safety

Institut für Automation & Industrial IT
Fachhochschule Köln
Cologne University of Applied Sciences
Prof. Dr. **Frithjof Klasen**

Safety schon im Kern berücksichtigen

Die funktionale Sicherheit von Maschinen und Anlagen ist heute einer der entscheidenden Faktoren für die Wirtschaftlichkeit und Wettbewerbsfähigkeit einer Produktion. An die Implementierung von Safety stellen die Gesetzgeber daher besonders hohe, international verbindliche Anforderungen. Die SIL 3 Zertifizierung nach IEC 61508 verlangt beispielsweise die umfassende Analyse des Gefahrenpotenzials von Maschinen und die Trennung von sicherheitsrelevanten und unkritischen Bereichen. Im Rahmen moderner Anlagenkonzepte, die auf kosteneffiziente Konsolidierung setzen, stellt die Einhaltung dieser Normen eine große Herausforderung dar. Einen neuen, adäquaten Lösungsansatz bieten die industrietauglichen Multicore-Prozessoren von Intel. Sie verfügen über Virtualisierungserweiterungen, mit deren Hilfe Separierungskonzepte effizient auf einer Hardware umgesetzt werden können.

Inhalte

I. Ausgangssituation 1
a) Internationale Standards für Safety 2
b) Konsolidierung – Zwei Welten wachsen zusammen..... 2

II. Neue Lösungen für Safety..... 2
a) Anforderungen an die Lösungen.... 2
b) Skalierbare Lösungen und Virtualisierung mit Intel Multicore Prozessoren 3
c) Erhöhte funktionale Sicherheit durch Intel® VT-x / VT-d..... 3

III. Ausblick:
Safety setzt Security voraus..... 4

I. Ausgangssituation

Seit der Einführung des einheitlichen europäischen Binnenmarktes wurden die nationalen Normen, die die technische Realisierung von Maschinen betreffen, konsequent harmonisiert. Dabei haben die Gesetzgeber grundlegende Sicherheitsanforderungen festgelegt, die beim Bau einer Maschine das Restrisiko für den Menschen und die Anlage in einem tolerierbaren Maß halten sollen.

Hinweise für die funktionale Sicherheit von computerbasierten Systemen und Software gibt die international verbindliche Norm IEC 61508. Als „Basic Safety Publication" findet sie seit dem 29. Dezember 2009 auch in der neuen Maschinenrichtlinie 2006/42/EG ihren Niederschlag, die für jeden Anlagenhersteller und -betreiber gesetzlich verpflichtend ist. Die Norm betrachtet erstmalig die gesamte Sicherheitskette, vom Sensor bis zum Aktor. Für die Erreichung eines vorgeschriebenen Sicherheitslevels ist es somit nicht mehr ausreichend, dass einzelne Komponenten entsprechend zertifiziert worden sind. Die gesamte Sicherheitsfunktion muss die definierten Anforderungen erfüllen.

a) Internationale Standards für Safety

Der Bereich Safety umfasst die Gewährleistung der funktionalen Sicherheit einer Anlage und deren Nutzer durch das Automatisierungssystem. Sicherheit lässt sich hier als „Nichtvorhandensein von Gefahren" beziehungsweise „wirksamer Schutz von Mensch und Maschine vor Risiken" beschreiben. Die potenziellen Gefährdungen werden von dem Anlagenbetreiber anhand einer Risikoanalyse bewertet. Abhängig vom Ergebnis der Analyse sind Maßnahmen zur Risikoreduzierung durch Fehlervermeidung, Fehlererkennung und Fehlerbeherrschung zu treffen.

