Evaluierung von formalen Methoden in der Softwareentwicklung von kleinen und mittleren Unternehmen.

(Evaluation of formal methods in software development for small and medium enterprises)

Aufgrund steigender Komfortansprüche und sich ändernder gesetzlicher Rahmenbedingungen nimmt der Anteil von sicherheitskritischen Software Systemen im Automobil ständig zu. Die Industrie begegnet dieser steigenden Komplexität und der notwendigen Qualitätssicherung mit erhöhtem Aufwand im Bereich der Validierung und Verifikation von Software. In der aktuellen Norm für sicherheitskritische elektronische Systeme in Kraftfahrzeugen (ISO26262) wird neben den üblichen Softwaretests speziell auch die formale Verifikation von Software als Mittel zur Verifizierung genannt.

Um der gestiegenen Komplexität auch in kleinen und mittelständischen Unternehmen (KMUs) gerecht zu werden müssen hierbei speziell die geringeren Ressourcen im Vergleich zu Großunternehmen berücksichtigt werden. Fehler in der Software müssen früher gefunden werden ohne die Softwaretests auszuweiten. Der Aufwand von Tests und Verifikationen soll reduziert und im Gegensatz dazu die Qualität erhöht werden. Hierfür müssen die Entwicklungsprozesse entsprechend ausgelegt sein und auch formale Maßnahmen zur Sicherung der Softwarequalität unterstützen.

Um diesen Ansprüchen gerecht werden zu können, soll in dieser Arbeit der Einsatz von formalen Methoden im Software-Entwicklungsprozess von KMUs analysiert werden. Hierbei ist speziell auf die Anwendbarkeit der einzelnen Methoden mit Hinblick auf Nutzung von Computerressourcen zu achten. Nach der Recherche über den Einsatz von formalen Methoden in der Industrie soll speziell die Verwendung des Modell-Checkers Arcade untersucht werden. Hierbei sind neu eingesetzte Abstraktionstechniken zur Reduktion des Zustandsraumes am Beispiel einer Motorsteuerung zur Steuerung von Verbrennungsmotoren zu evaluieren. Weiterhin sollen neue Analysen der Software des Steuergerätes entwickelt werden, um unbekannte Fehler zu finden und bekannte Fehler in neuen Softwareversionen auszuschließen.

Zur Reduktion des Zustandsraumes und die damit einhergehende Reduktion der Rechenzeit können in Arcade Modelle der Umgebung genutzt werden. Um die Integration dieser Technik in den VEMAC Entwicklungsprozess zu überprüfen soll ein entsprechendes Modell aufgebaut und am Beispiel der Motorsteuerung evaluiert werden.

Abschließend sollen die entwickelten Konzepte und Methoden auf eine Plattform für den Einsatz von sicherheitskritischen elektronischen Systemen übertragen werden und am Beispiel einer Watchdog-Funktion überprüft werden. Alle Ergebnisse sind ausführlich und sorgfältig zu dokumentieren.