

INTELLIGENTES SICHERHEITSKONZEPT HILFT ZEIT UND GELD SPAREN

Funktionale Sicherheit leicht gemacht

Die Grundidee bei der Entwicklung sicherer Systeme ist es, einen zuverlässigen Betrieb zu gewährleisten und das Verhalten im Fehlerfall genau zu definieren. Traditionell waren Sicherheits-Software, -Hardware und -Tools Insellösungen, die zwar Einzelteile der Anforderungen erfüllten, aber nicht Hand in Hand arbeiteten. Das „PRO-SIL“-Konzept stellt nun eine komplette Lösung dar, mit der sich das Risiko minimieren, die Kosten senken und die Komplexität reduzieren lassen.

MANFRED CHOUTKA

Der Standard IEC 61508 wurde Mitte der 1980er-Jahre entwickelt und seitdem ständig verbessert. Er definiert das Design von sicheren Systemen für elektrische und elektronische Geräte. Die Maßnahmen, die sicherstellen, dass ein System IEC-61508-konform ist, hängen vom geforderten Sicherheits-Integritätslevel für jede Systemgefährdung ab (SIL 1 bis SIL 4 für Industrieanwendungen und ASIL A bis ASIL D für Automotive-Applikationen).

Bei einer Single-Channel-Architektur mit nur einem Mikrocontroller ist das höchste Sicherheits-Integritätslevel auf SIL 2 beschränkt. SIL-3- oder ASIL-C/D-Systeme und -Sicherheitsprodukte wurden mithilfe von mehreren CPUs entwickelt, die sich um den Selbsttest kümmern und die Redundanz sicherstellen. Aber dieser Ansatz ist komplex und kostenintensiv, er benötigt eine große Leiterplattenfläche, und die Abdeckung ist aufgrund von Synchronisations- und Kommunikationsproblemen zwischen den zwei CPUs eingeschränkt. Ein neuer Ansatz überwindet

KONTAKT

INFINEON TECHNOLOGIES AG,
85579 Neubiberg,
Tel. 0800 951951951,
Fax 089 2349553431,
www.infineon.com,
Embedded World: 4-142

diese Einschränkungen und die mittelmäßige Diagnoseabdeckung, indem spezielle externe Hardware-Blöcke hinzugefügt werden und eine Software-Bibliothek auf einem Standard-32-Bit-Mikrocontroller mit zwei Prozessorkernen läuft. Mit diesem Ansatz kann ein System schnell und zuverlässig sicher gemacht werden, denn der Entwicklungsaufwand und die Materialkosten reduzieren sich nur noch auf einen Mikrocontroller und ein intelligentes Sicherheitskonzept mit allen dazugehörigen Komponenten, einschließlich der Anwendung von Selbsttestfunktionen, die gemäß IEC 61508/ ISO 26262 entwickelt wurden.

Anstatt einen zweiten externen Prozessorkern zu nutzen, um funktionale Fehler des Mikrocontrollers zu evaluieren, ist der „TriCore“ bereits mit zwei Kernen ausgestattet (**Bild 1**) – mit der eigentlichen TriCore-CPU (Mikrocontroller und DSP) und dem Peripheral-Control Processor (PCP) – womit ein externer zweiter Core für die Sicherheitsevaluierung überflüssig wird.

TOOLBOX

Das Servicepaket „SafeTkit“. In Partnerschaft mit dem Toolanbieter Hitex (www.hitex.com) hat Infineon ein umfassendes Service-Paket entwickelt. Das SafeTkit ist eine Lösung auf Board-Niveau, welche die TriCore-MCU, den CIC61508, alle relevante Software und die dazugehörige Dokumentation enthält. Damit können die Zertifizierungen gemäß IEC61508 einfach und schnell erreicht werden. Neben der SafeTcore-Testsoftware enthält das Design-Paket eine komplette Tool Chain inklusive eines kostenlosen TriCore-Compilers. Darüber hinaus bietet Hitex umfassende Design-Unterstützung, Training und Beratung an.

