5º SeP P&D

Seminário de Projetos de Pesquisa e Desenvolvimento em Veículos Espaciais e Tecnologias Associadas & Workshop Tendências Futuras para Veículos Lançadores

VERIFICAÇÃO E VALIDAÇÃO DE SOFTWARE PARA PROJETOS ESPACIAIS

Carlos Henrique Netto Lahoz – Miriam Célia Bergue Alves

Divisão de Eletrônica/Instituto de Aeronáutica e Espaço
(lahozchnl; miriammcba)@iae.cta.br
Comando-Geral de Tecnologia Aeroespacial - São José dos Campos - SP

OBJETIVO E JUSTIFICATIVA

No cenário internacional, os sistemas espaciais desenvolvidos pela indústria e pelo governo crescem em tamanho e complexidade, exigindo que o desenvolvedor e o cliente tenham completa confiança de que o sistema está correto e que ele atende a padrões de desenvolvimento, segurança, verificação e validação Este projeto visa à formação, à capacitação de recursos humanos e agregação de especialistas, que possam contribuir para a Verificação e Validação (V&V) de sistemas de software espaciais empregados no desenvolvimento e inovação tecnológica de veículos espaciais brasileiros, em particular nos lançadores de satélite. Os resultados obtidos com a aplicação do projeto incluem (a) formação e capacitação de recursos humanos nestas técnicas para a área espacial, tanto aqueles pertencentes ao IAE como os bolsistas envolvidos, que estarão, assim, melhor preparados para emprego na indústria aeroespacial; (b) obtenção de recomendações de melhorias para os projetos atuais e futuros do IAE, com infusão de técnicas inovadoras de V&V.

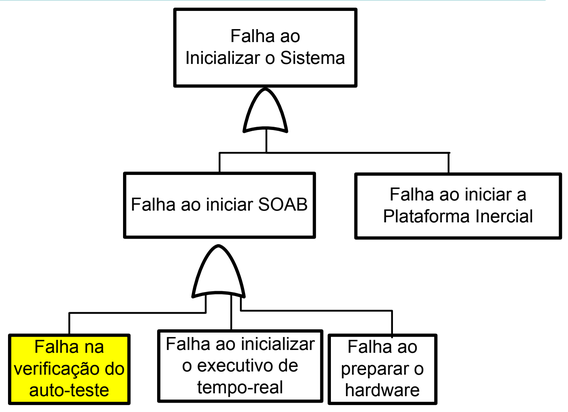
Fase 1: ANÁLISE DE DEPENDABILIDADE:

Compreende o uso integrado de técnicas de análise de segurança, voltadas à identificação e correção de possíveis falhas de sistemas fortemente baseados em software. Serão utilizadas as técnicas SFTA (Software Fault Tree Analysis), SFMECA(Software Failure Mode and Effect and Criticality Analysis), SHAZOP (Software Hazard and Operability studies).

A metodologia da abordagem proposta é dividida em quatro fases distintas:

1) Preparação para aplicação do processo de análise de dependabilidade. Nesta fase são definidos os modos de falha genéricos e específicos aos requisitos e suas funções associadas, a classificação da severidade e da probabilidade.

2) Aplicação de SFTA nos requisitos do sistema para software e em seus respectivos requisitos de função de software. O evento será caracterizado pela falha do requisito de sistema para software e os eventos primários caracterizados pelas falhas de software em atender o requisito de sistema.



3) Aplicação de SFMECA aos eventos básicos da SFTA, identificando os possíveis modos de falha, suas conseqüências, criticalidade e provisões de compensação.

4) Identificar, a partir das provisões de compensação, requisitos funcionais e não funcionais que devem ser incorporados ao sistema para aumentar a confiança no seu funcionamento.

Modo de Falha	Causa de Falha	Efeito Local	Efeito Final	Severidade	Provisões Compensatórias
Função não executada (resultados não produzidos)	Cálculos computacionais não realizados. – *Verificações e produção de resultados não realizados.*	Função termina (abruptamente) sem realizar as verificações necessárias para produzir o resultado da função. Resultados não são produzidos.	Não é emitido o fluxo Ini_Sis. A passagem para o modo SEG fica desabilitada e permanece no modo VER. Sistema fica no estado de verificação.	Elevado	A ocorrência de uma falha em qualquer uma das subfunções da função "Iniciar SOAB" implica que o sistema deve continuar no estado de verificação. ***Referência:*** *SRS – Processo – 1.1 Iniciar SOAB*
	Resultados não produzidos – *Apesar de serem realizadas as verificações necessárias, os resultados não são produzidos.*	Função termina (abruptamente) apesar de ter realizado as verificações necessárias para produzir o resultado da função. A variável de estado de função ESTADO_AUTO_TESTE fica por definir. Resultados não são produzidos.	Não é emitido o fluxo Ini_Sis. A passagem para o modo SEG fica desabilitada e permanece no modo VER. Sistema fica no estado de verificação.	Elevado	A ocorrência de uma falha em qualquer uma das subfunções da função "Iniciar SOAB" implica que o sistema deve continuar no estado de verificação. ***Referência:*** *SRS - Processo-1.1 Iniciar SOAB*