Soll die Risikoreduzierung mit Mitteln der Prozessleittechnik erfolgen, sind für die verwendeten Komponenten die Anforderungen des internationalen Standards IEC 61508 maßgeblich. Die Norm beinhaltet allgemeine Vorgaben für die Vermeidung und Beherrschung von Ausfällen in elektrischen, elektronischen oder programmierbaren elektronischen Geräten. Damit einher geht die Vorgabe von organisatorischen und technischen Anforderungen sowohl für die Geräteentwicklung als auch für den Gerätebetrieb. Für Anlagen und risikoreduzierende Maßnahmen werden dabei vier Sicherheitsstufen unterschieden – von SIL1 für ein geringes Risiko bis SIL4 für ein sehr hohes Risiko. Je höher die Sicherheitsstufe ist, desto zuverlässiger müssen die Maßnahmen zur Risikoreduzierung sein.

b) Konsolidierung – Zwei Welten wachsen zusammen

Die industrielle Automatisierungstechnik führt schon lange kein technologisches Eigenleben mehr. Allgemein anerkannte Methoden und Standards der IT setzen sich in der Steuerungstechnik immer mehr durch. Dazu gehören vor allem der Einsatz von Embedded-PCs in der automatisierten Produktion, Schnittstellentechnologien und Protokolle wie OPC, XML oder TCP/IP. Letztere gewährleisten, dass alle fertigungsbezogenen Daten zum Auftrags- und Materialfluss, zu den Kosten und zur Produktqualität aus den verschiedenen IT-Systemen und Produktionsbereichen sowie aus dem Shop-Floor-System zusammengeführt und in Echtzeit verfügbar gemacht werden.

Controller, HMI-Panels, Drives und die dazugehörige Engineering-Software bilden in diesem System ein abgestimmtes Angebot für Maschinen nahe Geräte. Charakteristisch ist dabei die Integration von deterministischen Systemen und Anwendersystemen, wobei die Echtzeitfähigkeit des Controllers ohne Einflussnahme der grafikbasierten Ausgabe gewahrt bleiben muss.

Der rasche Anstieg an Durchlässigkeit und Komplexität sowie die damit verbundenen Entwicklungskosten für Industrielösungen verlangen eine umfassende Konsolidierung. Einen adäquaten Lösungsansatz hierfür bietet Intel mit seinen industrietauglichen Multicore-Prozessoren, die in Kombination mit Intel® VT-x / VT-d die Umsetzung von Virtualisierungs- und Separierungskonzepten in der Industrieautomatisierung ermöglichen.

II. Neue Lösungen für Safety

a) Anforderungen an die Lösungen

Die zunehmende Bedeutung der Konsolidierung in modernen Maschinen- und Anlagekonzepten legt nahe, sicherheitskritische Programme auf derselben Hardware zu betreiben wie sicherheitsunkritische. Nach der richtungsweisenden Norm IEC 61508 sind hierbei hohe Anforderungen zu erfüllen.

Für alle Sicherheitsfunktionen muss gewährleistet sein, dass die Software zuverlässig ausgeführt wird und dass alle Teile der Software auch wirklich abgearbeitet werden. Darüber hinaus wird ein quantitativer Nachweis für das verbleibende Restrisiko auf Basis der Berechnung der Wahrscheinlichkeit nicht erkannter Fehler verlangt.

Bei der Verwendung eines monolithischen Hardwarekonzepts sollte sichergestellt werden, dass auch die Applikationen des sicherheitsunkritischen General Purpose Operating System (GPOS) gegen Ausfälle geschützt werden. Eine weitere wichtige Anforderung sind flexible Upgrades der GPOS-Applikationen, ohne dass dabei gleich das gesamte Gerät inklusive aller sicherheitskritischen Anwendungen neu zertifiziert werden muss. Außerdem muss gewährleistet sein, dass das GPOS keinen Einfluss auf die Deterministik des sicherheitskritischen Echtzeitsystems nimmt.

