Meet Automotive Software Safety and Security Standards Expectations More Quickly

Authors : Jean-François Pouilly

Abstract : This study addresses the growing complexity of embedded systems and the critical need for secure, reliable software. Traditional cybersecurity testing methods, often conducted late in the development cycle, struggle to keep pace. This talk explores how formal methods, integrated with advanced analysis tools, empower C/C++ developers to 1) Proactively address vulnerabilities and bugs, which includes formal methods and abstract interpretation techniques to identify potential weaknesses early in the development process, reducing the reliance on penetration and fuzz testing in later stages. 2) Streamline development by focusing on bugs that matter, with close to no false positives and catching flaws earlier, the need for rework and retesting is minimized, leading to faster development cycles, improved efficiency and cost savings. 3) Enhance software dependability which includes combining static analysis using abstract interpretation with full context sensitivity, with hardware memory awareness allows for a more comprehensive understanding of potential vulnerabilities, leading to more dependable and secure software. This approach aligns with industry best practices (ISO2626 or ISO 21434) and empowers C/C++ developers to deliver robust, secure embedded systems that meet the demands of today's and tomorrow's applications. We will illustrate this approach with the TrustInSoft analyzer to show how it accelerates verification for complex cases, reduces user fatigue, and improves developer efficiency, cost-effectiveness, and software cybersecurity. In summary, integrating formal methods and sound Analyzers enhances software reliability and cybersecurity, streamlining development in an increasingly complex environment.

Keywords : safety, cybersecurity, ISO26262, ISO24434, formal methods
Conference Title : ICCV 2025 : International Conference on Connected Vehicles
Conference Location : Zurich, Switzerland
Conference Dates : January 16-17, 2025