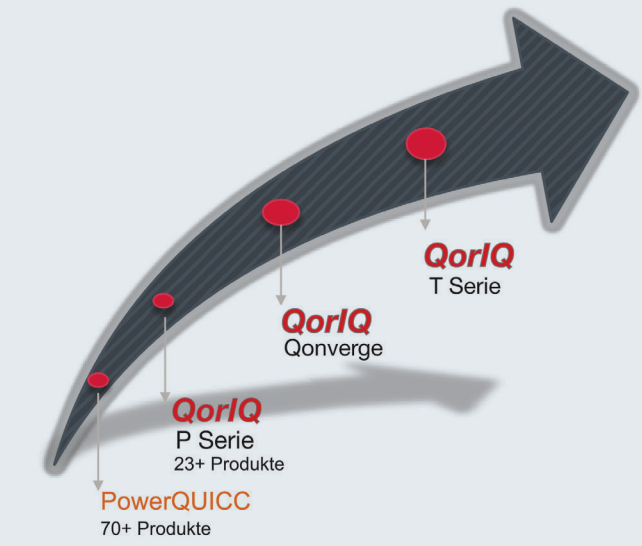
Ohne Verletzungsgefahr

Maschinensicherheit und Produktivität mit QorIQ-Multicore-Prozessoren.
Sicherheitsvorschriften wie die Maschinenrichtlinie haben unter anderem Auswirkungen auf die Architektur des Steuerungs-Subsystems. Anhand von QorIQ-Multicore-Prozessoren werden Lösungsansätze klar, die nicht nur den Sicherheitsaspekten Rechnung tragen, sondern darüber hinaus die Produktivität der jeweiligen Anlage gewährleisten oder sogar verbessern.

QorIQ-PLATTFORM: ENTWICKELT FÜR LEISTUNG UND ZUVERLÄSSIGKEIT



Vorteile der QorIQ Prozessoren

QorIQ Prozessoren

- Dual-thread 64-bit Kerne, SIMD Vektoreinheit
- Integrierter Ethernet Switch
- DSP und MPU Fusion mit QorIQ Qonverge Produkten
- Hardware Unterstützung für Hypervisor, asymmetrisches und symmetrisches Multiprocessing
- CoreNet gemultiplexte, nicht-blockierende Verbindungsmatrix
- Skalierbare Multi-Core-Kommunikationsprozessoren einschließlich doppelt genauer Fließkommaeinheit
- QUICC Engine Multi-Protokoll Paketverarbeitung und Sicherheitsbechleunigungseinheit

Bild 1

John Ralston

In Europa und Nordamerika findet sich wohl kein Haushalt, in dem nicht das allseits bekannte UL- oder CE-Logo zu sehen ist. Weniger bekannt ist allerdings, wofür diese Zeichen stehen und wie anspruchsvoll die Prozesse sind, die Hersteller implementieren müssen, um diese Logos verwenden zu dürfen.

Den harten Vorgaben liegen in erster Linie Sicherheitsaspekte zugrunde, die alle Geräte und Anlagen betreffen – von Heimwerkerwerkzeug über Aufzüge, Bahnsysteme und Robotik in der Automobilfertigung bis hin zu Atomkraftwerken, Öl- und Gaspipelines. Gerade bei letzteren kommt der Sicherheit ein übergeordneter Stellenwert zu, aber auch Geräte für den Alltagsgebrauch müssen ähnlich sorgfältig und mit Bedacht realisiert werden.

