QA MISRA 技术手册

产品概述

在开发过程中，越早发现并消除软件错误，成本就越低。QA-MISRA 检查源代码中的 900 多个潜在软件错误。通过使用 QA-MISRA 进行静态分析，可以在早期阶段轻松发现危险结构以及安全、维护和移植问题。

C/C++代码的快速分析

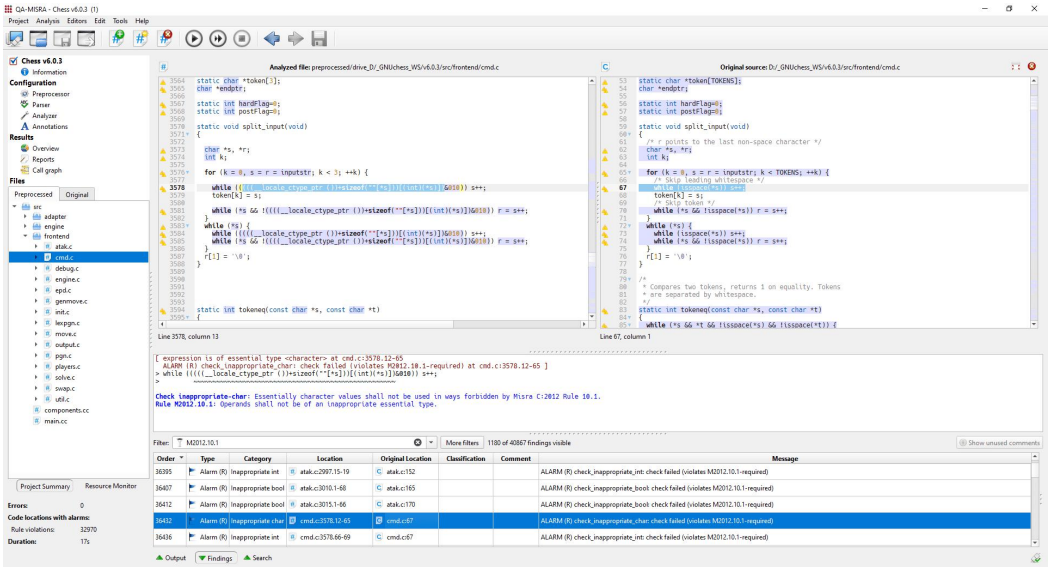
QA-MISRA 可以非常快速地分析大量复杂的软件包，不管大小如何。这简化了质量管理，并帮助用户遵守相关的安全标准。用户的代码是否符合项目所需的标准？

可靠、可移植、可维护

使用 QA-MISRA 检查的程序代码可靠、可移植且易于维护。因为有了 QA-MISRA，用户的软件变得更统一、更简单、更强大。

安全关键标准合规性

QA MISRA 自动检查用户的 C 或 C++代码符合 MISRA 和 AUTOSAR 规则，以及安全标准：SEI Cert C/C++，CWE，ISO/IEC TS 17961，HIS Metrics 等。



EMAIL : contact@watertek.com
TEL : 010-82695188

功能特性

静态代码分析

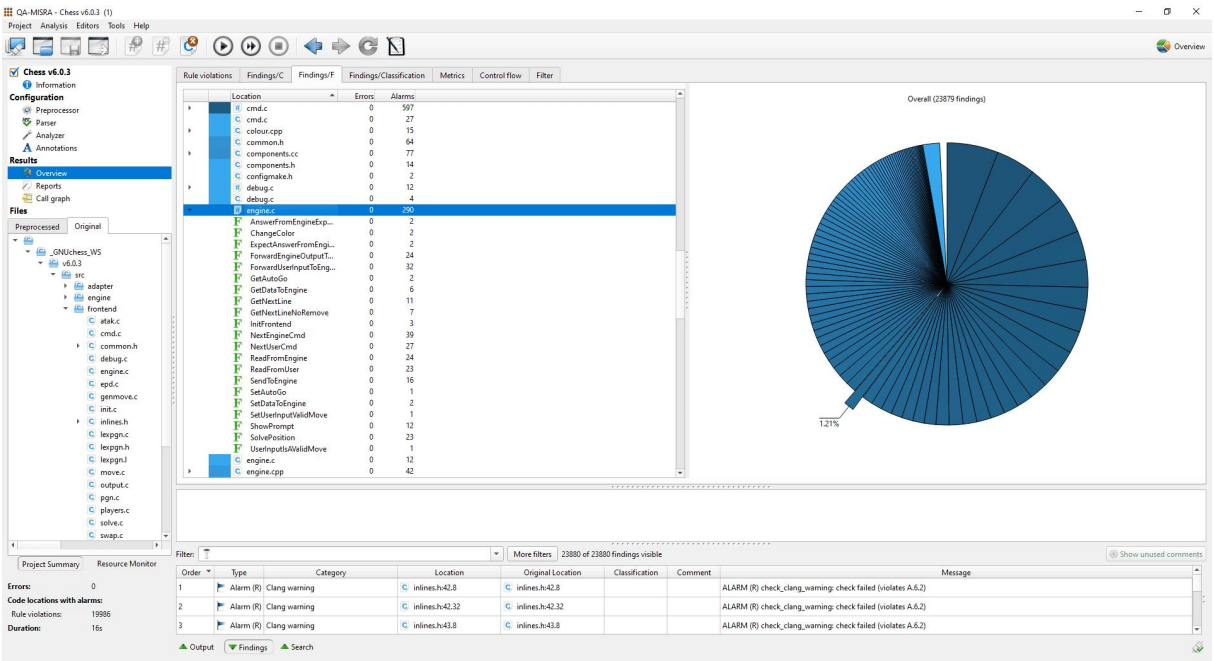
静态分析持续检查和报告软件缺陷、语言实现错误、不一致、危险用法、编码标准违背和安全漏洞。

