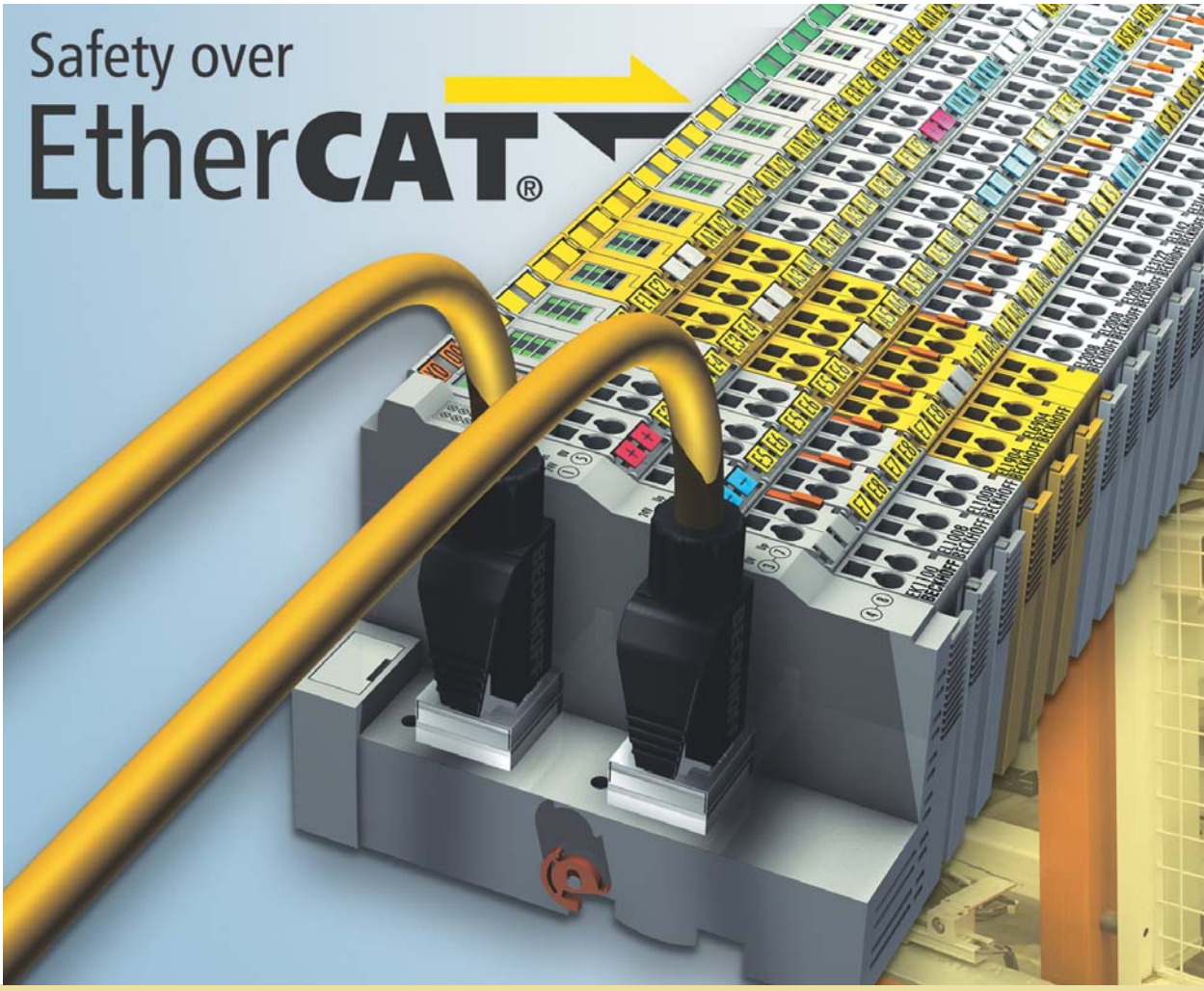
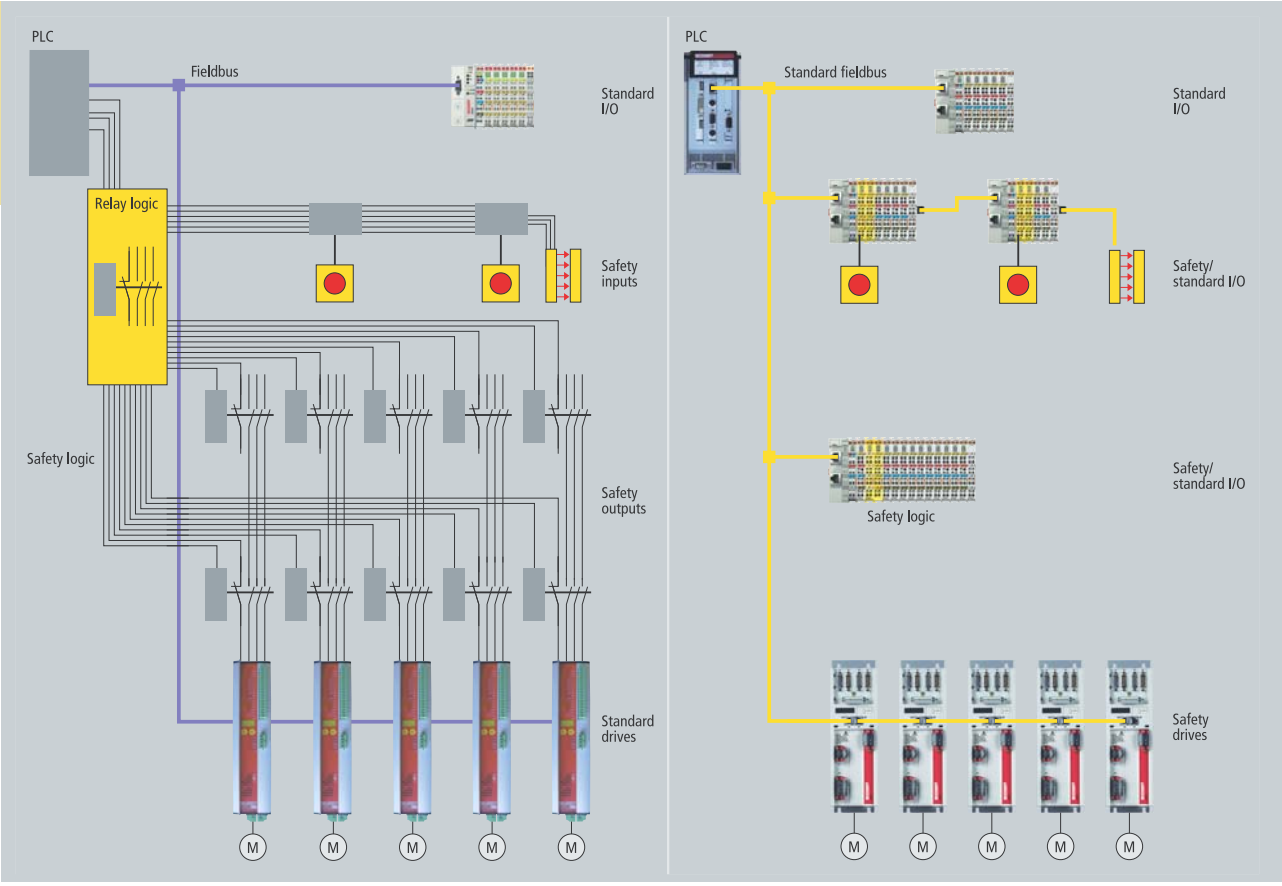
Die Sicherheitslösung für EtherCAT

