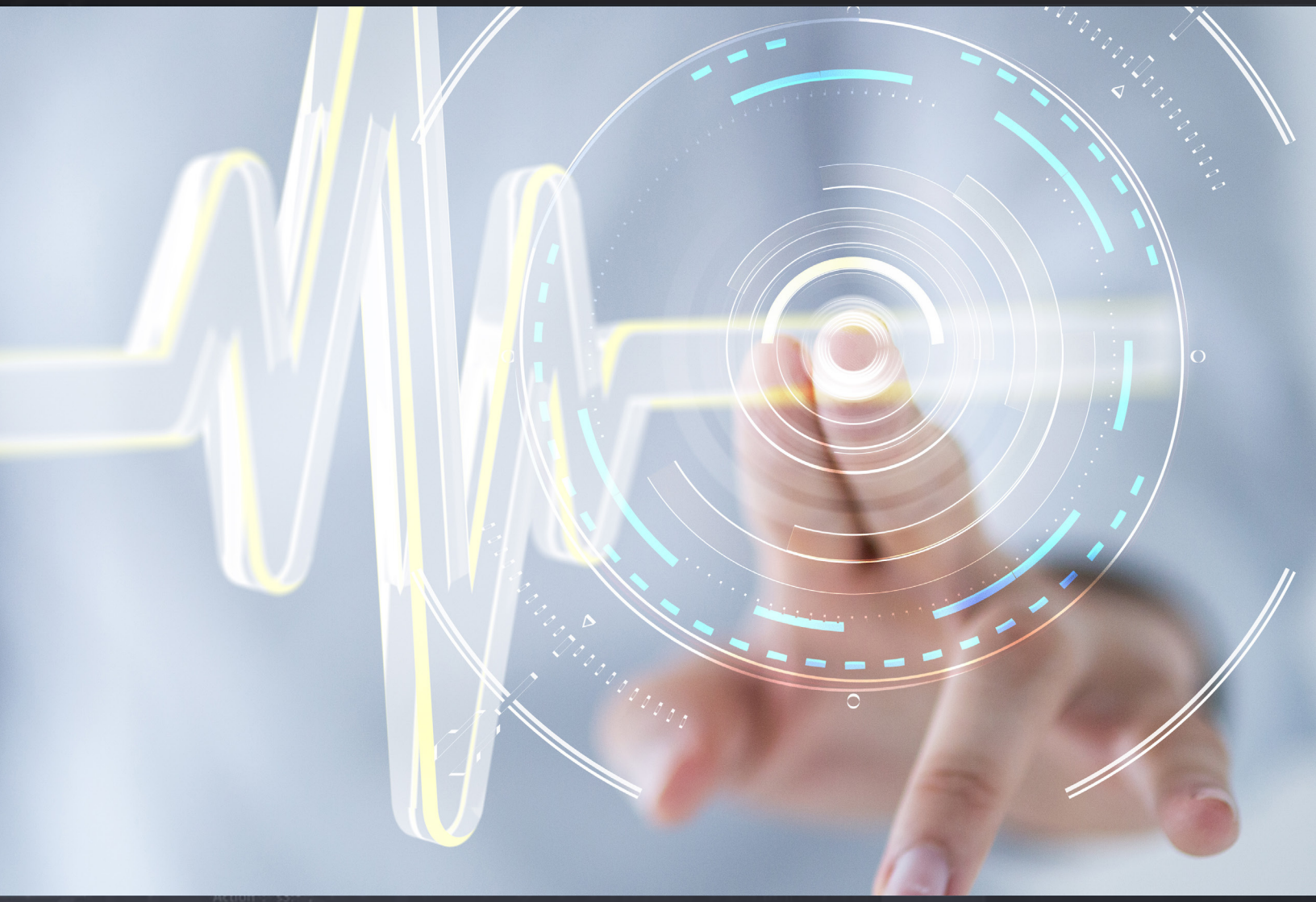
GRAMMATECH

NEW APPROACHES NEEDED FOR MEDICAL DEVICE SOFTWARE DEVELOPMENT



TRUSTED LEADERS OF SOFTWARE ASSURANCE AND ADVANCED CYBER-SECURITY SOLUTIONS

WWW.GRAMMATECH.COM

BACKGROUND

Modern medical devices are more complex than they used to be, and as the connectivity to the outside world via the Internet and the Cloud increases, so does the security challenge. Further, medical devices for home use are increasing exponentially, which means devices must withstand both non-clinical environments as well as use on insecure home networks.

As the security challenge increases, so does the impact on safety, risk, development cost, and liability. Use of third-party software, including operating systems, libraries, and legacy code is also a risky reality for all products. Managing this software supply chain and associated risk of using it in patient-critical systems is an increasingly critical part of medical device software development.

NEW CHALLENGES DRIVING NEW APPROACHES

COMPLEXITY AND CONNECTIVITY

Medical device software grows in complexity each year. This is a direct result of increased functionality, safety, and security requirements; connectivity of devices to networks and the internet; and consolidation of multiple functions into a single device. The expectation of each new generation of medical device is smarter, better, faster, cheaper, safer, and more secure than the previous generation. The recent market advances, specifically the growth of home health care, personal medical devices, and device connectivity to improve control, monitoring, and reporting, are beneficial to the market but mean that medical devices are exposed to more potential security threats than ever before.

SECURITY AS A NEW RISK FACTOR

As security has become an increasingly important consideration, the FDA has addressed this with the recent guidance on the topic. Security design, coding, and testing often fall outside the expertise of managers and developers in embedded software since it requires a unique set of skills. In addition, security is not top-of-mind when managing third-party code, including operating systems, libraries, and open source software. Evaluating these outside sources of software is time consuming and costly. (Automated tools such as static analysis can alleviate this.)

MULTICORE PLATFORMS

Multicore hardware platforms are a reality for medical devices and while they bring unprecedented power to performance ratios, software development on these new platforms introduces new complexities. New programming techniques are often required, as is more thorough debugging and performance testing. Secure and safe development on multicore is still a relatively new territory, which increases risk.

