

Coverity White Paper

Managing Risk: Ensure Software Quality and Security Across the Automotive Supply Chain

January 2012

Managing Risk: Ensure Software Quality and Security Across the Automotive Supply Chain

The Automotive industry is undergoing a radical transformation. There's been tremendous industry consolidation due to the recent economic slump. The OEMs and suppliers emerging from this period are increasingly turning to complex software for differentiation and to spur new sales. In fact, the average car is expected to contain 300 million lines of code in the next decade, up from 10 million lines of code in today's cars¹. Software and electronics are expected to account for 90% of automobile innovation. With the exponential growth of software comes a dramatic increase in software defects. The average car is expected to contain up to 150,000 bugs², many of which could damage the brand, hurt customer satisfaction, and in most extreme cases, lead to a catastrophic failure.

The Smartphone On Wheels

Consumers are increasingly demanding that their vehicles are connected to their computers, mobile phones, work and homes. To meet this demand and reenergize new vehicle sales, OEMs and suppliers are trying to capitalize on this trend by investing in sophisticated in-vehicle infotainment systems (IVI). According to a recent report,³ 35 million IVI systems are expected to ship in 2015. And because of wide consumer acceptance, the smartphone is expected to be the preliminary source of infotainment and connectivity prompting some to liken newer cars to a "smartphone on wheels." Leading IVI systems such as Ford's Synch are comprised of components delivered from multiple suppliers that provide connectivity, media playback, climate control and navigation. A single IVI solution may be comprised of components from 10 to 20 ISV suppliers. Ensuring the quality of each of the individual components and the aggregated solution can be extremely difficult and time consuming which can put project schedules at risk and threaten the OEM's brand as well as damage supplier relationships.

The Evolution of Infotainment and Telematics

As OEMs deploy more sophisticated IVI systems in their vehicles, there are growing concerns over driver distraction. The National Highway Transportation Safety Authority (NHTSA) estimates that distracted driving accounts for nearly 30% of all accidents today⁴ and is calling for a ban on cell phone use while driving to try to reduce the risks. The auto industry's response to the risk created by their infotainment innovations has been to create software in their Telematics units to help mitigate the risks of distracted driving. Top automotive suppliers are creating sophisticated active safety systems that utilize radar to identify vehicles on the road that may be on a collision course and adjust the steering wheel to avoid collision, and software is being utilized to maintain a safe distance from other cars on the road, adjust headlights and determine if drivers are drowsy and then sound an alarm to awaken them.

And it's not driver distraction issues that are creating the explosive growth in Telematics software. Since the 1960s, OEMs have been replacing the mechanical systems with software-controlled subsystems including transmission control, body control, starter and power generation systems and more. With the increasing popularity of hybrid vehicles and the rise of electric vehicles, the rapid growth of software innovation is expected to continue. The Chevy Volt contains 10 million lines of code and over 100 electronic controls and there is little doubt that those numbers are only going to grow as OEMs find themselves in a virtual arms race for innovation.

Software in the Headlines

While software innovation is grabbing attention at Consumer Electronics Show (CES), it's also making headline news when things go wrong:

Nissan issued a service bulletin for 5,300 of its new battery-powered Nissan Leaf vehicles to correct a software problem that would keep some of them from restarting after an air conditioner sensor was activated and the vehicle turned off.

- Jaguar recalled 17,500 cars due to software glitch. A problem with engine management control software meant drivers had to turn off the ignition to disengage cruise control.
- University researchers released a report documenting how they could hack into a vehicle's Telematics unit and create an exploit that would allow them to reprogram all of the other computers in the car including locking individual brakes and disabling all interior and exterior lights.⁵

The Strain on Resources

With the increasing reliance on software and growing complexity of software supply chains, the focus on quality and now security has never been more important. Traditional approaches to dealing with quality are no longer sufficient. And most OEMs and suppliers are not accustomed to addressing software security but the security vulnerabilities can have a direct impact on the functional safety of the vehicle. Traditional approaches to testing typically look for expected behavior; does the component do what it was intended to do. It doesn't enable organizations to test for the unexpected: behavior that may only exhibit itself in specific circumstances. Plus, the later software bugs are found in the lifecycle, the longer and more expensive and time consuming they are to address. OEMs and suppliers are operating with such slim margins, tight resources, and immovable deadlines that they cannot afford to waste any resources or time yet the need to manage liability and warranty risk has never been more acute. According to a recent study conducted by Forrester on behalf of Coverity, the biggest impacts of finding defects later in the lifecycle include:

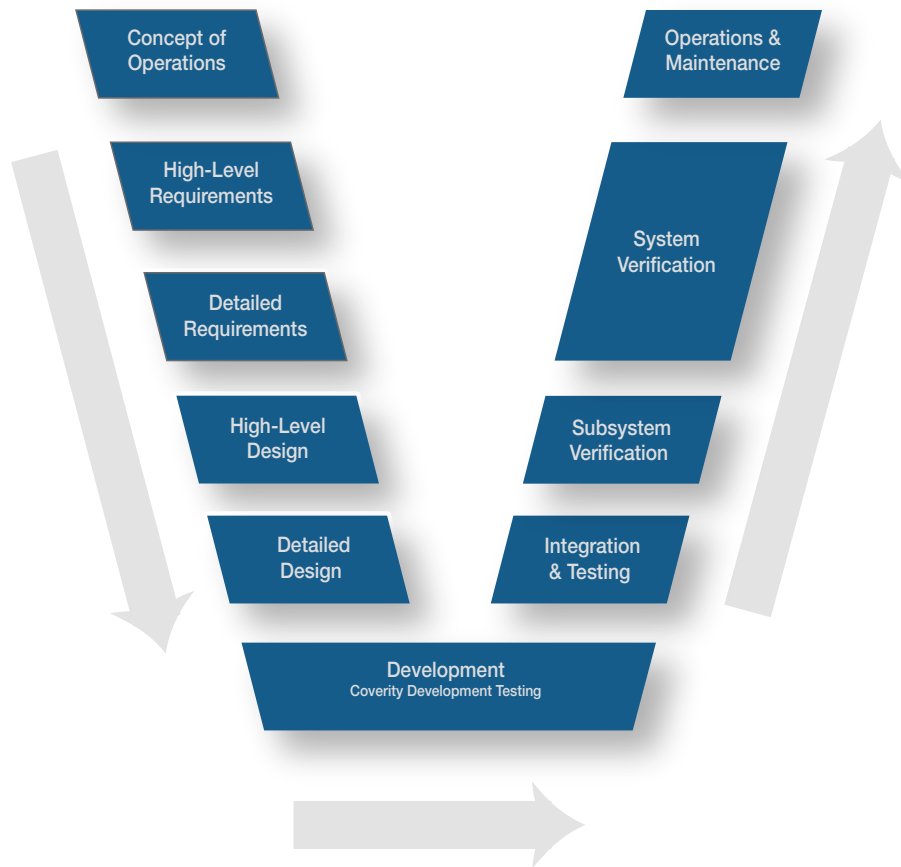
- Increased costs (77% of respondents)
- Delays in time to market/project release schedule (35%)
- Negatively impacted developer productivity (28%)

Reducing Liability Across the Supply Chain:

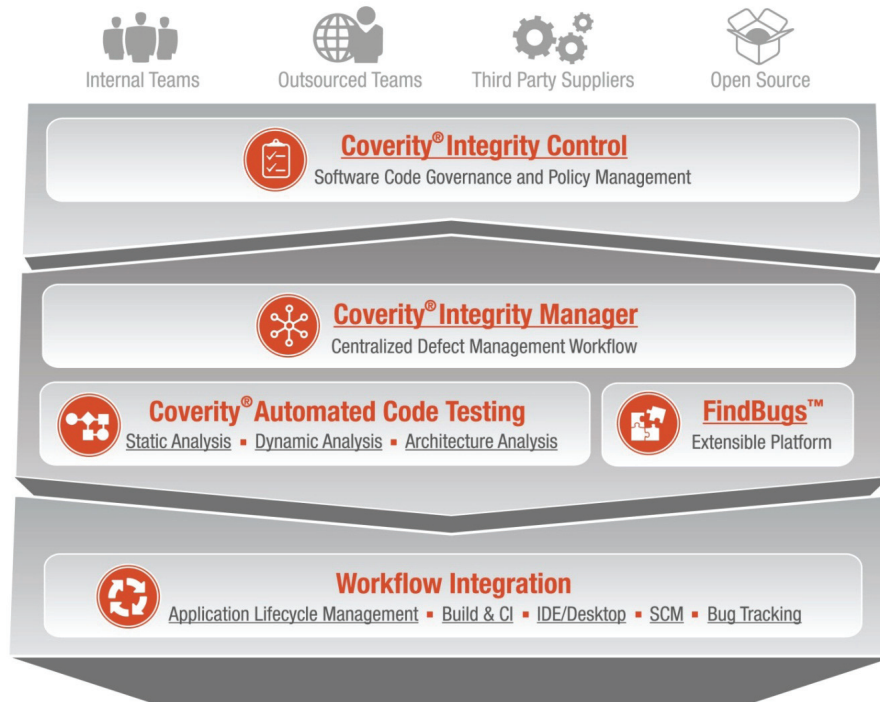
With the growing complexity of software components and supply chain, visibility into quality and security has never been more important. OEMs must ensure their brand is protected as every drop in brand equity could result in millions of dollars in lost revenue and Tier 1 suppliers must limit their liability exposure. A recall can cost up to \$500 per vehicle on average. One recent high profile recall was estimated to cost 2 billion dollars.⁶ OEMs and suppliers alike must have better visibility and control over the quality of all of the software in IVI and Telematics systems alike.

Coverity Development Testing Platform

Coverity development testing is used by some of the world's leading OEMs, Tier-1 suppliers, Integration partners, OS, Silicon, and ISV vendors to Suppliers, and Automotive suppliers during the integration and coding phase of the v-model to help effectively manage the quality, security, and complexity of code—and the efficiency of the teams that develop it.



By setting standard software development policies, based on OEM or supplier requirements, automatically testing code in development against those policies, and controlling internal teams, outsourced teams, projects, and third party suppliers against common and defined metrics development organizations gain visibility and early warning of risks across their complex software supply chain.



Defining Software Policies and Thresholds

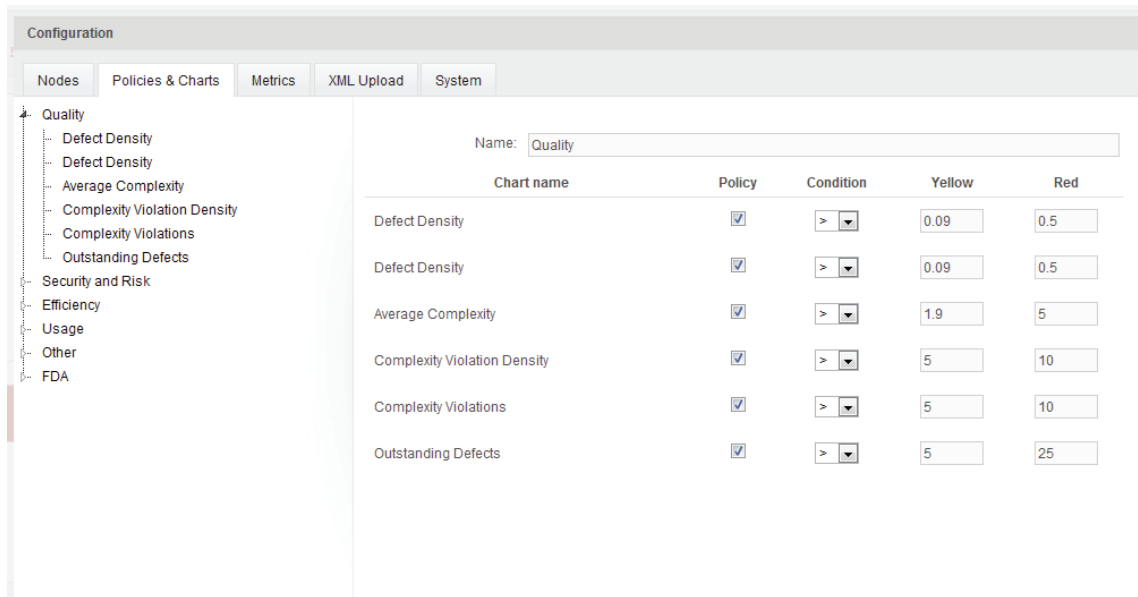
Coverity® Integrity Control lets you centrally define your software quality and security acceptance criteria as configurable policies. Once defined, the policies are centrally published and then shared with geographically dispersed internal teams and with external software suppliers. Specific policies which can be defined include:

Quality policies: You can set policies for defect density, critical defects and uninspected defects. Defect density represents the number of outstanding high or medium-risk defects per 1,000 lines of code. Critical defect policies can be established as well as thresholds for uninspected defects since these defects could represent a risk to the overall code quality.

Security policies: You can establish and enforce policies for defects identified as security risks by the industry standard Common Weakness Enumeration (CWE), and establish policies for security defect density.

R&D productivity: You can establish policies for your internal teams and third-party suppliers for critical metrics tied to R&D efficiency. Key automotive standards such as ISO 26262 specifically address the need to avoid excess complexity in code. Comments are also particularly important when taking delivery of code from a third-party or if you have a large development department with high attrition rates. You can manage complexity inherited from suppliers by establishing thresholds for acceptable comment density levels and cyclomatic complexity which measures the number of linearly independent paths through a program's source code.

Usage and savings policies: You can establish policies around the usage of Coverity® Static Analysis and Coverity® Dynamic Analysis. Policies can be established for the number of active users, projects and lines of code being scanned. This can be critical in enforcing code quality and security across your organization and supply chain.



Set standard thresholds, SLAs and policies

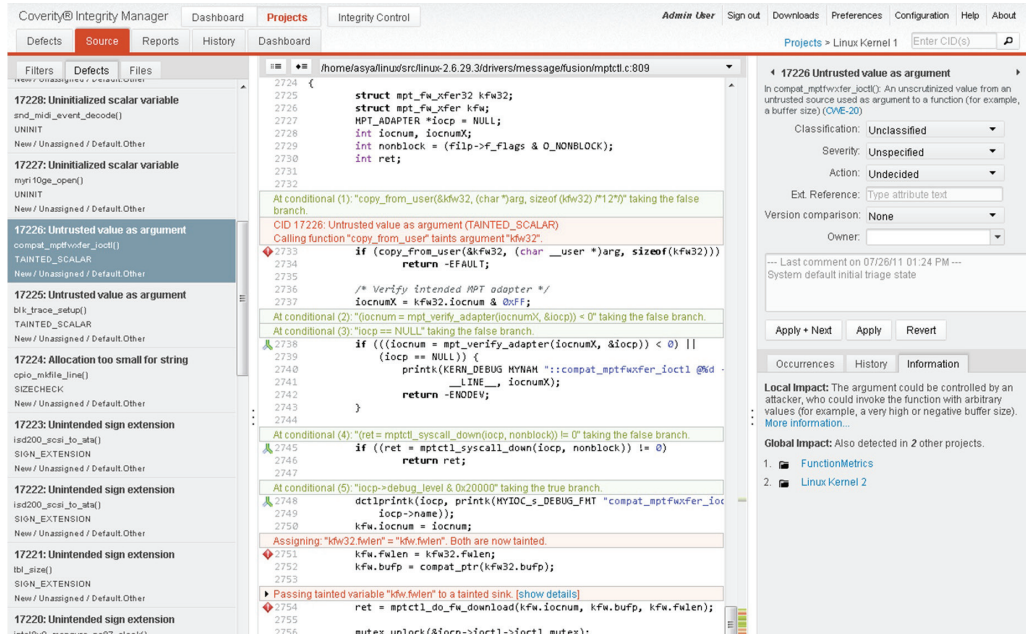
Testing Often and Early

Coverity development testing solutions enable you to test against established policies while the code is still in development, and where issues are least expensive and time consuming to fix. Coverity Static Analysis uses sophisticated algorithms to identify and triage high risk defects in C/C++, Java and C# code bases that could result in software crashes, security breaches, or safety issues. It enables you to find hard-to-spot issues such as null reference pointers, memory leaks, and potentially exploitable security flaws in the largest, most complex codebases. Once defects are found, your developers are automatically notified of defects within their existing workflow, prioritized by risk and impact, so they know which problems to fix first. They have access to a rich defect knowledge base, along with source code navigation to show them exactly where the defect exists in the code and guidance on how to fix it.

