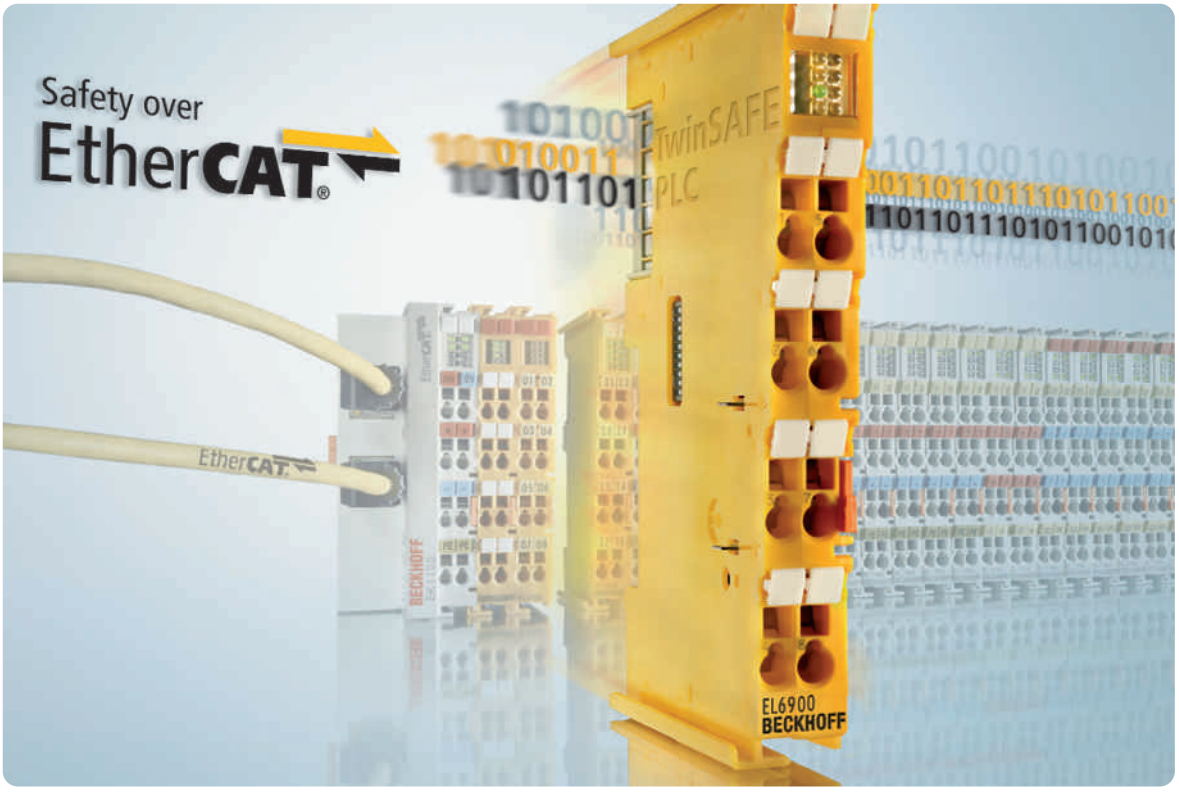


Safety-over-Ethercat:

Von sicheren I/Os bis zum sicheren Antrieb

Das Safety-over-Ethercat-Profil ist innerhalb der Ethercat Technology Group (ETG) offen gelegt und sorgt für eine sichere Übertragung von Daten zwischen Sicherheitseingängen wie Lichtgittern, Schutztürüberwachungen, Not-Aus-Tastern, einer sicheren Logik und sicheren Ausgängen (z.B. antriebsintegrierte Sicherheitsfunktionen).

