Using CMM with DO-178B/ED-12B for Airborne System Development

WHITE PAPER

Author: Narasimha Swamy (Project Manager, Avionics Practice)

Most aircraft companies develop onboard systems software for civilian aircraft based on the guidelines RTCA DO-178B/ED-12B "Software Considerations in Airborne Systems and Equipment Certification". This, apart from ensuring the reliability of the software, also addresses the issues involved in certification of the onboard system. SEI-CMM is used to measure organization's capability in software development and also improvement. As the costs and timelines become stringent, it becomes necessary for companies to improve their software development process by adopting SEI-CMM to make sure that the software is developed as per plan and there is involvement of the higher management in the development process.

This paper looks at these two standards with a view to implement DO-178B in organizations which are SEI-CMM level 5 certified and vice versa. Implementing DO-178B within SEI-CMM is required only if the company is involved in development of safety critical softwares.

Keywords:
SEI-CMM, SW-CMMI, RTCA DO-178B, RTCA DO-2488B, FAA, Process, Software Development
Table of Contents

Introduction ........................................................................................................... 3

Overview of SEI-CMM ........................................................................................... 3
  Mature Organization .................................................................................................. 4
  Levels of Maturity ...................................................................................................... 4
  Key Process Areas (KPAs) .......................................................................................... 6
  Advantages of using CMM ......................................................................................... 6

Overview of RTCA DO-178B ................................................................................. 6
  Software Levels ........................................................................................................ 6
  Life Cycle .................................................................................................................... 7
  Certification Issues ..................................................................................................... 7
  Advantages of DO-178B .............................................................................................. 7

Comparison of SEI-CMM and DO-178B ................................................................. 7

Conclusion .................................................................................................................. 8

References ................................................................................................................... 9

About Wipro Technologies ......................................................................................... 9

Wipro in Embedded Technologies .......................................................................... 10
Introduction

There have been a number of standards/guidelines used in the development of software for various purposes. They have evolved over a period of time as with the evolution of the software industry. Different industries require different standards/guidelines based on its necessity. Even though these standards/guidelines have some similarity, they also have typical uniqueness that distinguishes them from others. This white paper studies two such standards used in software development - the DO-178B and SEI-CMM. A comparison is made between the two standards and the differences are highlighted.

RTCA DO-178B sets the guidelines for the development of software for onboard systems. It has been used generally by civilian aircraft industries. It also finds usage in other safety critical applications like nuclear power plant, space and missile technologies. It is necessary that DO-178B guidelines are used for the development of software for any onboard system to facilitate certification.

SEI-CMM is used to measure/indicate organization's process capability in software development and also its improvement. It is a general standard and has been used by many organizations worldwide in software development. Usage of it has improved the software development process and also made such organizations trustworthy. CMM aims at improving the product quality by improving the processes used in product development.

As organizations grow in size, it becomes necessary to have a tighter control over project execution, maintaining the schedule & effort and at the same time keeping the quality of the product high. This implies that there should be means of control/involvement from the top management to make sure that the project goals are met. It also implies that there should be scope for innovation and improvement in process based on past experience. This is the reason why CMM was introduced and which has been adopted by many organizations worldwide. DO-178B specifically does not allow this kind of management and innovation and hence restricting itself to only product development. This argument proves that, when dealing with the development of safety critical systems for onboard use, we need DO-178B, which concentrates on product, and at the same time from an organizational point of view we need CMM or any of its kind of standard to be adopted.

Organizations that are executing projects in the aerospace domain or developing systems that are safety critical will have to build their development process such that they combine both CMM and DO-178B or similar standard. That kind of a process will have dual goal of organizational control/involvement and at the same time meeting the quality requirements of the standard being followed.

As organizations decide to have both DO-178B based product development as well as CMM based Project Management, it becomes necessary for them to understand both these standards and also find the differences that exist need to be handled. This will be the first step in adoption of both the standards. The following paragraphs explain both CMM and DO-178B briefly and then state where and how they differ.