Ziel dessen, was die Industrie "Funktionale Sicherheit" nennt, ist es, für die Nutzer von Geräten oder Maschinen alle Risiken für Verletzungen oder gesundheitliche Beeinträchtigungen auszuschließen. Die Geräte

KONTAKT

Freescale Halbleiter Deutschland GmbH
Technical Information Centre
Schatzbogen 7
81829 München
Tel.: +49 89 92103-559
E-Mail: support@freescale.com
www.freescale.com

SICHERHEIT UND PRODUKTIVITÄT

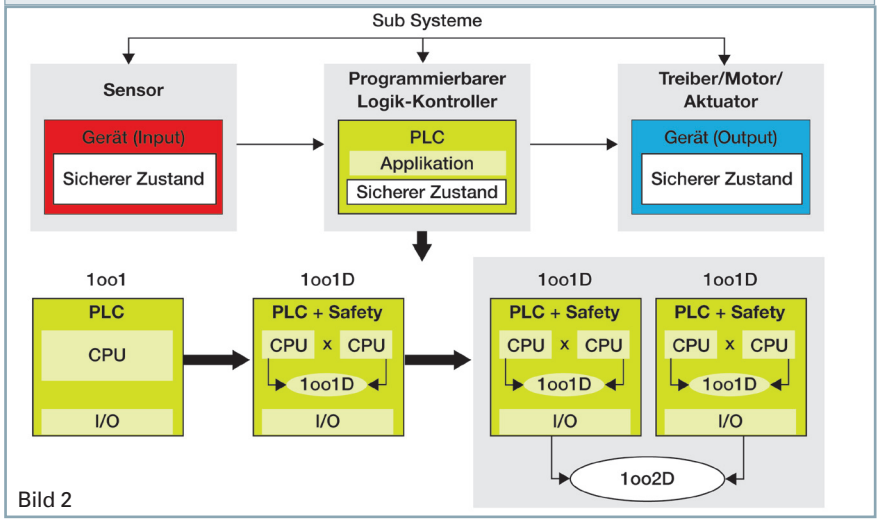


Bild 2

müssen nicht nur korrekt auf Eingaben reagieren, sondern ebenso alle Bedienfehler, Hardwareausfälle oder Änderungen ihrer Betriebsbedingungen sicher bewältigen können.

Maschinen sicher machen

Die Standards für Funktionale Sicherheit werden in den jeweiligen Ländern durch die Behörden festgelegt. Für EU-Länder dient die IEC 61508 als Basis. In Nordamerika wird die ISO-Spezifikation 13849 umgesetzt. Das Erreichen der Zertifizierung setzt eine Reihe von Schritten voraus, in denen die erforderlichen Sicherheitsfunktionen, mögliche Gefahrenpotenziale und Maßnahmen zur Risikoreduktion identifiziert werden. Dies führt zur Festlegung des erforderlichen Safety Integrity Levels (SIL). Andere Schlüsselfaktoren, die es in diesem Prozess zu berücksichtigen gilt, sind unter anderem die Hardware-Fehlertoleranz (HFT, die Anzahl der tolerierbaren Fehler) und die Safe Failure Fraction (SFF, die Wahrscheinlichkeit, dass das System im sicheren Zustand ausfällt). Die Verantwortung für diese Aspekte liegt in den Händen entsprechend geschulter Ingenieure, die im Einklang mit den Standards einem ganzheitlichen Systemansatz folgen müssen.

Das programmierbare Steuerungs-Subsystem

HFT und SFF sind insofern von Bedeutung, als sie als Maß für Redundanz und Diagnosefunktionen des Subsystems dienen. Der HFT-Wert hängt von der verfügbaren Redundanz und der Arbitrierungsstrategie des Systems ab. Der SFF-Wert ist ein Maß für die Ausfallsicherheit des Designs und die Qualität der integrierten Diagnosefunktionen.

Bild 2 zeigt ein zweifach redundantes System mit eins aus zwei Voting-Architekturen und Diagnose (1oo2D). 1oo2D heißt, dass zwei Kanäle die gleichen Eingangswerte verarbeiten und eine bestimmte Aktion anfordern. Der Voter vergleicht die Anforderungen beider Kanäle, verwendet aber nur die Daten aus dem Kanal mit guten Diagnoseergebnissen.

