Hardware-independent safety solutions with SIListra Systems and innotec

Martin Süßkraut, SIListra Systems GmbH, martin.suesskraut@silistra-systems.com;
Claudio Gregorio, innotec GmbH, claudio.gregorio@innotecsafety.com

Abstract

innotec GmbH and SIListra Systems GmbH work together in the field of functional safety. Interested parties have comprehensive access to specialist expertise in order to implement holistic solutions in the field of functional safety. On the basis of SIListra Systems technologies and innotec's specific experience, customers can implement solutions faster and efficiently. The objective is to reach the optimal cost in safety projects, through an innovative process and solution, without compromising on the fulfillment of safety integrity requirements.

Introduction

Not requiring a SIL-graded hardware for functional safety solutions is a game changer.

Developers can skip the process of designing and developing a SIL-graded hardware and instead allocate safety functions to existing Commercial Off the Shelf (COTS) hardware. Coded processing and diversified encoding eliminate the need for any software required to control and supervise hardware safety features (hardware diagnostic realized in SW, RAM tests, Self Test Libraries, etc.). Thus, the safety function becomes more portable, because the hardware-dependent supervising code is not necessary anymore.

Coded processing also allows to mitigate the risk of hardware supply problems and discontinuation of hardware parts. Once a safety function is implemented with coded processing on non-safety-hardware, it can be moved easily to comparable hardware, because the safety function does not depend on any specific safety hardware or component anymore. This also results in improved scalability. When a safety function would require a faster CPU or faster RAM, etc. the hardware design can be changed with comparable effort to the one needed for the non-safety-critical functions.

A hardware independent safety solution is usually already a mixed-criticality system. The control of the underlying hardware can be left to commercial of the shelf (COTS) operating system (e.g. Linux). This further improves the portability and allows to profit from state-of-the-art security mechanisms that are part of such operating systems.

Finally, completely new safety solutions become possible. Safety functions can run on industrial PCs, IT servers and even on the edge-cloud. Virtualization (e.g. with containers) becomes available and enables to manage safety functions like other IT services. This enables completely new approaches to availability for safety functions, that were previously exclusive to non-safety functions.

Coded Processing

Figure 1 below shows the one main use-case for coded processing.

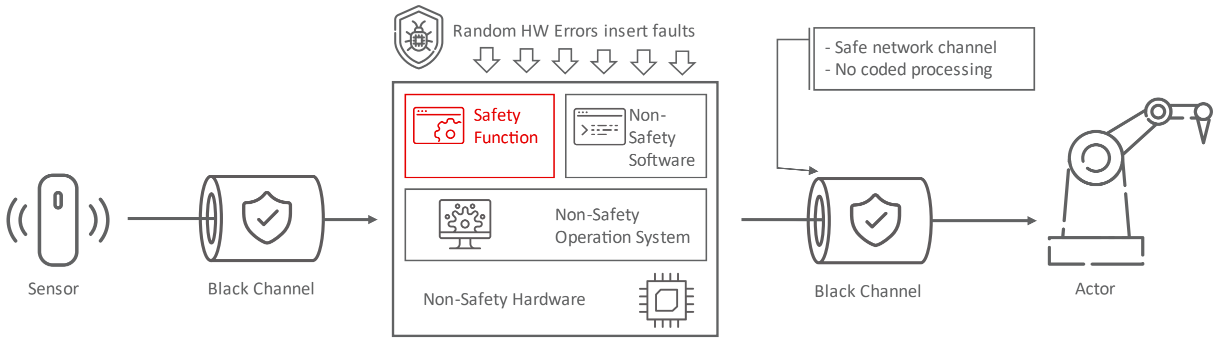


Figure 1. End-to-end safety architecture by using of coded processing and diversified encoding

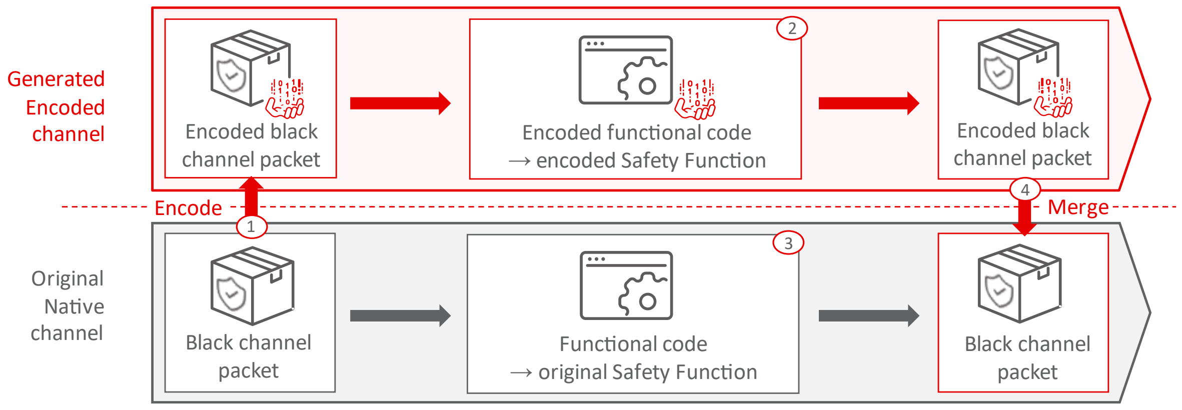
The safety function implements the desired safety functionality. It reads data from sensors and can switch the actors into a safe state, if necessary. The communication between the safety function and the sensors and actors happens via a black channel and uses therefore communication protocols with appropriate safety integrity measures (IEC 61784 based protocols like FSoE, Profisafe, CIP Safety, etc. or other proprietary ones). Coded processing enables the safety function to run on hardware that is neither specially designed nor certified for safety, e.g., non-safety PLCs, industrial PCs, IT servers or edge-cloud servers.