Safety-over-EtherCAT



Moderne Kommunikationssysteme erfüllen heute nicht nur den deterministischen Transport von Steuerungsinformationen, sie bieten außerdem die Möglichkeit, sicherheitsrelevante Daten auf dem gleichen Medium zu übertragen. EtherCAT setzt dabei auf das sichere Protokoll Safety-over-EtherCAT.

„Die Konstruktion der Maschine ist fertig!" Herr Fastsicher ist zufrieden. Sein Kollege Herr Sicher weist ihn jedoch darauf hin, dass für eine CE-Konformität „…der Hersteller verpflichtet ist, eine Gefahrenanalyse vorzunehmen, um alle mit der Maschine verbundenen Gefahren zu ermitteln…". Herr Fastsicher ist demnach aufgefordert, nach einer entsprechenden Risikoanalyse notwendige Sicherheitsmaßnahmen an seiner Maschine zu erweitern. Dieses Beispiel spiegelt die bisher häufig vorzufindende Einstellung zur funktionalen Sicherheit an Maschinen wider. Sicherheitsfunktionen werden getrennt von den Automatisierungsfunktionen entwickelt und erst sehr spät in das Maschinenkonzept integriert. Dies führt zu umständlichen und wenig flexiblen Lösungen, die zeitweise sogar die Bedienung der Maschine einschränken. Eine Sicherheitsfunktion, die die Funktionalität der Maschine einschränkt, birgt aber immer die Gefahr, dass sie vom Anwender umgangen und damit wirkungslos wird.
Sicherheitssensoren wie Lichtgitter, Schutztürüberwachungen oder Zweihandbediengeräte werden in der Regel über eine Vielzahl von Auswertegeräten überwacht, die wiederum über eine unflexible Relaislogik auf die sicheren Ausgänge wirken. Zur Abschaltung der gefahrbringenden Bewegung werden redundante Netz- und/oder Motorschütze in den Leitungen der Antriebe eingesetzt, um diese momentenlos schalten zu können.
Der Trend allerdings geht in eine neue Richtung: Intelligente Sicherheitslösungen in den Automatisierungskomponenten und in den Kommunika-



Konventionelle Sicherheitstechnik (links) im Vergleich zu modernen Maschinenkonzepten mit integrierter Sicherheitsfunktion (rechts).

