Addressing Today’s Medical Device Challenges

The medical device market is undergoing tremendous transformation due to significant societal, business, and technology shifts. The transformation begins with a large and aging population with longer life spans, requiring more medical care at a time when the industry is facing an increasing shortage of physicians and hospital care while costs continue to climb.

To improve efficiency and reduce business costs, the medical industry is searching for solutions that are mobile and can share data broadly by connecting the hospital, remote doctors, labs, and homes. To exacerbate the situation, as the technical complexity of medical devices increases, medical device failures are becoming more commonplace which is subsequently causing government agencies to increase focus on regulatory compliance.

To address this problem, and to further reduce risk and cost, device manufacturers are moving from a mindset of innovation to one of evolution; requiring the reuse and extension of investments related to medical device software and related regulatory compliance.

The Mentor® Solution for Medical Devices has been built to address this transformation, enabling medical device manufacturers to leverage proven and existing investments. The Mentor solution enables the creation of feature-rich, power-efficient, connected, reliable, safe, and secure systems. It allows for securely connected devices locally and to the extended cloud. This multiplatform approach includes proprietary and open source runtime environments, a multicore framework to accelerate complex heterogeneous system development and enable reuse, rich graphics support, integrated tools, security and safety and security certifications that are relevant to developers of medical devices (making it easier to achieve certification to the highest medical safety requirements.) The solution includes a comprehensive security process and a team that ensures critical security defects are addressed.

SOLUTION FEATURES:

- A complete medical device solution encompassing a broad embedded suite of open source and propriety runtime environments, tools, and services
- Backed by the people, process, and technology to address the critical safety and security considerations of medical devices
- Multicore framework and virtualization technologies enable code reuse and supports leading edge homogenous and heterogeneous SoC architectures
- Complemented by a diverse and well-integrated partner ecosystem
- Global support and services

BENEFITS:

Streamlined path to regulatory compliance
Mentor’s proven and reliable solutions, augmented with security processes and safety artifacts to IEC 62304 Class C reduce the time and cost to meet stringent regulatory compliance.

Cost and risk reduction through convergence
The convergence of product features and capabilities reduces risk and cost by enabling IP reuse, reducing power usage (electricity costs), and decreasing downtime (security vulnerabilities).

Realize medical IoT and cloud strategies
The Mentor portfolio supports all major connectivity protocols to create devices that can be securely integrated into private or public cloud infrastructures.

Reduce time to productivity, time to market
Only Mentor provides the industry’s broadest portfolio of runtime environments, integrated tools, services and partner technologies – allowing projects to get off the ground quickly.
tracked, evaluated, and fixed. The solution is further augmented with a rich ecosystem of partners who complement the solution with a breadth of connectivity and security capabilities.

COTS Software and Medical Devices

As part of the hazard analysis performed by the device manufacturer, the potential impact of failure of COTS software that might be used in the design on the patient is considered. Depending on the severity of impact on the patient, one of two different levels of documentation might be required by the United States’ FDA: “basic” and “SPECIAL” (as outlined in “Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf (OTS) Software Use in Medical Devices, 9/9/1999). Basic documentation essentially only requires basic commercial processes (which are fully performed by Mentor), the SPECIAL requirements put a much stronger burden on both the manufacturer and the COTS software provider:

1. Provide assurance to FDA that the product development methodologies used by the OTS Software developer are appropriate and sufficient for the intended use of the OTS Software within the specific medical device. FDA recommends this include an audit of the OTS Software developer’s design and development methodologies used in the construction of the OTS Software. This audit should thoroughly assess the development and qualification documentation generated for the OTS Software.

2. Demonstrate that the procedures and results of the verification and validation activities performed for the OTS Software are appropriate and sufficient for the safety and effectiveness requirements of the medical device. Verification and validation activities include not only those performed by the OTS Software developer, but also include those performed by the medical device manufacturer when qualifying the OTS Software for its use in the specific medical device.

3. Demonstrate the existence of appropriate mechanisms for assuring the continued maintenance and support of the OTS Software should the original OTS Software developer terminate their support.

Mentor can support the device manufacturer with each of these in a comprehensive fashion. For Mentor® Embedded Linux® (MEL) customers, it starts with the industry standard Linux operating system which is used by manufactures around the world to create highly secure, safety critical devices. Mentor then hardens the distribution as needed, pre-integrates important utilities and packages and comprehensively validates the package using well-documented and traceable development processes. Beyond that, Mentor is best suited to support the three major FDA requirements for COTS software in SPECIAL applications as follows:

1. As recommended by the FDA, the manufacturer is welcome to review and audit Mentor’s Quality Management System, as required to meet these regulatory requirements.

2. The Mentor testing activities are fully documented, as far as the verification of the Linux kernel and packages included in MEL are concerned. Of course, the user should perform their own verification, which will further exercise the specific configuration of MEL used in the application.

3. Mentor provides commercial support for product releases for a period of five years; this support includes high priority and security issues that might be identified by our customers, internally or by the Linux community. If the lifetime of the medical device is expected to extend beyond five years, or if higher levels of premium support are required, then Mentor has long-term and premium support options to support any manufacturer use case.

Assuring Cyber Security in Medical Devices

As medical devices become more and more connected to the Internet, both inside and outside of the hospital, cyber security is of increasing concern. Security issues are not only a concern from a pure patient information/HIPAA perspective, but also because security issues provide a convenient vector for the injection of safety issues that can be exploited by criminals (Ransomware) or cyber terrorists.