Das Safety-over-Ethercat-Protokoll (FSoE) ist bereits seit 2005 in zahlreichen Automatisierungskomponenten im Einsatz. 2006 wurde das Protokoll der ETG als Sicherheitsprotokoll vorgeschlagen und dort akzeptiert. Damit konnte der Funktionsumfang der Ethercat-Technologie um eine sicherheitsrelevante Übertragung vervollständigt werden. Schnell fanden sich weitere ETG-Mitglieder, die dieses Protokoll in ihre Systementscheidung einbezogen und mit der Entwicklung von Geräten begannen. Heute unterstreicht der Einsatz in zahlreichen Anwendungen die Akzeptanz bei den Anwendern und Geräteherstellern.

Das Safety-over-Ethercat-Protokoll

Bei der Definition des Protokolls wurde auf eine einfache Implementierung und Parametrierung Wert gelegt. Die Protokollmechanismen und Übertragungsdienste dienen als Grundlage für eine einfache Architektur. Die entscheiden-

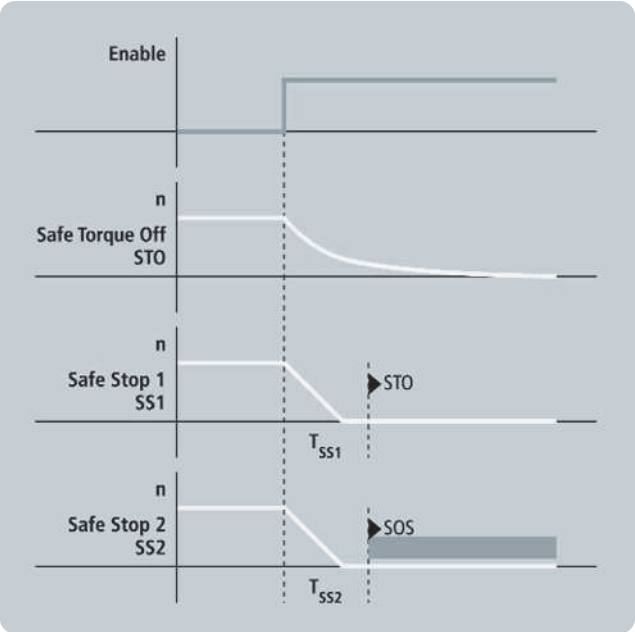


Bild 2: Sichere Stoppfunktionen

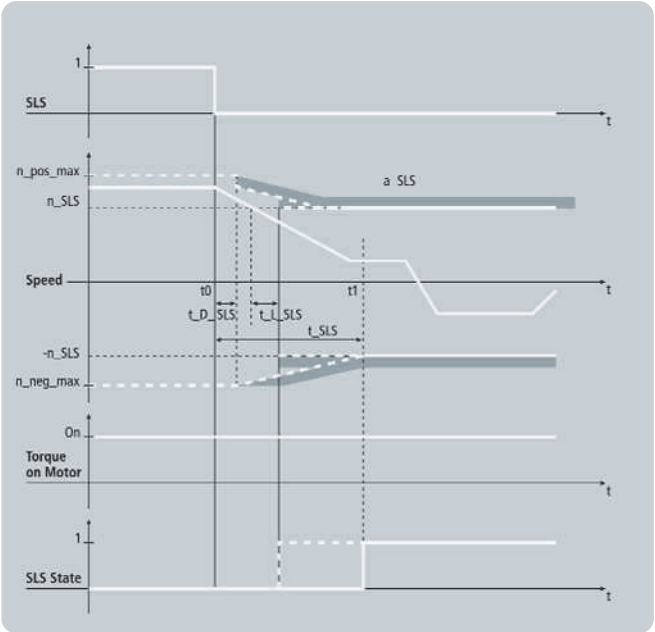


Bild 3: Sicherheitsfunktion Safety Limited Speed (SLS) mit Überwachung der Bremsrampe

den Eigenschaften sind eine schmale Spezifikation, die Unabhängigkeit vom Kommunikationskanal sowie die Variabilität in der zur Verfügung stehenden Datenbreite. Die Implementierung des Protokolls ist durch diese Eigenschaften einfach möglich – und somit wenig anfällig für systematische Fehler.