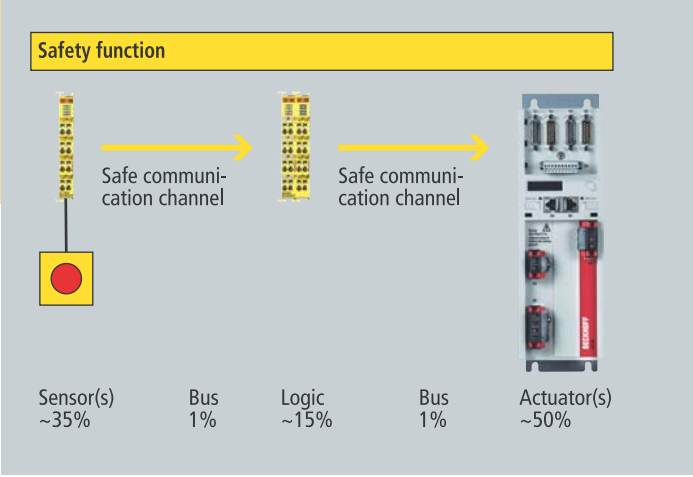
tionssystemen ermöglichen eine Integration der Sicherheitstechnik in das Maschinenkonzept. Im Bereich der Sicherheitssensorik sind dies Schutzeinrichtungen, die bereits funktionale Erweiterungen, wie z. B. Muting, integrieren. Neueste Entwicklungen sind kamerabasierte Sensoriksysteme mit räumlichen Überwachungsfunktionen, um in der Bereichsabsicherung neue Möglichkeiten der Interaktion zwischen Mensch und Maschine zu ermöglichen. Für die Auswertung und Sicherheitslogik werden bereits neben den „großen" Sicherheitssteuerungen kleine, dezentrale Logikgeräte angeboten, die auf die jeweilige Aufgabe skalierbar sind; unflexible Relaislogik kann damit entfallen. Auch die Antriebstechnik bietet integrierte Sicherheitsfunktionen zum schnellen und kurzzyklischen Stillsetzen des Antriebs und zum sicheren Überwachen von Funktionen wie der sicher begrenzten Geschwindigkeit.

Ermöglicht wird die Integration unter anderem durch eine sichere Datenübertragung zwischen den Komponenten. Eine solche sichere Übertragung ist in dem im Folgenden beschriebenen Safety-over-EtherCAT-Protokoll spezifiziert.

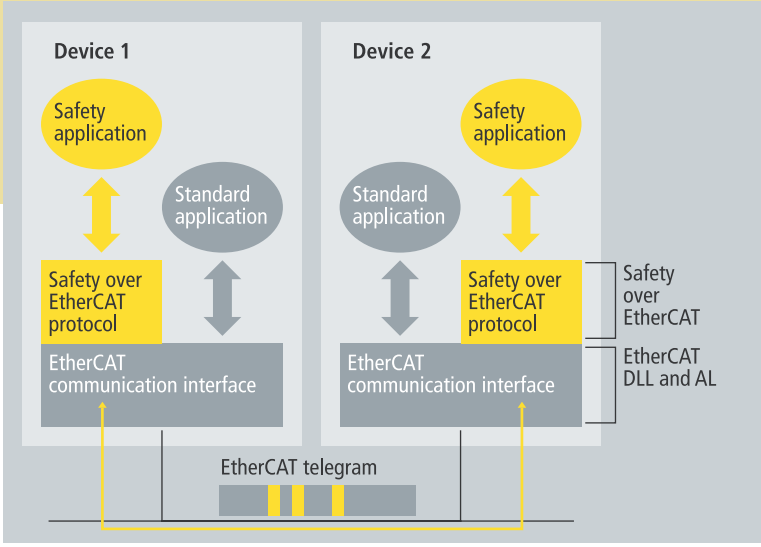
Die Normenwelt hat sich als Grundvoraussetzung ebenfalls mit den neuen Gegebenheiten auseinandergesetzt und ermöglicht die Bestimmung des Sicherheitslevels auch für softwarebasierte, programmierbare Sicherheitsgeräte (siehe IEC 61508, IEC 62061 und auch ISO 13849).

Die Vorteile:

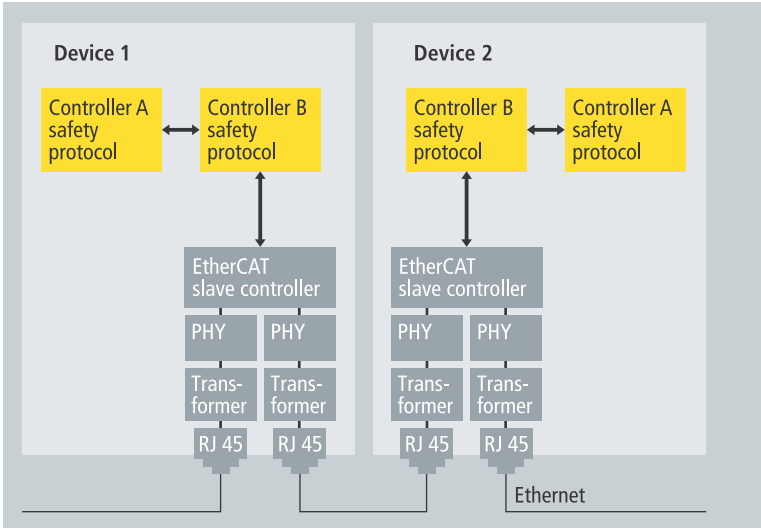
- nahtlose Integration des Sicherheitskonzepts in das Maschinenkonzept
- keine getrennten Entwicklungswerkzeuge für Standard- und Sicherheitsapplikation
- einfache Handhabung und Transparenz der Sicherheitsfunktionen
- sehr gute Diagnosemöglichkeiten der Sicherheitsfunktionen
- ein Kommunikationssystem für steuerungs- und sicherheitsrelevante Informationen
- keine Einschränkungen der Performance bzgl. Echtzeit und Determinismus
- flexible Erweiterungsmöglichkeiten



