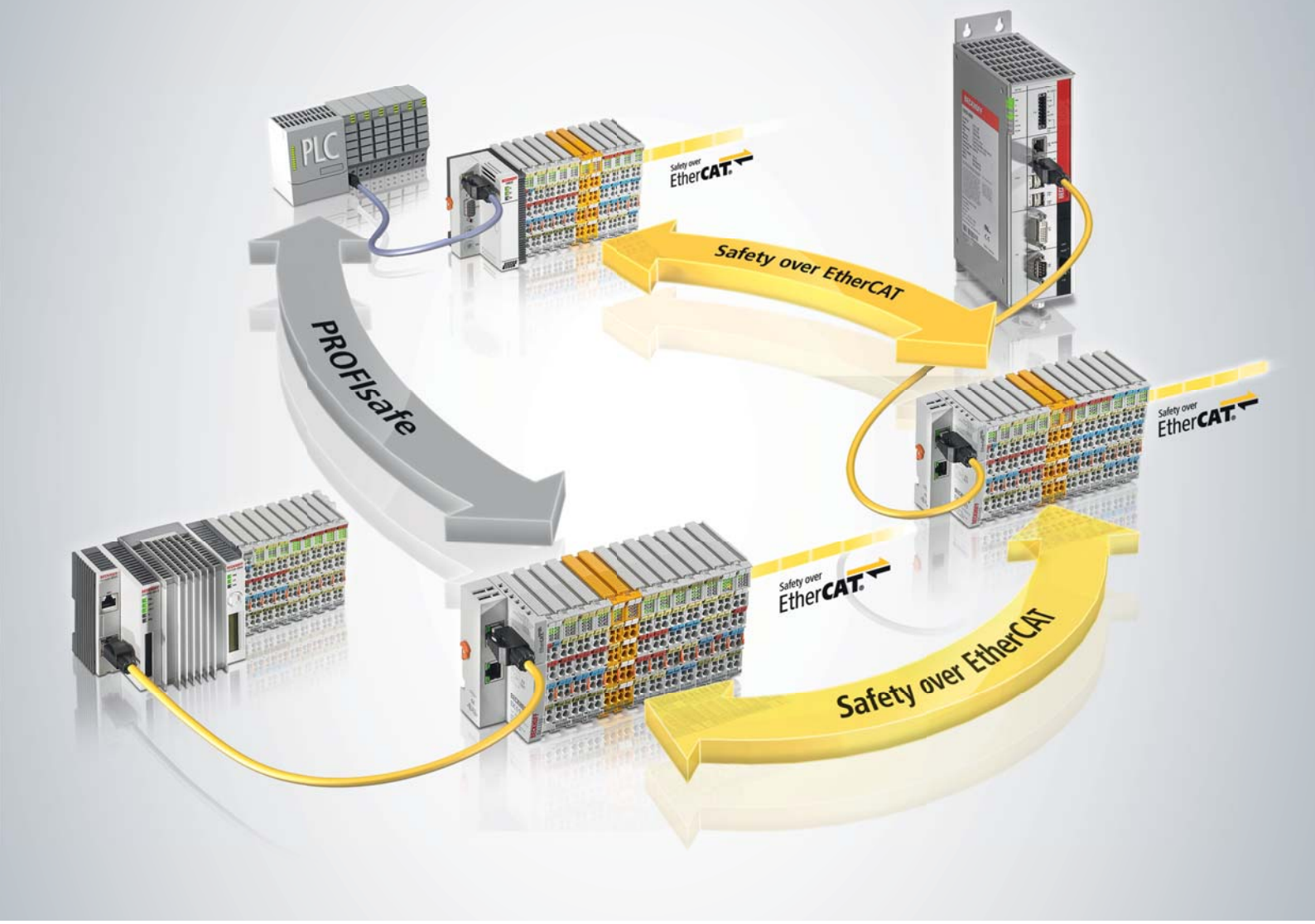


Durchgängige Safety-Lösung

Safety-over-EtherCAT als Grundlage für eine anlagenweite Sicherheitsarchitektur

Produktionsanlagen bestehen häufig aus mehreren Prozessschritten, die jeweils von separaten Maschinenmodulen ausgeführt werden. Die lokalen Sicherheitsfunktionen der Maschinenmodule werden in der Regel innerhalb des Moduls gelöst. Anlagenweit müssen zudem zwischen den Maschinenmodulen Sicherheitsinformationen ausgetauscht werden, um z. B. übergreifende Not-Aus-Funktionen zu realisieren oder um Vorgänger- und Nachfolgemodule über die Aktivierung von Stillstandfunktionen zu informieren. Die TwinSAFE-Produktreihe von Beckhoff bietet sowohl innerhalb eines Moduls also auch für die anlagenweite Modulverknüpfung intelligente Lösungsmöglichkeiten auf Basis des Safety-over-EtherCAT-Protokolls.

