

HyperSecured PLC

Virtuelle Security für Automatisierungslösungen

Mit der konsequenten Vernetzung von Maschinen und Anlagen ergeben sich neue Möglichkeiten zur Fernwartung aber auch neue Herausforderungen im Bereich der Netzwerksicherheit. Die physikalische Trennung der Funktionen von Steuerung oder HMI und einer Appliance für die Netzwerksicherheit bieten den Vorteil der vollständigen Kapselung: Die jeweiligen Funktionen beeinflussen einander nicht; Entwickler und Zulieferer können sich jeweils auf ihre Kernkompetenzen konzentrieren. Nachteilig sind jedoch die entstehenden zusätzlichen Kosten. Durch den Einsatz virtueller Appliances für Steuerung oder HMI und Netzwerksicherheit können die Vorteile der getrennten Appliances erhalten werden, die Kosten werden jedoch durch die gemeinsame Nutzung der Hardware gesenkt.

Einführung

Die permanente Weiterentwicklung der Halbleiterprozesse führt zu einem stetig besser werdenden Verhältnis von Leistung zu Preis bei Computerprodukten („Moore's Law“). Im Maschinen- und Anlagenbau führt dies zu einer Verlagerung von Hardwarekomponenten zu Softwarefunktionen. Diese Tendenz findet ihre Grenze in der notwendigen Modularisierung, ohne die sich technische Risiken nicht beherrschen lassen und die Zusammenführung von Systemen verschiedener interner oder externer Zulieferer nicht möglich ist.

Um die Kostenvorteile der immer weiter entwickelten Halbleiterprodukte bei gleichzeitiger Modularisierung nutzen zu können, bieten sich Virtualisierungslösungen an.

Virtualisierungsanforderungen und -konzepte

Die Virtualisierung von Servern in IT-Landschaften ist heute Stand der Technik. Ziel ist dabei neben der effizienten Nutzung von Hardware insbesondere die Trennung der Aufgabe von der darunterliegenden Hardware. Der virtualisierte Server soll möglichst nicht von einer speziellen Hardware abhängig sein, sondern auf einer virtualisierten Hardware laufen, die herstellerunabhängig ist und eine beliebige Migration erlaubt. Typischerweise werden die virtuellen Server im Netzwerk auf einer Computerfarm mit gemeinsamer Storage-Lösung betrieben.

In der Steuerungstechnik liegen die Anforderungen anders. Die hierbei eingesetzten Systeme arbeiten auf dedizierter Hardware ohne Operatoreingriff. Typischerweise hat mindestens eine Komponente Echtzeitanforderungen.

Hardwarevirtualisierung

Bei der Hardwarevirtualisierung wird dem Gastsystem ein vollständiger eigener Computer vorgegaukelt.

- Das Gastsystem behält seine eigene Zeitscheibenverwaltung, eine Echtzeitfähigkeit ist hierdurch nicht möglich.
- Das Gastsystem kann je nach Implementierung (Unterstützung durch die verwendete Hardware) auf unterliegende Hardwarekomponenten direkt zugreifen. Andere Komponenten werden komplett simuliert, wodurch ein sehr komplexer Hypervisor beziehungsweise ein Wirtssystem mit Virtualisierungslösung notwendig werden.
- Die Performance des Gastsystems kann etwa die eines eigenständigen Systems erreichen, solange keine Ein-/Ausgabeoperationen über simulierte Komponenten erfolgen.

Paravirtualisierung

Bei der Paravirtualisierung wird das Gastsystem modifiziert, um besser mit dem Hypervisor oder Wirtssystem kooperieren zu können.

- Zeitscheiben- und Speicherverwaltung können enger miteinander verflochten werden, so dass Echtzeitverhalten erzielt werden kann.
- Die interne Kommunikation zwischen Gastsystemen oder Gastsystem und Hypervisor erfolgt über effiziente spezialisierte Schnittstellen.

Hypervisor/Wirtssystem

Der Hypervisor ist die Virtualisierungssoftware, die die virtuelle Maschine bereitstellt.

- **Typ 1** Hypervisoren laufen direkt auf der Hardware und koordinieren nur die vorhandenen Hardwareressourcen. Soll der Hypervisor selbst auf Hardware zugreifen können, muss er über entsprechende Treiber verfügen.
- **Typ 2** Hypervisoren laufen selber als Applikation in einem Wirtssystem. Der Hypervisor kann sich hier der Treiber des Wirtssystems bedienen, die erzielbare Performance sinkt aber durch die zusätzliche Betriebssystemschicht.