- 早期检测缺陷，防止代价昂贵的错误

QA-MISRA 检查源代码中的 900 多个潜在软件错误。通过使用 QA-MISRA 进行静态分析，可以在早期阶段轻松发现危险结构以及安全、维护和移植问题。

- 生产干净的行为可预测的代码

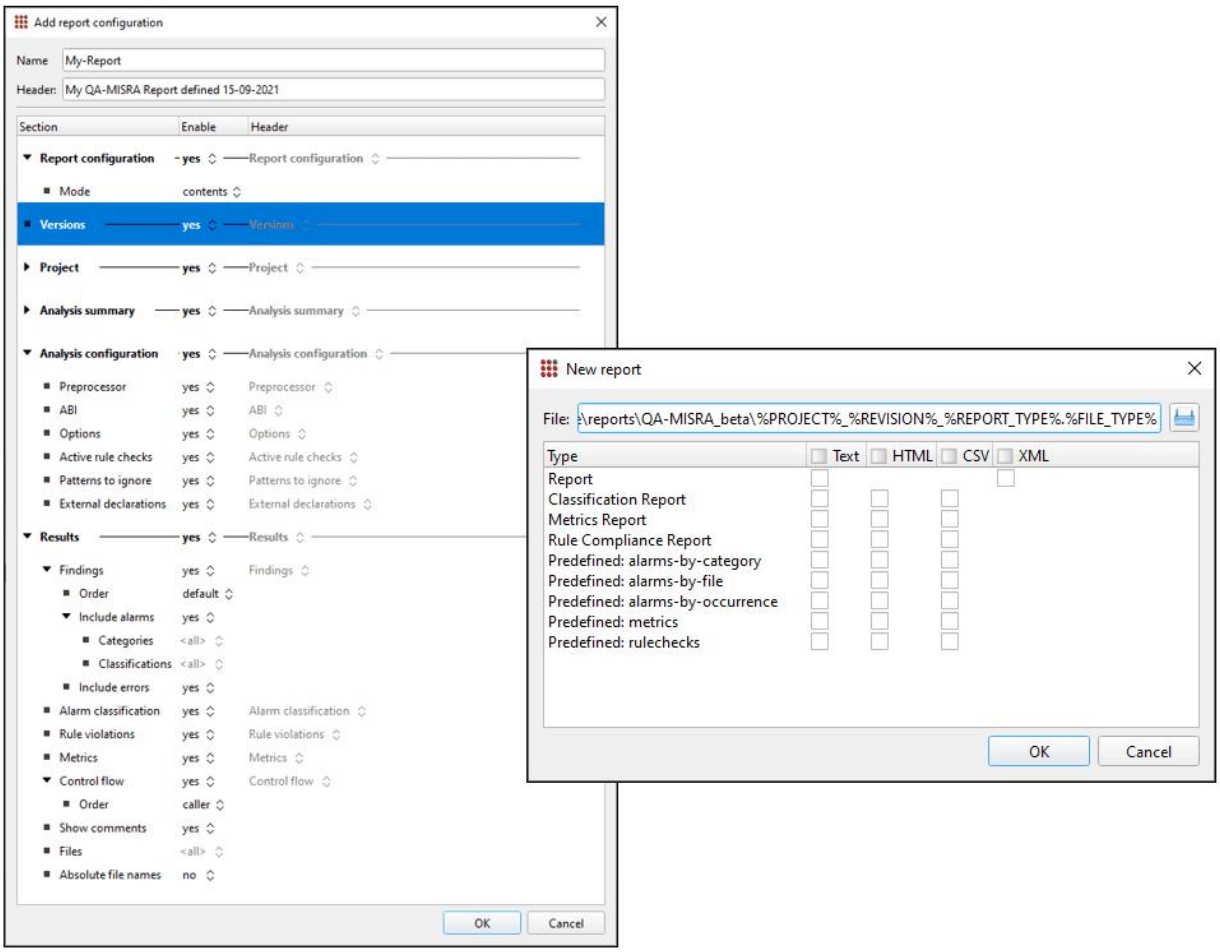
即使是符合 ISO 标准的软件，其行为也可能与预期不同，因为并非所有在开发过程中可能导致问题的因素都被安全标准归类为不正确。这就是为什么使用 QA-MISRA 进行静态分析也会显示代码中经常被开发人员和编译器忽略的问题。QA-MISRA 中的测试完全自动化，节省了宝贵的开发人员资源。



