



SUCCESS STORY - FUNCTIONAL SAFETY

Functionally safe drive technology module for cobots



The collaboration between a customer and MESCO Engineering in the development of a functionally safe drive technology module for collaborative robots (cobots) with MESCO Safety Design Packages has set new standards. The creation of the Safety Drive not only illustrates the capabilities of the companies involved, but also the strategic focus on the highest safety standards.

Certified functional safety for cobots

The resulting product redefines the standard for cobots by being the first integrated motion device in an extremely compact design to offer certified functional safety in accordance with IEC61508, SIL3, EN ISO 13849, PL-e and IEC61800-5-2.

The close cooperation enabled the perfect integration of the brake system, two integrated encoders and safety electronics with ten certified advanced safety functions in the smallest possible installation space.

Safety Drive: Technical challenge and solution approach

The development of the product was based on an existing servo drive from the customer. The challenge was to expand the electronics in accordance with the standards for functional safety, with the Safe Motion Option Board (SMO) playing a decisive role as the safety monitoring electronics. MESCO designed and developed the SMO, while the customer implemented the hardware based on the MESCO safety concept approved by TÜV SÜD.

The challenge during development was to accommodate the redundant safety electronics (1oo2) in the smallest possible space and to implement all the required safety drive functions in accordance with IEC61800-5-2 for SIL3.



Safe Motion option board, safety functions and implementation

The SMO extends the existing safety functions of the basic drive series (with Safe Torque Off and Safe Brake Control) with complex additional features. MESCO implemented the safe communication technology EtherCAT FSoE and the required safe drive functions in accordance with IEC61508, SIL3, EN ISO 13849 PLc:

- STO – Safe Torque off
- SBC – Safe Brake Control
- SS1 – Safe Stopp 1
- SS2 – Safe Stopp 2
- SLS – Safe Limited Speed
- SLP – Safe Limited Position
- Safe Velocity Process Data
- Safe Position Process Data
- Safe Digital I/O and Analogue Inputs

Functional safety management: realization in the development process

The project was realized as part of the TÜV-certified development process at MESCO according to the V-model. First, the system requirements specification was created, followed by the safety software concept with the necessary hardware and software requirements. These documents were submitted to TÜV SÜD for concept review and approved by them.

