TrustInSoft Extends Formal Verification to Rust and Real-Time Systems

PARIS, FRANCE, November 4, 2025 /EINPresswire.com/ -- TrustInSoft, a pioneer in exhaustive static code analysis, today announced the availability of TrustInSoft Analyzer 2025.10, the latest release of our formal verification toolchain. The update introduces comprehensive Rust analysis capabilities for detecting undefined and unwanted behaviors and delivers an improved multithreading experience. It enables development teams working with Rust or mixed-language codebases in safety-critical environments to gain formal, mathematical confidence in the safety and reliability of their software.

TrustInSoft Extends Formal Verification to Rust and Real-Time Systems

> TrustInSoft Analyzer 2025.10 delivers what developers and security teams have been asking for: a tool that doesn't guess, doesn't miss and doesn't stop at 'probably OK'"
>
> *Caroline Guillaume, TrustInSoft CEO*

"TrustInSoft Analyzer 2025.10 delivers what developers and security teams have been asking for: a tool that doesn't guess, doesn't miss and doesn't stop at 'probably OK,'" said Caroline Guillaume, TrustInSoft CEO. "It brings formal, mathematical confidence to the newest and most complex parts of the modern codebase. This release isn't just a step forward. It's a leap into the future of safe, secure and standards-compliant software development."

Rust Support

Rust has taken center stage in the world of systems programming, praised for its built-in memory safety. However, there are safety guarantees that Rust doesn't provide, including protection against overflows and safe calling into C functions. Rust also has an unsafe sublanguage where the proof of memory safety needs to be conducted by the user.

In March 2025, TrustInSoft formed a partnership with Ferrous Systems, the leader in Rust-based

tooling and solutions for safety-critical and embedded systems, to bring Rust support and the benefits of their qualified compiler toolchain, Ferrocene, to TrustInSoft's formal analysis engine. TIS Analyzer 2025.10 now provides the same interactive root cause investigation, code coverage, and mathematical proof guarantees for Rust as it does for C and C++. For engineering teams mixing Rust with legacy C/C++ or working in safety-critical environments, this means something concrete: a way to detect undefined and unwanted behaviors, panics, and memory vulnerabilities in mixed-language codebases before they hit production.

TrustInSoft Logo

"Writing software that is correct and reliable starts with confidence in both the tools and the process," said Florian Gilcher, managing director of Ferrous Systems. "Rust's memory safety, our qualified compiler toolchain, Ferrocene, and the formal verification in TIS Analyzer provide complementary capabilities that, when used together, help development teams navigate critical paths with confidence and deliver software they can trust."

Concurrency Analysis

Concurrency bugs can be elusive. TIS Analyzer 2025.10 introduces native support for analyzing concurrent code—including real-time operating systems, interrupt-driven firmware, and multi-instance threading scenarios.

The Analyzer doesn't just simulate a few scenarios. It explores all execution paths, flagging race conditions and non-deterministic behaviors with the same mathematical confidence it brings to single-threaded code.

C23 and Smarter Triage

TIS Analyzer 2025.10 also rounds out support for C23 language features. Developers can now analyze code using _BitInt, constexpr, and nullptr—with improved structure visualization in the Root Cause Investigator.

Alarm triage is also getting smarter. Teams can now collaborate more effectively with features for reviewing, classifying, commenting on, and linking alarms to external bug-tracking systems.

Learn more about TrustInSoft Analyzer.

About TrustInSoft

TrustInSoft is a leader in advanced software analysis tools and services that specialize in formal verification of C and C++ source code to ensure safety, security and reliability. Recognized by the US National Institute of Standards and Technology (NIST) for leveraging advanced formal methods, including abstract interpretation, TrustInSoft can mathematically guarantee analyzed software is free of critical runtime errors and vulnerabilities. TrustInSoft serves a diverse range of

industries including automotive, aerospace, defense, consumer electronics, and IoT industries.

Media Contact:
Natasha Le Marquand at natasha@napierb2b.com
Phone: +44 (0)1243 531123

Natasha Le Marquand
Napier
+44 1243 531123
email us here
Visit us on social media:
LinkedIn
X
YouTube
Facebook
