Mit modularen Hardware-Architekturen zur zukunftssicheren funktionalen Sicherheit

Functional Safety inklusive

Die funktionale Sicherheit minimiert das Risiko von Verletzungen und Beschädigungen im Zusammenwirken von Mensch und Technik; Redundanz und mehrkanalige Datenverarbeitung gewährleisten Hochverfügbarkeit und verhindern katastrophale Fehlfunktionen. Während die Zertifizierung sicherheitsrelevanter Steuerungssysteme weiterhin Sache der Hersteller der Gesamtsysteme bleibt, bietet der Markt bereits zertifizierungsfreundliche System-on-Modules und eine einbaufertige Hardwareplattform.

TEXT: Peter Kemptner, Fachredakteur aus Salzburg **BILDER:** Microsys; iStock, indigolotos

Geräte, Fahrzeuge, Maschinen oder Anlagen sind heute oft hoch automatisiert, tauschen Daten aus und interagieren miteinander, teilweise auch vollkommen autonom. Das Internet der Dinge (IoT) beschleunigt diesen Trend zunehmend. Dennoch erfolgt in den meisten Fällen immer auch eine direkte oder indirekte Interaktion zwischen Mensch und Maschine.

Fehlfunktionen verhindern

Eine wesentliche Voraussetzung für die Nutzung automatisierter Systeme ist deren sicherer Betrieb. In allen technischen Branchen, von Kraftwerken und Verkehrsmitteln über Industrieanlagen und Medizintechnik bis zu Haushalts- und Unterhaltungsgeräten, spielt deshalb die funktionale Sicherheit (engl. Functional Safety; FuSa) eine zentrale Rolle.

Um das Risiko von Verletzungen und Beschädigungen zu minimieren, muss FuSa Fehlfunktionen infolge von Konstruktions-, Produktions- oder Dokumentationsfehlern, betrieblichen Ausnahmesituationen und Fehlbedienungen verhindern

und das System in einen sicheren Zustand versetzen. Um das Verletzungsrisiko zu minimieren, entziehen Maschinen- und Anlagenhersteller die beweglichen Komponenten komplexer Maschinen dem menschlichen Zugriff. Eine Schutzverletzung durch ungewolltes Öffnen von Türen oder Abdeckungen führt ebenso wie das Betätigen eines Notausschalters zum absoluten Stillstand der Anlage.

Mit Sicherheit produktiver

Dazu wurden Sicherheitsschaltungen lange Zeit durch harte Verdrahtung in Relaistechnik realisiert. Diese waren von der Steuerungselektronik unabhängig und erschwerten flexible, über eine plötzliche Systemabschaltung hinausgehende Reaktionen. Zudem erschwerte deren geringe Flexibilität Aus- und Umbauten an den zu schützenden Anlagen. Immer komplexere, häufig modular aufgebaute und im Betrieb veränderliche Maschinen und Anlagen machen eine differenziertere Reaktion auf unterschiedliche Schutzverletzungen erforderlich. Auch ist es nicht immer einfach möglich, Maschinen oder Anlagen einzuzäunen. Speziell bei mobilen Arbeitsmaschinen oder Transportsystemen entfällt diese Option, während deren zunehmender Automatisierungsgrad die Sicherheitsanforderungen an ihre Steuerungssysteme weiter steigen lässt.

Deshalb sind mittlerweile die frei programmierbare Sicherheitssteuerungen Standard. Gemeinsam mit diesen bildet eine fortschrittliche sicherheitsgerichtete Sensorik die Basis für eine zugleich anwendungsfreundliche und effektive Gestaltung der Sicherheitstechnik. So ermöglichen zum Beispiel 360°-Laserscanner und Time-of-Flight (ToF) Kameras die sicherere Gegenstands- und Personenerfassung. Diese Technologien dienen als Grundlage eines sicheren Betriebs von fahrerlosen Transportfahrzeugen (FTF/AGV) und autonomen mobilen Robotern (AMR).

Der Datenaustausch mit IO-Baugruppen, Sensoren und Aktoren erfolgt in modernen FuSa-Konzepten über Datenbusse. Dabei kommt, zumindest in Ethernet-basierten Netzwerken, meist das „Black Channel“ Prinzip zu Anwendung, bei dem die potentiellen Fehlerquellen der Übertragungsstrecke über Safety-Datenprotokolle abgefangen werden. Auf der Telegrammebene sind beispielsweise Daten mehrfach vorhanden und durch Prüfsummen oder kryptografisch geschützt. So können Nachrichten bestätigt und die Übertragungsstrecke periodisch auf Funktion geprüft werden.

