CLIENT	**TrustInSoft**
PROJECT	**White paper on ensuring software compliance with ISO/SAE 21343**
OBJECTIVE	**Explain why automotive software developers need to see beyond ISO/SAE 21434 to ensure effective cybersecurity and how that goal can be achieved using TrustInSoft Analyzer.**

COPY EXCERPT

ISO/SAE 21434 from a Software Development Perspective

How sound, exhaustive static analysis can help ensure air-tight automotive cybersecurity while lowering its costs

Call or write CopyEngineer to receive a PDF of the complete case study.

Or view/download it online at: bit.ly/TrustInSoft-WP-ISO-SAE-21434

TrustInSoft Analyzer – the ultimate weapon against undefined behaviors

We mentioned earlier that the systematic detection of undefined behaviors requires a specialized, purpose-built tool. That tool is TrustInSoft Analyzer.

TrustInSoft Analyzer is a hybrid code analyzer that combines static and dynamic analysis techniques together with formal methods to produce existence proofs of properties that cannot be confirmed using static techniques only.[21] It is the formal methods that are key to these existence proofs.

Formal methods are ideal for validating code that needs to be perfect. They use mathematical techniques to "solve" the logic of computer programs or other systems (integrated circuits, for example) to answer questions about their behavior. For example, if you want to know if there is any way a buffer overflow could occur in your program, formal methods can be used to determine that.

What's more, a state-of-the-art formal methods tool can answer those questions automatically.

TrustInSoft Analyzer is a sound formal methods tool designed specifically to detect undefined behaviors. An analyzer is considered "sound" with respect to a specific guideline if it cannot give a false-negative result—if it finds all violations of the guideline within the program.

In other words, when TrustInSoft Analyzer is used to exhaustively analyze a program for specific undefined behaviors, it will find all instances of those undefined behaviors. It will report every UB in your code. Once those instances have been eliminated, you have an absolute guarantee that those undefined behaviors cannot occur in the program.

Thanks to its soundness, TrustInSoft Analyzer provides you, your customer, and any regulatory authorities with proof that no undefined behaviors exist within your software.

In addition, TrustInSoft Analyzer accounts for the configuration of your target hardware. It provides target emulation for embedded hardware platforms that enables testing in an environment that closely resembles your target architecture. Target emulation helps you find vulnerabilities that unit testing in a host environment cannot possibly reveal. And everything that can change from one platform to another is configurable in the Analyzer…

[21] Black, P.; Badger, L.; Guttman, B.; Fong, E.; *Dramatically Reducing Software Vulnerabilities: Report to the White House Office of Science and Technology Policy*; National Institute of Science and Technology (NIST), November 2016.