Moderne Sicherheitsarchitekturen nutzen sichere Netzwerke

Die sicherheitsrelevante Kopplung der Geräte erfolgt in vielen Maschinenkonzepten auch heute noch durch eine I/O-Verschaltung: Sicherheitssensoren, wie Lichtgitter, Schutztürüberwachungen oder Zweihandbediengeräte, werden über eine Vielzahl von Auswertegeräten überwacht, die wiederum über eine relativ unflexible Relaislogik auf die sicheren Ausgänge wirken.

Es ist allerdings ein klarer Trend zur Nutzung von Kommunikationssystemen mit sicherheitsrelevanter Übertragung zu erkennen. Intelligente Sicherheitssensoren, wie Laserscanner oder kamerabasierte Überwachungssysteme, sowie Antriebe mit integrierten sicheren Überwachungs- und Abschaltfunktionen können über einen Sicherheitsbus an eine sichere Logik angeschlossen werden. Durch die Verwendung eines solchen Sicherheitsbusses ergeben sich Vorteile für die Sicherheitsarchitektur, wie sie von der Einführung der Feldbussysteme im Standardbereich bekannt sind:

- kurze Reaktionszeiten und damit erhöhte Sicherheit der Maschine
- sehr gute (kanalspezifische) Diagnosemöglichkeiten
- flexible Erweiterungsmöglichkeiten
- übersichtliche Maschinenarchitektur

Wenn alle Sicherungsmaßnahmen zur Aufdeckung von Übertragungsfehlern in einen „Safety-Container" gekapselt werden, ist die Verwendung eines Sicherheitsprotokolls, unabhängig vom verwendeten Standard-Kommunikationssystem, möglich. Gegebenenfalls verwendete Datensicherungsmaßnahmen des Kommunikationslayers werden für die sichere Übertragung nicht berücksichtigt: Man spricht hier vom „Black-Channel-Prinzip". Dies hat den Vorteil, dass sicherheitsrelevante und Standard-Prozessdaten auf dem gleichen Kommunikationssystem übertragen werden können. In der IEC 61784-3 werden die Anforderungen für eine sichere Kommunikation, basierend auf dem Black-Channel-Prinzip, definiert und verschiedene Sicherheitsprotokolle beschrieben.

Autor: Dr. Guido Beckmann, Technologie-Marketing, Beckhoff

Safety-over-EtherCAT ist ein solches sicheres Protokoll, das in der IEC 61784-3 standardisiert ist. Die TwinSAFE-Produktreihe von Beckhoff nutzt dieses Protokoll zur sicheren Datenübertragung. Für den Anwender ergeben sich zusätzliche Vorteile:

- einheitliches Kommunikationssystem für Standard- und sicherheitsrelevante Daten
- Routing des Sicherheitsprotokolls über Standard-Gateways, Rückwandbusse, andere Feldbussysteme oder auch per Funk
- Nutzung einer dezentralen Sicherheitslogik und Beibehaltung der Standard-SPS zur Maschinensteuerung
- Nutzung der sicheren Prozessdaten auch in der Standardsteuerung
- Gerätevielfalt durch die Verwendung eines weitverbreiteten standardisierten Protokolls

Die TwinSAFE-Klemmen für das EtherCAT-I/O-System nutzen die hohe Performance von EtherCAT optimal aus: So lassen sich an die Safety-PLC EL6900, im Gehäuse einer nur 12 mm breiten elektronischen Reihenklemme, bis zu 128 sicherheitsrelevante Busteilnehmer bis SIL 3, nach EN IEC 61508, und DIN EN ISO 13849-1 Ple anschließen. In die Safety-PLC sind 256 Funktionsbausteine integriert, die – je nach Anwendung – konfiguriert oder programmiert werden. Für den Anschluss der Sicherheitssensoren bzw. -aktoren stehen Digital-Eingangsklemmen (EL1904) für 24 V DC sowie Digital-Ausgangsklemmen (EL2902 2,3 A und EL2904 0,5 A) für 24 V DC zur Verfügung. Die Safety-PLC EL6900 ist auch als Sicherheitssteuerung für die über EtherCAT angebundenen Beckhoff-Servoverstärker AX5000 einsetzbar.

