WHITEPAPER

Safety for AGV/AMR

Use of MESCO Design Packages

AGV/AMR safety is a new domain in which safety standards are applied. Many concepts and solutions from other areas can be reused. The MESCO design packages offer a good basis for a risk-minimized safety development in this domain.

AGV/AMR Safety Standards

Flexible automated guided vehicle and autonomous mobile robots have a rapidly growing market in the field of intra-logistics. There are special requirements for functional safety regarding IEC 61508 and ISO 13849. The relevant requirements for Safe AGV/AMR functions are based on ISO 3691-4. This product standard defines in its current version 29 safety related functions that can be used to reduce risk in processes involving:

- Safe stop and emergency stop
- Safe brake and safe parking
- Safe personnel detection system
- Safe speed supervision
- Safe stop during charging
- Safe load handling and stability supervision
- Safe automatic, manual and maintenance modes

The safety functions of the drive system of an AGV/AMR are related to IEC 61800-5-2. Some of the safety functions of this standard are listed below:

- STO: safe torque off
- SS1: safe stop 1
- SS2: safe stop 2
- SOS: safe operating stop advanced position functions
- SDI: safe direction advanced speed functions
- SMS: safe maximal speed
- SLS: safely-limited speed
- SSM: safe speed monitor brake functions
- SBC: safe brake control
- SBT: safe brake test

A mapping between ISO 3691-4 functions and the IEC 61800-5-2 functions is possible and depends on the area of application of a AGV/AMR. For this reason, the following table is an example of what this assignment may look like.

ISO 3691-4 / IEC 61800-5-2	STO, SS1	SOS, SS2	SDI	SMS	SLS	SSM	SBC, SBT
Safe stop and emergency stop	X	X					
Safe brake and safe parking	X	X					X
Safe personnel detection system			X	(X)	(X)		
Safe speed supervision				X	X	X	
Safe stop during charging	X	X					X
Safe load handling and stability supervision	X	X		(X)	(X)	(X)	X

AGV/AMR Safety

The requirements for the safety of AGVs/AMRs are derived from IEC 61508 as the basic safety standard and ISO 13849 as the sector standard. ISO 3691–4 provides the product standard for AGVs and AMRs.
All three standards should be considered. The required performance level (PLa-PLe) and SIL level (SIL1 - SIL4) are determined from:

- The risk graph of the standards
- The required failure probabilities PFH and PFD
- The required diagnostic coverage DC
- The minimum required performance level

Early considerations of these aspects are crucial for the selection of the safety solution independent of the domain where it is applied.

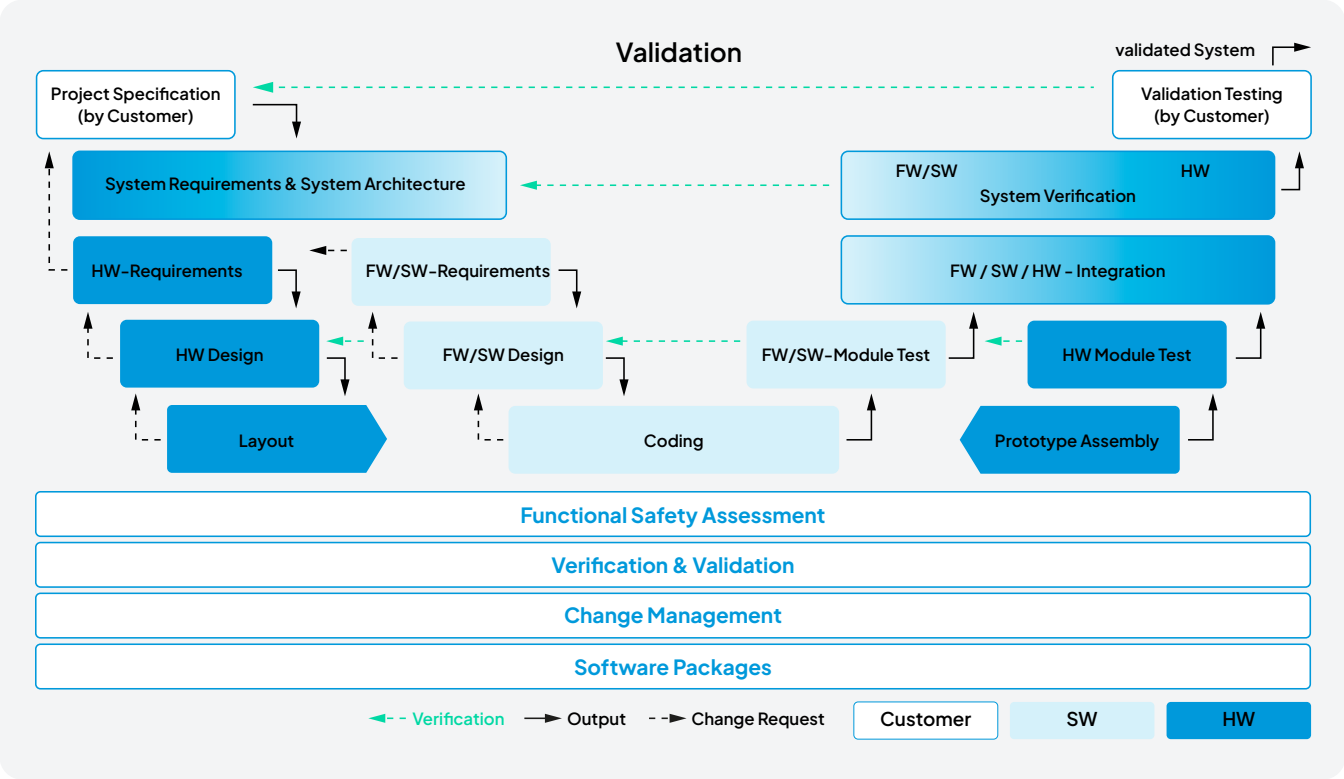
MESCO Design Packages up to SIL3 / CAT3 / PLe

