Verificação e Validação na terceirização de software embarcado em aplicações espaciais

Maria de Fátima Mattiello-Francisco[1], Valdivino Alexandre de Santiago Jr[1], Ana Maria Ambrosio[1], Ricardo Costa [2], Leise Jogaib [2]

[1]Instituto Nacional de Pesquisas Espaciais (INPE)
Caixa Postal 515 – 12.227-010 – São José dos Campos – SP – Brazil

[2]DBA Engenharia de Sistemas Ltda
Av. Presidente Vargas 3131, 3° Andar, CEP 20210-030 – RJ – Brazil

{fátima, ana}@dss.inpe.br valdivino@das.inpe.br {rcosta, ljogaib}@dba.com.br

Abstract. *This paper reports INPE's experience in outsourcing the development of satellite payload embedded software to DBA, a Brazilian Software supplier, CMMI 3 certified, following the software verification and validation processes recommended by ECSS standards. The software item, SWPDC, under development by DBA Software Factory, is part of ongoing Quality of Space Application Embedded Software (QSEE) project. Among others aspects, QSEE project aims to evaluate the conformance of a Software Factory processes with INPE requirements for embedded software development process. Independent Verification and Validation (IVV) approach is used by INPE in order to delegate the software acceptance activities to a third part team. Lessons learned and contributions for improvements on DBA software testing process are presented.*

Resumo. *O presente artigo relata as experiências adquiridas pelo INPE e a DBA com a aplicação das normas ECSS no processo de verificação e validação do software embarcado em cargas úteis de satélites científicos. O software piloto SWPCD, objeto da terceirização da Fábrica de Software da DBA pelo INPE, encontra-se em fase de desenvolvimento no escopo do projeto Qualidade do Software Embarcado em Aplicações Espaciais (QSEE), que tem como um dos objetivos avaliar a aderência dos processos de uma Fábrica de Software nacional, nível 3 CMMI, às especificidades requeridas pelo cliente INPE no desenvolvimento do software embarcado. Explora-se a abordagem de Verificação e Validação Independente de Software como parte do processo de aceitação do produto de software terceirizado pelo cliente. Contribuições do projeto para a melhoria do processo de testes da DBA também são discutidas.*

1. Introdução

Sistemas espaciais são reconhecidos, de forma geral, como sistemas críticos. Sua engenharia está fundamentada na aplicação das mais recentes tecnologias e altos níveis de especialização, as quais elevam significativamente os custos do projeto. A

preocupação das agências espaciais mundiais com a qualidade do projeto de tais sistemas, somada à inserção do setor industrial na área espacial na última década, tem demandado grandes investimentos na melhoria dos processos adotados para o desenvolvimento de softwares críticos, o que especialmente envolve a aplicação de metodologias e técnicas da qualidade na gestão de projeto.

Como resultado de um esforço conjunto da Agência Espacial Européia (ESA) com a associação de indústrias Européias, as normas *European Cooperation for Space Standardization* (ECSS) têm o propósito de facilitar a relação cliente/fornecedor no desenvolvimento de projetos na área espacial. Em consonância com este tema, o Instituto Nacional de Pesquisas Espaciais (INPE), responsável pela execução dos programas de satélites brasileiros, desde o final dos anos 90, segue a padronização ECSS para conduzir as atividades de desenvolvimento de missões de satélites científicos.

Ao longo dos anos, vários modelos têm sido utilizados para descrever as diferentes fases de um projeto. Os modelos identificam os componentes de um projeto e ressaltam suas interdependências ou inter-relações. Embora cada modelo tenha suas próprias características e vantagens, eles freqüentemente estão fundamentados no ciclo de vida do produto.

O modelo usado pelas normas ECSS para o desenvolvimento de missões espaciais está baseado no ciclo de vida da missão que consiste de 6 fases: 0+A- Identificação das Necessidades e Análise de Viabilidade da Missão, B- Definição Preliminar dos Requisitos do Projeto e Produto da Missão, C- Definição Detalhada do Produto, D- Produção/ Teste de Qualificação em Solo, E- Operação, F- Descarte [ECSS-M-30A 1996]. Ao longo delas, 7 atividades principais são conduzidas: concepção da missão, definição dos requisitos, especificação técnica, verificação e qualificação, produção, operação e encerramento.