Anlagenstrukturen

Eine Anlage zur Produktion von Schrankwänden ist ein Beispiel für eine typische, modulare Struktur: ein Modul zur Beschickung der Anlage mit neuen Spanplatten, eine Streifensäge sowie eine fliegende Säge zur Ablängung, verschiedene Bohr- und Fräsautomaten sowie eine Kantenbearbeitungseinheit. Mechanisch verbunden werden diese Module z. B. durch Rollenbahnen, die zu einer Stapel- oder Verpackungseinheit am Ende führen.

Die Interaktion der Maschinenmodule – geführt durch eine Leitsteuerung, die vorgibt, welches Schrankteil gefertigt werden soll – wird über eine anlagenweite Vernetzung realisiert. Nutzen die Maschinenmodule das gleiche Kommunikationssystem, sprechen wir von einer homogenen Kommunikationsstruktur. Wenn die Anlage aber aus Modulen von unterschiedlichen Herstellern zusammengestellt wird, kommen unter Umständen intern unterschiedliche Kommunikationssysteme zum Einsatz. Wir bezeichnen dies als eine heterogene Anlagenstruktur.

Sicherheitsfunktion innerhalb der Maschinenmodule

Die Sicherheitsfunktionen der Maschinenmodule werden in der Regel innerhalb des Moduls gelöst. Muss zum Beispiel, durch das Öffnen einer Schutzklappe, eine Stoppfunktion ausgelöst werden, dann werden die gefahrbringenden Bewegungen innerhalb des Moduls sicher stillgesetzt (z. B. durch Stillsetzen des Sägeblattes). Die Sicherheitssteuerung verarbeitet die Eingangsinformationen der Sensoren und bestimmt die sicheren Reaktionen an den Ausgängen bzw. Aktoren.

Sichere Gateway-Funktionalität integriert in der Sicherheits-SPS.

Hierfür sind innerhalb des Maschinenmoduls detaillierte Informationen über den Status und die Funktionsfähigkeit der beteiligten Komponenten notwendig. Abhängig vom auslösenden Eingangssignal müssen unterschiedliche Reaktionen an den Aktoren ausgelöst werden. Zudem sind kanalspezifische Diagnoseinformationen für den Anwender wichtig, um möglichst schnell auf einen detektierten Fehler reagieren zu können. Wird ein defekter Sensor entdeckt, etwa über eine Querschluss-Erkennung, dann wird für diesen Sensor eine spezifische sichere Funktion aktiviert und der Anwender kann gezielt auf das fehlerhafte Gerät hingewiesen werden.

Fabrikweite Sicherheitsarchitektur

Auch anlagenweit müssen zwischen den Maschinenmodulen Sicherheitsinformationen ausgetauscht werden, um z. B. übergreifende Not-Aus-Funktionen zu realisieren oder um Vorgänger- und Nachfolgemodule über die Aktivierung von Stillstandfunktionen zu informieren. Idealerweise werden alle von einem Not-Aus-Taster einsehbaren Bereiche durch die Aktivierung dieses Tasters stillgesetzt. In einer Gefahrensituation ist es unerheblich, ob der Not-Aus-Taster an dem Maschinenmodul angebracht ist, in dem die Gefahr erkannt wird, oder nicht – wichtig ist eine schnelle Reaktion.

Für das Be- und Entladen einer Station ist es zudem notwendig, sicherheitsrelevante Informationen zum Vorgänger- bzw. Nachfolgemodul auszutauschen. Ein Materialaustausch darf beispielsweise nur freigegeben werden, wenn sich kein Anwender in der Gefahrenzone befindet.

Auf Ebene der anlagenweiten Maschinenkommunikation ist es daher nicht wichtig, kanalspezifische Informationen der einzelnen Sensoren und Aktoren auszutauschen; vielmehr sind der sicherheitsrelevante Gesamtstatus eines Maschinenmoduls und die zentrale Aktivierung von Sicherheitsfunktionen von Bedeutung. Die Schnittstelle zu jedem Maschinenmodul erfolgt also in der Regel durch vorverarbeitete, gefilterte Informationen; sie ist damit schlank und kann über ein offenes Schnittstellenprofil standardisiert werden.

