适航认证中的目标码覆盖率分析工具VerOCode

VerOCode for Airworthiness Certification

北京旋极信息技术股份有限公司　任建国

任建国

2000 年至今就职于北京旋极信息技术股份有限公司，现任职软件测试技术经理，负责软件测试的开发、维护及技术支持工作，曾参与神州飞船某测试项目、某研究所 GJB5000A 管理平台搭建与培训、航空某适航测试项目等。

监控和测试程序（测试控制和被测单元）在 PPC 目标机上执行，覆盖率在机器码级获得。由于目标系统提供 printk 函数，可在串口打印数据输出，通过超级终端或其他串口监控程序获得数据结果。一个测试运行以后，收集的覆盖率数据通过串口上传到宿主机来分析。

在 DO-178B 6.4.4.2 中要求：“覆盖率分析可以在源代码上开展，对于 A 级软件并且编译器产生的目标代码不能直接追踪到源代码的语句，那么需要对目标码进行额外的验证工作以确保产生的代码序列是正确的。”

这里提到的“基于目标码的额外验证工作”可以由目标码覆盖率分析来实现，即编译器在编译过程中在目标码中添加了额外的代码，可以通过目标码覆盖率分析发现这部分代码，并且可以建立源代码与目标代码之间的关系。而源代码覆盖率方法由于进行了代码插装，测试的对象已经改变了，无法对编译器多添加的代码进行验证。在国外的适航认证经验中，目标码覆盖率分析已经得到广泛的使用，并且被适航认证局所认可。

关于目标码覆盖

1 目标码覆盖的出处

目标码覆盖的概念和要求在 RTCA/DO-178B 标准中明确提出，相关内容摘录如下：

6.4.4.2 结构覆盖分析

结构覆盖分析的目的是确定在基于需求的测试过程中，哪些代码结构没有被执行。基于需求的测试用例可能没有完全执行所有的代码结构，因此需要进行结构覆盖分析，并要求进行覆盖分析验证。

结构化语言的覆盖分析可以在源代码级别进行。但是如果是 DO-178B A 级软件并且编译器产生的目标代码不能直接追踪到源代码中的语句，那么验证工作就需要采取额外地分析方法，即在目标代码的级别上验证编译器产生的代码序列的正确性。在目标代码中的数组边界检查就是编译成生成（compiler-generated）的不能直接追踪到源代码的目标代码的一个实例。

进行目标码验证的原因

（1）测试充分性要求。

目标码的验证关心编译器产生的目标码的控制流结构有多少与源代码不一致。这些不一致产生的原因有许多，如：编译器的解释、优化

等。然而，传统的结构化语言的覆盖率技术使用的是源码级的，尽管在处理器上执行的是目标码，二者之间控制流结构的不同在测试过程中会产生重大的差距。

MISRA C:2004 认为 C 程序设计中存在的风险可能由 5 个方面造成：程序员的失误、程序员对语言的误解、程序员对编译器的误解、编译器的错误和运行时的错误。

（2）程序员对编程语言和编译器的误解。

编译器的行为不符合程序员的想法。很多高级语言标准特别是工业级语言标准的定义并不精确。如果一个语言的某些特征是不完全定义的，或者说是歧义的，那么就可能出现程序员的意思与编译器的解释不一致的情况。所以对于不同的编译器，相同的源代码其行为可能不同；同一个编译器，其行为也可能因为上下文的不同而不同。

（3）编译器的错误。

语言的编译器本身是一个软件工具，它编译代码并不总是正确的。例如可能在某些情况下它没有遵守语言标准，或者它本身就有错误。随着编译器验证技术的不断发展，越来越多的编译器问题被暴露出来。

针对嵌入式软件，由于运行资源有限，有时编译器产成的代码本身并没有问题，但仍然会导致系统失效。

关于编译器验证

由此可见，对于高级语言程序，编译器经常会引入风险。

对编译器进行验证是保证其正确产生目标码的最直接的方法。然而，目前对编译器的完全验证还存在非常困难的技术问题。编译器是一种特殊的系统软件，编译器的输入和输出都是应用软件或系统软件。编译器的这个特殊性和编译器本身结构的复杂性，使得编译器的测试验证面临着巨大的挑战。目前，关于编译器的验证问题已经有广泛的研究，例如编译器使用的主要算术逻辑的验证、算术表达式的验证、编译器结构的验证等。但这些编译器的验证方法都比较复杂，实用性和灵活性也不强。此外，编译器验证软件的价格昂贵，编译器验证的效果难以估计，一般的软件开发单位也不会出资进行编译器验证。

