
Processos de desenvolvimento de software para a área espacial

Carlos H. N. Lahoz

Martha A. D. Abdala, Miriam C. B. Alves

Instituto de Aeronáutica e Espaço (IAE)

Simpósio Internacional de Melhoria de Processo de Software

São Paulo 5 de Dezembro de 2007

SIMPROS 2007

1

Objetivo desta palestra é apresentar:

O IAE e o projeto VLS;

O padrão ESA;

Os processos de software para a área espacial;

Algumas considerações sobre os atuais desafios da área espacial.

SIMPROS 2007

2

O IAE e o Projeto VLS



SIMPROS 2007

3

Veículo Lançador de Satélites

“A construção de veículos lançadores, outro ponto decisivo para a estratégia do Programa Espacial no País, não apenas garante e preserva a necessária autonomia para o acesso ao espaço, como possibilita, também, a exploração comercial de serviços de lançamento.”

Programa Nacional de Atividades Espaciais (PNAE) 2005-2014, Agência Espacial Brasileira.



SIMPROS 2007

4

Veículo Lançador de Satélites



Características principais do VLS:

- ◆ 100 a 380 Kg de capacidade de lançamento;
- ◆ 7 motor-foguetes distribuídos em 4 estágios;
- ◆ Propelente sólido;
- ◆ 20 m de altura;
- ◆ 50 t de peso.

SIMPROS 2007

Veículo Lançador de Satélites

Projeto de longa duração:

- ◆ Foram planejados quatro vôos para a qualificação do veículo;
- ◆ Componentes e subsistemas de desenvolvimento próprio (“in house”) são aperfeiçoados ao longo do tempo;
- ◆ Decisões de projeto mudam requisitos a cada versão do veículo (impacto na configuração do software embarcado);
- ◆ Itens comerciais de hardware e software (COTS), usados no projeto, estão continuamente evoluindo.

SIMPROS 2007

6

VLS - Histórico dos vôos

◆ **1997: VLS-1 V01:** Operação Brasil

O mau funcionamento do “dispositivo mecânico de segurança” (DMS) em um dos motores do primeiro estágio abortou a missão.

◆ **1999: VLS-1 V02:** Operação Almenara

Logo após o acendimento do propulsor do segundo estágio, o veículo foi destruído por uma explosão.

◆ **2003: VLS-1 V03:** Operação São Luís

Acidente na Torre Móvel de Integração provocou o início do funcionamento intempestivo, porém nominal, do propulsor A do primeiro estágio.

VLS1 -V03

Algumas recomendações do Relatório da Investigação do Acidente:

- ◆ Revisão de planos e procedimentos de segurança;
- ◆ Elaboração de análise de risco do sistema VLS-1;
- ◆ Adoção de normas para a garantia da qualidade e gerenciamento de projetos e procedimentos de certificação;
- ◆ Realização de revisões de engenharia e segurança.

(Comando da Aeronáutica. DEPED - Relatório da Investigação do acidente ocorrido com o VLS1-V03, em 22 de agosto de 2003, em Alcântara, Maranhão. São José dos Campos, Fev. 2004)

VLS – Software Aplicativo de Bordo

Projeto iniciado em 1994:

- ◆ Equipe composta de mais de 30 pessoas e 3 fornecedores (*);
- ◆ Análise: metodologia estruturada de Hatley-Pirbhai, com recursos para modelagem de sistemas de tempo real;
- ◆ Projeto: metodologia de Page-Jones, com uma carta de estrutura para cada tarefa identificada;
- ◆ Ciclo de vida baseado no modelo em cascata;
- ◆ Utilização da linguagem de desenvolvimento C estruturado.

VLS – Software Aplicativo de Bordo

Até o VLS-1 V03, abordagem focada na garantia de produto:

- ◆ Norma DoD-STD-2167A aplicada como instrumento de delineamento e registro das atividades a serem realizadas;
- ◆ Plano da Garantia da Qualidade (PGQS) baseado na IEEE 993/86 – Software Quality Assurance Planning.
- ◆ PGQS estabelecia diretrizes a serem cumpridos durante desenvolvimento, aquisição e suporte dos sistemas de software;

O padrão ESA:

