FATE

Fault-based Analysis and TEsting for Design Robustness and Stability

Programm / Ausschreibung	IKT der Zukunft, IKT der Zukunft, IKT der Zukunft - 10. Ausschreibung (2021)	**Status**	laufend
Projektstart	01.11.2022	**Projektende**	31.10.2025
Zeitraum	2022 - 2025	**Projektlaufzeit**	36 Monate
Keywords	mixed signal design, verification, testing, human-centered design		

Projektbeschreibung

Moderne cyber-physische Systeme (engl. "cyber-physical systems“, CPS) mit leistungsfähigen Chipsätzen gewinnen an Relevanz in vielen Bereichen von Wirtschaft und Gesellschaft. Automobil- und Industrie Anwendungen, Smart Home und Smart Grid sind einige der Bereiche, in denen Systeme mit bisher unerreichter Komplexität benötigt werden. Solche Systeme sind zumeist sicherheitskritisch, und ihr Versagen kann zu teuren Sachschäden und sogar zur Bedrohung von Menschenleben führen. Die Korrektheit und Robustheit solcher Systeme muss auch bei kleinen Designabweichungen und Produktionsfehlern unbedingt gegeben sein.
Allerdings ist die Entwicklung sicherer und robuster cyber-phsyischer Systeme eine extrem herausfordernde Aufgabe. Erstens weisen diesee eine komplexe Dynamik auf, die schwer zu testen und zu analysieren ist. Zweitens sind bisher verfügbare Test-und Verifikationstools bekanntermaßen schwer zu handhaben und erfordern erhebliches Expertenwissen. Beide Probleme müssen bereits in den frühen Phasen des Design bis hin zur eigentlichen Produktion adressiert werden.
Das Projekt FATE (Fault-driven Analysis and Testing for Design Robustness and Stability) liefert einen menschzentrierten, fehlergetriebenen Ansatz für den Entwurf und die Analyse korrekter und robuster cyber-physischer Systeme, mit besonderem Schwerpunkt auf den Komponenten integrierter Schaltkreise. FATE greift Fortschritte der künstlichen Intelligenz und des maschinellen Lernens auf und entwickelt in Kombination mit etablierten Verifikationsmethoden aus dem Bereich der formalen Methoden und des Software-Engineerings einen Ansatz zur Prüfung der Korrektheit und Robustheit vom frühen Konzeptentwurf bis zur Produktionsphase. Das Projekt konzentriert sich hierbei auf zwei spezifische Aspekte: automatisierte Inferenz von Monitoren, die während des Konzeptentwurfs zwischen korrekten und fehlerhaften Systemen unterscheiden können, und intelligentes Testen zur Design-Space Exploration, um potenzielle Produktionsfehler zu erkennen.
Besonderes Augenmerk wird auf ein menschenzentriertes Design gelegt, indem eine effiziente Erkundung des Design Spaces ermöglicht wird, der für Benutzer mit unterschiedlichen Arbeitsrollen, Gestaltungsinteressen und Fachkenntnissen zugänglich ist. Ein wesentliches Merkmal dieses menschenzentrierten Visualisierungs- und Interaktionsansatzes ist die Verknüpfung von Reliability Displays mit den Systemeinschätzungen zu möglichen Produktionsfehlern. Durch die Angabe von Unschärfe und Zuverlässigkeit können die Benutzer ihr Vertrauen in die Systemempfehlungen und Verifizierungsergebnisse in jeder Entscheidungssituation kalibrieren.
Die Ergebnisse des Projekts FATE tragen zur Sicherheit und Robustheit von cyber-physischen Anwendungen bei. Weiters

wird dadurch eine erhebliche Verringerung von Feldrückläufern durch fehlerhaft ausgelieferte Chips erreicht. Die einfachere und vertrauensvollere Bedienung im Rahmen der Design Space Exploration und bei der Interpretation der Testergebnisse erhöht die Produktivität der Ingenieure, was zu einer höheren Produktqualität und einer Verringerung der Verifikations- und Testkosten führt. Somit fördert FATE die Wettbewerbsfähigkeit der österreichischen Halbleiterindustrie und unterstützt die Zielsetzungen des europäischen Chip-Gesetzes.

Abstract

Modern cyber-physical systems, with advanced chips at their core, play an ever-increasing role in our society. Automotive and industrial applications, smart homes and energy grids are few examples of systems that are reaching unprecedent levels of complexity. These systems are safety-critical, and their failure can result in expensive material damage and even loss of human lives. The system correctness and robustness to small design variations and production faults is hence of uttermost importance. However, developing safe and robust cyber-physical systems is an extremely challenging task. First, this class of systems have sophisticated dynamics that is hard to test and analyse. Second, existing verification tools and testing workflows are notoriously hard to use and require significant expert knowledge. Both problems must be tackled from the early stages of the concept design down to the actual design production.
FATE will provide a human-centred, fault-driven approach to the design and analysis of correct and robust cyber-physical systems, with a special focus on the integrated circuit components. By leveraging recent advances in artificial intelligence and machine learning, and in combination with well-established verification methodologies from formal methods and software engineering, the proposed approach will address the problem of testing correctness and robustness from the early concept design to the production phase. The project will focus on two specific aspects of this topic: automated inference of monitors that can distinguish between correct and faulty system during the concept design, and smart testing for the exploration of the design configuration space to detect potential production faults.
Special attention will be given to achieving human-centered design by properly calibrating the trust that the engineer has in her design, and by improving the experience of applying the resulting methods and tools, regardless of the educational background or gender of the user. The proposed approach will be instantiated on an industrial voltage regulator with special focus on the stability property.
The project results will contribute to the safety and robustness of cyber-physical applications and will significantly reduce the field returns in the semiconductor industry to faulty chips delivered to customers. The human-centric approach adopted in this project will facilitate its adoption and will increase the productivity of the engineers, resulting in higher product quality and a reduction of verification and testing costs. Together, these project impacts will have a positive effect on the competitivity of the Austrian semiconductor industry and will support the EU Chip Act vision.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- Infineon Technologies Austria AG
- Technische Universität Graz