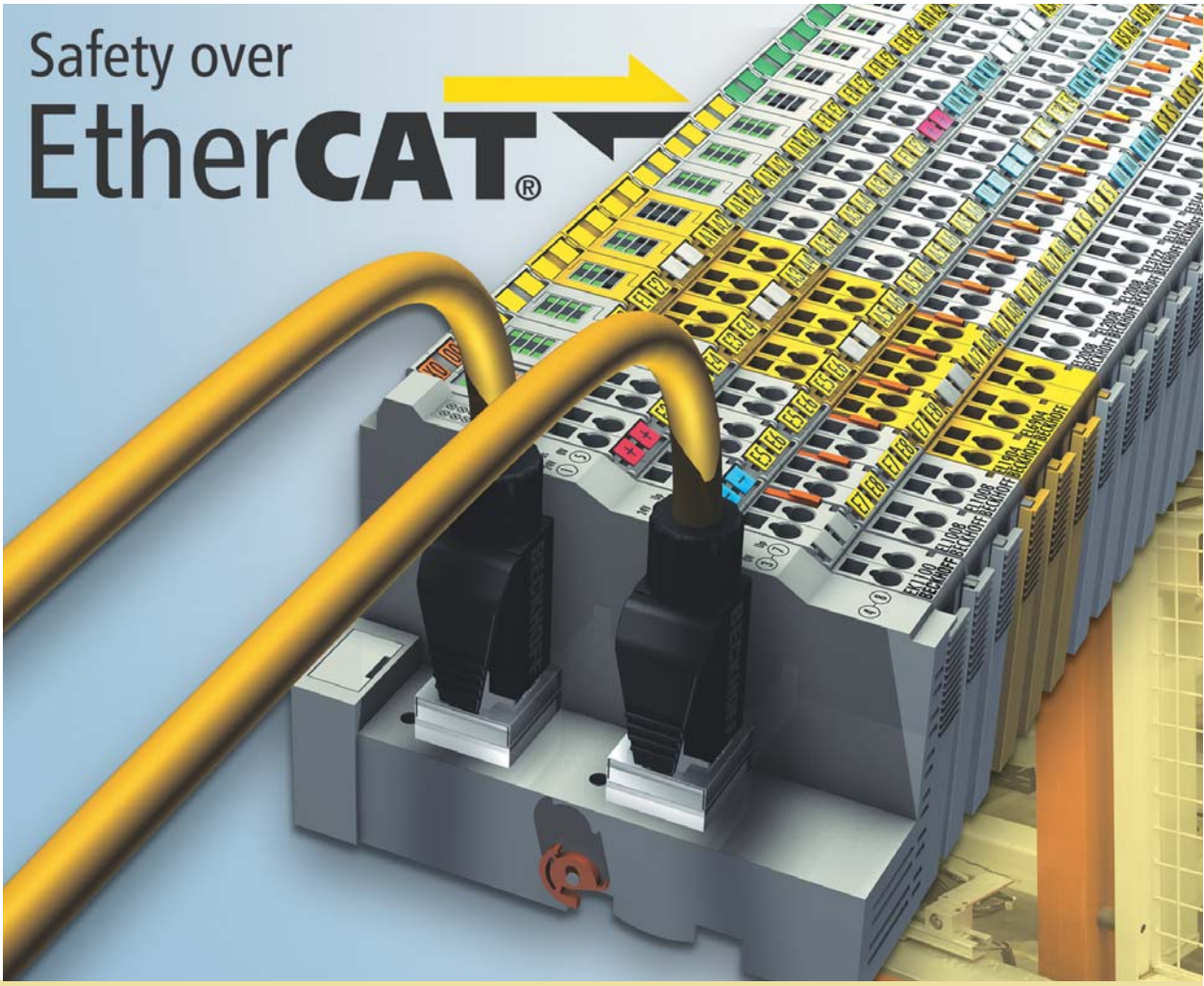