A Figura 1 apresenta o ciclo de vida de uma missão espacial e os marcos criados para envolver a indústria na execução de tais atividades, como fornecedores para o programa espacial [Mattiello-Francisco, et al. 2005]. Os círculos inferiores representam a seqüência de revisões formais recomendadas para projetos de missões espaciais: *MDR- Mission Definition Review, PRR- Preliminary Requirements Review, SRR- System Requirement Review, PDR- Preliminary Design Review, CDR- Critical Design Review, QR- Qualification Review, AR- Acceptance Review, ORR- Operation Requirements Review, FRR- Flight Readiness Review. DDR- Detailed Design Review* é uma revisão especialmente recomendada para projetos de software.

Em missões espaciais, o produto de software é geralmente caracterizado como um subsistema na hierarquia do desenvolvimento de sistemas. Na coluna direita da Figura 1 destaca-se a correspondência das atividades das missões espaciais com as atividades típicas dos processos do ciclo de vida do software, descritas na norma ECSS-E-40 1B (2003) de forma consistente com a família de documentos ISO 9000 e processos do ciclo de vida do software ISO/IEC 12207. As barras cinza representam os períodos necessários para realização das atividades da missão espacial do ponto de vista de sistema. As barras negras correspondem ao tempo associado à realização de tais atividades no contexto de desenvolvimento do subsistema de software espacial.

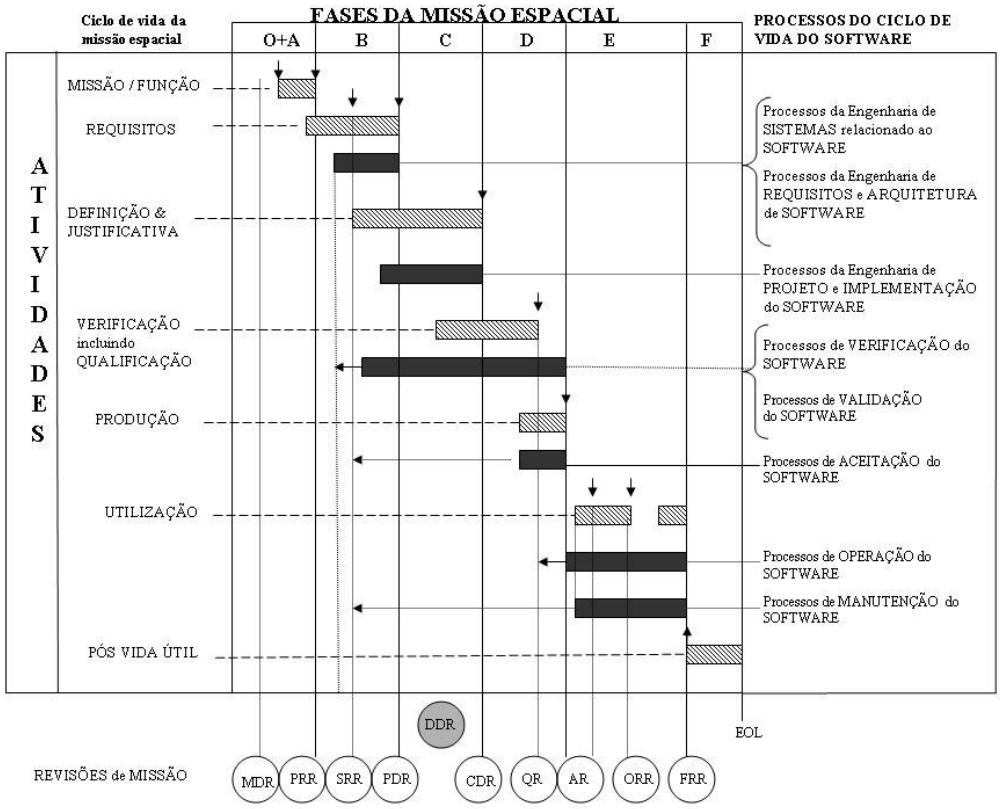

Figura1. Ciclo de vida típico ECSS

No caso das missões de satélites, um aspecto muito importante contemplado pelas fases de desenvolvimento da missão é a produção de diferentes modelos do satélite considerados necessários pela garantia da qualidade do produto, como por exemplo: o modelo de engenharia, o modelo de qualificação e o modelo de vôo. Cada um deles requer um conjunto específico de facilidades de testes para ser validado. Particularmente, software embarcado em cargas úteis é um subsistema do Instrumento a bordo do satélite, cujas fases de desenvolvimento e qualificação do produto envolvem vários níveis de integração.

