AUTOSAR 编码指南

简介

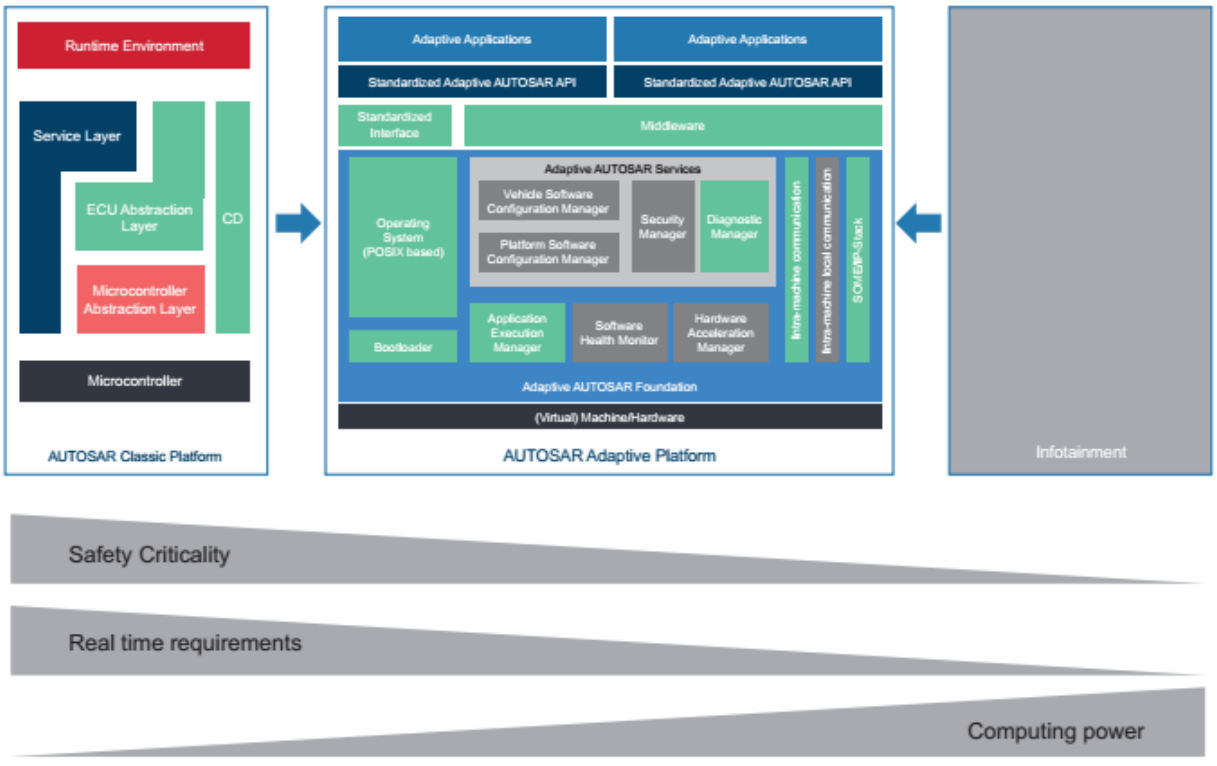
软件开发对汽车应用越来越重要。越发严苛的安全要求、环境要求和便利性要求，大大增加了车辆电子系统的数量。90%的技术创新都是基于软件驱动的电子部件。这些部件占汽车开发成本的 40%。发展的步伐以及整合更多功能和控制单元的持续性需求，对汽车制造商构成了重大挑战。本白皮书简要介绍了新的 AUTOSAR 编码指南，并就如何遵守这些指南提供了指导。

什么是 AUTOSAR？

AUTOSAR（汽车开放系统架构）旨在标准化和面向未来的基础软件元件、接口和总线系统，帮助汽车制造商管理不断增长的系统复杂性，同时降低成本。它为汽车电子控制单元（ECU）开发标准化的开放软件架构。

AUTOSAR 是由 180 多家汽车制造商、汽车供应商、工具供应商和半导体供应商组成的合作伙伴。 核心成员是：宝马、博世、大陆、戴姆勒、福特、通用、标志雪铁龙、丰田和大众。

AUTOSAR 开发的第一个开放架构是“经典平台”，针对车辆功能，具有严格的实时要求和安全关键性，在基本的微控制器上实现。现在，为了满足快速增长的联网车辆和高度自动化驾驶技术的市场需求，AUTOSAR 开发了一种新的联网和自动驾驶车辆的“自适应平台”标准。驱动自适应平台标准的技术的例子是：具有外部存储器的高功率 32/64 位微处理器，并行处理和高带宽通信。



根据自适应平台标准开发的软件可以和根据“经典平台”标准开发的现有系统集成。

经典平台明确允许用 C、C++和 Java 实现，但 C 是主要的编程语言。现在，自适应平台中的 API 是用 C++定义的，表明 AUTOSAR 将 C++视为新型自适应平台组件的首选语言。

C 和 C++是用于汽车嵌入式系统的主要编程语言。这在很大程度上是因为它们允许对硬件进行直接的、确定性的控制，并给予开发人员灵活性。这也带来一定的风险。具有未定义行为的代码，或者是当编译和运行在不同目标硬件上时其行为难以确保相同的代码，是能够得到编译的。即使是最有经验的开发人员也可能会无意中引入缺陷。

什么是 AUTOSAR 编码指南？

为了帮助确保 AUTOSAR 软件实现代码的安全性和保全性，AUTOSAR 邀请 Perforce Software 成为开发合作伙伴，并加入工作组开发“关键和安全相关系统中使用 C++ 14 语言的指南”（简称“指南”）。作为 AUTOSAR 静态分析开发的独家合作伙伴，我们贡献了我们在过去 30 年中获得的关于 C++编程语言和软件开发最佳实践的专业知识。

