Bild: Infineon Technologies AG

Bedeutung von funktionaler und Datensicherheit

Nicht nur schmückendes Beiwerk

Anfang des 20. Jahrhunderts revolutionierte Henry Ford die Automobilfertigung. Angeregt wurde er durch den Einsatz von Förderbändern in Getreidespeichern. In Verbindung mit anderen Produktivitätssteigerungen, die aus der Fließbandfertigung resultierten, konnte Ford so den Zeitaufwand für die Herstellung eines Fahrzeugs von mehr als zwölf Stunden bis auf fast 90 Minuten verkürzen. Heute entstehen die meisten Produkte durch Zusammenarbeit von Menschen und Maschinen, wobei die Menschen durch Türen, Lichtschranken und Verriegelungsmechanismen vor möglichen Schäden geschützt werden. Um allerdings von weiteren möglichen Produktivitätssteigerungen profitieren zu können, müssen wir den Sprung von der einfachen Zusammenarbeit zu echtem gemeinschaftlichen Arbeiten schaffen. Durch Initiativen rund um Industrie 4.0 werden Roboter intelligenter und – durch ihre Sensoren – besser dafür ausgerüstet, mit ihrer Umgebung zu interagieren. Aber eine große Frage bleibt offen: Kann diese Revolution auch sicher stattfinden?

Das Fließbandkonzept erlaubt es uns, von der Geschwindigkeit und Leistungsfähigkeit von Maschinen zu profitieren. Gleichzeitig schränkt es aber auch ein, wie Produkte hergestellt werden können. Solange die hergestellten Produkte alle gleich sind – kein Problem. Aber die Kunden von heute erwarten Auswahlmöglichkeiten, individuelle Anpassung und Einzigartigkeit. Das passt nicht zu einem linearen Fertigungsablauf. Statt sich auf diesen linearen, Schritt für Schritt ausgeführten Prozess zu beschränken, gibt es inzwischen andere Möglichkeiten. Innovationen, die das Konzept Industrie 4.0 bietet, erlauben andere Wege zur Verwirklichung von Fertigungsprozessen. Eine Methode ist dabei der Übergang zu einer Reihe von Fertigungsinseln, wobei jede Insel ein Element des Fertigungsprozesses ausführt. Das herzustellende Produkt wird dann von einer Station zur anderen befördert, wobei jede Station die zugewiesene Aufgabe erledigt. Das bietet auch die Möglichkeit, das gleiche Produkt in verschiedenen Variationen zu liefern. Das Basismodell eines Produkts muss nur die wichtigsten Fertigungsstationen absolvieren, während ein höherwertiges Modell weitere Stationen durchläuft, wo zusätzliche Fertigungsschritte erfolgen.

Sicherheitskonzept für Mensch/Maschine-Interaktion

Diese Fertigungsschritte können in einigen Fällen menschliches Eingreifen erfordern. Um die Interaktion zwischen Mensch und Maschine zu ermöglichen, ist allerdings ein Sicherheitskonzept erforderlich. Dieses muss bereits zu Beginn der Entwicklung des Produktionssystems festgelegt werden. Das ist auch bei der Entwicklung von Systemen in vielen Branchen üblich, beispielsweise im Automobilbau. In der Automobilbranche sind die Insassen auf Elektronik angewiesen, die viele wichtige Systeme steuert. Fehlfunktionen oder Komplettausfälle können sich sowohl auf Passanten als auch auf Fahrzeuginsassen auswirken. Das gilt beispielsweise für ABS-Bremsanlagen, elektronische Feststellbremsen und Servolenkungen. Wenn solche Produkte definiert und die zugehörigen Steuersysteme ausgewählt werden, muss die Implementierung der funktionalen Sicherheit in jeder Phase berücksichtigt werden. Die Architektur von Bauelementen wie den 32Bit-Mikrocontrollern der Aurix-Familie ist speziell auf Anwendungsfälle ausgelegt, die hohe Anforderungen an die Sicherheitsintegrität stellen. Sie erfüllen die strengsten ISO26262-Anforderungen der Automobilbranche und können daher zusammen mit Safety Manuals und dedizierten Sicherheits-Softwareroutinen in Systemen verwendet werden, um die Vorgaben der IEC61508 zu erfüllen. IEC61513 ist eine Adaptierung von IEC61508 für Maschinen, während sich IEC61511 an die Prozessindustrie richtet. Um sicherzustellen, dass ein Ausfall des Verarbeitungselements innerhalb eines Systems erkannt werden kann, verwenden viele funktionssichere Systeme zwei verschiedene Mikrocontroller. Einer dieser Mikrocontroller führt das Anwendungsprogramm aus, während der zweite den ersten überwacht. Dieses