ECSS

<http://www.estec.esa.nl>

<http://www.ecss.nl/>



SIMPROS 2007 11

ECSS

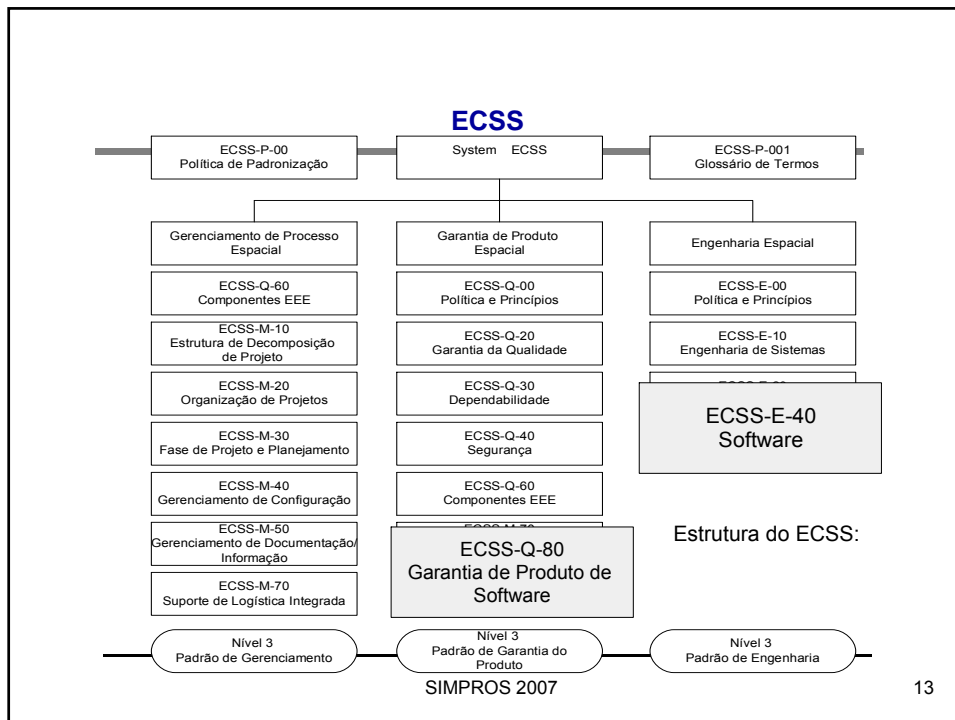
ECSS : European Cooperation for Space Standardization - 1994

Esforço cooperativo entre a ESA, as agências espaciais dos países europeus e a indústria europeia, com o objetivo de desenvolver e manter padrões europeus relacionados a programas espaciais.

Objetivo:

- ◆ desenvolver e manter padrões europeus (área espacial);
- ◆ redução de custos;
- ◆ melhoria da qualidade;
- ◆ entendimento comum.

SIMPROS 2007 12



ECSS E-40

ECSS E-40:

- ◆ Define as atividades de engenharia, associadas a diferentes processos de desenvolvimento de software;
- ◆ Cobre todos os aspectos da Engenharia de Software Espacial;
- ◆ Dois segmentos:
 - Espaço: computador embarcado, sistema de manipulação de dados e sistemas de órbita e atitude;
 - Solo: sistemas de controle de missão, simuladores, de dinâmica de voo, ferramentas de análise de voo, de dados de estações terrestres- telemetria e telecomando e redes de comunicações.

ECSS Q-80

ECSS Q-80:

- ◆ Define os requisitos de garantia de produto de software:
 - desenvolvimento e manutenção de software para sistemas espaciais;
 - processos de forma individual;

- ◆ Auxiliam a garantir a qualidade:
 - processo de desenvolvimento;
 - produto de software final.

Os processos de software para a área espacial

A estratégia de desenvolvimento para o
Software Aplicativo de Bordo
SOAB

SOAB : Estratégia de Desenvolvimento Atual

- ◆ Garantir que a organização interna do projeto tenha uma estrutura capaz de atender ao cumprimento da missão do software, de forma segura e confiável;
- ◆ Incorporar as modificações propostas pelo documento de Especificação dos Requisitos de Sistema para Software para o próximo voo;
- ◆ Modificar o produto, respeitando todas as fases de um ciclo de vida de software.

