Automatisierte Assistenz bei der Entwicklung sicherheitskritischer Echtzeitsoftwaresysteme

Nils Berg

Bei der Entwicklung von sicherheitskritischen Softwaresystemen (z.B. nach IEC 61508 oder ISO 26262) sind zusätzlich zur regulären Entwurfs- und Entwicklungsarbeit weitere Arbeitsschritte notwendig, um den Anforderungen der Zertifizierungsprozesse zu genügen.

Ziel dieses Projekts soll sein, einen Teilbereich in diesem “overhead” zu identifizieren und (teilweise) zu automatisieren, um den Entwicklungsprozess einerseits zu beschleunigen, andererseits aber auch zuverlässiger zu machen, indem menschliche Fehler reduziert werden.

Dazu sollen die folgenden Schritte im Laufe der Projektzeit durchgeführt werden:

- Den State of the Art bei Entwurf und Entwicklung sicherheitskritischer Echtzeitsoftwaresysteme nach internationalen Standards begutachten
- Bereiche identifizieren, in denen Teile der Arbeit durch unterstützende Softwaresysteme bereits automatisiert werden, und solche, für die weitere Automation denkbar ist
- Abwägen, in welchem dieser Bereiche durch im Zeitrahmen des Projekts zu entwickelnde Assistenzsysteme der größte Nutzen erzielt werden kann
- Ein solches System entwerfen und implementieren, mit besonderem Augenmerk darauf, dessen korrekte Operation stichhaltig nachweisen zu können.

Parallel zu dem noch nicht näher definierten Assistenzsystem soll außerdem als Proof-of-Concept für dessen Wirksamkeit beispielhaft eine konkrete Echtzeitkomponente, nämlich eine Kinematik-Bibliothek zur Verwendung mit Roboterarmen, entwickelt werden. Diese soll mindestens ein Safety Integrity Level (SIL) von 2 erreichen.
Diese Bibliothek soll einerseits als Beispiel dienen, dass das Assistenzsystem seinen Zweck erfüllt, und andererseits als Fallstudie, um empirisch zu ermitteln wie viel Arbeit das System dem Entwickler in einem tatsächlichen Anwendungsfall abnimmt.

Die Hauptergebnisse des Projekts werden demzufolge sein:

- Zwei Softwarepakete - ein Helfersystem und eine Kinematik-Bibliothek, bei deren Entwicklung das Helfersystem genutzt wurde
- Nachweise, dass das Helfersystem seine Funktion korrekt ausführt
- Belege, dass die Kinematik-Bibliothek den Ansprüchen des angestrebten SIL genügt, bzw. - falls sie das nicht tut - wie sie verändert werden müsste, um sie zu erreichen
- Eine Analyse, wie viel Zeit (und welche Menge an menschlichen Fehlern) durch den Einsatz des Helfersystems eingespart wurde