

The original URL of this page is:

<http://www.tmcnet.com/voip/1009/a-matter-of-integrity-tools-that-deliver-software-assurance-go-mainstream.htm>

---



[ADVERTISE WITH US](#) | [TMCNET HOME](#) | [PAST ISSUES](#)

October 2009 | Volume 12 / Number 10

Feature Story

[Internet Telephony Magazine Table of Contents](#)

# A Matter of Integrity: Tools That Deliver Software Assurance Go Mainstream

By: Paula Bernier



The failure of the levees in New Orleans and the collapse of the I-35W bridge in Minneapolis gave many of us a greater appreciation for the importance of ensuring vital infrastructure is sound. Businesses and organizations would do well to apply these lessons to the area of software development. And many already have.

Software that hasn't been thoroughly vetted can result in lapses in safety and security, customer-affecting performance issues and lost revenue – some of the most catastrophic problems a business can face.

Case in point: A major telephone company recently was working with a supplier to implement a new CRM software revision for its FTTx network and, as one Internet Telephony source who asked not to be named put it: “All hell broke loose.” The CRM system was tied to the telco's order entry system, and the new software release resulted in lost orders. So the service provider had to revert to the prior software revision. This little fly in the ointment cost the service provider a lost day or two in production and a whopping \$60 million in revenue.

This example focuses on telecommunications, but it could just as easily have been about a company in

finance, retail, health care or any other vertical. According to industry research, global businesses' critical systems go down 30 times a year on average, although not all outages are recognizable to the outside world.

Organizations of all stripes can significantly lessen the likelihood of this kind of problem by making a concerted effort to locate and address weaknesses in their code, whether that code is destined to be used in air traffic control applications, manufacturing systems, wireless handsets, financial tracking tools or whatever.

But looking for holes in software code is a manually intensive process, which can require significant expense and human resources. According to Lev Lesokhin, vice president of worldwide marketing for CAST Software, it's generally as expensive to fix software development problems as it is to create the applications in the first place. He adds that CAST Software's experience has shown that 30 to 50 percent of most software budgets are spent on rework – that is, fixing the errors made during development.

The good news is that tools from companies like CAST, Coverity and Klocwork now make it relatively simple to check for software integrity in a more cost-effective and less work-intensive way.

## The Time is Now

Static software integrity tools have been around for many years, but in their earlier iterations were very complicated solutions that perhaps only one developer within an organization would have the expertise to use, says Dave Peterson, chief marketing officer at Coverity, a privately held company headquartered in San Francisco, which more than 100,000 developers and 600 companies use to help them ensure the delivery of high integrity software.

### **100% Free Network Management Software and Helpdesk Tools**

Download a completely free network management software solution for IT pros. Spiceworks provides several tools and functionality to help simplify IT such as: network monitoring, help desk, virtualization management, warranty tracking, SQL server monitoring, network inventory & PC troubleshooting tools, and more. [Download Now.](#)

“People were aware of [software integrity], but they just didn't believe it was something they could use in their day to day,” says Peterson. That has changed, he continues, as today Coverity offers tools that allow any developer in an organization of any size to check for software integrity.

Gwyn Fisher, CTO of Klocwork, adds that the sale of software integrity tools has gone from a market push to a customer pull.

“It's getting further and further entrenched in the zeitgeist of technology,” says Fisher of Klocwork, whose software is used by more than 500 customers to enable risk assessment and fast critical-bug fixing in mission-critical C, C++ and Java software. That, he adds, makes software development more an engineering effort than an art form.

Klocwork and some of its competitor work closely with leading academic institutions, so more graduates are going into the workplace with an understanding about the availability and benefits of software integrity products and practices, Fisher continues.

For many organizations, ensuring software integrity is less a choice than an imperative. For example, Klocwork's Fisher says the Federal Aviation Administration has a requirement known as DO178B, which looks at reliability of any software going airborne – whether it's used in a system to make coffee

or to help with a safe landing. The Food and Drug Administration, meanwhile, has issued statements discussing the need for software integrity in medical devices, says Fisher, adding that right now those are just strong suggestions, but that FDA requirements in this area are expected in the near future.