Fixing Defects Across Code Branches

Because many organizations create a common platform servicing multiple OEMs, the ability to quickly find defects in shared code and across all code branches is critical. Coverity enables the development team to quickly find defects and then shows all of the places that particular defect exists across multiple code branches. Developers can then quickly fix all occurrences saving valuable time and resources.

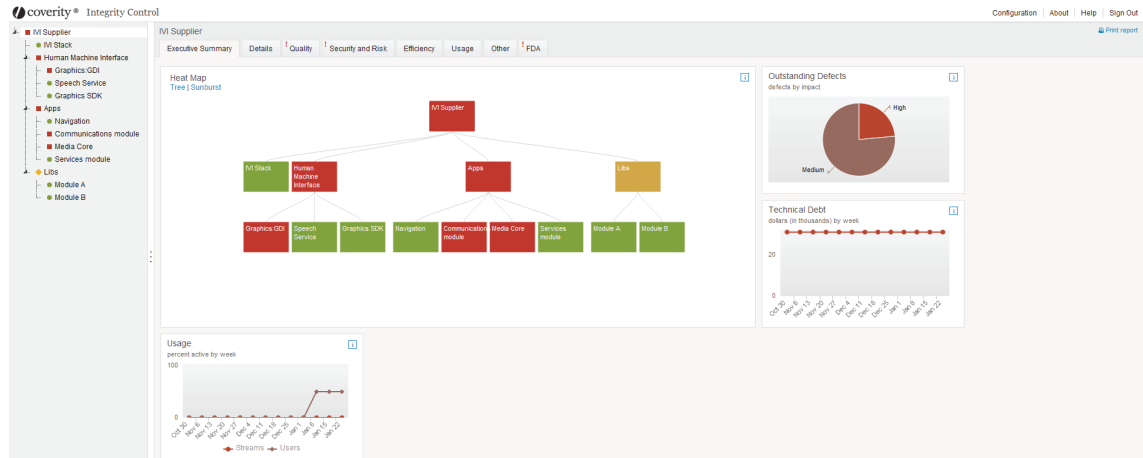
Because Coverity solutions are designed with developers in mind, Coverity’s testing platform fits within existing development workflows, enabling developers to quickly identify quality, security and safety defects from within their IDE at their desktop, or as part of the continuous or central build system.



Test for quality defects and security vulnerabilities in development

Controlling Risk and Liability


Once you have established your quality and security policies and tested against them, it is critical to have visibility into the risk across all of your teams and suppliers. Coverity Integrity Control provides you with a visual representation of the areas of risk across your projects and teams. As a Development Manager or an Application Owner, you can view a hierarchical heat map that is tailored specifically to the needs of your organization. You can track distributed teams to ensure they are executing consistently and will be able to quickly address any potential areas of risk and skills gaps. You are also able to track by product portfolio or by project component delivered from each team. Coverity Integrity Control provides the visibility and control needed to consistently measure internal teams as well as suppliers against the same standards for quality and security – with the ability to audit SLA violations on-demand. You can drill down into each policy to pinpoint the full context of the code problem, identify the specific policy in violation and where it originated. An updated risk profile is produced with every code iteration and test.



Executive-level visibility into areas of risk

In addition, you can easily notify teams and third-party code suppliers of code governance violations by sending them a Coverity Software Integrity Report summarizing the high risk defects that exist in their software, or violations from established policies. Once developers and suppliers receive the automatic notifications, they can quickly begin the triage or inspection process to fix new defects. This can also be used to help with internal audits as part of the compliance process.