MESCO has used the expertise gained over many years to create a platform that is the basis for all functionally safe developments. This platform consists of many different IP blocks from which a customized system can be developed at low cost and low risk.

How such a development can be carried out based on these IP blocks is briefly outlined in the following chapters.

MESCO Development Process

MESCO has a TUV certified development process following the V-Model according to IEC 61508 and ISO 9001. This reduces the risk and effort regarding additional process overhead needed for functional safety on customer side.



In a first phase in the collaboration with the customer the requirements are elaborated and written down in the requirements documents. This phase attempts to keep the development object as close to the existing IP blocks as possible. If required, a proof of concept can also be built up in a very early phase of the project on the basis of the existing evaluation module and the software to reduce risks and to get clarity on the requirements.

Subsequently, the development of the hardware and software is started, which integrates the existing IP blocks and implements additional customer-specific functionalities if required.

As the last major step of a development, the software and hardware are tested individually and are then put toge-ther to prove that the desired requirements are met. Once the complete V has been run through, this is the right time to discuss deviations and changes to the requirements and to start with a redesign of the product. Underly-ing the entire V-model are the supporting processes of functional safety such as Functional Safety Assessment.

MESCO (Safety) Design Packages

The modular platform of software/hardware artefacts can be used, for example, for the development of:

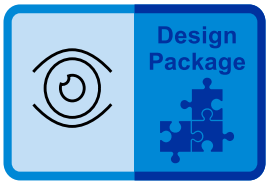
- Industrial Ethernet interfaces
- Functional safety systems up to SIL3 / CAT 3 / PLe
- Functional safety related remote I/O system
- Functional safety related drive systems

... and of course to develop AGV / AMR

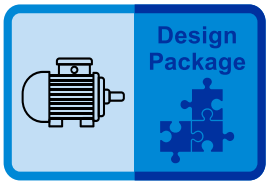
MESCO Hardware Evaluation Board

Your benefits

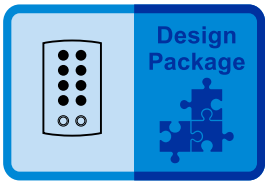
- Reduced development risk
- Project cost reduction
- Shorter time to market
- Easy protocol-certification
- TUV-certification