Mit Sicherheit mehr Freiheit

Dadurch lassen sich sicherheitsgerichtete Steuerungen und I/O-Baugruppen zur Anbindung der Sensoren an beliebiger Stelle im System platzieren. Zudem bieten elektrische Antriebe heute mit sicherheitsgerichteten Funktionen nach EN 61800-5-2 wie sicher abgeschaltetes Moment (STO), sichere Bewegungsrichtung (SDI), sichere Geschwindigkeit (SLS) oder sicher begrenzte Beschleunigung (SLA) zahlreiche Alternativen zur bloßen Abschaltung.

Der Einsatz dieser sanfteren Mechanismen zum Schutz des Personals hilft unter anderem, Beschädigungen durch abrupte Sicherheitsabschaltungen zu vermeiden. Ein sicherer Zustand ohne vollständigen Stillstand erleichtert den Einrichtebetrieb und ermöglichte die Entwicklung kollaborativer Industrieroboter, sogenannter Cobots. Diese sind auch ohne trennende Schutzeinrichtung ausreichend sicher, um

Die einfach zu integrierenden System-on-Module (SoM) auf Basis moderner Multicore-Prozessoren von NXP eignen sich durch deren Architektur und ihr zertifizierungsfreundliches Design bestens für die Entwicklung sicherer Steuerungssysteme.

mit dem menschlichen Kollegen zeitgleich Hand in Hand zu arbeiten.

Über den gemeinsamen Bus kann die nicht sichere Steuereinheit auch den aktuellen Zustand der Sicherheits-Sensorik abfragen. Das ermöglicht die einfache Inbetriebnahme oder Diagnose bei Fehlerzuständen. Zudem lassen sich bei sicherheitsbedingten Stillständen durch entsprechende Prozessanpassungen problematische Anlagenzustände im Vor- oder Nachlauf verhindern. Eine parametrierbare und damit modifizierbar gestaltete FuSa-Programmierung kann darüber hinaus auch bedarfsgerechte Veränderungen der Konfiguration modularer Maschinen oder Anlagen zulassen, um diesen die Eignung für die Herausforderungen von Industrie 4.0 zu verleihen.

Sicherheit durch Verfügbarkeit

Während es bei Industriemaschinen und -anlagen gute Praxis ist, sie in einen definierten Zustand mit reduziertem Gefahrenpotenzial zu bringen, gibt es einen solchen bei anderen Anwendungen oft überhaupt nicht. Man denke an einen Trieb- oder Leitwerksausfall im fliegenden Flugzeug, an ein Bremsversagen im Eisenbahnzug oder an eine Fehlfunktion der Lenkung im Automobil.

Diese Fälle erfordern eine andere Form der Sicherheit, nämlich einen Schutz vor Systemausfall durch hohe Verfügbarkeit. Hergestellt wird die sogenannte Ausfallsicherheit meist durch redundant aufgebaute Computersysteme. Dies kann von einer einfachen Verdoppelung der Rechenkanäle mit Informationsredundanz (beide haben Zugriff auf Ein/Ausgangsdaten) bis hin zu mehrfach redundant-dissimilaren Systemen mit 5-15 Steuerungsrechnern, mit diversen Rückfallebenen und Notbetriebsmodi im Luftfahrtbereich reichen.

Besonders gefragt ist die Dissimilarität der Berechnungskanäle in Anwendungen mit sehr hohem Gefährdungspotential, etwa in der Luftfahrt, aber auch für Anwendungen der höchsten Sicherheitslevel (SIL3, SIL4) in Industrie- und Bahnanwendungen. Um Single-Event-Upsets, Speicherfehlern oder besonders schwer aufzulösenden Fehlerkaskaden sowie Common-Cause-Failures zu begegnen, kommen dabei zumeist unterschiedliche Prozessoren in den redundanten Rechenkanälen zum Einsatz. Dies schützt auch vor Chargenfehlern eines Herstellers, die bei Ziel-Ausfallraten unterhalb von 10-9 beziehungsweise 10-10 pro Betriebsstunde ebenfalls zu betrachten sind.

