Tools Ensure Reliability of Critical Software

NASA Technology

In November 2006, after attempting to make a routine maneuver, NASA's Mars Global Surveyor (MGS) reported unexpected errors. The onboard software switched to backup resources, and a 2-day lapse in communication took place between the spacecraft and Earth. When a signal was finally received, it indicated that MGS had entered safe mode, a state of restricted activity in which the computer awaits instructions from Earth. After more than 9 years of successful operation—gathering data and snapping pictures of Mars to characterize the planet's land and weather—communication between MGS and Earth suddenly stopped.

Months later, a report from NASA's internal review board found the spacecraft's battery failed due to an unfortunate sequence of events. Updates to the spacecraft's software, which had taken place months earlier, were written to the wrong memory address in the spacecraft's computer. In short, the mission ended because of a software defect.

Over the last decade, spacecraft have become increasingly reliant on software to carry out mission operations. In fact, the next mission to Mars, the Mars Science Laboratory, will rely on more software than all earlier missions to Mars combined. According to Gerard Holzmann, manager at the Laboratory for Reliable Software (LaRS) at NASA's Jet Propulsion Laboratory (JPL), even the fault protection systems on a spacecraft are mostly software-based. For reasons like these, well-functioning software is critical for NASA.

In the same year as the failure of MGS, Holzmann presented a new approach to critical software development to help reduce risk and provide consistency. He proposed "The Power of 10: Rules for Developing Safety-Critical Code," which is a small set of rules that can easily be remembered, clearly relate to risk, and allow compliance to be verified. The reaction at JPL was positive, and developers in the private sector embraced Holzmann's ideas.

JPL's Laboratory for Reliable Software (LaRS) works to ensure the reliability of spacecraft software and prevent failures like the one that cut short the operations of the Mars Global Surveyor (pictured here). For a deeper look at LaRS, scan this code.

Partnership

To demonstrate the feasibility of using a tool to automatically check software for compliance with Holzmann's rules, JPL awarded Small Business Innovation Research (SBIR) funding to GrammaTech Inc. of Ithaca, New York. The software development company adapted its existing software code analysis product, CodeSonar, to include verification of The Power of 10. Michael McDougall, a senior scientist at GrammaTech, says, "JPL was already using CodeSonar to check its software; however, there are things that might be acceptable in a desktop application that are unacceptable in an environment like on Mars or the Moon. CodeSonar didn't have rules specifically crafted for this type of critical software." After successfully adapting CodeSonar to check for the NASA-derived rules, GrammaTech transitioned the changes into its commercial version of the product in 2008.

Benefits

As a static analysis tool, CodeSonar finds problems in software without executing any part of the program. The tool produces a list of potential violations, including complex programming bugs that can result in system crashes and memory corruption. Compared to traditional software testing methods, CodeSonar checks more code in less time and saves time and expense by finding problems before the software is completed and distributed to users.

The design of CodeSonar allows users to configure how thoroughly it performs a check. The tool can warn about every potential issue, only critical violations, or a combination of both. McDougall explains, "Depending on the application, the software may not need to be as reliable as a Mars rover, but it can still be troublesome if it crashes at the wrong time. Users can choose the level of compliance that suits their context."

Today, CodeSonar has hundreds of users worldwide, including Fortune 500 companies, startup businesses, educational institutions, and government agencies working on satellites, avionics, industrial controls, medical devices, wireless devices, networking equipment, and consumer electronics.

In response to a widespread medical device recall, the U.S. Food and Drug Administration (FDA) started encouraging manufacturers of infusion pumps to utilize static code analysis tools like CodeSonar to check the pumps' software. Commonly used to deliver fluids into a patient's body, infusion pumps have been responsible for a number of deaths and injuries since 2005. In one instance, investigators at the FDA used CodeSonar to help determine the root cause of malfunction in a widely-deployed, commercial infusion pump.

Cell phone developers like LG Electronics Inc., Samsung, and Panasonic are also using CodeSonar. McDougall explains, "Cell phones are expected to function 24 hours a day, 7 days a week. The software that runs the internal cell phone, changes what is on the screen, and manages the address book, all has to be very reliable. Users do not want to have to reboot or install updates in the middle of a phone call."

Items as varied as infusion pumps, cell phones, and aircraft components are made using CodeSonar, a product from GrammaTech Inc. that incorporates rules developed at the Jet Propulsion Laboratory, to quickly find problems in the products' software.

GE Aviation, a provider of jet engines and components, as well as avionics, electric power, and mechanical systems for aircraft, uses CodeSonar to ensure the software in aircraft functions properly. "Software is an important part of engine design, and a lot of how planes work is controlled by software. You want it to be perfect—or as close to perfect as possible," says McDougall.

With public and private entities employing CodeSonar, Holzmann is hopeful that more organizations will be inspired to improve software development practice. "If the technology continues to be adopted, we will have made a contribution to making the computer systems we rely on safer and more reliable," he says.

Since developing The Power of 10, Holzmann has devised a single coding standard called the JPL Institutional Coding Standard for the Development of Flight Software. McDougall expects the standard will be incorporated in the next commercial version of CodeSonar. ❖

CodeSonar® is a registered trademark of GrammaTech Inc.