Chancen und Herausforderungen des Einsatzes von Remote-Laboren in der Lehre: Sicherheitskonzepte

Georg Jäger[1], Sebastian Zug[1], Anja Hawlitschek[2], Till Krenz[3], Ronny Stolze[4] und Nancy Brinkmann[4]

Abstract: Mit dem unmittelbaren Zugriff auf ein reales Laborexperiment bieten Remote-Labore erhebliche Chancen, aber auch technische Risiken. Das Paper erörtert die Gefahrenpotentiale zweier Szenarien und zeigt Detektionsmöglichkeiten auf.

Keywords: Remote-Labore, Interdisziplinarität, Sicherheit Architektur

1 Identifikation von Sicherheitsrisiken

Basis für die Analyse ist das Projekt Industrial-eLab[5], das darauf abzielt, einheitliche Konzepte für die Umsetzung von Remote-Ansätzen in unterschiedlichen Domänen zu entwickeln. Den Rahmen dafür bildete auf Seiten der Otto-von-Guericke Universität die Ausbildung im Bereich der Mikrocontrollerprogrammierung (Robotik) und für die Hochschule Magdeburg-Stendal die Variation von Stellgrößen beim Drehprozess (Fertigungstechnik). Für beide Szenarien wurde im Rahmen des Projektes sowie durch Erfahrungen im Einsatz in der Lehre, ein Katalog von Gefährdungen abgeleitet. Die Tabellen 1a und 1b fassen diese zusammen und assoziieren mögliche Konsequenzen.

2 Sicherheitsmethoden

Für diese Aufstellung untersucht Abbildung 1 die Anwendbarkeit unterschiedlicher Detektionsstrategien. So eröffnet die automatisierte Codeanalyse die Möglichkeit sowohl statische Fehlermuster (fehlende Funktionsaufrufe, falsche Parameter) innerhalb des Quellcodes zu erkennen, als auch durch eine Simulation fehlerhaftes Verhalten in Abhängigkeit von externen Anregungen zu prädizieren. Monitoring-Konzepte hingegen

[1] Otto-von-Guericke Universität (OVGU), Institut für Intelligente Kooperierende Systeme, Universitätsplatz 2, 39106 Magdeburg, {gjaeger|zug}@ovgu.de
[2] Hochschule Magdeburg-Stendal, Zentrum für Hochschuldidaktik und angewandte Hochschulforschung, Breitscheidstraße 2, 39114 Magdeburg, anja.hawlitschek@hs-magdeburg.de
[3] Otto-von-Guericke-Universität Magdeburg, FHW, Zschokkestr. 32, 39104 Magdeburg, till.krenz@ovgu.de
[4] Hochschule Magdeburg-Stendal, Institut für Maschinenbau, Breitscheidstraße 2, 39114 Magdeburg, {vorname.nachname}@hs-magdeburg.de
[5] Die Förderung erfolgt durch das BMBF im Programm "Forschung zur digitalen Hochschulbildung", siehe Projektwebseite http://www.elab.ovgu.de

	Fehler	Sicherheitsrisiko
A1	Unerlaubtes Aktivieren von Komponenten	Unkontrollierte Bewegungen
A2	Falsche Input/Output Konfiguration	Elektrische Beschädigung des Controllers
A3	Falsche Konfiguration der Motoren	Beschädigung der Motoren
A4	Bewegungsmuster mit hohen Beschleunigungen	Mechanische Beschädigung des Roboters
A5	Permanente Kreisbewegungen	Abreißen der Verbindung
A6	Kollisionen mit der Bande	Beschädigung der Sensoren

(a) Embedded-Lab

	Fehler	Sicherheitsrisiko
B1	Unerlaubte Verfahrbewegungen der Werkzeugmaschine	Beschädigung der Werkzeugmaschine / Personenschaden
B2	Falsche Maschinen- / Prozessparameter	Beschädigung der Werkzeugmaschine und deren Komponenten
B3	Falsches Werkzeug	Beschädigung des Werkzeuges / Werkstückes
B4	Spannfehler im Gesamtsystem	Beschädigung der Werkzeugmaschine
B5	Fremdeingriff in Maschinenraum	Personenschaden

(b) Maschinen-Lab

Tab. 1: Mögliche Sicherheitsrelevante Fehler in den Szenarien des eLab Projektes

evaluieren die Korrektheit zur Laufzeit im System. Dies kann entweder durch zusätzliche Funktionalität in Software oder aber interner bzw. externer Hardware erfolgen.

	Identifikationsmethode				
	Codeanalyse		System-Monitoring		
			integriert		
	unmittelbar	simulativ	Software	Hardware	extern
Embedded-Lab	Code check, Mustersuche A1,A2,A3	μC Simulation A1,A2,A3,A5	Wrapper, Dekoratoren A4	zusätzliche Controller A1,A3,A4,A6	Kameras an der Arena A1,A4,A5,A6
Maschinen-Lab	Abgleich Parameter B1, B2, B3	G-Code Simulation B2	Prüffunktionen B2, B3	Kraftsensor B1, B2, B3, B4	Kameras an der Maschine B1, B5

Abb. 1: Potentielle Elemente einer Sicherheitsarchitektur für Remote-Labore und deren Anwendung

3 Bewertung und zukünftige Arbeiten

Die Gegenüberstellung verdeutlicht, dass einige Fehler mit mehreren Strategien detektierbar sind (A1, B2), während andere individuelle Ansätze erfordern (A5, B5). Weiterhin lässt sich ableiten, dass bspw. für das Embedded-Lab auf die simulative Codeanalyse verzichtet werden kann, sofern externe Kameras zum Einsatz kommen.

Im Weiteren sollen diese Erkenntnisse in einer modularen Sicherheitsarchitektur mit übertragbaren Teillösungen für die genannten Projekte und allgemeinen, technischen Remote-Ansätzen münden.