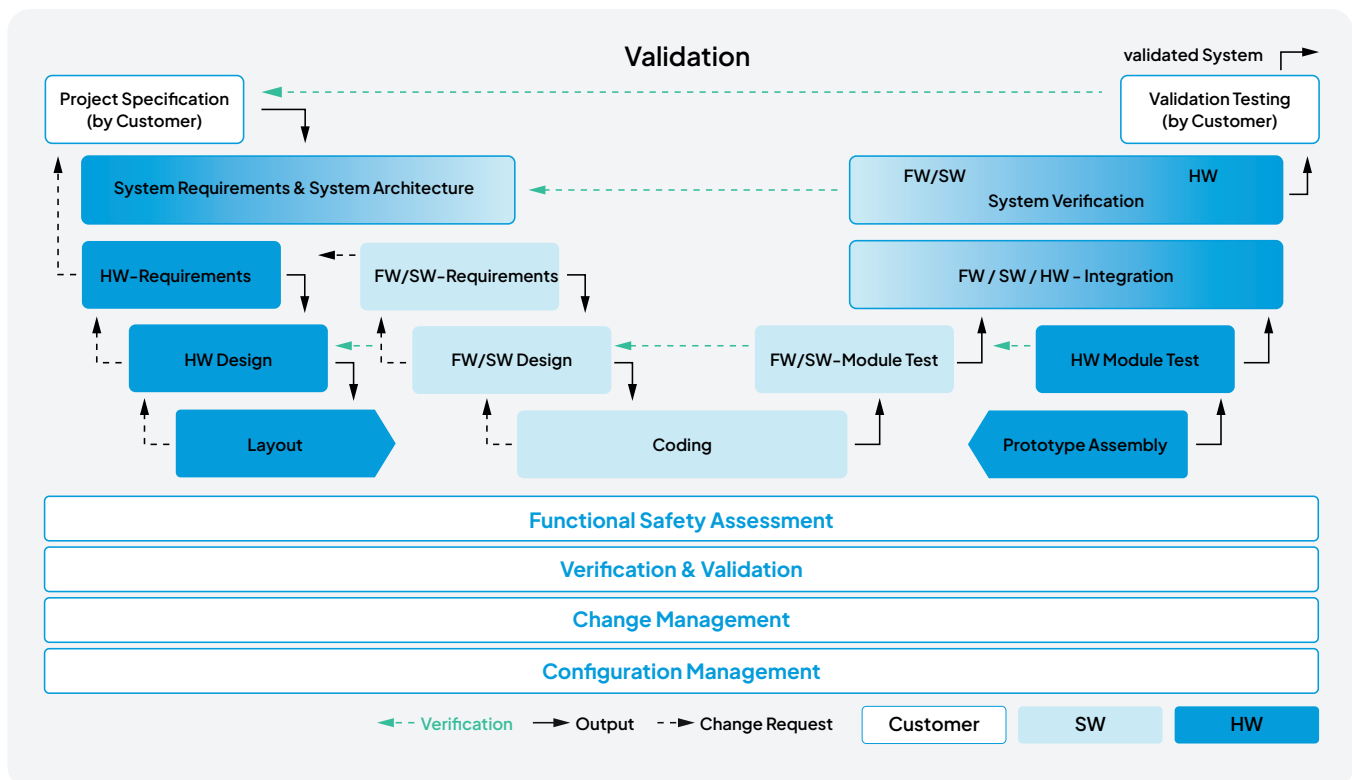


Fig1: The TÜV-certified development process for functional safety management at MESCO Engineering



After concept approval, the hardware/software sub-development projects were split between MESCO and the customer, with the latter taking over the safety-relevant hardware development with support and reviews from the MESCO safety engineers. MESCO implemented the software design after the TÜV concept approval, carried out the coding as well as module and unit tests and supported the product validation tests on the customer side.

MESCO Safety Design Packages

MESCO's core software development was based on artifacts from the proven MESCO **Safety Design Packages**.