Sensors/Actors



Motion Control



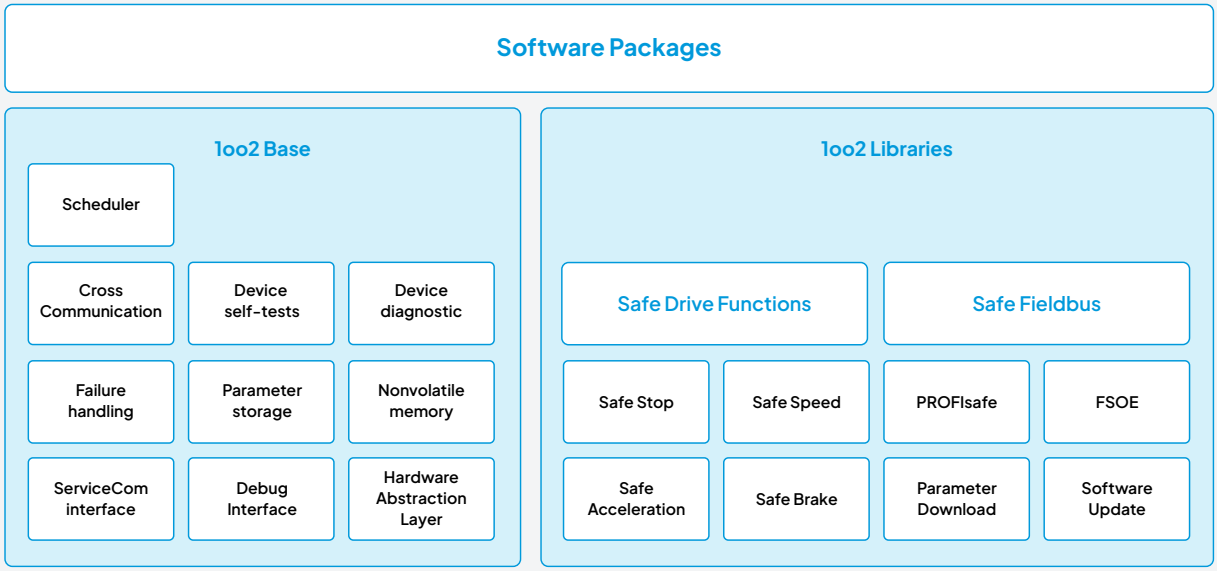
I/O Modules

The modular hardware platform consists of the following modules:

- Industrial Ethernet interfaces
- 1oo2 microcontroller cores (up to SIL3)
- 1oo2 modular Inputs / outputs / OSSD
- 1oo2 Brake / STO output
- Carrier Module with power supply
- Breadboard to integrate/connect customer specific electronics.

With these modules any functional safety system can be built and customer-specific hardware can be integrated just as easily. Of course, there are certain limitations due to the existing hardware evaluation modules, all of which have been solved so far, possibly through targeted reduction of the functionality on the evaluation modules. Since the evaluation modules divide the system into small parts, it is possible to redesign a part to support the full functionality of the target system.

MESCO Software Packages



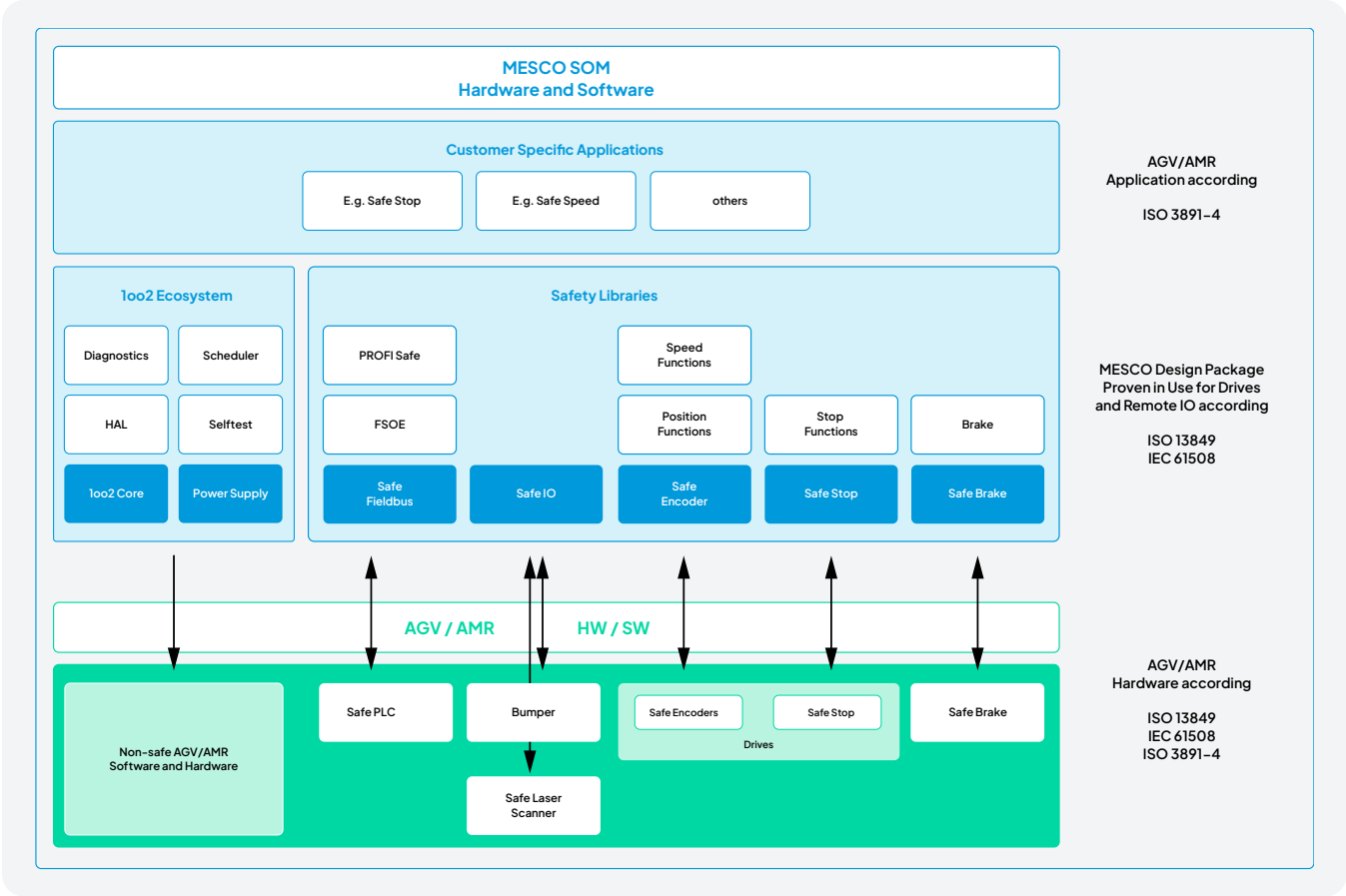
The modular software is developed according to IEC 61508 and ISO 13849 and split into two main portions:

- 1oo2 Base
  - Our own base system for all safety developments at MESCO
- 1oo2 Libraries (domain specific safety functions)
  - Safe drive functions according IEC 61800-5-2
  - Safe fieldbus according IEC 61784-3

Both parts are very modular and can be adapted to customer-specific circumstances. Due to the dependencies and functionalities of the 1oo2 base system, this is significantly more complex to implement than the 1oo2 libraries. That's why we highly recommend to not introducing any change in our base system. Changes and adjustments, on the other hand, are easy to implement in 1oo2 Libraries, for example, it is easy to add another safe communication protocol to the already existing ones we already support like PROFIsafe or FSOE.

Use of MESCO Design Packages for an AGV/AMR

The design packages for AGV/AMR are based on proven MESCO design packages including a 1oo2 ecosystem, safety libraries used for drives, remote I/Os and complex sensors and actors. The safety function listed in ISO 3891-4 will be realized on top of the underlying design package based on individual customer needs.



MESCO Safe AGV/AMR Monitor

The module is the hardware and software which is added to the AGV/AMR to enable safety features.
The module relies on safe sensor and actors on the AGV/AMR. The system can be split in:

Application Software

The safety related application functions will be developed by the customer or in close collaboration with the customer. The functions are implemented according individual needs by using the design package as functional base.

Design Package Software

The safety related software is reused in source code and is customized with appropriate glue code and configuration files. The customer application software will be integrated with the same reusable architecture concepts as the design package. The software consists of the 1oo2 ecosystem, which provides usage-independent functionality, and the 1oo2 libraries, which provide flexible safety functions.

Design Package Hardware

The safety related hardware will be reused on schematic level and customized in appropriate hardware extension and adaption to the customer needs. The SOM hardware can be a separated module or be integrated into a customer PCB.

AGV/AMR Software / Hardware

The non-safety parts and safety actor and sensors will be in full responsibility of the AGV/AMR supplier.
The SOM module uses suitable safe interfaces to implement the safety functions.

Use of MESCO Design Packages for AGV/AMR components

The Safe AGV/AMR Monitor may be also used to enable components of the AGV/AMR for safety.
Typical components may by safe drives, safe laser scanner and other complex parts.

MESCO Safe AGV/AMR Monitor (Evaluation Kit)

The evaluation kit consists of:

- Carrier board with 6 slots
- 1oo2 Safe Core (Redundant MCU)
- Safe Brake / STO board (Bipolar Output)
- Safe Input / Output board (Redundant IOs with feedback)
- Breadboard to integrate / attach customer specific hardware into MESCO's Platform

Glossary

SPDU	Safety Protocol Data Unit
AGV	Automated Guided Vehicle
AMR	Autonomous Mobile Robot
PLC	Programmable Logic Controller
SOM	Safety Option Module
PCB	Printed Circuited Board

Get in touch with us

We are looking forward to your inquiry.

Peter Bernhardt
Head of Sales & Marketing
Tel.: +49 7621 1575 0
peter.bernhardt@mesco-engineering.com

MESCO Engineering GmbH
Berner Weg 7
79539 Lörrach
Germany