CODESYS® Safety

DIN 61508 Safety software – solutions for all SIL2 and SIL3 applications, fully integrated in CODESYS.
CODESYS Safety

Tried and tested safety software

CODESYS is the leading IEC 61131-3 automation software. Programmable Logic Controllers (PLCs), ECUs/mobile controllers, panel controllers, motion controllers and additional automation devices in very different branches of industry are programmed with CODESYS. The deciding factor for the success of the tool is the complete integration of functionality, which otherwise usually requires additional software or hardware.

CODESYS integrates safety products for the project planning of machines and systems in accordance with the requirements of the machine guideline, EN/ISO 13849, IEC 62061 or IEC 61508. Each CODESYS Safety product is therewith exactly geared to the requirements of the respective branches of industry, such as e. g. to factory automation or the automation of mobile processing machines. These products are developed, validated and certified by prestigious institutions for proper use in accordance with IEC 61508.

With CODESYS Safety products manufacturers of safety controllers reduce the expenditure for the implementation of their safety controllers. This brochure gives device manufacturers the most important information about product selection and use.

Generation of executable application code for industrial controllers with integrated code generators on different architectures – for operating and safety functions. More than 2 million industrial applications throughout the world work with this technology.

Development and porting of runtime systems for different hardware or software platforms. The safety runtime systems developed in accordance with IEC 61508 are modular in design and can be easily implemented among others on TriCore-, ARM- or PowerPC systems.

Industry-specific technical requirements e. g. in the areas of production engineering, factory automation, mobile machines, and embedded systems are taken into consideration in the CODESYS Safety solutions. As a result these products are custom-tailored for the respective field of application.

Offer for provision of services for the implementation of devices with functional safety. That way initial hurdles can be overcome rapidly and the development of safety controllers with CODESYS Safety is assisted competently.

A reliable industrial partner for safety software

3S-Smart Software Solutions, the company behind CODESYS, is the main contact for manufacturers of safety controllers when it comes to safety software. CODESYS Safety clients can rely on the company’s extensive expertise and long years of experience:

- Generation of executable application code for industrial controllers with integrated code generators on different architectures – for operating and safety functions. More than 2 million industrial applications throughout the world work with this technology.
- Development and porting of runtime systems for different hardware or software platforms. The safety runtime systems developed in accordance with IEC 61508 are modular in design and can be easily implemented among others on TriCore-, ARM- or PowerPC systems.
- Industry-specific technical requirements e. g. in the areas of production engineering, factory automation, mobile machines, and embedded systems are taken into consideration in the CODESYS Safety solutions. As a result these products are custom-tailored for the respective field of application.
- Offer for provision of services for the implementation of devices with functional safety. That way initial hurdles can be overcome rapidly and the development of safety controllers with CODESYS Safety is assisted competently.
In any event, before selecting the right safety software there must be a risk analysis and/or definition of the field of application of the safety controller. Depending on the results of this analysis the appropriate CODESYS Safety product is selected.

The CODESYS Safety products - optimized for different performance requirements

In any event, before selecting the right safety software there must be a risk analysis and/or definition of the field of application of the safety controller. Depending on the results of this analysis the appropriate CODESYS Safety product is selected.

Fieldbus technology with integrated solutions for practically all popular systems. This makes a convenient integrated configuration of Profsafe, FSoE or CANopen Safety possible in combination with standard field bus systems.

Cooperation with leading certification institutions, such as e.g. TÜV SÜD and TÜV Rheinland. The experience gained helps in:
- shortening learning curves,
- realistic estimation of safety projects,
- meet institute requirements with 100% accuracy,
- effective development and approval of safety controllers – right up to certification in accordance with IEC 61508.

Separate team exclusively for the development of safer software products. Standard-compliant implementation of safety software as well as continuous further development guaranteed with specialists for:
- pre-project consultancy for device manufacturers
- qualified editors, project configurators and fieldbus protocols
- quality assurance as well as test automation for safety software
- standard-compliant processes in accordance with IEC 61508
- support in the implementation of the validated/certified safety runtime systems on the target device.