SPS MAGAZIN

Auszug aus dem SPS-MAGAZIN, Fachzeitschrift für Automatisierungstechnik, Ausgabe 9/2018.

Konzept gewährleistet die Diversität innerhalb des Steuersystems, da ein Softwarefehler oder Ausfall des einen Bauelements in dem anderen Bauelement nicht ebenfalls auftreten wird. Die Aurix-Architektur erreicht die entsprechende Sicherheitsfunktionalität innerhalb des Bauelements durch ihre diversitäre Lockstep-CPU. Die Lockstep-CPU arbeitet mit derselben 32Bit-TriCore-Architektur wie die Haupt-CPU. Ansonsten haben sie aber nichts gemeinsam. Die Lockstep-CPU ist physikalisch von ihrem Pendant getrennt, und ihre Schaltung ist völlig anders aufgebaut. Außerdem werden die Befehle im Lockstep-Kern um zwei Takte verzögert ausgeführt. Das bietet Schutz, da Ereignisse, die die Befehlsausführung im Hauptkern stören könnten, im Lockstep-Kern nicht ebenfalls auftreten können. Am Ende der Verzögerung werden die Ergebnisse der Befehlsausführung aus dem Haupt- und dem Lockstep-Kern miteinander verglichen. Falls sie nicht übereinstimmen, kann der Prozessor den Fehler behandeln.

Integrierter Selbsttest

Ein integrierter Selbsttest (BIST) für die interne Bauelemente-Logik, der beim Einschalten durchgeführt wird, stellt sicher, dass der Aurix-Baustein einwandfrei funktioniert bevor Applikations-Code ausgeführt wird. Weitere Tests, wie etwa einen Speicher-BIST, können zur Anwendungssoftware hinzugefügt werden. Infineon bietet auch Software-Bibliotheken wie Pro-SIL SafeTlib und SBST an, um Entwickler eingebetteter Systeme bei ihren Designs zu unterstützen. Um sicherzustellen, dass die verschiedenen Prozessorkerne nicht die Kontrolle über die Peripherie des jeweils anderen übernehmen oder Speicher überschreiben, der anderen Kernen zugewiesen ist, ist ein Speicherschutzsystem vorhanden. Darüber hinaus verfügt jede Peripherie und gemeinsam genutzter SRAM über einen eigenen lokalen Zugriffsschutzmechanismus. In Verbindung mit einem Hypervisor ist es außerdem möglich, Software die mehr oder weniger kritisch ist, auszuführen, ohne die Echtzeit-Leistungsfähigkeit zu beeinträchtigen. Mit Kommunikations-Schnittstellen für GBit-Ethernet, Ethercat oder CAN ist die Aurix-Familie der zweiten Generation eine geeignete Plattform für Industrieroboteranwendungen, unter anderem für fahrerlose Transportfahrzeuge (AGVs).

