

Praxis der Forschung

Reliability in by-Construction Engineering

Supervisor: Maximilian Kodetzki
maximilian.kodetzki@kit.edu

Summer term 25 / winter term 25/26

Correctness-by-Construction (CbC) ist ein bewährter Ansatz zur formalen Softwareentwicklung, bei dem Programme schrittweise durch Verfeinerung aus einer abstrakten Spezifikation abgeleitet werden. Die funktionale Korrektheit ergibt sich dabei direkt aus der Einhaltung streng definierter Verfeinerungsregeln. Dieser methodische Rahmen bietet eine hohe Sicherheit hinsichtlich der Übereinstimmung zwischen Spezifikation und Implementierung und findet insbesondere in sicherheitskritischen Bereichen Anwendung.

Allerdings beschränkt sich der klassische CbC-Ansatz primär auf funktionale Anforderungen. In modernen Softwaresystemen spielen jedoch nicht-funktionale Eigenschaften wie Verlässlichkeit, Sicherheit, Effizienz oder Performanz eine zunehmend zentrale Rolle. Verlässlichkeit – verstanden als die Fähigkeit eines Systems, erwartungsgemäß zu funktionieren, auch unter unvollständigen oder gestörten Bedingungen – ist insbesondere in sicherheitskritischen, medizinischen oder industriellen Anwendungen essenziell. Dennoch fehlt es in bestehenden CbC-Methoden an systematischen Mitteln, um solche Eigenschaften formell zu modellieren und im Entwicklungsprozess explizit zu berücksichtigen.

Ziel dieses Projekts ist es daher, die Verlässlichkeit als nicht-funktionale Eigenschaft in den Correctness-by-Construction-Ansatz zu integrieren. Dazu sollen zunächst formale Konzepte und Spezifikationsmechanismen entwickelt werden, um Verlässlichkeit auf abstrakter Ebene ausdrücken zu können. Darauf aufbauend werden Verfeinerungsregeln formuliert, die sicherstellen, dass Verlässlichkeitseigenschaften im Verlauf der Entwicklung bewahrt oder gezielt verstärkt werden können. Langfristig soll ein methodischer Rahmen entstehen, der es ermöglicht, funktionale und nicht-funktionale Anforderungen gleichermaßen präzise und formal fundiert zu behandeln. Dies trägt zur Entwicklung robuster, vertrauenswürdiger Software bei und stärkt die praktische Relevanz des CbC-Ansatzes in modernen Anwendungskontexten.