Black Duck Newsroom

Synopsys Expands Software Integrity Strategy to Enable Development of Safer and More Secure Automotive Software

Highlights:

- Synopsys' Coverity® and Test Advisor™ software integrity solutions receive ISO 26262 and IEC 61508 certification for use in development of safety-critical automotive software
- Synopsys collaborating with automotive industry leaders to improve security testing requirements for software development and supply chain management
- Synopsys' Mike Ahmadi helps form SAE Cybersecurity Assurance Testing Task Force, actively contributes to developing community-driven cybersecurity standards

Disclaimer: The Synopsys Software Integrity Group is now Black Duck®. Click here to learn more.

MOUNTAIN VIEW, Calif., May 23, 2016 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today announced that it is expanding its Software Integrity strategy to address the cybersecurity and safety challenges faced by the automotive industry. With more than 100 million lines of code in modern cars, increasing connectivity and the imminence of autonomous driving, secure software development practices, vetted testing tools and standards compliance are essential for automotive manufacturers and their suppliers. To address these critical needs, Synopsys is enhancing its Software Integrity Platform to support existing functional safety standards and is collaborating with automotive industry stakeholders to establish new standards that focus on cybersecurity.

Coverity and Test Advisor Receive ISO 26262 and IEC 61508 Certification for Use in Development of Safety-critical Automotive Software

ISO 26262 is an international standard, based on the more generic IEC 61508 safety standard, which specifically addresses possible hazards caused by malfunctioning electronic and electrical systems in road vehicles. The standard requires essential tools used in the development of safety-critical systems to be independently certified. TÜV SÜD Product Service GmbH, a leading independent certification body with over a century of automotive safety and performance experience, has certified that Coverity and Test Advisor, two of the applicable tools in Synopsys' Software Integrity Platform used for static analysis and test optimization respectively, are compliant with the ISO 26262 and IEC 61508 standards.

To learn more about how Coverity and Test Advisor can streamline the development of ISO 26262-compliant software, download the white paper: Meeting ISO 26262 Guidelines with the Synopsys Software Integrity Platform.

Going Beyond Current Industry Standards

In addition to providing solutions that support existing industry standards such as ISO 26262 and MISRA (The Motor Industry Software Reliability Association), Synopsys is collaborating with vehicle manufacturers, their suppliers and other industry stakeholders to establish new standards that go beyond functional safety and coding guidelines to specifically address cybersecurity risk throughout the software development lifecycle and software

supply chain .

Catalyzed by the widely publicized remote vehicle hack demonstrated by Charlie Miller and Chris Valasek and the subsequent recall of nearly 1.4 million vehicles, Synopsys has produced and is freely distributing a sample procurement document for establishing basic software security testing requirements across the automotive supply chain.

Shortly after the vehicle hack, Mike Ahmadi, Synopsys' global director of critical systems security convened with several representatives from automotive manufacturers and suppliers to form a grassroots working group that was recently formalized as the Cybersecurity Assurance Testing Task Force under SAE (TEVEES18A1). The task force's charter is to create a consistent framework whereby all systems and components throughout the extended automotive supply chain can be evaluated against a common set of criteria. Ahmadi, who has extensive experience working with standards bodies, actively contributes to the task force's community-driven efforts to develop new cybersecurity standards for the automotive industry.

Evolving Automotive Software Challenges

In its "Connected Car Driving Change in the Defect Detection" white paper, VDC Research reported that some modern vehicles contain over 100 electronic control units (ECU) and greater than 100 million lines of code, and the automotive industry as a whole lacks the cognizance, resources and institutionalized best practices necessary to test and secure systems at the pace in which they're being introduced.

"The automotive industry, which has by and large revolutionized modern quality assurance and supply chain management practices on the hardware front, needs to evolve to address the challenges of developing and testing secure software," said Chris Rommel, executive vice president of IoT and embedded technology at VDC Research.

"As the automotive industry turns to connectivity and increasingly complex, interconnected software systems to drive innovation, the risks of insecure software development practices and poor software supply chain management are now a board-level concern," said Andreas Kuehlmann, senior vice president and general manager of Synopsys' Software Integrity Group. "Mitigating these risks will require close industry collaboration, as well as advanced testing methodologies and comprehensive tool suites."

Software Integrity Platform

Synopsys' Software Integrity Platform is based on an integrated development and testing methodology pioneered by Synopsys called 'software signoff.' Software signoff implements a series of automated testing processes at critical progression points throughout the software development lifecycle and software supply chain to elevate confidence in the quality and security of software.

- **Coverity** solution – Synopsys' ISO 26262-certified static code analysis tool automatically identifies critical quality defects and security vulnerabilities in source code.
- **Test Advisor** solution – Synopsys' ISO 26262-certified test optimization tool improves the efficiency of automated software testing by analyzing and prioritizing code change impact.
- **Protecode™** solution – Synopsys' software composition analysis tool identifies known vulnerabilities and license risks in third-party software.
- **Defensics®** solution – Synopsys' intelligent fuzz testing tool discovers unknown vulnerabilities in a software

systems' communication protocols such as CAN BUS, Bluetooth and Wi-Fi.

To learn more, visit Synopsys' webpage about Software Integrity solutions for the automotive industry.

About Synopsys

Synopsys, Inc. (Nasdaq:SNPS) is the Silicon to Software™ partner for innovative companies developing the electronic products and software applications we rely on every day. As the world's 15th largest software company, Synopsys has a long history of being a global leader in electronic design automation (EDA) and semiconductor IP and is also growing its leadership in software quality and security solutions. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing applications that require the highest quality and security, Synopsys has the solutions needed to deliver innovative, high-quality, secure products. Learn more at www.synopsys.com.

Editorial Contacts:
Mark Van Elderen (Software Integrity Group)
Synopsys, Inc.
415-266-6408
mvanelde@synopsys.com

Monica Marmie (Corporate)
Synopsys, Inc.
650-584-2890
monical@synopsys.com

Logo - http://photos.prnewswire.com/prnh/20160325/348205LOGO

SOURCE Synopsys, Inc.

---

https://news.blackduck.com/2016-05-23-Synopsys-Expands-Software-Integrity-Strategy-to-Enable-Development-of-Safer-and-More-Secure-Automotive-Software