面向目标平台的高可靠、高安全软件测试方案

——软件时间、空间复杂度测试方案

挑战

随着机载嵌入式软件规模的大幅增加，越来越多与安全强相关的关键软件被应用于机载系统，以实现预期的飞行器功能，另外一方面，由于经济性和盈利的压力，许多工程组织被要求以更少的投入完成更多的事，再加上开发方式的丰富（基于模型设计工具和各种自动代码生成工具）等，使得软件生命周期验证变得更为复杂。因此，尽早消除软件生命周期引入的错误，保证软件生命周期阶段输出产物的可靠性和标准符合性显得尤为重要。

另外，严格的行业标准对测试进程的准确性、规范性和完整性的要求越来越高，如何能够在保证测试质量的同时，加快测试的进程成为一个亟需解决的问题。

软件验证目标

适航标准将软件等级分为 A-E 五个等级，软件级别与软件失效可能导致的最严重的系统安全性影响程度相对应，不同等级的软件，需满足的目标也不尽相同。D 级软件需满足 28 个软件目标、C 级软件 57 个、B 级软件 65 个、A 级软件 66 个。其中，RVS 系列工具能够帮助客户完成对软件编码和集成过程输出结果的验证、软件集成过程输出结果的测试和软件验证过程输出结果的验证，主要目标包括：

- 源代码准确并且一致

在检查源代码时，需要对如下情况进行重点检查，包括堆栈的使用、内存的使用、定点运算的溢出、浮点运算、资源竞争和限制、最坏情况运行时间、异常处理、使用非初始化变量、缓存区管理、未用变量、任务或中断冲突导致的数据冲突等，来保证源代码的准确性和一致性。

- 可执行目标代码与目标计算机兼容

可执行目标代码就是将目标代码连接后形成的可执行文件，属于二进制代码。该目标是要验证可执行目标代码与目标计算机的兼容程度，可通过执行软硬件集成测试来实现。

- 完成对高级需求/低级需求的测试覆盖

这里所谓的测试覆盖包括基于需求的测试覆盖和结构测试覆盖。本目标要求针对软件高级/低级需求设计测试用例，保证每个软件高级/低级需求都对应有相应的测试用例，并且对应的测试用例完全覆盖了高级/低级需求中的全部功能。

- 完成对软件架构（修正条件/判定覆盖）的测试覆盖
- 完成对软件架构（判定覆盖）的测试覆盖

- 完成对软件架构（语句覆盖）的测试覆盖
- 完成对软件架构（数据耦合和控制耦合）的测试覆盖

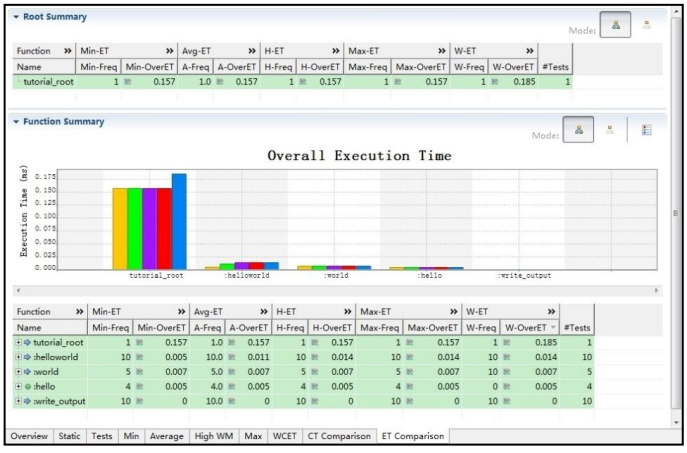
面向目标平台的软件验证解决方案

Rapita Verification Suite（简称：RVS），为英国 Rapita Systems 公司提供的一套针对嵌入式软件目标平台测试工具。RVS 可以对软件的时间性能（WCET）进行全面的测试分析及验证，广泛应用于具有高可靠性要求的软件中，支持多种目标硬件上的动态测试。其产品符合 ISO-26262、DO-178B/C、IEC-61508 等行业规范要求，兼容 Vxworks、AUTOSAR 操作系统，支持 C、C++、Ada 多种语言，全方位支撑 PowerPC、Intelx86、ARM、Infineon 等主流处理器。

1、软件性能评估工具箱-RapiTime

RapiTime 能够进行软件时间性能的测量，通过分析得出最差执行时间数据，并为代码优化提供指导，其主要功能如下：

- ▼ 检查不同的函数对于最差、最优以及平均执行时间的影响
- ▼ 通过大量调用来查看执行时间的变化
- ▼ 对于函数自身的上下文、循环以及数据块进行分析
- ▼ 定位产品的性能瓶颈
- ▼ 可视化的显示每个函数对最差情况执行时间的影响
- ▼ 检查最差情况的出现频率
- ▼ 识别代码在最差情况下的执行路径
- ▼ 显示由于硬件性能不同对于执行时间的影响