Das SafeTkit ist eine Lösung auf Board-Niveau; sie beinhaltet die TriCore-MCU, den CIC61508, die relevante Software sowie die Dokumentation



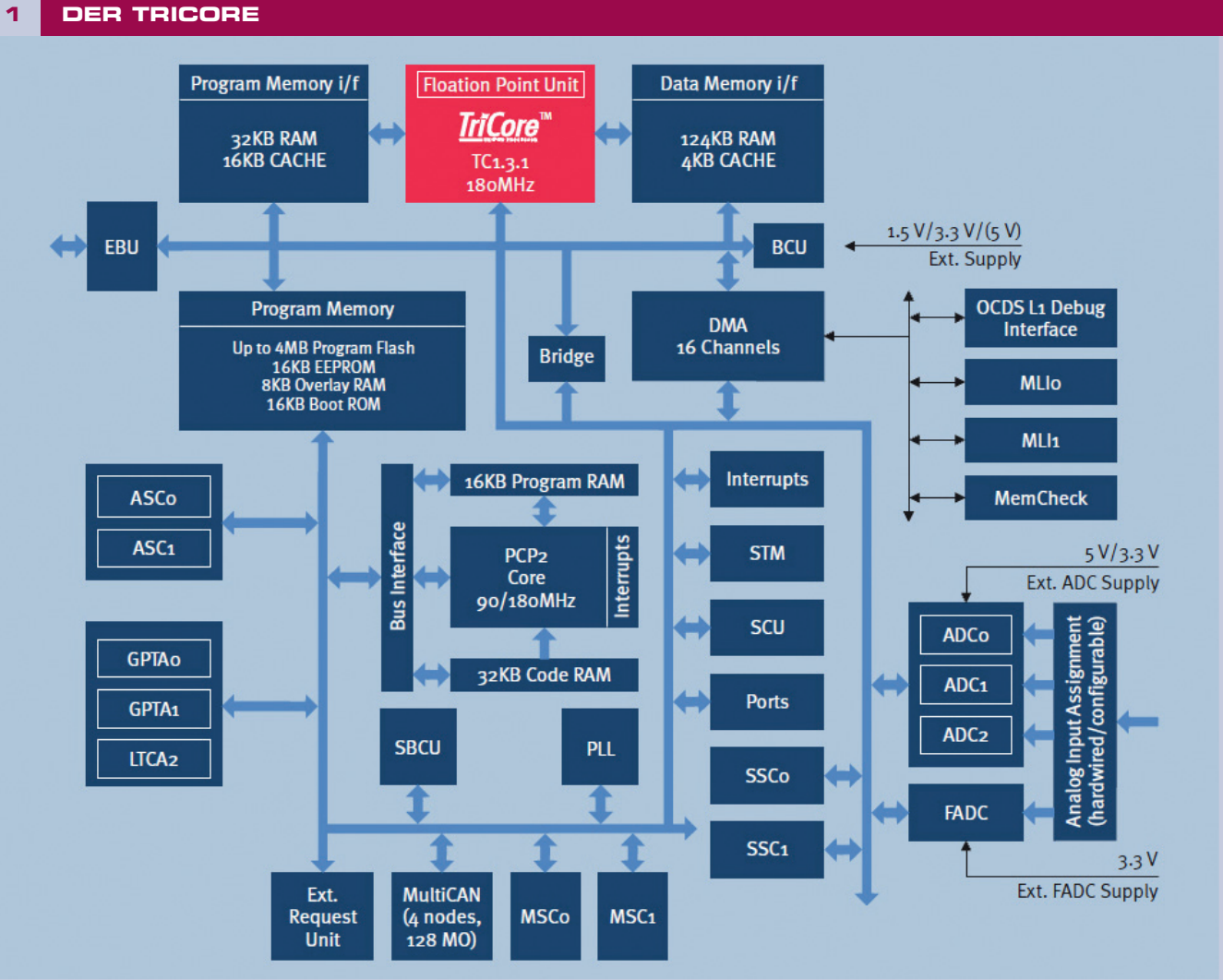


Bild 1. Der PCP implementiert die Selbsttestfunktionen

Komplettes Design-Paket

Es gibt bereits verschiedene Lösungen am Markt, um sicherheitskritische Applikationen zu implementieren. Während die meisten Anbieter solche Ansätze für Automotive-Anwendungen anbieten, ist die Verfügbarkeit für andere Anwendungsgebiete, einschließlich industrieller Applikationen, beschränkt, und die Produkt-Roadmaps sind limitiert. Aufbauend auf seinen Erfahrungen mit stringenten Sicherheitsanforderungen im Automotive-Segment hat Infineon seine PRO-SIL-Familie mit Sicherheitsprodukten entwickelt, mit denen das Unternehmen die steigenden Sicherheitsanforderungen des Industriemarkts adressiert. Die bewährten Automotive-Lösungen können einfach in anderen Applikationen genutzt werden, während gleichzeitig ein großes Produktspektrum zur Verfügung steht. Die PRO-SIL-Imple-