- 监控代码库 – 综合的可配置报告

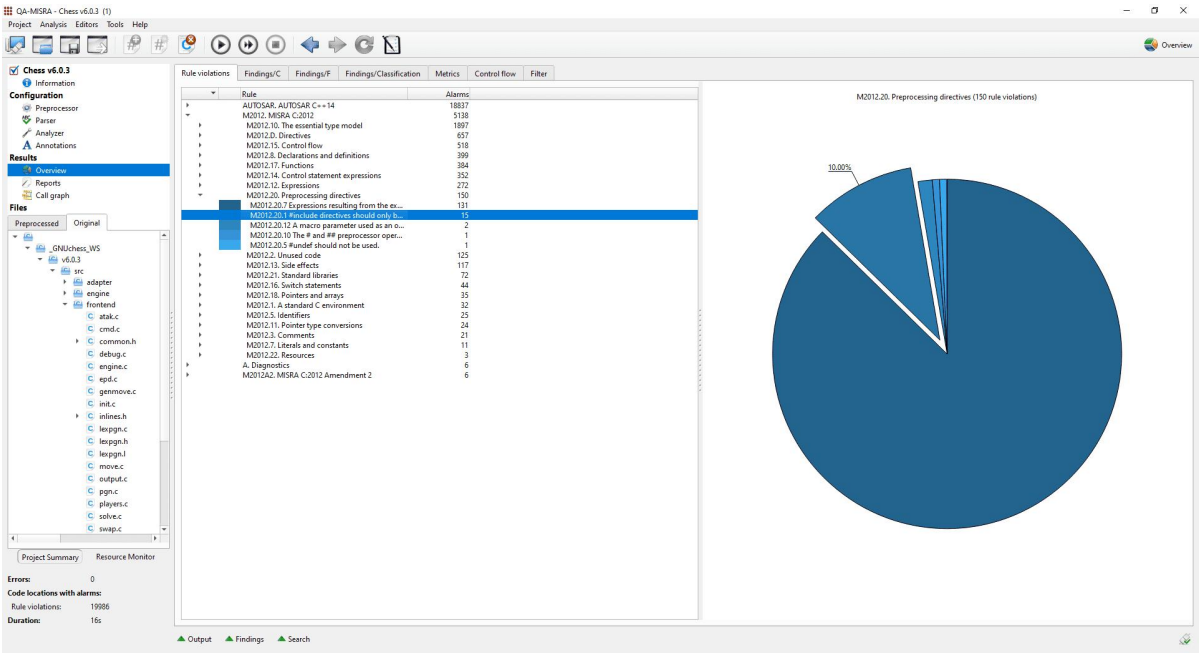
综合报告帮助用户查找问题，显示应该加以留意的地方。

- 合规性报告，指出需要更多工作以提高合规程度的区域
- 分类报告，检测出的规则违背由用户进行分类
- 度量报告，提供文本、HTML 和 CSV 格式的度量数据



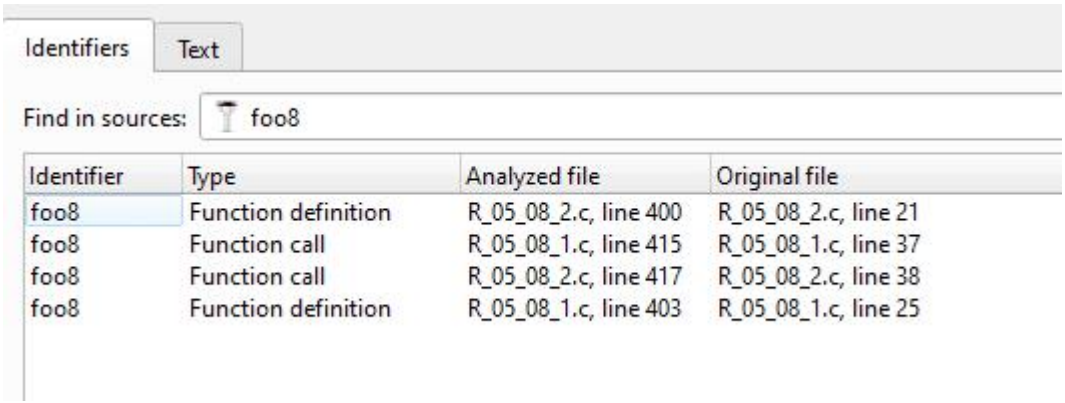
- 违反约束

QA-MISRA 可以帮助用户在语法正确但语义不正确、未指定或未定义的代码中查找错误。在某些情况下，这可能会导致编译器产生错误并停止工作，但 QA-MISRA 也可以检测到不妨碍编译器工作的错误。



- 跨多个模块的分析

QA-MISRA 识别链接器无法解决的不合规行为。整个项目中的外部对象和函数的递归以及相互矛盾的声明很容易被检测到。



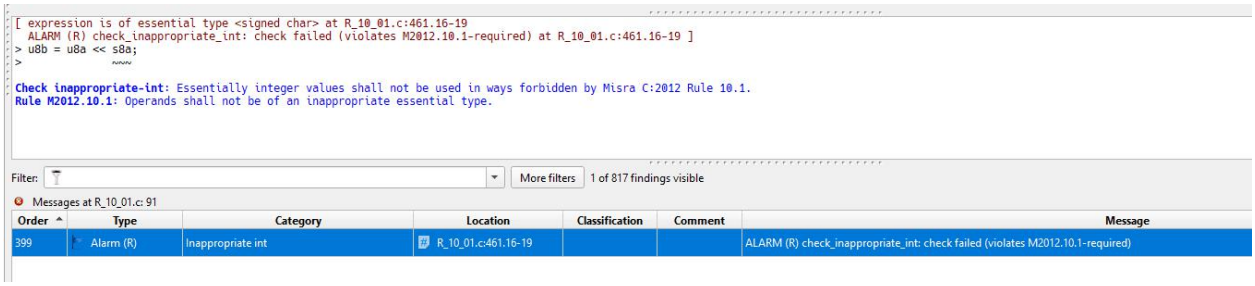
- 可移植性

QA-MISRA 促使代码在不同的编译器和平台之间保持一致，同时认识到标准的局限、语言扩展和实现定义的行为。

- 类型转换

QA-MISRA 确定数据类型之间的隐式转换（默认参数、整数提升、函数返回）。

EMAIL : contact@watertek.com
TEL : 010-82695188



- 冗余代码

QA-MISRA 检测未使用的变量、函数和参数以及结果不会改变的条件（始终为真或始终为假）。

- 语句和操作

QA-MISRA 可检测可疑的比较操作，包括使用不正确的类型，并可以发现会产生误解或难以理解和维护的结构，即使它们是允许使用的。

- 命名规范

QA-MISRA 通过正则表达式鼓励使用统一格式。所有标识符都可以检查。

对标准的符合性

QA-MISRA 的开发是与 MISRA 委员会专家密切合作的成果。如何理解和改进报告的 MISRA 违规行为？它为开发人员提供了全面的知识库和广泛的示例代码，帮助遵守 MISRA 标准。