Overview of SEI-CMM

The process maturity framework was first developed in September 1987 by Software Engineering Institute (SEI) of Carnegie Mellon University with the assistance of Mitre Corporation. After 4 years of experience with software process maturity framework, the SEI evolved the maturity framework into Capability Maturity Model (CMM) for software.
The Capability Maturity Model provides software development organizations with guidance on how to gain control of their processes for developing and maintaining software and evolving a culture of software engineering and management excellence.

**Mature Organization**

A mature software organization possesses an organization-wide ability for managing software development and maintenance processes. The software process is accurately communicated to all the employees and work activities are carried out according to the planned process. The processes mandated are usable and consistent with the way the work actually gets done. These defined processes are updated when necessary and improvements are made through controlled pilot-tests and/or cost benefit analysis. Roles and responsibilities within the defined process are clear throughout the project and across the organization.

In a mature organization, managers monitor the quality of the software products and the process that produce them. There is an objective, quantitative basis for judging product quality and analyzing problems with the product and process. Schedules and budgets are based on historical performance and are realistic; the expected results for cost, schedule, functionality, and quality of the product are usually achieved. In general, a disciplined process is consistently followed because all of the participants understand the value of doing so, and the necessary infrastructure exists to support the process.

**Levels of Maturity**

The CMM suggests five levels of maturity of the company process. The maturity level of a company indicates the effectiveness of company's software development practices. Maturity level 1 is the lowest one and at this level, the practices of the company are vague and does not provide stable environment for developing and maintaining the software. Maturity level 5 is the highest and at this level the company is said to be at the optimizing level and has practices to develop and maintain software efficiently. The five levels are briefly described below and is pictorially represented in Fig 1.

<table>
<thead>
<tr>
<th>Level 1: Initial Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>At this level, the organization does not have any defined process and the development activities are chaotic. The success and repeatability depends on the individual/team but there is no structured help from the organization.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 2: Repeatable Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>At the Repeatable Level, policies for managing a software project and procedures to implement those policies are established. Planning and managing new projects is based on experience with similar projects. Process capability is enhanced by establishing basic process management discipline on a project by project basis. An effective process can be characterized as one which is practiced, documented, enforced, trained, measured, and able to improve.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 3: Defined Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>At the Defined Level, the standard process for developing and maintaining software across the organization is documented, including both software engineering and management processes, and these processes are integrated into a coherent whole. This standard process is referred to throughout the CMM as the organization's standard software process. Processes established at Level 3 are used (and changed, as appropriate) to help the software managers and technical staff perform more effectively.</td>
</tr>
</tbody>
</table>
Level 4: Managed Level
At the Managed Level, the organization sets quantitative quality goals for both software products and processes. Productivity and quality are measured for important software process activities across all projects as part of an organizational measurement program. An organization-wide software process database is used to collect and analyze the data available from the projects' defined software processes. Software processes are instrumented with well-defined and consistent measurements at Level 4. These measurements establish the quantitative foundation for evaluating the projects' software processes and products.

Level 5: Optimizing
At the Optimizing Level, the entire organization is focused on continuous process improvement. The organization has the means to identify weaknesses and strengthen the process proactively, with the goal of preventing the occurrence of defects. Data on the effectiveness of the software process is used to perform cost benefit analyses of new technologies and proposed changes to the organization's software process. Innovations that exploit the best software engineering practices are identified and transferred throughout the organization.

Figure 1: Key process Area by maturity Level
Key Process Areas (KPAs)
As seen in Figure 1, each level is associated with certain Key Process Areas, also called as KPAs. The KPAs at each level give the desirable practices that are required by the software development process. The organization's maturity level is based on the KPAs that it completely practices till that level. So, if a company is certified at Level 4, it indicates that all KPAs of Level 2 and Level 3 are also met along with the KPAs of Level 4.

Advantages of using CMM
By properly implementing the CMM recommendations, organizations will have the following advantages and gains, but not just limited to them.