The programming model of the products is based on the definitions of the Technical Committee of the PLCopen Safety Group (Standardization group of IEC 61131-3 for safety requirements). Safety controllers can be programmed in basic level, extended level and/or system level. Depending on the programming level the language capabilities increase, conversely there is more responsibility for the approval of applications created with a higher programming level on the part of the user. The following holds true for all of our products: the project planning of operation and safety function is integrated in the CODESYS Development System within a project.
CODESYS Safety — a certified software to create an IEC 61508 SIL3 controller

CODESYS Safety simplifies the development of safety controllers as add-ons to existing PLC systems and their certification in accordance with IEC 61508 SIL3. CODESYS Safety is ideal for any platform from different manufacturers and is used, e.g., at Bosch Rexroth AG, Berghof Automationstechnik GmbH, Yacoub Automation GmbH, KEB GmbH, Kendrion Kuhnke Automation GmbH as well as at other well-known automation companies.

Safety controllers with CODESYS Safety are designed as add-ons to standard controllers. The system is dual channel (1oo2) and communicates via the standard controller with the CODESYS Development System as well as with non-secure I/Os. The programming takes place with a certified plug-in completely integrated in the CODESYS Development System.

Architecture of CODESYS Safety
Typical system structures

Safety controller as expansion module on a standard controller
- PROFIsafe F-Host and CIP Safety Originator as external expansion module

Remote safety controller on the network of the fieldbus system
- FSoE Master as EtherCAT modul
- Optional: safe cross-communication with other safety controllers (SafetyNetVars)

Integrated standard and safety controller within a device

Scope of supply
- Platform-independent runtime system toolkit (CODESYS Safety Runtime Toolkit) for dual channel hardware, pre-certified in accordance with IEC 61508 for applications in accordance with SIL3. Separate hardware abstraction layer – no subordinate operating system required
- CODESYS Development System, expanded by certified add-on package for application development in accordance with IEC 61508 SIL3
- Application-oriented function modules in accordance with PLCopen Safety for typical safety devices in factory automation such as e.g. emergency off buttons, two-handed operation, safety door, etc.
- Fieldbus support with separate certified implementations of FSoE (Failsafe over EtherCAT) and PROFIsafe (F-Host). Integration of additional protocols by customers possible (e.g. CIPSafety)
- Cross-communication between safety controllers (SafetyNetVars)
- TÜV approved safety integration and test manual which documents the integration interfaces incl. hardware abstract and adoptions
- Safety Verification Package: includes framework for OEM tests with CODESYS Test Manager generating automated test cases, instructions and reports.
- Approved safety manual for users
- Orientation workshop, consultancy and ongoing support
Required implementation steps

- Submission of safety concept to certification institute (recommended: TÜV Rheinland)
- Porting of the CODESYS Safety Runtime System to dual channel safety controllers (e.g. to ARM or TriCore) in accordance with integration manual. If necessary expansion by one’s own safety components (e.g. specific fieldbus protocol stack)
- Implementation of the hardware abstraction layer
- Module and integration test with the CODESYS Test Manager (together with extensive test script supplied with the CODESYS Safety Verification Package)
- System test of the finished device

Range of services

As a component of the CODESYS Safety Runtime Toolkit | Optional
---|---
- Communication of the fundamentals and presentation of the system interfaces within the scope of the orientation workshop
- Consultation for detailed solutions and procedure
- Final completion of the controller software:
  - Submission of safety concept to certification institute
  - Complete implementation of the CODESYS Safety Runtime System above the firmware level
  - Test development and performance
  - Creation of all required certification documents

The services of 3S-Smart Software Solutions end above the driver layer. Upon request we can put you in touch with possible partners for hardware and driver development.

Application of CODESYS Safety for the creation of SIL3 safety functions

- Safety controller: subnode of the standard controller with an application and task as well as global variable lists, POEs and logical I/Os
- Fieldbus configuration on the standard controller with reliable editors
- Configuration/mapping of secure I/Os on the safety controller with secure editor
- Test and debugging functions
- Programming according to user manual with integrated FBD safety editor (in accordance with IEC 61131-3 with certified qualification for IEC 61508 SIL3 applications) in basic/extended level with the help of certified components (IEC 61131-3 standard or in accordance with PLCopen Safety)
- Additional functions for the protection of the safety function, such as e.g. change tracking, safe signal flow, safe versioning (pinning), separation safe operation/debug mode, etc.

The services of 3S-Smart Software Solutions end above the driver layer. Upon request we can put you in touch with possible partners for hardware and driver development.