- 未来趋势——内嵌的

无论软件开发市场走向何方，使用 QA-MISRA 的用户将始终处于领先地位。毕竟，作为“行业标准”，MISRA 的规则集将保持并加强其地位。

- 高度可配置性

QA-MISRA 的特殊之处：QA-MISRA 可以定制为在用户的开发环境中工作，具有高度可配置的 MISRA 合规性规则集，用于定义公司特定的子集以检查合规性。

- 更好的软件

QA-MISRA 通过有效检测代码中的错误、不一致性、过时功能和对标准的一般违反，确保用户的软件满足 MISRA 标准的严格要求。错误可以在成本效益仍然可以实现的阶段纠正。

- 更好的理解——一致性开发

QA-MISRA 确保用户的所有代码都符合 MISRA 规则。而且它有助于开发人员在软件中安全使用 C 和 C++语言同时满足 MISRA 标准。使用 QA-MISRA 开发的代码往往不那么复杂，因为单个开发人员和团队可以遵循一致的标准。

- 可测试、可维护和可移植

使用 QA-MISRA 创建的软件可以在开发的所有阶段进行测试。如果软件符合 MISRA 标准，那么代码的维护和移植就容易多了。

- 缩短上市时间

可以在非常早期的阶段可靠地识别和纠正错误，从而使用户能够更快地发布软件，而不会危及质量。

(一) 使用 QA-MISRA 促进 MISRA 合规性

符合 MISRA 的开箱即用代码：

- 帮助用户根据 MISRA 指南开发软件
- 适用于 MISRA 标准的完全集成环境
- 更好的代码，同时遵守标准规范
- 适用于所有安全关键软件行业
- 提升开发人员的专业技能并推广最佳实践
- 提高代码的可移植性和可重用性
- 在用户的开发环境中进行即时且可重复的测试

- MISRA C

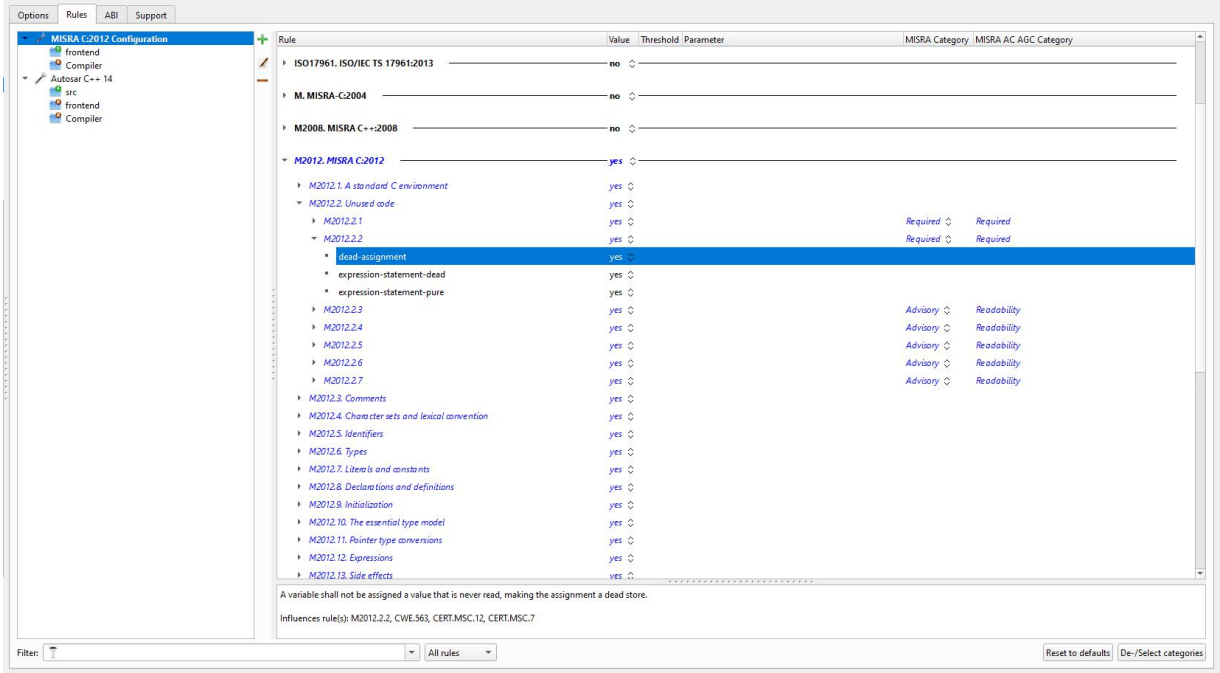
MISRA C 最初是为了满足 1994 年“车载软件开发指南”中确定的“标准化编程语言的限制子集”的需要而开发的，它的开发也反映了在汽车应用中使用 C 开发嵌入式软件的新兴要求。MISRA C 发布后，其与其他应用的相关性很快被注意到，随后的标准修订涉及来自不同行业和工具供应商的许多专家。今天，MISRA C 是使用 C 开发软件的事实上的标准，在这些软件中安全性、保全性和代码质量非常重要。MISRA C 的未来发展将继续扩展对语言的新版本和其他特性的支持。

- MISRA C++

认识到 C++在关键应用中的使用日益增加，MISRA C++最初发表于 2008 年 6 月。最近的工作是在修订本上开始的，2017 年 MISRA 宣布将把 AUTOSAR C++指南整合进新版的 MISRA C++中。MISRA 指南将结合最新版本的 C++语言——C++17——以及将来发布的 C++20。