Because of the safe communication protocol, the sensors and actors do not need to be adapted to coded processing. The endpoints of the safe communication protocol are usually part of the safety function.

Coded processing is restricted to the safety function application. The safety function consists now of two redundant software channels, i.e., the safety function is executed twice. In order to achieve the desired diagnostic coverage, the two channels are diverse to each other. The native channel implements the safety function without any additional diagnostic for random hardware failures. The encoded channel implements the same safety function together with coded processing as diagnostic method for random failures. Together both channels provide sufficient diagnostic coverage for

- Random failure up to SIL3 (IEC 61508:2010)
- Interference from non-safety-critical software (i.e., the operating system and other non-safety software) according i.e. to requirements of Annex F – IEC 61508:2010

Figure 2 below illustrates one task cycle of the safety function at runtime (example). First any inputs are read from the black channel and provided to the native and the encoded channel. Then, both channels check these inputs and compute outputs (safety logic). The two channels run separately from each other and each channel has its own state. At the end of the cycle, the outputs of both channels are merged together similar to the merging of outputs for two-channel-hardware. The merged output is then sent to the sensors and actors via the black channel.



Generated Encoded channel
Encoded black channel packet
Encoded functional code → encoded Safety Function
Encoded black channel packet
2
Encode
1
Merge
4
Original Native channel
Black channel packet
Functional code → original Safety Function
3
Black channel packet

Figure 2. Diversified encoding: native and encoded channel as 2-channel-solution

The source code of the native channel must obviously be developed in accordance with the appropriate safety standards, to assure that the correct specification is implemented.

The SIListra Safety Transformer automatically generates the source code of the encoded channel from the source code of the native channel (see Figure 3 below).

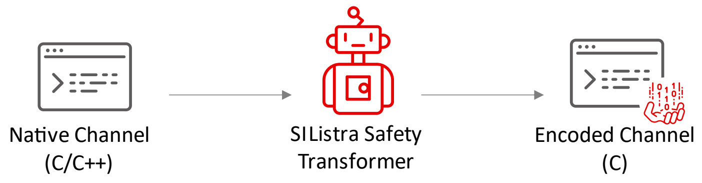


Figure 3. The input and output of the tool SIListra Safety Transformer

The SIListra Safety Transformer is qualified for use in safety related applications and certified accordingly by TÜV SÜD based on the following standards:

- IEC 61508:2010 (up to SIL3)
- ISO 13849-1:2023 (up to PLe)
- IEC 62061:2021 (up to SIL3)
- ISO 26262:2018 (up to ASIL-D)

The SIListra Safety Transformer supports as input languages C and C++. Because its output language is C, the code generated by the SIListra Safety Transformer can be compiled for almost any hardware platform. To support other programming languages (e.g. IEC 61131-3 languages and Simulink), the SIListra Safety Transformer can be chained with other code generators as long as C or C++ are produced as output code.

Application

Based on coded processing automatization by SIListra Safety Transformer, safety functions used on several applications can be implemented on non-safety-hardware.

SIListra Systems support users that want to apply coded processing and use the SIListra Safety Transformer with its unique know-how.

Functional safety is however not only handling of hardware failures.

innotec support users of the SIListra Safety Transformer with the experience in practical application of a broad range of safety standards, combined with the deep understanding of the SIListra Systems coded processing based technology.

With this background innotec can guide customers, starting from creation of the optimal technical safety concept based on coded processing to all relevant lifecycle aspects, including requirements analysis, architecture, software design, test, and verification.

Examples of consultancy activities in collaboration with SIListra Systems, can be:

- Concept discussion: safety concept, architecture overview
- Integration of SIListra Systems toolchain into user development processes and toolchain
- Definition of additional support activities (Functional Safety Management, and more)
- Support during verification activities
- Coordination of all activities with the final assessor, notified body, Safety Manager

innotec has a proven track record of successfully completed projects, directly supporting the coded processing technology in collaboration with SIListra Systems.

The support includes the development of tailored solutions for your projects and assistance with all necessary functional safety activities. Through the strong partnership with SIListra Systems, innotec's experts are able to deliver the precise and customized functional safety solution users need.