Verteilung der Restfehlerrate in einem Sicherheitssystem



Safety-over-EtherCAT – Software-Architektur



Safety-over-EtherCAT – Hardware-Architektur

Safety-over-EtherCAT

Zur Realisierung einer sicheren Datenübertragung für EtherCAT ist innerhalb der EtherCAT Technology Group (ETG) das Protokoll Safety-over-EtherCAT offen gelegt. Bei der Entwicklung dieses Protokolls waren die folgenden Eigenschaften von entscheidender Bedeutung.

- Einhaltung der SIL 3 der IEC 61508
- sichere und unsichere Informationen auf einem Kommunikationssystem
- Unabhängigkeit des Protokolls vom Übertragungssystem und -medium
- Die Länge der sicheren Prozessdaten wird vom Protokoll nicht eingeschränkt.
- Sehr kurze Framelängen werden ermöglicht.
- keine Einschränkungen bezüglich Übertragungsgeschwindigkeit und Zykluszeit

Die Einhaltung der Anforderungen nach IEC 61508 SIL 3 ist für einen uneingeschränkten Einsatz im Bereich der industriellen Automatisierung zwingend notwendig. Für das Bussystem bedeutet dies, dass die gefährliche Restfehlerwahrscheinlichkeit $< 10^{-9}$ pro Stunde eingehalten werden muss. Das entspricht 1 % der für den SIL 3 in einem System mit hoher Anforderungsrate geforderten Restfehlerrate von $\geq 10^{-8}$ bis $< 10^{-7}$; die anderen 99 % werden für die Sicherheitskomponenten wie Sensoren, sichere Logik und Aktorik gewahrt, die ebenfalls an der Realisierung der Sicherheitsfunktion beteiligt sind. Übrigens bedeutet $< 10^{-9}$ pro Stunde, dass im ständigen Betrieb ca. 100.000 Jahre lang kein gefährlicher Fehler auftreten darf, der unentdeckt bleibt.

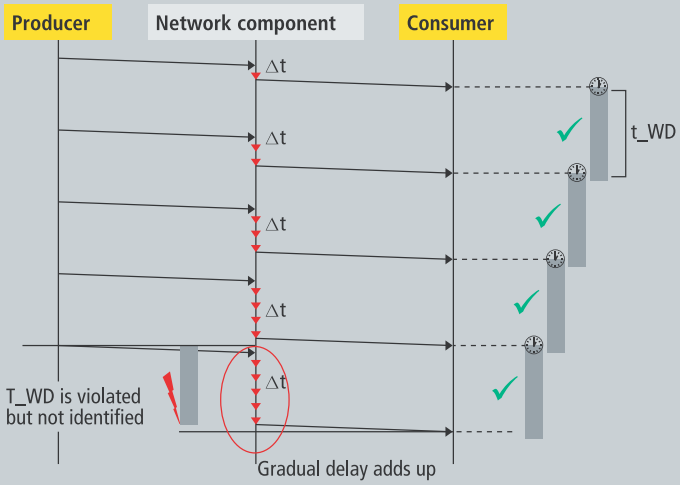
EtherCAT wird als einkanaliges Kommunikationssystem genutzt, um sichere und unsichere Informationen zu übertragen. Das Transportmedium wird dabei als „Black Channel" betrachtet und dementsprechend nicht in die Sicherheitsbetrachtung einbezogen. In die EtherCAT Prozessdaten wird ein Safety-Frame mit den sicheren Prozessdaten und der notwendigen Datensicherung gepackt. Dieser Container wird in den Geräten auf Applikationsebene sicher ausgewertet.

Die Kommunikationsanschaltung bleibt einkanalig. Dies entspricht dem Modell A aus dem Anhang der preIEC 617843. Diese derzeit in der Abstimmung befindliche Norm beschreibt Anforderungen an die Übertragung von sicherheitsrelevanten Nachrichten auf industriellen Netzwerken.