CLOUD AND INTERNET OF THINGS

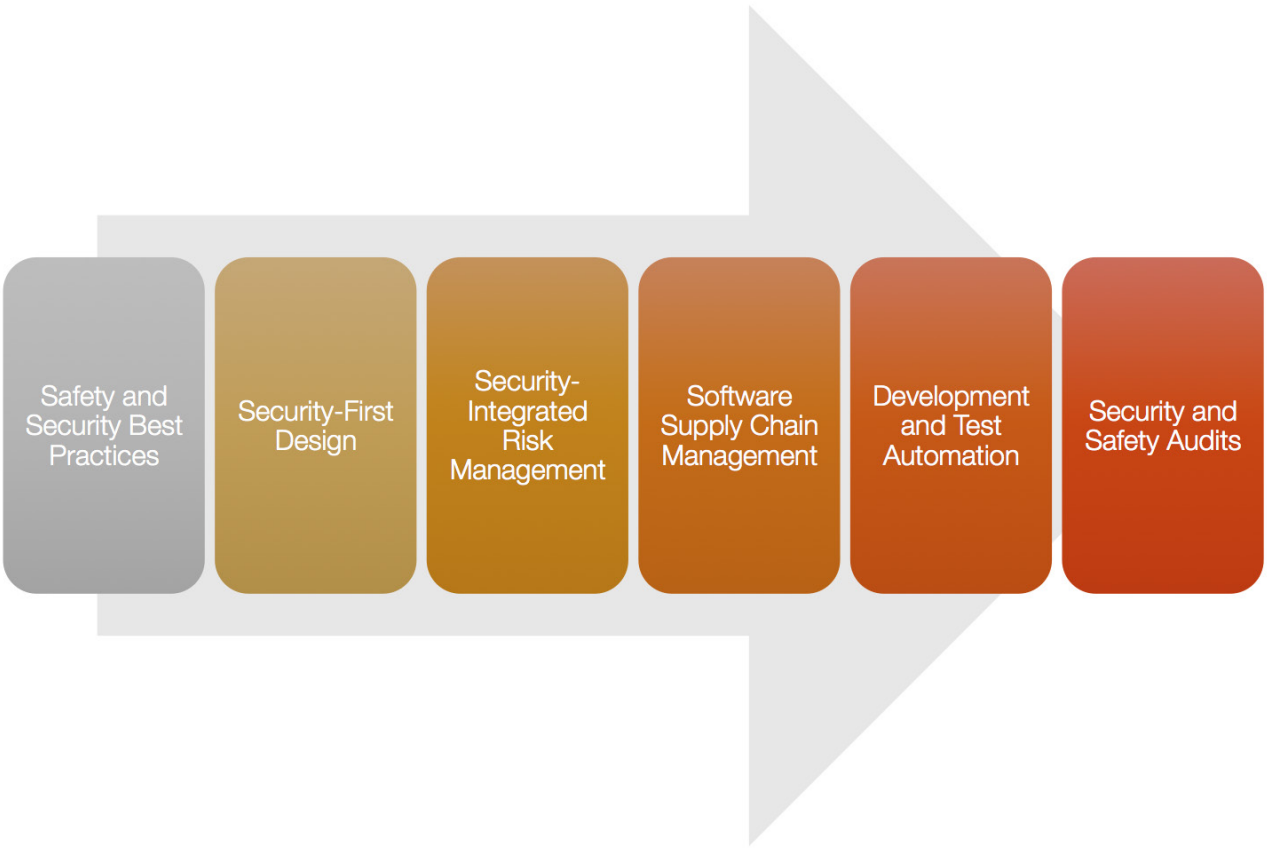
Medical device connectivity and the increasing use of cloud storage, analysis, and control

means increased functionality and outcomes for medical devices and non-clinical usage. The cloud and IoT raises privacy and security concerns that are relatively new to medical devices, and with it a new emphasis on the importance of security, something the FDA has recently addressed in its guidance on managing cybersecurity.

SOFTWARE SUPPLY CHAIN

Medical devices rely on third-party and in-house existing software to meet functionality, cost, and time-to-market concerns. Although software of unknown pedigree (SOUP) is a well-known concept and software supply chain risk management is already a reality in medical device software development, till recently risk management has often ignored the risk of third-party components, without sufficient technology to analyze and understand the impact of this software. Medical device software developers need improved development approaches, tools and techniques to overcome these challenges.

Of course, safety is the paramount concern, but security is becoming equally important, with cyber-attacks being able to jeopardize safety, among other possible dangers. With this increased risk from outside software sources, it's important to leverage technologies developed to analyze and fix vulnerabilities in software. Static analysis can now provide insight into third-party code, even in binary form, lending a great aid to supply chain risk management.



NEW APPROACHES

New approaches to medical device software development are required if current development can't keep pace with market challenges. The following approach can help lower risk and liability in the face of big changes in device development:

- **Training on and adoption of new software development, safety, and security best practices and guidelines:** Software development is evolving, as are techniques and methodology for developing security-critical and safety-critical devices. A long-term plan for the adoption of incremental and iterative development, risk management, and security best practices are beneficial, both in product quality and development productivity. Including software as part of supply chain management is critical, evaluating this software for safety, quality, and security.
- **Design with a security-first philosophy:** Treating security as a primary requirement alongside safety and functionality is crucial in developing secure medical devices. Security can't be just added on later – software security requirements evolve from detail threat analyses.
- **Combine risk management with security threat analysis and assessments:** As with treating security properly at all stages of development, security must be part of a medical device risk management plan. The scope of this assessment must include SOUP and other code from the supply chain. An insecure device is most likely not a safe device and a safety analysis can overlook security.
- **Management of the software supply chain:** Most projects require reuse or build upon open source or commercial products. Assessing the quality and security of SOUP and other code, internal or external to the company, in part with the aid of advanced static analysis, can reduce risk.
- **Integrate development and testing tool automation:** Software development tools are advancing along with new techniques and methodologies. Advanced static analysis tools such as GrammaTech CodeSonar play an important role in automating the detection of defects and security vulnerabilities. CodeSonar forms part of a modern tool chain that is critical in seizing the increased security, quality, and safety that new techniques and approaches offer.
- **Continuous security and safety audits:** Auditing software under development on a continuous basis and ensuring quality, security, and safety at all stages is critical to success. Ensuring that products meet the audit standard before shipping illustrates proper due diligence and risk management required for FDA pre-market approval, for example.

This list seems like a tall order to adopt in the short term; fortunately, it is a long-term recommendation. For an example of what to do now, starting with a basic security audit is a great way to understand your starting point.

BINARY CODE ANALYSIS

GrammaTech CodeSonar's binary analysis technology can evaluate object and library files for quality and security vulnerabilities. Binary analysis augments static source code analysis by detecting tool-chain induced errors and vulnerabilities. It can also be used to evaluate the correct use of library functions from the calling source into a binary object, making the combination of source and binary analysis a very powerful tool indeed.

Although the possibility of investigating and fixing the issues is often limited, it does provide a bellwether of the quality and security of the code. Customers of commercial off-the-shelf COTS products can go back to technical support of the vendor and ask for confirmation and analysis of the discovered vulnerabilities. Key here is that the impact on risk management is better understood. Software that has poor analysis results must be dealt with appropriately in the risk management plan.

CERTIFIED TOOLS AND TRUSTED VENDORS

GrammaTech has a long history of providing software tools to manufacturers of safety-critical products. GrammaTech CodeSonar is also a qualified tool under several safety-critical standards which, although not specifically called out for by the FDA for software development, does provide assurance that due diligence was carried out by the software vendor.

Confidence is required in an automated tools' results in order for them to be acceptable certification evidence such as in pre-market approval required by the FDA. Recognizing this need, GrammaTech CodeSonar is independently certified for use in development of safety-critical software for ISO 26262, IEC 61508, and EN 50128 standards. This certification signifies that developers can use the tools with confidence that the results produced are acceptable to approval bodies during certification.

COMPETITIVE ADVANTAGES

Although these new challenges facing modern medical devices might be overwhelming, the upside is that organizations that are aware of and able to succeed in this new environment will find a significant competitive advantage. Medical devices that support secure connectivity that protects user data is clearly preferred. Devices that exploit new hardware advancements while maintaining robust operation win out over devices with higher power consumption and bill of materials costs. Medical devices developed to up-to-date methodologies with due diligence in safety and security have much lower lifecycle costs over the competition. Overcoming these new challenges by leveraging new methods, new standards, and advanced tools can give your product the advantage it needs.

CONCLUSION

Medical device software developers need to deal with changing market challenges. Security has become a number one concern, but safety and adaptation to new market requirements remains important. Bringing in external source code and binary code has its risks, though, and proper management of risk in terms of safety and security is required in order to market the device. Combined with source-based static analysis, new binary code analysis technology provides a practical way to assess third-party binaries and libraries.

Adopting new strategies and approaches can help teams evolve their development process, including new tools and techniques to adapt to the changing marketplace. Companies that do this will best stand to reap the benefits of a fast-growing market.

GrammaTech, Inc. is a leading developer of software-assurance tools and advanced cybersecurity solutions. GrammaTech helps organizations develop and release high quality software, free of harmful defects that cause system failures, enable data breaches, and increase corporate liabilities in today's connected world. GrammaTech's CodeSonar is used by embedded developers worldwide.