Como conseqüência de cooperações internacionais, as normas ECSS são adotadas nas missões de satélites científicos do INPE, inclusive com o envolvimento da indústria brasileira no fornecimento de subsistemas. Porem, é a primeira vez que se experimenta a terceirização do desenvolvimento de software embarcado para uma Fabrica de Software. O desenvolvimento do software piloto Software para o Computador da Carga Útil (SWPDC) embarcado na carga útil do satélite Monitor e Imageador de Raios X (MIRAX) iniciou em 2005 no escopo do projeto QSEE, financiado pela FINEP, como um projeto de transferência tecnológica do INPE para a indústria brasileira do setor de software. O MIRAX é uma missão de satélite de astronomia cujos objetivos científicos estão baseados na observação contínua (no mínimo 9 meses por ano) de uma rica região de fontes de Raios X [MIRAX 2006]. Pelo fato do projeto piloto SWPDC ser um estudo de caso, a especificação do subsistema de software do MIRAX foi simplificada [QSEE 2006].

Tendo por meta avaliar a aderência dos processos da Fábrica de Software da DBA, nível 3 CMMI, às especificidades requeridas pelas normas ECSS, descritas nos segmentos Engenharia de Software (ECSS-E-40 Part 1B) e Qualidade do Produto de Software (ECSS-Q-80B) o projeto QSEE centrou esforços na adequação dos 5 processos do ciclo de vida do software: Engenharia de Requisitos e Arquitetura do Software, Projeto e Implementação do Software, Verificação do Software, Validação do Software e Entrega e Aceitação do Software. De forma simplificada, o processo de Engenharia de Requisitos de Sistema foi cumprido pelo cliente INPE por meio dos documentos considerados entrada para os processos citados acima: RB (Requisitos Base do Software) e EI (Especificação das Interfaces contendo os protocolos de comunicação associados).

O escopo do presente artigo limita-se aos processos de verificação e validação do software. Como pode ser observado na Figura 1, eles iniciam na fase B, logo após a definição dos requisitos do software e, só terminam na fase D, após o teste de qualificação do satélite.

2. Interação com a Fábrica de Software

Conforme recomendado em ECSS-E-40 1B, além dos itens que descrevem os requisitos funcionais, de desempenho, de operação, dependabilidade, manutenção e interface, o documento RB contem os requisitos de Verificação e Validação do produto do software onde são apresentados pelo cliente os marcos considerados essenciais para o acompanhamento do processo de desenvolvimento realizado pelo fornecedor. A Figura 2 apresenta a linha base de entregas e revisões de documentações solicitadas pelo cliente INPE ao fornecedor DBA para o produto SWPDC. Observa-se que foi feito um espelhamento das revisões recomendadas pelas normas ECSS em nível de sistema, apresentadas na Figura 1, para o nível de subsistema. O software embarcado no Modelo de Engenharia é entregue pelo fornecedor na revisão CDR para ser validado pelo cliente, iniciando o processo de aceitação. Primeiro ele é validado em nível de subsistema da missão de satélite e, posteriormente em nível de sistema.

A Figura 2 também ressalta ao fornecedor a necessidade da sua participação na verificação e validação do Modelo de Vôo do satélite quando o software embarcado no Instrumento já se encontra na sua configuração final.