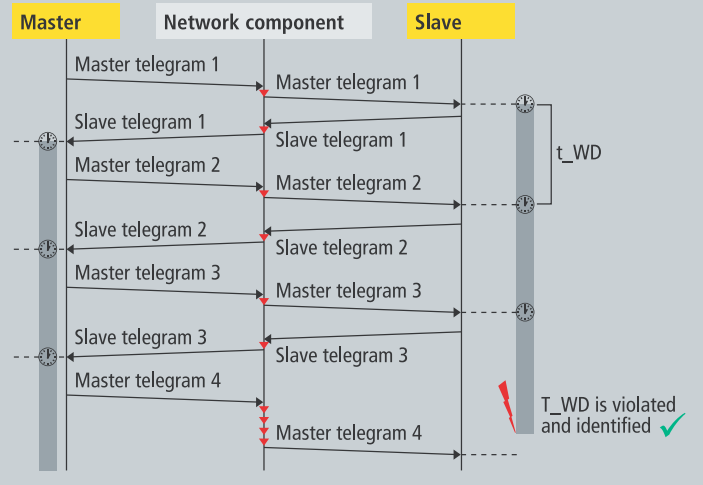
Die Berechnung der Restfehlerwahrscheinlichkeit für das Safety-over-EtherCAT-Protokoll nimmt keinen Kredit von den Fehlererkennungsmechanismen des Kommunikationssystems. Damit ist eine Übertragung des Protokolls auch über andere Kommunikationssysteme möglich. Genutzt wird dies u. a. bei der Verwendung von internen Subbus-Systemen in den Komponenten wie sie in modularen I/O-Systemen verwendet werden, die einen Buskoppler zum Anschluss an das Steuerungsbussystem besitzen und einen eigenen Subbus zum Einsammeln des Prozessabbilds der gesteckten I/O-Komponenten. Der Safety-Frame kann ohne Einschränkungen vom EtherCAT-Buskoppler über den Subbus an die sicheren I/O-Terminals weitergereicht werden.

Safety-over-EtherCAT – Technologiebeschreibung

Ein erster Prüfgrundsatz für die Prüfung und Zertifizierung von Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten wurde erstmals vom Fachausschuss Elektrotechnik des HVBG im Jahre 2000 vorgestellt. Dieser Prüfgrundsatz in der aktuellen Version [GSET26] ist Grundlage für die internationale Norm preIEC 61784-3. In dieser Norm werden unter anderem folgende Fehlerannahmen für ein solches Netzwerk getroffen: Verfälschung, Wiederholung, Vertauschung,



Die aufsummierte Verzögerung in einer Netzwerk-Komponente führt zu einem unentdeckten gefährlichen Fehler bei einer reinen Zeitüberwachung zwischen Producer und Consumer.



Master-Slave-Beziehung mit Watchdog; alle gefährlichen Verzögerungen werden sicher aufgedeckt.

Verlust, Verzögerung, Einfügung, Maskerade und falsche Adressierung von Nachrichten. Alle diese Fehler müssen von einem Sicherheitsprotokoll über geeignete Maßnahmen beherrscht werden, d. h. sie müssen entsprechend der angestrebten Sicherheitskategorie aufgedeckt werden.

Besonders die Annahme der Verzögerung von Nachrichten gewinnt für Ethernet-basierte Systeme an Bedeutung. Durch die Verwendung von Infrastrukturkomponenten wie beispielsweise Switche oder Router, die nicht sicherheitsrelevant abgenommen werden, besteht grundsätzlich die Möglichkeit, dass Nachrichten verzögert werden. Selbst eine Zeitüberwachung (Watchdog) der eintreffenden Nachrichten ist nicht ausreichend.

In der Grafik (oben) ist eine Producer-Consumer-Beziehung dargestellt. Der Consumer überwacht das zyklische Eintreffen der Nachrichten vom Producer mit Hilfe eines Watchdogs. In der Netzwerkkomponente werden die Nachrichten aber in jedem Zyklus um ein Δt verzögert, dass nicht von der Zeitüberwachung erkannt wird. Wenn sich diese Verzögerung über mehrere Zyklen aufsummiert, dann kann der Consumer nicht erkennen, dass eine Nachricht bereits über das erlaubte Maß hinaus veraltet ist. Im Extremfall heißt das, dass eine Not-Aus-Anforderung eines Sensors (Producers) erst nach Minuten am Antrieb (Consumer) gemeldet wird.

Eine Maßnahme zur Beherrschung solcher Fehler ist die Einführung einer globalen Uhrzeit und das Übertragen von Nachrichten mit einem Zeitstempel. Hierbei ist allerdings zu beachten, dass ein ggf. im Kommunikationssystem vorhandener Uhrzeitsynchronisationsmechanismus nicht ohne weiteres verwendet werden kann: Die Synchronisation muss zusätzlich auf Ebene des Sicherheitsprotokolls erfolgen. Safety-over-EtherCAT nutzt daher eine einfachere Methode. Über die Verwendung einer eindeutigen Master-Slave-Beziehung zwischen zwei Teilnehmern, der Safety-over-EtherCAT-Connection, kann gewährleistet werden, dass jeder Teilnehmer erst nach dem Erhalt einer neuen Nachricht seine eigene neue Nachricht zurücksendet. Der komplette Übertragungspfad zwischen Master und Slave wird damit in jedem Zyklus überwacht; das Aufsummieren von Verzögerungszeiten wird ausgeschlossen bzw. erkannt. Hierdurch ist eine sehr „schlanke" Implementierung des Protokolls möglich und die Anforderungen an den Zugriff des Kommunikationssystems bleiben moderat, da keine harten Timings für die Uhrzeitsynchronisation eingehalten werden müssen. Die Tatsache, dass es im Netzwerk unter Umständen zu vermehrten Datenaufkommen kommt, ist aufgrund der verfügbaren Bandbreite unkritisch und im praktischen Einsatz kein Nachteil.

