Validation Suites vs. Validation Kits

A Side by Side Comparison

Validated Software Corporation (VSC) offers a set of turnkey certification products for Micrium's µC/OS real-time operating system (RTOS) that are collectively known as "Validation Suites". Each of the individual Validation Suites is specific to a market(s) and standard(s). VSC released the first Avionics DO-178B (Level A) Validation Suite for µC/OS in 1999.Today our µC/OS verification, validation and certification products are used in many different market segments:

- Avionics Equipment
- Automotive and Hybrid Vehicles
- Rail and Transportation
- Industrial Process and Measurement
- Medical Devices
- Oil and Gas

Introduction to Validation Suites

Validation Suites contain all software development life-cycle documents, test results and essential evidence demonstrating that the µC/OS kernel embedded in your hardware meets the strict standards, requirements and objectives set forth in the applicable standard(s).

Independent of the actual requirements of the application for which they are used, Validation Suites are developed and tested to meet the highest Level, SIL or Class defined by: IEC 61508, IEC 62304, EN 50128, DO178C, etc.

Comprehensive Unit and Integration Testing provide:

- 100% Feature/Function coverage
- 100% Statement coverage
- 100% Decision coverage
- 100% MCDC coverage (Avionics)
- 100% Object Code coverage

For more details on what artifact types are included in a Validation Suite, Table 1 has a generic listing of the highlevel artifacts that are included in our RTOS Validation Suites.

Because a Validation Suite is the design, development, and test artifacts for an RTOS like µC/OS as it is actually embedded in the hardware, Validation Suites share many of the attributes of RTOS. They have artifacts that are independent of the hardware and therefore apply to all processor architectures. Validation Suites also have artifacts that are created in support of the unique RTOS hardware abstraction layer (AKA Port) for the processor.

Core Validation Suite

While it is important that the port software for one's processor exists, it is the RTOS APIs and services that bring value to the application developer's efforts. The benefits are many:

- it is a cost effective alternative to monolithic executive loops that aid in reducing complexity of the application code
- it abstracts the application code from the realities of the underlying hardware
- it promotes modular software designs which in turn makes it easier to reuse both during a project as well as follow on projects
- it increases the predictability of new code or modifications to existing application code

- it makes code easier to test and to debug application code

Similarly, the bulk of the value contained in a Validation Suite is contained in the Core Validation Suite (Core VS). The Core VS corresponds to RTOS source code i.e. APIs and services and embodies 90% or more of the total effort involved in creating a complete Validation Suite. The Core VS is defined by two characteristics, the version of RTOS source code it applies to, and the development standard that it complies with. Continuing with the analogy from above, the Core VS is the design, development and test artifacts for RTOS prior to its instantiation on a specific processor. Because the Core VS corresponds to the RTOS source code and that source code is abstracted from the underlying hardware, the Core VS is also is independent of the hardware. Once it is created it supports the RTOS certification on any processor.

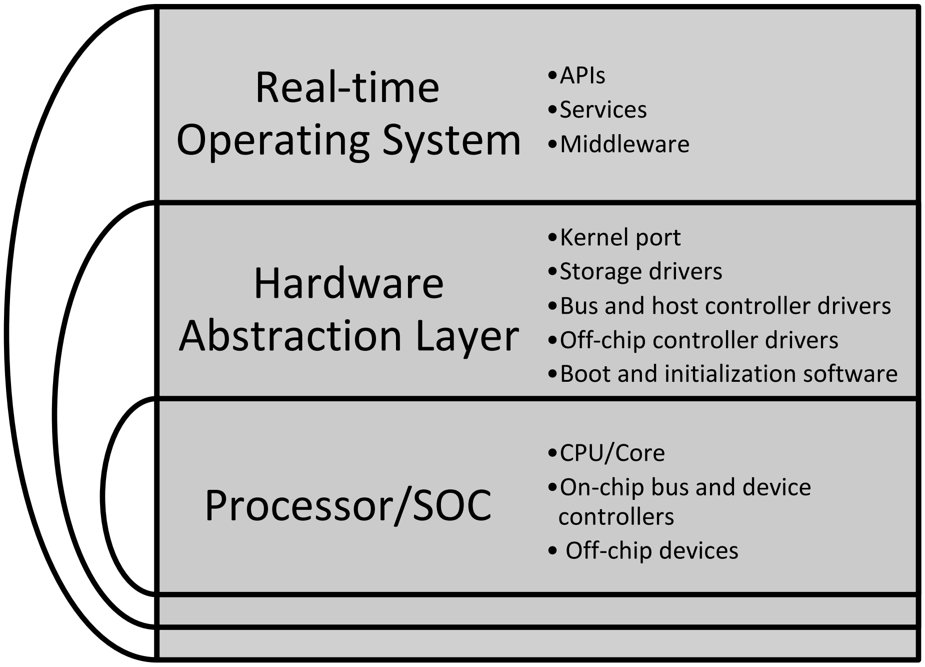
Real-time Operating System
•APIs
•Services
•Middleware
Hardware Abstraction Layer
•Kernel port
•Storage drivers
•Bus and host controller drivers
•Off-chip controller drivers
•Boot and initialization software
Processor/SOC
•CPU/Core
•On-chip bus and device controllers
• Off-chip devices