Zusätzlich zu den technischen Anforderungen schreibt die Norm IEC 61508 organisatorische und strukturelle Anforderungen an den Entwicklungsprozess vor, um systematische Fehler und das verbleibende Restrisiko zu minimieren.

b) Skalierbare Lösungen und Virtualisierung mit Intel Multicore Prozessoren

Das bislang noch vorherrschende Separierungskonzept sieht vor, die Systemkomponenten, die sich auf unterschiedlichen Safety-Levels befinden, auf räumlich und zeitlich getrennte Subsysteme zu verteilen. Bei größeren Maschinen mit komplexen sicherheitsgerichteten Einrichtungen ist der Hardware-Aufwand dadurch enorm, so dass dieses Vorgehen schnell unwirtschaftlich wird.

Integrierte Safety-Lösungen auf Basis von VT-fähigen Intel Multicore-Prozessoren verringern den Hardware-Aufwand und erhöhen die Maschinensicherheit. Über die Hardware-Virtualisierung können Prozessorkerne, Speicher und I/O Geräte in unabhängige virtuelle Maschinen aufgegliedert werden. Als Kontrollinstanz und unterliegende Softwareschicht fungiert dabei der Hypervisor, der die Hardware-Ressourcen verwaltet und auf die darüber liegenden virtuellen Maschinen verteilt.

Bei der Aufteilung der Ressourcen auf die Steuerung und das HMI wird erstere eigenständig auf einem Prozessorkern ausgeführt, um die Echtzeitfähigkeit zu bewahren und jegliche Einflussnahme einer grafikbasierten Ausgabe auszuschließen. Der zweite Kern stellt für das HMI eine allgemeine Betriebssystemplattform bereit, bei der nicht die Deterministik, sondern die grafischen Möglichkeiten im Vordergrund stehen. Auf diese Weise reduziert sich die Gesamtkomplexität einer Anlage deutlich, was ein enormes Einsparungspotenzial bietet.

Darüber hinaus wird die Deterministik über den Einsatz der Multicore-Systeme optimiert – unterstützt von der Virtualisierung, die über VT-d den direkten Zugriff der virtuellen Maschine auf die Hardware-Schnittstelle erlaubt. Durch eine verbesserte Skalierbarkeit und mehr Leistung pro Watt vermindern die Multicores auch das Risiko, dass bei steigender Prozessorleistung die Stromaufnahme und die Verlustwärme schnell einen kritischen Punkt erreichen.

Der Multicore-Ansatz verspricht außerdem eine beinahe lineare Steigerung der Performance mit der Zunahme der CPU-Kerne und der fortschreitenden Optimierung der X86-Architektur. Letztere bietet eine einheitliche Software-Plattform für unterschiedlichste Geräteklassen – vom Motion Control bis zum HMI.

c) Erhöhte funktionale Sicherheit durch Intel® VT-x / VT-d

Die SIL3 Zertifizierung nach IEC 61508 verlangt eine umfassende Analyse des Gefahrenpotenzials von Maschinen und schreibt eine Trennung der sicherheitsrelevanten und nicht sicherheitskritischen Bereiche vor. Entsprechend dieser Risikobeurteilung sind technische Maßnahmen zu ergreifen, um den sicheren Betrieb einer Maschine während aller denkbaren Betriebszustände zu gewährleisten.

Die Multicore-Prozessoren von Intel verfügen über Virtualisierungserweiterungen (Intel® VT-x, VT-d), welche Teile des Hypervisor in die Hardware implementieren. Prozesse und Anwendungen mit unterschiedlichen Anforderungslevels für Safety können so künftig parallel auf einer Hardware ausgeführt werden, ohne dass diese sich gegenseitig beeinträchtigen. Im Gegensatz zu den vergleichsweise schwachen Mechanismen zur Prozessisolation eines Standardbetriebssystems lassen sich so auch hochkritische Bereiche im Produktionsablauf von weniger schützenswerten oder nicht sicherheitsrelevanten Bereichen isolieren. Die Domaintrennung findet dabei über die Bindung an den jeweiligen Prozessorkern statt, die sichere Kommunikation gewährleistet der Hypervisor.