Die Diagnosefunktionen signalisieren Software- oder Zufallsfehler, inkorrekte Benutzereingaben oder auf eine gemeinsame Ursache zurückzuführende Fehler (Common Cause Failure) aufgrund von Umwelteinflüssen – beispielsweise Fehler im Speicher oder auf dem Datenbus durch elektromagnetische Störungen, Vibrationen, Temperatur- oder Druckänderungen. Will man Systeme sicher machen, braucht man zusätzliche Rechenleistung, um die entsprechenden Echtzeitberechnungen und Diagnosefunktionen zu realisieren. Doppelt vorhandene Hardwareressourcen liefern die Redundanz, die nötig ist, um das System im Falle eines Fehlers in einem sicheren Zustand zu halten.

Redundanz und Echtzeit-Diagnose

Genau darin liegt die Herausforderung für die Hersteller von Geräten und Maschinen: Zusätzliche Redundanz wirkt sich direkt auf die Hardwarekosten aus, weil in der Regel zusätzliche Controllermodule oder Prozessorkomponenten erforderlich sind. Zwei wichtige Fragen stellen sich: Lässt sich Funktionale Sicherheit auch ohne Replikation von Hardware realisieren? Und können intelligentere und höher integrierte Diagnosefunktionen dazu beitragen, gleichzeitig Funktionale Sicherheit und Produktivität zu steigern? Um die zweite Frage zu illustrieren, dient ein Roboter in der Situation in einer Fertigungslinie. Der Roboter wird mit Hilfe von Lichtschranken geschützt.

Der Unterschied zwischen Bild 3a) und Bild 3b) ist klar erkennbar: Das erste Bild zeigt einen Zwischenfall, bei dem das Bedienpersonal der Gefahr einer Verletzung ausgesetzt ist und deshalb der Roboter gestoppt oder vom Netz getrennt werden muss. Dies ist im zweiten Bild nicht der Fall. Hier wäre es vermutlich ausreichend, den Roboter langsamer arbeiten zu lassen. Ein System, das entsprechende Unterscheidungen treffen kann, steigert die Produktivität, da es einerseits allen Sicherheitsaspekten Rechnung trägt, aber andererseits die Fertigungslinie am Laufen hält. In dieser Situation könnte eine weitere Lichtschranke eingesetzt werden, um einen Pufferbereich und einen Arbeitsbereich zu schaffen. Die richtige Antwort könnte die Integration einer Bildverarbeitung ins System sein. In beiden Fällen muss die Steuerung jetzt weitere Sensoreingänge berücksichtigen, und zusätzliche Berechnungen müssen in Echtzeit ausgeführt werden.

QorIQ-Multicore-Prozessoren

Antwort auf beide Problemstellungen geben die QorIQ-Multicore-Prozessoren.

ABSCHALTEN ODER HERUNTERFAHREN

Bild 3a:
In den gesicherten Bereich gefallen

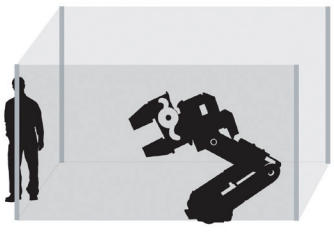


Bild 3b:
Zufällig den Lichtkreis unterbrochen ohne den gesicherten Bereich zu betreten