SOAB : Métodos, Processos e Padrões

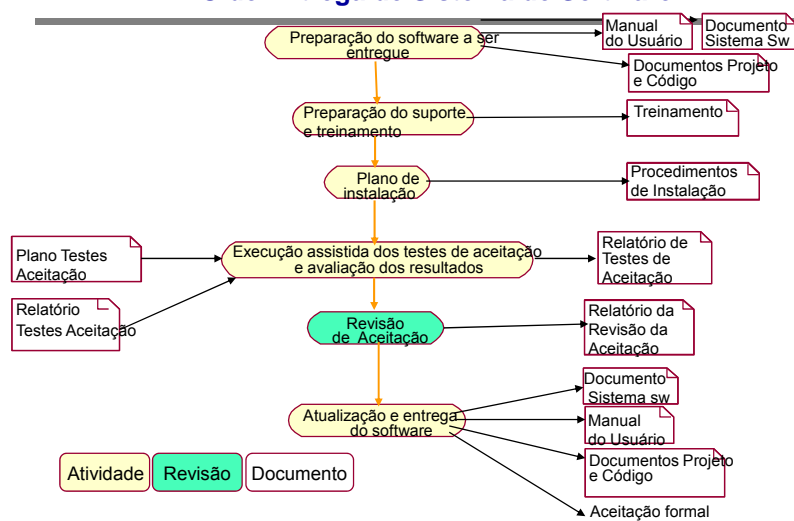
- ◆ Os documentos gerenciais do projeto serão de acordo com o modelo de documentação da ECSS;
- ◆ Padrão de documentação de projeto e metodologia de desenvolvimento para o software serão baseados nos utilizados no desenvolvimento da versão anterior ;
- ◆ Abordagem focada na garantia de produto e de processo.
- ◆ O processo de desenvolvimento do software será de acordo com os Procedimentos Operacionais (POs) definidos pela equipe de software.

Procedimentos Operacionais (PO)

Seis Procedimentos Operacionais (baseados na ECSS E-40, NBR 15100, e Processo Unificado UP):

- ◆ Análise do Serviço Solicitado;
- ◆ Planejamento e Desenvolvimento de Sistema de Software;
- ◆ Entrega de Sistema de Software;
- ◆ Aquisição de Sistema de Software;
- ◆ Recebimento de Sistema de Software;
- ◆ Manutenção de Sistema de Software.

PO de Entrega de Sistema de Software



SOAB : Ambiente de Desenvolvimento e Testes

- ◆ Laboratório de Engenharia de Software:
 - ◆ aquisição de ferramentas para desenvolvimento e garantia dos produtos do projeto;
 - ◆ capacitação dos membros da equipe.

- ◆ Laboratório de Simulação e Teste:
 - ◆ idealização de um ambiente de testes adequado para qualificação do software;
 - ◆ atividades de "procurement" para o projeto e para o desenvolvimento do ambiente de testes.

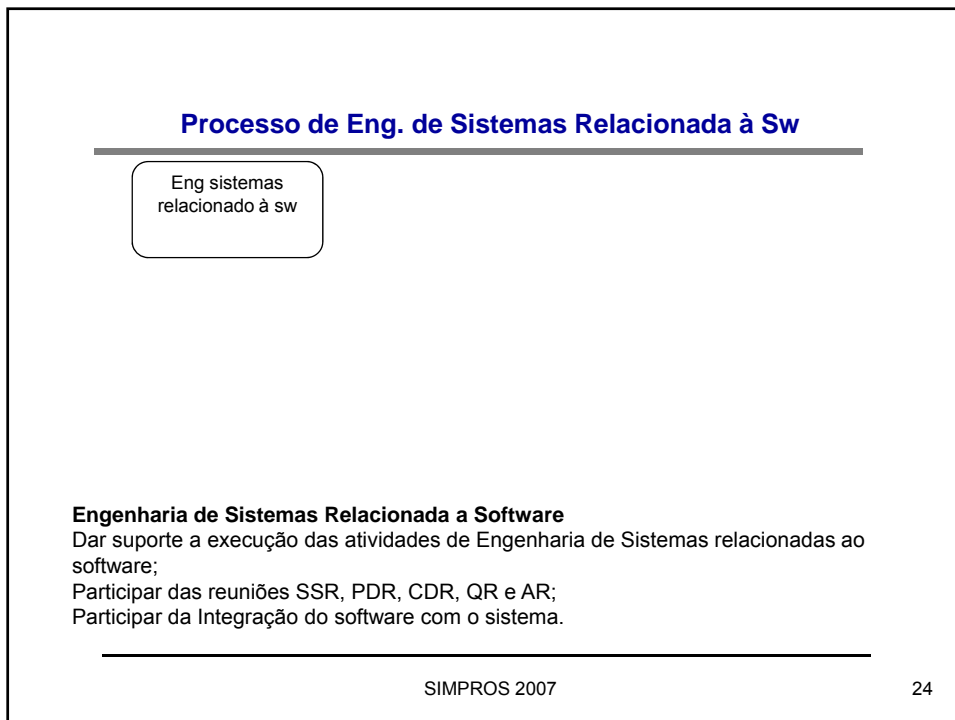
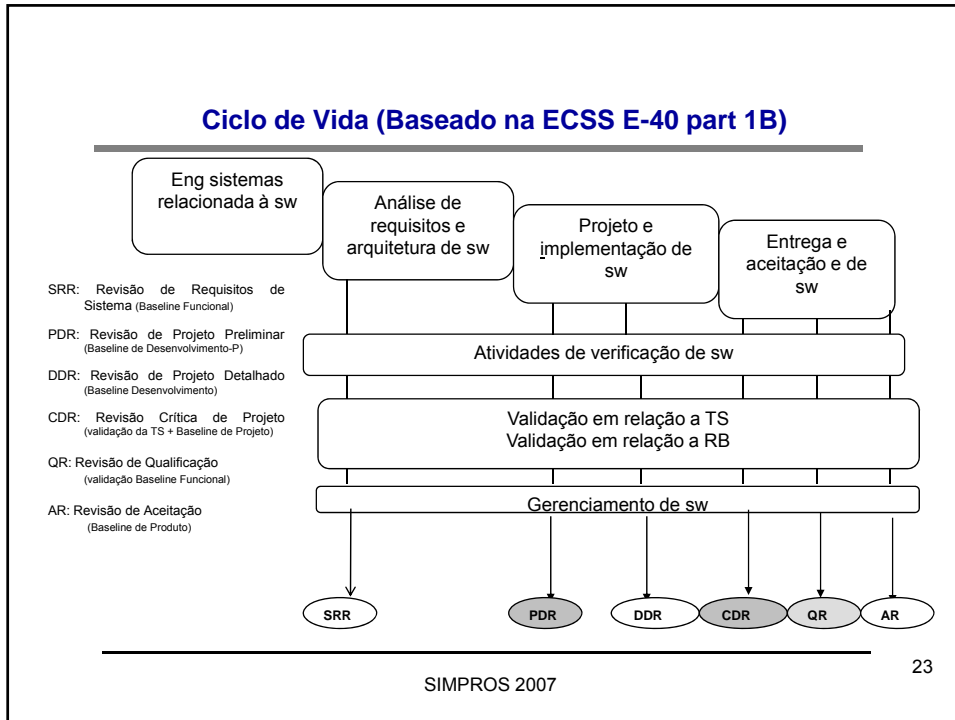
SOAB : Reutilização