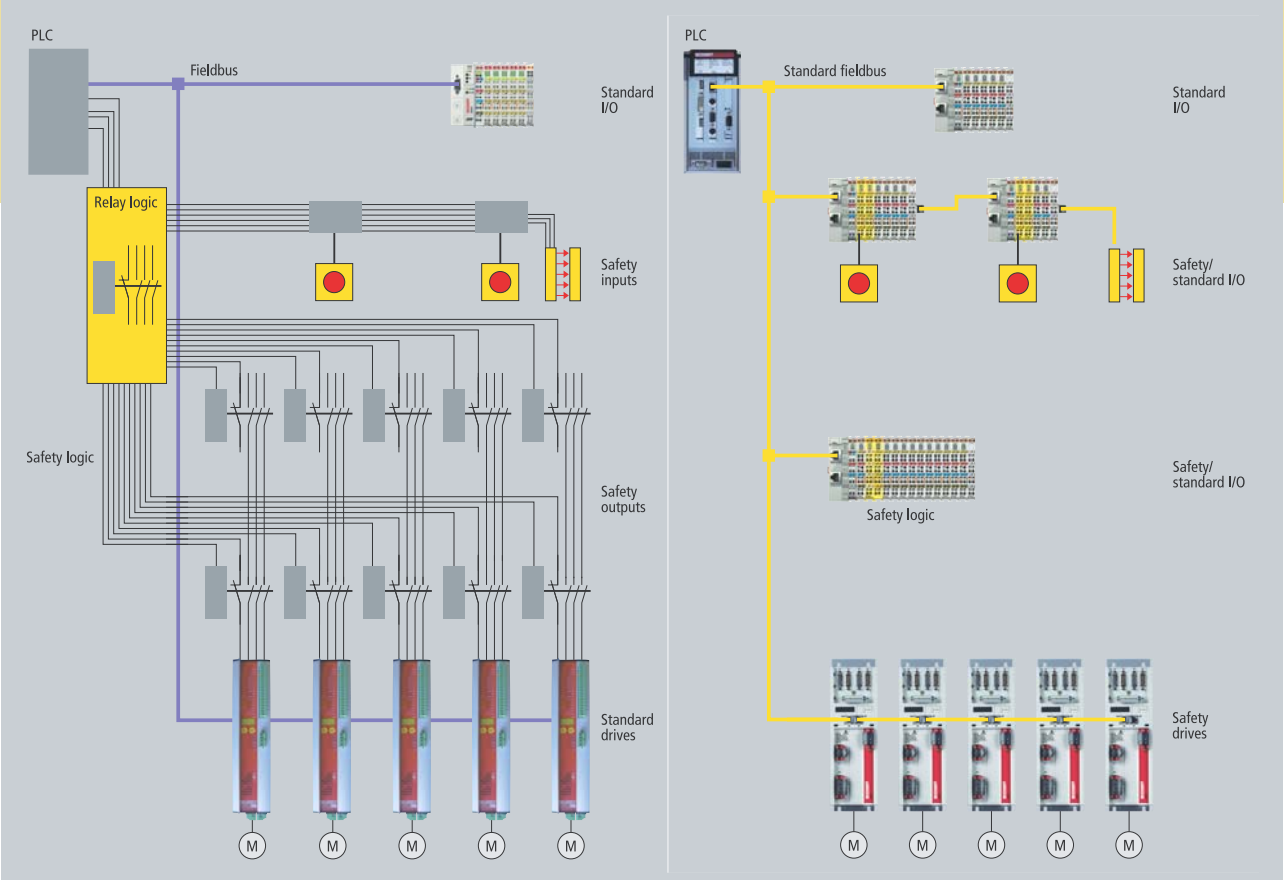
The safety solution for EtherCAT