## **Jenga! Jenga!**

Of course, software integrity tools differ, but the basic idea is to give developers a way to analyze source code to find specific violations and get metrics to detect stability and risks, says CAST's Lesokhin.

"It's almost like looking at a bridge to look at where cracks are that could make the bridge fall," Lesokhin explains.

## **The Coverity Lineup**

All of Coverity's products, which include four key modules, fall under the umbrella of what the company calls the Coverity Integrity Center. Here's what that includes:

### **Architecture Analysis**

This involves analysis of software design to ensure it can be easily modified and reused for maximum business agility. It uses architectural visualization to identify hidden security backdoors in code that cause costly breaches and data loss. And it maintains application structure across multiple iterations.

### **Build Analysis**

This option does analysis of software builds to identify problems and inefficiencies in the assembly of software that are the source of costly product delays. It ensures all the components in final applications are up to date, and verifies that any open source components used are documented for compliance and free of known security vulnerabilities.

### **Dynamic Analysis**

This tool does analysis of applications as they execute in test environments to amplify existing testing efforts. It is designed to make even the most complex multi-threaded software meet stringent performance requirements by eliminating hard-to-find concurrency defects and other crash causing software problems that corrupt software behavior.

### **Static Analysis**

This module helps users analyze source code for defects with Coverity Prevent to find and eliminate the root-cause of product delays or costly product recalls. It exposes security flaws early in the lifecycle so security audit teams don't slow down efforts with rework. And it helps the teams generally improve the quality of their code early in the application lifecycle.

That's especially important in the area of IT, he adds, because rather than doing software development

for a specific product like a mobile handset or a vehicle, IT departments are always under the gun and making adjustments and upgrades on a variety of fronts.

“It’s like a Jenga tower, you’re always building on top of the existing tower until it falls and you have to start a new one,” Lesokhin says. “And people hate that because it costs millions of dollars.”

The importance of ensuring software integrity has become even more important in the past decade, he continues, because that’s when outsourcing development migrated offshore. And, according to Lesokhim, offshore IT talent is “still developing.”

In fact, some big telcos’ contracts with offshore programming houses specify that the work they deliver must pass the test of CAST’s Application Intelligence Platform. Until they deliver code that passes the test, they don’t get paid. This helps the telcos make sure that they’re getting what they pay for, and that they’re not putting flawed software into production. And it makes offshoring as practical as it is inexpensive, according to CAST, which provides development tools for such telecom giants as AT&T, France Telecom and T-Systems.

## Ready to Launch

Regardless of where the code in question is developed, however, the use of integrity tools can accelerate software’s time to market by 15 percent, enabling companies to launch new products and capabilities much more quickly and reliability than previously possible, says Tom Schultz, Coverity’s director of products.

When a potential customer comes to Coverity, the company typically begins the relationship by performing a trial on some code provided by that customer so it can analyze the software and point out the problems. Customers that sign on with Coverity receive software integrity software through a term-based license – usually a year – which they can run a server on the desktop.

While Coverity’s model is based on licensing, the company will offer software integrity assurance as a service in special cases, says Schultz. He adds that the company operates the Coverity Scan Initiative (<http://scan.coverity.com/>), started on the behalf of the Department of Homeland Security in 2006, to analyze open source code for defects.

Next on the agenda for Coverity is the introduction of a new solution that not only allows customers to find defects in their code, but also connects those defects with the actual products, services or systems to which they are related.

“It’s one thing to have problems, it’s another thing to know how it’s going to affect your business,” says Peterson of Coverity, which expects to launch this new capability in November. **IT**

» [Internet Telephony Magazine Table of Contents](#)

Copyright 2010 Technology Marketing Corporation (TMC) - All rights reserved