Schmale Spezifikation

Alle Fehler, die bei der Übertragung eines sicheren Datums anzunehmen sind, werden vom FSoE-Protokoll mit der geforderten Restfehlerwahrscheinlichkeit erkannt und damit beherrscht – bis zu SIL3 nach der IEC61508. Bei den Erkennungsmaßnahmen wurde darauf geachtet, dass die Implementierung möglichst einfach erfolgen kann. Anhand eines Beispiels wird dies deutlicher: In einem Ethernet-basierten Netzwerk besteht durch die Verwendung von Infrastrukturkomponenten, wie beispielsweise Switches oder Routern, die nicht sicherheitsrelevant abgenommen werden, grundsätzlich die Möglichkeit, dass Nachrichten verzögert werden. Einzelne verzögerte Nachrichten können in der Regel durch einen lokalen Watchdog erkannt werden. Es können aber auch ganze Datenpakete mit einer Sequenz von Telegrammen zwischengespeichert werden. Wenn diese Sequenz zu einem späteren Zeitpunkt weitergeleitet wird, dann wird der lokale Watchdog im Empfänger (z.B. Aktor) richtig getriggert und der Fehler kann nicht erkannt werden. Eine fatale Situation, wenn zu diesem Zeitpunkt der Aktor eigentlich in den sicheren Zustand schalten sollte.

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 gegebenenfalls im Standard-Kommunikationssystem vorhandener Uhrzeit-Synchronisationsmechanismus nicht ohne Weiteres verwendet werden kann: Die Synchronisation muss zusätzlich auf Ebene des Sicherheitsprotokolls erfolgen. Dies bedeutet eine relativ aufwendige sicherheitsrelevante Implementierung in allen Teilnehmern. Zudem müssen vom Kommunikationssystem Datenpfade zum Austausch einer Uhrzeitinformation zwischen allen Teilnehmern zur Verfügung gestellt werden. Safety-over-Ethercat wählt darum eine andere Methode: In einer definierten Verbindung (Connection) versendet der Safety Master sichere Nachrichten zu einem Safety Slave. Dieser muss zunächst mit einer eigenen sicheren Nachricht antworten, bevor eine neue Nachricht vom Master generiert wird. Beide Teilnehmer starten jeweils beim Senden der eigenen Nachricht einen Watchdog und überwachen, dass von der Gegenstelle eine neue Nachricht innerhalb der Watchdog-Zeit empfangen wird. Dieses Verfahren überwacht die komplette Übertragungsstrecke zwischen Master und Slave, ist in den Teilnehmern einfach zu implementieren und bedarf keinerlei zusätzliche Kommunikationswege. Die Implementierung des Protokolls in ein Gerät benötigt nur wenige Ressourcen und kann eine hohe Performance und damit kurze Reaktionszeit erreichen. Besonders in Maschinenanwendungen, die eine schnelle, sicherheitsgerichtete Reaktion auf ein Eingangssignal benötigen, ist dies wichtig. Dabei muss das Eingangssignal nicht immer durch eine Aktion des Bedieners ausgelöst werden: Elektronische Überwachungssensoren (z.B. sichere Drehzahlüberwachung) können viel schneller eine kritische Situation erfassen, als dass ein Bediener einen Not-Aus-Schalter betätigen könnte. Reaktionszeiten im Bereich weniger Millisekunden sind für hochdynamische Antriebe daher sinnvoll und nun auch über eine sichere Kommunikation realisierbar.

