Medical device software under the microscope

Stephen Allen, Coverity

Stephen Allen

Technology plays an integral role in driving medical innovation forward. The past few years have seen an even larger increase in the advancement of software in medical devices. According to the Institute of Medicine (IOM), medical device manufacturers rely more than ever on the software to build new devices and to add new capabilities.[1]

More than 50% of existing medical devices depend on software in some form or another – the software is either embedded in the devices or plays an important role in the production of the device. Companies that lead the medical device market in innovation and efficiency rely heavily on software for new product lines and enhanced functionality.

As a result, the complexity of software in these devices has steadily increased. The benefits of software, however, come with the cost of risk of failure due to the presence of defects – there is typically a strong correlation between code complexity and the number of defects in the software. The safety-critical nature of medical devices requires that a variety of testing methods be employed to ensure that defects don't slip through development and end up risking the lives of those who use them.

Regulatory oversight

To ensure proper verification and validation of medical devices, a strong emphasis is placed on regulatory oversight and device approval before market release. However, in a recent report by the IOM titled 'Medical Devices and the Public's Health: The FDA 510(k) Clearance Process at 35 Years', the group evaluated the 510(k) process and recommended an overhaul of the approval process. Given the increasing use of software, the IOM committee reported on the increasing uncertainty introduced by device complexity as well as potentially unsafe interactions with other software systems and suggested that the Food & Drug


Administration (FDA), which is responsible for regulatory oversight on medical software development process and testing, review and update its guidance on software validation.

Device manufacturers met these suggested regulatory overhauls with concern. According to them, introducing new regulations on the industry would stifle innovation, increase costs, and slow down the process of bringing new and valuable devices to the market.

In the past, the FDA has done its part when it has recognised a need for introducing new guidelines or updating existing ones. For medical device software, the FDA introduced the guidelines in the form of General Principles of Software Validation (created in 1997, updated in 2002). Such guidelines serve to help the device manufacturers put in processes and take specific actions to validate the software that helps operate medical devices. Most recently, the FDA issued guidance for mobile medical applications after acknowledging the recent growth in the use of mobile device applications for improving and facilitating patient care.[2] These guidelines contain recommendations for software verification, defect prevention, software validation after changes to a code base, independent review and developer testing.

Software analysis

Device manufacturers take guidelines and modifications to existing approval processes very seriously and use tools such as static analysis to ensure their development process aligns with federal requirements. Since 2006, the use of static analysis to test code within traditional software verification and validation (V&V) processes has seen a dramatic rise. Modern static
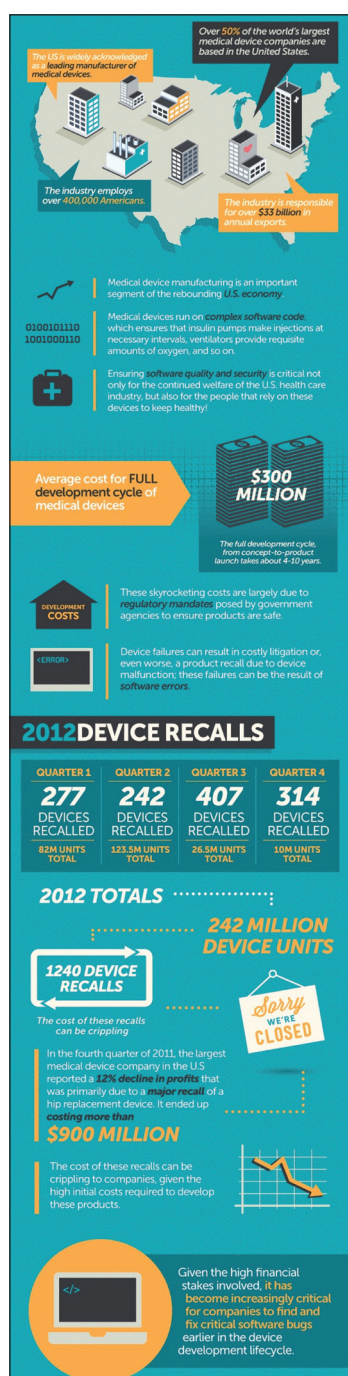
analysis can discover complex defects in the code by simulating every possible execution path of the program without the need to actually execute the code. Additionally, by focusing on 'run-time defects', new static analysis technologies evaluate more of the intricate interactions within code bases.

