A Joint Venture of TÜV Austria and TU

Safety and Security in Industry Research Lab „SafeSecLab“

#SafeSecLab

PhD 8: Safety- and Security-Related Assessment Methods for Continuous Integration and Deployment (CI/CD)

This project is dedicated to the question of what effects the short-cycle software updates have on the direct interaction between man and machine and how it can be ensured that personal safety is guaranteed at all times. In the course of this, a prototype will also be developed that will provide the risk assessment and corresponding measures to ensure safe operation during short-cycle software updates in production.

Dipl.-Ing. Bernd Hader

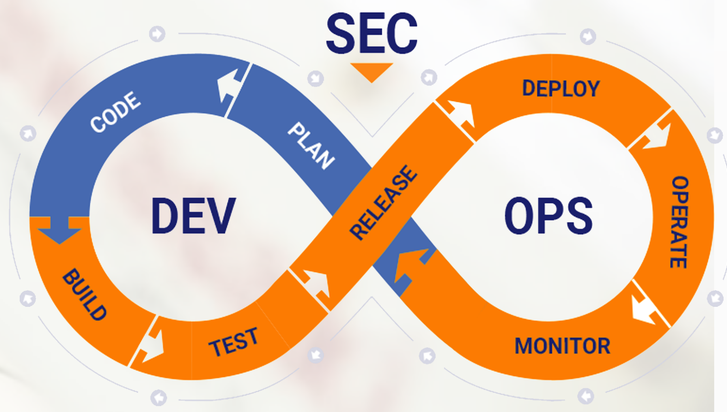
Education/Work Experience
- Business Informatics Studies
- 5 years experience as software developer

Interests
- Human-Machine-Interaction
- Software Engineering

Contact: bernd.hader@tuwien.ac.at

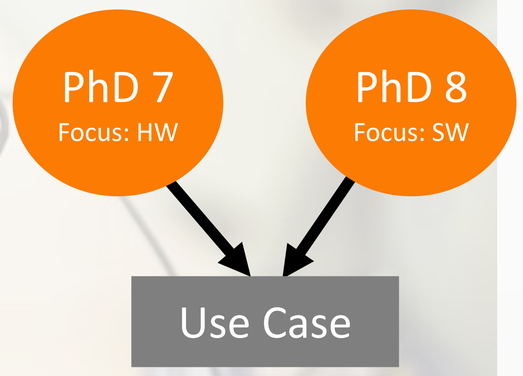
Motivation & Problem Statement

- Increasing interconnectivity in the industrial environment – Industry 4.0
- Frequent updates will be necessary in industry in the future [1, 2]
- Why? Vulnerabilites + New Functionalities [2, 3, 4]
- DevOps & DevSecOps enable short cycle-updates [5]
- Typically Safety & Security are considered separately
- DevSecOps focuses only on security[5], SafeScrum only on safety [6]



Source:[7] (modified)

HOW CAN THE SAFETY AND SECURITY OF SHORT-CYCLE SOFTWARE UPDATES OF HUMAN-MACHINE SYSTEMS BE ASSESSED AND ENSURED?



Expected Research Results

- Framework for Continuous Integration and Deployment (CI/CD) for safety-critical systems in manufacturing
- Inclusion of relevant safety & security standards
- Combination of safety & security (assessment) into whole lifecycle
- Proof of concept evaluation with real use case in pilot factory

Source:[7] (modified)

Picture by Michal Jarmoluk

[1] Edward A. Lee, “CPS foundations,” Proceedings of the 47th Design Automation Conference, 2010, pp. 737–742.
[2] Stamatis Karnouskos et al., “A SOA-based architecture for empowering future collaborative cloud-based industrial automation,” IECON 2012, 2012, pp. 5766–5772. isbn: 9781467324212. doi: 10.1109/IECON.2012.6389042.
[3] Moamar Sayed-Mouchaweh, “Diagnosability, security and safety of hybrid dynamic and cyber-physical systems,” Springer International Publishing, Mar. 2018, pp. 1– 327. isbn: 9783319749624. doi: 10.1007/978-3-319-74962-4.
[4] Vladimir Kutscher et al., “Upgrading of Legacy Systems to Cyber-Physical Systems,” Vol. 2020. 2020, pp. 11–15.
[5] Michelle Ribeiro, “Learning DevSecOps,” O’Reilly Media, Inc, 2022. isbn: 9781098106935.
[6] Geir Kjetil Hanssen et al.. SafeScrum® - Agile Development of Safety-Critical Software. Springer International Publishing AG, 2018.
[7] ThreatPost, „Apps Built Better: Why DevSecOps is Your Security Team’s Silver Bullet“, https://bit.ly/3Lp2hzO, visited 03-27-2022.

Supervisor: Sebastian Schlund (TU Wien)
Co-Supervisor: Wolfgang Kastner (TU Wien)
Contact person: Thomas Doms (TÜV)