Unabhängigkeit vom unterlagerten Kommunikationssystem

Das Transportmedium wird bei Safety-over-Ethercat als 'Black Channel' betrachtet und daher nicht in die Sicherheitsbetrachtung einbezogen. Das Kommunikationssystem Ethercat bleibt einkanalig und überträgt sichere und Standardinformationen gleichzeitig. Hierfür werden in die Prozessdaten die Safety Frames als Container mit den sicheren Prozessdaten und der notwendigen Datensicherung verschickt. Es sind unterschiedliche Medien möglich: Lichtwellenleiter, Kupferleiter, Funk- oder auch andere Datenstrecken, wie z.B. Datenlichtschranken, sind erlaubt. Die Adressierung des Safety Slaves wird in der Connection über eine Safety-Adresse und eine eindeutige Connection-ID gesichert. Durch diese Unhabhängigkeit ist auch die Vernetzung verschiedener Anlagenteile sicherheitsrelevant möglich. Der Safety-over-Ethercat-Container wird über die Steuerungen geroutet

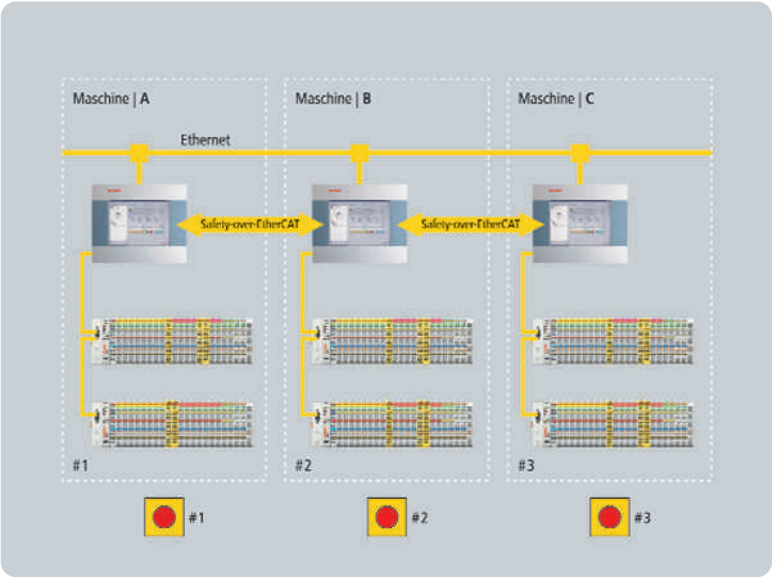


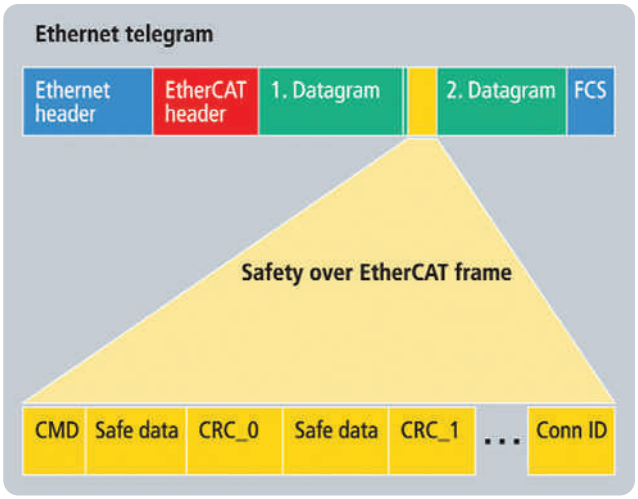
Bild 4: Anlagenvernetzung mit Safety-over-Ethercat

und im anderen Anlagenteil ausgewertet. Übergreifende Not-Aus-Funktionen und gezieltes Stillsetzen von Anlagenteilen sind somit problemlos lösbar, auch wenn diese über andere Kommunikationsmedien wie z.B. Ethernet miteinander gekoppelt sind.