Name	Description	Name	Description
BCU	Bus control check	MPU	Memory Protection check
Boot ROM	Boot code integrity check	PCP CRC	PCP SafeTcore integrity check
CAN	CAN check	PCP ISR	PCP interrupt routine priorities
CAN LLC	CAN Link Layer Controller	PCP Protection	PCP memory access protection
Core SFR	CPU SFR configuration check	RAM	RAM check
DMA	DMA check	RAM	RAM Protection check
ECC Flash	ECC Flash check	SBST	Opcode test
ECC LMB	ECC system on LMB bus	SFR	Peripheral SFR check
ECC MultiCAN	ECC check MultiCAN RAM	Trap	Trap system test
FLX	FlexRay check	Watchdog	Internal watchdog test
FLX RAM	FlexRay RAM	ASIC	Connectivity to ext. watchdog
ICACHE	Instruction Cache check	APPL ADDR	User Application Address test
ISR	Interrupt structure	APPL RAM	User Application RAM test
MEMCHK	CRC32 check	APPL ROM	User Application ROM test

Tabelle A. SafeTcore-Testbibliothek: Die meisten dieser Tests sind bereits implementiert, sodass sie schon beim Start laufen können

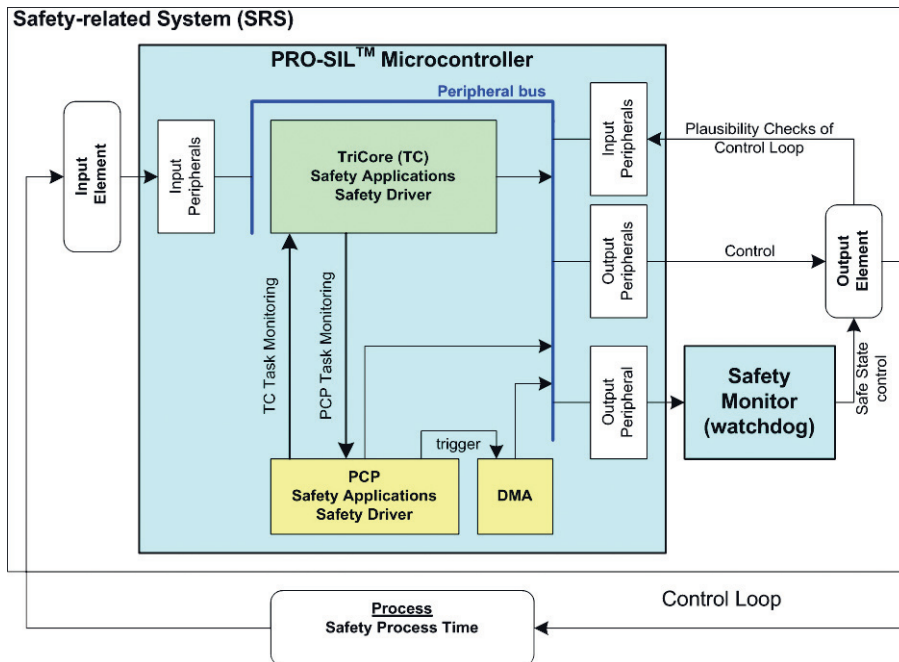


Bild 2. Ein SRS, das mithilfe eines TriCore als Haupt-Controller, eines Sicherheitsüberwachungs-Chips (Watchdog) und der SafeTcore-Testbibliothek realisiert wurde

mentierung beruht auf dem 32-Bit-TriCore oder dem 16-Bit-„XC2300“-Mikrocontroller, der „SafeTcore“-Testbibliothek und dem Watchdog-Chip „CIC61508“ (**Bild 2**). Diese vollständig verifizierte Implementierung ist konform mit den Anforderungen gemäß IEC 61508.