在不能完全信赖编译器的情况下，进行目标码验证是唯一的选择。

最佳解决途径

美国 Verocel 公司专门为安全关键软件领域中适航认证提供专业技术和服务。其服务包括开发、评审软件计划和标准、软件需求和测试开发、软件结构覆盖率分析、生命周期数据可追踪性，以及外包支持，主要客户包含波音、Windriver 等。Verocel 公司在为客户进行适航取证过程中，专门开发了一系列的工具以提高适航资料开发的效率，包括：

- VeroTrace：需求及生命周期追踪工具，管理认证可追踪性数据的产生和评审。
- VerOSource/VerOSourceA：源码级覆盖率验证工具，通过插装的方法验证被测试代码的语句、分支、MC/DC 覆盖率。
- VerOCode：目标码验证工具，允许在不插装源代码或使用特殊硬件的情况下，在目标计算机的目标代码级测试结构覆盖率。
- VerOLink：验证目标链接工具，帮助满足 DO-178B 的控制目标。
- VerOStack：验证目标程序运行时最差堆栈情况。

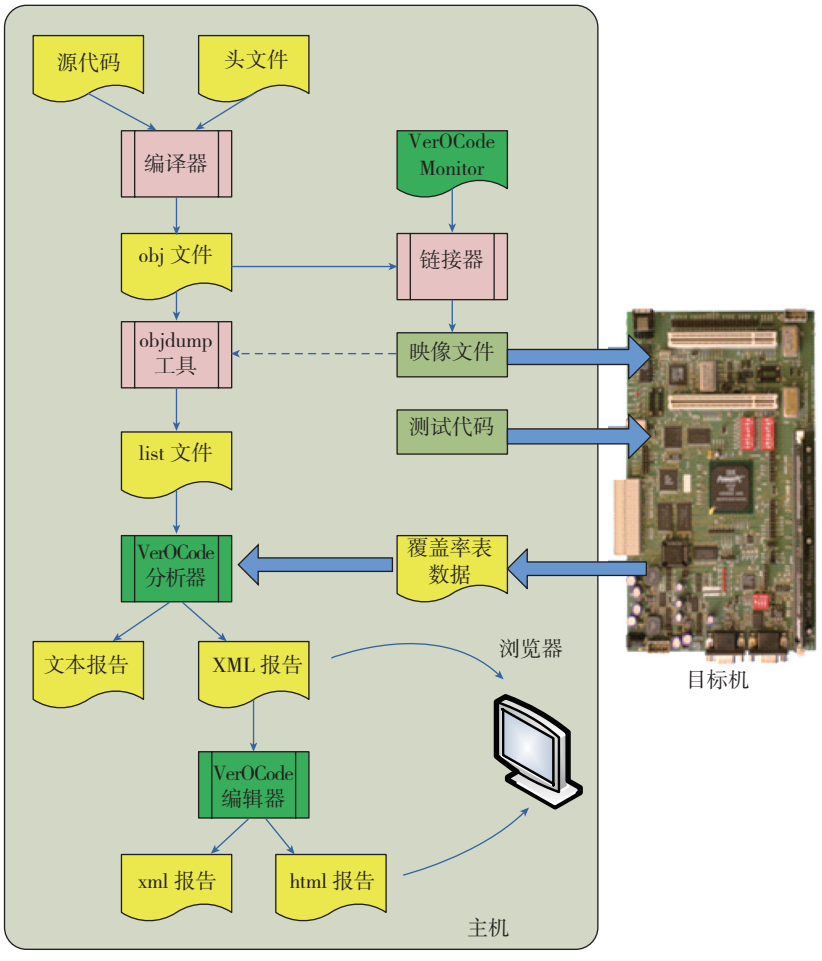

图1 VerOCode在Host-Target模式下的工作流程

其中，VerOCode 是目标码覆盖率分析工具，VerOCode 不需要特殊硬件，被测试的代码也不需要插装。应用代码在目标计算机（例如 PowerPC）上执行，执行的数据图表收集到一个宿主机上（PC）。VerOCode 使用收集的执行数据图表与链接器符号信息和编译器产生的清单一起，可以显示出哪些指令执行了，哪些指令没有执行，以及条件指令执行过程中的分支条件代码状态。产生的 VerOCode 结果清单包含了 DO-178B A 级，适航认证最高级别的安全性要求所要求的目标码覆盖覆盖率分析的证明。

VerOCode 已成功实施到国内某航空总体所的实际项目之中，针对 PPC 裸板应用和使用 DeltaOS 的 PPC 板应用，VerOCode 实现了目标码级的覆盖率分析。

VerOCode 记录和显示被测试程序中执行的目标码指令。对于条件指令，VerOCode 显示每次指令执行时的条件代码的状态。VerOCode 工作在 Host-Target 模式，其工作流程如图 1 所示。