Variable Datenbreite

Die minimale Anzahl sicherer Daten (SafeData) beträgt 1Byte. Eine maximale Anzahl ist vom Protokoll praktisch nicht beschränkt. Dies liegt am gewählten Sicherungsverfahren. Je 2Byte SafeData werden durch eine 2Byte-CRC gesichert. Die Anzahl solcher Daten/CRC-Blöcke ist beliebig; die Anforderung des Safety-Gerätes legt dementsprechend die Anzahl der SafeData für die Eingangs- und die Ausgangsrichtung fest. Um die notwendige Bandbreite auf dem Kommunikationsmedium gering zu halten, kann sich die Anzahl zudem je Richtung unterscheiden. Die Anwendungsbereiche des Safety-over-Ethercat-Protokolls reichen daher von einfachen sicheren Eingangs- oder Ausgangsbaugruppen mit wenigen Bits SafeData bis hin zu komplexen Sicherheitssensoren, wie z.B. sicherheitsrelevante Kamerasysteme-, oder sichere Antriebsfunktionen, die viele Nutzdaten benötigen.

Bild 5: Safety-over-Ethercat-Container



Automatischer Parameter-Backup für Master und Slave

In einem Sicherheitssystem müssen die sicherheitsrelevanten Parameter in den Geräten entsprechend des geforderten SIL konfiguriert werden. Für die Kommunikation muss z.B. die sichere Watchdog-Zeit einer Connection anlagenspezifisch, eingestellt werden. Für die sichere Funktion der Teilnehmer können weitere applikationsspezifische sicherheitsrelevante Parameter notwendig sein (z.B. sicher reduzierte Drehzahlgrenze). Safety-over-Ethercat bietet im Protokoll die Möglichkeit, gerätespezifische Parameter während des Aufbaus einer Connection vom Safety Master auf den Safety Slave zu laden. Die Datenhaltung für die Konfiguration des Sicherheitssystems kann damit zentral auf dem Safety Master erfolgen. Die Safety Slaves werden bei jedem Hochlauf neu parametriert. Ist ein Safety-Slave-Gerät defekt, kann dieses einfach ausgetauscht werden. Die Safety-Slave-Adresse muss mit der des ausgetauschten Gerätes übereinstimmen und schon werden beim nächsten Hochlauf wieder die gleichen Parameter vom Safety Master geladen. Der Austauschfall eines Safety Masters benötigt erweiterte Mechanismen, da dieser die komplette Konfiguration des Sicherheitssystems enthält. Bei der Inbetriebnahme der Maschine wird die Konfiguration erzeugt und über ein Tool in den Safety Master geladen. Hierbei können mögliche Fehler erkannt werden, da eine Interaktion zwischen dem Tool, dem Gerät und dem Bediener erforderlich ist. Das automatische Laden einer Konfiguration nach einem Gerätetausch birgt die Gefahr, dass ein falscher oder verfälschter Konfigurationssatz heruntergeladen wird und damit die Sicherheitsfunktion der Anlage nicht mehr garantiert werden kann. Im Safety-over-Ethercat-Protokoll ist aber auch hierfür ein Mechanismus beschrieben. Bei der Inbetriebnahme wird über den Konfigurationssatz vom Tool eine Prüfsumme gelegt. Diese wird benötigt, um die Konsistenz der Daten sicherzustellen. Die Prüfsumme wird aber nicht nur im Safety Master abgelegt, sondern auch als Parameter in den Safety Slaves. Wenn der Master ausgetauscht wurde, erkennt er beim Hochlauf, dass er keine Konfiguration gespeichert hat. Er kann dann eine Konfiguration vom Kommunikationsmaster (z.B. Standard-SPS) anfordern. Nach dem Laden der Konfiguration prüft der Safety Master diese auf Konsistenz und vergleicht die Prüfsumme mit denen, die in den ihm zugeordneten Slave-Geräten abgelegt sind. Nur wenn diese Überprüfung erfolgreich war, wird der Konfigurationssatz übernommen und die Safety-Verbindungen hochgefahren. Für den Anwender bietet diese Methode den Vorteil, dass sowohl Safety-Slave- als auch Safety-Master-Geräte getauscht werden können, ohne dass ein Konfigurationstool benötigt wird. Für die Sicherheit bedeutet dies, dass ein falscher Konfigurationssatz, der auf den Master gespielt wird, automatisch erkannt wird. Dies ist bei Systemen, die manuell oder über wechselbare Speichermedien konfiguriert werden, nicht immer der Fall.