Integrity Control is a powerful software governance solution. It enables organizations to establish a baseline for quality and drive continuous improvement from that baseline for internal and external teams. It also allows managers to quickly identify teams that need additional skills development, which will be increasingly important as automotive companies are expected to fill talent shortages with new workers in emerging markets.⁷ Many of these workers may not have the same level of development skills as more experienced workers. Coverity Development Testing will enable you to more effectively teach your developers to code more cleanly by providing them immediate visibility into coding errors and tracking improvement over time.



Software Integrity Report

Project Name: IVI Supplier
Version: Unknown
Project Description:

Lines of Code Inspected: 388,192

Integrity Level **RED**

| | |
|--|--|
| Customer Name: | Coverity Product: Coverity® Static Analysis |
| Point of Contact: | Product Version: |
| Customer email: | Coverity Point of Contact: |
| Report Date: Jan 26, 2012 4:00:28 PM | Coverity Email: |
| Report ID: abd41347-bcff-43b7-9730-af1f091d9f9e | |

The Coverity® Software Integrity Report provides a summary of the compliance status of a particular project, component or team based upon the policies established in Coverity Integrity Control™ and the results of the testing completed with Coverity® Static Analysis and/or Coverity® Dynamic Analysis. In addition to the summary, this report also provides a detailed breakdown of the areas in violation of established policies, at risk of violating established policies and in compliance with established policies. Organizations can use this report to facilitate a discussion with internal teams and third party suppliers.

Copyright © 2004-2011 Coverity, Inc. All rights reserved worldwide.

COVERITY CONFIDENTIAL. The information contained in this document is the proprietary and confidential information of Coverity and its licensors, and is supplied subject to, and may be used only by Customer in accordance with the terms and conditions of a license agreement previously accepted by Coverity and Customer.

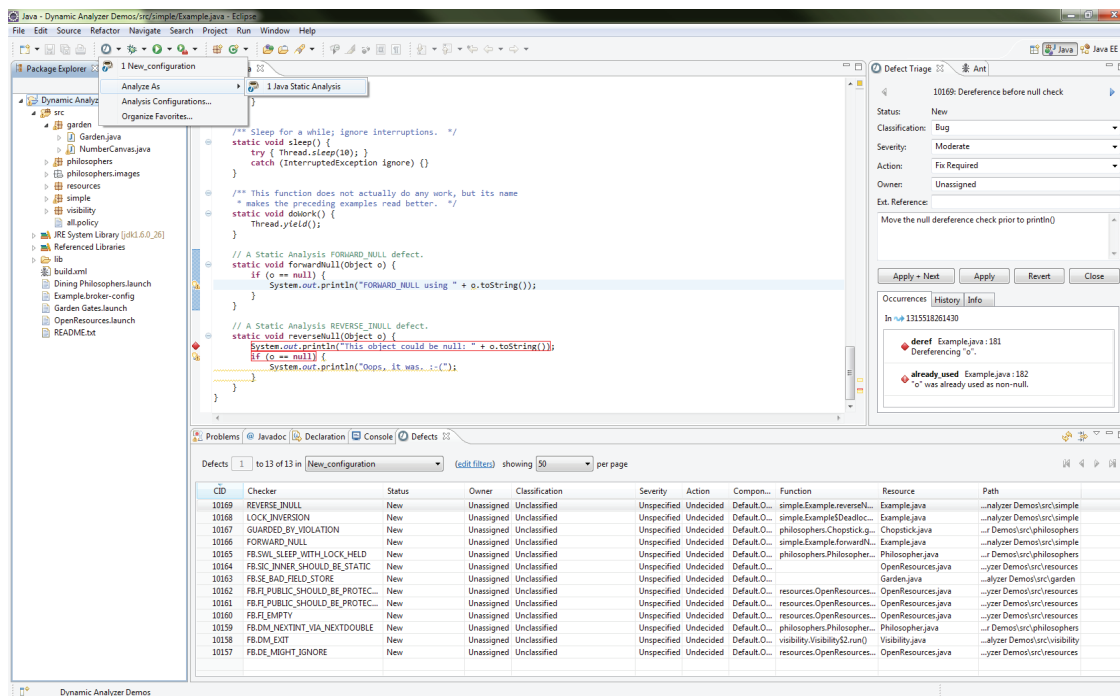
[Automatically communicate with suppliers when they are out of compliance](#)

An Extensible Platform

Coverity provides an extensible platform that enables organizations to integrate third-party tools such as coding style tools, SCM systems, bug tracking systems and more. Managers get a holistic view of the overall quality, security and safety of their projects.

