SIListra Systems Pressemitteilung / Dresden, den 19. Dezember 2023

Sicherheitsteuerungen und -applikationen bis SIL3 ohne Spezial-Hardware

SIListra Safety Transformer zertifiziert nach IEC 61508 durch TÜV SÜD

Einführung / Kurzfassung

Mit dem neuen SIListra Safety Transformer 2.0 wird erstmals eine zertifizierte Lösung für die Umsetzung von Sicherheitsteuerungen und -anwendungen auf Standard-Hardware angeboten. Standard-Hardware war bisher für Sicherheitsanwendungen aller Art mit mittleren und hohen Sicherheitsanforderungen aufgrund von fehlender Diagnose für zufällige Fehler nicht zulässig. Für SIL3 Komponenten oder Systeme nach IEC 61508 (bzw. PLe nach ISO 13840) musste eine spezielle 2-kanalige Hardware entwickelt werden.

SIListra Systems revolutioniert die Entwicklung von Sicherheitssteuerungen und -anwendungen, indem die Diagnose für zufällige Fehler in Software gelöst wird. Somit entfällt die kostspielige Entwicklung einer eigenständigen speziellen Sicherheitshardware. Zugleich können damit SIListras Kunden deutlich schneller in den Markt eintreten. Ein weiteres Alleinstellungsmerkmal der Lösung von SIListra Systems ist die Lauffähigkeit auf Industrie-PCs (IPC), IT-Servern und in der Edge-Cloud. Damit eröffnen sich komplett neue Einsatzmöglichkeiten:

- Sicherheitssteuerungen und -anwendungen können wie IT-Anwendungen auf IT-Servern verwaltet werden. Fällt ein Server aus, kann innerhalb von kurzer Zeit ein Ersatzserver hochgefahren werden. Der aufwändige Austausch von SPS-Geräten entfällt.
- Mixed-Mode Anwendungen welche aus Sicherheitsanwendungen und Nicht-Sicherheitsanwendungen bestehen, lassen sich durch SIListras Lösung leichter als jemals zuvor einfach auf der Hardware der Nicht-Sicherheitsanwendung(en) integrieren.

Langfassung

Vor dem SIListra Safety Transformer 2.0.0 gab es bisher keine, generisch verfügbare, performante und zertifizierte Lösung für Coded Processing. SIListra Systems bietet hiermit die weltweit erste und einzigartige Lösung auf Basis von Coded Processing an. Und dass obwohl Coded Processing seit Jahrzehnten bekannt ist und in Sicherheitsnormen, wie der IEC 61508 sowie der ISO 26262 als Möglichkeit für die Diagnose von zufälligen Fehlern mit hoher Diagnosedeckungsrate gelistet ist. Ermöglicht wird dies durch die Weiterentwicklung von Coded Processing durch die Experten von SIListra Systems, so dass es für Anwendungen mit Zykluszeiten im Millisekunden-Bereich und darunter einsetzbar ist. Außerdem werden gleichzeitig die Sicherheitsanforderungen von ISO 26262:2018 bis ASIL D, sowie IEC 61508:2010 bis SIL 3, ISO 13849-1:2023 und der IEC 62061:2021 erfüllt.

Der SIListra Safety Transformer 2.0 kann beliebige in C/C++ geschriebene Sicherheitsanwendungen automatisiert um die notwendige Diagnose von zufälligen Fehlern auf Basis von Coded Processing erweitern. Damit sind diese Sicherheitsanwendungen in der Lage auf Standard-Hardware die Anforderungen der im vorherigen Paragraphen genannten Standards an die Diagnose von zufälligen Fehlern zu erfüllen. SIListras Lösung basiert auf 2 Software-Kanälen, welche gemeinsam auf derselben Standard-Hardware zum Einsatz kommen. Dabei können die beiden Kanäle auch auf demselben CPU-Kern ausgeführt werden.

Der erste Kanal ist die originale Implementierung der Sicherheitsanwendung. Demgegenüber wird der Source-Code des zweiten Kanals automatisiert vom SIListra Safety Transformer aus dem Source-Code des ersten Kanals erzeugt. Das SIListra Werkzeug baut dabei Coded Processing in den Source-Code des zweiten Kanals ein. Dies wiederum stellt sicher, dass auch Fehler, die sich auf beide Kanäle auswirken mit der notwendigen Wahrscheinlichkeit erkannt und behandelt werden können.