Application of CODESYS Safety for the creation of SIL3 safety functions
Integrated Safety editor for programming safety applications in the basic level

### Business model

- **Prerequisite:** CODESYS compatible standard controller
- **Purchase of the CODESYS Safety Runtime Toolkit:**
  - Runtime system as Software Developer Kit (SDK) for a platform including service
  - User workshop and ongoing support after implementation
  - CODESYS Development System with regular safety upgrades
  - CODESYS Verification Package
  - User manual
- **Yearly maintenance fee**
- **Optional safety components:**
  - Safety Fieldbus: CODESYS FSoE Master or CODESYS PROFIsafe Master/F-Host
  - Cross-communication add-on for Safety Controllers (Safety NetVars)
  - Factory Function Package including PLCopen Safety function block library
  - Expanded range of services according to OEM specifications and/or OEM customized CODESYS including tests on OEM systems
- **Purchase of runtime licenses per safety controller**

### The benefits of a SIL3-Safety controller with CODESYS Safety

- **Approved safety concept** → fewer iteration cycles to certification institute
- **Numerous tested functions** available as product for the software portion of a safety controller → Safety controller can be implemented significantly faster
- **Integrated project planning** of the safety function in the standard IEC 61131-3 programming system → accustomed convenience in the project planning and data exchange between the safety and operation function
- All aspects for the implementation of the safety function include: programming, configuration of secure fieldbuses, secure library modules → no separate add-on software required
- **Pre-fabricated automated tests** for the complete safety runtime system → Time savings for tests
- By using a software product validated/pre-certified in accordance with IEC 61508 SIL3 substantially reduced time and effort in the implementation of the software part of a safety controller
CODESYS Factory

CODESYS Development System
- Programming SIL3-Safety function with validated editors
- Additional safety function
- Commissioning/Maintenance Service/Diagnosis
- Integrated in the standard IEC 61131-3 development system

CODESYS Visualization
- CODESYS HMI / CODESYS WebVisu
- Machine/system visualization
- Data logger/Data distributor
- Diagnosis/Remote maintenance/Commissioning

Ethernet

CODESYS Control
- Standard controller
- Processing of the operation function
- Fieldbus master
- Communications gateway for safety controller
- optional: CODESYS TargetVisu

SIL3 Safety controller as expansion module

Standard I/O Terminal

Remote SIL3 Safety controller

Standard fieldbus with secure protocol layer (Proflbus/Profisafe/Profinet or EtherCAT/FSoE)

CODESYS Control Safety (SIL3)
- Processing of the SIL3 safety function
- Safety communication (Profisafe/FSoE)

CODESYS Visualization
- CODESYS TargetVisu
- Machine visualization/Diagnosis

CODESYS Factory

CODESYS Development System
- Programming SIL2 safety function with validated editors
- Additional safety function
- Commissioning/Maintenance Service/Diagnosis
- Integrated in the standard IEC 61131-3 development system

CODESYS Visualization
- CODESYS TargetVisu
- Machine visualization/Diagnosis

CANopen with secure Protocol Layer CANopen Safety
CODESYS Safety for EtherCAT Safety Module

Integrated project planning of safety applications in accordance with IEC 61508 SIL3 with certified safety logic terminal

CODESYS Safety for EtherCAT Safety Module is a certified product for users and device manufacturers who do not have their own safety controllers.

Only the EtherCAT Safety Module and a CODESYS standard controller with EtherCAT are required for use.

No adjustments, toolkits or add-on software are necessary.

Typical system structure (simplified):

The EtherCAT Safety Module can be used together with safety I/Os anywhere on the network.

The Beckhoff TwinSafe Logic Controller EL6900 is integrated in the EtherCAT network for the use of CODESYS Safety for EtherCAT Safety Modules. Programming and configuration of the safety I/Os take place after an upgrade directly in the CODESYS Development System via a controller with CODESYS EtherCAT Master. If necessary, the safety logic terminal can be integrated into one’s own product line by arrangement with the manufacturer (Brand-Labeling).