Sicherheit heute und in der Zukunft

Bisher sind Industrieroboterarme unabhängig von den Werkzeugen entwickelt worden, mit denen sie bestückt werden. Üblicherweise wird das Stromversorgungs- und Steuersystem eines Schweißwerkzeugs über ein schweres Kabelbündel an der Seite des Roboterarms befestigt. Zum Teil erfolgt diese Trennung aus Sicherheitsgründen, da sie dem Anbieter des Roboterarms ermöglicht, die vollständige Kontrolle über sein sicherheitszertifiziertes Gerät zu behalten. Und zwar unabhängig davon, von welchem Hersteller die verwendeten Werkzeuge stammen. Wenn er seine Kommunikationsbusse und Stromversorgungssysteme mit Werkzeugen von Fremdanbietern teilen würde, wäre es schwierig, die Sicherheit des Systems zu ermöglichen. Mit Industrie 4.0 entsteht jedoch die Notwendigkeit, alle Systeme und Sensoren miteinander zu vernetzen, damit die Maschinen in der Lage sind, miteinander und mit ihren menschlichen Bedienern zu kommunizieren und zusammenzuarbeiten. Das kann zu einem möglichen Sicherheitsrisiko führen: eine

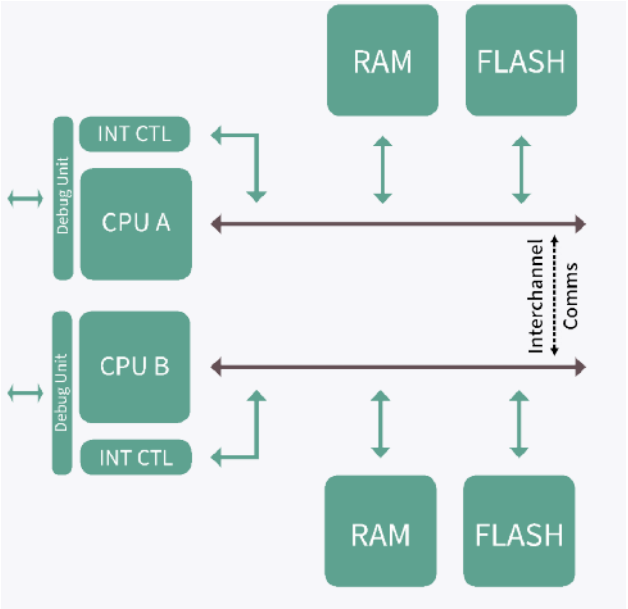


Bild: Infineon Technologies AG

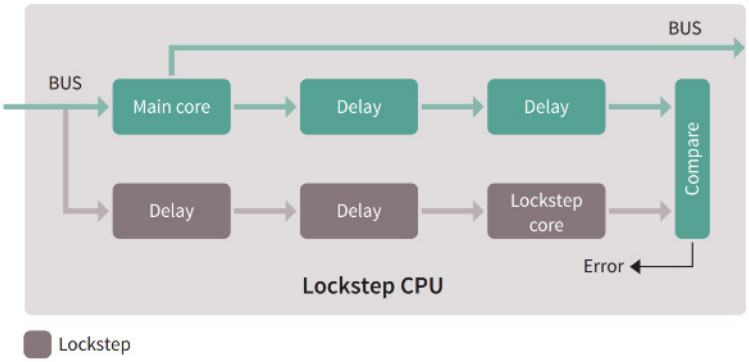
Um eine ausreichende Diversität für sicherheitskritische Anwendungen zu erreichen, werden oft zwei verschiedene Mikrocontroller in einer lose synchronisierten Zweiprozessorarchitektur verwendet.

Schwachstelle, die als Angriffspunkt missbraucht werden könnte. Noch kritischer ist, dass zukünftig Erweiterungen und Werkzeuge hinzugefügt werden könnten, deren Sicherheitsimplementierung nicht angemessen geprüft worden ist. Solche Elemente könnten zu einer Hintertür für Netzangriffe werden, oder sie könnten sogar missbraucht werden, um Industrieanlagen und die Roboter selbst zu rekonfigurieren. Angesichts der Tatsache, dass Mensch und Maschine einander so nahe sind, besteht eine erhebliche Gefahr für Leib und Leben, wenn Roboter umprogrammiert werden oder sich auf manipulierte Sensordaten verlassen. Zuverlässige Werkzeuge und Sensoren sowie Zubehör- und Ersatzteile werden unverzichtbar sein, damit in der Fabrik der Zukunft nicht nur die funktionale Sicherheit, sondern auch die Netzsicherheit (Security) erhalten bleiben. Allerdings ist es in der schnelllebigen Fertigungswelt ebenso wichtig, dass die Implementierung zuverlässiger Systeme die Instandhaltung oder den Ersatzteilaustausch nicht behindert. Denn das würde unweigerlich zu längeren Stillstandzeiten führen.

