Building Accountable Cyber-Physical Systems

Master's/Bachelor's Thesis

Supervisor: Prof. Dr. Alexander Pretschner
Advisor: Severin Kacianka
Email: {pretschn, kacianka}@in.tum.de
Phone: +49 (89) 289 - 17340
Starting date: immediately

Fakultät für Informatik
Lehrstuhl 4
Software & Systems Engineering
Prof. Dr. Alexander Pretschner

Boltzmannstraße 3
85748 Garching bei München

Tel: +49 (89) 289 - 17340
https://www4.in.tum.de

Context

Accountability is the property of a system that enables the uncovering of causes for events and helps to understand the responsibilities for these event. This is an essential step to analyze security and safety incidents, to improve systems in the future and also to resolve questions of responsibility and liability.

While there are many theories of accountability, we currently lack a unified view of accountability and it is unclear how to best realize it in real systems. At the chair of Software and Systems Engineering we are working on systematizing and formalizing notions of accountability and the associated reasoning. To aid in this endeavor, we are looking for students who have previous experience working on Cyber-Physical Systems such as robots, drones, cars or control systems. In their thesis we want to build upon that expertise to advance the scientific understanding of accountability in such systems.

Since this proposal is very broad, we ask interested students to contact Severin Kacianka (kacianka@in.tum.de) to tailor a proposal to their skills and specific interests.

Goal

The goal for a thesis in this context is to

1. Build (or ideally reuse) a Cyber-Physical Systems and a corresponding system model
2. Analyze the system's architecture
3. Extend the system to enable specific notions of accountability
4. Evaluate the system's accountability, characterize its limits and relate it to existing systems

Literature

[1] Kacianka et al. (2017) How accountability is implemented and understood in research tools. https://doi.org/10.1007/978-3-319-69926-4_15

[2] Doshi-Velez et al. (2017) Accountability of AI under the law: The role of explanation. https://arxiv.org/pdf/1711.01134.pdf

[3] Kacianka et al. (2016) Towards a unified model of accountability infrastructures. http://dx.doi.org/10.4204/EPTCS.224.5

[4] Rahman et al. (2016) Forensic-by-design framework for cyber-physical cloud systems. http://ieeexplore.ieee.org/abstract/document/7420536/

[5] Lindberg (2013) Mapping accountability: core concept and subtypes. http://journals.sagepub.com/doi/full/10.1177/0020852313477761