TECHNISCHE UNIVERSITÄT DRESDEN

Hauptseminar SS-2021

Prof. Dr. Frank J. Furrer

© https://www.123rf.com/photo_115434623 Used with permission {28.12.2019}

Engineering Principles for Safety and Security for Cyber-Physical Systems

Summary

Cyber-physical systems are computer-controlled systems that interact with the physical environment, some of them autonomous. Typical examples include autonomous cars, an autopilot in an airplane, cooperating robots in a manufacturing line, or a heart-pacemaker.

Because of their impact on their real-world environment, ***safety*** and ***security*** are fundamentally essential properties of cyber-physical systems. Engineering safety and security for cyber-physical systems has become an engaging, relevant, and rich engineering discipline. This Hauptseminar elaborates on the ***engineering principles*** for safe and secure cyber-physical systems.

Context

A long time ago, computers were just processing data, such as keeping accounts or managing inventory. 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 of an autonomous vehicle.

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

Safety and security are based on proven ***engineering principles***. These engineering principles guide the development and operation of safe and secure cyber-physical systems ([4]). This Hauptseminar centers on the application of these principles.

Seminar Work

This seminar will work on the central theme: *Each participant chooses one safety accident or security incident of a cyber-physical system and elaborates, which safety or security principle was violated.*

The initial work activities are:

1. Read the mandatory literature (see below);
2. The Web contains many examples of accidents and incidents related to cyber-physical systems (Autonomous cars, plane electronics, heart-pacemakers, etc.). Choose one, understand, and document it. **Examples**:
    - Web search: "satellite cyber attacks"

- Web search: "pacemaker cyber attacks"
- Web search: "Tesla truck crash"
- Web search: "water treatment plant cyberattack"
- Web search: "scada cyber attack"
- Web search: "airplane hacking"
- Web search: "hacking cars"
- Web search: "GPS spoofing"
- Web search: "cyber-physical system cyberattack"
- Web search: "industrial plant cyber attack"
- Web search: "drone hacking"
- Web search: "traffic light hacking"
- Web search: "solarwind hack"
- Web search: "autonomous robot accicdents"
- etc.

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

- An introduction day: ***Engineering Safety and Security in 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 Safety and Security for Cyber-Physical Systems");

(b) To author a good scientific paper;

(c) To hold a convincing presentation;

(d) To experience the peer-review process;

(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 are awarded*** for successful participation (Equivalent to 2 SWS).

The audience is limited to 6 active participants. Please register in advance (jExam). Waiting List at: frank.j.furrer@bluewin.ch

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 6.1.2019]

(2) ***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 6.1.2019]

(3) ***Security***:
Sean Peisert, Jonathan Margulies, Himanshu Khurana, Chris Sawall: *Designed-in Security for Cyber-Physical Systems*. IEEE Computer and Reliability Societies, September/October 2014, p. 9-12. Free pdf-Download from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6924670 [last accessed 6.2.2020]

(4) ***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. [https://link.springer.com/book/10.1007%2F978-3-658-19938-8]
- Ajeet Singha, Anurag Jain: *Study of Cyber Attacks on Cyber-Physical Systems*. 3rd International Conference on Advances in Internet of Things and Connected Technologies, ICIoTCT 2018. Downloadable from: https://www.researchgate.net/publication/325330593_Study_of_Cyber_Attacks_on_Cyber-Physical_System/link/5da1665c92851c6b4bcda99c/download [Last accessed: 28.3.2021]

Seminar Schedule:

Kick-Off Meeting (Introduction): ~~Monday, **April 26, 2020**: 09:20 – 10:50 (2. DS)~~
>>>>>>> Replaced by ZOOM-Meeting (Invitation follows to participants)

Seminar Day 1: Monday, **May 31, 2020**: 09:20 – 10:50/11:10 - 12:40 (2. + 3. DS)

Seminar Day 2: Monday, **July 5, 2020**: 09:20 – 10:50/11:10 - 12:40 (2. + 3. DS)

Location: HSZ/108
(https://navigator.tu-dresden.de/etplan/hsz/01/raum/136101.0080)

Note: Due to Corona-restrictions a face-to-face Hauptseminar may not be possible and will be replaced by short ZOOM-meetings. Please check the Website for News.

More information (slides, etc.) can be found on the HS-Website:

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

For further inquiries, please contact:

Prof. Dr. Frank J. Furrer

frank.j.furrer@bluewin.ch

frank.furrer@mailbox.tu-dresden.de