

USE **FORMAL METHODS** TO OPTIMIZE THE COSTS OF **DO-178C/ED-12C** CERTIFICATION

TrustInSoft Analyzer is a groundbreaking technology for source code analysis that can be deployed to reduce the costs of software verification by using formal methods.

TrustInSoft Analyzer allows you to validate DO-333/ED-216 compliant software in a cost-effective manner. By optimizing software verification, you can gain a competitive advantage and significantly cut costs and reduce lead time.

TRUSTINSOFT ANALYZER CAN OPTIMIZE THE FOLLOWING ACTIVITIES:

(Listed in the Formal Methods supplement in section FM.6.3.4.)

COMPLIANCE WITH LOW-LEVEL REQUIREMENTS

The Airbus Group replaced the Unit testing with “Unit Proof” for the A380, the A400M, and the A350 for Level A software.

- Souyris, Wiels, Delmas, Delseny, *Formal Verification of Avionics Products in FM'2009*, LNCS Springer

SOFTWARE INTEGRATION VERIFICATION

Dassault Aviation conducted conclusive experiments for robustness analysis.

- Ledinot, Pariente, *Formal methods and compliance to the DO-178C/ED-12C standard in aeronautics*, Wiley Eds.

COMPLIANCE WITH THE SOFTWARE ARCHITECTURE

The Airbus Group used our technology to check that the data flow and control flow of the source code matched the software architecture.

- Cuoq, Delmas, Duprat, Fan-C, *a Frama-C plugin for data flow verification*, ERTSS'2012.

VERIFIABILITY

Identify unverifiable source code automatically using custom tool extensions.

- Reference Classified

CONFORMANCE TO STANDARD

Custom programming rules allow for an easy extension of TrustInSoft’s unified framework, based on formal methods.

- Delmas, Duprat at al., *Taster a Frama-C plugin to enforce coding standards*, ERTSS'2010

ACCURACY AND CONSISTENCY

Operate TrustInSoft Analyzer to check: memory usage; arithmetic overflows; floating point arithmetic; use of uninitialized variables or unused variables.

- Reference Classified

TRUSTINSOFT'S EXPERTS HAVE MORE THAN 10 YEARS OF INDUSTRY EXPERIENCE AND CAN PROVIDE AN END-TO-END SOLUTION DURING THE OVERALL V&V PROCESS, INCLUDING:

Definition of the needs and selection of the the most efficient formal method for your methodology

Customization of TrustInSoft's diagnosis and analysis tools

Deployment of the tools and selection of the right technology

Preparation of the certification artifacts for your software developments

Preparing the software tool's qualification to remain compliant with DO-330/ED-215

PRODUCTS & SERVICES

TrustInSoft provides tools and services that enable our customers to exhaustively verify properties of software.

We offer:

Verification kits for commercial software components (COTS). We validate common software components such as communication stacks, parts of operating systems, and web servers. These widely used pieces of COTS software have already been "TrustInSoft Verified" by our experts. The verification kit contributes to your certification file.

TrustInSoft Analyzer. Our exclusive software analyzer tool pre-installed on a stand-alone workstation or adapted to your IT infrastructure. It allows you to validate in-house software with formal methods.

Expertise and Training. TrustInSoft experts and our selected Business Partners work with you every step of the way.

Cut Costs & Reduce Lead Time with the TrustInSoft Analyzer

A VERIFIED SSL STACK

Using TrustInSoft Analyzer, we were the first to validate an open source implementation of an SSL/TLS software stack, and assess its immunity against weaknesses CWE #119 to 127, #369, #415, #416, #457, #476, #562, and #690.

TrustInSoft is the only commercially available software solution that is capable of achieving this ultimate level of quality assurance. This SSL/TLS stack is now immune to threats like Heartbleed.

SECURITY PROPERTIES

Software developers and integrators have several methods to check that the software components they use and deploy can resist external attacks. They may follow a quality process (CMMI, Common Criteria, etc.), hire an expert to find security flaws, or use a commercially available source code analysis tool.

Using TrustInSoft's technology, you can guarantee the absence of complete families of software flaws: most common CWEs are systematically removed. TrustInSoft's competitors do not and cannot provide such a feature. TrustInSoft has created a new kind of product: off-the-shelf security analysis for common software components marketed and distributed as verification kits.

INTERNATIONAL RECOGNITION

TrustInSoft's technology is the only technology able to meet NIST's SATE V Ockham Criteria.