"A good Governance, Risk and Compliance (GRC) policy that builds on the strengths of automated code testing with static analysis can make medical devices safer and the development process more efficient"

A simple example of this is tracking the values of variables as they are manipulated down a path through the code or the relationship between how parameters of functions are treated and the corresponding return values. To analyse code with this additional level of sophistication, mature analysis solutions combine path flow analysis with inter-procedural analysis to evaluate what happens when the flow of control passes from one function to another within a given software system. The entire analysis is automated and does not require a substantial modification to the existing development process.

The use of static analysis has given rise to building long-term best practices in the software development process for medical software. A good Governance, Risk and Compliance (GRC) policy that builds on the strengths of automated code testing with static analysis can make medical devices safer and the development process more efficient. Such policies allow development organisations to define and test code against compliance and regulatory requirements to manage development risk throughout the development process. It also allows the organisation to be proactive, prescriptive, and in control of the quality and safety of the software and devices they produce.

Quality of life

It doesn't matter whether you're a consumer or a device manufacturer, software is essential for creating breakthrough devices that improve the quality of people's lives. However, risk of failure and complexity inherent in software are two challenges that medical device manufacturers must be prepared to tackle.

The rapid evolution of devices may even increase the importance of bug-free software not only to improve the devices' efficiency but also to reduce the security threats. The question of security is crucially important as more devices incorporate features that require connectivity for control, reporting and monitoring. *The Economist* talked about the possibility of reprogramming an implantable cardioverter defibrillator either to unexpectedly withdraw therapy or to produce unnecessary shocks.

The magazine also quoted Dr Fu, a computer science professor at the University of Massachusetts, who argued that, "Many manufacturers do not have the expertise or the willingness to utilise new tools being developed in computer science."

Fortunately, development testing solutions together with best practices are able to prevent security breaches and ensure the integrity of safety-critical code bases.

About the author

Stephen Allen is the vice president of EMEA operations at Coverity. He is responsible for driving the company's continued growth and overseeing all revenue-related field operations in the region. A seasoned sales executive with more than three decades of experience, Allen previously oversaw EMEA field operations for BEA Systems and took that company from a startup to more than $300m in annual revenue. He has also held senior international positions with Verint Systems (formerly Witness Systems), Walker Interactive Systems and SAP, among others.

References

1. Institute of Medicine. Home page. Accessed Feb 2014. www.iom.edu.
2. 'Mobile Medical Applications: Guidance for industry and Food and Drug Administration staff'. FDA, 25 Sep 2013. Accessed Feb 2014. www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm263366.pdf.

A vision for cloud security

Hongwen Zhang, Wedge Networks

Hongwen Zhang

Water is the stuff of life: nearly 60% of our bodyweight is made of water and the presence of water is the first thing astronomers look for when considering a habitable planet. Find a good source of clean water and you are established for life: ancient trade routes went from water source to water source, and cities grew up around those precious assets.
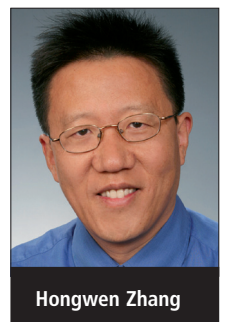
In cyberspace it is not water but information that flows to those nodes. But the same rule applies: deliver good information and business will flourish.

For the service provider the information comes from the cloud, just as water ultimately comes from the clouds, but is it as clean? How might a service provider

benefit if it could promise not just data, but pure data for its customers?

What's in it for the service provider?

Customer churn is one of service providers' biggest headaches. The annual churn rate in global mobile telecommunica-