Application Note

How MontaVista can help address FDA security requirements for the Medical market?

The U.S. Food and Drug Administration (FDA) has been actively addressing cybersecurity concerns in medical devices. The FDA provides guidelines and recommendations to manufacturers to ensure the security of medical devices, especially those with embedded software.
The FDA's approach emphasizes a risk-based framework, and it encourages manufacturers to consider and address software security vulnerabilities, including Common Vulnerabilities and Exposures (CVEs).

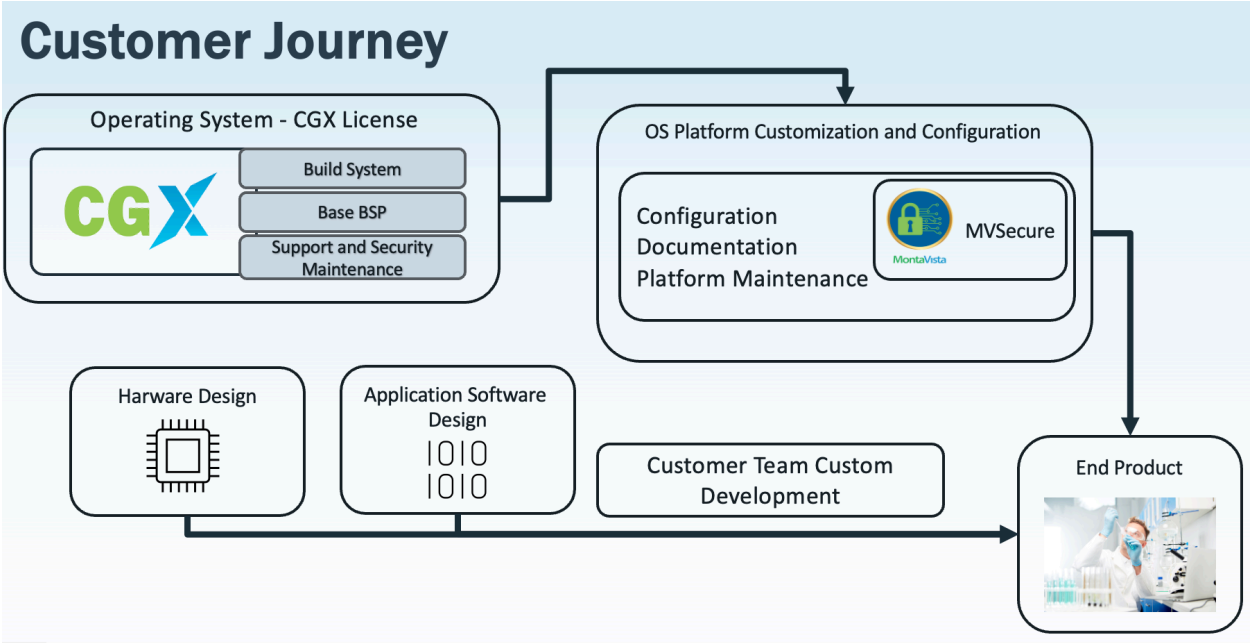
To start with, here are some key aspects of the FDA's requirements and recommendations as we see them at Montavista:

1. Pre-market and Post-market Guidance:
    - Pre-market: Manufacturers are expected to include cybersecurity considerations in the pre-market submission of medical devices. This involves providing information about the design, testing, and validation of the device's cybersecurity features.
    - Post-market: Continuous monitoring and management of cybersecurity risks are essential. Manufacturers are expected to have mechanisms in place to assess and respond to new vulnerabilities that may arise after the device is on the market.
2. Risk Assessment:
    - Manufacturers are encouraged to conduct a risk assessment that includes the identification of potential cybersecurity vulnerabilities. The assessment should consider the impact on patient safety and the effectiveness of the device.
3. Applying Security Controls:
    - Implementing security controls and best practices to mitigate identified vulnerabilities is a key expectation. This includes encryption, access controls, authentication mechanisms, and other security measures to protect the confidentiality, integrity, and availability of the device and its data.
4. Information Sharing:
    - The FDA encourages collaboration and information sharing within the healthcare and cybersecurity communities. This includes sharing information about vulnerabilities and potential threats to enhance the overall security posture of medical devices.
5. Coordination with NIST Guidelines:
    - The FDA often aligns its recommendations with the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Manufacturers are encouraged to follow relevant NIST guidelines for managing cybersecurity risk.
6. Software Development Life Cycle (SDLC):
    - Manufacturers should integrate cybersecurity into the entire software development life cycle, from design to maintenance. This involves secure coding practices, testing for vulnerabilities, and addressing any identified issues.
7. Incident Response and Recovery:

- Having an incident response plan in place is crucial. Manufacturers should be prepared to respond effectively to cybersecurity incidents, including timely communication with users and appropriate remediation actions.