Advanced communication systems not only offer deterministic transmission of control information, they also enable transfer of safety-relevant data over the same medium. The solution for EtherCAT is based on the Safety over EtherCAT protocol.

"The machine design is ready!" Mr. Almostsafe says, pleased. However, his colleague, Mr. Safe points out that for CE conformity, "...the manufacturer is obliged to carry out a risk analysis in order to determine all risks associated with the machine..." Mr. Almostsafe is therefore required to extend the safety measures on his machine following a risk analysis.
This example reflects common attitudes towards functional machine safety today. Safety functions are developed separately from automation functions and only integrated into the machine concept at a later stage. This often leads to cumbersome and inflexible solutions that may even restrict machine operation. In addition, with a safety function that limits the functionality of the machine, there is always a risk that the user will circumvent the function, thereby making it ineffective and unsafe.
Safety sensors such as light curtains, safety door monitoring devices or two-hand control units are generally monitored via a number of evaluation devices, which themselves have an effect on the safe outputs via inflexible relay logic. Redundant mains and/or motor contactors are installed in the drive cables so that they can be controlled moment-free for switching off dangerous motion.

However, there is a trend in a new direction: Intelligent safety solutions in the automation components and communication systems enable integration of safety technology into the machine design. In the sphere of safe-



Conventional safety technology compared with advanced machine concepts with integrated safety function

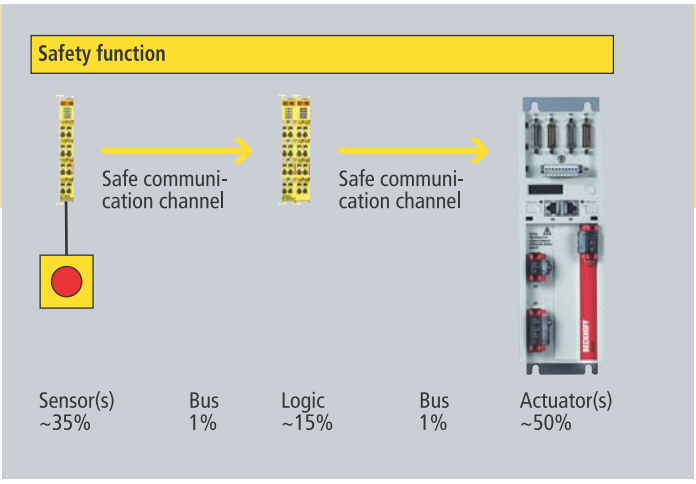
ty sensors these are safety devices that already integrate functional extensions such as muting. Recent developments include camera-based sensor systems with spatial monitoring functions that enable new operator/machine interaction options for area protection. For the evaluation and safety logic – in addition to "large" safety controllers – small, local logic devices are already offered that are scalable to suit the respective task. Inflexible relay logic thus becomes a thing of the past. Drive technology also offers integrated safety functions for fast stopping of the drive with short response time, and for safe monitoring of functions such as safe velocity limitation.

One of the factors enabling this kind of integration is safe data communication between components. Safe transfer is specified in the Safety over EtherCAT protocol described below.

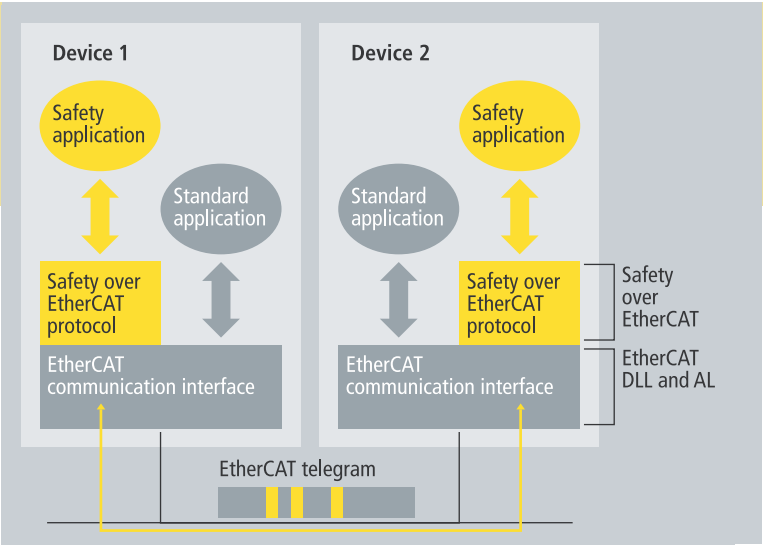
The standards world also started addressing the new circumstances as a basic prerequisite and enables determination of the safety level for software-based, programmable safety devices (see IEC 61508, IEC 62061, ISO 13849).