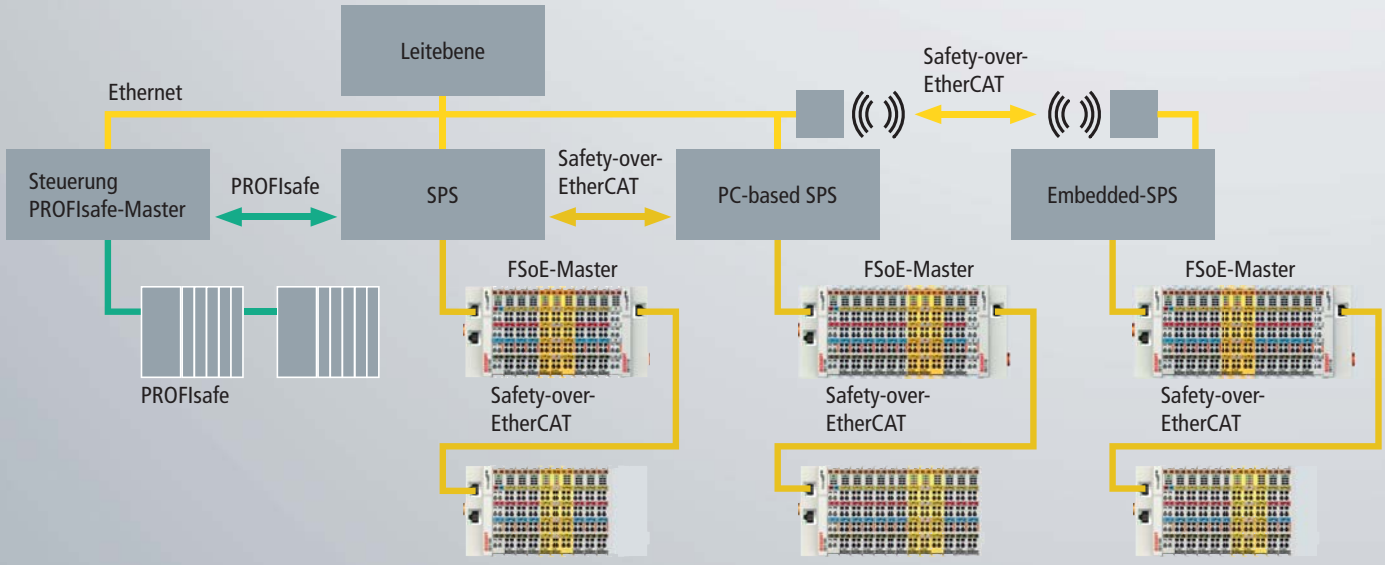
Heterogene Kommunikationsstruktur

Die Kommunikation auf der Feldebene verwendet immer häufiger Ethernet-basierte Echtzeit-Kommunikationssysteme für den Austausch von I/O-Daten der Sensoren und Aktoren. Verschiedene Technologien haben sich hierfür im Markt etabliert: EtherCAT, PROFINET, Ethernet/IP und weitere. Auf der Ebene der Leitrechner oder der Maschinenvernetzung werden einzelne Maschinenmodule zu einer Produktionsanlage zusammengeführt. Die Kopplung der Maschinenteile erfolgt in der Regel über eine übergeordnete Master-Master-Kommunikation; die Maschinensteuerungen arbeiten als Gateway zwischen dem internen Kommunikationssystem und dem übergeordneten Leitsystem.

Für die sicherheitsrelevante Kopplung der Maschinenteile gelten ähnliche Randbedingungen. Unter Berücksichtigung der unterschiedlichen nativen Safety-Protokolle der etablierten Bussysteme innerhalb der Maschinenmodule wird für die anlagenweite Vernetzung der Module eine sichere Gateway-Funktion benötigt.