Resultados obtidos até o momento (março/2011):

1) Contratação de um Bolsista DTI:para realizar a análise de dependabilidade de um estudo de caso do sistema computacional de um foguete hipotético, baseado no VLS-1.
2) Modelagem da SFTA dos requisitos de sistema e de software do estudo de caso.
3) Preparação para a análise SFMECA do estudo de caso.
4) Participação de um membro da Equipe no "Workshops on Spacecraft Flight Software", EUA.
5) Participação de um membro da equipe no "IEEE International Conference on Software Testing, Verification and Validation", Alemanha.
6) Aceitação de dois trabalhos para serem apresentados no "Fifth Latin American Symposium on Dependable Computing", Brasil.

Fase 2: VERIFICAÇÃO E VALIDAÇÃO COM ENFOQUE NA TOLERÂNCIA A FALHAS

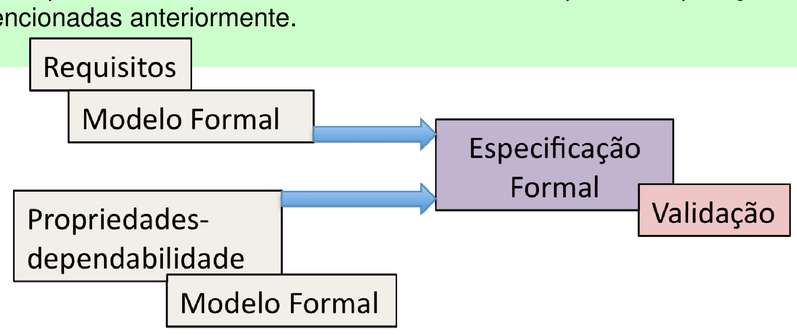
Nesta fase será investigado o uso de técnicas formais em adição as técnicas de análise de dependabilidade. Um dos grandes benefícios desta abordagem é que ela move alguns dos testes realizados somente no código fonte finalizado para ao atuais requisitos do sistema. Ou seja, técnicas formais são utilizadas para validar os requisitos e não somente o código que é gerado a partir dos requisitos (vide figura abaixo). Os requisitos funcionais e não funcionais resultantes da fase 1 serão modelados formalmente e validados para assegurar que os resultados e recomendações desta primeira fase de estudos foram aplicados e implementados corretamente no sistema. Esta fase compreende as seguintes macro etapas:

1) Criação dos modelos formais (uma ou mais técnicas poderão ser empregadas).

2) Verificação automática do modelo e suas propriedades (Validação assistida por computador).

3) Avaliação dos resultados da aplicação dos métodos formais e análise de dependabilidade no sistema em estudo pelos colaboradores externos. Serão analisados os resultados da aplicação destas técnicas no estudo de caso com a participação de consultores externos especializados.

4) Análise comparativa do sistema em estudo antes e depois da aplicação das técnicas e análises mencionadas anteriormente.



Fase 1: NOV/2010 a OUT/2011

Descrição das atividades	periodo
Levantamento e exercício de técnicas de dependabilidade para serem aplicadas no projeto. Definição do estudo de caso e início da aplicação de técnicas de dependabilidade.	JAN a ABR/11
Contratação de um bolsista DT2 (24 meses). Compras de material/serviço de custeio.	NOV/10 a OUT/11
Visita de um colaborador internacional no Brasil.	SET/11
Reunião técnica no NASA IV&V para dois membros da equipe de projeto (2011).	AGO/11
Participação em evento internacional de dois membros do projeto.	DEZ/10 e MAR/11

Fase 2: NOV/2011 a OUT/2012

Descrição das atividades	periodo
Construção dos modelos formais. Aplicação de técnica de V&V. Verificação automática dos modelos assistida por computador.	NOV/11 a AGO/12
Análise de dependabilidade dos modelos do sistema em estudo e nova aplicação de técnicas para prevenção, tolerância e remoção das fragilidades ainda identificadas nesta fase de análise.	JAN a AGO/12
Análise comparativa do sistema em estudo antes e depois da aplicação das técnicas e análises.	JAN a AGO/12
Continuação de uma bolsa e contratação de mais 2 bolsistas DTI 2 por 12 meses.	NOV/11 a AGO/12
Visita de um colaborador internacional ao Brasil.	SET/12
Participação em evento internacional de dois membros do projeto.	ASD
Fechamento do projeto, com a compilação dos estudos e das recomendações feitas pela equipe de projeto e divulgação dos resultados.	SET a OUT/12

Fonte de Financiamento:
Edital CNPq/MCT/AEB 33/2010
Processo 559973/2010-1

Custo do Projeto:

Bolsas DTI :	144.000,00
Custeio:	80.128,00
Capital:	2.000,00

Os autores gostariam de agradecer o suporte do CNPq através do Auxilio Financeiro a Projeto – processo #559973/2010-1