Das Sicherheitskonzept basiert auf der so genannten Challenge-Response-Technik, bei der der PCP auf dem TriCore-Chip als Challenger fungiert und die Haupt-CPU des TriCore die Tests ausführt. Informationen werden über eine gemeinsame Speicherstruktur ausgetauscht, wobei die Daten in unterschiedlichen Bereichen redundant gehalten werden. Auf dem PCP sind Selbsttestfunktionen implementiert, die von einem externen intelligenten Watchdog (CIC61508), der wiederum mit dem TriCore-Chip über eine SPI-Schnittstelle verbunden ist, zusätzlich überwacht werden (**Bild 3**). Der Watchdog ist eine effektive Maßnahme, um Ausfälle (Common Cause Failures, CCF) zu minimieren. Der Watchdog kommuniziert mit dem TriCore-Chip in speziellen Zeitfenstern, um den Takt, die Spannungen und den korrekten Betrieb des TriCore-Chips gemäß den Standards zu überprüfen. Der TriCore wiederum überwacht im Gegenzug die Stromversorgung des CIC61508-Bausteins und den korrekten Betrieb über Ferndiagnosemaßnahmen. Die Fehlererkennung (Hardware-Fehler und die Überwachung der Tasks) ist aufgeteilt auf die Haupt-CPU des TriCores und den PCP.

Die PCP-Software besteht aus dem PCP-Selbsttest, der C/R- (Challenge/Response-) Kommunikation, der Watchdog-Kommunikation, einem Test-Execution- und einem Task-Monitor. Die SafeTcore-Bibliothek, die auf dem TriCore



APPLIKATION

Mobiler Sicherheits-

Controller. Parker Hannifin hat das PRO-SIL-Konzept zur Entwicklung eines neuen programmierbaren Hydraulik-Controllers „IQAN-MC3“ genutzt, den OEMs und Systemintegratoren in mobilen Anwendungen und Off-Highway-Equipment einsetzen können. Christer Sahlberg, Projekt-Manager bei

Parker Hannifin, kommentiert das Projekt wie folgt: „Das Design basiert auf einem „TC1197“. Die Komplexität lässt sich an folgenden Zahlen verdeutlichen, denen sich unsere Entwickler beim Design des IQAN-MC3 stellen mussten: 687 Design-Anforderungen bedeuteten 674 Zeilen Fehleranalyse in FMEDA, 2800 Software- und mehr als 500 Hardware-Tests. Dank des PRO-SIL-Konzepts waren wir in der Lage, das komplexe Design schnell und sicher abzuschließen.“

Die Markteinführung des neuen Controllers passt zeitlich zu dem steigenden Bedarf an Komponenten und passender Software, den Hersteller von mobilen Anwendungen und Off-Highway-Equipment für die Produktion und Entwicklung von Sicherheitssystemen haben. Denn sie wollen einerseits eine höhere Leistungsfähigkeit und andererseits eine Zertifizierung nach gültigen Standards zur funktionalen Sicherheit, wie EN ISO 13849-1 (Maschinenrichtlinie) oder IEC 61508, erreichen. Um diese Ziele zu erreichen, hat Parker Hannifin den IQAN-MC3 gemäß den IEC-61508-Vorgaben mithilfe der PRO-SIL-Produkte entwickelt. Damit sind der Betrieb und die Systemleistung aller Sicherheitsfunktionen gemäß SIL 2 gewährleistet.



Parker Hannifin nutzte das PRO-SIL-Konzept für die schnelle und sichere Entwicklung des programmierbaren Hydraulik-Controllers IQAN-MC3



FAZIT

Das PRO-SIL-SafeTcore-Paket

ist eine vollständige Lösung, die optimierte Halbleiter wie die TriCore- und XC2300-Mikrocontroller, Sicherheits- und Test-Software-Bibliotheken, Services und die dazugehörige Dokumentation beinhaltet. Das Paket eröffnet einen einfachen Weg zu einer erfolgreichen Zertifizierung der funktionalen Sicherheit. Das Konzept unterstützt sicherheitsrelevante Systeme nach IEC 61508 bis hin zu SIL 3.

läuft, ist ein konfigurierbarer Frame, der Testfunktionen anbietet, mit denen die Integrität des Prozessors und des Systems validiert werden können (**Tabelle A**). Die meisten dieser Tests sind bereits implementiert, sodass sie schon beim Start laufen können – oder aber während der Laufzeit im Hintergrund. Das typische Diagnoseintervall liegt bei 6,4 ms. Der komplexeste Test ist der auf dem Opcode basierende Selbsttest der TriCore-CPU. Mithilfe des Sicherheitskonzepts kann er insgesamt eine Diagnoseabdeckung von 96,5 Prozent erreichen. Dieser Wert ist im Vergleich zu anderen Tests, die auf dem Instruktionssatz basieren, deutlich besser. Hinzu kommt noch der Vorteil, dass der

Test unterbrechbar ist und eine niedrige Latenzzeit aufweist.

