Diss. ETH No. 20818

Paradigms and tools for developing dependable realtime software

A dissertation submitted to the
ETH ZURICH

for the degree of
Doctor of Sciences

presented by
DANIEL KELLER
Dipl. Informatik-Ing. ETH
born April 12, 1972
citizen of Konolfingen (BE)

accepted on the recommendation of
Prof. Dr. Jürg Gutknecht, examiner
Prof. Dr. Peter Müller, co-examiner
Prof. Dr. med. Patrick Hunziker, co-examiner

2013

Abstract

This thesis presents research into application-aware operating systems (OS) for safety-critical applications. It has been motivated by the necessity to develop of a “next generation” wearable medical monitoring device. Commercially available devices are often based on 16 bit microcontrollers with limited possibilities in many respects. A paradigm shift towards fully fledged 32 bit technology is overdue. It allows a new generation of *wearable devices* following the “multiple parameter, multiple purposes” paradigm to be developed. Such devices offer great flexibility regarding their field of application, and they will finally replace simpler single purpose devices and even some of the stationary monitoring systems.

A de facto prerequisite to the design and build of complex embedded systems is the availability of an OS that offers a sufficiently abstract application programming interface (API) and programming model. In the case of safety-critical applications, like the one envisioned here, the OS must in addition be highly *dependable*. This thesis presents an approach towards the goal of a fully dependable OS based on a natively implemented runtime layer with some provable properties. To accompany this, an evolved high-level programming language will be introduced to support the development of dependable application software.

The scientific contribution of this work largely lies in the symbiotic relationship between programming language and OS. In particular, how to take advantage of the programming language in order to exploit and build on particular static properties of the runtime system and increase its runtime predictability will be explored.

As proof of concept, a wearable device based on a 32 bit ARM processor technology and operated by the entirely developed OS was built and field-tested in the context of a medical application with the goal of reliably monitoring

heart patients and detecting abnormalities.

Zusammenfassung

Diese Arbeit präsentiert ein applikationsspezifisches Betriebssystem für sicherheitskritische Anwendungen. Ausgangspunkt war die Entwicklung eines neuartigen, tragbaren medizinischen Überwachungsgerätes. Kommerziell erhältliche Geräte basieren häufig auf 16 bit Mikrokontrollern und sind in mehrfacher Hinsicht limitiert. Ein Paradigmenwechsel hin zu voll ausgebildeten 32 bit Prozessoren ist überfällig. Dieser Paradigmenwechsel erlaubt den Bau einer neuen Generation von Geräten, die verschiedenartigste Sensoren für diverse Zwecke nutzbar machen. Solche Geräte sind flexibel einsetzbar und können einfachere oder sogar stationäre Überwachungssysteme substituieren.

Eine Voraussetzung um komplexe, eingebettete Systeme zu bauen, ist die Verfügbarkeit eines Betriebssystems, das ein genügend abstraktes Programmiermodel und eine genügend abstrakte Programmierschnittstelle bietet. Bei den angepeilten sicherheitskritischen Anwendungen wird zusätzlich ein hohes Mass an Zuverlässigkeit gefordert. Diese Arbeit präsentiert Schritte hin zu einem vollständig zuverlässigen Betriebssystem basierend auf einem nativen System mit beweisbaren Eigenschaften. Um die Entwicklung zuverlässiger Applikationssoftware zu ermöglichen, wird die Evolution einer Programmier-Hochsprache wird eingeführt, .

Der wissenschaftliche Beitrag dieser Arbeit liegt in der Symbiose zwischen Programmiersprache und Betriebssystem. Im Speziellen wird untersucht, wie die Programmiersprache genutzt werden kann, um statische Eigenschaften des Betriebssystems zu stärken und das Laufzeitverhalten deterministischer zu machen.

Als Machbarkeitstudie wurde ein tragbares Gerät basierend auf einem 32 Bit ARM Prozessor und dem vollständig entwickelten Betriebssystem vorgestellt. Die medizinische Applikation um Herz Patienten zu überwachen, wurde im Feld getestet.