Safety-over-Ethercat setzt Standards

Von Anfang an wurde die Safety-over-Ethercat-Technologie offen innerhalb der ETG verwendet. Jetzt wird das Protokoll auch in die internationale Norm IEC61784-3 eingebracht. Diese Norm

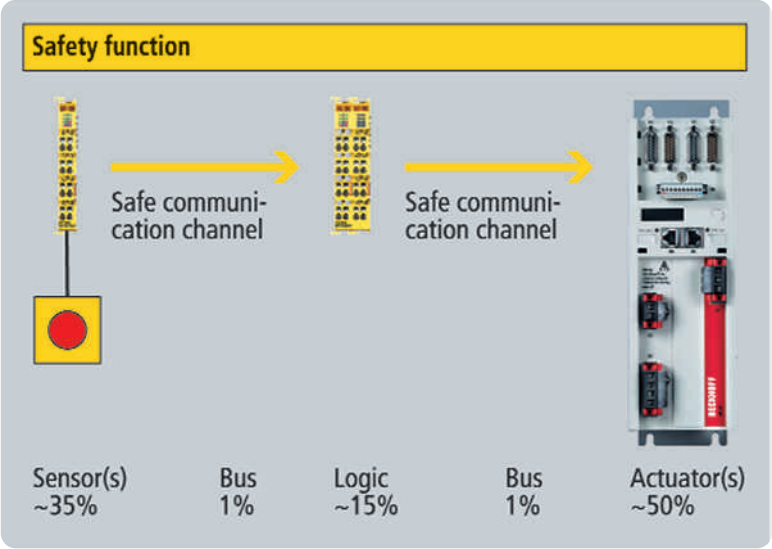


Bild 6: Anforderungen an die gefährliche Ausfallrate

beschreibt die grundlegenden Anforderungen an ein sicheres Kommunikationssystem. Hierfür werden Fehler definiert, die bei einer Übertragung über ein Kommunikationssystem auftreten können und die vom Safety-Protokoll beherrscht werden müssen. Für die Bestimmung des Safety Integrity Levels ist die gefährliche Ausfallwahrscheinlichkeit (Probability of dangerous failure on demand, kurz PFD, bzw. Average frequency of dangerous failure per hour, kurz PFH) des gesamten Sicherheitssystems zu betrachten. Die sichere Übertragung ist dabei nur ein kleiner Teil des Systems. Den Hauptteil nehmen die sicheren Eingänge (inklusive Sensoren), die sichere Logik (Programmable Electronic System, kurz PES) und die sicheren Ausgänge (inklusive Aktoren) ein. Daher wird in der IEC61784-3 gefordert, dass für die sichere Übertragung nur 1% der maximalen PFD bzw. PFH des angestrebten SIL aufgewendet wird. In Zahlen bedeutet 1% Versagenswahrscheinlichkeit für einen angestrebten SIL3, dass maximal 10^{-9} Fehler/Stunde auftreten dürfen. Umgerechnet sind dies etwa 100.000 Jahre Übertragung ohne unerkannten, gefährlichen Fehler. Diese Anforderung wird vom Safety-over-Ethercat-Protokoll eingehalten.