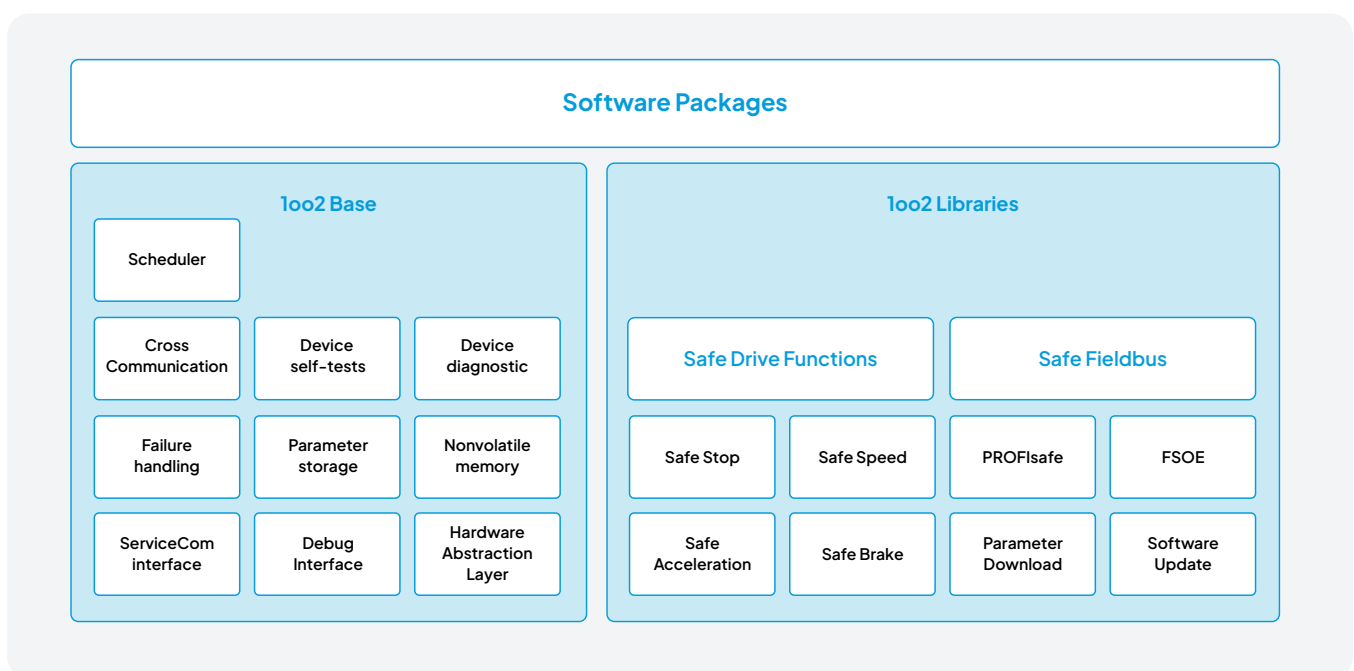


Fig 2: Overview of the MESCO Safety Design Packages, software packages for SIL3 applications

The Design Packages are a kind of eco-system and provide the functions frequently used in drive technology in tested software modules. The software libraries for the Advanced Safety Functions (ASF) were also used here. This significantly reduced the time and effort required for implementation and documentation.



Saving time through simultaneous soft- and hardware development

This basic implementation formed the basis for an initial software prototype. This allowed the first hardware prototypes to be put into operation at an early stage, which brought a significant time advantage.

The customer's product developers perfected the drive enclosure, hardware board and application software in parallel with MESCO's development of the security software. MESCO supported the optimisation of the hardware design with agile reviews. The ideas were perfected with the help of suggestions and proposals.

The development process was accelerated through a parallel approach with simultaneous hardware and software development.

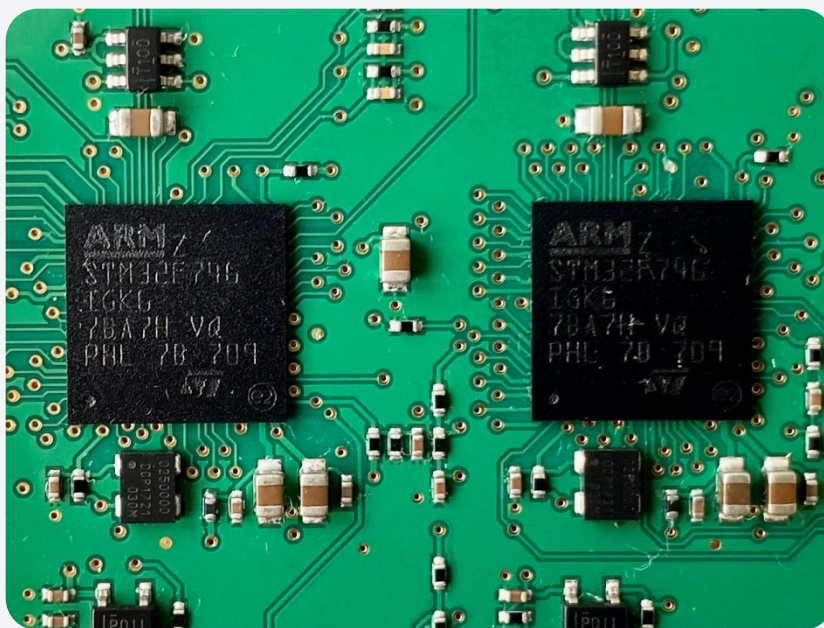


Fig 3: Close-up of 1oo2 PCB layout (SIL3 architecture)



Redundant system architecture and maximum functional safety

Due to the high demands on the safety functions, a redundant Ioo2 system architecture was chosen. The safety core components included two STMicroelectronics STM32F7 microcontrollers with synchronized cross-communication, redundant power supplies, decoupling measures, redundant I/Os and the standard-compliant implementation of safe Ethernet communication EtherCAT/FSoE.