The benefits:

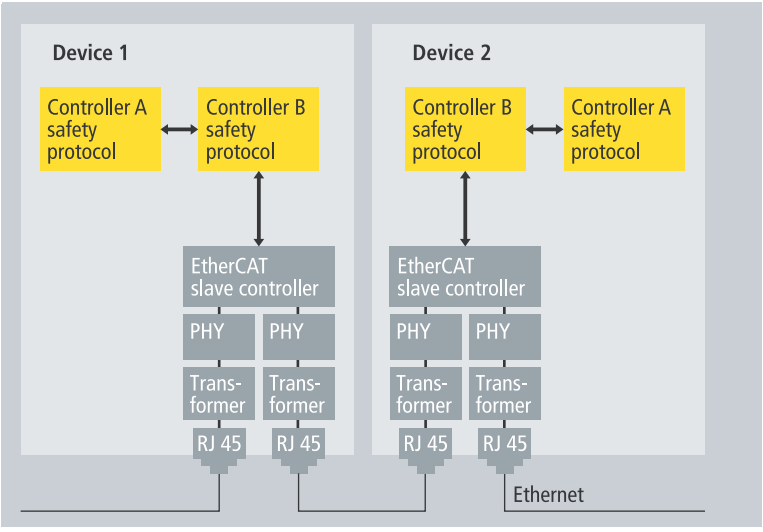
- Seamless integration of the security safety concept into the machine design
- No separate development tools for standard and safety application
- Simple handling and transparent safety functions
- Very good diagnostic options for the safety functions
- Single communication system for control and safety information
- No performance limitations in terms of real-time and determinism
- Flexible expansion options



Distribution of residual fault rate in a safety system



Safety over EtherCAT software architecture



Safety over EtherCAT hardware architecture

Safety over EtherCAT

In the interest of realizing safe data communication over EtherCAT, the Safety over EtherCAT protocol has been disclosed within the EtherCAT Technology Group (ETG). The following features were crucial in the development of this protocol:

- Compliance with SIL 3 of IEC 61508
- Safe and non-safe information on the same communication system
- Independence of the protocol from the transfer system and medium
- The length of the safe process data is not restricted by the protocol.
- Very short frame lengths are possible.
- No limitations with regard to transfer speed and cycle time

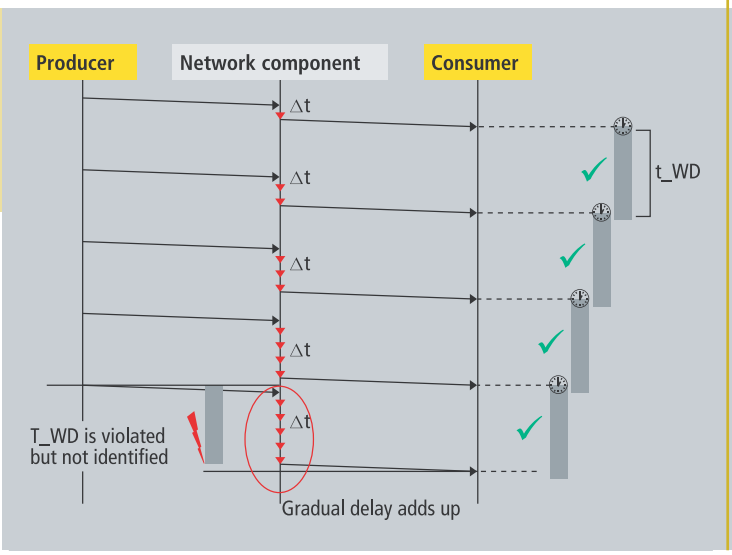
Compliance with the requirements of IEC 61508 SIL 3 is essential for unrestricted application in industrial automation. For the bus system this means that the dangerous residual error probability of $< 10^{-9}$ per hour must be met. This corresponds to 1 % of the residual error rate of $\geq 10^{-8}$ to $< 10^{-7}$ required for SIL 3 in a system with stringent requirements; the other 99 % are reserved for other safety components such as sensors, safe logic and actuators involved in realizing the safety function. Incidentally, $< 10^{-9}$ per hour means that no dangerous error must occur and remain undetected during continuous operation over 100,000 years.