监控和测试程序（测试控制和被测单元）在 PPC 目标机上执行，覆盖率在机器码级获得。由于目标系统提供 printk 函数，可在串口打印数据输出，通过超级终端或其他串口监控程序获得数据结果。一个测试运行后，收集的覆盖率数据通过串口上传到宿主机来分析。测试数据格式以字母 H 作为开头行，D 行和 Z 行交替出现作为数据行，T 行作为结束行。

VeroMon.o 监控程序要求必须运行在系统态（supervisor-level），它要调用 mfmsr 等特权指令读取寄存器状态。同时被测试系统的剩余内存分配必须满足 VeroMon.o 的内存要求：

.text - Monitor's code (approx. 5KB)；

.data - initialized data (approx. 1KB)；

.bss - coverage data table (256 KB, global symbol coverageDataTable).

对于 PPC 裸板应用，VerOCode 提供的 Monitor 代码不需要做任何定制即可实现目标码覆盖的验证，并通过目标板下载程序运行，得到详细的目标码覆盖率报告。

对于使用国产 DeltaOS 操作系统的 PPC 板，由于 RTOS 控制了目标板的所有硬件资源，通过分析其 RTOS 的硬件 Vector 列表，重新对 Monitor 进行定制，实现 VerOCode 代码与 DeltaOS 代码的兼容，从而实现了航空专用嵌入式操作系统“道 DeltaOS”的支持。

由于 VerOCode 完全满足客户的目标码验证要求，该所购买了多套 VerOCode 投入到实际的测试项目之中，满足了该所 A 级软件对于目标码覆盖率分析的需求。

关于适航认证

当前我国正在大力推进大型商务飞机的开发，国产大型客机 C919 将在 2014 年首飞，2016 年交付。参与大型客机开发的各级设备制造商需要在 C919 取得整机适航认证之前对其设备进行适航取证的工作。适航认证对设备研制单位而言是一个巨大的挑战，与传统的开发过程相比，要达到适航要求的软硬件开发所投入的费用将会是 2~5 倍。按照国际上的工程经验而言，适航所带来的额外工作量是原来的 2~4 倍，最短周期为 2 年。适航认证过程如图 2 所示。

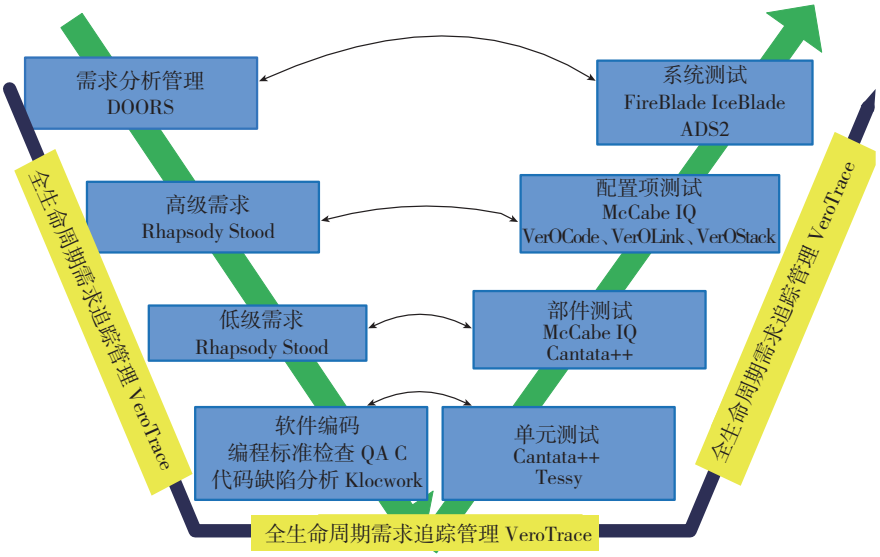

图2 适航认证过程

国外的先进做法是采用适航取证工作整体外包的方式，由在适航取证方面拥有丰富的专业公司对其提供的软件进行适航资料的开发和认证，这样可以达到让软件开发单位更专注于产品的实现。美国 Verocel 公司在适航认证领域拥有很好声誉，其管理层在安全关键软件验证和认证材料开发方面拥有超过 20 年的丰富经验。公司中三人是 DO-178B、DO-178C 和 DO-297 特别小组的成员，承担了多项 FAA 关于操作系统认证、IMA 架构验证方法的研究课题，与 FAA 和 EASA 关系密切。Verocel 也开发了一些能够提高认证资料开发效率的专业工具。

旋极公司作为长期服务于航空航天等领域的本土软件公司，已联合 Verocel 公司为国内航空工业研制单位提供完善的 DO-178B、DO-178C、DO-297 适航认证资料开发服务，并提供适航认证咨询。（责编 夏宛）