

Im Turck-Programm finden Anwender ein großes Angebot unterschiedlicher Sicherheitskomponenten, vom sicheren Sensor über mechanische Schalter bis zu Safety-Controllern



Aber sicher!

Relaisbasiert, zentral oder dezentral: Viele Wege führen zur sicheren Maschine – Turck unterstützt Anwender dabei mit einem umfangreichen Safety-Portfolio

Jeder Hersteller muss das Risiko seiner Produkte im Rahmen der Maschinenrichtlinie 2006/42/EG bewerten, um Menschen zu schützen, die mit der Maschine in Kontakt kommen. Um die von der Maschine ausgehende Gefahr auf ein vertretbares Restrisiko zu senken, folgen Hersteller einem dreistufigen Prozess: Zunächst gilt es, Risiken so weit wie möglich konstruktiv zu minimieren. Verbleibende Risiken müssen durch technische Schutzmaßnahmen reduziert werden. Die dritte Stufe der Reduktion fordert vom Hersteller die Erstellung von Benutzerinformationen wie etwa Bedienungsanleitungen, die über den sachgerechten Umgang mit einem Produkt aufklären.

Spricht man von Safety oder Maschinensicherheit, ist meist die zweite Stufe gemeint. Wie diese technischen Schutzmaßnahmen ausgelegt werden müssen,

ist jedoch nicht exakt festgelegt. Folglich existieren unterschiedliche Sicherheitskonzepte mit spezifischen Vor- und Nachteilen: Da sind zum einen zentrale, hartverdrahtete Systeme mit Sicherheitsrelais, zum anderen zentral verdrahtete Applikationen mit Sicherheits-Controllern oder Sicherheitssteuerungen. Eine dritte Variante sind dezentrale Sicherheitskonzepte mit IP67-I/O-Modulen, kombiniert mit zentralen Sicherheitssteuerungen oder dezentralen IP67-Safety-Controllern. Auch passive Sicherheitslösungen sind eine Option für geeignete Anwendungen.

Zentrale Sicherheitssysteme mit Relaisstechnik

Wie die klassische Automatisierungstechnik, so basierte auch die Automatisierung von Sicherheitsfunktionen ursprünglich auf Relaisstechnik. Sichere Relaisstechnik



wird auch heute noch eingesetzt. Die Logik wird dabei über hartverdrahtete Kontakte abgebildet. Der Vorteil dieser Installationen ist, dass sie hardwareseitig relativ kostengünstig sind und weltweit verstanden werden können. Software kommt nicht zum Einsatz. Bei größeren und komplexeren Sicherheitsinstallationen wird die Relais-technik allerdings unübersichtlich. Suche und Diagnose von Fehlern sind sehr aufwendig. Eine Selbstprüfung des Systems ist nicht möglich.

Zentrale Systeme mit Sicherheits-Controllern

Ab einem gewissen Komplexitätslevel ist es günstiger, Sicherheitsapplikationen mit Sicherheits-Controllern zu realisieren. In Controllern oder Sicherheitssteuerungen können Programme geschrieben werden, die – vereinfacht ausgedrückt – Aktionen mit Bedingungen und Boole'schen Operatoren (UND, ODER, NICHT, XOR) verknüpfen. Die Verdrahtung dieser Applikationen ist zwar einfacher als bei Relais-technik, aber alle sicheren Signale müssen zum zentralen Controller im Schaltschrank geführt werden, was lange Inbetriebnahmezeiten bedingt.

Der Vorteil der Safety-Controller ist, dass Sicherheitsprogramme kopiert und mehrfach für gleichartige Maschinen eingesetzt werden können. Erweiterungen der Sicherheitsfunktionen sind relativ einfach möglich.

Zudem lassen sich die Sicherheitsapplikationen grafisch auf HMIs darstellen. Informationen und Signale gelangen sowohl vom Controller zur SPS als auch von der SPS in den Controller.

