

Safety-Steuerungen auf Standard-Hardware für hochpräzise Anwendungen mit Fließkommaberechnungen

SIListra Systems präsentiert Technologie-Weltneuheit für die Entwicklung von Sicherheitslösungen auf nicht-sicherer Standard-Hardware zur SPS 2025 in Halle 7 auf Stand 677

Kurzfassung

Mit dem *SIListra Safety Transformer 3.0.0* setzt die SIListra Systems GmbH aus Dresden einen neuen Standard in der funktionalen Sicherheit: Erstmals ermöglicht die Lösung die direkte Nutzung von Fließkommaarithmetik (`float`, `double`, IEEE 754) mit Coded Processing – ohne aufwändige Emulation. Damit wird die Entwicklung hochkomplexer und gleichzeitig effizienter Safety-Steuerungen auf Standard-Hardware Realität. Darüber hinaus wird erstmalig mit der neuen Version der Aufbau von modularen Architekturen möglich, da sich Softwarekomponenten unabhängig absichern und flexibel zu neuen Anwendungen kombinieren lassen. Zusammen mit der optionalen *SIListra Safety Math Library* für performante mathematische Funktionen bietet der SIListra Safety Transformer Kunden entscheidende Wettbewerbsvorteile bei der Realisierung skalierbarer und zuverlässiger Lösungen entwickelt u.a. nach IEC 61508 – von Robotik über industrielle Automatisierung und Prozesssteuerungen bis hin zu Sensorfusionsanwendungen.

Langfassung

Systementwickler in den Bereichen industrielle Automatisierung, Robotik und Sensortechnik müssen immer mehr Anforderungen an die funktionale Sicherheit (Safety) erfüllen. Zufällige Fehler müssen von der Systemlösung sicher diagnostiziert und behandelt werden (u.a. Bit-Flips bei Berechnungen in Hardware oder bei der Speicherung und Übertragung von Daten).

Für die Diagnose von zufälligen Fehlern gibt es zwei in der Praxis bewährte Methoden: Hardware-Redundanz und Coded Processing. Bei Hardware-Redundanz wird die Hardware doppelt in zwei Kanälen ausgelegt. Diese beiden Kanäle vergleichen Zwischenergebnisse und Ausgaben, um zufällige Fehler aufzudecken. Zweikanalige Hardware, die einen Kreuzvergleich ermöglicht, muss speziell entworfen werden, was die Komplexität sowie Entwicklungskosten im Vergleich zu Standard-Hardware deutlich erhöht.

Im Gegensatz dazu ermöglicht Coded Processing die Ausführung von Sicherheitsanwendungen auf Standard-Hardware (Commercial-off-the-shelf, COTS). Bei Coded Processing wird die Redundanz in Software umgesetzt. Erstens werden durch die Kodierung die zwei Software-Kanäle unterschiedlich umgesetzt, so dass ein gemeinsamer Fehler die Kanäle unterschiedlich verfälscht. Damit können Fehler durch Vergleich der Ausgaben der Kanäle aufgedeckt werden. Zweitens ist die Kodierung in der Lage, schon in einem einzelnen Software-Kanal, Fehler aufgrund von Informationsredundanz aufzudecken.

Die bisherigen Coded Processing Lösungen können üblicherweise nur mit Ganzzahlarithmetik umgehen. Anwendungen, die Fließkommaarithmetik benötigten, waren nur mit aufwändiger

Softwareemulation umsetzbar. Erstmals stellt SIListra Systems eine direkte Unterstützung für Fließkommaarithmetik durch Coded Processing vor. Die aufwändige Emulation in Software von Fließkommaarithmetik mittels Ganzzahlarithmetik wird dadurch obsolet.

Die neue Version 3.0.0 des Entwicklungswerkzeuges *SIListra Safety Transformer* unterstützt die gängigen Fließkommadatentypen `float` (32-bit) und `double` (64-bit) und alle Berechnungen nach IEEE 754 in C und C++, die mit diesen Datentypen möglich sind. Die neue, optionale Erweiterung *SIListra Safety Math Library* stellt darauf aufbauend performante und sichere Implementierungen für mathematische Funktionen (beispielsweise Trigonometrie) mit definierter Genauigkeit zur Verfügung. Die Lösung setzt lediglich eine IEEE 754 konforme Hardware voraus, welche jeder CPU-Hersteller seit Jahren bietet.

Eine weitere Charakteristik von komplexen Sicherheitsanwendungen ist ihre Modularität: eine Sicherheitsanwendung besteht aus mehreren getrennt voneinander entwickelten Softwarekomponenten. Mit dem SIListra Safety Transformer 3.0.0 können Anwender einzelne Komponenten unabhängig voneinander mit Coded Processing absichern. Damit können mit dem neuen SIListra Safety Transformer verifizierte Softwarekomponenten leicht zu neuen Anwendungen kombiniert werden.

