MicroSys
Creating Embedded Systems

Whitepaper

Plattformen für Functional Safety

Mit modularen Hardwarearchitekturen zur zukunftssicheren funktionalen Sicherheit

Einleitung

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 Gesamtsystemhersteller bleibt, bietet MicroSys diesen zertifizierungsfreundliche System-on-Module und eine einbaufertige Hardwareplattform. Das erleichtert und beschleunigt die Entwicklung anwendungsspezifischer sicherer Lösungen für hochautomatisierte Maschinen und Anlagen.

Geräte, Fahrzeuge, Maschinen oder Anlagen sind heute hoch automatisiert, tauschen Daten aus und interagieren miteinander, teilweise auch vollkommen autonom. Das Internet der Dinge (IoT) beschleunigt diesen Trend. Dennoch erfolgt 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.

Oberstes Ziel der funktionalen Sicherheit ist es, das Risiko von Verletzungen und Beschädigungen zu minimieren, indem sie Fehlfunktionen infolge von Konstruktions-, Produktions- oder Dokumentationsfehlern, betrieblichen Ausnahmesituationen und Fehlbedienungen sowie Hardwaregebrechen verhindert und automatische Systeme in Gefahrensituationen in einen für Menschen ungefährlichen Zustand bringt.

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 Öffnen von Türen oder Abdeckungen führt ebenso wie das Betätigen eines Notausschalters zum Stillstand der Anlage.

Mit Sicherheit produktiver

Dazu wurden Sicherheitsschaltungen lange Zeit durch harte Verdrahtung in Relaistechnik realisiert. Diese waren von der Steuerungselektronik völlig 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 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 360°-Laserscanner und Time-of-Flight (ToF) Kameras die sicherere Gegenstands- und Personenerfassung 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 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

Während in industriellen Anwendungen die Sicherheit in der Vergangenheit in erster Linie durch Schutzumhausungen hergestellt wurde, verlangen offene Lösungen für die Produktionsautomatisierung wie kollaborative Roboter, fahrerlose Transportsysteme und autonome mobile Roboter nach differenzierten Lösungen zur Sicherstellung der funktionalen Sicherheit. Zukunftsthemen wie autonome Fahrzeuge oder Baumaschinen wären ohne FuSa völlig undenkbar.

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 mit dem menschlichen Kollegen 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.

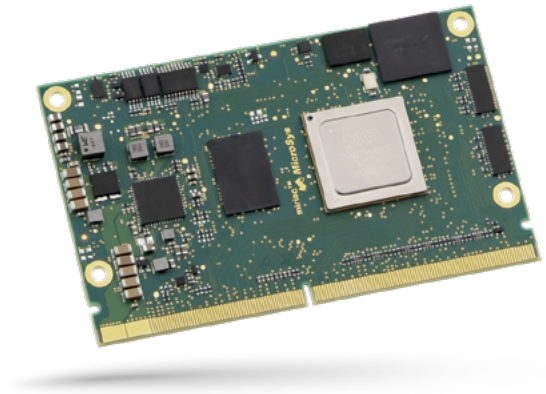
Solche Fälle erfordern eine andere Form der Sicherheit, nämlich einen Schutz vor Systemausfall durch hohe Verfügbarkeit. Hergestellt wird die sogenannte Ausfallsicherheit meist durch redundant aufgebaute Computersysteme. Dies kann von einer einfachen Verdoppelung der Rechenkanäle mit Informationsredundanz (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 bzw. 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. 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 Soft-



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

miriac® MPX-S32G274A

ware und die Bedienung handhabbarer Schnittstellen an den Modulgrenzen konzentrieren.

Der bayerische Hersteller MicroSys Electronics GmbH entwickelt und produziert als Gold Partner des europäischen Prozessorherstellers NXP SoMs auf Basis von dessen Prozessortechnologie. „Moderne Multicore-Prozessoren von NXP wie der S32G sind nicht nur sehr leistungsfähig, sondern eignen sich durch ihre spezifische Architektur besser als viele andere für die Entwicklung sicherer Steuerungssysteme“, erklärt Jörg Stollfuß, Field Application Engineer bei MicroSys Electronics. „Auf dieser Basis schufen wir einfach zu integrierende Module mit zertifizierungsfreundlichem Design als Alternative zu FuSa-Eigenentwicklungen auf Platinenebene.“

Die miriac® SoMs von MicroSys 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 z. B. 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 Software. Deshalb sind SoMs im Gegensatz etwa zu sicherheitsgerichteten Sensoren nicht als vorzertifizierte generische Sicherheitselemente verfügbar.