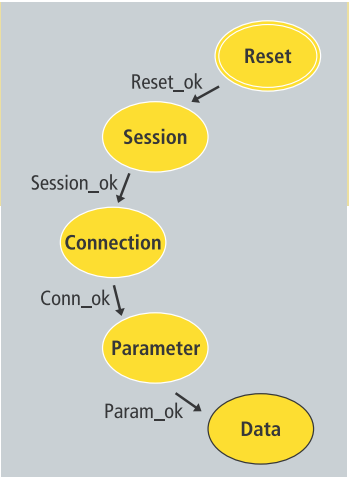
Für die Beherrschung der anderen anzunehmenden Fehler enthält das Safety-over-EtherCAT-Protokoll zusätzlich:

- **eine Session-Nummer,**
  um das Zwischenspeichern einer kompletten Hochlaufsequenz zu erkennen.
- **eine eindeutige Connection-ID und eine eindeutige Slave-Adresse,**
  um über eine eindeutige Adressbeziehung fehlgeleitete Nachrichten sicher zu detektieren.
- **eine CRC-Prüfsumme,**
  um eine Verfälschung der Nachrichten von der Quelle bis zur Senke zu erkennen. Zudem kann hierüber eine Vertauschung der Informationen innerhalb des Safety-Containers erkannt werden, wenn der Container auf dem Transport beispielsweise gesplittet wurde. Die Properness und die Eignung des Codes sowie die geforderte Unabhängigkeit zu der unterlagerten Kommunikation wurden nachgewiesen.
- **eine Sequence-Nummer,**
  um ein Vertauschen, die Wiederholung, das Einfügen oder den Verlust von ganzen Nachrichten zu erkennen.

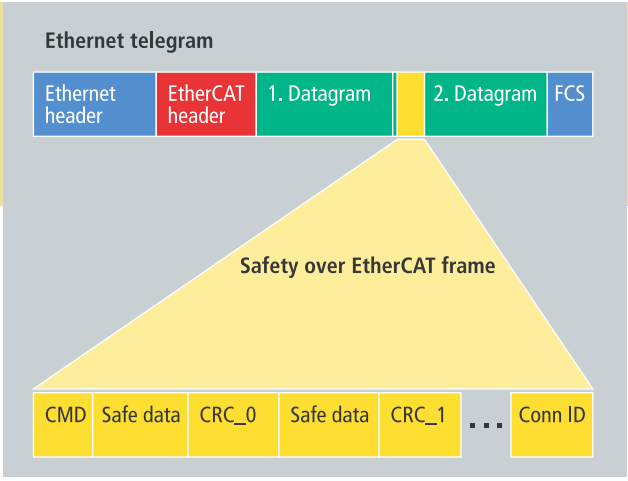
Dabei ist das Telegramm über entsprechende Vorschriften so gestaltet, dass bereits mit minimal 6 Byte Containerlänge alle Sicherungsinformationen inklusive einem Byte sicherer Prozessdaten übertragen werden können. Eine Beschränkung der Länge der sicheren Prozessdaten ist übrigens durch das Protokoll nicht gegeben. Das bedeutet, dass auch Sicherheitskomponenten mit vielen sicheren Prozessdaten unterstützt werden. Zum Beispiel könnte ein sicherer Antrieb neben einer sicheren Statusinformation auch die intern ermittelte sichere Position, sichere Drehzahl und/oder das sichere Moment zusätzlich übertragen.

Ebenso ist eine minimale Zykluszeit des Containers nicht eingeschränkt. Aus der geschickten Wahl der Sicherungsinformationen ergibt sich, dass für das Safety-over-EtherCAT-Protokoll die Übertragungsrate keinen Einfluss auf die Restfehlerwahrscheinlichkeit hat.

Zum Hochfahren einer Safety-over-EtherCAT-Connection wird sowohl im Master als auch im Slave eine Zustandsmaschine abgearbeitet.



