SIListra Systems press release / Dresden, December 19th, 2023

Safety controllers and applications up to SIL3 without special hardware

SIListra Safety Transformer certified according to IEC 61508 by TÜV SÜD

Introduction/ Abstract

The new SIListra Safety Transformer 2.0 is the first certified solution for the implementation of safety controller and applications on standard hardware. Standard hardware was previously not permitted for safety applications of all kinds with medium and high safety requirements due to a lack of diagnostics for random faults. Special 2-channel hardware had to be developed for SIL3 components or systems in accordance with IEC 61508 (or PLe in accordance with ISO 13840).

SIListra Systems is revolutionizing the development of safety control systems and applications. The development of independent special safety hardware is no longer necessary. This allows SIListra's customers to enter the market more quickly. Another unique selling point of the SIListra Systems solution is that it runs on industrial PCs (IPC), IT servers and in the edge cloud. This opens up completely new application possibilities:

- Security controllers and applications can be managed like IT applications. If a server fails, a replacement server can be started up within a short time. The time-consuming replacement of PLC devices is no longer necessary.
- - Mixed-mode applications, which consist of safety and non-safety applications, can thus be integrated more easily than ever before on the hardware of the non-safety application.

Full Version

SIListra Systems revolutionizes the development of safety control systems and applications by implementing the diagnosis of random errors solely in software. This eliminates the costly development of dedicated safety hardware. At the same time, this enables SIListra's customers to enter the market much faster. Another unique benefit of the SIListra Systems solution is its ability to run on industrial PCs (IPC), IT servers and in the edge cloud. This opens up completely new application possibilities:

- Security controllers and applications can be managed like IT applications on IT servers. If a server fails, a replacement server can be started up within a short time. The time-consuming replacement of PLC devices is no longer necessary.
- Mixed-mode applications that consist of safety and non-safety applications can be easily integrated on the hardware of the non-safety application(s) more effectively than ever before with SIListra's solution.

The new SIListra Safety Transformer 2.0 is the first certified solution for implementing safety control systems and applications on standard hardware. Standard hardware was previously not permitted for safety applications with medium and high safety requirements due to a lack of diagnostics for random faults. Special 2-channel hardware had to be developed for SIL3 components or systems in accordance with IEC 61508 (or PLe in accordance with ISO 13840).

Before SIListra Safety Transformer 2.0.0, there was no generic, high-performance and certified solution for coded processing available. SIListra Systems now offers the world's first and unique solution based on Coded Processing. This is despite the fact that coded processing has been known for decades and is listed in safety standards such as IEC 61508 and ISO 26262 as a way of diagnosing random faults with a high diagnostic coverage rate. This is made possible by the improvements of Coded Processing by the experts at SIListra Systems, making it usable for applications with cycle times in the millisecond range and below. It also meets the safety requirements of ISO 26262:2018 up to ASIL D, IEC 61508:2010 up to SIL 3, ISO 13849-1:2023 and IEC 62061:2021.

The SIListra Safety Transformer 2.0 can automatically extend any safety application written in C/C++ to include the necessary diagnostics of random errors based on Coded Processing. This enables these safety applications to fulfill the requirements of the standards mentioned in the previous paragraph for the diagnosis of random errors on standard hardware. SIListra's solution is based on 2 software channels which are used together on the same standard hardware. Furthermore these two channels can also be executed on the same CPU core.

The first channel is the original implementation of the safety application. The source code of the second channel is automatically generated by the SIListra Safety Transformer from the source code of the first channel. The SIListra tool integrates coded processing into the source code of the second channel, which in turn ensures that errors that affect both channels can be detected and handled with the necessary probability.

Fundamentally, the SIListra Safety Transformer is a software tool that is used during the development of a safety controller, PLC or application with the aim of enabling the execution of the safety controller/application on standard hardware. With the new version 2.0 of the SIListra Safety Transformer, the manual review of the generated source code for the second channel is no longer necessary compared to previous versions. This is made possible by a completely new module, the Checker, which is provided as part of SIListra Safety Transformer 2.0. This Checker fully automates this review. Another new feature is the SIListra Safety Transformer’s robust C++ support. This allows safety applications to be written in C++14 (including classes, virtual methods, templates, constexpr, etc.). Furthermore, the SIListra Safety Transformer can now handle all integer data types in standard C/C++ with the new support for 64-bit integers. In addition, support for integer arithmetic (including comparisons and bool), structs, arrays and all standard-compliant control flow constructs (function calls, if, while, for, …), which has already established in C, has been transferred to C++. Furthermore, the SIListra Safety Transformer now supports C up to C11. Moreover, support for function pointers has also been added in C and C++.

The availability of the product certificate makes it much easier for developers to certify their own safety application. This is due to the Safety Manual of the SIListra Safety Transformer that comprehensively defines the use case of the SIListra Safety Transformer and thus the developers do not have to provide additional proof of its safety themselves.

In addition to the high-performance and safe coded processing implementation of SIListra Systems, the audit by TÜV SÜD included the specification of the SIListra Safety Transformer with its safety analyses and safety manual. The safe development process and the Functional Safety Management (FSM) of SIListra Systems was also tested. The accompanying documentation includes the User Manual, the Safety Manual and a comprehensive tutorial. The latter uses a complex example to show how a safety application can be practically implemented with the SIListra Safety Transformer.