EtherCAT is used as a single-channel communication system for transferring safe and non-safe information. The transport medium is regarded as a "black channel" and not included in safety considerations. A safety frame containing the safe process data and the required data backup is included in the EtherCAT process data. This "container" is safely analyzed in the devices at the application level. Communication remains single-channel. This corresponds to Model A from the Annex of pre-IEC 61784-3. This standard, which is currently being finalized, describes requirements for the transfer of safety-relevant messages in industrial networks.

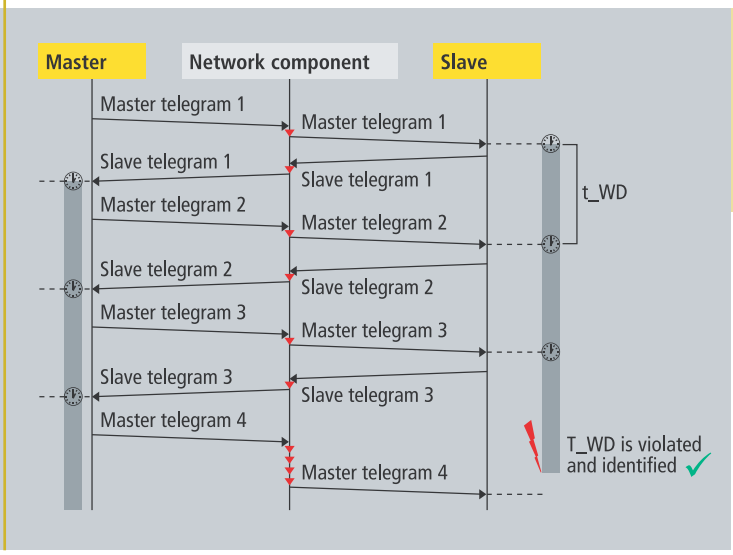
The calculation of the residual error probability for the Safety over EtherCAT protocol takes no credit from the error detection mechanisms of the communication system. This means that the protocol can also be transferred via other communication systems. This is utilized, for example, in internal sub-bus systems for modular I/O system components, which have a Bus Coupler for connection to the control bus system and have their own sub-bus for gathering the process image of the I/O components used. The EtherCAT Bus Coupler can forward the safety frame without restrictions to the safe I/O terminals via the sub-bus.

Description of the Safety over EtherCAT technology

A basic principle for testing and certification of bus systems for transferring safety-relevant messages was first presented in 2000 by the HVBG electrical engineering committee. The basic testing principle specified in the current version



With pure time monitoring between producer and consumer, the accumulated delay in a network component leads to an undiscovered, dangerous error.



Master/slave relationship with watchdog; all dangerous delays are safely detected.

[GS-ET-26] is the basis for the international pre-IEC 61784-3 standard. This standard defines the following error assumptions for such a network: corruption, repetition, interchanging, loss, delay, insertion, masquerading and invalid addressing of messages. A safety protocol must be able to handle all these errors via suitable measures, i.e. they must be detected according to the required safety category.

The message delay assumption is particularly relevant for Ethernet-based systems. The application of non-safety-certified infrastructure components such as switches or routers creates scope for message delays. Even time monitoring (watchdog) of arriving messages is not sufficient.

The chart (above) shows a producer/consumer relationship. The consumer monitors cyclic arrival of messages from the producer with the aid of a watchdog. In the network component, the messages are delayed by Δt in each cycle, which is not detected by the watchdog. If this delay accumulates over several cycles, the consumer can no longer detect that a message is outdated beyond the permitted level. In the worst case, this could mean that an emergency stop request from a sensor (producer) does not arrive at the drive (consumer) until several minutes later.