1. Mature development procedures
2. Better Risk Management and mitigation plans
3. Better defect prevention mechanism
4. High visibility on deliverable quality with minimum overheads
5. Better estimations based on available metrics
6. Better documentation at each stage
7. Better Team Management with clear roles and responsibilities
8. Organizations focus on continuous process improvement
9. Identification of process weakness and effort to rectify them

Overview of RTCA DO-178B
As the use of software in the on-board systems of aircraft increased, a need was felt to have a guideline that describes the procedure for developing the software and also the certification requirements. RTCA DO-178 was first published in 1982 and later on, the revised guideline DO-178B was published in 1992. This has become a standard, presently used in all airborne system software of civilian aircrafts. Along with DO-178B, DO-248B is also used. This document gives the clarifications, corrections and answers to frequently answered questions about DO-178B and was released by RTCA in 1996.

Software Levels
The software development activity of any airborne system as per DO-178B starts with the system safety assessment. During this, the effect of failure of the system on the overall working of the aircraft is studied and its effect is analyzed. Based on this, the software to be developed is classified into five categories as shown in the table below. The table also gives the process objectives that each class of software has to satisfy. Process objectives are the objectives that DO-178B expects to be satisfied for certification. For example, MCDC testing is one objective that has to be performed for Level software but is not done for other levels. Similarly the decision coverage and statement coverage are other two objectives. The total number of objectives that are to be satisfied for each level is listed in the table. Annexure A of DO-178B document gives the objectives that have to be complied with, for each level.

<table>
<thead>
<tr>
<th>DO-178B Software Level</th>
<th>Failure Condition</th>
<th>Process Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Catastrophic</td>
<td>66</td>
</tr>
<tr>
<td>B</td>
<td>Hazardous</td>
<td>65</td>
</tr>
<tr>
<td>C</td>
<td>Major</td>
<td>57</td>
</tr>
<tr>
<td>D</td>
<td>Minor</td>
<td>28</td>
</tr>
<tr>
<td>E</td>
<td>No Effect</td>
<td>00</td>
</tr>
</tbody>
</table>
Life Cycle
DO-178B does not prescribe any particular life cycle but describe separate processes that comprise most life cycle and interactions between them. DO-178B describes the following three processes.

1. Software Planning Process: Planning process defines and coordinates the activities of the software development and integral processes for a project.
2. Software Development Process: This defines the processes that produce the software product. These processes are the software requirements process, the software design process, software coding process and the integration process.
3. Integral Process: This process is performed concurrently with the software development processes throughout the software life cycle. They ensure correctness, control and confidence of the software life cycle processes and their output. The integral processes are verification & validation, Configuration Management, software quality control and certification liaison.

Certification Issues
Every onboard system that is developed has to go through the process of certification, along with the software that goes into the system. Certifying agencies present in each country are responsible for evaluating the product prior to certification. Necessary supporting documents have to be provided by the product company intending certification for the system. These typically include proof of software development as per the stated plan, documents to indicate that all the objectives are satisfied and recorded outputs of each activity.

For certification, the system is also checked for any Previously Developed Software (PDS) or Commercial Off The Shelf software (COTS). This would include operating system or any other software component that was developed earlier. But the PDS or COTS software should have full documentation and proof that they were developed in a controlled way. Another aspect of certification is that the certifying agency is involved with the vendor from the beginning and will have proof of the controlled development process followed.

Advantages of DO-178B:
By using the DO-178B or similar standards like ED-12B, organizations will have the following advantages.

1. High degree of product focus leading to quality product.
2. Safety assessment of the product done in accordance with its role. The safety assessment is done at the beginning of the development cycle and based on the assessment the objectives for the level are complied with.
3. Very good verification & validation procedures to remove defects at each stage. Procedures like MCDC test are done to remove all possible defects in the system.
4. Gives framework for development of safety critical systems
5. Makes sure that qualified tools and other COTS software are only used for critical systems by evaluating the procedure adopted in the development of such tools & COTS software.
6. Clear documentation that will facilitate certification and long product life cycles.
7. Well planned quality assurance, change control and Configuration Management.

**Comparison of SEI-CMM and DO-178B**

As was mentioned earlier, the aim and scope of these two standards are very different and hence no comparison per se can be done. But as we have understood above, these two standards can be in place together too. A lot of industries that are developing software as per DO-178B are moving towards CMM for better efficiency and mature process practices. The rest of this paper discusses the main differences in these two standards and then the advantages of using both these together.