ZUORDNUNG DER FUNKTIONEN ZUM QorIQ MULTI-CORE-PROZESSOR

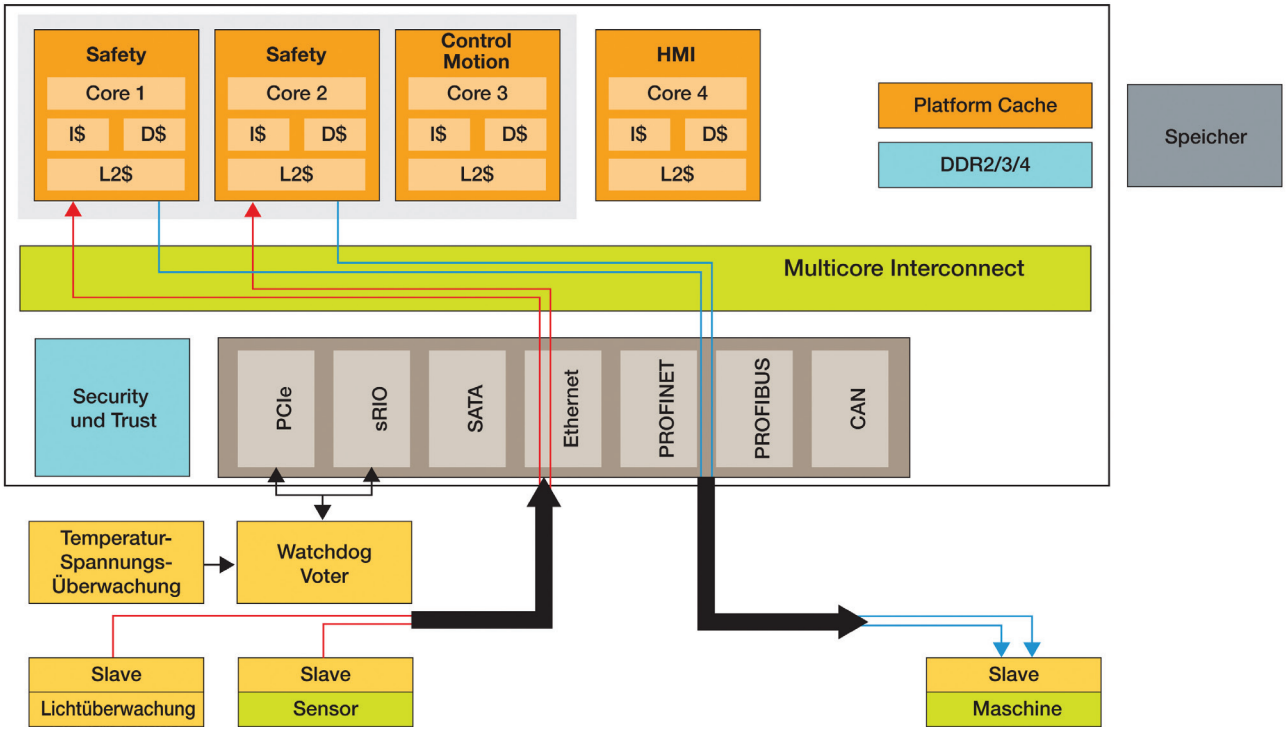


Bild 4

Es handelt sich um eine Familie von Prozessorplattformen mit einem, zwei, vier oder noch mehr Rechenkernen, die alle auf 32- beziehungsweise auf 64-Bit Power-Architektur-Strukturen mit integrierten Double-Precision-Floating-Point-Funktionen basieren. Die QorIQ-Multicore-Prozessorplattform wurde für Märkte wie Telekommunikation, Enterprise-Anwendungen und Datenzentren sowie industrielle Projekte konzipiert – dort, wo Zuverlässigkeit und höchste Verfügbarkeit vorausgesetzt werden. Die konstruktiven Besonderheiten von Rechenkern, Interconnect-Struktur, I/O- und Speicher-Subarchitektur sind natürlich nicht nur auf den hier beschriebenen Anwendungsfall beschränkt, sondern auch für andere Marktsegmente relevant.

Bild 4 zeigt, wie die programmierbare Steuerung und die Sicherheitsfunktionen auf einem QorIQ Multicore-Prozessor koexistieren können. Die verschiedenen Funktionen können auf dieser Architektur laufen, indem sie gemeinsame oder dezidierte Interconnect-, Speicher- und I/O-Ressourcen nutzen. Aufgrund der rigorosen Strukturierung der Hardware können die verschiedenen Funktionen ohne Störung von anderen Funktionen auf anderen Rechenkernen oder externen Hosts laufen. Abbildung 4 unterstreicht die spezifischen Hardwaremerkmale, die dies ermöglichen.

Dieses Konzept erlaubt die Konsolidierung von Komponenten oder Modulen. Durch den hohen Integrationsgrad werden zudem bessere Diagnosefunktionen möglich, die ihrerseits zu einer höheren Verfügbarkeit oder Produktivität der Maschine beitragen. *(sc)* ■

Autor

John Ralston ist Industrial System Architect bei Freescale.

Freescale auf der SPS IPC Drives 2014: Halle 6, Stand 137