静态代码分析工具 C-STAT

通过静态代码分析，确保代码质量

静态代码分析通过在源代码级别进行分析，帮助您发现代码中的潜在问题。静态代码分析工具 C-STAT 完全集成在 IAR Embedded Workbench IDE 中，提供了一种简单的方法，确保您的应用程序符合 MISRA 定义的编码标准以及源自 CWE 和 CERT 的数百种其他检查。

关键功能亮点：

- 分析 C 和 C++ 代码
- 包含近 700 项检查，其中一些符合 MISRA C:2012、MISRA C++:2008 和 MISRA C:2004 定义的规则
- 超过 250 项检查与 CWE 涵盖的问题相对应
- 检查符合 CERT C 安全编码标准
- 完全集成在 IAR Embedded Workbench IDE 中
- 提供全面且详细的错误信息
- 执行速度快

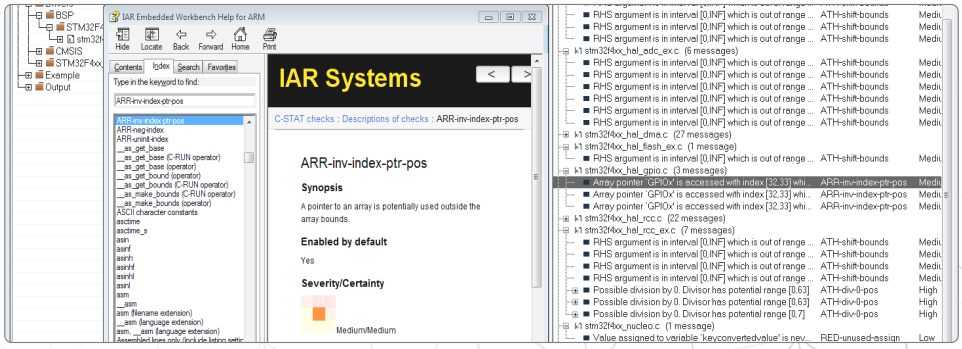
C-STAT 检查代码是否符合行业标准 MISRA、CWE 和 CERT C/C++

C-STAT 进行多项安全检查，以确保符合 MISRA 规则集和 CERT C/C++ 安全编码标准所定义的规则，以及 CWE 所定义的若干弱点。为进一步简化合规任务，C-STAT 提供的输出与 CWE 弱点命名保持一致。

MISRA (the Motor Industry Software Reliability Association) 规则已经在全球范围内扩展到不同的行业领域，并且该规则集现在是嵌入式行业中最广泛使用的 C 子集。最新版本的 MISRA-C:2012 包含 182 条规则和 18 条所谓的指令。这些规则被分类为强制、必需或建议，涵盖了避免可能的编译器差异（如整数大小）、避免使用易于失败的函数和结构、限制代码复杂性以及确保代码可维护性（例如通过使用命名约定和注释）等方面。

