Wie sich sicherheitsrelevanten und nicht-sicherheitsrelevante Funktionen auf medizinischen Embedded-Systemen effizient trennen lassen.

Effizient separieren

Embedded-Systeme spielen eine wesentliche Rolle bei vielen medizinischen Anwendungen, von Defibrillatoren über MRI-Geräte bis hin zur Roboter-assistierten Chirurgie. Hierbei sollen medizinische Geräte neben ihrer medizinischen Funktionalität auch eine gute Bedienbarkeit und einen gewissen Bedienkomfort aufweisen, etwa in Bezug auf umfangreiche grafische Bedienoberflächen, Datenspeicherung und Netzwerkkommunikation. Dies stellt die Entwickler solcher Geräte vor die Herausforderung, im selben Gerät Funktionen verschiedener Kritikalität integrieren zu müssen, d.h. Funktionen, deren Ausfall im schlimmsten Falle zur Verletzung oder dem Tod eines Menschen führen kann, wie auch Funktionen, deren Ausfall keine schwerwiegenden Konsequenzen hat. Für die Softwareentwicklung stellt sich hierbei die Frage, wie die verschiedenen zugehörigen Softwarekomponenten effizient entwickelt und auf einem medizinischen Gerät integriert werden können, d.h. auf eine Weise, die bei vertretbarem Entwicklungsaufwand die Sicherheit des Geräts garantiert. Ein gängiges Konzept für die Entwicklung ist die Segregation der Software in Komponenten mit unterschiedlichen Software-Sicherheitsklassen, welche eine Differenzierung beim Entwicklungsaufwand der Komponenten erlaubt. Die Herausforderung hierbei ist dann, zur Laufzeit sicherzustellen, dass eine hinreichende Trennung von Komponenten höherer und niedrigerer Sicherheitsklasse gewährleistet wird.

Diagramm 1 zeigt einen schematischen Aufbau eines typischen Embedded-Systems mit verschiedenen funktionalen Komponenten, die oft unterschiedliche Kritikalität bezüglich der Gerätesicherheit haben können. In allen Komponenten können zufällige und systematische Fehler auftreten. Wie unter diesen Voraussetzungen trotzdem die Freiheit von nicht-vertretbaren Risiken gewährleistet werden kann, wird im Folgenden beschrieben.

