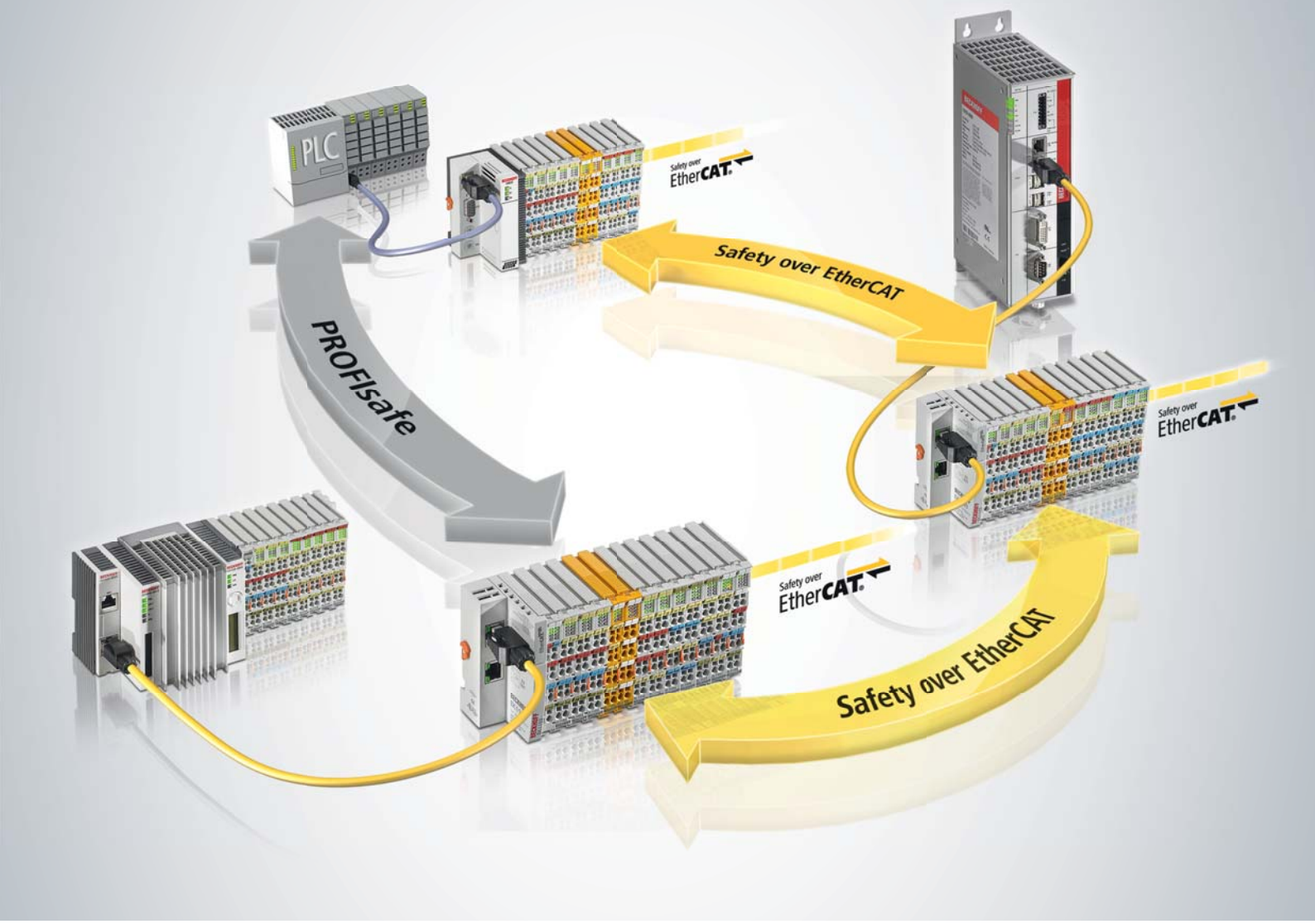


Universal safety solution

Safety over EtherCAT as the basis for plant-wide safety architectures

Production facilities are frequently plants that consist of several process steps, which are each performed by separate machine modules. The local safety functions of the machine modules are usually solved within that module. In addition, safety information must be exchanged plant-wide between the machine modules in order, for example, to implement comprehensive emergency stop functions or to inform upstream and downstream modules about the activation of the stop functions. The TwinSAFE product range from Beckhoff offers intelligent solutions on the basis of the Safety over EtherCAT protocol, both within a module and for plant-wide networking.

Modern safety architectures use safe networks

Even today the safety-relevant coupling of the devices still takes place in many machine concepts via an I/O connection: Safety sensors such as light curtains, protective door monitors or two-hand operating devices are monitored by a large number of evaluation devices, which in turn act on the safe outputs via relatively inflexible relay logic.

