Dr.-Ing. Jörg Herter

ingenieur
wissenschaften
htw saar

Embedded Systems & Virtuelle Maschinen und Programmanalyse

Abschlussprojekt WiSe 21/22

1 Projektbeschreibung

Ziel des Projektes ist, in Teams einen Roboter (Lego Mindstorms) zu entwickeln, dessen Steuerungssoftware aktuellen Industrierichtlinien für sicherheitskritischen C-Code entspricht.

Ihre Roboterentwicklung soll typische Arbeitsprozesse der Entwicklung (sicherheitskritischer) eingebetteter System nachspielen. Besonderes Augenmerk wird hierbei auf Verifikations- und Validierungsphasen gelegt.

2 Roboterkonstruktion

Konstruieren Sie einen Ballkicker-Mindstorms wie weiter unten beschrieben.

3 Roboterprogrammierung

Implementieren Sie die Steuersoftware für Ihres Roboters. Befolgen Sie die MISRA C:2012-Kodierrichtlinien.

Testen Sie Ihren Roboter.

4 Verifikationsphase

Analysieren Sie Ihre Steuersoftware mit Astrée. Beginnen Sie Ihre Analysen bereits in der Entwicklungsphase.

Zeigen Sie mittels statischer Quellcodeanalyse, dass Sie MISRA-konform programmiert haben. Versuchen Sie für möglichst große Teile Ihres C-Codes die Abwesenheit von Laufzeitfehlern formal zu zeigen (bei Kombination mit VMPA).

5 Zusatzaufgabe VMPA

Ihnen steht zur Projektausführung mit Astrée ein Werkzeug zur Verfügung, das garantieren kann, keine *Fehler* der ihm bekannten Fehlerklassen in C-Code zu übersehen.

Finden Sie mit Astrée in den *"fehlerfreien"* Teilen des Juliet-Benchmarks (`https://samate.nist.gov/SRD/testsuites/juliet/Juliet_Test_Suite_v1.3_for_C_Cpp.zip`) oder des ITC-Benchmarks (`https://samate.nist.gov/SARD/view.php?tsID=104`) unbeabsichtigte und ggf. seit Jahren unentdeckten Fehler. Injizieren Sie die gleichen Fehler in Ihre Robotersteuerung und wiederholen Sie mit dem modifizierten Steuercode Ihre Verifikationsphase. Zeigen Sie, dass dieser Fehler in Ihrer Verifikationsphase gefunden wird.

6 Abgabe und Projektpräsentation

Abgabe- und Präsentationstermin ist der 31.03.2021.

- Demonstration der Funktionsweise des Roboters
- Präsentation Steuerungssoftware und Analyseergebnisse
- Detaillierte Präsentation und Diskussion der Analyseergebnisse (bei Kombination mit VMPA)
- Fragen und Diskussionen

7 Anhang

7.1 Ballkicker

Ballkicker ist ein einfaches Zweipersonenspiel bzw. Zweiroboterspiel, bei dem es darum geht, nach einem festen Regelwerk Bälle von einem Tisch zu entfernen und bei dem der Spieler oder Roboter gewinnt, der den letzten Ball vom Tisch kickt.

Regelwerk Beide Spieler entfernen abwechselnd Bälle vom Tisch, nach den folgenden Regeln:

- ist die Anzahl der noch auf dem Tisch befindlichen Bällen eine Primzahl, darf der Spieler einen oder zwei Bälle vom Tisch stoßen,
- ansonsten muss genau ein (1) Ball vom Tisch entfernt werden.

Sobald der Roboter am Zug ist (unabhängig davon, wer zuerst anfängt) wird dieser aktiviert. In jeder Runde soll der Roboter dann die Anzahl der Bälle bestimmen, die vorberechnete Anzahl an Bällen vom Tisch stoßen, auf seine Startposition zurückkehren und ein Ende der Runde signalisieren.

Das Spielfeld, das Aussehen, sowie die genaue Funktionsweise des Roboters ist frei wählbar.

Zum Zählen der Bälle kann der Infrarotsensors verwendet werden. Hierzu muss der Roboter eine bestimmte Strecke abfahren und die Anzahl der Objekte bzw. der Lücken zählen. Rundenende sowie Sieg/Niederlage des Roboters kann mittels der Soundausgabe signalisiert werden.

Die vorberechnete optimale Strategie kann fest in die Ablaufsteuerung des Roboters einprogrammiert werden.