Figure 1

Port Aspects of Certification

The RTOS hardware abstraction layer (also known as the "port software" or "port") is the glue that that binds the hardware independent RTOS functions to the processor hardware. *It is where the specific implementation details of the architecture, core, processor and compiler are "translated" or mapped for use by the RTOS.*

Within the context of the various software development standards, the RTOS software (with its associated Core VS having undergone prior certification scrutiny) may be a pre-existing software element. The RTOS port software is new, untried software. The "Port Aspects of Certification" are Validation Suite artifacts that apply to the (new) RTOS port software. In addition to the RTOS version and applicable development standard, the Port Aspects of Certification have two additional defining characteristics: they have to accommodate (1) the processor specific RTOS port software and (2) the compiler that is used for the project.

Testing

To this point, testing and test results have not been mentioned as a specific activity or artifact for either the Core VS, or the Port Aspects of Certification. There will be more on this topic in the Validation Kit section but it is important to note that the construction of the Core VS is in part based on the test results being included as part of the Core VS. The artifacts contained in the Core VS are largely provided in .pdf format. They do not require any input on the part of the user. They are not meant to be changed. The basic assumption is that they are correct. This assumption is tested by running the Core VS test suite on the target hardware and gathering the results of the test run for evaluation.

For Validation Suites that originate from VSC, we create the test suite for the port software as we create the rest of the “Port Aspects of Certification”.

Bringing it Together

From an implementation perspective, Validation Suites can be viewed as two mini or sub-Validation Suites (See Table 1 for additional details). The Core VS is the pre-existing set of artifacts for the RTOS software and account for approximately 90% of the Validation Suite content. The Port Aspects of Certification are the new artifacts that support the port software. If a Validation Suite for a specific processor isn’t already available “off the shelf” the port aspects can be created and a Validation Suite delivered, typically in less than 60 days.

It is important to note that the degree of portability i.e. ratio of new to pre-existing software has a direct bearing on the cost of using the software in a certified device. Estimates vary but range up from $150 per line of code. It is reported that the space shuttle’s ~420,000 lines of code cost $1,200 each. The µC/OS has a well-defined hardware abstraction layer that is proven on most if not all combinations of 32-bit commercial processors and compilers. The ratio of preexisting to new code for µC/OS is 10:1. In real-terms, this equates to *tens of thousands of dollars, and man-months of savings* relative to in-house efforts.

NOTE: The cost is not based on the developer’s time alone. It is the sum of the contributions from all those involved in the software development process starting with requirements and planning and ending with the software’s certification and release. Thus it includes the contributions of Test Engineers, QA staff, Architects, etc.

Validation Kits

Validation Kits may be thought of as Validation “Suite” kits. They were originally created as a internal tool for creating Validation Suites. Later, they were productized so that users could create their own Validation Suites. Validation Kits are made up of two main components:

- The Core VS – Exactly the same as in the Validation Suite
- The Port Aspects of Certification and Testing Kit

As with the Validation Suite, the Core VS is described by the version of RTOS source code it applies to, and the development standard that it complies with. For Suites and Kits corresponding to the same RTOS version and standard, they use the same Core VS.

While the Core VS is distinct from the underlying hardware, the “Port Aspects of Certification” and the “Testing Kit” are directly associated with the hardware.

Samples, Examples and Templates

The “Port Aspects of Certification” portion of the kit contains the set of forms, samples, examples and templates that are customized by the user for their RTOS port software. They are organized the same way as those found in the Core VS; and have the same form and function as well. Their purpose is to provide a consistent methodology for developing the port software artifacts. They range in “completeness” from ready to adopt “as is” to template format. For example, Micrium’s coding standard is provided. So, if Micrium provides the port software no additional effort is required on that front. On the other extreme the code and document review sheets are fill-in-the-blank forms.

The Core VS is a standalone component and independent of the Port software artifacts.