Scope of supply

- Upgrade of the CODESYS Development System for integrated development of the safety function with a proven FBD editor. Range of functions tailored to the possibilities of the safety logic terminal
- I/O configuration or mapping with safe editor
- Library for access to internal safety function blocks of the EtherCAT safety module with typical safety functions of factory automation, such as e.g. emergency off, safety door monitoring, two-hand control
- Data exchange with the standard controller
- Certified user documentation
Implementation

CODESYS Safety for EtherCAT Safety Modules is delivered as a CODESYS package and installs seamlessly in the CODESYS Development System. A license on the main controller is required for application, but no additional software. The product is certified for use of the EtherCAT Safety Module in applications of factory automation up to SIL3 in accordance with IEC 61508 or DIN EN 13849 PLe.

Integrated creation of safety functions with EtherCAT safety logic terminal

In the CODESYS Development System the safety logic terminal is configured as a fieldbus device in the tree of the EtherCAT network together with the standard and secure I/Os. The safety function is implemented in the safety application below. Communication with the standard controller takes place via special network variables.

The user programs the safety function with the safe FBD editor integrated in the CODESYS Development System. The available safety components of the terminal are consolidated in a library.

Business model

- Prerequisite: CODESYS compatible standard controller with CODESYS EtherCAT
- Purchase of individual licenses for CODESYS Safety for EtherCAT Safety Modules per standard controller.
  Included in delivery:
  - Package for the CODESYS Development System with all required safety upgrades including safety function component library.
  - User manual

The benefits of CODESYS Safety for EtherCAT Safety Module

- Easy upgrade of standard controllers by a SIL3 certified safety controller without time-consuming adjustments
  - Immediately available safety add-on for device manufacturers and users
- Programming of operation and safety function with the same development system
  - Project planning and data exchange without add-on software
- Change operation function or fieldbus configuration without influencing the safety function
  - Reduced certification expenditure for the entire application
- Safety logic terminal on the EtherCAT network freely scalable
  - Cost-effective implementation tailored to the application

Diagram:

- Standard controller
- Variables for data exchange
- EtherCAT Master
- Safety controller EL6900
- Safety POU
- Safety Inputs
- Safety Outputs
- Program (POU) (Estimated Level 0)
CODESYS Safety SIL2 – Software for safe mobile controllers/ECUs

CODESYS Safety SIL2 simplifies the development of safety controllers for use in mobile work machines and facilitates certification in accordance with SIL2 (IEC 61508) or Pld (EN ISO 13849). It is based on the standard CODESYS Development System as well as the CODESYS Control Runtime System, in each case expanded by qualified safety concepts.

Manufacturers of mobile controllers such as Inter Control GmbH & Co. KG and Sensor-Technik Wiedemann GmbH choose this solution to be able to offer their clients qualified software for safety applications.

The implementation of safety controllers in accordance with SIL2/Pld requires the implementation of the CODESYS Control SIL2 Runtime System in accordance with the certified integration manual. A safety plug-in adds to the functionality of the CODESYS Development System. Access to safe I/Os via CANopen Safety can be realized with the portable protocol stack. Configuration of the CANopen/CANopen Safety network takes place with the integrated configurator.
### Recommended system architectures of the safety controller

<table>
<thead>
<tr>
<th>Standard CPU / Lockstep CPU</th>
<th>Standard CPU / Lockstep CPU</th>
<th>Lockstep &amp; Standard CPU</th>
<th>Lockstep CPU &amp; Watchdog</th>
<th>Lockstep &amp; Standard CPU &amp; Watchdog</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Architecture 1" /></td>
<td><img src="image2.png" alt="Architecture 2" /></td>
<td><img src="image3.png" alt="Architecture 3" /></td>
<td><img src="image4.png" alt="Architecture 4" /></td>
<td><img src="image5.png" alt="Architecture 5" /></td>
</tr>
<tr>
<td>PLd Cat. 2</td>
<td>PLd Cat. 2</td>
<td>PLd Cat. 2</td>
<td>PLd Cat. 3</td>
<td>PLd Cat. 3</td>
</tr>
</tbody>
</table>

### Scope of supply

- **Platform-independent toolkit (CODESYS Safety SIL2 Runtime System Toolkit)** for single channel or dual channel hardware – pre-certified in accordance with IEC 61508 SIL2 or EN ISO 13849 PLd (Category 2 or 3)
- Development system: CODESYS Development System including compilers for different CPU platforms (including TriCore/ARM/PowerPC), expanded by safety components. Certified suitability for application development in accordance with IEC 61508 SIL2/EN ISO 13849 PLd
- Fieldbus support with separate configurator and protocol stack for CANopen Safety (master/slave), support of mixed operation of CANopen Safety and CANopen devices
- CODESYS Safety Verification Package: TÜV approved certification concept/integration manual for controller firmware, test framework, automated test scripts for verification of the runtime system and the CODESYS compiler
- TÜV approved safety manual for users
- Orientation workshop and consultation