- 更安全的 C/C++语言子集

所有编程语言（包括 ISO C 和 C++标准）都含有未经完全指定或定义的用法，对相同的语言结构不同的编译器有不同的实现。对安全关键的系统来说，MISRA 中的“建议（Advisory）”和“要求（Required）”类规则定义了 C 和 C++的一个更安全的子集，用以改善程序可移植性、安全性和保全性。这些子集合只是完整语言的一个受限版本，因此可以使用标准的商业现成工具链，同时提供更安全的程序，在不同环境中按照程序员的预期运行。



(二) 使用 QA-MISRA 促进 AUTOSAR 合规性

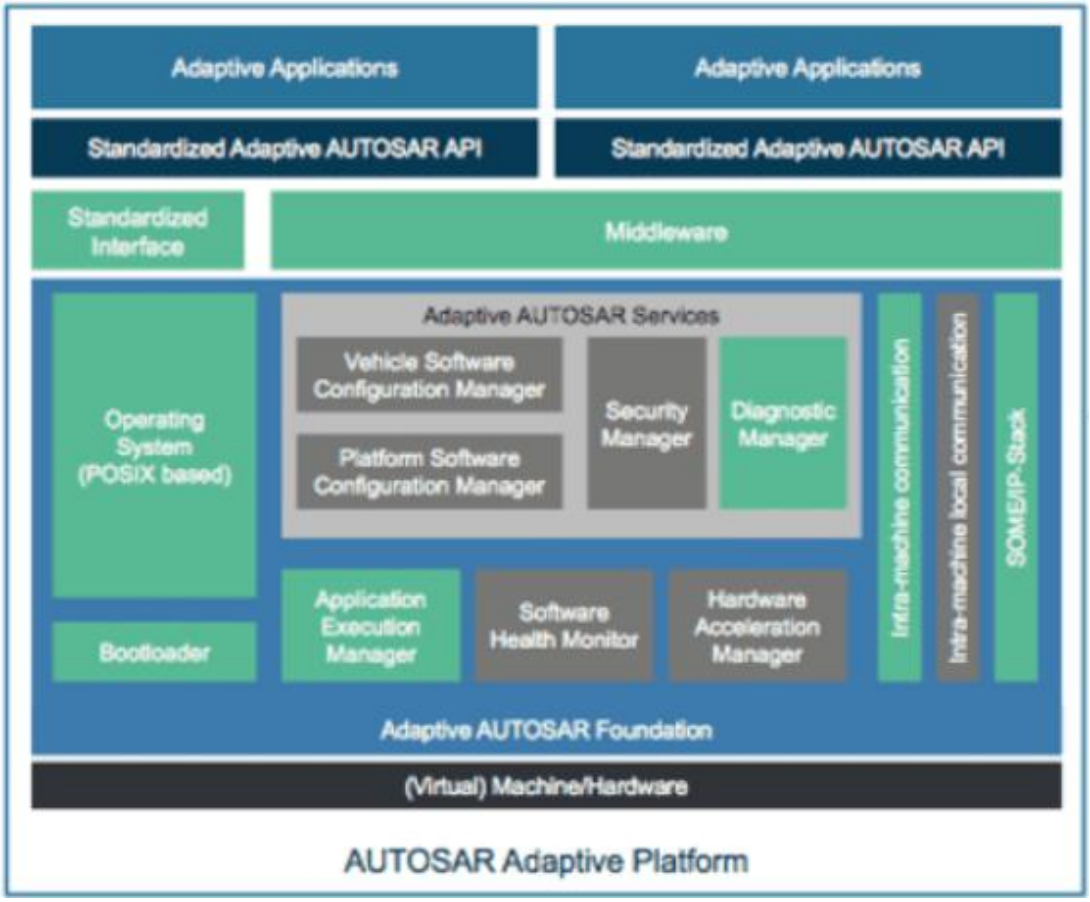
- 突出编程规则违背
- 报告未指定、未定义或编译器依赖的行为
- 清晰标记可能的运行时问题

● 用于自动和互联车辆技术的 AUTOSAR“自适应平台”