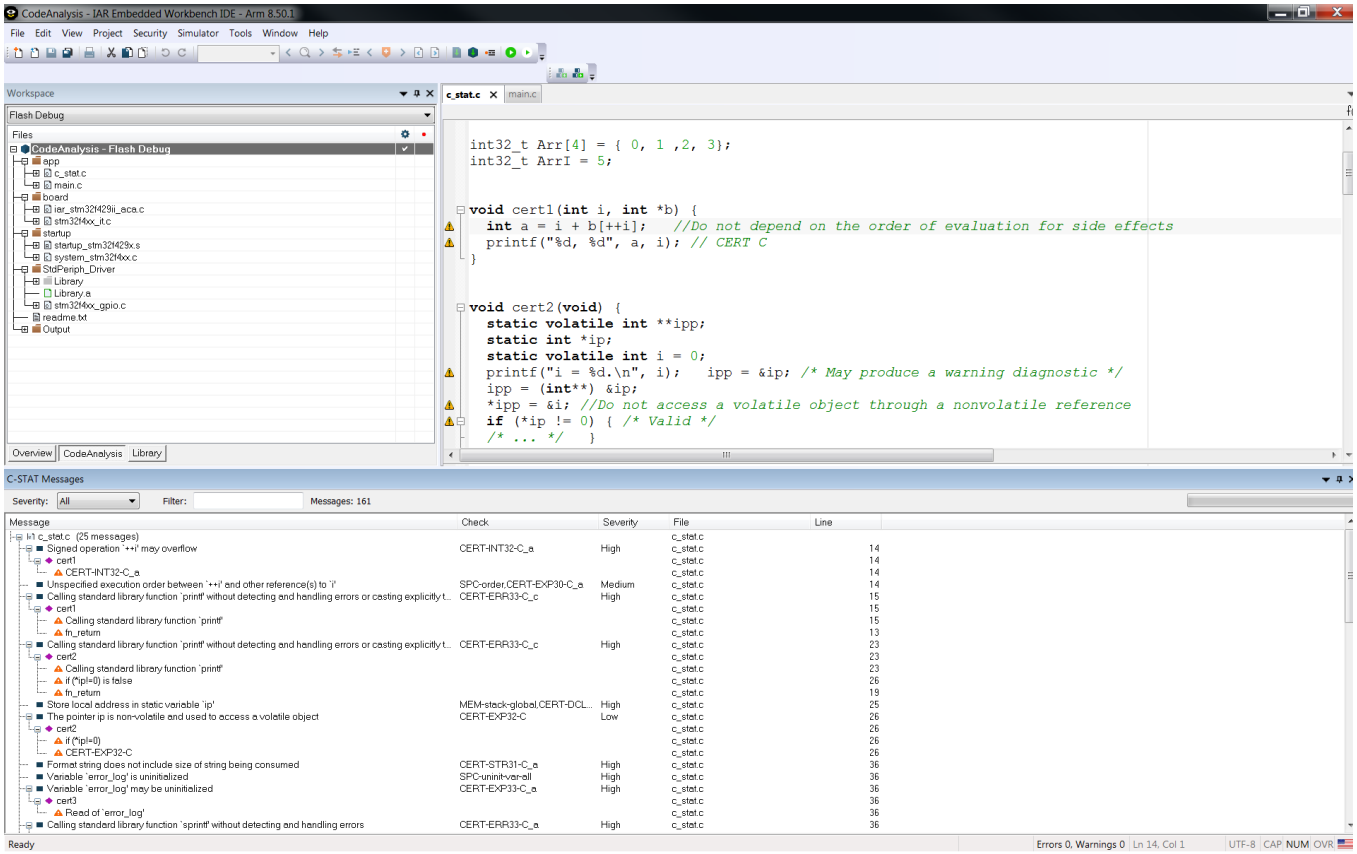
CWE (the Common Weakness Enumeration) 是一个社区开发的字典，描述了弱点及其潜在后果、可能的缓解措施、代码示例、分类法和参考资料。它旨在帮助更好地理解和管理软件弱点，并更有效地选择和使用能够发现这些弱点的软件安全工具和服务。

CERT (Computer Emergency Response Team) 提供了 C 和 C++ 安全编码的规则集。每个指南包括标题、描述、不符合规定的代码示例和符合规定的解决方案示例。这些标准包括避免编码和实现错误的指南，以及低级设计错误。标准的目的是消除不安全的编码实践和未定义的行为，这些行为可能导致可利用的漏洞。



完全集成到 IDE 中

C-STAT 完全集成到 IDE 中，使用起来就像常规构建工具一样简单。无需复杂的工具设置，也无需处理语言支持和常规构建问题。不同标准中的规则相互重叠并互为补充。没有任何编码标准包含 CWE 中的所有条目，因为并非所有条目都存在于一种编码语言中。由于这些标准具有相互支持的作用，咨询所有这些实例以确保软件的安全和可靠是明智的，甚至是必要的。无论您使用的是哪个规则集，C-STAT 都会检查您的代码是否合规，且 C-STAT 中的所有检查都经过详尽的文档记录，并引用了 CWE、MISRA 和 CERT 标准中的相应条目。您可以选择根据规则集或个别规则来检查您的代码。



IAR Embedded Workbench

IAR Embedded Workbench 是一个完整的 C/C++ 嵌入式应用开发工具链。该工具链提供领先的代码质量、卓越的尺寸和速度优化，以及强大的调试功能，配备完全集成的调试器，支持模拟器和硬件调试。C-STAT 完全集成在 IAR Embedded Workbench IDE 中，帮助开发人员在早期阶段确保代码的安全性和高质量，从而帮助企业缩短产品上市时间，因为后期发现和修复错误会非常耗时且昂贵。