One measure for controlling such errors is the introduction of a global time and message transfer with a timestamp. However, it should be noted that it may not necessarily be possible to use a time synchronization mechanism that may already exist in the communication system: The synchronization must additionally cover the safety protocol level.

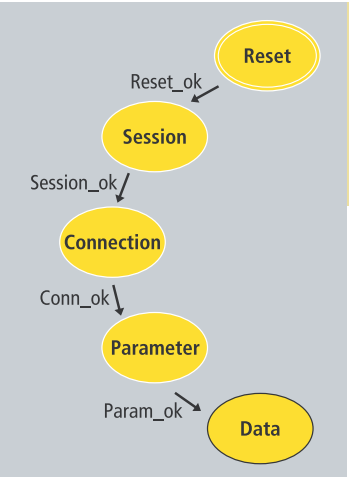
Safety over EtherCAT therefore uses a simpler method. A unique master/slave relationship between two devices, the Safety over EtherCAT connection, can ensure that each device only returns its own new message once a new message has been received. The complete transfer path between master and slave is thus monitored in each cycle; accumulation of delay times is eliminated or detected. This enables very "lean" implementation of the protocol, with moderate requirements in terms of communication system access, since no hard timings for time synchronization have to be adhered to. The fact that this may lead to increased data traffic in the network is non-critical due to the available bandwidth and is not a disadvantage in practice.

For controlling the other errors, the Safety over EtherCAT protocol also includes:

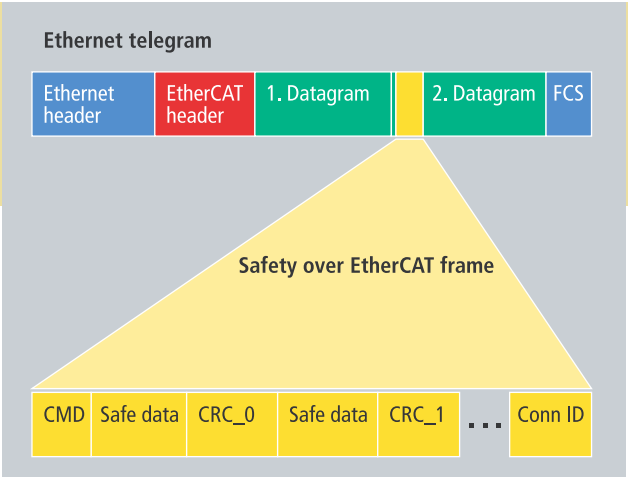
- **A session-number**
  for detecting buffering of a complete startup sequence.
- **A unique connection ID and a unique slave address**
  for safely detecting misrouted messages via a unique address relationship.
- **A CRC checksum**
  for detecting message corruption from source to sink. In addition, this technique enables interchanging of information within the safety container to be detected, for example, if the container was split en route. The properness and suitability of the code and the required independence from the subordinate communication have been verified.
- **A sequence number**
  for detecting interchange, repetition, insertion or loss of whole messages.

Via suitable procedures, the frame is designed such that a minimum container length of 6 bytes is sufficient for transferring all error detection and correction information, including one byte of safe process data. Incidentally, the protocol does not impose any limits regarding the length of safe process data. This means that safety components with many safe process data are also supported. For example, in addition to safe state information, a safe drive may also transfer the internally determined safe position, safe speed and/or safe torqueAnd there is no limit regarding the minimum cycle time of the container. With appropriate selection of the error detection and correction information, the transfer rate has no influence on residual error probability for the Safety over EtherCAT protocol.

During startup of a Safety over EtherCAT connection, a state machine is processed both in the master and in the slave.