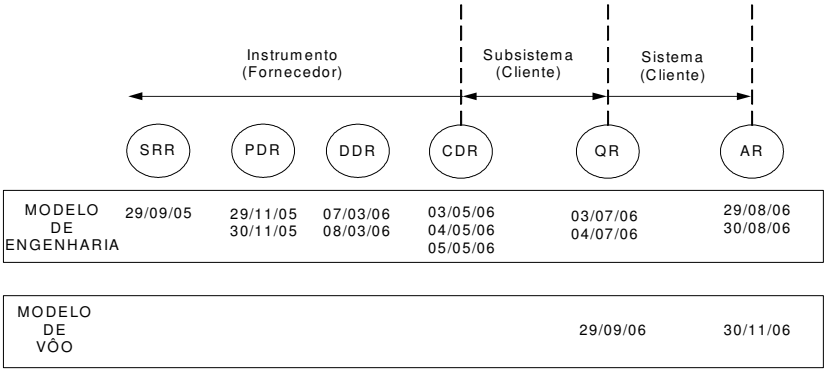

Figure 2. Relacionamento entre as revisões técnicas, os níveis de verificação e os modelos de hardware

O fornecedor acompanha todo o processo de aceitação do software que culmina com a revisão AR do Modelo de Vôo. A presença do fornecedor é fundamental para realizar eventuais modificações do software decorrentes de inconsistências observadas. É com base nos requisitos estabelecidos no documento RB que o fornecedor elabora o Plano de Desenvolvimento do Software (PDSw) um dos objetos da revisão formal SRR. Os produtos associados a cada revisão técnica são listados como entregas no Plano de Desenvolvimento de Software elaborado pelo fornecedor.

A Fábrica de Software da DBA, avaliada oficialmente CMMI Nível 3, possui como ciclo de projeto de software as fases de Análise de Requisitos para a Contratação, Planejamento, Projeto Lógico, Projeto Físico, Construção, Teste, Controle de Qualidade de Software e Entrega/ Homologação que inclui o acompanhamento da aceitação do produto de software pelo cliente. Estas fases são totalmente aderentes às Áreas Chave de Processo do CMMI Níveis 2 e 3, por exemplo: Gerenciamento de Requisitos, Planejamento de Projeto, Supervisão e Acompanhamento de Projeto, Gerenciamento de Riscos, Verificação, Validação, Medição e Análise, Garantia de Qualidade de Software, Gerência de Configuração de Software, Engenharia de Produtos de Software e Revisão por Pares, entre outros. O lado esquerdo da Figura 3 apresenta as fases de vida do software na Fábrica de Software e o lado direto destaca **a**lguns dos Processos de apoio às fases do ciclo de vida e aderentes ao CMMI níveis 2 e 3.

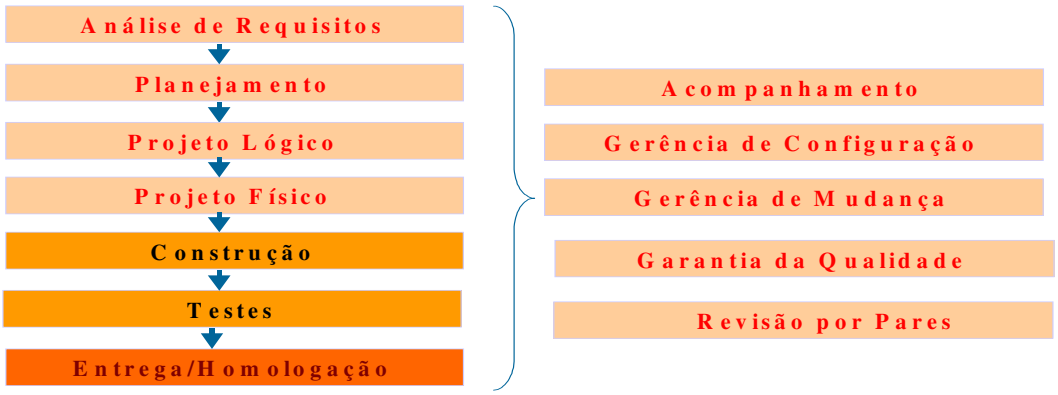

Figure 3. Fases do ciclo de vida na DBA e processos de Apoio

Cada fase do ciclo de vida é descrita em sub-processos que são seguidos pela equipe da Fábrica de Software. Um exemplo é o sub-processo Correção dos Defeitos encontrados na revisão pertencente ao processo Revisão por Pares. Todo serviço enviado à Fábrica de Software é caracterizado como um projeto cujos aplicativos são agrupados em módulos de um sistema ou em um sistema completo. Os módulos são encomendados à Fábrica de Software e possuem datas definidas para o envio da cada demanda e para a entrega dos produtos ao demandante.