互联与自动驾驶技术正在快速大幅发展，这些变化要求对新的和现有的 ECU 软件平台都有全新的开发要求。

AUTOSAR 为高度自主和互联网连接的驾驶技术开发的新“自适应平台”标准有助于满足这些快速增长的市场需求。

推动自适应平台标准的一些技术包括：高性能 32-/64 位微处理器（带外部存储器）、并行处理、高带宽通信。



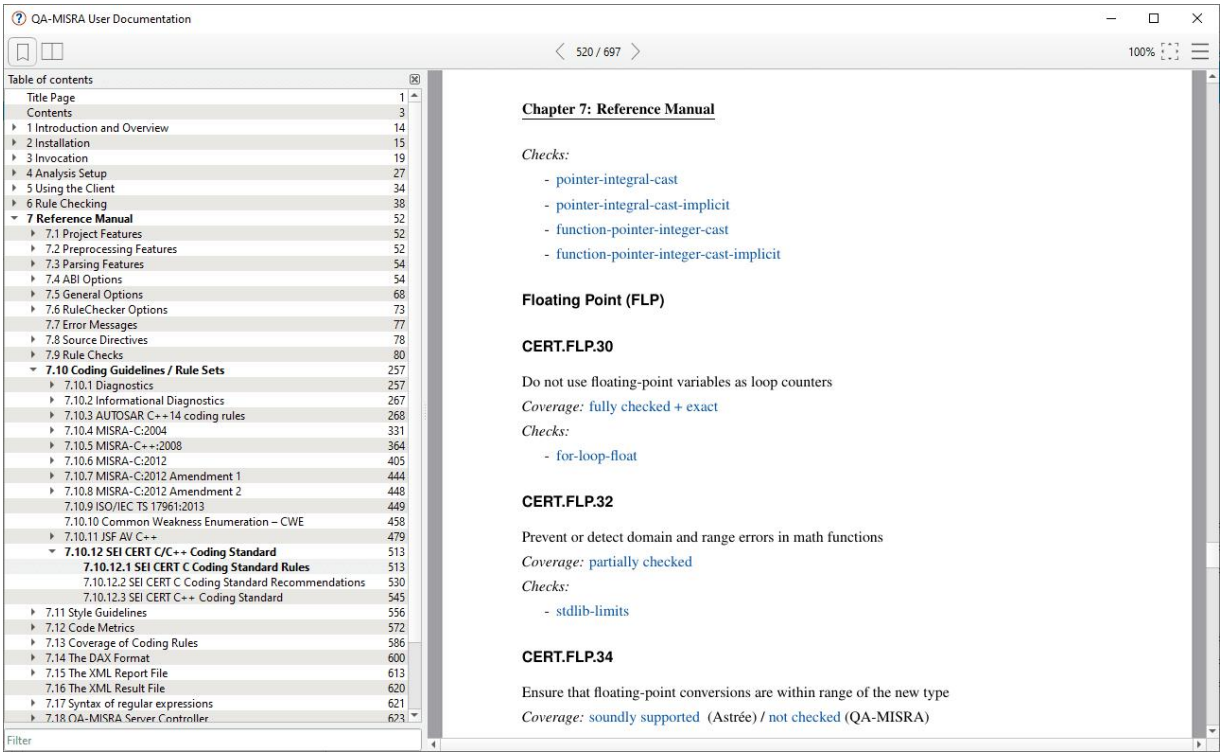
(三) 使用 QA-MISRA 促进 CERT C/C++合规性

通过将应用程序安全措施合并到用户的设计和编码过程中，实现一个严格的、可重复的、以安全为中心的开发过程。我们的自动化静态分析工具可帮助用户：

- 消除不安全的代码实践
- 消除未定义行为
- 避免经常被利用的漏洞
- 改善整体系统质量

- 什么是软件漏洞？

CERT 将漏洞描述为影响信息系统安全性的软件缺陷。该缺陷可能很小，因为它不会影响软件产生的性能或结果，但可能会被导致严重违反安全性的攻击所利用。CERT 估计，高达 90%的报告安全事件是由于利用软件代码或设计中的缺陷造成的。



(四)　使用 QA-MISRA 促进 CWE 合规性

CWE 提供了已知弱点的综合存储库，而 CERT C 安全编码标准确定了可能暴露软件弱点的不安全编码结构。

并非所有 CERT C 编码指南都直接映射到 CWE 中的弱点，因为某些编码错误可能以各种方式表现出来，而这些方式与任何给定的弱点都没有直接关联。同样，CWE 确定的并非所有弱点都存在于编码标准中，因为有些弱点与高级设计有关。

CWE 由一系列视图组成，如 dictionary 视图和 development 视图。CWE-734 视图列举了 CERT C 安全编码标准解决的弱点，包括 799 个 CWE 中的 103 个。如果开发者遵守 CERT 编码标准，他们可以完全或部分防止 CWE-734 中确定的弱点。