Modulare Sicherheit

Für die sicherheitsgerichtete Ausgestaltung von Maschinen oder Anlagen für die industrielle Produktion bieten sich handelsübliche, nach IEC 61508 zertifizierte Safety-Systeme arrivierter Automatisierungssystemhersteller an. Dagegen für zahlreiche andere Aufgaben, aber auch für Entwicklung und Herstellung dieser Safety-CPUs ist es erforderlich, hardwareseitig auf einer anderen Ebene anzusetzen.

Dafür bietet sich als oft wirtschaftlichere und risikoärmere Alternative zur völligen Neuentwicklung vom Halbleiter weg die Verwendung von System-on-Modules (SoMs) an. Diese haben den Vorteil, dass sich Systemhersteller bei der Entwicklung von Elektronikbaugruppen nicht mit den komplexen prozessornahen und bei heutigen Taktraten tief in die Physik reichenden Themen herumschlagen müssen. So können sie sich bei der Systementwicklung auf die Entwicklung der Software und die Bedienung handhabbarer Schnittstellen an den Modulgrenzen konzentrieren.

Die miriac SoMs von Microsys etwa bringen alle Voraussetzungen mit, um bei entsprechender Außenbeschaltung und Software auf dem Weg zur Zertifizierung nicht auf hardwareseitige Hürden zu stoßen. Dazu gehören Merkmale wie zum Beispiel eine separate Überwachung der Stromversorgung, die auch das Realisieren eines unabhängigen Watchdog Timers ermöglicht. Auch verbaut MicroSys in den miriac-SoMs nach der strengen Automobilnorm AEC-Q100 qualifizierte Bauteile , um erhöhte Anforderungen an die Fertigungsqualität der Halbleiter mit abzudecken. Wesentlichen Einfluss auf die Zertifizierbarkeit von Rechnersystemen hat allerdings die anwendungsspezifische

Die aufgaben-, aber nicht kundenspezifisch entwickelte Autonomous Control Unit ist eine einbaufertige, modular ausbaufähige Hardwareplattform für die sichere Automatisierung.

Software. Deshalb sind SoMs im Gegensatz etwa zu sicherheitsgerichteten Sensoren nicht als vorzertifizierte generische Sicherheitselemente verfügbar.

Application Ready Plattform

Die Mehrkern-Prozessorarchitektur moderner Prozessoren lässt sich nicht ohne weiteres dazu nutzen, sichere und nicht-sichere Applikationen (Mixed-Criticality) auf einem einzigen Prozessor parallel abzuarbeiten. Noch weniger eignet sie sich aufgrund der vielfältigen Common-Cause-Fehlerpotentiale und der generellen Basisausfallrate der komplexen Halbleiter für den Aufbau von redundanten Systemen oder gar eines mehrkanaligen Systems für hoch sichere Anwendungen auf Basis eines einzigen Prozessors.

Deshalb entwickelte Microsys die Hardware für eine aufgaben-, aber nicht kundenspezifische Steuerungsplattform als einbaufertiges Gesamtsystem, zunächst in erster Linie für mobile Arbeitsmaschinen. Kernprodukt ist ein Carrierboard, das neben dem zentralen miriac MPX-LX2160A über drei M.2 Slots verfügt, die für bis zu drei SSD-Speichermodule oder ein bis zwei Hailo-8 KI-Prozessormodule genutzt werden können. Optional ist die Erweiterung mit einem miriac MPX-S32G274A oder miriac MPX-S32G399A angedacht. Auf diese Weise kann es eine sehr hohe Rechenleistung für komplexe Aufgaben erlangen, alternativ aber auch einen unabhängigen, dissimilaren internen Rechenkanal. Damit lässt sich die Sicherheitsstufe SIL 3 erzielen.

Neu entwickelt wurde auch das Gehäuse, das die Elektronik erst zu einem einbaufertigen Gesamtsystem macht. Staub- und wasserfest nach Schutzart IP 68, dient es neben dem Schutz der verbauten Elektronik der Wärmeableitung. Da es dem Unternehmen gelungen ist, die Leistungsaufnahme der voll bestückten Einheit trotz der extrem hohen Verarbeitungsleistung und der Vielfalt an Schnittstellen auf 60 W zu begrenzen und vollständig passiv abzuführen, kommt das Gerät ohne Lüfter oder andere aktive Kühlung aus. ❐