3. Verificação e validação

Os processos de verificação e validação do software SWPDC foram estabelecidos com base nos conceitos de verificação e validação de sistemas computacionais críticos [Storey 1996] onde *verificação* é definido como o processo adotado para determinar

que um sistema ou módulo corresponde à sua especificação e, *validação* é o processo para determinar que um sistema atende seu propósito de funcionamento (em termos de requisitos do usuário).

Em termos de verificação, o processo existente na Fábrica de Software foi facilmente adequado às exigências do cliente e consolidado na revisão SRR com a aprovação do documento PDSw e o documento de Especificação Técnica do Software (ETS), analisado na PDR, ambos elaborados pelo fornecedor. No ETS, o fornecedor apresentou seu entendimento sobre os requisitos do produto de software fornecidos pelo cliente INPE no RB e listou de forma detalhada os requisitos de sistema a serem desenvolvidos utilizando a abordagem de casos de uso da UML. Os artefatos de desenvolvimento do software produzidos ao longo do projeto do piloto SWPDC, tipo casos de uso, diagramas de seqüência UML e casos de testes são correlacionados com a lista de requisitos para facilitar a rastreabilidade. Práticas da Fábrica de Software como Revisão por Pares, não exigidas pelo cliente, foram mantidas por contribuírem na qualidade do produto.

A validação do SWPDC no contexto da Fábrica de Software segue a abordagem de teste: unitário e integrado implantada nos sub-processos de Teste definido na Fábrica de Software da DBA: Planejamento dos Testes, Elaboração dos Casos de testes, Alteração dos casos de testes, Preparação e Execução do teste unitário, Preparação e Execução do teste integrado. Os erros encontrados devem ser corrigidos e os aplicativos re-testados. Para a realização do Teste Integrado, são utilizados o Plano de Integração, os Aplicativos, os Arquivos compilados, os Casos de Teste, a Especificação Técnica, o Plano de Teste e os Padrões do projeto.

A abordagem de verificação e validação independentes foi adotada no contexto do cliente, com o objetivo de exercitar o envolvimento de uma terceira parte para apoiar o cliente no recebimento e aceitação do produto de software desenvolvido pela Fábrica de Software. O termo independente caracteriza-se pelo envolvimento de pessoas (papéis) não vinculadas ao desenvolvimento do produto, nas atividades de validação e verificação. No projeto QSEE esta equipe foi constituída por um pesquisador sênior do INPE e um pesquisador do IC/Unicamp.

O processo de verificação e validação independente inicia com a construção de uma matriz de verificação onde são estabelecidos os métodos de verificação (inspeções e testes) exigidos pelo cliente nos diferentes estágios de desenvolvimento e integração do produto de software no Instrumento, no Subsistema do satélite e Sistema do satélite para cada requisito do usuário (cliente) definido no documento RB. Na revisão SRR o documento PVVIS (Plano de Verificação e Validação Independente do Software) elaborado pela equipe V&V independente, é revisado, consolidando assim a matriz de verificação. A definição dos casos de testes pela terceira parte evolui paralelamente ao desenvolvimento do produto do software, assim como a preparação do ambiente onde os testes serão executados. A elaboração de casos de testes pela terceira parte e a execução dos testes de aceitação em um ambiente diferente do contexto em que o software piloto SWPDC foi produzido na Fábrica de Software caracterizam as condições de independência requeridas pelo cliente para aceitar o produto.

4. Aderência aos Processos da Fábrica de Software

O nível de maturidade 3 CMMI da Fábrica de Software da DBA permitiu à equipe da Garantia da Qualidade do Software identificar, de forma relativamente simples, as necessidades requeridas pelo cliente INPE para o produto de software embarcado. Em função do engajamento deste produto no ciclo de vida da missão espacial, as exigências de revisões formais ao longo do desenvolvimento do software foram compreendidas pelo fornecedor. Os mecanismos existentes nos processos da qualidade da empresa facilitaram a implantação das adequações que se mostraram necessárias como, por exemplo, a elaboração do conjunto de documentos exigidos pelo cliente nas revisões formais de projeto, seguindo os padrões ECSS.