At MontaVista, we are actively building a framework for security:
a) In the underlying SW products, CGX and MVShield, we build tooling to support compliance and handle the required incident response requirements via our maintenance and support services.
b) We extend this solution via our MVSecure offering that allows customers to take advantage of MontaVista's Linux platform expertise to address specific customizations for their platforms.

The following is a very high-level illustration of our approach in practical terms:



Diving to the next level of detail, please see the following for an overview of the solution areas we offer:

1. Root-of-Trust and Platform Security:
    - Help implement secure boot mechanisms to ensure the integrity of the bootloader and kernel. Many of our CGX BSPs contain this as a standard, and for the others as well as customer's custom devices, we offer this as a service.
    - As a standard component in our CGX licenses we provide regular updates and patches to the Linux kernel and associated components to address known vulnerabilities (including CVEs).
    - CGX utilizes firewalls and other network security measures, such as SELinux, Linux integrity management, Snort intrusion detection etc as necessary to protect communication interfaces. Many of these features come as standard components in CGX, however, we always offer MVSecure services to custom configure these for customers.
2. Risk Assessment:
    - Via MVSecure, we can work with you to conduct a thorough risk assessment to identify potential security vulnerabilities and assess their impact on patient safety as well as define and implement security controls based on the risk assessment findings.
3. Software Development Life Cycle (SDLC):

- With our tools in CGX, the build tooling to maintain SBOMs and CVE scanning compliance built into CGX, we help integrate security into the entire software development life cycle, including design, coding, testing, and maintenance.
- We can work with the customer team to build a eLAB service, a MontaVista dedicated engineering platform management package, to maintain such a cycle completely for your platform.

4. Updates and Patching:
    - CGX contains tooling to establish a process for monitoring and applying Linux kernel and provide Over-the-air software updates promptly to address security vulnerabilities.
    - With our TUF-based NASA-validated framework, we help validate updates to ensure they do not adversely affect the functionality or safety of the medical device.
    - Together with MVSecure and the eLAB offering we can facilitate this process end-to-end for customers as necessary
5. Authentication and Authorization:
    - We can help customers using our MVSecure services and the tooling and functionality in CGX, like the root-of-trust components in (1), OpenSSL, PAM and others, to implement strong authentication mechanisms for device access, including user authentication and authorization controls.
    - Together we can ensure that only authorized individuals have access to critical functions and data.
6. Data Protection:
    - With encryption facilities like openssl, TPM-backed keys and dm-crypt partition encryption, we help implement encryption mechanisms to protect sensitive data stored on the device.
    - We allow secure data transmission protocols for communication between the medical device and other systems in the vast protocol support in CGX.
7. Quality Management System (QMS) Integration:
    - As a specific service via MVSecure, we can help customers even to take full ownership of the product platform creation and help integrate the use of embedded Linux into the overall Quality Management System (QMS) for the medical device at the customer.
    - MontaVista would in these projects ensure that processes related to software development, risk management, and quality assurance align with FDA regulatory requirements as it comes to the Linux platform allowing customers to focus on their value-add applications and the product design itself.
8. Incident Response:
    - Last but not least, we help to develop and maintain an incident response plan to address cybersecurity incidents promptly. We can help to build this via MVSecure, and the tooling that supports and maintains services with custom service-level agreements is a standard component of the CGX product.

We invite all interested parties to contact MontaVista via the means below, or via your local MontaVista contact.

Let’s build more secure embedded devices for the medical market together!

About MontaVista Software

MontaVista Software, LLC, is a leader in embedded Linux commercialization. For over 20 years, MontaVista has been helping embedded developers get the most out of open source by adding commercial quality, integration, hardware enablement, expert support, and the expert resources of the MontaVista development community. Because MontaVista customers enjoy

faster time-to-market, more competitive device functionality, and lower total cost, more devices have been deployed with MontaVista than with any other Linux.

For more information about MontaVista, visit http://www.mvista.com

Media Contact:

MontaVista Software LLC | E: pr-contact@mvista.com | T: +1 (669) 777-6841