WNDRVR

STRENGTHEN CYBERSECURITY IN MEDICAL DEVICE DEVELOPMENT WITH SIMULATION TECHNOLOGY

MEDICAL DEVICE CYBERSECURITY

The cybersecurity threat to medical devices is growing. That is why the U.S. FDA and international regulatory agencies have added regulations to strengthen the protection of medical device software and hardware from security risk.

The first weapon to lower medical device cybersecurity risk is defeating threats at the source — as the medical system software is being developed. Starting in the software development planning and process, a medical device developer can proactively counter the threat of cybersecurity problems through security vulnerability testing, known as penetration testing or pen testing, or through fault injection by the embedded engineering community.

PENETRATION TESTING

Wind River® cybersecurity experts stress that security vulnerability testing, or penetration testing, should be one of the first major weapons against cybersecurity threat. Pen testing should be implemented during the initial development of the device software, and its use can be continued throughout the lifecycle. Intel® Simics®, a full-system simulator used by software developers to simulate the hardware of devices and complex electronic systems, can be used to conduct cybersecurity pen testing.

A pen test simulates an attack on a system to detect known vulnerabilities. The developer uses a library of known cyberattacks or faults to drive an automated tool that injects each fault and analyzes the device-under-test (DUT) response. As new vulnerabilities are discovered, the developer team can add them to the library of cybersecurity threats and improve the pen-testing process. The use of pen testing is one of the best ways for medical device developers to mitigate cybersecurity risk, because it applies throughout a medical system's lifecycle: during development, deployment, and after each modification.

INTEL® SIMICS

- Simulate your target medical system, including processors, devices, full boards, and systems.
- Run the same software on Simics that runs on the physical target.
- Conduct penetration testing for security vulnerabilities.
- Simulate Arm®, Intel, and PowerPC target architectures.
- Create a virtual environment for DevSecOps for development of medical and other systems.
- Analyze and debug the full system as a unit.

View the Simics product overview for full information.

One highly effective way to deploy pen testing is via cybersecurity simulation, which exposes known and unknown vulnerabilities by putting medical device security defenses under evolving, real-world security threat settings. But because such testing runs on a virtual device, no unintentional interference or damage is caused. Simics and simulation engines enable medical device system developers to test system cybersecurity in a controlled environment. Simics decouples the development work from the physical medical hardware, while maintaining the ability to connect the physical device hardware if required. The Simics-created virtual hardware gives on-demand access to any target system, allowing continuous integration and automated testing by members of the device development team or by suppliers for the system.

SIMICS FOR CYBERSECURITY SIMULATION FOR A MEDICAL DEVICE SYSTEM

Simics full-system simulation enables medical device developers to detect cybersecurity threats to the medical device that can originate when one element attacks others. With this approach, developers can:

- Conduct tests that are impossible on physical medical hardware, such as spoofing malware to trigger responses and thus expose the threat's existence
- Test defense-in-depth strategies, such as flagging a suspect component as inoperable so it can be isolated from the medical system
- Have Simics act as a cybersecurity sandbox, safely containing suspect malware for forensic analysis

DEVELOP MEDICAL DEVICE SOFTWARE IN A VIRTUAL ENVIRONMENT WITH SIMICS

Beyond cybersecurity simulation, Simics can be a valuable technology for developing medical and other software in a virtual environment. Simics provides the access, automation, and collaboration required to enable DevSecOps and continuous development practices. As the complexity of developing medical devices and systems grows, Simics can help test by modeling complete networked systems and running a full production software stack of unmodified binaries, including binary input-output systems (BIOS), firmware, operating systems, and applications.

Simics supports multi-core and parallel core processing as well as the distribution of complex, multi-core simulations across available host resources. The capacity of the simulation host network is the only restriction on system complexity or its performance requirements. And with Simics, you can run code in reverse to isolate issues, fix them in place, and then test the fix immediately before committing the code.

Simics can offer a development and test environment even before you have hardware available, or when there are not enough test platforms for the entire team. This can represent a huge savings of time and cost on resource-squeezed projects. Additionally, given virtual environments, developers can change configurations, parameters, or test harnesses without worrying about any impact on the parallel efforts of teammates.

EXPLORE SIMICS FOR ALL SOFTWARE DEVELOPMENT

Simics can be utilized for product software development for all industries. By using virtual platforms and simulation, software developers can decouple their work from physical hardware and its limitations during development. To discover the full features and benefits of Simics for software development in a virtual environment, visit Simics.

WNDRVR