Safety over EtherCAT state machine for a master/slave connection

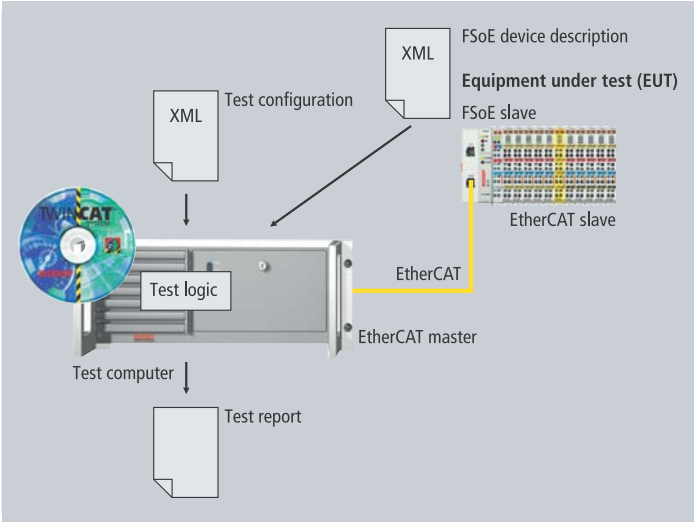


Embedding of the Safety over EtherCAT frame in the EtherCAT process data

Here too, the focus was on a simple structure in order to make implementation as simple as possible. State transitions are initiated by the master and acknowledged by the slave. The state also involves exchange and checking of information for the communication relation. The watchdog time is exchanged in the *parameter* state, for example. This time is strongly dependent on the transmission link and on the safety devices and therefore has to be configured individually. Safe application parameters can also be transferred from the master to the slave in this state. This enables safe central data management in the master. The application parameters can be up to 2^{16} bytes long per connection, which is sufficient for transferring a configured protective field of a laser scanner, for example.

The safe output state can only quit in the *data* state. This state is the normal operating state for exchanging safe input and output data. If one of the devices detects a communication relation error during startup or data exchange, it changes to reset state, thereby resetting the connection.

Configuration of a Safety over EtherCAT conformance test



Certification

The Safety over EtherCAT protocol has been assessed by German Technical Inspection Agency (TÜV). It is certified as a protocol for transferring process data between Safety over EtherCAT devices up to SIL 3 according to IEC 61508. The implementation of the Safety over EtherCAT protocol in a device must meet the requirements of the safety target. The associated product-specific requirements must be taken into account.

Any transmission link can be used, including fieldbus systems, Ethernet or similar transfer routes, optical fiber cables, copper cables, or radio links. There are no restrictions or requirements for Bus Couplers or other devices located along the transfer route.

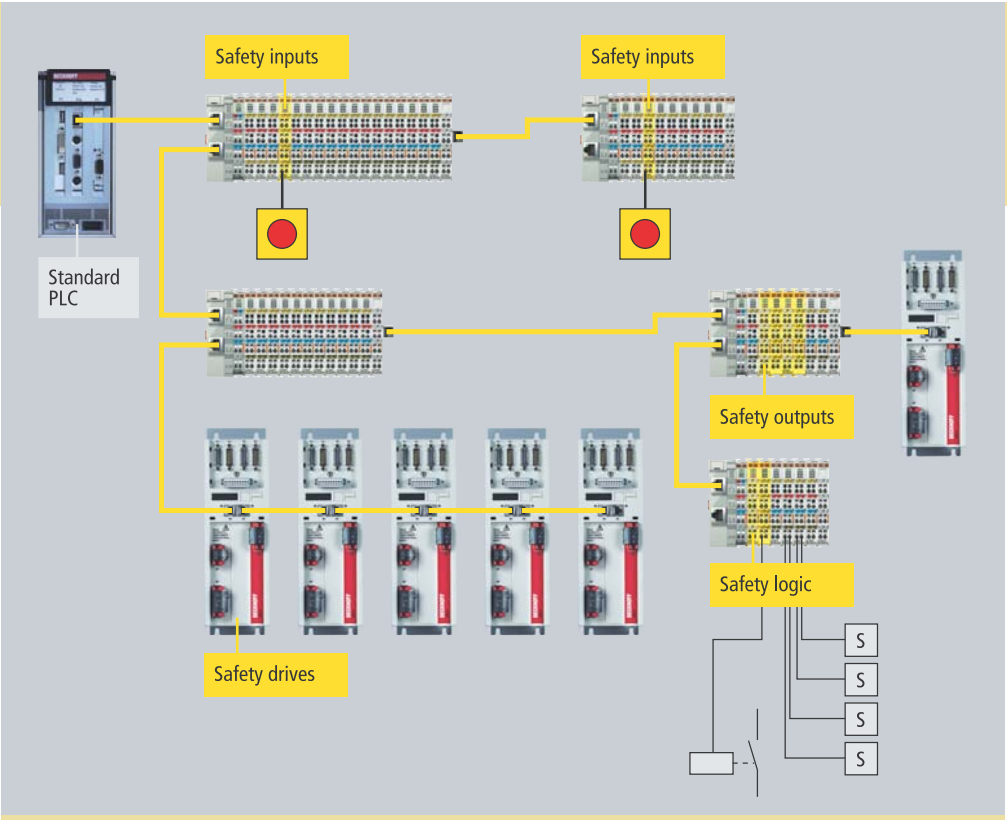
A conformance test for supporting implementation of the protocol in devices is currently being developed. This test is a pure protocol test for checking the behavior of the safety protocol via the communication interface of a test device (black box test).