Sicherheits-Controller XS26 einfach erweiterbar

Turck bietet für zentrale Installationen die Sicherheits-Controller SC10, SC26 und XS26 seines Partners Banner Engineering an. Alle drei Geräte sind als Device/Slave in Profinet, Modbus-TCP oder Ethernet/IP-Netzwerken einsetzbar. Anwender können so immer die gleiche Sicherheitsarchitektur und Applikation einsetzen, egal für welchen Markt eine Anlage bestimmt ist.

SCHNELL GELESEN

Die one-fits-all-Lösung gibt es auch bei Maschinensicherheitslösungen nicht. Je nach Umfang und Anwendung eignen sich zentral gesteuerte Installationen, dezentrale oder solche mit passiver Sicherheit am besten. Wer allerdings Flexibilität und kurze Inbetriebnahmezeiten für preissensible Applikationen sucht, kommt an dezentralen Sicherheitslösungen mit robusten IP67-Komponenten nicht vorbei. Turck hat dazu das passende Safety-Portfolio für unterschiedlichste Anwendungsszenarien.



Diese Sicherheitsapplikation wird zum Testen im Werk über das TBPN (links) gesteuert. Im Live-Betrieb beim Endkunden übernimmt dann eine Profisafe-Steuerung die Applikation. Alle Aktoren, die am IO-Link-Master (Mitte) hängen, werden über die TBSB-Box (oben) sicher abgeschaltet

Sicherheitsprogrammierung per Drag-and-Drop

Die Programmierung der Steuerungsapplikation nehmen Anwender in Banners kostenloser Safety-Controller-Software vor. Sie bietet eine einfache grafische Oberfläche zur Konfiguration und Simulation von Sicherheitsapplikationen und diverse Exportmöglichkeiten für die Dokumentation. Vorgefertigte Bausteine für klassische Sicherheitskomponenten erlauben die Programmierung von Sicherheitsapplikationen per Drag-and-Drop ohne Programmiercode. Über USB-Sticks lassen sich die Programme kopieren und auf andere Controller übertragen. So lassen sich die Programme am Desktop entwerfen, testen und später auf die Applikation übertragen. Die Verdrahtung muss vor Ort im Feld über klassische Punkt-zu-Punkt-Verbindungen erfolgen.

Ein besonderes Feature des Safety Controllers SC10 ist das ISD-Sicherheitsprotokoll. Über ISD (In-Series Diagnostics) können bis zu 32 Sicherheitsgeräte als Slaves verkettet angeschlossen werden. Das Protokoll wird auf die 24-V-Spannung aufmoduliert. So sind Informationen über Schaltzustände und Diagnosen der Sicherheitssensoren über die Steuerung abrufbar. Dieses Feature bieten sonst nur teurere sichere Steuerungen mit Feldbus- oder Ethernet-Kommunikation.

Viele Sicherheits-Controller lassen sich zudem einfach erweitern. Wenn alle Eingänge und Ausgänge am XS26-Controller belegt sind, kann deren Zahl durch Ergänzungsmodule aufgestockt werden. Der Anwender kann bis zu acht Elemente ergänzen. Zur Wahl stehen Ein- oder Ausgangs- sowie OSSD- oder Relais-Module.

Ein Nachteil der zentralen Sicherheitsarchitekturen ist häufig die aufwendige Verdrahtung bei der Inbetriebnahme. Eine Zwischenlösung können dann lokale Schutzkästen sein, in denen die IP20 Controller dezentral verbaut werden.