Safety Drive Profile

Der Standard IEC61800-5-2 definiert sicherheitsrelevante Funktionen für Antriebe. Mit diesen Funktionen ist ein sicheres Stoppen des Antriebs, z.B. Safe Torque Off (STO) oder Safe Stop 2 (SS2), oder eine sichere Überwachung der Bewegung, z.B. die sicher begrenzte Geschwindigkeit (SLS), realisierbar. Hierdurch können gefahrbringende Bewegungen bei der Inbetriebnahme einer Maschine oder bei einem zyklischen, manuellen Eingriff vermieden oder sicher begrenzt werden. Zur Ansteuerung und Konfiguration dieser antriebsintegrierten Sicherheitsfunktionen wurde in der ETG das Safety-over-Ethercat-Protokoll um ein sicherheitsrelevantes Geräteprofil für Antriebe (Safety Drive Profile) erweitert. Die Definition eines einheitlichen Steuer- und Statuswortes ermöglicht es dem Anwender, Antriebe verschiedener Hersteller auf die gleiche Art und Weise an seiner Sicherheitssteuerung zu betreiben. Damit wird die Vielfalt von Funktionsbausteinen in der Steuerung verringert und der Betrieb vereinfacht. Angelehnt an die Funktionen, die in der IEC61800-5-2 definiert sind, wird ein Steuerwort spezifiziert, das die separate Aktivierung dieser Funktionen im Antrieb ermöglicht. Jede Funktion wird dabei über ein Bit im Steuerwort repräsentiert. Ob eine Sicherheitsfunktion im Antrieb gerade angewählt ist und die Grenzen einhält, wird über das sichere Statuswort an die überlagerte Logik zurückgemeldet. Da die IEC-Norm diese Funktionen nur sehr vage definiert, wurde im Safety-Drive-Profil der ETG auch die Funktionsweise im Detail beschrieben. Hierfür sind für alle Funktionen Timing-Diagramme erstellt worden, anhand derer mögliche und notwendige Parameter beschrieben werden. Typische Implementierungen werden berücksichtigt. Somit entsteht ein Objektverzeichnis und der Anwender erhält ein einheitliches, implementierungs- und herstellerunabhängiges Verständnis für die hinterlegte Funktion im Antrieb. Die Ethercat Technology Group strebt an, die Nutzung des Safety-Drive-Profiles – das vom Aufbau her unabhängig vom verwendeten Sicherheits-Bussystem ist – auch anderen interessierten Organisationen bzw. Technologien zu ermöglichen.

Zusammenfassung

Safety-over-Ethercat beschreibt ein offenes Kommunikationsprofil zur sicheren Übertragung von Nachrichten. Entsprechend dem Ansatz 'simple is safety' wurden bei der Spezifikation einfache Methoden zur Fehlererkennung und Fehlerbeherrschung gewählt. Trotzdem bietet das Protokoll herausragende Eigenschaften für den Einsatz in der Automatisierung:

- keine Abhängigkeit vom unterlagerten Kommunikationssystem
- keine Einschränkung der Datenlänge
- einfache Implementierungsmöglichkeit und dadurch kurze Stacklaufzeiten
- hohe Performance und kurze Reaktionszeiten.

Über zusätzliche (optionale) Funktionen kann das Profil erweitert werden. Ein Backup-Mechanismus für die Safety Slaves, aber auch für den Safety Master ist definiert und gestattet einen Gerätetausch ohne manuelle Konfiguration durch den Anwender. Die internationale Standardisierung des Protokolls ist eingereicht und unterstreicht die Offenheit der Technologie. Zudem steht mit dem Safety Drive Profil ein Geräteprofil zur Verfügung, das eine einheitliche Bedienung und Parametrierung von sicheren Antriebsfunktionen ermöglicht. Zahlreiche Firmen setzen Safety-over-Ethercat bereits heute in ihren Anlagen und in ihren Geräten ein. Der Zuwachs der Ethercat Technology Group mit heute bereits 940 Mitgliedsfirmen lässt erwarten, dass die Verbreitung der Ethercat-Technologie weiter zunehmen wird – und für sicherheitsrelevante Geräte auch die Verbreitung der Safety-over-Ethercat-Technologie. ■

www.ethercat.org

www.beckhoff.de/Safety-over-EtherCAT

Autor: Dr. Guido Beckmann, Technologiemarketing Safety-over-Ethercat, Beckhoff Automation GmbH