SIListra Systems Pressemitteilung / Dresden, den 15. Juli 2019

[Headline] Diversified Encoding - eine anerkannte Diagnosemethode zur Erkennung von Hardware-Ausführungsfehlern

[Subheadline] Anwendung für sicherheitskritische Softwareentwicklung

[Teaser]Vorspann/Einleitung

Diversified Encoding ist eine Diagnosemethode, um Hardware-Ausführungsfehler in sicherheitskritischen Systemen zu erkennen, damit sie rechtzeitig behandelt werden. Das besondere an dieser Diagnosemethode ist, ihre geringen Anforderungen an die zugrunde liegende Hardware in Bezug auf detaillierte Hardware-Fehleranalyse und Selbsttests von Hardware-Fehlermodi. Während etablierte Lösungen oftmals mit zusätzlicher oder spezieller Hardware umgesetzt werden - beispielsweise komplett 2-kanaliger Hardware oder LockStep-CPUs - kann Diversified Encoding auf **C**ommercial **O**ff-**T**he-**S**helf -Hardware angewendet werden. Damit ist diese Methode für alle sicherheitskritischen Projekte interessant, bei denen die Hardware-Fehler-Diagnose nicht in Hardware umgesetzt werden soll oder kann. Im ersten Halbjahr 2019 wurde die SIListra-Methode Diversified Encoding von **TÜV SÜD Rail** erfolgreich in sicherheitsrelevanten Projekten überprüft.

[Mittelteil]Details

Im Kern setzt Diversified Encoding auf das Coded Processing Verfahren. Coded Processing erkennt Fehler im Datenfluss von Programmen durch Informationsredundanz. Diversified Encoding setzt auf zwei logische Software-Kanäle. Die 2-Kanaligkeit ist komplett in Software umgesetzt und stellt keine besonderen Anforderungen an die zu Grunde liegende Hardware. Der „native Kanal“ ist die originale Sicherheitsfunktion, wie sie vom Entwickler programmiert wurde. Der „kodierte Kanal“ ist die originale Sicherheitsfunktion mit Coded Processing. Durch Coded Processing ist der kodierte Kanal bereits alleine fehlererkennend. In Kombination mit dem nativen Kanal erhöht sich die Fehlererkennungswahrscheinlichkeit weiter über die Erkennungswahrscheinlichkeit des kodierten Kanals hinaus. Das Diversified Encoding Framework bringt beide Kanäle zusammen: Es verteilt die sicheren Eingaben an beide Kanäle und kombiniert die Ausgaben beider Kanäle zu sicheren Ausgaben. Typischer Weise sind Netzwerkstacks für sicherheitskritische Nachrichtenprotokolle Teil der beiden Kanäle, um die Eingaben zu überprüfen und sichere Ausgaben zu erzeugen. Darüber hinaus enthält der kodierten Kanal noch eine feingranulare, patentierte Kontrollflussüberwachung. Die Kontrollflussüberwachung prüft jede Kontrollflussanweisung zur Laufzeit und ist mit Coded Processing integriert.

Die TÜV SÜD Rail GmbH hat in Rahmen einer Konzeptprüfung die Diversified Encoding Methode von SIListra Systems GmbH erfolgreich geprüft. Ziel der Prüfung war eine Anwendung von Diversified Encoding im Kontext der IEC 61508 (bis SIL3). Neben der eigentlichen Methode hat der TÜV SÜD auch die von der SIListra Systems GmbH verwendete Variante von Coded Processing, die Kontrollflussüberwachung und die vom Verfahren erreichten Aufdeckungswahrscheinlichenkeiten bewertet. Die erfolgreiche Prüfung ermöglicht den Einsatz von Diversified Encoding von SIListra Systems GmbH in Projekten nach der Norm IEC 61508 (bis SIL3) und verwandten Anwendungsbereichen, beispielsweise im Automatisierungsumfeld.

Bild: SIListra Systems GmbH

Über SIListra Systems:

Die SIListra Systems GmbH ist ein innovatives IT-Unternehmen, das 2012 aus der TU Dresden ausgegründet wurde. Bereits vor der Gründung arbeiteten unsere Mitarbeiter an speziellen Software-Verfahren und deren Umsetzung in Entwicklungswerkzeuge für den Einsatz auf dem Gebiet der funktionalen Sicherheit. Mit dem Einstieg des Mehrheitsgesellschafters TraceTronic GmbH im Jahr 2016 wird die Markteinführung serientauglicher SIListra-Lösungen vorangetrieben. Mehr Informationen zu Unternehmen und Lösungen sind verfügbar unter silistra-systems.com.

SIListra Systems-Kontakt:

Jens Schindler, Geschäftsführer

SIListra Systems GmbH
Königsbrücker Str. 124
01099 DRESDEN - GERMANY

Phone: +49 351 418 909 34
Fax: +49 351 418 909 36
E-mail: jens.schindler@silistra-systems.com