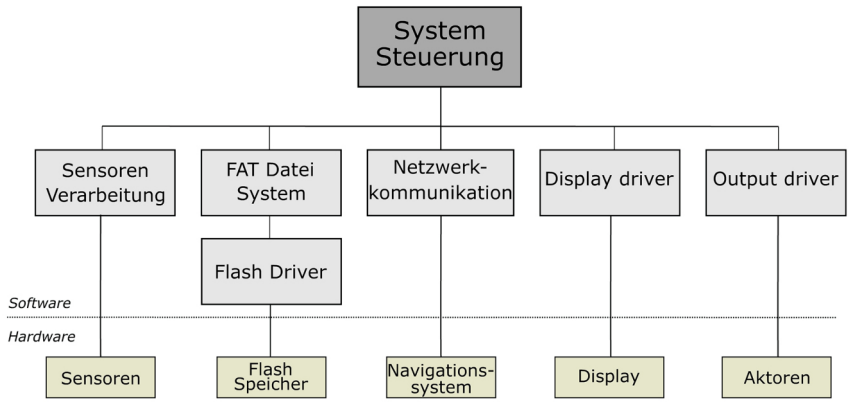

Diagramm 1: Schematischer Aufbau eines typischen Embedded-Systems

Software-Partitionierung

Ein übliches Konzept zur Trennung sicherheitsrelevanter und nicht-sicherheitsrelevanter Softwarekomponenten ist die Zuordnung zu unterschiedlichen Hardware-Komponenten (d.h. physikalisch getrennten Prozessoren, Speicherbereichen). Dies erhöht in der Regel allerdings den Entwicklungsaufwand und die Kosten, erhöht die Gerätegröße und schränkt die Interaktion zwischen den Softwarekomponenten ein. Die physikalische Trennung ist daher oft keine realistische Lösung, vielmehr ist eine Koexistenz von sicherheitsrelevanten und nicht-sicherheitsrelevanten Softwarekomponenten auf derselben Hardware-Komponente wünschenswert. Ohne zusätzliche Schutzmaßnahmen birgt dies allerdings die Gefahr von Interferenzen zwischen Softwarekomponenten, selbst wenn diese gemäß Segregation für jede Softwaresicherheitsklasse separat entwickelt wurden. Um eine zuverlässige zeitliche Trennung (im Sinne des Prozess-Schedulings) und räumliche Trennung (im Sinne von Speicherbereichen) zu erreichen, müssen daher sicherheitskritische und nicht-sicherheitskritische Funktionen in getrennten Prozessbereichen ausgeführt werden.

Virtualisierung als Partitionierungstechnik

In den letzten Jahren hat die Technologie der Virtualisierung zur Partitionierung von Prozessbereichen auch im Bereich der Embedded-Systeme Verbreitung gefunden. Bei dieser Technologie werden mithilfe eines Hypervisors virtuelle Maschinen (oder Partitionen) erzeugt, wobei diese Partitionen isolierte Prozessbereiche darstellen und mittels virtueller Ressourcen auf die verfügbaren physikalischen Ressourcen des Systems zugreifen können. Hypervisoren ermöglichen so eine funktionale Trennung, eine bessere Fehlerbehandlung und die Koexistenz verschiedener Betriebssysteme (z.B. Real-Time und Nicht-Real-Time OS) auf einer Hard- »

Bilder: embeX GmbH

ware-Plattform. Die in diesem Artikel beschriebene Strategie zur Separation von Prozessen unterschiedlicher Kritikalität nutzt einen Typ1-Hypervisor mit Paravirtualisierung, auch als „bare-metal“ Hypervisor bezeichnet. Diese Art von Hypervisor (siehe Diagramm 2) läuft direkt auf der Hardware des Systems und eignet sich in Kombination mit Paravirtualisierung sehr gut für Embedded-Systeme aufgrund der geringen Größe, der guten Geschwindigkeitsperformance und des einfachen Aufbaus.

Die Nutzung eines fixen zyklischen Schedulings im Hypervisor und einer Memory Management Unit (MMU), wie sie in vielen Embedded-Plattformen verfügbar ist, ermöglicht eine starke zeitliche und räumliche Trennung der verschiedenen Funktionen des Systems. Vom Hypervisor bereitgestellte Kommunikationsschnittstellen erlauben eine Kommunikation der Partitionen untereinander.