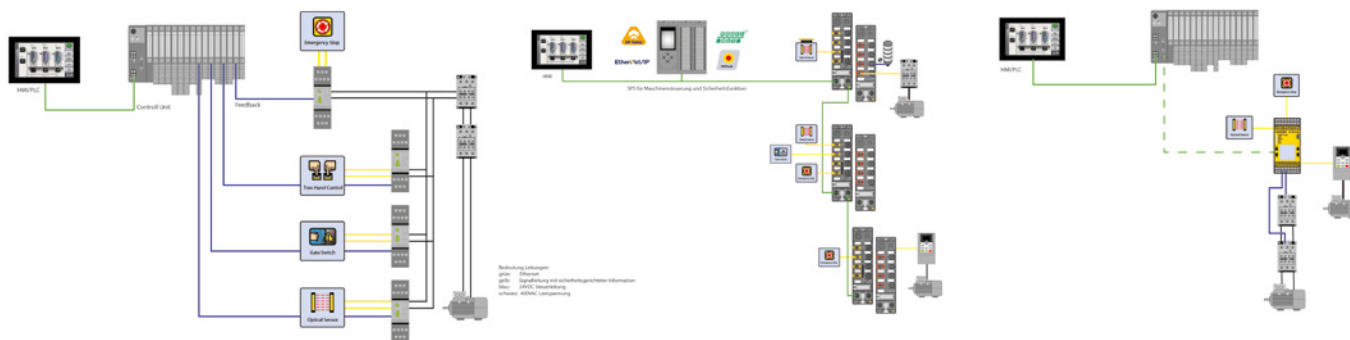
Schnelle Inbetriebnahme durch Offline-Engineering

Die Sicherheitsapplikation kann auf dem autarken Safety-Controller von Banner vorprogrammiert und getestet werden, auch wenn eine Maschine oder das einzelne Maschinenmodul noch offline sind. Der Test von Sicherheitsprogrammen am Schreibtisch und in der Werkstatt beschleunigt die Inbetriebnahme erheblich. Im Live-Betrieb kann die zentrale Sicherheitssteuerung über Multiprotokoll-Ethernet die Applikation dann übernehmen. Konsequenterweise modulare Maschinen können so ihre Sicherheitsfunktionen lokal am Modul steuern.

Dezentrale Sicherheitskonzepte, zentral gesteuert

Wer den Aufbau von Schutzgehäusen zentral oder dezentral minimieren möchte, um seine Maschinen schnell verdrahten und in Betrieb nehmen zu können, der kommt an dezentralen Sicherheitsinstallationen mit IP67-Komponenten nicht vorbei. Wie in der Automatisierungstechnik allgemein, setzen sich auch in der Sicherheitstechnik dezentrale Architekturen zunehmend durch.

Dabei sind zwei Typen zu unterscheiden: Dezentrale Konzepte, die sichere Signale auf IP67-I/O-Modulen sammeln und über Feldbusse oder sichere Ethernet-Protokolle zur zentralen Sicherheitssteuerung bringen. Und volldezentralisierte Installationen, die Sicherheitsapplikationen direkt im Feld auf IP67-Safety-Controllern steuern. Welche der beiden Alternativen besser ist, entscheidet sich im Einzelfall. Beide dezentralen Architekturen bieten den Vorteil effizienter Verdrahtung mit Ethernet-Leitungen über Standard-Steckverbinder. Die hohe Informationsdichte und die Möglichkeit der Kommunikation von Metainformationen erleichtern Inbetriebnahme und Diagnose der Applikationen.



Hohe Zykluszeiten fordern hohe Sicherheitsabstände

In Applikationen mit zentralen Sicherheitssteuerungen kann es bei Berücksichtigung der Buszykluszeiten und bei verketteten Nachrichten dazu kommen, dass höhere Reaktionszeiten einkalkuliert werden müssen, was wiederum größere Abstände der Schutzeinrichtungen zu den Gefahrenquellen erfordert.

Mit Turcks Sicherheits-I/O-Modulen TBPN für Profisafe und TBIP für CIP Safety können beide Lösungen umgesetzt werden – zentral oder dezentral gesteuert. Beide Modulversionen sind als Full-Safety-Module mit vier sicherheitsgerichteten universellen Ein-/Ausgängen und vier sicherheitsgerichteten Eingängen erhältlich, die bis zu 16 einkanalige sichere Signale sammeln können. Die Module schalten zuverlässig bis zu 2 Ampere pro Ausgang, bei maximal 9 Ampere pro Modul. Sie sind einsetzbar bis zu PL e, Kat. 4, SILCL 3.