Verifying the Validation Kit’s Core VS Test Results

The Core VS contains the test results that were generated by VSC’s in-house testing ina Win32 environment. These results should be verified by the user on their own target hardware. The testing portion of the “Port Aspects of Certification and Testing Kit” provides all of the test source code to complete this task. The testing portion of the kit contains the PC-Lint configuration files, run-time libraries, unit and integration test code that the user uses to verify that their results match those provided by VSC.

The user builds the test code that is provided by VSC, downloads object code to their target and runs each of the test files on their target. The test results are typically returned via a serial port with the results collected via a terminal session. VSC provides a simple polled serial driver that is easy to adapt to the hardware. The results file contains a complete set of results with the identification of all source files used in the test. Other than your IDE, PC-Lint and Microsoft Word no additional software or tools are needed to create a Validation Suite. The Kit is completely selfcontained.

Side by Side

Table 1. below contains a side by side comparison of Validation Suites with Validation Kits. Each of the artifacts contained in a suite or kit falls into 1 of 5 categories:

●	Core VS artifact, is complete, requires no additional effort. A similar document type is also found in the port
●■	Shared Core VS and Port artifact, is complete, requires no additional effort.
■	Port artifact, is complete, requires no additional effort
▣	Port artifact, requires customization to complete
□	Port artifact, Takes the form of one or more forms or checklists

	Suite		Kit	
Master Artifact Set	Core	Port	Core	Port
Project Checklist	●	■	●	□

Software Safety Validation Plan (IEC, EN)	●	■	●	▣
Plan for Software Aspects of Certification (AV)	●	■	●	▣
Software QA Plan	●■		●■	
Software Configuration Management Plan	●■		●■	
Software Validation Plan	●■		●■	
Software Configuration Index	●	■	●	▣
Software Trace Matrix	●	■	●	▣
Software Requirements Document	●	■	●	▣
Software Design Plan	●	■	●	▣
Software Design Document	●	■	●	▣
Software Integration Test Plan	●	■	●	▣
Software Integration Test Procedure	●	■	●	▣
Software Integration Test Report	●	■	●	▣
Software Unit Test Plan	●	■	●	▣
Software Unit Test Procedure	●	■	●	▣
Software Unit Test Report	●	■	●	▣
Software Accomplishments Summary	●	■	●	▣
Safety Manual (IEC, EN)	NA	■	NA	▣
Users Manual (AV)	NA	■	NA	▣
	Suite		**Kit**	
Standards	Core	Port	Core	Port
Code Developer's "C" Coding Standard	●■		●■	
VSC's "C" Coding Standard	●■		●■	
ASM Coding Standard	●■		●■	
Code Review Procedure	●■		●■	
Document Review Procedure	●■		●■	
Port Requirements Document	NA	■	NA	■
Software Problem Reporting Procedure	●■		●■	
Software Design Standard	●■		●■	

Software Requirements Standard	●■		●■	
External Standards Referenced	●■		●■	
	Suite		**Kit**	
Audit	Core	Port	Core	Port
QA Check Lists	●	■	●	□
Code Review Sheets	●	■	●	□
Document Review Sheets	●	■	●	□
	Suite		**Kit**	
Source Code	Core	Port	Core	Port
Source Code Projects - All	●	■	●	NA
Source Code	●	■	●	NA
	Suite		**Kit**	
Test Harness	Core	Port	Core	Port
Run-Time Library for Compiler/Processor	●	■	●	NA
Unit Test Code	●	■	●	NA
Integration Test Code	●	■	●	NA
Source Code Coverage	●	■	●	NA
	Suite		**Kit**	
Test Results	Core	Port	Core	Port
IT Test Results	●	■	●	NA
UT Test Results	●	■	●	NA
Lint Test Results	●	■	●	NA
Code Coverage Results	●	■	●	NA
	Suite		**Kit**	
Test Coverage	Core	Port	Core	Port
100% Feature/Function coverage	Yes	Yes	Yes	No
100% Statement coverage	Yes	Yes	Yes	No
100% Decision coverage	Yes	Yes	Yes	No
100% Object Code coverage	Yes	Yes	Yes	No

Summary

We have endeavored to provide a clear and concise comparison of Validation Suites and Validation Kits. The primary concepts are:

- The Core VS contains the bulk of the value
- The Core VS is common between Kits and Suites
- No matter who creates the Validation Suite, they use a Validation Kit as the starting point

If would like to know more about Validation Suites, Validation Kits or other VSC products. Please contact us at

info@validatedsoftware.com

OR

Visit us at our website – WWW.VALIDATEDSOFTWARE.COM