Konzept

Die in der Beispielimplementierung zu lösende Aufgabe ist die Kombination einer echtzeitfähigen Profinet-Steuerung mit einer Security Appliance als Firewall und Fernwartungslösung.

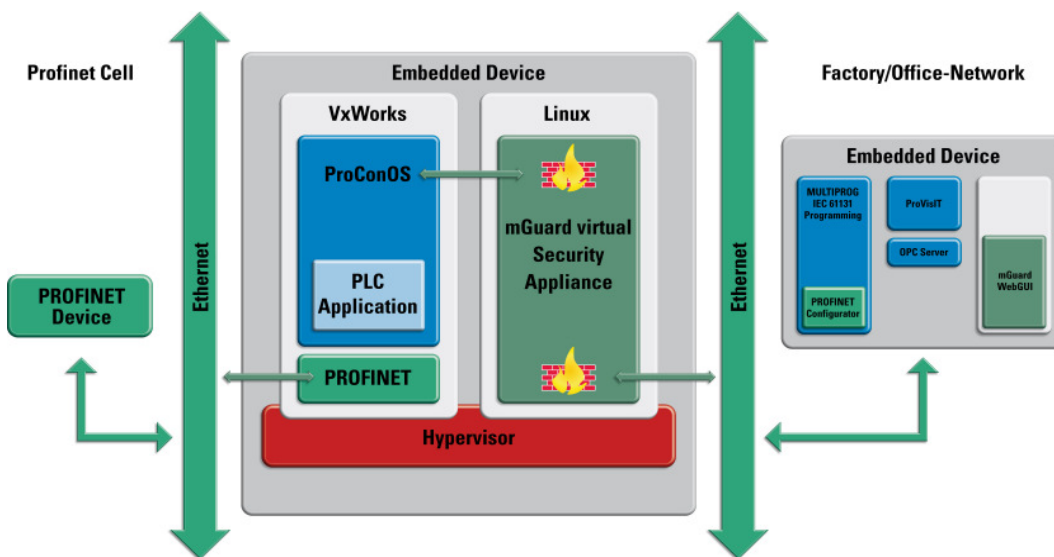


Bild 1: Struktur der HyperSecured PLC

Die Struktur der Lösung ist in Bild 1 dargestellt:

- Die Profinet-Kommunikation zwischen Steuerung und den anderen Komponenten findet in einem eigenen Ethernet-Netzwerk statt, welches keine weiteren Verbindungen nach außen hat. Hierdurch ist die zeitkritische Kommunikation jederzeit sichergestellt, da keinerlei Störungen aus anderen

Bereichen einwirken können.

- Die Kommunikation der Steuerung zur Außenwelt (Statusinformationen, Konfiguration) erfolgt durch die Security Appliance hindurch, der Rechner mit der Programmiersoftware und andere Komponenten befinden sich im ungesicherten Bereich.
- Die interne Kommunikation zwischen der Steuerung und der Security Appliance erfolgt rein netzwerkbasierend mittels einer virtuellen Netzwerkschnittstelle.

Hardware

Es kommt eine embedded PC Plattform bestehend aus einer CPU-Platine mit einem Trägerboard für die Peripherieanschlüsse zum Einsatz. Die Hardware ist lüfterlos und ohne drehende Teile bei Gesamtabmessungen von 120x70cm.

- Intel Atom Z530 CPU mit 1.6GHz (1 Core)
- 512MB RAM
- 2 Gbit-Ethernet Anschlüsse (On-Board+PCIe)

Wind River Hypervisor

Der Wind River Hypervisor ist als Typ 1 Hypervisor mit ca. 0,5 MB sehr ressourcenschonend, die Umsetzung der echtzeitfähigen HyperSecured PLC erfolgt mittels Paravirtualisierung zur optimalen Ausnutzung der Ressourcen.

- Für die Lösung der Aufgabenstellung wird der einzelne CPU Core durch den Hypervisor auf zwei virtuelle Boards abgebildet.
- Die Zuweisung der Zeitscheiben für die virtuellen Maschinen erfolgt mittels eines statischen Modells, so dass ein definiertes Zeitverhalten erzielt wird.
- Die für den Betrieb notwendigen Peripheriekomponenten, insbesondere die Netzwerkschnittstellen, werden den einzelnen virtuellen Maschinen direkt zugewiesen. So wird der I/O-Speicherbereich zugeordnet und die Interrupts werden exklusiv durch die virtuelle Maschine bedient.