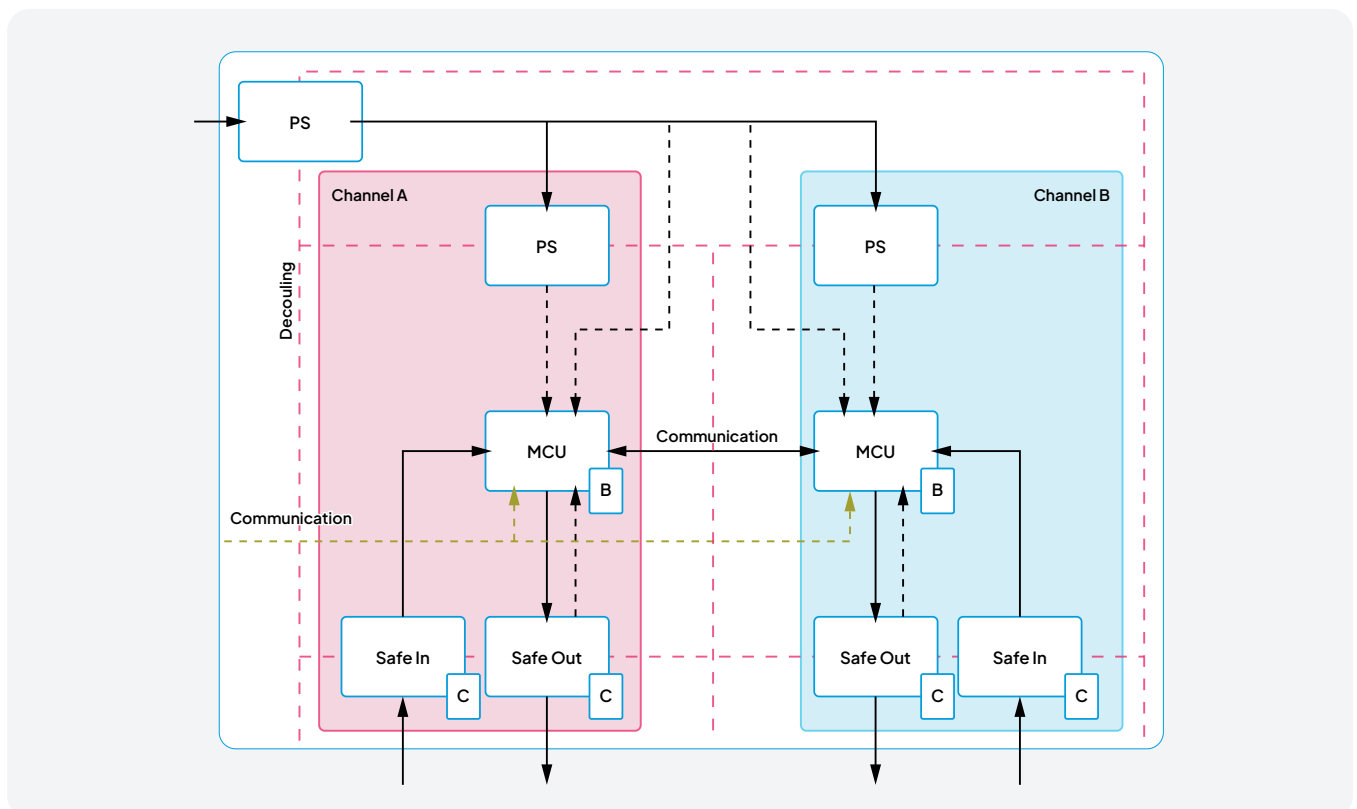


Fig 4: Architecture block diagram with redundant microcontroller architecture, safe power supply and black channel communication with EtherCAT/FSoE.

Functional safety for cobots: success factors and outlook

The agile and cooperative project process made it possible to develop the highly complex and safety-relevant product within budget and on time, with a calculable development risk and achieved TÜV certification from TÜV SÜD.

