Andy Chou on ASQA: Automated Software Quality Assurance Really Matters (2)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT


3) What's your elevator speech to sum up the advantages of ASQA?

Software should work: it shouldn’t fail. There are horrible stories on software failures [MK adds that the RISKS FORUM DIGEST<http://catless.ncl.ac.uk/risks> is full of those stories] and many don’t get publicity. The costs are high – a 2002 by NIST showed that $60B per year was being lost due to software failures at the start of this decade,<http://www.computerworld.com/s/article/72245/Study_Buggy_software_costs_users_vendors_nearly_60B_annually> “with more than half of the cost borne by end users and the remainder by developers and vendors….”

Automated software quality testing has potentially fuller coverage, and you find defects as early as possible, as soon as they are introduced into the code. The earlier they’re found, the cheaper it is to fix them – you save time and money. You also reduce the risk of critical defects making it into shipped products, and there is a greater chance that your product is safe, secure and working the way you want it to.

People expect systems to work and they get upset when software fails. Automated software integrity analysis increases reliability and it helps users trust the systems they’re working with. Businesses have to ask themselves, can you deliver the same reliability, the same value, to your customers without software integrity?

4) How do you identify the organizations and projects that benefit most from implementing ASQA?

Companies that benefit the most from automated software integrity include:

- Companies that make **safety-critical** systems that operate in aircraft, automobiles and transportation systems, medical devices, etc
- Companies that make **mission-critical** systems such as aerospace and defense, energy infrastructure, communications
- Companies that make **business-critical** systems such as software products, mobile and consumer electronics, online banking systems, etc

Any company with a large amount of software or a large-scale software development organization can benefit from automated software integrity analysis. Large code bases are complex and tough to manage. No single person can understand these software systems.
Automated software integrity can control that complexity and manage the risk.

5) As you think about the many cases of implementation of ASQA you have been involved in, does one come to mind as the quintessential demonstration of the ASQA value proposition?

A recent example comes to mind. Frequentis<http://www.frequentis.com/>, an international supplier of communications and information solutions for safety-critical applications, recently standardized on Coverity static analysis technology as an added layer of software quality to its already rigorous development process. Frequentis’ solutions are deployed in mission-critical fields, such as civil air traffic management, defense, public safety, public transport and maritime, where safety can’t be compromised. You can read about their implementation in a published case study.<http://www.coverity.com/library/pdf/frequentis_case_study.pdf>

Another great example has been our ongoing work with the U.S. Department of Homeland Security (DHS) – the Coverity Scan Open Source Report.<http://scan.coverity.com/> Since 2006, we’ve analyzed over 11 billion lines of code from 280 open-source projects as part of the largest public-private sector research project focused on open source software integrity.

Why is this a good demonstration of the value of automated integrity testing? Because automated testing was really the only way the DHS could analyze such a large proportion of open-source code. Hiring people to do it manually would be exorbitantly expensive and largely ineffective.

We’ve also helped to scan the code that went into the Mars Rover<http://marsrover.nasa.gov/home/> – when that guy ships, nobody is going on-site for software fixes!

The last part of this interview will be published in the next column.

* * *

Andy Chou<http://coverity.com/html/about_leadership.html>, PhD is co-founder and Chief Scientist of Coverity, Inc.<http://coverity.com/html/about_fact.html> He is responsible for advancing source code analysis technology at Coverity as well as furthering the state of the art in software integrity industry-wide.


Copyright © 2010 Andy Chou & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.