Steuerung

Die Profinet-Steuerung wird durch das Laufzeitsystem ProConOs unter VxWorks realisiert. Die Steuerung kommuniziert zur Laufzeit über ein separiertes und exklusives Ethernet-Netzwerk mit weiteren Profinet-Komponenten. Zur Programmierung und Statusüberwachung wird der Zugang zum externen Netzwerk benötigt, welcher mittels einer virtuellen Netzwerkschnittstelle geschützt durch die Security Appliance erfolgt.

Der Ressourcenbedarf der Steuerung liegt bei ca. 1.5 MB. Die zur Paravirtualisierung notwendigen Eingriffe erfolgten nur im VxWorks. Für das Laufzeitsystem war die Einbindung in die Gesamtlösung transparent.

mGuard Security Appliance

Die mGuard Security Appliance liegt auf der „unsicheren“ Seite. Ein Zugriff auf die Steuerung wird durch die mGuard Firewall blockiert, solange nicht eine spezielle Regel für den Zugriff vom Projektierungsrechner aktiviert wird.

Der mGuard stellt dabei einen umfassenden Schutz sicher, da durch die direkte Hardwarezuweisung der Netzwerkschnittstellen nur der mGuard mit dem unsicheren Netzwerk in Kontakt gerät. Probleme im Netzwerkstack einer anderen Appliance oder eines Wirtssystems sind daher ausgeschlossen. Auch der Überlastschutz greift aufgrund der direkten Hardwarekontrolle. Im Extremfall eines Denial of Service (DoS)-

Angriffs könnte höchstens der mGuard komplett überlastet werden und Pakete verwerfen oder ausgebremst werden. Aufgrund der vollständigen Trennung der Systeme hinsichtlich Speicher und Rechenzeit durch den Hypervisor bleibt die Funktion der Steuerung hierdurch aber unbeeinträchtigt.

Durch die integrierte Virtual Private Network (VPN)-Funktion per IPsec mit sicherer Authentifizierung und Verschlüsselung kann der Zugriff auf die Steuerung auch aus der Ferne erfolgen, wobei der VPN-Tunnel vom mGuard terminiert wird. Die Steuerungssoftware sieht nur normale IP-Kommunikation.

Zur Paravirtualisierung mussten Änderungen am Linux-Kern vorgenommen werden, außerdem wurde die Systemkonfiguration auf die virtuelle Maschine angepasst. Für die x86-Architektur ist der mGuard auf einen Speicherbedarf von 128 MB konfiguriert.

Integration

Für die Integration der Gesamtlösung mussten die virtuellen Appliances zusammengebunden werden, wobei die virtuellen Maschinen getrennt und unabhängig bereitgestellt wurden. Eine Beeinflussung untereinander fand also nicht statt. Die erwünschte Trennung der Funktionen und Entwicklungskompetenzen wurde vollständig erreicht.

Bezogen auf die Ressourcenaufteilung kann festgestellt werden, dass bereits die verwendete, für eine x86-Architektur nicht üppig ausgestattete Plattform deutlich mehr Rechenleistung und Speicher bereitstellen kann als für die Anwendung notwendig.

Zusammenfassung

Mittels einer Virtualisierungslösung, welche speziell für den Embedded- bzw. Industrial-Markt konzipiert ist, ist eine zukunftsweisende Konsolidierung von Funktionen auf eine einzelne Hardware möglich, wobei die Vorteile getrennter Maschinen hinsichtlich der Zuverlässigkeit und Modularisierung vollständig erhalten werden.

Ausblick

Die vorgestellte Musteranwendung ist problemlos auf weitere Anwendungen skalierbar. Auf einem Single-Core-System lässt sich die Hardware in mehr virtuelle Boards unterteilen. Durch die Verwendung eines Multi-Core Prozessors kann die Performance erheblich gesteigert werden.

Durch die Verwendung weiterer virtueller Boards und die Unterstützung zusätzlicher Betriebssysteme z.B. unter Ausnutzung von Hardware-Virtualisierung lassen sich weitere Komponenten integrieren. So könnte z.B. eine auf der Hardware vorhandene Display-Ansteuerung verwendet werden, um auch die Bedieneroberfläche, welches häufig unter Microsoft Windows läuft, zu integrieren. Durch die vollständige Trennung der virtuellen Systeme ergäbe sich ein hochzuverlässiges System bei gleichzeitig optimierten Hardwarekosten.

Kontakt

Innominate Security Technologies AG
protecting industrial networks
Rudower Chaussee 13
12489 Berlin
Tel.: +49.30.921028-0
Fax: +49.30.921028-020
contact@innominate.com
www.innominate.com