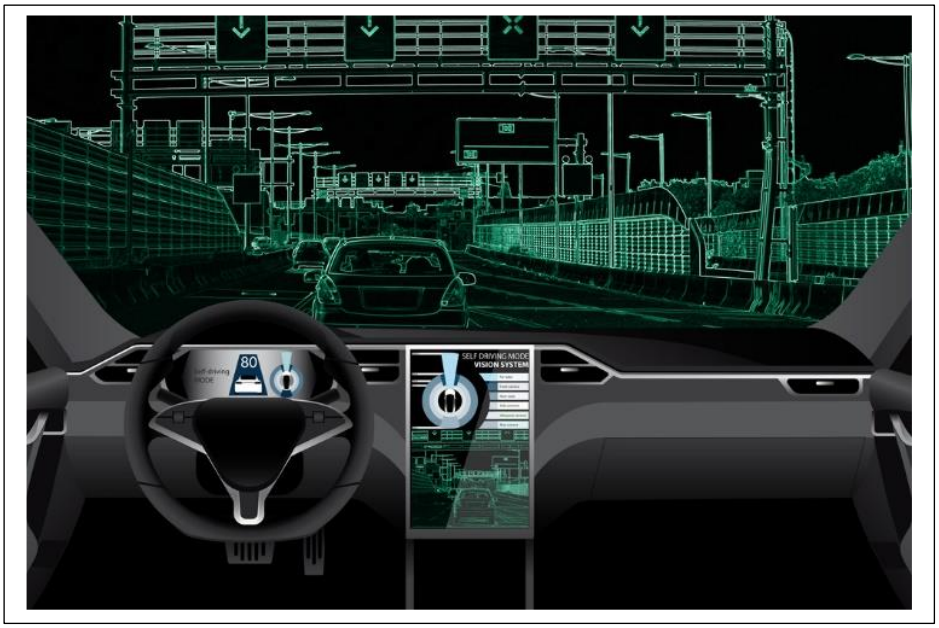
TECHNISCHE UNIVERSITÄT DRESDEN

Hauptseminar Sommersemester 2023

Prof. Dr. Frank J. Furrer (10.2.2023)

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, autopilot in an airplane, a heart pacemaker, cooperating robots in a manufacturing line, or a water control plant. 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 comprehensive entry.

Context

A long time ago, computers were merely 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 heart pacemakers to large applications, such as autonomous container ships.

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 malicious cyber-attack – either in the software or in the execution platform – can have grave consequences, such as accidents, crashes, or casualties. In today's environment, malicious interactions, such as hacking, malware infiltration, etc., can also inhibit the correct operation and 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. Proven ***engineering principles*** for the construction and operation of trustworthy cyber-physical systems are available and must be strictly respected.

This Hauptseminar focuses on the two central properties of cyber-physical systems: ***safety*** and ***security***.

Seminar Work

This seminar will work on the central theme: *Which safety or security principles have been violated in the chosen safety accidents or security incidents*?

Each participant chooses <u>one of the two</u> topics:

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 accidents"`);

<u>or:</u>

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 systems cyber-attacks"`);

The Hauptseminar has three seminar days:

- Hauptseminar Day 1: ***Safety and Security of 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 the draft of 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;
- Oral exam (on Day 3):

Learning Outcome

The participants will learn: (a) to do focused research in a specific area ("Analysis of a Safety Accident or a Security Incident 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 are:

- **Hauptseminar Day 1**: Monday, April 17, 2023: 09:20 – 10:50 (2. DS) /Room APB/INF 2101
- **Hauptseminar Day 2**: Monday, May 22, 2023: 09:20 – 10:50/11:10 - 12:40 (2. + 3. DS) /Room APB/INF 2101
- **Hauptseminar Day 3**: Monday, July 3, 2023: 09:20 – 10:50/11:10 - 12:40 (2. + 3. DS)/Room APB/INF 2101
- **Exams**: Monday, July 3, 2023: 15:00 – 17:00/Room APB/INF 2101 (Individual appointments).

3 ECTS credits will be awarded for successful participation. A grade will be assigned, which is averaged from the research paper, the oral presentation, and the final oral exam.

The audience is limited to 6 active participants. Please register in advance (jExam or directly to frank.j.furrer@bluewin.ch). The closing date for registration is Tuesday, April 11, 2023.

Mandatory Reading

Frank J. Furrer: **Safety and Security of Cyber-Physical Systems – *Engineering dependable Software using Principle-based Development***. Springer-Vieweg Verlag, Wiesbaden, Germany, 2022. ISBN 978-3-658-37181-4.

The book will be distributed to the participants free of charge. The electronic version is available for free from the TUD Campus network.

More information can be found on the HS-Website:

https://st.inf.tu-dresden.de/teaching/hs