Reutilização e atualização dos produtos de software já existentes:

- ◆ Algoritmos de controle do veículo;
- ◆ Modelos lógicos;
- ◆ Documentação;
- ◆ Definição de Interfaces;
- ◆ Código fonte;
- ◆ Casos de Testes.

Levando-se em consideração:

- ◆ Avaliação do item em relação aos requisitos aplicáveis, incluindo os requisitos de qualidade;
- ◆ Realização de inspeção nos produtos (os reutilizados inicialmente);
- ◆ Fortemente baseado na validação e teste.



Processo de Análise de Requisitos e Arquitetura de Sw

Análise de
requisitos e
arquitetura de sw

Análise de Requisitos e Projeto de Arquitetura de Software

Definir o quanto do software já desenvolvido na versão anterior, incluindo seus modelos, será reutilizado;

Analisar e especificar os requisitos de software;

Especificar a arquitetura do software;

Elaborar Documentação (Doc Req, Sw, Doc Projeto Sw, Plano Teste e Integração Sw);

Participar e Elaborar o relatório da PDR.

SIMPROS 2007

25

Processo de Projeto e Implementação de Sw

Projeto e
implementação de
sw

Projeto e Implementação de Software

Elaborar o projeto detalhado dos componentes de software;

Elaborar os testes das unidades e componentes de software;

Preparar o ambiente de testes

Codificar e executar testes de software;

Executar a integração CSW-CSW no ambiente de desenvolvimento;

Executar a integração CSCI -Target no ambiente de desenvolvimento;

Efetuar a análise de confiabilidade e segurança do software e emitir o Relatório de Análise da Criticalidade do Software.

SIMPROS 2007

26

Processo de Verificação de Sw

Atividades de verificação de sw

Verificação

Elaborar e implantar o Plano de V&V de Software;
Executar as atividades de verificação de Interfaces (ICD);
Executar as atividades de verificação da Arquitetura do Software;
Executar as atividades de verificação do Projeto Detalhado;
Executar as atividades de verificação do Código Fonte;
Executar as atividades de verificação da integração CSW-CSW;
Executar as atividades de verificação das especificações de testes;
Preparar a Matriz de Rastreabilidade de Requisitos.