AUTOSAR 指南规定了 342 条编码规则。其中 154 个直接使用了已被广泛采用的 MISRA C ++标准； 131 个基于其他众所周知的编码标准中定义的规则，比如 Helix QAC 的 High Integrity C++；57 个是基于其它研究或资源。指南允许一些以前的标准所禁止的语言特征，例如：动态内存、异常、模板、继承和虚函数，当然另有规则来确保这些语言功能只能以安全的方式使用。

AUTOSAR 开发的原则之一就是验证规范与标准化。自适应平台通过 AUTOSAR 内部实现进行验证，内部实现以 C++编写，被称为自适应平台验证机（Demonstrator）。 AUTOSAR 使用了来自独

家静态分析开发合作伙伴 Perforce Software 的先进分析工具 Helix QAC，以确保验证机源代码的质量，并验证符合编码指南。

为什么需要 AUTOSAR 编码指南？

在 AUTOSAR 指南之前，在安全关键型软件中没有适用于现代 C++标准（C ++ 11 和 C ++ 14）的的编码标准。可用标准要么是不完整的、针对传统 C++标准编写的，要么是不适用于安全关键的应用程序。 MISRA C ++:2008 是汽车行业中最广泛使用的 C++编码标准，但它是为 C++ 03 编写的，而 C++03 已经过去了 15 年。

自引入 C++ 03 以来出现的如下许多变化降低了 MISRA 标准对于 AUTOSAR 项目的相关性：

1. C++的发展
2. 编译器的改进
3. 测试、验证和分析工具的改进
4. 车辆功能安全标准 ISO 26262 的发布
5. 将更广泛的安全和保全专业知识融入其他标准中，例如：
   - High Integrity C ++（Perforce Software）
   - 联合打击战斗机 C ++（洛克希德马丁公司）
   - CERT C ++（卡耐基梅隆）
   - C++核心指南（Bjarne Stroustrup 和 Herb Sutter）

AUTOSAR 设计的指南被用作现有 MISRA C ++标准的扩展。它规定了新的规则和 MISRA 规则的更新，并指出哪些 MISRA 规则已经过时。

谁使用 AUTOSAR 编码指南？

指南的“目标”章节指出：“主要的应用领域是汽车，但也可以用于其他嵌入式应用领域...。AUTOSAR C ++14 编码指南面向的是在 32 位和 64 位微控制器上提供了高效全面的 C++ 14 语言支持、使用 POSIX 或类似操作系统的高端嵌入式微控制器。”

因此，Perforce Software 建议任何使用 C++ 14 开发嵌入式软件的组织都应该考虑使用这些指南。

如何保证代码符合 AUTOSAR 指南？

传统方式下，工程师进行费力的手动代码审查，以确保代码是按照他们选择的标准编写的。这个过程很容易出错，也不适合处理当今庞大而复杂的代码。幸运的是，这些检查现在可以使用工具自动进行。“静态分析器”就是为此设计的一种工具。静态分析器不仅报告违反编码规则，而且执行深入的代码检查以突出显示任何未定义的、未指定的或与编译器相关的行为。它分析程序

的所有可能的执行路径来标记潜在的运行时问题。通常情况下，它可以发现测试活动发现不了的问题。静态分析器是用于开发安全、保全和可靠软件的工具集的重要组成部分。

AUTOSAR 使用 Perforce Software 的静态分析工具 Helix QAC 来确保其验证机源代码的质量，对编码指南的遵守也提供了宝贵的见解。 这些见解结合 Perforce Software 对指南的贡献，为开发符合 AUTOSAR 标准唯一静态分析解决方案奠定了基础。

Perforce Software 的 AUTOSAR 适应性模块对 Helix QAC 进行了扩展，以获得符合 AUTOSAR 指南的开箱即用。对于大中型开发团队来说，通过 Perforce Software 的代码质量管理控制中心 QA • Verify，该解决方案可以进一步增强。 这保证了所有团队成员在项目期间除了跟踪和报告代码质量外，还一致地应用编码规则。

总结

AUTOSAR 标准将作为未来汽车应用实施的平台，最大限度地减少当下功能域之间的障碍。为达此目的，标准将使功能和功能网络映射到系统中的不同控制节点，几乎独立于相关的硬件。这些指南虽然是针对汽车行业开发的，也可以被任何使用 C++ 14 开发嵌入式软件的组织或部门使用。在任何应用程序中，使用 Perforce Software 静态分析工具 Helix QAC 将确保代码没有错误，并且符合编码准则。

关于旋极信息

北京旋极信息技术股份有限公司（以下简称“旋极信息”）成立于 1997 年，于 2012 年上市（股票简称：旋极信息，股票代码：300324），现注册资本 11 亿元，公司总部位于北京市海淀区永丰产业基地，在上海、西安、成都、深圳、杭州等拥有 30 余家分子公司。

公司主营业务围绕“智能防务、智慧金融、智慧城市、大数据”四大板块紧密开展。公司为首批通过国家军用标准 GJB9001B-2009 武器装备质量体系认证、武器装备生产许可证、装备承制资格审查认证的民营企业，具备二级保密资格资质等。

公司在现有保障体系下，以北京旋极信息总部为中心，以上海、成都、深圳、西安、沈阳、郑州、南宁等公司基地为支撑，采用“统一指挥、统筹调配、就近保障”原则，为用户提供及时、快捷的售后服务保障。