Grundsätzlich handelt es sich bei dem SIListra Safety Transformer um ein Software-Werkzeug welches während der Entwicklung einer Sicherheitssteuerung oder -anwendung zum Einsatz kommt, um diese später auf Standard-Hardware sicher ausführen zu können. Mit der neuen Version 2.0 des SIListra Safety Transformers entfällt, im Vergleich zu vorherigen Versionen, das manuelle Review des generierten Source-Codes für den zweiten Kanal. Dies wird dies durch ein komplett neues Modul ermöglicht, dem Checker, der als Teil des SIListra Safety Transformers 2.0 ausgeliefert wird. Dabei automatisiert der Checker dieses Review vollständig. Neu ist außerdem eine stabile C++ Unterstützung des SIListra Safety Transformers. Damit können Sicherheitsanwendungen in C++14 (inklusive Klassen, virtuellen Methoden, Templates, constexpr, etc.) geschrieben werden. Des Weiteren kann der SIListra Safety Transformer nun mit der Unterstützung von 64-bit Integern alle Integer-Datentypen in Standard-C/C++ absichern. Überdies wurde die bereits in C bewährte Unterstützung von Integerarithmetik (inkl. Vergleiche und Bool), Structs, Arrays und allen Standard-konformen Kontrollflusskonstrukten (Funktionsaufrufe, if, while, for, …) auf C++ übertragen. Ferner unterstützt der SIListra Safety Transformer nun C bis zu C11. Zudem hinzugekommen in C ist die Unterstützung von Funktionspointern.

Mit der Verfügbarkeit des Produktzertifikates wird den Entwicklern die Zertifizierung ihrer Sicherheitsanwendung erheblich erleichtert. Dies ist auch auf das Safety Manual des SIListra Safety Transformers zurückzuführen, welches den Anwendungsfall des Softwaretools umfassend definiert und Entwickler damit nicht selbst und zusätzlich dessen Sicherheit nachweisen müssen.

Die Prüfung durch den TÜV SÜD umfasste, neben der hoch performanten und sicheren Coded Processing Umsetzung von SIListra Systems, die Spezifikation des SIListra Safety Transformers mit dessen Sicherheitsanalysen sowie Safety Manual. Daneben wurden der sichere Entwicklungsprozess und das Funktionale Sicherheitsmanagement (FSM) von SIListra Systems geprüft. Im Lieferumfang der beiliegenden Dokumentation enthalten sind das User Manual, das Safety Manual sowie ein umfassendes Tutorial. Letzteres zeigt an einem komplexen Beispiel wie sich eine Sicherheitsanwendung mit dem SIListra Safety Transformer praktisch umsetzen lässt.

Nutzbar ist das Tool je nach Bedarf in kleinen oder großen Teams. Sowohl Einzelplatz- als auch Netzwerklizenzen werden angeboten. Ergänzend können Kunden für die automatische Qualitätssicherung CI-Lizenzen für ihren Build-Server erwerben. Damit kann der SIListra Safety Transformer effektiv in die Testinfrastruktur und die Continuous-Integration-Prozesse eingebunden werden.

Interessenten können sich mit den SIListra Safety Transformer in einem Pilot- bzw. Evaluierungsprojekt vertraut machen. Speziell bei der Einführung von Coded Processing unterstützt und berät SIListra Systems. Je nach Kundenbedarf können Leistungen wie eine gemeinsame Erstellung von Sicherheitskonzepten, Machbarkeitsstudien, gemeinsame Gespräche mit Zertifizierungsstellen, Unterstützung bei der Integration des SIListra Safety Transformers sowie Schulungen/Workshops vereinbart werden. Darüber hinaus kann SIListra Systems bei der Umsetzung der in der Automatisierungsbranche weit verbreiteten Programmiersprachen, zum Beispiel aus der IEC 61131-3, zur Seite stehen. So können Know-How und existierende Implementierungen beim Anwender weiterverwendet werden und bereits getätigte Investitionen erhalten bleiben.