However, a clear trend can be discerned toward the use of communication systems with safety-relevant transmission. Intelligent safety sensors, such as laser scanners or camera-based monitoring systems as well as drives with integrated safe monitoring and shutdown functions, can be connected via a safety bus to safe logic. The use of such a safety bus results in benefits for the safety architecture like those that are already familiar from the introduction of standard fieldbus systems:

– short reaction times and thus increased machine safety
– very good (channel-specific) diagnostic options
– flexible expansion options
– clear machine architecture

If all safeguards for the detection of transmission errors are encapsulated in a "safety container," then the use of a safety protocol is possible irrespective of the standard communication system employed. Any data security measures used for the communication layer are not taken into account for the safe transmission: this is known as the "Black Channel principle." The advantage of this is that safety-relevant and standard process data can be transmitted in the same communication system. IEC 61784-3 defines the requirements for safety communication based on the Black Channel principle and describes various safety protocols.

Author: Dr. Guido Beckmann, Technology Marketing, Beckhoff

Safety over EtherCAT is one such safety protocol as standardized in IEC 61784-3. The TwinSAFE product range from Beckhoff uses this protocol for safety data transmission. Additional benefits arise for the user, including:

– uniform communication system for standard and safety-relevant data
– routing of the safety protocol via standard gateways, backplane buses, other fieldbus systems or even wireless
– use of decentralized safety logic and retention of the standard PLC for machine control
– additional use of the safe process data in the standard controller
– greater variety of devices due to the use of a widespread and standardized protocol

The TwinSAFE terminals available in the EtherCAT I/O system exploit EtherCAT's high performance to the maximum: as a result, up to 128 safety-related bus devices up to SIL 3, according to EN IEC 61508, and DIN EN ISO 13849-1 PLe can be connected to the EL6900 Safety PLC in the compact housing of an electronic terminal block with a width of just 12 mm. The safety PLC features 256 integrated function blocks that can be configured or programmed depending on the application. 24 V DC digital input terminals (EL1904) and 24 V DC digital output terminals (EL2902 – 2.3 A and EL2904 – 0.5 A) are available for connecting the safety sensors or actuators respectively. The EL6900 Safety PLC can also be used as a safety controller for the Beckhoff AX5000 Servo Drives with the safety drive option card AX58xx, which are linked via EtherCAT.

Plant structures

A plant for the production of cabinet walls is an example of a typical modular structure: a module for feeding the plant with new particle boards, a strip saw and a flying saw for cutting to length, various drilling and milling machines as well as an edge machining unit. These modules are mechanically connected, for example, by roller conveyors that lead to a stacking or packaging unit at the end. The interaction of the machine modules – guided by a master controller, which specifies which cabinet part must be produced – is realized via a plant-wide network. If the machine modules use the same communication system, then this is referred to as a homogeneous communication structure. If, however, the plant is made up of modules from different manufacturers, then different communication systems may be used internally under certain circumstances. We call this a heterogeneous plant structure.

Safety functions within machine modules

The safety functions of the machine modules are usually solved within the module. For example, if a stop function must be initiated when a protection cover is opened, then the hazardous movements inside the module are stopped safely (e.g. by stopping the saw blade). The safety controller processes the input information from the sensors and determines the safe reactions at the outputs or actuators.

Detailed information about the status and the functional capability of the components involved is necessary within the machine module for this. Depending on the triggering input signal, different reactions must be triggered at the actuators.

Safe gateway functionality integrated into the Safety PLC

In addition, channel-specific diagnostic information is important for the user in order to react as fast as possible to a detected error. If a defective sensor is discovered, for instance via cross-circuit detection, then a specific safe function is activated for this sensor and the user's attention can be drawn specifically to the faulty device.

Factory-wide safety architecture

Safety information must also be exchanged plant-wide between the machine modules in order, for example, to implement comprehensive emergency stop functions or to inform upstream and downstream modules about the activation of stop functions. Ideally all areas that are visible from an emergency stop button are stopped by activating this button. In a dangerous situation it is irrelevant whether or not the emergency stop button is mounted on the machine module in which the danger is recognized – what is important is a fast reaction.

For the loading and unloading of a station it is additionally necessary to exchange safety-relevant information about the upstream or downstream module. For example, the exchange of material may only be enabled if no user is in the shared danger zone.

At the plant-wide machine communication level, therefore, it is not important to exchange channel-specific information for the individual sensors and actuators; much more important are the safety-relevant overall status of a machine module and the central activation of safety functions. The interface to each machine module is thus usually effected via pre-processed, filtered information; this means it is lean and can be standardized via an open interface profile.