The first step is reading the device description file of the test device in order to determine the possible parameters for the test. Test scripts from a configuration can then be executed on a standard PC. The test device is subjected to correct and faulty frames and the response is compared with an expected result. A test report summarizes the results of the individual test steps.

The test cases are reviewed and approved by a test center and can be used by the device manufacturer for ensuring conformity with the protocol specification. The establishment of an independent conformance test laboratory has been proposed. This laboratory will carry out tests and certify conformity. The certification authority of the device manufacturer is thus able to approve the safety functionality of this protocol. However, the test does not cover the implementation (e.g. two-channel calculation) of the Safety over EtherCAT protocol. As for safe application of the device, this has to be done by the manufacturer according to the requirements of the safety target of the certifying authority.

Summary

- Safety over EtherCAT describes the safety protocol for EtherCAT.
- The protocol has no restrictions with regard to safe process data length, communication medium, or transfer rate.
- EtherCAT is used as a "black channel", i.e. the communication system plays no part in the safety considerations.
- The protocol has been specified and reviewed and meets the requirements of IEC 61508 SIL 3.
- Products offering the Safety over EtherCAT protocol have been available since 2005.



Sample application for TwinSAFE system with Safety over EtherCAT protocol

Application example

The safety and functionality of a safe transfer protocol can only be proven through implementation of the specification in a product. Devices with Safety over EtherCAT have been available since 2005. Safety over EtherCAT is therefore one of the first Industrial Ethernet real-time communication systems supporting a safe protocol.

This application (see example above) utilizes the benefits of the technology. The safety components are deployed wherever they are required in the automation system. Scalable local input and output components can be used in the system. An additional input or output can be extended flexibly using safety and non-safety Bus Terminals as required.

The safety logic is also embedded within the network strand. A standard PLC can thus continue dealing with control tasks without a safety extension. Safe input and output functions are linked in the local safety logic in the form of an intelligent, safe Bus Terminal. This saves the costs otherwise required for an expensive safety PLC and enables scaling of the logic according to the task at hand. Only the messages between the Safety over EtherCAT master and the allocated safe slaves are routed via the non-safe, standard PLC.

Beckhoff currently offers three safe I/O components: an input terminal with four safe inputs, an output terminal with four safe outputs, and a Logic Terminal with configurable safety logic and four local safe outputs. Safety-relevant parameterization of the devices can be implemented via a safe configuration tool integrated in the standard programming environment (TwinCAT). Finally, the resulting safe parameter set is uploaded (password-monitored) to the safe logic terminal. During each startup, the Logic Terminal distributes the safe application parameters to the configured input and output terminals. This enables simple exchange of input and output terminals without having to adapt or reload the configuration.