### Required implementation steps

- Submission of safety concept to certification institute (recommended: TÜV SÜD)
- Porting of the CODESYS Control SIL2 Runtime System on the safety controller in accordance with integration manual.
- Development of custom firmware extensions, protection of safe parts from standard components through MMU/MPU. Optional: Usage of the fully adapted and precertified project files from the CODESYS Safety SIL2 PSP for different CPU platforms (e.g. Texas Instruments RM48)
- Module and integration test with the CODESYS Test Manager. A license for this add-on tool comes supplied together with extensive test scripts of the CODESYS Safety Runtime Toolkit.
- Implementation of self tests, hardware test as well as general safety functions of the controller
Range of services

<table>
<thead>
<tr>
<th>CODESYS Safety SIL2 Runtime Toolkit</th>
<th>Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Communication of the fundamentals and presentation of the system interfaces within the scope of the orientation workshop</td>
<td></td>
</tr>
<tr>
<td>• Consultation for detailed solutions and procedures</td>
<td></td>
</tr>
<tr>
<td>• Support in the implementation of the CODESYS Control Runtime System</td>
<td>• Submission of safety concept to certification institute</td>
</tr>
<tr>
<td></td>
<td>• Complete implementation of the CODESYS Control Runtime System above the firmware level</td>
</tr>
<tr>
<td></td>
<td>• Test development and performance</td>
</tr>
<tr>
<td></td>
<td>• Creation of all required certification documents for CODESYS integration</td>
</tr>
</tbody>
</table>

Upon request additional services can be undertaken by external partners.

Creation of safety functions with CODESYS Safety SIL2

- Dependent on the system architecture:
  - Development of a secure overall application.
  - Development of safety function and operation function separately in different applications.
- Development in IEC 61131-3 in accordance with certified user manual with the standard editors FBD/LD/ST in basic/extended/system level. Support for most standard functions of the CODESYS Development System (e.g. remote visualization, trace, monitoring, etc.)
- Additional functions:
  - Safe operation/debug mode
  - Display page for safety information
- Fieldbus configuration with reliable CANopen-Editor

Typical project structure: safety and operation function separated in different applications
**Business model**

- Purchase of the CODESYS Safety SIL2 Runtime Toolkit with:
  - Runtime system as Software Developer Kit (SDK) for a platform including service
  - CODESYS Development System with SIL2 Safety upgrades
  - CODESYS Safety SIL2 Verification Package
  - User manual
- Optional: Purchase of the CODESYS Safety SIL2 PSP (Platform Support Package) with:
  - CODESYS Safety SIL2 Runtime Toolkit
  - fully adapted and precertified project files for the SIL2 runtime system
  - Test scripts for final integration tests
- Optional: CODESYS CANopen/CANopen Safety
- Optional: expanded range of services to customer specifications
- Purchase of runtime licenses per safety controller

**The benefits of CODESYS Safety SIL2**

- Certified safety concept of a tested software product ⇒ fewer iteration cycles to certification institute
- Hardware-independent implementation ⇒ support of different system architectures
- Complete test framework for secure runtime system functions ⇒ fast time-to-market
- Optional integrated CANopen/CANopen Safety fieldbus connection ⇒ no add-on software required
- Integrated project planning of the safety function in the standard IEC 61131-3 development system ⇒ familiar user convenience in project planning
- Substantially reduced time and effort in the implementation of the software part of an IEC 61508 SIL2/EN ISO 13849 PLoD Safety controller with validated/pre-certified software product

CODESYS Safety SIL2 is used in safety critical applications, including in mobile cranes.
CODESYS – the manufacturer-independent
IEC 61131-3 automation software.

CODESYS Product Families:

- Engineering
- Visualization
- Fieldbus
- Motion + CNC
- Runtime
- Services

CODESYS® is a registered trademark
of 3S-Smart Software Solutions GmbH.
Technical specifications are subject to change. Errors and omissions excepted. No reproduction or distribution, in whole or in part, without prior permission.

Note: Not all CODESYS features are available in all territories. For more information on geographic restrictions, please contact support@codesys.com.