Für Partner und Kunden, die auf SIListra Systems Tools und die zugehörigen Produkt- bzw. Serviceangebote setzen, ergeben sich erhebliche Wettbewerbsvorteile. Speziell die Realisierung neuer modularer, skalierbarer und effizienter Safety-Steuerungen für höchst komplexe Anwendungen, wie beispielsweise Objekt- und Personenerkennung und Bahnberechnung in der Robotik, wird dadurch ermöglicht. Derartig bewährte Implementierungen werden nunmehr vom SIListra Safety Transformer unterstützt und können somit mit Coded Processing abgesichert werden.

Die Grundlagen für diese neue Produktlösung wurden im Rahmen des ZIM-Projektes SafeFloat gemeinsam mit dem Institut für Steuerungstechnik der Werkzeugmaschinen und Fertigungseinrichtungen (ISW) an der Universität Stuttgart im Zeitraum 01.01.2023 bis 30.06.2025 entwickelt. Das ZIM-Projekt wurde vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) aufgrund eines Beschlusses des Deutschen Bundestages gefördert.



Bild 1: Der SIListra Safety Transformer 3.0.0 unterstützt erstmals Fließkommaarithmetik und ist damit u.a. bestens geeignet zur Absicherung von Robotersteuerungen.

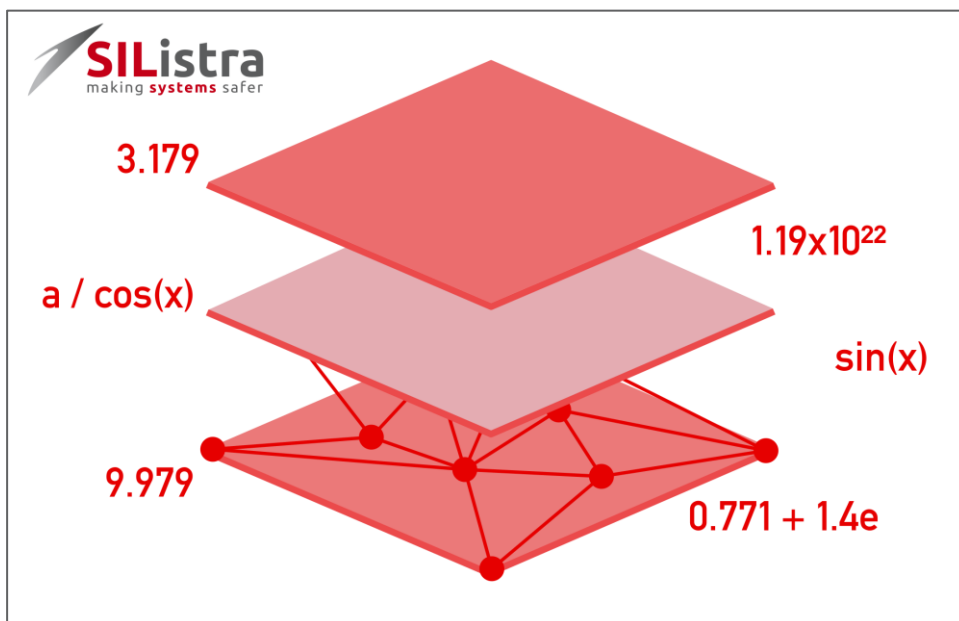


Bild 2: Die SIListra Safety Math Library bringt performante und genaue Unterstützung für die wichtigsten mathematischen Funktionen mit.

Über SIListra Systems:

Die SIListra Systems GmbH ist ein hoch spezialisiertes Technologieunternehmen, das 2012 aus der TU Dresden ausgegründet wurde. Mit den software-basierten Lösungen der Firma können sicherheitskritische Anwendungen auf Standard-Hardware realisiert werden. Automatisierungs-, Robotik- und Sensor-Hersteller in Deutschland, Österreich, Frankreich und Italien nutzen die Technologien und Softwaretools von SIListra Systems. Mehr Informationen zur Firma, dem TÜV SÜD zertifizierten Entwicklungswerkzeug und Engineering-Service sind unter silistra-systems.com verfügbar.

SIListra Systems Kontakt:

Jens Schindler
Geschäftsführer

SIListra Systems GmbH
Königsbrücker Str. 124
01099 DRESDEN - GERMANY

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

Dr. Martin Süßkraut
ppa. Entwicklungsleiter

SIListra Systems GmbH
Königsbrücker Str. 124
01099 DRESDEN - GERMANY

Phone: +49 351 418 909 34
E-mail: martin.suesskraut@silistra-systems.com