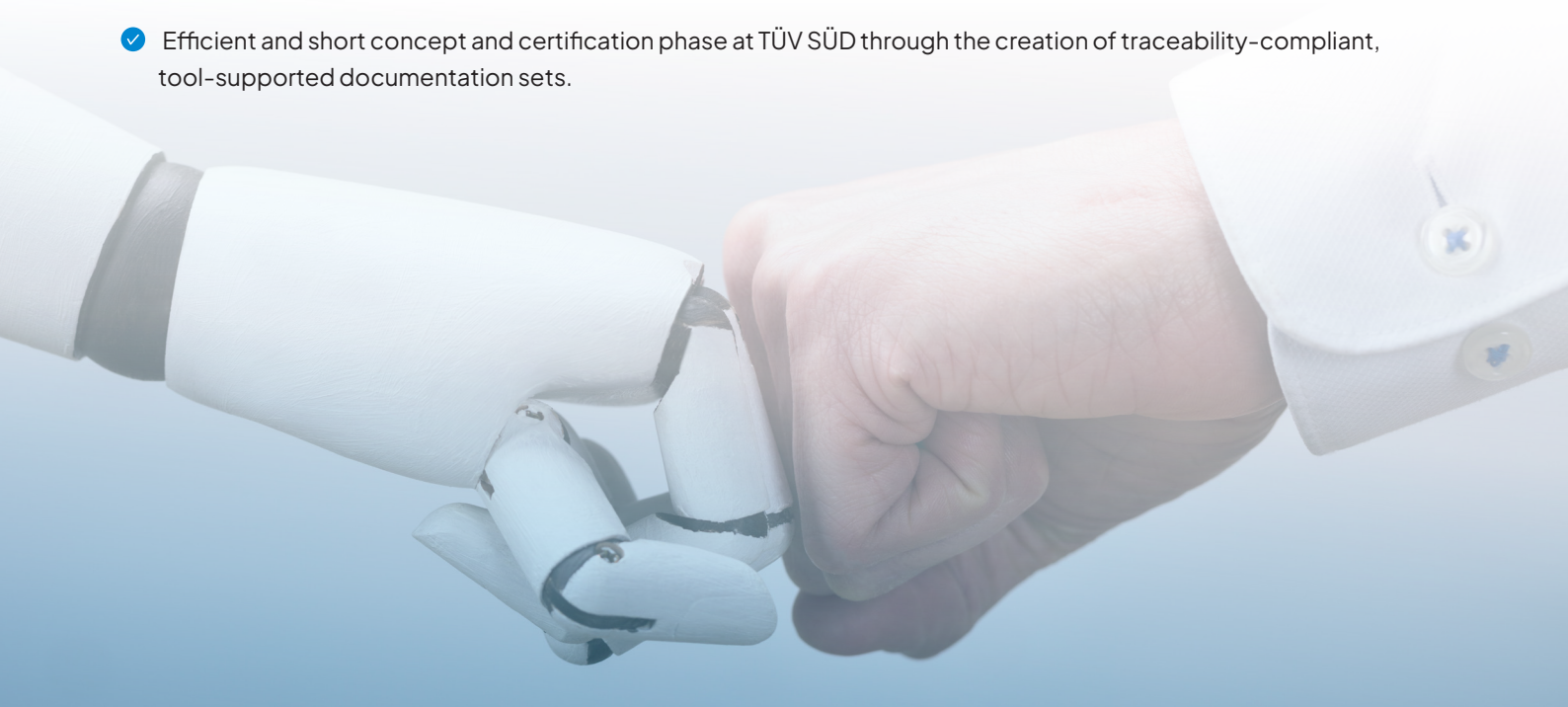
Thanks to the joint development with MESCO and the practical application of the standards, the necessary and relevant safety processes were quickly introduced in the customer company.

The short development time provides the decisive market advantage.



The key factors for success:

- ✓ Very close and trusting cooperation with a strong focus on the respective core competencies of the companies involved throughout the entire development period.
- ✓ Early implementation of the MESCO Safety Software prototypes on the Design Package Evaluation Board hardware to minimize risk and optimize project duration.
- ✓ Use of the MESCO Safety Design Package SW libraries, documentation templates and test procedures. This greatly reduces the development time by using the existing development artifacts.
- ✓ Use of common tool chains and security development processes for optimum coordination and collaboration in the development phases.
- ✓ Efficient and short concept and certification phase at TÜV SÜD through the creation of traceability-compliant, tool-supported documentation sets.



We develop for you!

...where ideas turn into success!

Press contact



Peter Bernhardt
Head of Sales & Marketing

Ph.: +49 76211575 441
peter.bernhardt@mesco-engineering.com

MESCO Engineering GmbH
Berner Weg 7
79539 Lörrach
Germany

Ph. +49 76211575 0
info@mesco-engineering.com
www.mesco-engineering.com