Energie-effiziente Systemarchitekturen für sicherheitskritische eingebettete Geräte

Felix Bruns

Eingebettete Geräte werden häufig in *sicherheitskritischen Anwendungen* eingesetzt, beispielsweise in medizinischen Geräten, wie Herzschrittmachern, oder potentiell gefährlichen Systemen, wie Chemieanlagen und PKWs. In diesen Anwendungsfällen ist der Einsatz eines eingebetteten Gerätes an strenge Auflagen für dessen Architektur, Entwicklung und Überprüfung geknüpft. So muss eine strikte Trennung zwischen verlässlicher, sicherheitskritischer Software und Software mit unbekannter Verlässlichkeit durchgeführt werden, um zu verhindern, dass die sicherheitskritische Funktionalität des Gerätes durch Fehler in nicht-sicheren Software Komponenten beeinträchtigt wird. Dieses Vorgehen wird als *Partitionierung* bezeichnet.

Während in der Luftfahrt- und Automobilindustrie der Einsatz von speziellen Betriebssystemen zur Partitionierung bereits verbreitet ist, werden diese in vielen anderen Arten von eingebetteten Geräten bisher nicht eingesetzt. Aufgrund der starken Energiebegrenzungen können häufig nur kleine Micro-Control-Units (MCUs) mit geringer Rechenleistung und kleinem Speicher eingesetzt werden, was den Einsatz komplexer Betriebssysteme erschwert. Aus diesem Grund wird die Trennung von sicherheitskritischer und nicht-sicherer Software in diesen sogenannten *tief-eingebetteten* Systemen bisher durch die Ausführung auf separaten MCUs erreicht. Die resultierende Architektur besitzt gute Sicherheitseigenschaften, resultiert aber in einem erhöhten Energieverbrauch sowie einer stark verminderten Flexibilität und Modularität. Aufgrund der wachsenden Komplexität, sowie der zunehmenden Vernetzung von Geräten und Systemen, ist es deshalb fraglich, ob diese herkömmliche Architektur den zukünftigen Herausforderungen gewachsen ist.

In dieser Arbeit werden Betriebssysteme zur Partitionierung von sicherheitskritischer und nicht-sicherer Software für Systemen mit stark begrenzten Ressourcen untersucht. Ausgehend vom Beispiel eines industriellen Messgerätes für sicherheitskritische Prozesse, werden die in dieser Klasse von Systemen auftretenden Randbedingungen und die sich hieraus ergebenden Herausforderungen bei der Partitionierung erläutert. Anschließend werden Techniken und Systemarchitekturen für partitionierte Systeme hinsichtlich ihrer Tauglichkeit für diese Klasse von Systemen analysiert.

Die in tief-eingebetteten Systemen häufig stark begrenzte Energieversorgung stellt eine besondere Schwierigkeit für die Entwicklung sicherer Geräte dar. Aus diesen Grund wird in dieser Arbeit ein Algorithmus zum energiebasierten Scheduling entwickelt, der eine exakte Kontrolle der Verlustleistung des Gerätes ermöglicht. Zudem erlaubt es der Algorithmus eine energetische Trennung zwischen sicherheitskritischer und nicht-sicherer Software durchzuführen. Somit kann eine Beeinflussung der Sicherheitsfunktion durch einen übermäßigen Energieverbrauch der nicht-sicheren Software verhindert werden. Hierdurch kann die Entwicklung sicherer Systemen mit stark begrenzter Energieversorgung erheblich vereinfacht werden.

Um geeignete Partitionierungsmechanismen für tief-eingebettete Systeme zu identifizieren, werden im zweiten Teil der Arbeit verschiedene Betriebssystemarchitekturen und Techniken zur Partitionierung hinsichtlich ihrer Effizienz, Echtzeiteigenschaften und Komplexität untersucht. Hierbei wird gezeigt, dass ein Virtualisierungsansatz in tief-eingebetteten Systemen sehr effizient realisiert werden kann. Weiterhin ermöglicht dieser Ansatz eine hohe Modularität und Rückwärtskompatibilität. Aufgrund dieser Vorteile wird in dieser Arbeit ein Hypervisor entwickelt, dessen Architektur und Mechanismen für tief-eingebettete Systeme optimiert ist. Hierbei werden die vergleichsweise geringe Komplexität, sowie die Besonderheiten von tief-eingebetteten Systemen ausgenutzt, um für diesen Fall optimierte, sichere Lösungen zu finden.

Im letzten Teil der Arbeit wird der Hypervisor zur Partitionierung des industriellen Messgerätes genutzt. Hierbei werden verschiedene Alternativen zur geräte-internen Kommunikation untersucht, und die Auswirkungen auf den Energieverbrauch und das Echtzeitverhalten des Messgerätes ermittelt. Das resultierende System wird mit dem ursprünglichen System verglichen und die Sicherheit und Rückwärtskompatibilität der vorgestellten Lösungen analysiert.

In dieser Arbeit wird Software-Partitionierung erstmalig für tief-eingebettete Systeme, welche weder über MMU noch sonstige Virtualisierungserweiterungen verfügen, untersucht. Eine herausragende Erkenntnis dieser Arbeit ist, dass Virtualisierungstechniken aufgrund der Eigenschaften dieser Systeme sehr effizient realisiert werden können. Durch eine flexible Nutzung der verfügbaren Rechenleistung zwischen verschiedenen Partitionen, sowie einer Reduktion des Kommunikationsaufwandes, ermöglicht der in dieser Arbeit entwickelte Virtualisierungsansatz signifikante Energieeinsparungen. Weiterhin erlaubt der Einsatz von Software-Partitionierung eine erhöhte Flexibilität und somit eine Verbesserung der Sicherheitsarchitektur. Die in dieser Arbeit vorgestellten Techniken ermöglichen somit effizientere, kleinere und kostengünstigere Systeme in einer Reihe von Anwendungsgebieten, insbesondere für industrielle Messgeräte, aber auch in anderen Einsatzgebieten, in denen sowohl Sicherheit als auch Energieeffizienz von hoher Bedeutung sind, beispielsweise medizinische oder drahtlose Geräte.