Again, security starts with the capabilities Mentor builds into its products. For MEL, sophisticated security extensions such as SELinux and SMACK are pre-integrated, available and fully supported by Mentor. These packages allow the highest level of security to be built into medical devices. However, to maintain security of devices in the field, updates to protect against newly discovered exploits must also be considered.
Again, security starts with the capabilities Mentor Graphics builds into their products. For MEL, sophisticated security extensions such as SELinux and SMACK are pre-integrated, available and fully supported by Mentor Graphics. These packages allow the highest level of security to be built into the system.

The FDA provides guidance to the device manufacturer on how to manage the use of COTS software in the more complex world of connected devices (“Guidance for Industry: Cyber security for Networked Medical Devices Containing Off-the Shelf (OTS) Software”). In this guidance, the FDA recommends an ongoing relationship with your COTS vendors and to make certain that you understand the vendor’s cyber security policies and capabilities as part of your overall cyber security maintenance plan.

Since the foundational software provided by Mentor is the first line of defense for the devices that are developed by our customers, we take these security threats very seriously. Mentor’s policies, plans, processes, and responsive-ness mean that the burden of monitoring newly emerging threats, determining if they apply to your software, and taking any necessary actions falls upon Mentor instead of our customers.

Mentor has a Core Critical Security Team that monitors newly discovered vulnerabilities from numerous sources. When a new vulnerability is detected, we quickly identify which of our products are impacted (if any), assess the exposure and severity of the vulnerability, and develop and/or integrate needed fixes as quickly as possible, with a target time of 24 hours. Once any updates are created, they are made available to our customers along with documentation to describe the vulnerability, workarounds (if any), and solutions.

This comprehensive response ability allows our customers to update their devices as needed to keep them safe and secure.

The Mentor Embedded Solution for Medical Devices includes:

**Mentor Embedded Linux**
Offering two industry leading commercial embedded Linux solutions based on the Yocto Project® and Debian offering rich graphics, secure IoT and cloud enablement, and comprehensive development tools. Both versions are portable across leading hardware architectures, and offer commercial maintenance, security vulnerability monitoring and patches, and customization services.

**Nucleus RTOS**
Deployed in over three billion embedded devices, the Mentor® Nucleus® RTOS is a reliable, scalable, and fully optimized RTOS perfectly suited for a range of medical devices. At its foundation, Nucleus focuses on a small footprint, scalability, and performance. Nucleus includes a user-space process model for application separation and reliability, a comprehensive power management framework, a breadth of connectivity and security options, broad graphics support, and advanced multicore support. Nucleus is further enhanced to address specific medical requirements with safety certification to IEC 62304 Class C, and GE Digital Achilles security certification.

**Mentor Embedded Multicore Framework**
Many of today’s medical designs are moving from a single-core, single-OS architecture to complex heterogeneous multicore, heterogeneous-OS environments. This rich palette of options enables the creation of extremely powerful, flexible feature-consolidated devices, but also creates many complexities related to system architecture, booting, IPC, development, test and debug.

The Mentor Embedded Multicore Framework enables code reuse by allowing developers to configure, deploy, and manage multiple operating systems and applications across homogeneous and heterogeneous processors. This comprehensive software framework allows developers to manage the many challenges associated with inter-process communication (IPC), resource management/sharing, and management of cores within a heterogeneous multicore/multi-OS environment. The framework is available in a native environment, or in an enforced separation environment via Mentor’s support for Arm® TrustZone® or Mentor’s small footprint type-1 embedded hypervisor.

**Medical Device Middleware**
Mentor Embedded runtime platforms include connectivity and middleware capabilities needed to build feature-rich medical device systems. Included in these features is Qt® Graphics; integrated, optimized and instrumented for embedded applications. The platforms also include IoT technologies to support private and public Cloud strategies. These technologies include protocol support such as CoAP, RESTful API support, XMPP, MQTT, 6LowPAN, and others.
Native capabilities are complemented with industry-leading partner technologies. The Floodgate family of products from Icon Labs provides a foundation for developing secure, trusted, authenticated, and managed embedded devices, with technologies for secure boot, firewall, and intrusion detection. Distributed communications are enabled with Connext DDS (Distributed Data Service) from Real Time Innovations. Fault-tolerant file system support is provided by Datalight, Inc., with a pre-ported version of Reliance Nitro. For extremely resource-constrained devices requiring graphics, Mentor partners with Tara Systems.

**Sourcery CodeBench**

Sourcery™ CodeBench goes beyond being a compiler to provide developers with powerful, open source C/C++ development tools to build, debug, analyze and optimize embedded software. Sourcery CodeBench delivers a powerful toolset that helps embedded software engineers efficiently develop and optimize software for a variety of targets and various domains including connectivity, graphics, and video applications.

**More about Mentor**

Mentor, now a Siemens business, offers a family of embedded software products and services, including embedded software IP, tools, and professional services to assist developers and silicon partners to optimize their products for design and cost efficiency.

The registered trademark Linux® is used pursuant to a sublicense from LMI, the exclusive license of Linus Torvalds, owner of the mark on a worldwide basis. Android is a trademark of Google Inc. Use of this trademark is subject to Google Permissions. Qt® is a registered trademark of the Qt Company Oy. Yocto Project® is a registered trademark of the Linux Foundation.

For the latest product information, call us or visit: www.mentor.com/embedded