CASE STUDY

In response to an alarming number of complaints, the FDA has announced more stringent safety requirements for new devices.

In addition to recommending static analysis tools to manufacturers, the FDA itself has been using GrammaTech's CodeSonar to investigate complaints and find out why medical devices fail in the field.

Federal Drug Administration (FDA) Recommends Static Analysis for Medical Devices

Recalls for medical devices are at an all time high, and defective software is one of the top causes. FDA data indicate that one in every three medical devices that use software for operation has been recalled due to failure in the software itself.

The FDA is now making medical device software quality a top priority, recommending better software development practices, including static analysis tools, to help manufacturers eliminate software defects during development.

Photo courtesty Daniel Rosenbaum/The NY Times/Redux

Prevalent Pump Problems

Infusion pumps are commonly used in patient care to deliver nutrients and medications into a patient's body in a controlled manner. In the last 5 years, the FDA has received over 10,000 complaints per year about these pumps. Device-related problems were responsible for a large number of serious injuries and more than 500 deaths. In that same time frame, manufacturers of infusion pumps issued 87 recalls, among the highest for any medical device.

Some pump manufacturers say that most problems occur when a nurse or health care worker enters incorrect data. However, FDA officials found that many deaths and injuries related to the devices were caused by product design and engineering flaws, rather than user error.

FDA Takes the Initiative

In response to this problem – one of the most widespread medical device recalls in recent history – the FDA introduced its Infusion Pump Improvement Initiative to establish requirements for pump manufacturers and proactively facilitate device improvements. With this aggressive and far-reaching initiative, the FDA is also driving the industry toward improved software development and verification practices. The Infusion Pump Improvement Initiative will eventually be broadened to cover other types of devices.

Currently, the FDA does not require third-party certification of source code for safety-critical software. The FDA requires only that manufacturers adhere to conventional development processes, and leaves validation and verification of

OTHER CUSTOMERS IN THE *MEDICAL DEVICE* INDUSTRY INCLUDE:

Boston Scientific
Bausch& Lomb
Cardinal Health
Covidien
Harvard Apparatus
HeartWare
Hologic
Philips Medical
VIASYS Healthcare
ZOLL Medical

"The purpose of software is to make the device safer and easier to use.

Users often do not realize the extent to which software determines many of the key functional and performance characteristics of the system until something goes wrong."

– FDA

software to the discretion of the manufacturer. In other words, there is no independent review required for software used in medical devices, and the FDA historically has not had the bandwidth to assess the quality of the code directly.

As a result, manufacturers have relied on system-level testing and code reviews for software verification and validation, but the run-time execution testing performed typically exercises only a small percentage of possible code paths. In the past, it was possible to augment the testing with a manual code review, which enabled the examination of significantly more paths; however, for the large code bases associated with modern medical devices, it is impossible to manually analyze the truly huge number of paths in the software. Traditional verification methods find some bugs but do not verify the reliability of the remaining code.

Exploring All Possible Paths

As part of its Infusion Pump Improvement Initiative, the FDA is encouraging manufacturers to use static code analysis. With static analysis, software problems are detected early in the device development process, and it is possible to examine all possible execution paths.

Static analysis examines a software application without actually executing the software. CodeSonar, GrammaTech's advanced static analysis tool, works very much like a compiler. It takes source code as input, which it then parses and converts to an intermediate representation (IR). Whereas a compiler would use the IR to generate object code, CodeSonar retains the IR, and uses the information to perform an abstract or symbolic execution of the program. During this execution, program variables containing

actual concrete values are replaced by corresponding symbolic values. The analysis proceeds by using these symbolic values to follow all possible paths through the code. Along each path, possible symbolic values are recorded. As this execution proceeds, the analysis may learn facts about the variables and how they relate to each other. It uses these facts to check for potential errors.

CodeSonar detects the most critical defect types and security vulnerabilities. These include run-time errors, such as buffer overruns, null pointer dereferences, race conditions, resource or memory leaks, and dangerous casts. CodeSonar also detects inconsistencies in the code that often indicate programmer misunderstandings, such as redundant conditions or erroneous assumptions. When a potential flaw is found in the software, CodeSonar generates a warning that allows the user to see not only where the flaw occurs, but the conditions that must hold in order for it to occur.

CodeSonar lends itself readily to verification and validation activities and can easily be incorporated as part of a manufacturer's software development processes. Doing so facilitates a deeper assessment of the code before releasing it to market and helps establish the conformance to good programming practices.

GRAMMATECH

For more information:
www.grammatech.com
Email: info@grammatech.com

GrammaTech Headquarters:
531 Esty Street
Ithaca, NY 14850

U.S. sales: 888-695-2668

International sales:
+1-607-273-7340

Email: sales@grammatech.com