持续集成

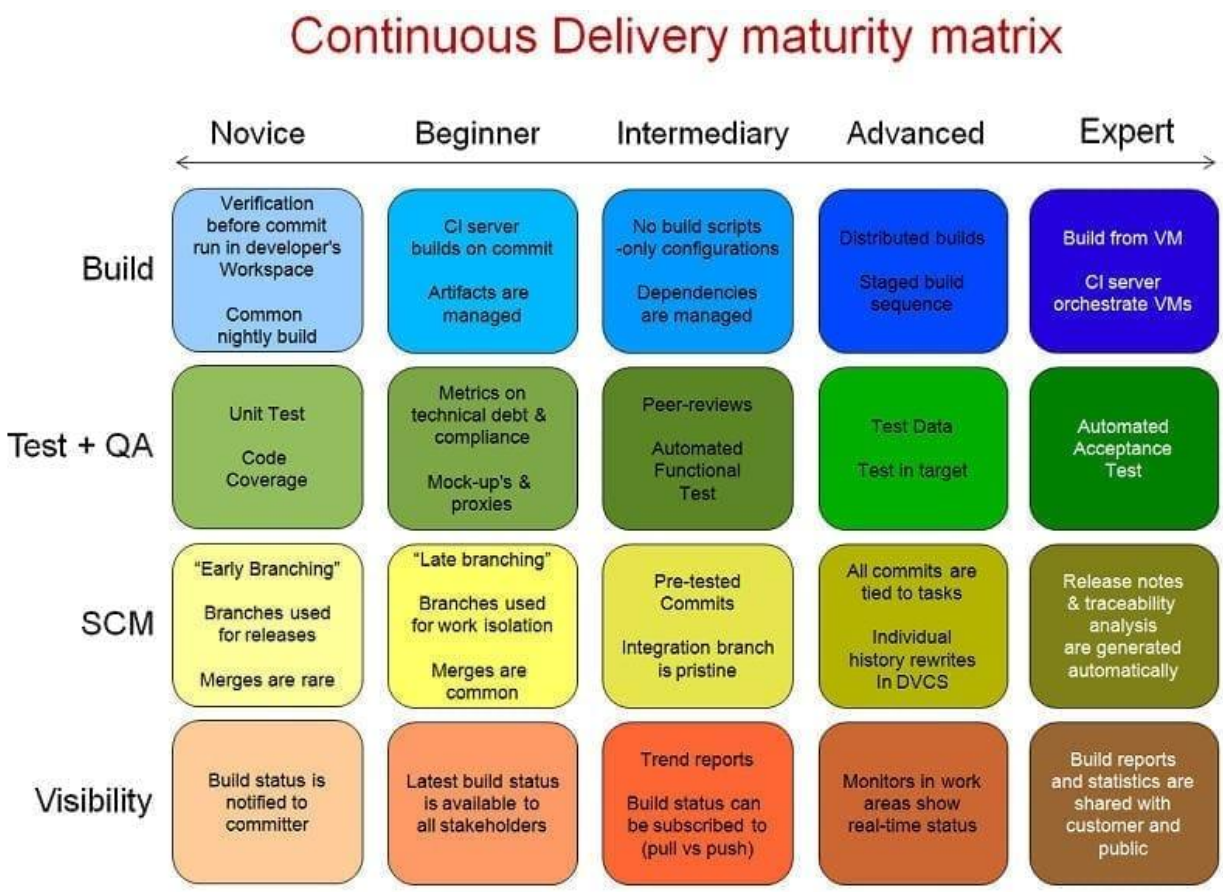
（一）什么是持续集成

持续集成原则鼓励开发人员和团队不断地共享和集成他们的所有贡献。

- 远离夜间构建的概念，转而接受连续构建的概念
- 远离政策执行，转而依靠质量执行

目标是获得对软件验证和软件依赖性的完全和自动化的控制，这样每个开发人员都有可能成为发布候选。

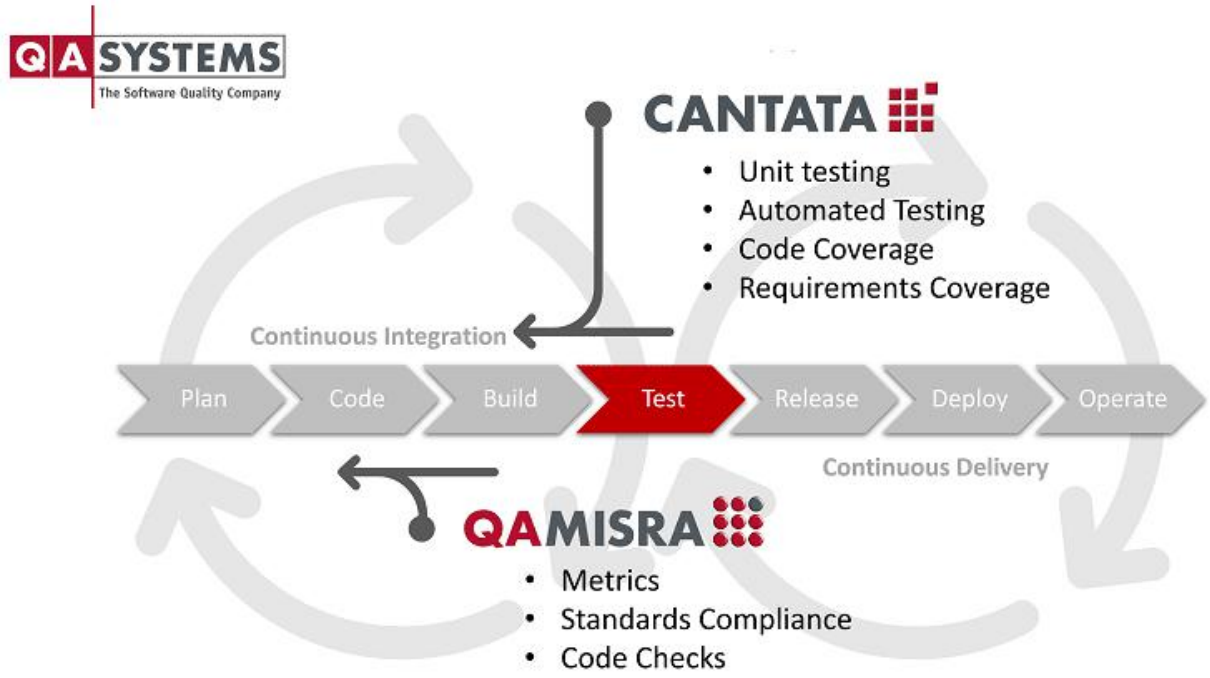
可以在命令行上运行测试工具，以便它们可以轻松地与许多 CI 工具集成。



（二）关键软件的以测试为中心的过程

QA-MISRA 和 CANTATA 一起支持验证代码的静态和动态方面。静态分析有助于在执行代码动态测试之前检测缺陷，节省时间。软件单元和集成测试验证正确的行为，以及不会发生不正确的行为，同时检查代码的执行路径和验证需求。每个阶段的自动化功能以及与 CI 构建系统和需求收集工具的可靠集成，将手动测试的需求降至最低。所

