



© SICK AG

## REUSE OF MODULAR FUNCTION BLOCKS IN SAFETY-CRITICAL CONTEXTS

### OUR COMPETENCIES AND SOLUTIONS

- Development of modular safety concepts
- Explicit safety argumentation for the certification of innovative safety concepts
- safeTbox – tool framework of Fraunhofer IESE for the development and certification of safety-critical systems

### THE CUSTOMER BENEFIT

- Reuse of functionality on different platforms and in different application contexts
- Transfer of the results of ongoing discussions into research and industry and of future safety standards into the customer process

### WHAT IT IS ALL ABOUT

Industry 4.0 opens up a new area of industrial automation. While large-scale mass production has been the driving force in the past, new technological possibilities allow for flexible and adaptive, yet highly automated manufacturing facilities even down to small batch sizes or customized products. Flexibility and modularity are two of the key enablers of this transition. As an innovation leader on the vanguard of developing cutting-edge sensor technology, SICK provides solutions that are ready for this challenge – with intelligent sensors that collect data, evaluate it in real time, adapt to their environment, and communicate in the network. Especially when it comes to safety-relevant data, the safety assurance of systems is of particular importance. This is one reason why SICK relied on the safety expertise and support of Fraunhofer IESE in this regard.

### THE CHALLENGE

Flexibility and adaptability also imply an increase of complexity. This is especially true at the interfaces between the digital world and the physical world of the manufacturing facilities – the sensors: The information for monitoring and controlling the quality, efficiency, and safety of production processes has to be provided with a very high degree of reliability. Making these sensors as intelligent as possible requires extensive use of software already at the level of individual sensors, and even more so within sensor systems and in the control system.

*Making the development of function blocks for safety-related applications modular and transparent was the goal of our joint project with Fraunhofer IESE. The model-based approach suggested by Fraunhofer IESE provided an ideal basis for this: All interfaces are well described with both the provided and required services and the safety-relevant properties. This allows executing function blocks on various platforms and makes them reusable in various sensor systems. Our colleagues from Fraunhofer IESE did an excellent job in understanding our challenges and tailoring their approach to our demands.*

Dr. Magnus Albert  
Expert Safety Methods  
Corporate Unit Functional Safety  
SICK AG



Especially when the data provided by the sensors is safety-relevant, the assurance of such systems becomes a challenging task. The goal of the project with Fraunhofer IESE was to develop and establish a methodology that allows for the engineering of modular and flexible, yet “safe” function blocks. This allows safety-related functionality to be composed out of multiple independent function blocks, to be executed on various platforms, and to be reused in different applications.

SICK approached the Fraunhofer Institute for Experimental Software Engineering IESE for various reasons: The institute has comprehensive competencies in Safety Engineering and model-based approaches. Combining IESE’s knowledge on Safety Engineering with SICK’s experience in sensor technology enabled a tailored solution for the development of safety-related function blocks in sensor systems.

## THE SOLUTION

The collaboration between SICK and Fraunhofer IESE focused on the engineering of a specific function block for collaborative applications, where human and machines share the same workspace. While embedding the function block into a real-world application helped to identify assumptions about the relevant context, the function block itself was developed as generically as possible to ensure maximum flexibility and reusability.

Using a service-oriented approach, the first step of the model-based engineering approach was to create a block model of the overall architecture of the application. On the basis of this service architecture, the horizontal interfaces to other services and the vertical interfaces to the platform services were identified. Comprehensive and service-specific lists of guide words were used to analyze each

individual interface and to identify all their relevant failure modes. The corresponding failure logics were then constructed using component fault trees. While focusing on the modular services during the analysis, combining the individual component fault trees for the overall system ensures completeness on the system level.

In the third and final step, the analysis was used to build a safety case providing a comprehensive and indispensable argumentation for the overall safety.

The model-based approach ensures that each of the three artifacts – service block diagram, component fault tree, and safety case – can be reused in other projects, along with the corresponding function block.

## THE RESULT

The model-based engineering approach suggested by Fraunhofer IESE could be incorporated successfully into the development project at SICK and has already been transferred successfully to other development projects. The safeTbox tool developed by Fraunhofer IESE combines all required model-based techniques in one toolbox and facilitates the deployment of the methodology.

Name: SICK AG

Website: [sick.com](https://www.sick.com)

Industry: sensor manufacturing

Headquarters: Waldkirch, Germany

Number of Employees: 9,700 (2018)

## Contact

Dr. Daniel Schneider  
Department Head Embedded Systems  
Quality Assurance (ESQ)  
Phone +49 631 6800-2187  
[daniel.schneider@iese.fraunhofer.de](mailto:daniel.schneider@iese.fraunhofer.de)

Jan Reich  
Expert „Dynamic Assurances of  
Connected Autonomous Systems“  
Phone +49 631 6800-2254  
[jan.reich@iese.fraunhofer.de](mailto:jan.reich@iese.fraunhofer.de)

[www.iese.fraunhofer.de](http://www.iese.fraunhofer.de)