Sollten in bestimmten Anwendungen weniger sicherheitsgerichtete Ein/Ausgänge ausreichen und gleichzeitig noch Standard-I/Os erforderlich sein, bietet Turck dafür mit seinen Hybrid-Modulen eine innovative Speziallösung, ebenfalls für Profisafe (TBPN) und CIP Safety (TBIP). Die Hybrid-Module bieten zwei sichere digitale Eingänge sowie zwei sichere, universelle digitale Ein- oder Ausgänge und vier universelle digitale Standard-Ein- oder Ausgänge. Sie schalten dieselben Ströme und sind in denselben Sicherheitskategorien einsetzbar wie die Full-Safety-Module. Die Hybrid-Safety-Module verfügen über zwei IO-Link Masterports Class A; der zweite Port kann sicherheitsgerichtet abgeschaltet werden.

Alle Turck-Safety-Module haben einen sicheren Controller an Bord, der Vorverarbeitungen bei zeitkritischen Anwendungen oder auch Sicherheitsapp-

likationen ohne Verbindung zu einer fehlersicheren Steuerung umsetzen kann. Die spätere Einbindung einer Stand-alone-Applikation in eine sichere Steuerung mit Profisafe- oder CIP-Safety-Kommunikation ist im Nachhinein immer möglich. Die Module lassen sich bequem via Softwaretool programmieren. Im Betrieb erleichtert ihr integrierter Webserver Diagnose und Inbetriebnahme. Mit ihrem robusten Design mit vollvergossener Modulelektronik eignen sich alle Module für den Einsatz im rauen Industrieumfeld. Sie erfüllen die Schutzarten IP65/IP67/IP69K und arbeiten zuverlässig auch in einem erweiterten Temperaturbereich von -40...+70 Grad Celsius.

Dezentrale Lösung mit passiver Sicherheit

Eine Variante dezentraler Sicherheitskonzepte ist die sogenannte passive Sicherheit. Diese Applikationen sind relativ kostengünstig und bieten eine ideale Kombination der Vorteile zentraler und dezentraler Sicherheitsarchitekturen. Passive Sicherheitsapplikationen versorgen im Unterschied zu klassischer Sicherheitstechnik nicht jeden Aktor über einen separaten sicheren Ausgang. Passive Safety stellt lediglich sicher, dass die Spannung einer Aktorengruppe in kritischen Situationen sicher abgeschaltet wird. Dazu trennen die eingesetzten I/O-Gruppen Sensorspannung (V1) galvanisch konsequent von der Aktorspannung (V2). Die Aktorik der Maschine wird unabhängig von ihrem Zustand abgeschaltet.

Sicherheit auch mit IO-Link

Turck bietet ein durchgängiges Konzept passiver Sicherheitslösungen an. Alle Turck-I/O-Komponenten inklusive der IP67-I/O-Link-Master bieten eine konsequente galvanische Trennung von V1 und V2. Auch Turck I/O-Hubs zur Übertragung von bis zu 16 digitalen Signalen über IO-Link trennen V1 und V2. Das erlaubt den Entwurf sicherer I/O-Link-Applikationen auch ohne ein IO-Link-Safety-Protokoll. Zur sicheren Abschaltung entwickelte Turck die TBSB-Abschaltbox. Sie wird an einen sicheren Kanal eines Safety-Moduls (von Turck oder anderen Herstellern) im Feld angeschlossen und schaltet im Sicherheitsfall die Aktorspannung der nachgelagerten Module sicher ab.

Dezentrale Sicherheitskonzepte bieten hohe Flexibilität, verkürzen Inbetriebnahmezeiten und erleichtern die Modularisierung



Dezentralen Sicherheitslösungen: Die TBSB schaltet die Aktorspannung V2 nachgelagerter Komponenten sicher ab

Autor | Michael Flesch ist Produktmanager für Sicherheitstechnik bei Turck
Webcode | more12070