SIListra Safety Transformer can be used in small or large teams as required. Both single-user and network licenses are available. In addition, customers can purchase CI licenses for their build server as part of the automatic quality assurance. This allows SIListra Safety Transformer to be effectively integrated into the test infrastructure and continuous integration processes.

Interested parties can familiarize themselves with the SIListra Safety Transformer in a pilot study or an evaluation project. SIListra Systems provides support and advice specifically for the introduction of Coded Processing. Depending on customer requirements, services such as the joint creation of safety concepts, feasibility studies, joint discussions with certification bodies, support with the integration of the SIListra Safety Transformer and training courses/workshops can be arranged. In addition, SIListra Systems can assist with the implementation of programming languages widely used in the automation industry, for example from IEC 61131-3. Thus, know-how and existing implementations can continue to be used by the customer and investments already made can be retained.

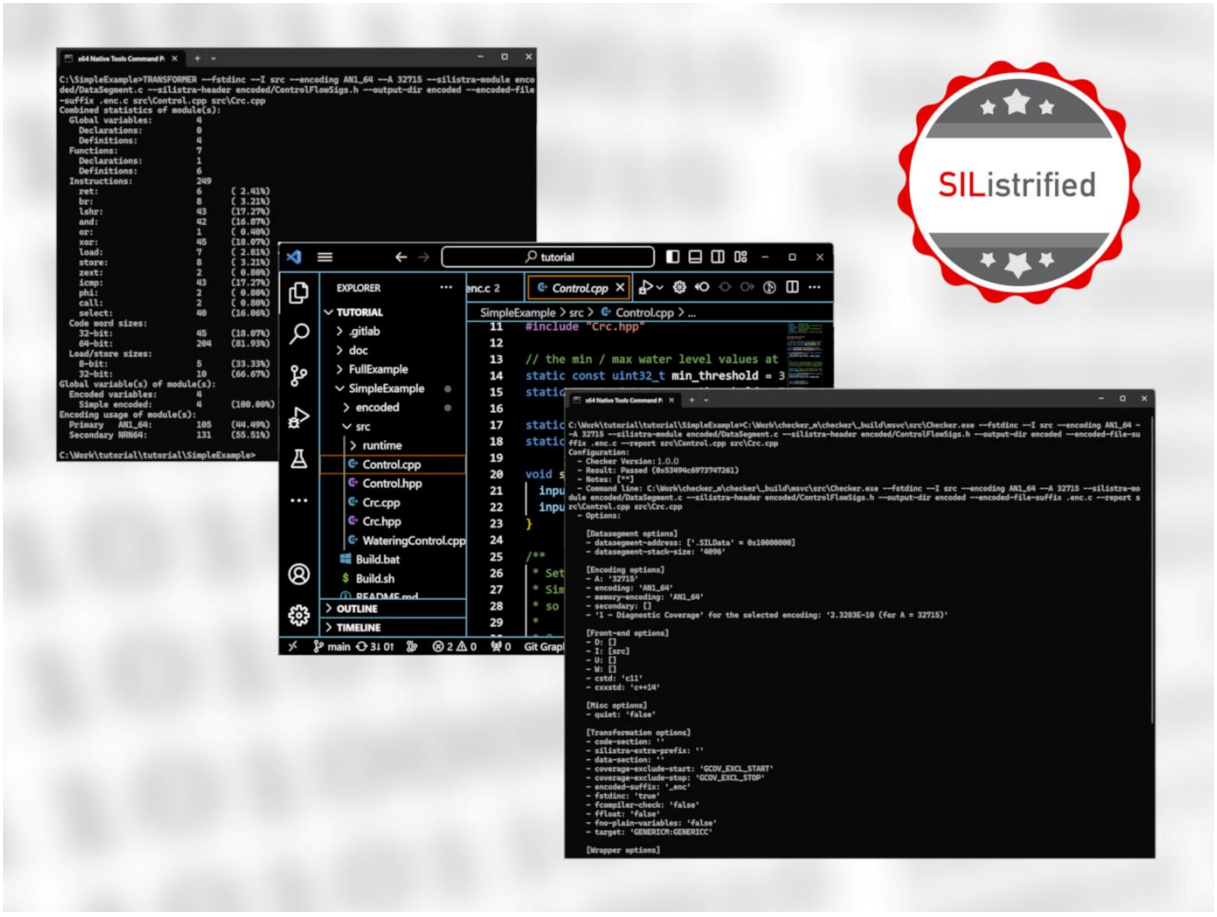

Figure 1: SIListra Safety Transformer 2.0

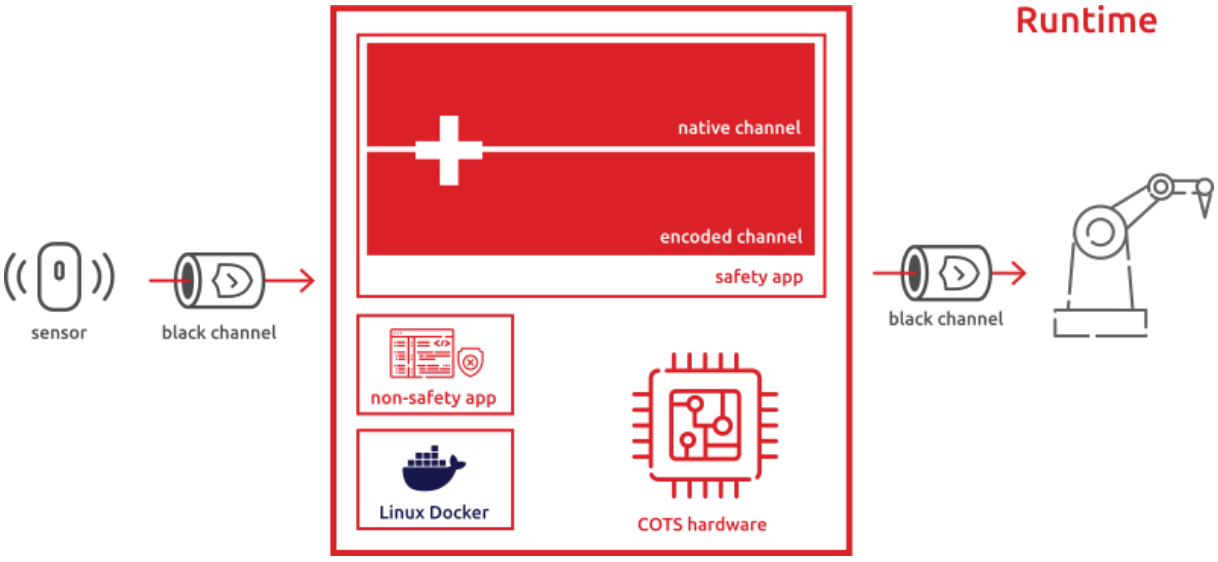