Integrated into the Software Development Lifecycle

Coverity enables you to choose best of breed technology while fitting into your existing software development lifecycle process such as the V methodology or Agile. Seamless integration with IDEs like Eclipse, Visual Studio and the WindRiver Workbench lets you view defects and understand their severity and impact. Once the code has been analyzed, you can check it into the continuous integration server or central build system where the analysis engine can evaluate the cumulative changes of the entire development team. To save time, you can also choose to utilize incremental analysis which only analyzes the files which have been changed or those affected by the change instead of the entire code stream. By scanning code from the desktop, you are able to address security and quality issues immediately—as part of your development process.



Developers can test their code within Eclipse, Visual Studio or WindRiver Workbench

One of the most common practices of Agile development is continuous integration (CI). By increasing the frequency of integration that CI provides, delivery teams improve their visibility of the overall quality of the software. Integration issues, build problems and code conflicts are surfaced more quickly allowing faster remediation. In order for a development testing solution to work in an agile environment, it is essential that the analysis is done as frequently as the source integration happens. The analysis needs to be automated, fast, and scalable, especially when the development team is large. Coverity Static Analysis is integrated with build tools such as Jenkins, which enables an automated continuous process for code assurance.

Fostering Development and QA Collaboration

Through the out-of-the-box integration with HP Application Lifecycle Management (ALM), Coverity development testing results are automatically surfaced in the ALM and HP Quality Center workflow, providing development and QA with a single platform and common workflow for collaboration through visibility into defects identified in development. With every code change, Coverity automatically tests the code for defects, surfaces them in HP ALM, and links them to the corresponding business requirement so development and QA know where to focus their efforts, reducing risk of releasing defects into production without impacting time, cost or speed of deployment. This level of collaboration, defect traceability and visibility within the existing workflow is critical to agile organizations trying to rapidly ship products to market while maintaining acceptable levels of quality.

Summary

Automotive executives are under more pressure than ever to deliver more innovation faster to the market at the lowest cost possible. To meet that challenge, organizations are investing heavily in IVI and Telematics software, and in the people building that software. Coverity allows organizations to best utilize their resources by enabling them to find and fix software defects during development where issues are fastest and least expensive to address. This allows the development teams to focus more of their resources on delivering innovation, while protecting themselves from risk. For the developer, Coverity provides highly accurate results that enable them to be more productive and create better code, without slowing them down. Coverity provides the industry's first developer friendly and enterprise ready development testing platform, empowering development organizations to adopt development testing as a seamless part of the development process.

Experience that Matters

Coverity works with some of the leading automotive OEMs and suppliers in the market today, including 4 out of the top 5 North America OEM suppliers, the top 2 global OEM suppliers, the world's leading navigation systems and industry leaders, such as Telenav, Mitsubishi Electric, Tom Tom, Denso Corporation, e.solutions GmbH and many more. Over 38 million cars sold include GPS, automotive navigation systems, and diagnostic control systems tested with Coverity. Coverity was utilized by the NASA Engineering and Safety Center (NESC) to investigate the Toyota Prius Unintended Acceleration issue.

Coverity acts as the quality, safety and security gate to the shipment of over 11 billion products.

For More Information

Find out how Coverity can help your organization improve the quality and security of your software and how it can be integrated into your software development lifecycle. Contact your Coverity representative or visit us at www.coverity.com.

For More Information:
www.coverity.com
Email: info@coverity.com

Coverity Inc. Headquarters
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: (800) 873-8193
International Sales: +1 (415) 321-5237
Email: sales@coverity.com