BILDER

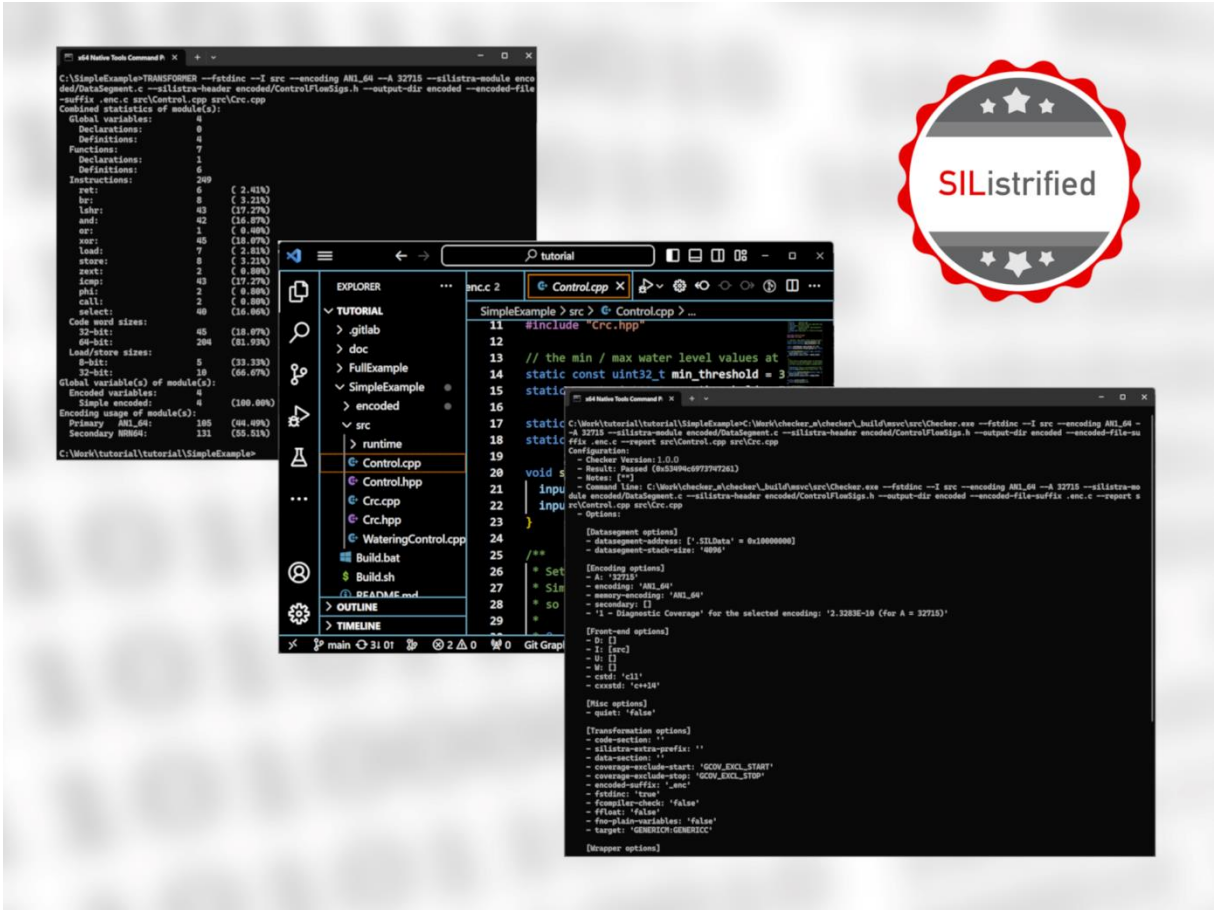

Bild1: SIListra Safety Transformer 2.0

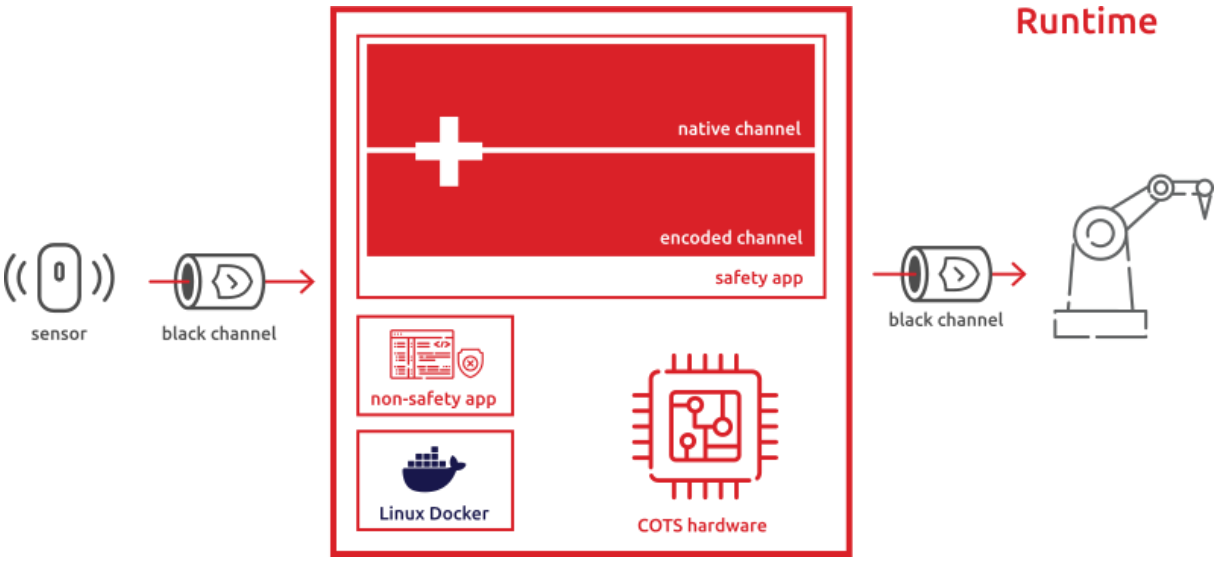

Bild2: Diversified Encoding: Zwei Software-Kanäle (native/encoded channel) auf einer Hardware

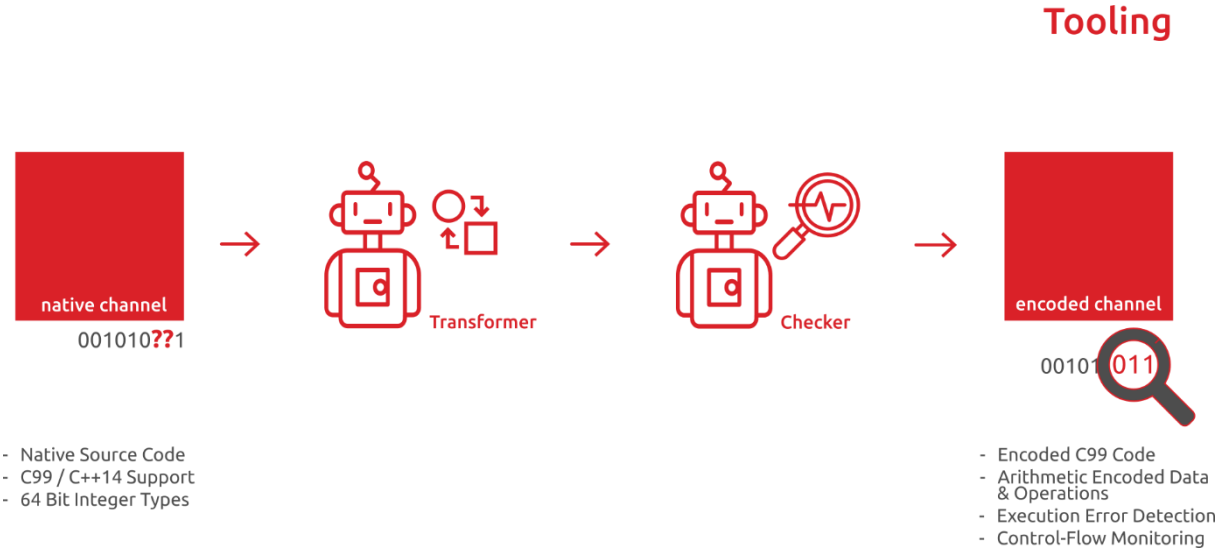

Bild3: Der SIListra Safety Transformer erzeugt den Source-Code des kodierten Kanals (encoded channel) aus dem Source-Code des nativen Kanals (native channel)

Über SIListra Systems:

Die SIListra Systems GmbH mit Sitz in Dresden ist ein innovatives, hoch spezialisiertes IT-Technologieunternehmen, das 2012 aus der TU Dresden ausgegründet wurde. Der Fokus liegt bei speziellen Software-Verfahren und deren Umsetzung in Entwicklungswerkzeuge für den Einsatz auf dem Gebiet der funktionalen Sicherheit bzw. bei der Automatisierung von sicherheitsrelevanten Anwendungen. SIListra Systems bietet sowohl mit dem SIListra Safety Transformer eine zertifizierte Produktlösung nach den Safety-Standards IEC 61508, ISO 26262, ISO13849 und IEC 62061 als auch zugehörige Engineering- und Consulting-Dienstleistungen weltweit an. Alle Entwicklungs- und Projekt-Mitarbeiter können eine Personenzertifizierung als Functional Safety Engineer, Professional oder Expert (FSCP) vorweisen. Mehr Informationen zum Unternehmen 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
Fax: +49 351 418 909 36
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
Fax: +49 351 418 909 36
E-mail: martin.suesskraut@silistra-systems.com