Security von Beginn an integrieren

Maßnahmen für die funktionale Sicherheit lassen sich, ebenso wie Security-Maßnahmen, nicht einfach so nachträglich hinzufügen. Daher muss die Security von Anfang in den Entwicklungsprozess integriert werden, damit sie den erforderlichen Schutz bietet und gleichzeitig intuitiv genutzt werden kann. Außerdem können Safety und Security nicht mehr unabhängig voneinander betrachtet werden. Bei kollaborativen Automatisierungssystemen kann die funktionale Sicherheit nur dann verwirklicht werden, wenn geeignete Security-Maßnahmen ergriffen worden sind: Bei redundanten Konfigurationen, wie sie bereits im Zusammenhang mit sicheren Mikrocontrollern erwähnt wurden, besteht die Gefahr eines unsicheren Verhaltens, wenn beispielsweise eine kritische Kalibrierung unbefugt manipuliert werden kann. Bei Aurix-Mikrocontrollern kümmert sich ein eingebettetes Sicherheitsmodul um dieses Problem. Meist gibt es keine Universallösung, die sich für alle Anwendungs-

Bild: Infineon Technologies AG



Die 32Bit-Mikrocontroller der Aurix-Familie erreichen die notwendige Diversität für sicherheitskritische Systeme mit ihrer Lockstep-CPU.

fälle eignet. Bei Verbrauchsmaterial ist möglicherweise eine einfache, kostengünstige Lösung ausreichend, um festzustellen, ob das verwendete Material tatsächlich vom Lieferanten zugelassen ist. Andererseits erfordert ein voll vernetztes Steuerungssubsystem die Selbstauthentifizierung mit einem Sicherheitsanker (Trust Anchor), bevor ihm die Teilnahme an einem kritischen Produktionssystem erlaubt wird. Roboter mit Steuersystemen müssen sich nicht nur gegenseitig authentifizieren – es ist auch unverzichtbar, dass diese Systeme gegen Datendiebstahl und Manipulation geschützt werden. Die Sicherung der Integrität von Robotern kann am besten durch IP-Schutz von Kalibrierdateien, Authentifizierung von Komponenten und geschützte Protokollierung realisiert werden, um das Erkennen von Angriffen zu unterstützen. Um bei intelligenten Robotern und in Industrienetzen die Sicherheit von Daten, Schnittstellen und Kommunikationskanälen zu schützen, bietet Infineon eingebettete Optiga-Sicherheitslösungen an, die einfach integriert werden können. Da Mensch und Maschine in näheren, engeren Kontakt kommen, hängt der Erfolg ihrer Zusammenarbeit zu einem großen Teil von Vertrauen ab. Dieses Vertrauen lässt sich aber nur aufbauen, wenn wir uns in Gesellschaft von Maschinen sicher fühlen. Die funktionale Sicherheit muss bereits zu Beginn der anfänglichen Konzeption integriert werden und bis zum fertigen Entwurf des Roboters, Cobots oder AGVs ständig überprüft werden. Aber auf sichere Software kann man sich nur dann verlassen, wenn sie unverändert ist und mit einem zuverlässigen Netz von Systemen, Modulen und Sensoren kommuniziert. Daher ist Security von Anfang an elementar. Sie erlaubt die Authentifizierung hochkomplexer Robotersysteme und ihrer menschlichen Bediener, um das äußerst wichtige Vertrauen aufzubauen und während des Betriebs aufrechtzuerhalten, indem sie die einwandfreie Integrität industrieller Geräte bestätigt. ■

Autor: ***Dr. Clemens Müller,***
Director Business Development Industrial Robotics,
Infineon Technologies AG
www.infineon.com