

Static analysis tool C-STAT

Ensuring code quality through static analysis

Catch issues before they become problems with C-STAT, the static analysis tool fully integrated into the IAR Embedded Workbench IDE. Effortlessly ensure your code complies with MISRA standards and hundreds of security checks from CWE and CERT, all without leaving your development environment.

Key Highlight Features

- Analysis of C and C++ code
- Includes more than 1000 checks in total, some comply with rules as defined by MISRA C:2023, MISRA C:2012, MISRA C++:2008 and MISRA C:2004
- More than 250 checks mapping to issues covered by CWE, SANS Top25 and OWASP
- Checks compliance with the coding standard CERT C for secure coding
- Fully integrated with the IAR Embedded Workbench IDE and the command-line IAR Build Tools
- Comprehensive and detailed error information
- Fast execution
- Available for most IAR Embedded Workbench and IAR Build Tools products
- Also available as TÜV SÜD certified version for selected IAR functional safety editions

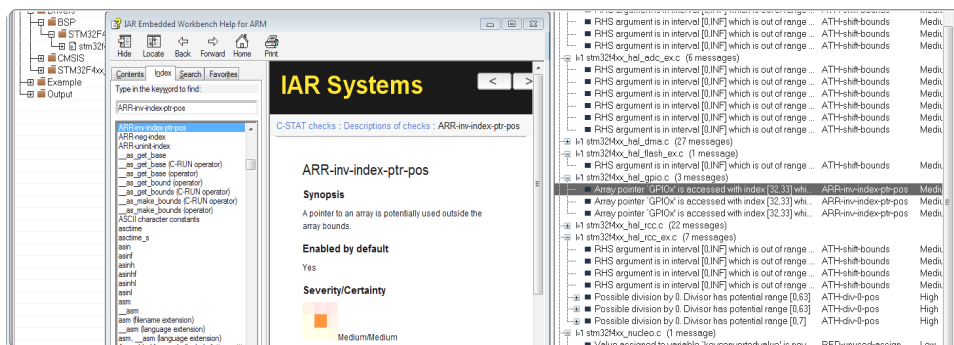
C-STAT checks code compliance with industry standards MISRA, CWE and CERT C/C++

C-STAT checks compliance with MISRA rules, CERT C/C++ Secure Coding Standards, and CWE-defined weaknesses, simplifying compliance with CWE-aligned output.

MISRA (the Motor Industry Software Reliability Association) rules, initially developed for the automotive industry, are now widely used across embedded systems. MISRA-C:2023 builds on MISRA-C:2012 (and amendments) with enhanced rules for modern safety and security challenges. The rules are classified as mandatory, required, or advisory, covering areas like compiler differences, avoiding unsafe functions, limiting code complexity, and ensuring maintainability.