Die SafeTcore-Testbibliothek

Das SafeTcore-Paket enthält Tools, mit denen sich einerseits die geforderte Zertifizierung nach SIL 1 bis 3 (oder ASIL B bis D) und andererseits eine schnelle Markteinführung erzielen lässt. Die größten Herausforderungen bei der Zertifizierung bestehen darin, die geforderten Tests auf Siliziumebene zu erreichen und die Dokumentation für den Safety Case zu haben. Das SafeTcore-Paket ermöglicht beides, und zwar durch die Kombination einer hochgradig konfigurierbaren Treiberbiblio-

thek für die TriCore-Bausteinfamilie mit der Verfügbarkeit eines kompletten Satzes an Safety Manuals, Safety Cases und Anforderungs/Traceability-Datenbasen. Mithilfe der leistungsfähigen Selbsttest-routinen aus dem SafeTcore-Paket, die auf dem PCP während des Hochfahrens und zyklisch aus der Applikation heraus ablaufen, kann die korrekte Ausführung der Anwender-Software und der eigentlichen TriCore-CPU verifiziert werden.

Die Core-Testfunktionen sind mit detaillierten Peripherietests und einem automatischen Support für den Safety-Monitor-Chip kombiniert. Die Software-Tests aus der SafeTcore-Bibliothek stellen auch eine Überwachungsfunktionalität für das Betriebssystem zur Verfügung, um eine komplexe Task- und Prozess-Flow-Überwachung durchzuführen, die eine sichere Code-Ausführung mit einer Diagnoseabdeckung von über 99 Prozent gewährleistet. Das SafeTcore-Paket enthält auch ein Safety Manual, mit dem verschiedene Bibliothekselemente in die User-Applikation integriert werden können und das für die Zulassung gemäß des Sicherheits-Integritätslevels notwendig ist. (m/)

3 DAS KONZEPT

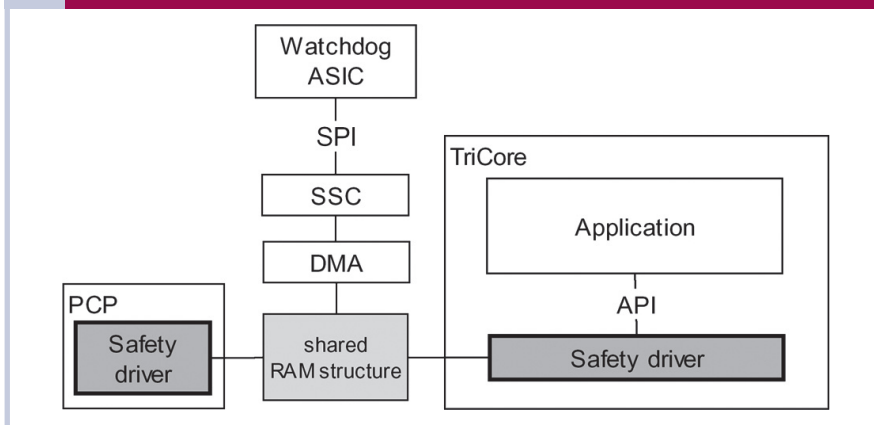


Bild 3. Das Sicherheitskonzept basiert auf einer Challenge-Response-Technik, bei welcher der PCP auf dem TriCore-Chip als Challenger fungiert und die Haupt-CPU des TriCores die Tests ausführt. Der PCP wiederum wird von einem externen intelligenten Watchdog (CIC61508) überwacht, der mit dem TriCore-Baustein über die SPI-Schnittstelle verbunden ist



DER AUTOR

MANFRED CHOUTKA ist Senior Manager Regional Marketing EMEA Microcontroller, Industrial and Multimarket, bei Infineon Technologies.

www.EL-info.de

615202