Adicionalmente, o treinamento em desenvolvimento de software embarcado dado no INPE, por seis meses, para a equipe do projeto QSEE (2 analistas de sistemas pleno com mestrado) posteriormente absorvida pela Fábrica de Software da DBA, facilitou a instanciação dos processos da Fábrica de Software para a produção de software embarcado em aplicações espaciais. A experiência da DBA no modelo de Fábrica de Software para produtos de software embarcado em celulares ajudou muito na correlação dos conceitos "modelo de engenharia", adotado em projetos espaciais, com "ambiente alvo", domínio da DBA. com as peculiaridades do domínio espacial contribuíram com a implantação de melhorias nos sub-processos do processo de Teste da Fábrica.

5. Lições aprendidas e resultados obtidos

Como lições aprendidas para a DBA, podem-se destacar: (1) A importância de o fornecedor entender, antecipadamente na fase de análise, as etapas e ambientes de teste, pelos quais o produto de software a ser fornecido será submetido na aceitação pelo cliente. Somente assim o planejamento das atividades e recursos necessários para a realização do projeto será consistente com a realidade de execução; (2) Projetos de software embarcado em aplicações espaciais em geral requerem o desenvolvimento de simuladores e ambientes de testes específicos para validarem o comportamento do software no modelo de engenharia. Estas necessidades têm que ser dimensionadas pelo líder do projeto no escopo do fornecedor, antes da Fábrica de Software ser envolvida no processo.

Do lado do cliente INPE, como lições aprendidas, pode-se destacar: (1) A necessidade de detalhar no documento RB aspectos operacionais do software embarcado. Isto decorreu da abordagem IVV adotada no processo de aceitação, pois para que uma equipe não envolvida com a solução possa planejar e aplicar testes operacionais conforme a especificação, esta deverá conter os requisitos de operação de forma muito clara. Como a abordagem IVV de software está sendo adotada pela primeira vez no INPE, no âmbito do projeto QSEE, os detalhes de operação necessários para a aceitação do software eram de domínio da equipe que definiu os requisitos, não sendo necessários sua incorporação no RB.

A Fábrica de Software da DBA obteve para seu acervo um *checklist* mais detalhado do que o padrão existente de itens a serem verificados em seu processo de Revisão por Pares, para a linguagem de programação C, adotada no projeto. O nível maior de detalhe e rigor adotado considerou o alto grau de criticidade da aplicação.

A exemplo da SRR recomendada nas normas ECSS, uma Validação de Requisitos foi incorporada ao ciclo de vida de desenvolvimento utilizado pela Fábrica de Software, anteriormente às Fases de Contratação e Levantamento de Requisitos. Observou-se que este procedimento evitou interpretações equivocadas do fornecedor em relação à especificação entregue pelo cliente, mitigando os riscos de eventuais problemas na entrega do produto do software e conseqüente retrabalho.

Agradecimentos

Os autores agradecem à Financiadora de Estudos e Projetos (FINEP) pelo suporte dado ao projeto Qualidade do Software Embarcado em Aplicações Espaciais (QSEE).

Referências

ECSS-M-30A Space Project Management – Project Phasing and Planning, April 1996.

Mattiello-Francisco, M.F.; Arias R, Hirata, C.M, Sakugawa, B.M, Yano, S.V. A comparative study between PMBoK/DoD and ECSS/management process for software acquisition. DASIA2005, May 2005. Edinburg, Scotland.

ECSS-E-40 Part 1B Space Engineering – Software – part 1: Principles and requirements, November 2003.

ISO/IEC 12207 Information Technology - Software Lifecycle Processes.

MIRAX – Monitor e Imageador de Raios X. Ciências Espacias e Atmosféricas, INPE. Em:<http://www.cea.inpe.br/cea/satelites/mirax/miraxproject.htm>. Acesso em: 10 março 2006.

QSEE - Qualidade do Software Embarcado e aplicações espaciais, financiado pela FINEP, Em: <http://www.cea.inpe.br/~qsee>. Acesso em: 20 março 2006.

ECSS-Q-80B Space Product Assurance: Software Product Assurance, October/2003.

Sorey, N. (1996), Safety-Critical Computer Systems, Addison Wesley, 1st edition.