



# SIListra SAFETY TOOLS

making systems safer

Current approaches to provide hardware safety will not be sufficient in future, because they become too costly. The SIListra Safety Tools are cost-effective and safe software-only solutions that provide reliable detection of hardware errors while at the same time reducing hardware and development costs. They are flexible and universally deployable.

## State of the art

Today, most of the current innovations, e.g., in the automotive industry rely heavily on automation and therewith on computing technology.

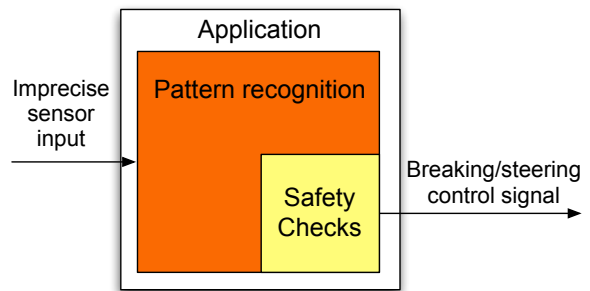
Standards like IEC 61508 and ISO 26262 define strict safety requirements for both hard- and software. To meet these requirements manufactures design and build complex (self-)checks into hardware *and* software.

These solutions increase complexity and therewith the costs of development and production of safety-critical systems.

## Future of hardware safety

Up-to-date architectural solutions are not prepared for the decreasing reliability of future hardware. The decreasing feature sizes of the next hardware generations result in a significant higher vulnerability to transient errors and permanent design faults. Dealing with this increased vulnerability within the current architectural solutions imposes a too high overhead for many applications for example in the automotive domain.

Another issue is that architectural solutions follow often an all-or-nothing approach: either the whole application is protected from hardware failures or there is no protection at all. However, many applications have only a



*Illustration 1: The architecture of an example application with only a small safety-critical part.*

small and restricted number of components that are responsible for the system's safety. Illustration 1 shows an application where only a small part (the safety checks) must be executed correctly, because the other parts relies on anyway imprecise input. Protecting the safety checks with the SIListra Safety Tools avoids expensive and complex architectural solutions where either the complete application runs on expensive hardware or the application is split into two hardware parts with different safety requirements.

In summary, our SIListra Safety Tools address the following challenges:

- Future hardware becomes increasingly unreliable.
- This causes high demand on detecting temporary and permanent execution failures.
- The requirements for safety increase.
- The demand for cost-effective, universal and flexible solutions for safety keeps rising.

## SIListra Safety Transformer

The SIListra Safety Transformer applies the Coded Processing technology to reliably detect hardware failures in all safety-critical parts of an application. The protection works

reliably regardless of the source of the failure during the runtime of the application. This allows systems using the SIListra Safety Transformer solution to run safety-critical parts and non-safety-critical parts of an application on the same up-to-date commodity hardware generation.

Illustration 2 shows the workflow of the SIListra Safety Transformer. The SIListra Safety Transformer directly works with the original application's source code. It automatically adds redundancy based on Coded Processing to the program. The output is in a generic source code format that can be compiled for the target platform.

The transformed application reliably detects temporary and permanent execution failures in its data-flow and control-flow. The added redundancy is hardware independent and does not rely on any costly redundant hardware solution. Hence, it can be flexibly applied to many different platforms and the hardware can be exchanged at later update cycles of the product.

The SIListra Safety Transformer is able to process C code. We support the all C control structures, functions, global variables, dynamic memory, and user defined data types. The transformer works also with generated code and can thus be used with modeling tools such as SimuLink.

## SIListra Safety Replicator

The SIListra Safety Replicator is optimized for detecting transient errors (soft errors). Because we derived it from the SIListra Safety Transformer, it supports the same



Illustration 2: The workflow of the SIListra Safety Transformer: it automatically transforms unprotected software into protected software, which detects execution failures at runtime.

	SIListra Safety Replicator	SIListra Safety Transformer
--	----------------------------	-----------------------------

Reduces design complexity	✓	✓
Fully-automated	✓	✓
ISO 26262 and IEC 61508	✓	✓
Hardware independent	✓	✓
Supports C and SimuLink	✓	✓
Detects transient errors	✓	✓
Detects permanent errors		✓

applications and C languages features. It can be used like the Transformer (see Illustration 2). The SIListra Safety Replicator uses a specially crafted form of software redundancy instead of the Coded Processing technology.

The SIListra Safety Replicator is an alternative to using costly dual core hardware to detect soft errors and it avoids the synchronization issues behind using dual core based redundancy.

## Summary

- More cost-effective than safe hardware-only approaches and certifiable.
- SIListra Systems funded as Spin-off of the Technische Universität Dresden.
- First pilot projects with big automotive OEM and suppliers.
- Started certification process according to ISO 26262 and IEC 61508.

## Contact

Technische Universität Dresden  
 Faculty of Computer Science  
 Chair for Systems Engineering  
 Contact: Dr.-Ing. Martin Süßkraut  
<http://www.silistra-systems.com/>  
 Email: martin.suesskraut@silistra-systems.com



DRESDEN  
concept  
Exzellenz aus  
Wissenschaft  
und Kultur

## Funding

Gefördert durch:



Bundesministerium  
für Wirtschaft  
und Technologie

aufgrund eines Beschlusses  
des Deutschen Bundestages