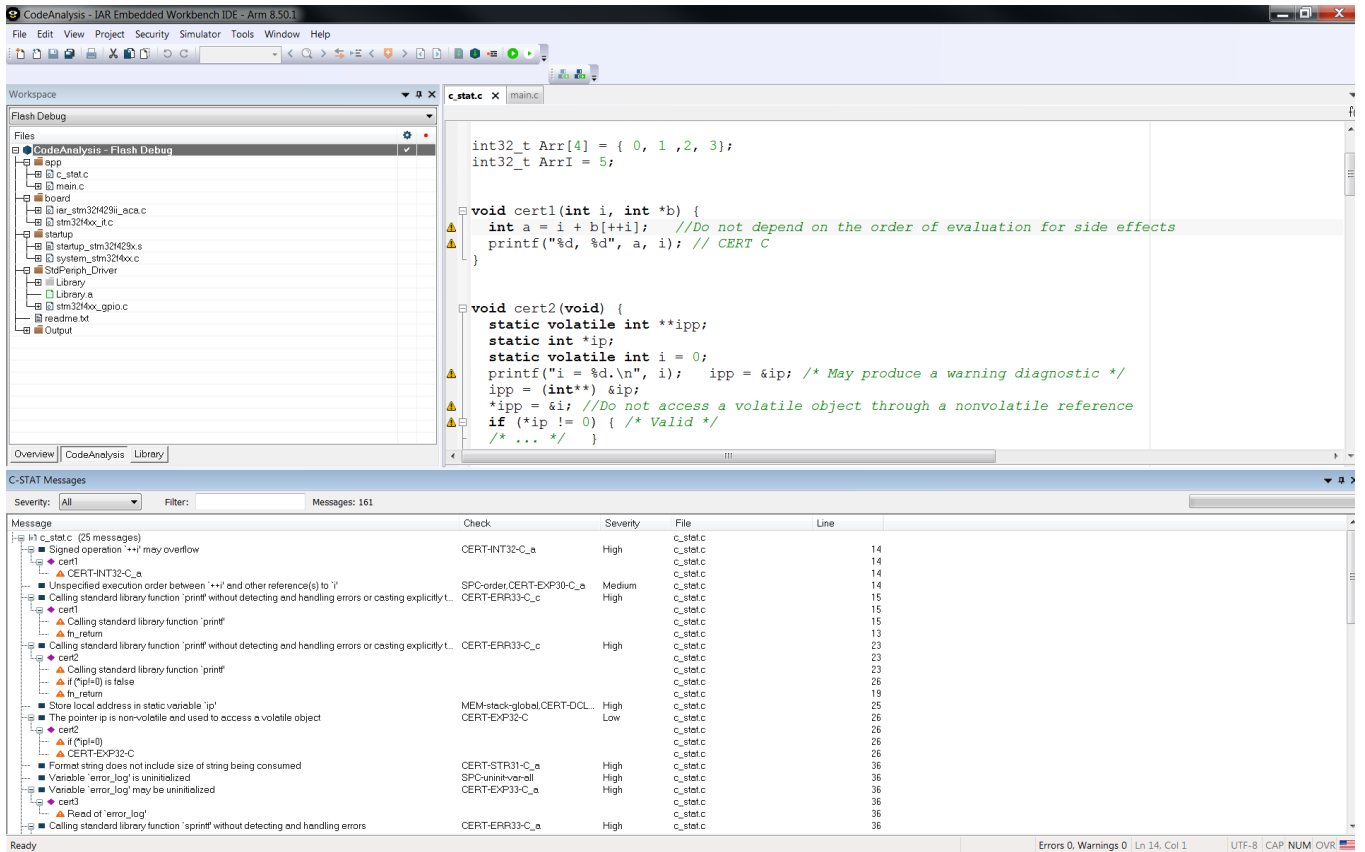
CWE (the Common Weakness Enumeration) is a community-developed dictionary of software weaknesses, detailing potential consequences, mitigations, code samples, and references to help manage vulnerabilities.

CERT provides secure coding rules for C and C++ to prevent coding and design errors that can lead to vulnerabilities. Each guideline includes a title, description, non-compliant code example, and compliant solutions, aimed at eliminating insecure practices and undefined behaviors.



Fully integrated into the IDE

C-STAT is fully integrated into the IAR Embedded Workbench IDE, making it as easy to use as standard build tools, with no need for complex setups. It checks your code against MISRA, CERT, and CWE standards, ensuring safety and security by referencing all relevant rules. Since these standards complement each other, C-STAT allows you to check against entire rulesets or individual rules, all thoroughly documented.



IAR Embedded Workbench

IAR Embedded Workbench is a complete C/C++ development toolchain for embedded applications, offering top-tier code quality, optimized performance, and extensive debugging tools. The integration of C-STAT helps developers ensure code quality early, reducing errors and speeding up time to market.

Do you need to ensure your code is secure, high-quality, and compliant with the standards?

We're here to support you every step of the way, from project start to product life-cycle completion.

Contact your local IAR team to get started: iar.com/contact