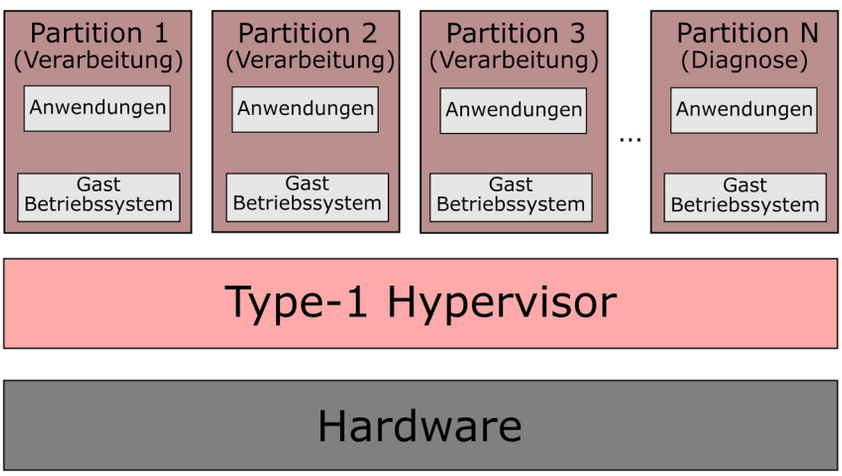

Diagramm 2: System Virtualisierung mit Type-1 Hypervisor

Sicherheitskette zur Behandlung von Fehlersituationen

Während die Partitionierung eine Trennung der Softwarekomponenten garantiert, muss zusätzlich noch die Behandlung von Fehlern sichergestellt werden, die innerhalb einer Partition (im enthaltenen Betriebssystem oder einer Anwendung) oder innerhalb des Hypervisors auftreten. Im Allgemeinen soll bei Auftreten eines Fehlers eine entsprechend zuständige Sicherheitsfunktion das Gerät in einen sicheren Zustand bringen, in dem das Gerät kein Risiko für seine Umgebung darstellt. Hierbei kann es von Vorteil sein, eine hierarchische Kette von Sicherheitsfunktionen einzuführen, so dass das Versagen einer Sicherheitsfunktion auf einer Ebene durch eine hierarchisch nächste Ebene festgestellt und eine entsprechende übergeordnete Sicherheitsfunktion ausgeführt wird, um somit das Gerät trotzdem in einen sicheren Zustand zu bringen.

In der hier beschriebenen Architektur (siehe Diagramm 3) wird das System zum einen in mehrere Verarbeitungspartitionen aufgeteilt, die jeweils für die Ausführung einer oder mehrere wohldefinierter Funktionen zuständig sind und die auch über bestimmte Sicherheitsfunktionen verfügen können, die bei Feststellung eines Fehlers innerhalb der Partition das System in einen sicheren Zustand überführen. Zum anderen wird eine Diagnosepartition eingeführt, die sowohl die Verarbeitungspartitionen wie auch bestimmte Funktionsparameter des Hypervisors überwacht und bei einer detektierten Fehlfunktion das Gerät in einen sicheren Zustand überführt. Die Funktionsfähigkeit der Diagnosepartition wird durch einen Hardware-Timer sichergestellt. Die Diagnosepartition setzt nach erfolgreicher Abarbeitung aller Diagnosefunktionen einen Reset-Trigger für den Hardware-Timer. Wird dieser Trigger wegen einer Fehlfunktion der Diagnosepartition nicht gesetzt, läuft der Hardware-Timer aus und das Gerät geht Hardware-initiiert in einen sicheren Zustand. Somit ist sichergestellt, dass auf jeder Ebene die vorhandenen Sicherheitsfunktionen entweder ausge- »

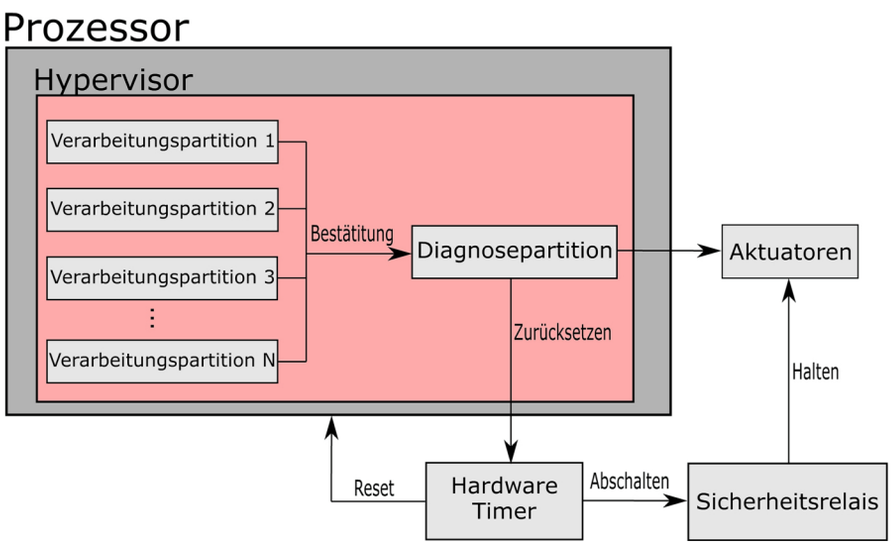

Diagramm 3: Sicherheitskette mit Diagnosepartition und Hardware-Timer

führt werden oder das Versagen einer Sicherheitsfunktion auf der jeweils nächsten Ebene detektiert wird und entsprechende Maßnahmen ergriffen werden.

Der oben beschriebene systematische Ansatz zur Separation sicherheitskritischer und nicht-sicherheitskritischer Softwarekomponenten auf Basis eines Typ1-Hypervisors wurde erfolgreich implementiert und es wurde seine Anwendbarkeit im Bereich medizinischer Embedded-Systeme gezeigt.