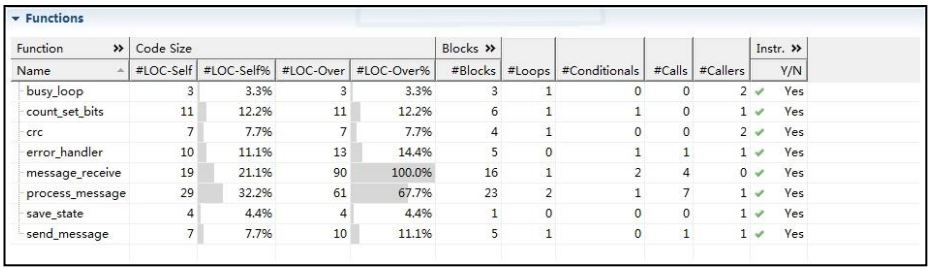


2、软件覆盖率分析工具箱—RapiCover

RapiCover 是一款基于目标硬件的嵌入式软件的测试覆盖率分析工具， 针对所使用的测试用例给出对应的现场测试覆盖率信息，其插桩点的开销极小，并能针对目标板的实际情况

提供灵活的支持方式。其主要功能如下：

- ▼ 支持 C、C++、Ada 编程语言
- ▼ 极小的时间开销
- ▼ 语句覆盖，变量定义、条件判断或循环
- ▼ MC/DC 覆盖、功能覆盖、调用覆盖
- ▼ 与 MATLAB/Simulink 无缝集成，可便捷集成 SIL/PIL/HIL 环境中
- ▼ 提供 DO-178B/C Ki



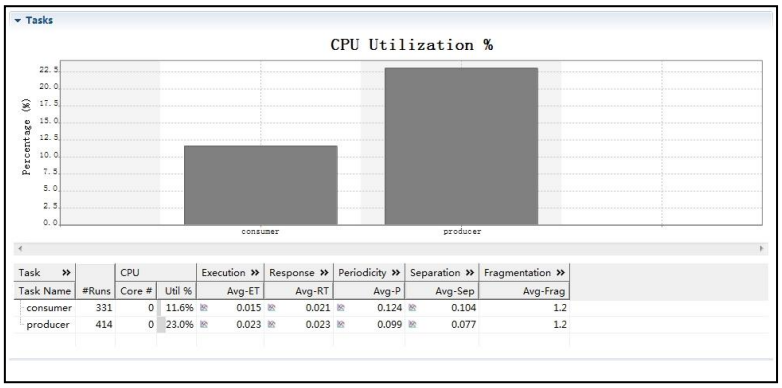
Functions

Function	Code Size				Blocks					Instr.
Name	#LOC-Self	#LOC-Self%	#LOC-Over	#LOC-Over%	#Blocks	#Loops	#Conditionals	#Calls	#Callers	Y/N
busy_loop	3	3.3%	3	3.3%	3	1	0	0	2	Yes
count_set_bits	11	12.2%	11	12.2%	6	1	1	0	1	Yes
crc	7	7.7%	7	7.7%	4	1	0	0	2	Yes
error_handler	10	11.1%	13	14.4%	5	0	1	1	1	Yes
message_receive	19	21.1%	90	100.0%	16	1	2	4	0	Yes
process_message	29	32.2%	61	67.7%	23	2	1	7	1	Yes
save_state	4	4.4%	4	4.4%	1	0	0	0	1	Yes
send_message	7	7.7%	10	11.1%	5	1	0	1	1	Yes

3、软件多任务调度分析工具箱—RapiTask

RapiTask 为复杂的嵌入式系统提供了可视化的操作系统的调度和事件跟踪。RapiTask 可以通过 RapiTime 的接口，进行对软件时间问题进行详细审查。其特点如下：

- ▼ 定位不常见的时间的事件，比如竞态条件
- ▼ 定位多任务和多核系统的系统容量和负载问题，消除系统集成风险
- ▼ 支持多个目标系统，而不是绑定到一个特定的操作系统



Task		CPU		Execution	Response	Periodicity	Separation	Fragmentation
Task Name	#Runs	Core #	Util %	Avg-ET	Avg-RT	Avg-P	Avg-Sep	Avg-Frag
consumer	331	0	11.6%	0.015	0.021	0.124	0.104	1.2
producer	414	0	23.0%	0.023	0.023	0.099	0.077	1.2

总结

面向目标平台的软件测试，是软件测试的难点，尤其是对软件最差运行时间和软件覆盖度的检查，RVS 工具可以以最简单的打桩方式，使软件能够面向目标平台进行性能测试，并且可自动生成检查报告，有效的解决了测试中的难题，为高可靠软件开发提供了保证。

RVS 工具提供 DO-178B/C 相关认证包，可以对该工具进行工具鉴定。

1、部分客户列表

2、用户案例

- ▼ 巴西航空工业公司使用 RVS 工具为飞控系统 Level A 级软件进行最差运行时间分析，为 DO178B 适航认证提供素材。
- ▼ Alenia Aermacchi 公司，使用 RVS 工具为 M-346 飞机软件进行最差运行时间分析，节省了 10%的测量时间，并且检查结果可信度更高。