有这些加起来大大减少了缺陷，并通过在开发周期中更快、更早地识别问题节省了时间。



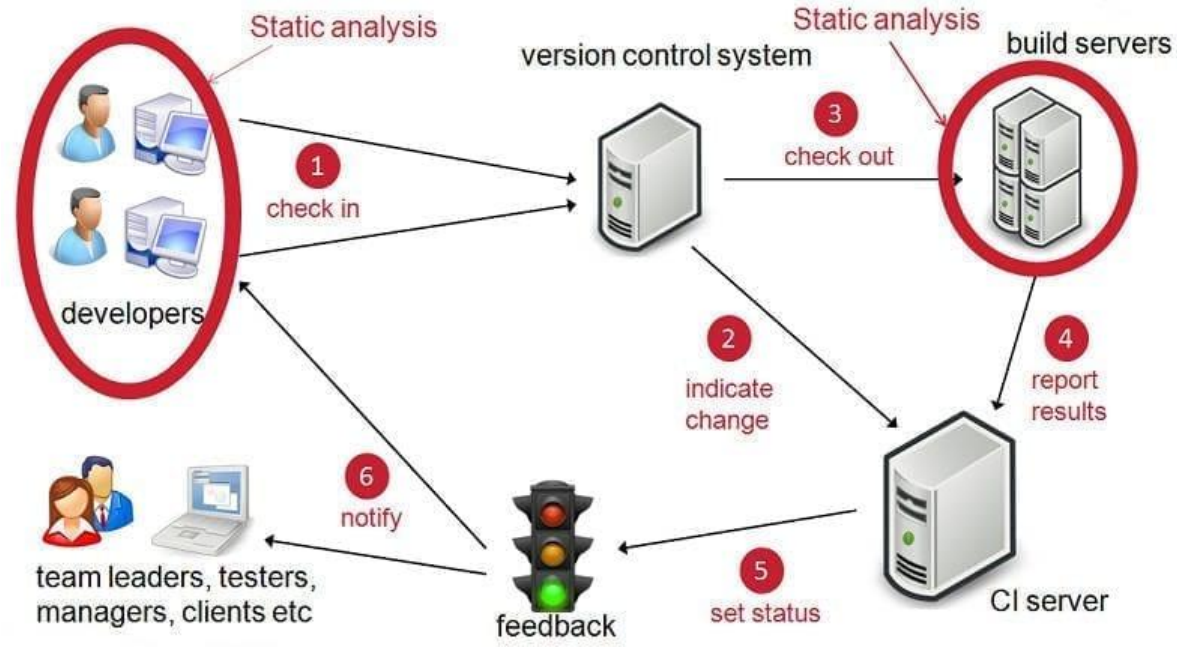
（三）Jenkins 插件

我们为静态分析解决方案倡导的“早期且经常”的方法显然与持续集成理念产生了共鸣，这种理念正越来越多地被作为软件质量的可靠方法采用。

Jenkins 插件将允许用户自动化启用的 C 和 C++项目的分析，将分析作为持续集成过程的一部分来执行。

该插件提供了一系列功能，包括：

- 自动检查每个 Jenkins 构建是否违反规则
- 直接在 Jenkins 工作区中归档分析报告
- 通过 Jenkins web 界面访问分析结果
- 根据用户的标准，根据分析结果自动将生成标记为错误
- 将不同版本的分析作为单独的分析修订版启动，以便于调试和记录进度



功能指标

主要利益

- 降低成本，同时缩短上市时间
- 降低程序失败的风险
- 在开发周期的早期识别编码问题
- 确保符合代码质量和编码标准
- MISRA 标准的完全集成环境
- 适用于需要安全关键软件的所有行业
- 加速并重新聚焦代码评审过程，并改进开发团队的协作
- 提升开发人员的专业技能并推广最佳实践
- 增强可靠性、可移植性和可维护性
- 提高代码的可移植性和可重用性
- 开发环境中的即时和可重复测试

EMAIL : contact@watertek.com
TEL : 010-82695188

主要特征

QA-MISRA 是一种静态分析器，旨在检查符合 C90、C99、C11、C18 和 C++98、C++11、C++14、C++17 语言规范的安全关键 C/C++程序的编码准则，计算代码度量。

- 快速易用
- 实施编码准则，包括 MISRAC:2004、MISRA-C:2012 和定制规则集
- 在句法规则上没有漏报和误报
- 与 Astrée 无缝集成，确保语义规则的零漏报和最小误报
- 代码度量的计算：HIS 度量和定制度量
- 强制执行度量阈值
- 报告的代码问题的完全可跟踪性
- 交互式结果探索
- 调查结果的稳健分类
- 可配置报告文件生成
- 项目进度和分析修订的跟踪和可视化
- 客户机/服务器体系结构，具有分析请求的队列处理，以及集中的用户管理和身份验证
- 具有开放接口和开放文件格式的独立工具
- MATLAB 集成与 TargetLink 耦合
- 根据安全标准进行自动工具合格审定

基本功能

- 命令行接口

EMAIL : contact@watertek.com
TEL : 010-82695188

- 交互式图形用户界面
- 在线帮助和 MISRA 知识库
- 概要和详细报告
- 集成到基于 Eclipse 的 IDE 中

代码分析功能

- 快速源代码分析
- 警报可根据注释进行分类
- ISO/IEC 9899:1990 (C90)
- ISO/IEC 9899:1999 (C99)
- ISO/IEC 9899:2011 (C11)
- ISO/IEC 9899:2018 (C18)
- ISO/IEC 14882:2011 (C++11)
- ISO/IEC 14882:2014 (C++14)
- ISO/IEC 14882:2017 (C++17)

持续集成环境

- Jenkins
- 其他 CI 环境可以通过命令行集成

支持的编程标准

- MISRA C:2004
- MISRA C:2012
- MISRA C:2012 修订 1&2

EMAIL : contact@watertek.com
TEL : 010-82695188

- MISRA AC AGC
- HIS Metrics
- ISO/IEC TS 17961:2013（C 安全编码规则）
- SEI CERT C 编程规范
- SEI CERT C++ 编程规范
- CWE
- MISRA C++:2008
- Adaptive AUTOSAR C++14
- 命名规范检查
- 可扩展的规则集

安全关键标准

通过使用“合格审定支持工具包”，QA-MISRA 支持以下安全标准：

- ISO 26262:2018（汽车电子）
- EN 50128:2011/A2:2020（轨道交通）
- EN 50657:2017（铁路轨道）
- IEC 62304:2006（医疗器械）
- IEC 61508:2010（工业自动化）
- DO-178B（航空航天与国防）
- DO-178C / DO-330（航空航天与国防）

系统需求

- Windows：64 位 Windows10

EMAIL : contact@watertek.com
TEL : 010-82695188

- Linux：64 位 CentOS/RHEL 7 或其他兼容发行版
- 4 GB RAM（建议使用 16 GB）
- 4 GB 存储空间

EMAIL : contact@watertek.com
TEL : 010-82695188