Autoren:
Jordi Bigorra Fibla
Entwicklungsingenieur
Dr. Michael Pfeiffer
Senior Systemingenieur
embeX GmbH

KONTAKT

embeX GmbH
Heinrich-von-Stephan-Str. 23
D-79100 Freiburg im Breisgau
Tel. +49 761 479 79 90
www.embeX.de

SCHALTNETZTEILSERIE RPS-500 FÜR MEDIZINANWENDUNGEN

Neu im Vertriebsprogramm der EMTRON electronic GmbH ist die RPS-500-Serie (500 Watt) von Mean Well für medizinische Applikationen.

Die Schaltnetzteile in offener Bauform punkten mit ihrer kompakten Größe von 5„ x 3“ und einem Universaleingang von 80 - 264 VAC. Angesichts der rasanten Entwicklung der Medizinindustrie und der steigenden Nachfrage nach Standardnetzteilen hat Mean Well die neue RPS-500-Serie mit 500 Watt auf den Markt gebracht, um den Anforderungen an leistungsstärkere Open-Frame-Lösungen für die medizinische Elektronik gerecht zu werden.

Die RPS-500-Serie bietet Mean Well in unterschiedlichen Bauformen an: Open-Frame (RPS-500), mit Abdeckung (Lochblech, lüfterlos, RPS-500-C) sowie im Gehäuse mit integrierten Lüftern (Top-Lüfter: RPS-500-TF, Seitenlüfter: RPS-500-SF). Mit den verschiedenen optionalen Bauformen stehen jetzt neue Standardlösungen für zahlreiche medizinische Anwendungen zur Verfügung. Die RPS-500-Modelle sind alle nach den neuesten medizinischen Sicherheitsstandards wie IEC 60601-1, ANSI/AAMI ES 60601-1 und TÜV EN 60601-1 zertifiziert. Mit doppelter Isolationsfähigkeit (2 x MOPP; MOPP = Means of Patient Protection/Patientenschutz) und extrem niedrigem Ableitstrom (<190 uA) ist die RPS-500-Serie für medizinische Anwendungen vom Typ BF geeignet.

Diese Netzteile überzeugen zudem durch eine niedrige Leerlaufleistung (<0,5 W durch PS-ON Funktion), eine Status-LED, einen geringen Standby-Verbrauch, Standby 5 VDC/0,6 A und Hilfsspannung 12 VDC/0,5 A.

Zum Einsatz kommen die Modelle bei einer Vielzahl von Behandlungs-, Diagnose-, Labor-, Überwachungs- und Medizinroboteranwendungen.

Merkmale:

- Leistungsstarkes, miniaturisiertes Design: 5„ x 3“
- 2 x MOPP Isolationslevel
- Extrem niedriger Ableitstrom <190 µA, geeignet für den Einsatz in medizinischen Anwendungen vom Typ BF
- 80 - 264 VAC Eingangsspannung mit integrierter PFC-Funktion
- 320 W mit Kühlung durch freie Luftkonvektion und 500 W mit 25 CFM forcierte Lüftung, 550 W Spitzenlast (3 Sekunden)
- Geeignet für den Einbau in Systeme der Klasse I (mit FG) oder der Klasse II (ohne FG)
- Leistungsaufnahme ohne Last < 0,5 W
- Hoher Wirkungsgrad bis zu 94 %
- Betriebstemperaturbereich -30 bis +70 °C
- Betriebshöhe bis zu 4.000 m
- Schutzfunktionen: Kurzschluss , Überlast, Überspannung, Übertemperatur
- Zusätzliche Funktionen: Standby 5 VDC/0,6 A, Hilfsspannung 12 VDC/0,5 A, Spannungskompensation
- Medizinische Sicherheitszulassungen: UL, cUL, TÜV, EAC, CB, CE
- LED-Anzeige für das Einschalten
- Abmessungen (L x B x H): 127 x 76,2 x 40 mm
- 3 Jahre Herstellergarantie

www.emtron.de