In diesem Zusammenhang wird häufig auch der Ansatz diskutiert, durch ein allgemeines, busunabhängiges Safety-Protokoll anlagenweite Sicherheitsfunktionen schließen zu können. Die Implementierung eines busunabhängigen Safety-Protokolls ist aber technisch schwierig und bringt einige wesentliche Einschränkungen mit sich:

– Die Zertifizierung eines Gerätes mit einer sicheren Kommunikationsschnittstelle ist aufwendig, da die Gerätehersteller für die Implementierung eines Safety-Protokolls Konformitätsnachweise und entsprechende Werkzeuge für jedes Kommunikationssystem benötigen. Diese werden von den Feldbusorganisationen für die nativen Safety-Protokolle bereitgestellt. Für ein



Homogene und heterogene Kommunikationsarchitektur mit Ethernet in der Leitebene: Ein offenes Schnittstellenprofil ermöglicht einen standardisierten Datenaustausch zwischen den Maschinenmodulen.

generisches Protokoll würden aber Konformitätsnachweise mehrerer nicht kooperierender Organisationen benötigt.

- Gerätehersteller werden vorrangig das native Safety-Protokoll für die unterstützte Busschnittstelle implementieren, um das Gerät in dem Markt für diese Kommunikationsschnittstelle erfolgreich platzieren zu können.
- Die Kosten für jedes Safety-Gerät würden sich erhöhen, wenn neben dem nativen Safety-Protokoll ein zweites sicheres Protokoll unterstützt werden müsste.
- Da nicht alle Gerätehersteller mehrere Safety-Protokolle unterstützen würden, würde sich für den Anwender die Auswahl der Geräte reduzieren und seine Gesamtkalkulation verschlechtern.

Das Beckhoff-TwinSAFE-System bietet daher eine Lösung, um an genau einer Stelle innerhalb eines Maschinenmoduls unterschiedliche Safety-Protokolle bedienen zu können: in der Sicherheitssteuerung, die in jedem Maschinenmodul vorhanden ist. Die Sicherheitssteuerung überwacht viele Verbindungen zu sicheren Kommunikationspartnern innerhalb des Maschinenmoduls. Wenn diese Steuerung für eine oder mehrere dieser Verbindungen ein weiteres Safety-Protokoll unterstützt, kann sie als eine sichere Gateway-Funktion arbeiten. Hierfür wird die Safety-PLC EL69xx durch die Eigenschaft erweitert, die Verbindung zu einem anderen Teilnehmer nicht nur mit Safety-over-EtherCAT zu realisieren, sondern auch mit einem anderen Safety-Protokoll, z. B. PROFIsafe (EL6930).

Standardisiertes Schnittstellenprofil

Innerhalb der EtherCAT Technology Group (ETG) wird derzeit eine Profilspezifikation erarbeitet, die oberhalb der Safety-Protokolle ein Applikationsprofil für den Datenaustausch zwischen den Modulen und zur Leitebene definiert. Es handelt sich hierbei um die komprimierten und vorverarbeiteten, sicheren Prozessdaten, die ein Maschinenmodul nach außen liefert beziehungsweise von außen bekommt.

Wenn sich zwei Maschinen miteinander „unterhalten", ist es für den Nachbarn nicht wichtig, ob sich dieser oder jener Antrieb in einem sicheren Zustand befindet oder ob ein Not-Aus-Schalter gedrückt wurde. Was aber tatsächlich interessiert, ist – um es einmal vereinfacht zu sagen – die Information, ob die Nachbaranlage ein Sicherheitsproblem hat, und wenn dem tatsächlich so ist, ob dann die eigenen Anlagenteile weiter produzieren dürfen. Das bedeutet, das tatsächliche Ausmaß an Sicherheitsinformationen, das außerhalb eines Anlagenmoduls dargestellt werden muss, ist recht überschaubar.

Inhalte des Schnittstellenprofils sind beispielsweise der allgemeine sicherheitsrelevante Maschinenzustand eines Moduls, die Information, ob das Modul sicher gestoppt wurde, oder auch eine übergeordnete Not-Aus-Anforderung. Findet man diese Informationen in Form eines Steuer- bzw. Statuswortes an fester Stelle auf der Schnittstelle wieder, dann ergeben sich erhebliche Vorteile durch vordefinierte Funktionsbausteine und durch wieder verwendbare Diagnosemöglichkeiten.

Im Gegensatz zu einem generischen Safety-Protokoll, das in alle Geräte zusätzlich integriert werden müsste, braucht die Gateway-Funktion nur einmal in einem Maschinenmodul realisiert zu werden. Und mit der EL69xx muss das Safety-Gateway nicht einmal als eigenständiges Gerät ausgeführt werden, sondern kann als Teilfunktion der Sicherheitssteuerung implementiert sein.

weitere Infos unter:
www.beckhoff.de/Safety
www.beckhoff.de/FSoE