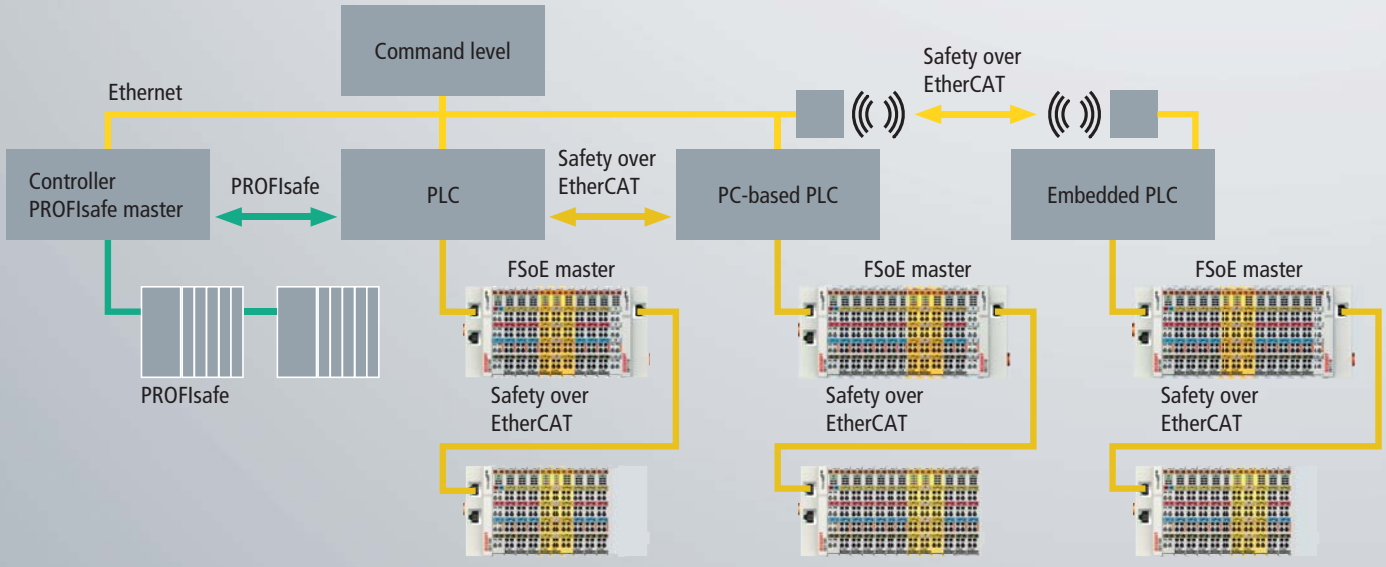
Heterogeneous communication structure

Communication at field level increasingly uses Ethernet-based real-time communication systems for the exchange of I/O data to and from the actuators and sensors. Various technologies for this have established themselves on the market: EtherCAT, PROFINET, EtherNet/IP and others. At the master computer or the machine network level, individual machine modules are combined to form a production plant. The machine parts are usually coupled via higher-level master-to-master communication; the machine controller acts as a gateway between the internal communication system and the higher-level control system.

The safety-relevant coupling of the machine parts is governed by similar boundary conditions. Taking into account the different native safety protocols of the established bus systems within the machine modules, a safe gateway function is required for the plant-wide networking of the modules.

In connection with this the approach of implementing plant-wide safety functions by a generic, bus-independent safety protocol is frequently the subject of discussion. However, the implementation of a bus-independent safety protocol is technically difficult and entails several significant restrictions:

– The certification of a device with a safe communication interface is complex, since the device manufacturers require proofs of conformity and suitable tools for each communication system in order to implement a safety protocol. These are provided by the fieldbus organizations for the native safety protocols. For a generic protocol, however, proofs of conformity would be required from several non-cooperating organizations.



Homogeneous and heterogeneous communication architecture with Ethernet at the command level: an open safety interface profile enables a standardized exchange of safety-related data between the machine modules.

- Device manufacturers will preferentially implement the native safety protocol for the supported bus interface in order to successfully place the device in the market for this communication interface.
- The costs of each safety device would increase if a second safety protocol had to be supported in addition to the native safety protocol.
- Since not all device manufacturers would support several safety protocols, the choice of devices would be reduced for the user and the overall costs would worsen.

The Beckhoff TwinSAFE system therefore offers a solution that allows different safety protocols to be used at precisely one place inside the machine module: in the safety controller, which is present in each machine module anyhow.

The safety controller monitors many connections to safe communication partners within the machine module. If this controller supports a further safety protocol for one or more of these connections, it can act as a safe gateway. To this end the EL69xx Safety PLC is supplemented with the ability to create the connection to another device using not only Safety over EtherCAT, but also another safety protocol, e.g. PROFIsafe (EL6930).

Standardized interface profile

A profile specification is currently being elaborated within the EtherCAT Technology Group (ETG) that defines an application profile for the exchange of data between the modules and the command level above the safety protocols. The data concerned here are the compressed and pre-processed safe process data that a machine module delivers to the outside or receives from the outside.

When two machines "converse" with one another, it is not important to the neighbor whether this or that drive is in a safe state or whether an emergency stop button has been pushed. What is actually of interest, however, is – to put it simply – the information as to whether the neighboring plant has a safety problem and, if that is actually the case, whether the plant equipment can continue to produce parts. This means that the actual scope of safety information that needs to be represented outside a plant module is quite manageable.

The contents of the interface profile are, for example, the general safety-relevant machine state of a module, the information about whether the module was safely stopped, or perhaps also a higher-level emergency stop request. If this information is reflected in the form of a control or status word in a fixed place at the interface, then considerable advantages arise through pre-defined function blocks and reusable diagnostic options.

As opposed to a generic safety protocol that would additionally have to be integrated into all devices, the gateway function need only be realized once in a machine module, and with the EL69xx the safety gateway does not even have to be a self-contained device, but can be implemented as a sub-function of the safety controller.

Further Information:
www.beckhoff.com/Safety
www.beckhoff.com/FSoE