Zustandsmaschine Safety-over-EtherCAT für eine Master-Slave-Connection

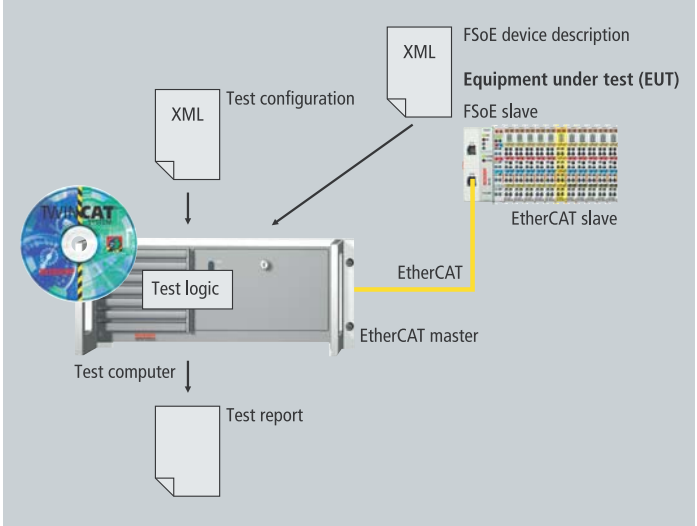


Einbettung des Safety-over-EtherCAT-Frames in die Prozessdaten von EtherCAT

Auch hier wurde Wert auf eine einfache Struktur gelegt, um die Implementierung möglichst einfach zu halten. Die Zustandsübergänge werden jeweils vom Master initiiert und vom Slave bestätigt. In den Zuständen werden Informationen für die Kommunikationsbeziehung ausgetauscht und überprüft. Im Zustand *Parameter* wird beispielsweise die Watchdog-Zeit ausgetauscht. Diese Zeit ist stark von der Übertragungsstrecke und den Sicherheitsgeräten abhängig und muss daher individuell konfiguriert werden. Zudem können in diesem Zustand sichere Anwendungsparameter vom Master zum Slave übertragen werden. Hierdurch ist eine zentrale sichere Datenhaltung im Master möglich. Die Länge der Anwendungsparameter kann bis zu 2^{16} Byte je Connection betragen und ist damit hinreichend groß, um z. B. auch ein konfiguriertes Schutzfeld eines Laserscanners zu übertragen.

Der sichere Zustand der Ausgänge kann erst im Zustand *Data* verlassen werden. Dieser Zustand ist der normale Betriebszustand zum Austausch von sicheren Eingangs- und sicheren Ausgangsdaten. Stellt einer der Teilnehmer einen Fehler der Kommunikationsbeziehung beim Hochlauf oder im Datenaustausch fest, dann wechselt er in den Zustand Reset und setzt damit die Verbindung zurück.

Aufbau Safety-over-EtherCAT-Conformance-Test



Zertifizierung

Das Protokoll Safety-over-EtherCAT ist vom TÜV begutachtet worden. Es wird bescheinigt, dass es sich um ein Protokoll handelt, mit dem Prozessdaten bis SIL 3 lt. IEC 61508 zwischen Safety-over-EtherCAT-Geräten übertragen werden können. Die Implementierung des Safety-over-EtherCAT-Protokolls in ein Gerät muss die Anforderungen des angestrebten Sicherheitsziels erfüllen. Hier sind die entsprechenden produktspezifischen Anforderungen zu beachten.

Die Übertragungsstrecke ist beliebig, es können Feldbussysteme, Ethernet oder ähnliche Strecken zur Übertragung eingesetzt werden ebenso wie Lichtwellenleiter, Kupferleiter oder auch Funkstrecken. Es gibt keine Einschränkungen oder Anforderungen an Buskoppler oder andere in der Strecke befindliche Geräte.

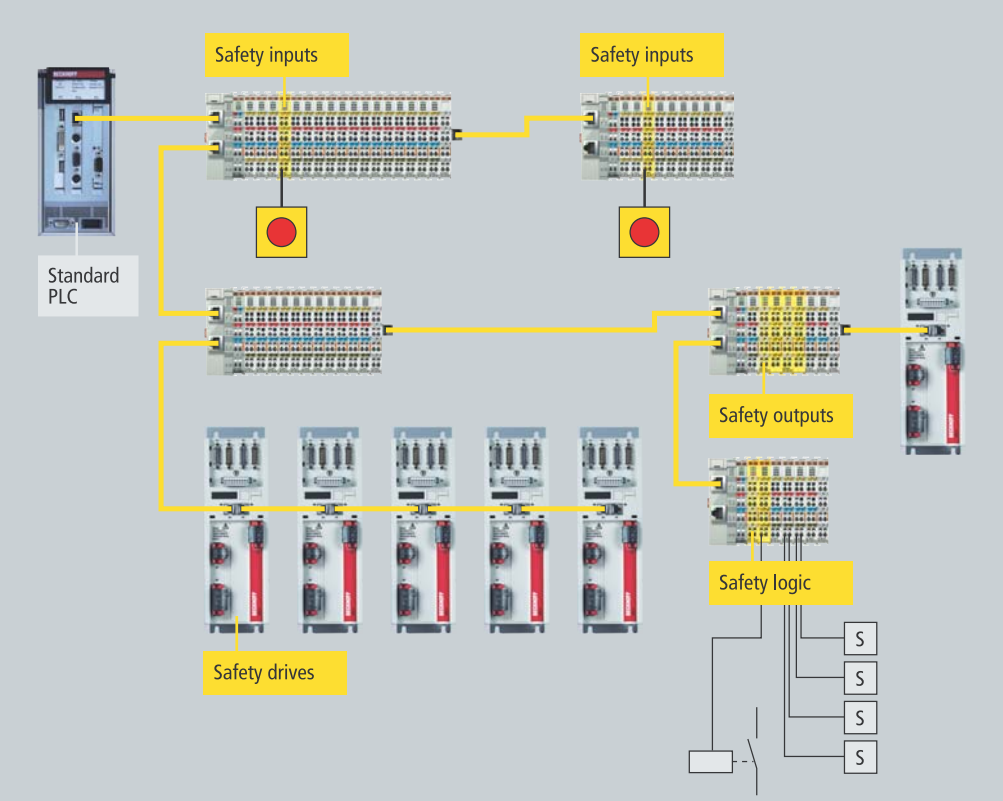
Zur Unterstützung der Implementierung des Protokolls in Geräte, wird derzeit ein Conformance-Test entwickelt. Dieser Test ist ein reiner Protokoll-Tester, der über die Kommunikationsschnittstelle eines Test-Gerätes das Verhalten des Sicherheitsprotokolls überprüft (Black-Box-Test).

