

Requirements, Configuration Management and Traceability for Safety Critical Software

George Romanski
Verocel, Inc.
Romanski@verocel.com

Software Requirements are the focal point from which traceability to all related artifacts are established during the certification of safety critical software. For the certification of air-borne software, the guidance document DO-178B, requires that the link between requirements, design, code and tests be documented and verified. The DO-178B document does not describe how this should be done, but it permits the re-engineering of information that is missing, to support the certification of commercial-off-the-shelf (COTS) products.

In the past, the engineers at Verocel had developed certification materials for COTS operating systems using a traditional phase driven waterfall model. This meant developing requirements to form a baseline document, reviewing it and then proceeding with the development/review of design, review of code and development/review of tests, analysis of coverage and so on. These materials were captured on paper and resulted in thirty-five pounds of paper for every thousand lines of code.

As the systems that were being prepared for certification at Verocel became larger and more sophisticated, this approach needed to be changed drastically. The development, management and delivery of the certification materials was automated as much as possible. Tools and processes were developed to allow us to manage requirements at a much finer granularity than the traditional approach. Requirements were entered in a database and evolved through a sequence that enforced the states described in company process documents. Requirements were hierarchical and dependency rules ensured that they were approved in the prescribed order. The requirements were very detailed. When the requirements were verified by tests, all robustness objectives were satisfied and complete coverage was obtained. Coverage in this case meant that all of the code and all conditions were exercised (on the target computer at the instruction level) and all the requirements based tests passed.

The design descriptions, source code, tests, results and so on were maintained in a Configuration Management (CM) system. The relationships between the requirements and these artifacts had to be established with appropriate

links from the Requirements Database to the CM system. The capture and review of the information in the CM system was directed through the requirements database. The review sequence for all requirements and their corresponding artifacts was enforced by the requirements traceability tool, but permitted work to be performed in parallel when this did not violate the process rules. This meant that software modules were at different stages of certification depending on staff availability.

The status and review comment information for all of the artifacts was captured in the requirement database, and the versioning information from the CM system was used to establish the relationships between the requirements and the actual artifacts recorded under CM. This data enabled tools to generate completed checklists that are then presented for electronic signature.

The requirement and traceability information was then extracted from the Requirements database and converted into a large number of XML files (20,000 files and 1,300 requirements). The referenced artifacts were extracted from CM automatically. All of these files were copied to a CD-ROM together with style sheets developed at Verocel. When viewed with an XML capable browser, the certification package appears like a local website, permitting navigation from requirements to any related artifact and also from any artifact to its hyper-linked artifacts and requirements.

The tools and certification evidence were presented during the certification of an operating system by the FAA and its designated engineering representatives on several occasions. The initial audits found some problems with this approach, and the tools and techniques had to be changed to address some concerns. The final audit was successful and the CD-ROM delivery of a requirements based certification package was accepted and commended. The details of the approach and the lessons learned will be presented.