As has come out from the introduction of CMM, it is a general standard and it focuses not only on product development but also on management of development process with the application of previous knowledge and with the involvement of other associated groups like quality and process group. It also ensures that the management policies are in place for practice of good processes. CMM level of the company represents the maturity of the organization in building the software and it will at no time substitute for DO-178B as per FAQ released by FAA as part of DO-248B. CMM is focused on business process measurement and improvement. It stipulates and assesses against many process attributes that are necessary, but not sufficient conditions for high product integrity and safety. For example, the SEI CMM has no process activities or capabilities or metrics associated with verification (review, analysis, or test) coverage, whereas this is a very significant aspect of DO-178B/ED-12B guidance, because verification is a key factor in system safety. The verification & validation has been introduced in the new CMMI and should address this vital need.

Another important point is that DO-178B activities are based on the system safety objectives whereas there is no such activity is prescribed in CMM. So the activities performed as per CMM guidelines will be general without the consideration of system safety level.

Unlike other standards like DOD2167A both CMM & DO-178B are non prescriptive with regard to procedure to be followed or template to be used for a certain activity. The users have to evolve their own procedure and templates for such a use. It is the responsibility of the vendor developing the airborne system to prove that the objectives are satisfied. This gives the users scope to have their own templates and procedures which are tuned to their requirements.

Even though CMM/CMMI has some KPAs like Requirement Management, verification & validation etc., it does not specify how and to what extent it has to be done. Whereas, DO-178B does get into specifics like clearly stating what level of verification has to be done for a particular level of software. In general DO-178B is descriptive about how any practice has to be followed whereas CMM just says what has to be done with out mentioning how it has to be done.

Another important thing about DO-178B is that it does not admit tailoring unlike CMM. The practices to be followed in DO-178B are given in DO-248B and have to be strictly followed.

**Conclusion**

Based on the discussion so far and particularly based on the advantages of each standard, it is clear that both these standards can be used simultaneously and that would add up the advantages of the software development process. If DO-178B is focused on product, CMM is focused on Management of the process of development. Organizations will gain very much by adopting both these standards for the development of safety critical
systems. As the computerization and need for safety critical systems increases in the coming years, there will be more need for well managed product development keeping in view the important metrics like schedule, effort and hence cost of development, under planned figures. This will also improve Resource Management. With the introduction of SW-CMMI by SEI, the organizations are set to gain more as CMMI presents an integrated approach to enterprise wise process improvement. CMMI focuses product engineering with much vigor than SW-CMM by introduction of process areas like requirements development, technical solution, v & v and product integration.

References
2. The Capability Maturity Model for Software by Mark C. Paulk et all.
3. Using the Software Capability Model for Certification Projects by Leena K Rierson
4. The Challenges of Software Certification by George Romanski

Wipro Technologies is a leading software consultancy and service provider, certified for CMMI Level 5. Also, Wipro has defined a DO-178B compliant process to address its clients’ needs in Aerospace and Avionics domains. This study of integration of the two standards was taken up as a result of using DO-178B within the framework of CMMI process model.

About Wipro Technologies
Wipro is the first PCMM Level 5 and SEI CMMi Level 5 certified IT Services Company globally. Wipro provides comprehensive IT solutions and services (including Systems Integration, IS Outsourcing, Package Implementation, Software Application Development and Maintenance) and Research & Development Services (hardware and software design, development and implementation) to corporations globally.
Wipro in Embedded Technologies

Wipro Technologies, a leading global provider of IT solutions and services company, has a wide ranging expertise in Datacom, Telecom, System Software and VLSI Systems. It has executed projects by using diverse real-time operating systems, networking technologies and associated tools. The areas in which we offer services include consumer electronics, Automotive electronics, real-time OS, semiconductors, mobile computing, device drivers, process control systems and multimedia.

© Copyright 2002. Wipro Technologies. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without express written permission from Wipro Technologies. Specifications subject to change without notice. All other trademarks mentioned herein are the property of their respective owners.

Specifications subject to change without notice.