Figure 2: Diversified Encoding: Two software channels (native and encoded channel) on one hardware channel.

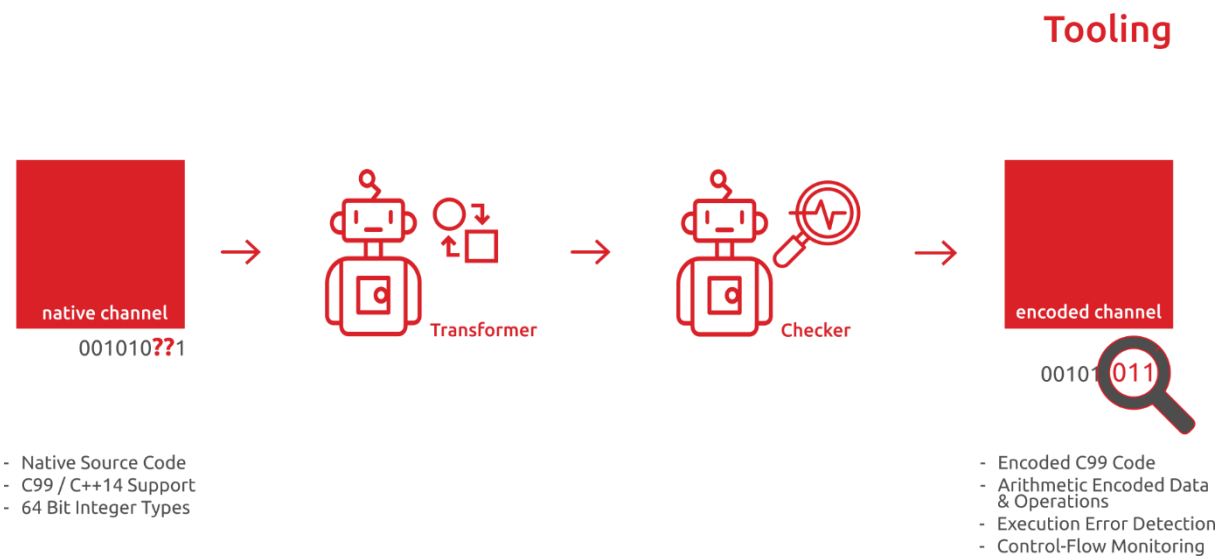

Figure 3: The SIListra Safety Transformer creates the source code of the encoded channel from the source code of the native channel.

About SIListra Systems

SIListra Systems GmbH, headquartered in Dresden, is an innovative, highly specialized IT technology company that is a spin-off of the Technische Universität Dresden founded in 2012. The focus is primarily on special software solutions and their implementation in development tools for use in the field of functional safety as well as the automation of safety-relevant applications. With the SIListra Safety Transformer, SIListra Systems offers a certified product solution in accordance with the safety standards IEC 61508, ISO 26262, ISO13849 and IEC 62061. Furthermore, associated engineering and consulting services worldwide are offered. All development and project employees are certified as Functional Safety Engineers, Professionals or Experts (FSCP). More information about the company is available at silistra-systems.com.

SIListra Systems contact:

Jens Schindler
Managing Director
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. Head of Devlopment
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