Application Ready Platform

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

The task specific but not custom Autonomous Control Unit can accommodate a miriac® MPX-LX2160A SoM and up to three SSD memory modules or one or twoHailo-8™ AI processor modules in three M.2 Slots. It is also prepared for an optional extension using a miriac® MPX-S32G274A or miriac® MPX-S32G399A SoM.This makes it a ready-to-install, modular hardware platform for use in safe automation systems.

macht. Staub- und wasserfest nach Schutzart IP 68, dient es neben dem Schutz der verbauten Elektronik der Wärmeableitung. Da es MicroSys 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.

„Mit dieser Autonomous Control Unit auf Basis des SoM-Moduls miriac® MPX-LX2160A bietet MicroSys nicht nur Herstellern mobiler Arbeitsmaschinen eine einbaufertige, modular ausbaufähige Hardwareplattform für die Automatisierung ihrer Produkte an“, bestätigt Ina S. Schindler, Geschäftsführerin der MicroSys Electronics GmbH. „Diese können sich daher voll auf die Entwicklung der Software konzentrieren.“ware und die Bedienung handhabbarer Schnittstellen an den Modulgrenzen konzentrieren.

Jörg Stollfuß, Field Application Engineer
bei der MicroSys Electronics GmbH

„Moderne Multicore-Prozessoren von NXP wie der S32G sind nicht nur sehr leistungsfähig, sondern eignen sich durch ihre spezifische Architektur besser als viele andere für die Entwicklung sicherer Steuerungssysteme. Auf dieser Basis schufen wir einfach zu integrierende Module mit zertifizierungsfreundlichem Design als Alternative zu FuSa-Eigenentwicklungen auf Platinenebene.“

„Mit der Autonomous Control Unit auf Basis des SoM-Moduls miriac® MPX-LX2160A als einbaufertige, modular ausbaufähige Hardwareplattform für die sichere Automatisierung können sich Systemhersteller voll auf die Entwicklung der Software konzentrieren.“

Ina S. Schindler, Geschäftsführerin
bei der MicroSys Electronics GmbH

Über MicroSys Electronics

MicroSys Electronics entwickelt und produziert seit 1975 Embedded Systemlösungen, ist Gold Partner von NXP und integriert maßgeblich deren S32 Automotive, Layerscape und QorIQ Prozessortechnologie. Designs auf Basis von System-on-Modules (SoMs) sind die Stärken des Unternehmens aus Sauerlach bei München. Das Portfolio reicht von applikationsfertigen SoMs über kundenspezifische Carrierboard-Designs bis hin zu komplett integrierten Systemen. Einsatzbereiche dieser besonders robusten und langzeitverfügbaren Designs finden sich vor allem in Märkten, in denen Sicherheitsstandards analog der IEC61508 gefordert sind, wie Bahntechnik (EN50155), Luftfahrt (DO-160) und Mobile Maschinen (ISO 13849) sowie Fertigungsroboter (ISO 10218), Steuerungen (IEC 61131-6) und Antriebssysteme (IEC 61800-5-2). Weitere Anwendungsbereiche finden sich in der Medizintechnik (60601) und in kritischen Infrastrukturen, wie dem Nuklearsektor (IEC 61513) oder der Prozessindustrie (IEC 61511). MicroSys arbeitet in all diesen Branchen eng mit seinen Kunden zusammen, um sicherzustellen, dass die jeweils zugehörigen Standards vollständig erfüllt werden.

Weitere Informationen unter www.microsys.de

NXP Gold Partner

MicroSys Electronics GmbH

Mühlweg 1
82054 Sauerlach, Germany
Tel: +49 (8104) 801-0
Fax: +49 (8104) 801-110
Web: www.microsys.de
Email: info@microsys.de