Zusammenfassung

Im BMBF-Projekt *SAMS* wurde ein nach DIN EN 61508 (SIL 3) zertifiziertes Programm zur Berechnung von Schutzfeldern in Abhängigkeit von Geschwindigkeit und Lenkwinkel entwickelt. Es dient zur Kollisionsvermeidung für Serviceroboter und fahrerlose Transportsysteme (FTS). Kern der Zertifizierung ist dabei die formale mathematische Modellierung und der Korrektheitsbeweis der Implementierung mit dem computergestützten Theorembeweiser Isabelle, flankiert durch zusätzliche Tests.

Die entwickelten Techniken zur Verifikation algorithmisch orientierter Programme sind generisch und werden in Zukunft bei der Zertifizierung weiterer Systeme eingesetzt.

Eine Generalisierung des entwickelten Verfahrens auf drei Dimensionen ermöglicht den Einsatz zur Kollisionsvermeidung von Roboterarmen (Patent eingereicht).

Projektpartner

Deutsches Forschungszentrum für Künstliche Intelligenz GmbH

Leuze electronic

Universität Bremen

Förderung

Bundesministerium für Bildung und Forschung

Kontakt

PD Dr. Christoph Lüth
Forschungsgruppe Sichere Kognitive Systeme
Enrique-Schmidt-Straße 5, Cartesium
D-28359 Bremen

E-Mail: christoph.lueth@dfki.de
Web: http://www.sams-projekt.de/

Deutsches Forschungszentrum für Künstliche Intelligenz GmbH
Sichere Kognitive Systeme

Der Fokus der Arbeiten des Bereichs *Sichere Kognitive Systeme* des *Deutschen Forschungszentrums für Künstliche Intelligenz* in Bremen ist die Entwicklung sicherer und kognitiv adäquater technischer Systeme.

Im Auftrag der Industrie und in öffentlichen Forschungsprojekten entwickeln, begutachten und verifizieren wir insbesondere Algorithmen zur Auswertung von Sensordaten für sicherheitsrelevante Zwecke.

Sprechen Sie uns an!

Direktor:
Prof. Dr. Bernd Krieg-Brückner

Kontakt:
Deutsches Forschungszentrum für
Künstliche Intelligenz
Forschungsbereich Sichere Kognitive Systeme
Enrique-Schmidt-Straße 5, Cartesium
D-28359 Bremen

E-Mail: sks-info@dfki.de
Tel: +49 (0)421 218-64 221
Fax: +49 (0)421 218-98 64 221

Weitere Informationen:
http://www.dfki.de/sks

Deutsches Forschungszentrum für Künstliche Intelligenz GmbH
Sichere Kognitive Systeme

SAMS

Sicherungskomponente für Autonome Mobile Serviceroboter

Sicherheit für Serviceroboter

Mobile Serviceroboter
Sicherheitsproblematik

TÜV-Zulassung
Maschinenrichtlinie
DIN EN 61508

SAMS

Garantierte Sicherheit
Softwareverifikation

Sicherheit vor Kollisionen zu gewährleisten ist eine gesetzliche Voraussetzung für die Zulassung jedes Serviceroboters. Die Erlangung eines von der Maschinenrichtlinie geforderten Konformitätsnachweises macht in der Praxis eine Entwicklung gemäß einschlägiger Sicherheitsnormen, wie der hier zur Anwendung kommenden DIN EN 61508, erforderlich.

Im Projekt *SAMS* wurde ein Sicherungsalgorithmus für mobile Roboter entworfen, implementiert, und die SIL 3-Konformität über den TÜV Süd nachgewiesen. Die Implementierung darf daher in einem Sicherheitsgerät eingesetzt werden.

Dynamische Schutzfelder

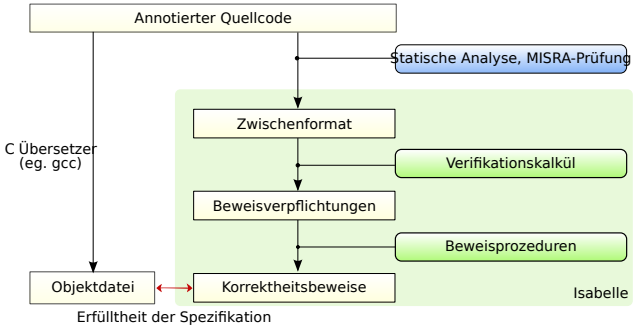
Bei industriell eingesetzten fahrerlosen Transportsystemen (FTS) überwacht ein Laserscanner als zugelassenes Sicherheitsbauteil ein Schutzfeld um das Fahrzeug und stoppt es, sobald sich ein Hindernis im Schutzfeld befindet. Die mangelnde Flexibilität und die begrenzte Anzahl solch handkonfigurierter Schutzfelder schränken Bahnführung und Geschwindigkeit unnötig ein.

Im Projekt *SAMS* wird das Schutzfeld abhängig von der Geschwindigkeit, einer eventuell möglichen Kurvenfahrt und dem Fahrzeugzustand (Beladungszustand, Bauteileverschleiß usw.) in Echtzeit berechnet. Durch dieses *dynamische Schutzfeld* wird dann so spät wie möglich, aber so früh wie nötig gebremst, was eine effektivere Bahnführung erlaubt.

Die Konfiguration des Bremsverhaltens erfolgt unkompliziert mit einer einfachen Messung des Bremsweges bei Geradeausfahrt.

Formale Verifikation

Kernbeitrag von *SAMS* ist der Nachweis der Korrektheit der Implementierung des Schutzfeldberechnungsalgorithmus und, darauf basierend, eine Zertifizierung durch den TÜV Süd nach EN 61508, SIL 3. Die formale Spezifikation der Software erfolgt über Korrektheitsannotationen, die direkt an den Programmcode angefügt werden.



Die Erfülltheit der Spezifikation wird mathematisch exakt mithilfe eines im computergestützten Beweiswerkzeug Isabelle entwickelten Verifikationskalküls nachgewiesen. Ein syntaktisches Analyseprogramm überprüft die Einhaltung von Programmierrichtlinien (insbesondere des MISRA Standards) und übersetzt den Quellcode in ein Zwischenformat. Mit dem Verifikationskalkül werden hieraus Beweisverpflichtungen errechnet, von denen ein Großteil — wie z. B. die korrekte Verwendung von Zeigervariablen oder die konservative Abschätzung von Seiteneffekten der Programmfunktionen — durch automatische Prozeduren bewiesen werden kann. Darüber hinausgehende Beweisverpflichtungen, vor allem geometrischer Art, werden interaktiv von Domänenexperten in Isabelle bewiesen. Durch die durchgängig formale Verifikation kann ein Höchstmaß an Zuverlässigkeit erzielt werden. Dies ermöglicht, auch anspruchsvolle Algorithmen erfolgreich zu verifizieren und damit zu zertifizieren.

SAMS 3D

Wir haben die 2D-Schutzfeldberechnung zu einem patentierten 3D-Verfahren generalisiert, z. B. für Roboterarme. Es berechnet in Echtzeit den Raum, den die verschiedenen Teile des Roboters beim Bremsen überstreichen. Das Ergebnis wird auf mögliche Kollisionen geprüft.

Das Anwendungsbeispiel zeigt den Roboter Justin des DLR beim „zusammenklatschen“ der Hände. Die berechneten Schutzfelder sind grün überlagert.