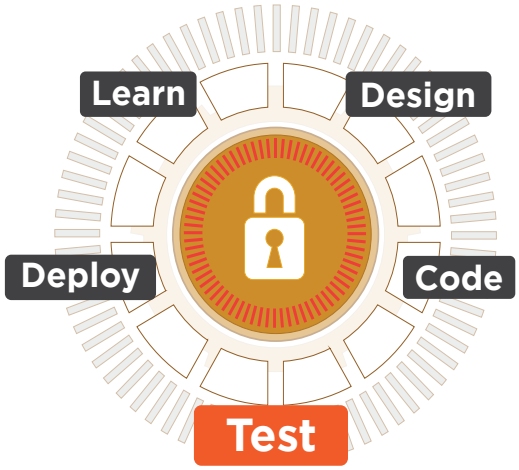
TRUST IN SOFT

TRUSTINSOFT ANALYZER FOR C/C++

COMPREHENSIVE SOFTWARE ASSURANCE

TrustInSoft Analyzer (TISA) delivers exhaustive static and dynamic analysis for C and C++ code, ensuring software safety, security, and reliability through advanced formal methods like abstract interpretation. TISA supports compliance with key industry standards while integrating seamlessly into existing workflows, providing mathematically proven assurance.



STANDARDS COMPLIANCE

- ISO 26262
- ISO 21434
- DO -178C
- IEC 61508
- AUTOSAR
- CERT C

KEY FEATURES

Exhaustive Analysis

Detects all undefined behaviors, including buffer overflows, integer overflows, and division by zero, with zero false alarms.

Full Path Context Sensivity

Thorough exploration of all execution paths, ensuring comprehensive coverage and robust code integrity.

Automated Generalization

Tests all potential code values, significantly increasing test coverage and reducing testing effort.

Hardware-Aware Analysis

Simulate and test software on specific hardware targets (X86, ARM, RISC-V) with detailed memory mapping.

Advanced Reporting Tools

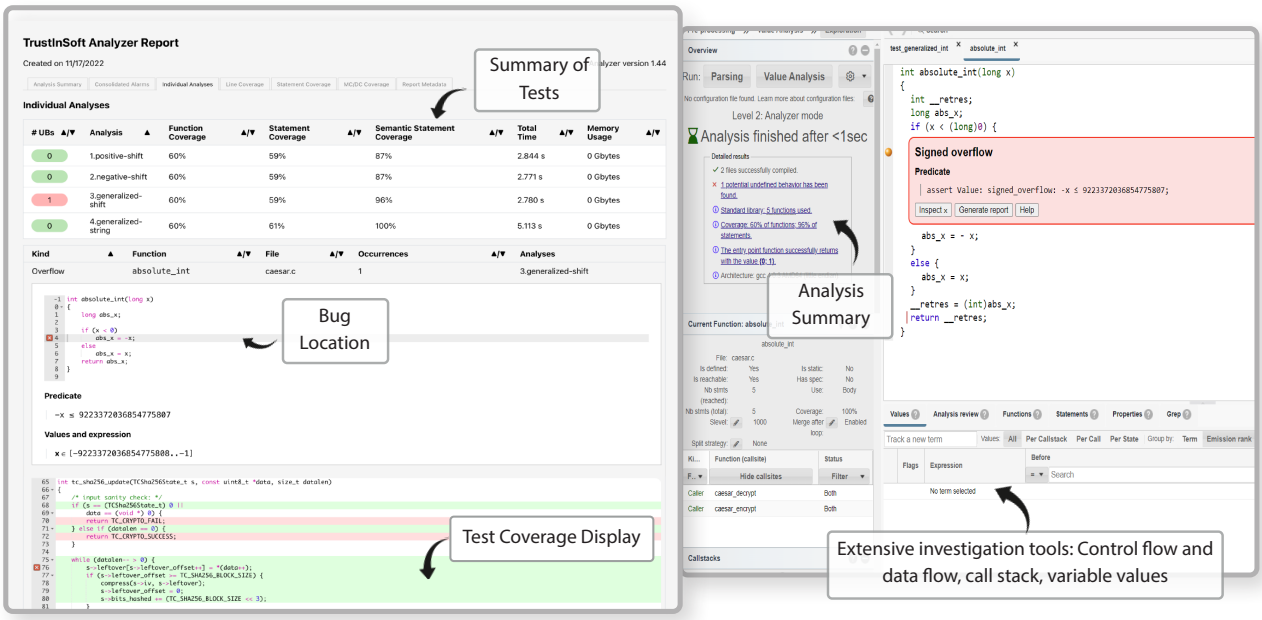
Streamlined generation of compliance reports, ensuring adherence to industry standards.

Seamless CI/CD Integration

Easily integrates into Agile and V-model workflows, enhancing your verification processes without disrupting existing pipelines.

AUTOMATED REPORTS

INVESTIGATION TOOLS



Mathematical Guarantees

TISA provides mathematically proven assurance of software safety, security, and reliability.

Efficient Compliance

TISA simplifies the compliance process with automated report generation, ensuring adherence to the most stringent industry standards.

Cost and Time Savings

TISA delivers comprehensive test coverage faster, reducing development time and costs.

TRUSTINSOFT ANALYZER DETECTS ALL UNDEFINED BEHAVIORS AND MORE

- Buffer overflow
- Use-after-free
- Division by zero
- Integer overflow
- Array subscript out of range
- Strict aliasing violation
- Dangerous function cast
- Uninitialized memory
- Memory leaks

These bugs are subtle and complex to detect with typical testing methods. They are used for cyberattacks. They also introduce non-deterministic behaviors and cause software to crash and are used for cyber attacks

GUARANTEE ZERO-BUG SOFTWARE WITH TRUSTINSOFT ANALYZER

TrustInSoft is a leader in advanced software analysis tools and services that specializes 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.

contact@trust-in-soft.com | EUROPE +33 1 84 06 43 91 | USA +1 (408) 829-5882

@TrustInSoft | trust-in-soft.com

TRUST IN SOFT