SIMPROS 2007

27

Processo de Validação de Sw

Validação em relação a TS
Validação em relação a RB

Validação

Elaborar e implantar o Plano de V&V de Software;
Executar as atividades de Validação em relação à Especificação Técnica - TS;
Executar as atividades de Validação em relação à Baseline de Requisitos - RB;
Preparar e participar da PDR e DDR, CDR, QR;
Validar a Matriz de Rastreabilidade de Requisitos;
Participar da execução dos Testes de Aceitação de Software - ATP;
Elaborar Relatórios de Testes de Validação;
Elaborar o relatório da CDR e QR.

SIMPROS 2007

28

Processo de Entrega e Aceitação de Sw

Entrega e
aceitação e de
sw

Entrega e Aceitação

Preparar o software para entrega e instalação no sistema;
Elaborar o procedimento de instalação;
Instalar o software no ambiente operacional;
Acompanhar o cliente na preparação e execução dos Testes e Aceitação;
Participar e elaborar o relatório da AR.

Processo de Entrega e Aceitação de Sw

Gerenciamento de sw

Gerenciamento do Desenvolvimento de Software

Elaborar o Plano de Desenvolvimento das Modificações do software;
Implantar o Plano de Desenvolvimento do software;
Gerenciar o desenvolvimento do software;
Gerenciar a procura e compra de móveis, utensílios, equipamentos, serviços e sw;
Gerenciar a execução do projeto e implantação das instalações necessárias ao desenvolvimento do software, incluindo área para reuniões;
Gerenciar o treinamento dos profissionais que participarão do desenvolvimento do sw;
Gerenciar os riscos;
Realizar a interface com as outras áreas de gestão do projeto;
Elaborar versões atualizadas deste Plano de Desenvolvimento SW na SRR, PDR e CDR, caso necessário;
Participar das Reuniões de Revisão;
Preparar e participar de Reuniões Internas.

Considerações finais

Considerações

As boas práticas para as atividades de gerenciamento e desenvolvimento de software crítico devem:

- ♦ Garantir a qualidade e a confiança no funcionamento de seus produtos e processos;
- ♦ Prover informações importantes relativas à habilidade que uma organização possui para produzir um software confiável e de boa qualidade;

Considerações

- ♦ Falhas em desenvolver e manter software de forma disciplinada podem resultar em um atraso caro e, no pior caso, em conseqüências catastróficas.
- ♦ Adotar padrões de software é um dos caminhos de manter o desenvolvimento de software sob controle e garantir um nível adequado de qualidade e confiabilidade.

Considerações: desafios da área espacial

Rápida evolução tecnológica: novas tecnologias são introduzidas muito rapidamente no mercado, diminuindo o tempo de amadurecimento de um produto. Introdução do conceito do desconhecido em sistemas (unknown unknowns).

Alteração da natureza dos acidentes: muita das abordagens para prevenir acidente que trabalharam com componentes eletromecânicos são ineficazes em controlar acidentes que surgem do uso de sistemas digitais e de software.

Considerações: desafios da área espacial

Novos tipos de riscos: software é um item de segurança-crítica, desempenhando um papel de importância crescentemente em acidentes.

Aumento da complexidade e do acoplamento: o desenvolvimento e operação de alguns sistemas é tão complexo que desafia a compreensão de qualquer pessoa e de até mesmos de peritos, que, muitas vezes não têm informações completas sobre seu comportamento potencial.

Considerações: desafios da área espacial

Intolerância cada vez maior com acidentes: as novas descobertas científicas e tecnológicas têm aumentado o grau dos perigos, criando novos (como exposição de radiação e poluição química), e podendo prejudicar potencialmente um número crescente de pessoas, através da poluição ambiental e de danos genéticos.

Mudanças de regulamentação e visões públicas de segurança: os indivíduos não têm mais a habilidade de controlar os riscos ao seu redor e o governo necessita assumir uma responsabilidade maior pelo controle da segurança, através das leis e das várias formas de fiscalização e regulamentação.

Considerações

Ao longo de história, invenções e novas tecnologias freqüentemente chegaram à frente do conhecimento atual da ciência e da engenharia, mas o resultado sempre foi um acréscimo nos riscos e nos acidentes.

Muitos dos acidentes recentes, onde foram atribuídos erros do operador, podiam ser mais precisamente endereçados como resultante de falhas de sistema, de software, ou de projeto de interface.

Considerações

A adoção de processos de desenvolvimento de software bem definidos na área espacial é mandatório.

Em áreas onde o uso e o domínio da tecnologia é essencial para que seja atingido um objetivo considerado estratégico para uma nação ou empresa, esta tem obrigação de buscar a melhoria contínua de seus processos, a fim de alcançar um índice de maturidade compatível com a tecnologia desenvolvida.

Obrigado pela atenção!

Contato:
lahoz@iae.cta.br
55 12 39474901

