X-by-Construction-Methoden für einen Pattern-basierten Entwurf zuverlässiger eingebetteter HW/SW-Systeme

Jürgen Becker und Tobias Dörr
Karlsruher Institut für Technologie – KIT

Abstract

Sicherheitskritische eingebettete Systeme, wie sie für das *Autonome Fahren* oder die *Urbane Luftmobilität* zum Einsatz kommen, unterliegen einer Vielzahl verschiedener Anforderungen. Durch die direkte Interaktion mit dem physikalischen Umfeld ist insbesondere die Einhaltung gesetzlicher und *normativer Sicherheitsvorgaben* nötig. Gleichzeitig sind Systeme dieser Art durch eine signifikante Anzahl externer Schnittstellen, einen verstärkten Einsatz von *Künstlicher Intelligenz (KI)*, den wachsenden Bedarf nach hochintegrierter Rechenleistung (eingebettetes *High-Performance Computing – eHPC*) sowie immer kürzere Hardware-/Softwareintegrationszyklen geprägt. In der Praxis bewährte Entwurfsmethoden decken diese Anforderungen häufig nur eingeschränkt ab. Eine explizit auf das Problemumfeld zugeschnittene Modellierungs- und Abbildungsmethodik, wie sie im Rahmen des EU-geförderten Forschungsprojekts „*XANDAR*“ erarbeitet wird, wirkt dieser Problematik durch eine ganzheitliche Systembetrachtung und einen hohen Automatisierungsgrad entgegen. Der im Projekt entwickelte Ansatz kombiniert die modellbasierte Beschreibung relevanter Anforderungen mit dem aus der Literatur bekannten *X-by-Construction*-Konzept. Ziel der *XANDAR*-Toolchain ist die automatische Erzeugung einer Systemimplementierung, die nicht nur funktional korrekt ist, sondern auch Garantien bezüglich der Erfüllung von *Safety-*, *Security-* und *Echtzeitanforderungen* umfasst. Ein konkreter Ansatz zur Komplexitäts- und Anforderungsbeherrschung ist dabei die auf einer parametrierbaren *Pattern-Bibliothek* basierende Generierung von *Safety-Mechanismen*. Patterns werden zielarchitekturspezifisch verifiziert und stehen dem Nutzer der *XANDAR*-Toolchain beim Systementwurf zur Verfügung. In diesem Vortrag werden zwei exemplarische Patterns aus der entwickelten Bibliothek vorgestellt:

(1) ein Ansatz zur modellbasierten *On-Chip-Isolation* auf heterogenen Mehrkernplattformen sowie

(2) eine automatisierte Methode zur *Laufzeitüberwachung von KI-Algorithmen*.

Anhand eines Anwendungsfalls (*Use-Case*) aus der *Urbanen Luftmobilität* wird die praktische Bedeutung der vorgestellten Methoden abschließend veranschaulicht und diskutiert.