Hierfür wird zunächst die Gerätebeschreibungsdatei des Prüflings eingelesen, um die möglichen Parameter für den Test zu ermitteln. Auf einem Standard-PC können dann Testscripte aus einer Testkonfiguration ausgeführt werden. Hierbei wird der Prüfling mit richtigen und fehlerhaften Telegrammen beaufschlagt und die Reaktion mit einem erwarteten Ergebnis verglichen. Das Ergebnis ist ein Testbericht, der die Resultate der Testschritte zusammenfasst.

Die Testcases werden von einer Prüfstelle begutachtet und freigegeben und können vom Gerätehersteller genutzt werden, um die Konformität mit der Protokollspezifikation sicherzustellen. Zudem ist geplant, an unabhängiger Stelle ein Conformance-Test-Labor zu errichten. In diesem Labor wird der Test ebenfalls durchgeführt und die Konformität bestätigt. Damit ist es für die Zertifizierungsstelle des Geräteherstellers möglich, die Sicherheitsfunktionalität dieses Protokolls abzunehmen. Die Implementierung (z. B. zweikanalige Berechnung) des Safety-over-EtherCAT-Protokolls kann allerdings nicht durch den Test getestet werden. Dies ist ebenso wie für die sichere Applikation des Gerätes direkt vom Hersteller entsprechend der Anforderungen des angestrebten Sicherheitsziels der abnehmenden Stelle darzustellen.

Zusammenfassung

- Safety-over-EtherCAT beschreibt das Sicherheitsprotokoll für EtherCAT.
- Das Protokoll enthält keine Einschränkungen bezüglich sicherer Prozessdatenlänge, Kommunikationsmedium oder Übertragungsrate.
- EtherCAT wird als „schwarzer Kanal" verwendet; d. h. das Kommunikationssystem geht nicht in die Sicherheitsbetrachtung ein.
- Das Protokoll ist spezifiziert, begutachtet und es erfüllt die Anforderungen der IEC 61508 SIL 3.
- Seit 2005 sind Produkte mit dem Safety-over-EtherCAT-Protokoll am Markt verfügbar.



Beispielapplikation TwinSAFE-System mit Safety-over-EtherCAT-Protokoll

Anwendungsbeispiel

Der Beweis der Sicherheit und der Funktionalität eines sicheren Übertragungsprotokolls kann nur über die Implementierung der Spezifikation in ein Produkt erfolgen. Geräte mit Safety-over-EtherCAT sind bereits sei 2005 verfügbar. Safety-over-EtherCAT ist damit eines der ersten Industrial-Ethernet-Echtzeitkommunikationssysteme, das ein sicheres Protokoll unterstützt.

In dieser Applikation werden die Vorteile der Technologie genutzt (Beispiel oben). Die Sicherheitskomponen-ten werden dort im Automatisierungssystem eingesetzt, wo sie benötigt werden. Dezentrale Ein- und Ausgangsbaugruppen können skalierbar in der Anlage eingesetzt werden. Auch ein zusätzlicher Eingang oder Ausgang kann flexibel erweitert werden – und das wahlfrei zwischen den sicheren und unsicheren Busklemmen.

Die Sicherheitslogik ist ebenfalls innerhalb des Netzwerk-Strangs eingebettet. Dadurch kann eine Standard-SPS weiterhin die Steuerungsaufgaben erfüllen und muss nicht sicherheitsrelevant erweitert werden. Die Verknüpfung der sicheren Eingangs- und Ausgangsfunktionen erfolgt in der dezentralen Sicherheitslogik, einer intelligenten, sicheren Busklemme. Das spart Kosten für eine teuere Sicherheits-SPS und ermöglicht die Skalierung der Logik entsprechend der geforderten Aufgabe. Über die unsichere Standard-SPS werden lediglich die Nachrichten zwischen dem Safety-over-EtherCAT-Master und den ihm zugeordneten sicheren Slaves geroutet.

Beckhoff bietet derzeit drei sichere I/O-Baugruppen: eine Eingangsklemme mit vier sicheren Eingängen, eine Ausgangsklemme mit vier sicheren Ausgängen und eine Logic-Klemme, die neben einer konfigurierbaren Sicherheitslogik auch vier lokale sichere Ausgänge integriert. Die sicherheitsrelevante Parametrierung der Geräte kann über ein in die Standard-Programmierumgebung (TwinCAT) integriertes sicheres Konfigurationstool einfach vorgenommen werden. Der resultierende sichere Parametersatz wird abschließend Passwort-überwacht auf die sichere Logic-Klemme geladen. Die Logic-Klemme verteilt bei jedem Hochlauf die sicheren Anwendungsparameter auf die konfigurierten Ein- und Ausgangsklemmen. Somit ist ein einfacher Austausch der Ein- und Ausgangsklemmen möglich, ohne die Konfiguration erneut anpassen oder herunterladen zu müssen.