Gegenüber bisherigen Ansätzen stellt das einen wesentlichen Vorteil dar, denn bisher wurde das Sicherheitslevel für alle Anwendungen eines Steuergerätes vom Safety-Status des am höchsten klassifizierten Prozesses bestimmt. Hinzu kommt, dass durch den Einsatz von Virtualisierungslösungen die jeweiligen internen Zugriffssteuerungen individuell angepasst und für Anforderungen jeder virtuellen Maschine ausgeführt werden können. Die Konsolidierung über Intels VT-fähige Multicore-Architekturen führt schließlich zu deutlichen Kostenvorteilen, denn die Separierung von kritischen und unkritischen Applikationen gelingt künftig auch auf einem einzigen System und damit ohne zusätzliche Hardware.

III. Ausblick

Safety setzt Security voraus

Wie beschrieben verlangt der aktuelle Paradigmenwechsel bei den Normen der funktionalen Sicherheit den Einsatz neuer Technologien, um in Zukunft die hohen Safety-Standards auf effiziente Weise einhalten zu können. Anders als in der Vergangenheit, befinden sich die funktional sicheren Anwendungen dabei immer seltener in geschlossenen Systemen. Mit dem Einzug des Industrial Ethernet und der zunehmenden Vernetzung von Maschinen mittels drahtloser Technologien wie Wireless LAN (WLAN) werden Safety-relevante Daten verstärkt auch über offene Kommunikationswege übertragen. Bezogen auf die Sicherheit des Kommunikationskanals muss also zur Einhaltung der Safety-Anforderungen immer auch die Informationssicherheit über spezielle Security-Mechanismen gewährleistet sein.

Unter dieser Prämisse gilt es, Safety- und Security-Aspekte in Zukunft in eine Gesamtlösung zu integrieren. Dafür müssen Schutzziele klar definiert und alle relevanten Bedrohungsszenarien aufgezeigt und berücksichtigt werden. Oberste Priorität hat dabei der sichere Betrieb des Netzes als Voraussetzung für eine hohe Verfügbarkeit der Produktionsanlagen, inklusive Unterbindung der Einflussnahme des unsicheren Systems auf das sicherheitskritische System.

Auf der Hardware-Seite bieten die VT-fähigen Multicore-Prozessoren von Intel Anlagebetreibern, OEMs und Entwicklern einen standardisierbaren Lösungsweg, der auch den zukünftigen Safety- und Performance-Anforderungen in der Industrieautomation gerecht wird. Kombiniert mit der passenden Hypervisor-Lösung stellen sie einen offenen und modularen Ansatz für kosteneffiziente Safety dar.

Institut für Automation & Industrial IT
Fachhochschule Köln
Cologne University of Applied Sciences

Über das Institut für Automation & Industrial IT der Fachhochschule Köln
Das Institut für Automation & Industrial IT gehört zu den führenden Forschungseinrichtungen im Bereich Industrial IT. Es unterstützt Hersteller und industrielle Anwender bei der Entwicklung und beim Einsatz von Embedded Lösungen und Netzwerklösungen in der Automation. Leitender Direktor ist Prof. Dr. Frithjof Klasen, der in Fachgruppen des ZVEI, der GMA und der PROFIBUS Nutzerorganisation an der Bewertung und Einführung von Informationstechnologien in der Automation mitarbeitet. Weitere Informationen unter **www.fh-koeln.de/ait.**

Über Intel
Intel (NASDAQ: INTC) ist das weltweit führende Unternehmen im Bereich der Halbleiterinnovation, das Technologien, Produkte und Initiativen entwickelt, die das Leben und die Arbeit der Menschen fortlaufend verbessern. Weitere Informationen unter **www.intel.com/community** und **www.intel.com/pressroom.**

Computacenter
Services & Solutions

Über Computacenter
Computacenter ist Europas führender herstellerübergreifender Dienstleister für Informationstechnologie. Für seine Kunden entwickelt, implementiert und betreibt er maßgeschneiderte IT-Lösungen. Weitere Informationen unter **www.computacenter.de.**