BEAM

Brückenschlag von SW-Engineering, MLOps und operativen Agenten: Grundlagen für Agentic-AI in cyber-physischen Systemen

Programm / Ausschreibung	KS 24/26, KS 24/26, BRIDGE 2025/01	**Status**	laufend
Projektstart	01.04.2026	**Projektende**	31.03.2029
Zeitraum	2026 - 2029	**Projektlaufzeit**	36 Monate
Projektförderung	€ 357.332		
Keywords	Software-Engineering für Machine Learning, Software-Architektur, Agentic-AI-Architekturen, Software Engineering für cyber-physischen Systeme		

Projektbeschreibung

Cyber-physische Systeme (CPS) integrieren Kommunikation und Steuerung für die Echtzeit-Interaktion mit der physischen Welt und nutzen zunehmend verschiedene KI-Agenten für Aufgaben wie Optimierung und adaptive Steuerung. Die nahtlose Zusammenarbeit zwischen verschiedenen Arten von Agenten im Betrieb und denen, die in der Software (SW) Engineering von CPS verwendet werden, sowie die effektive Integration menschlicher Ziele bleiben jedoch offene Herausforderungen im CPS-Engineering und im Betrieb.

Dieses Projekt zielt darauf ab, ein integriertes Ökosystem zu schaffen, in dem teilweise autonome KI-Agenten sowohl die CPS-Entwicklung als auch den Betrieb unterstützen. Die Forschung befasst sich damit, wie die Zusammenarbeit von Agenten in den Bereichen Engineering und Betrieb eines CPS systematisch modelliert, beobachtet und verwaltet werden kann, wie verschiedene Agententypen und menschliche Stakeholder integriert werden können und wie eine effektive Spezifikation und Validierung menschlicher Absichten neben Mechanismen für kontinuierliches bidirektionales Feedback sichergestellt werden kann.

Dazu sollen die Zusammenarbeit zwischen Agenten und das Lebenszyklusmanagement, sowie Kollaborationsprotokolle, formalisiert werden, um die Integration von KI- und Nicht-KI-Agenten in MLOps/SW-Engineering-Workflows zu ermöglichen, menschliche Ziele in Agent-AI-Prozesse einzubetten und MLOps/ SW-Engineering mit CPS-Betriebsagenten zu integrieren. Neue Methoden und Agentic-AI-basierte Systemarchitektur-Konzepte sollen entworfen werden, um die Kollaboration von MLOps und SW-Engineering-Agenten im CPS-SW-Engineering deutlich zu verbessern. Dabei sollen neue Konzepte für proaktive SW-Engineering- und MLOps-Agenten entwickelt werden, die Entwickler oder Architekten beobachten und nahtlos in IDEs oder CI/CD-Pipelines integriert werden können. Darauf basierend sollen dann Konzepte für die Kollaboration der SW-Engineering- und MLOps-Agenten mit CPS-Betriebsagenten entworfen werden. Für beide Arten der Agentenkollaboration, sollen partizipatives Design und LLM-basierte Techniken zum Erfassen und Validieren menschlicher Ziele zum Einsatz

kommen. Prototypen werden in Open-Source- und industriellen CPS-Umgebungen empirisch validiert.

Durch die Überbrückung der Lücke zwischen CPS-Engineering und -Betrieb durch kollaborierende, teilweise autonome Agentenökosysteme geht dieses Projekt weit über die derzeitige toolzentrierte Automatisierung hinaus und liefert adaptives, stärker automatisiertes, nachvollziehbareres und menschenorientiertes CPS-SW-Engineering. Die neuartige Integration von kollaborativer Agentic-AI-Architekturen und -Konzepten, MLOps-Methoden, Softwarearchitekturkonzepten und Human-in-the-Loop-Methoden wird die Autonomie und Flexibilität von CPS der nächsten Generation erheblich verbessern.

Abstract

Cyber-physical systems (CPS) integrate communication and control for real-time interaction with the physical world and increasingly use various AI agents for tasks such as optimization and adaptive control. However, seamless collaboration between different types of agents in operation and those used in CPS software (SW) engineering, as well as the effective integration of human goals, remains an open challenge in CPS engineering and operation.

This project aims to create an integrated ecosystem in which partially autonomous AI agents support both CPS development and operation. The research addresses how agent collaboration in the engineering and operation of a CPS can be systematically modeled, observed, and managed, how different agent types and human stakeholders can be integrated, and how effective specification and validation of human intentions can be ensured alongside mechanisms for continuous bidirectional feedback.

To this end, collaboration between agents and lifecycle management, as well as collaboration protocols, will be formalized to enable the integration of AI and non-AI agents into MLOps/SW engineering workflows, embed human goals in Agentic AI processes, and integrate MLOps/SW engineering with CPS operational agents. New methods and Agentic AI-based system architecture concepts will be designed to significantly improve the collaboration of MLOps and SW engineering agents in CPS software engineering. New concepts for proactive SW engineering and MLOps agents will be developed that can observe developers or architects and be seamlessly integrated into IDEs or CI/CD pipelines. Based on this, concepts for the collaboration of SW engineering and MLOps agents with CPS operations agents will then be designed. For both types of agent collaboration, participatory design and LLM-based techniques for capturing and validating human goals will be used. Prototypes will be empirically validated in open-source and industrial CPS environments.

By bridging the gap between CPS engineering and operations through collaborative, partially autonomous agent ecosystems, this project goes far beyond current tool-centric automation and delivers adaptive, more automated, more traceable, and more human-centric CPS software engineering. The novel integration of collaborative Agentic AI architectures and concepts, MLOps methods, software architecture concepts, and human-in-the-loop methods will significantly improve the autonomy and flexibility of next-generation CPS.

Projektkoordinator

- Universität Wien

Projektpartner

- Siemens Aktiengesellschaft Österreich