6º 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 Sistemas de Software para Projetos Espaciais

Coordenador: Carlos H.N. Lahoz
Equipe: Miriam C. B. Alves
Martha A. D. Abdala
Luciene Bianca Alves (bolsista DTI)
Fernando Nicodemos (bolsista DTI)

Apoio

Tópicos:

1- Objetivo

2- Cronograma

3- Custo total estimado/fonte de financiamento

4- Abordagem adotada

5- Resultados (obtidos até a presente data)

6- Perspectivas futuras

7- Agradecimentos

Referencias

1- Objetivos

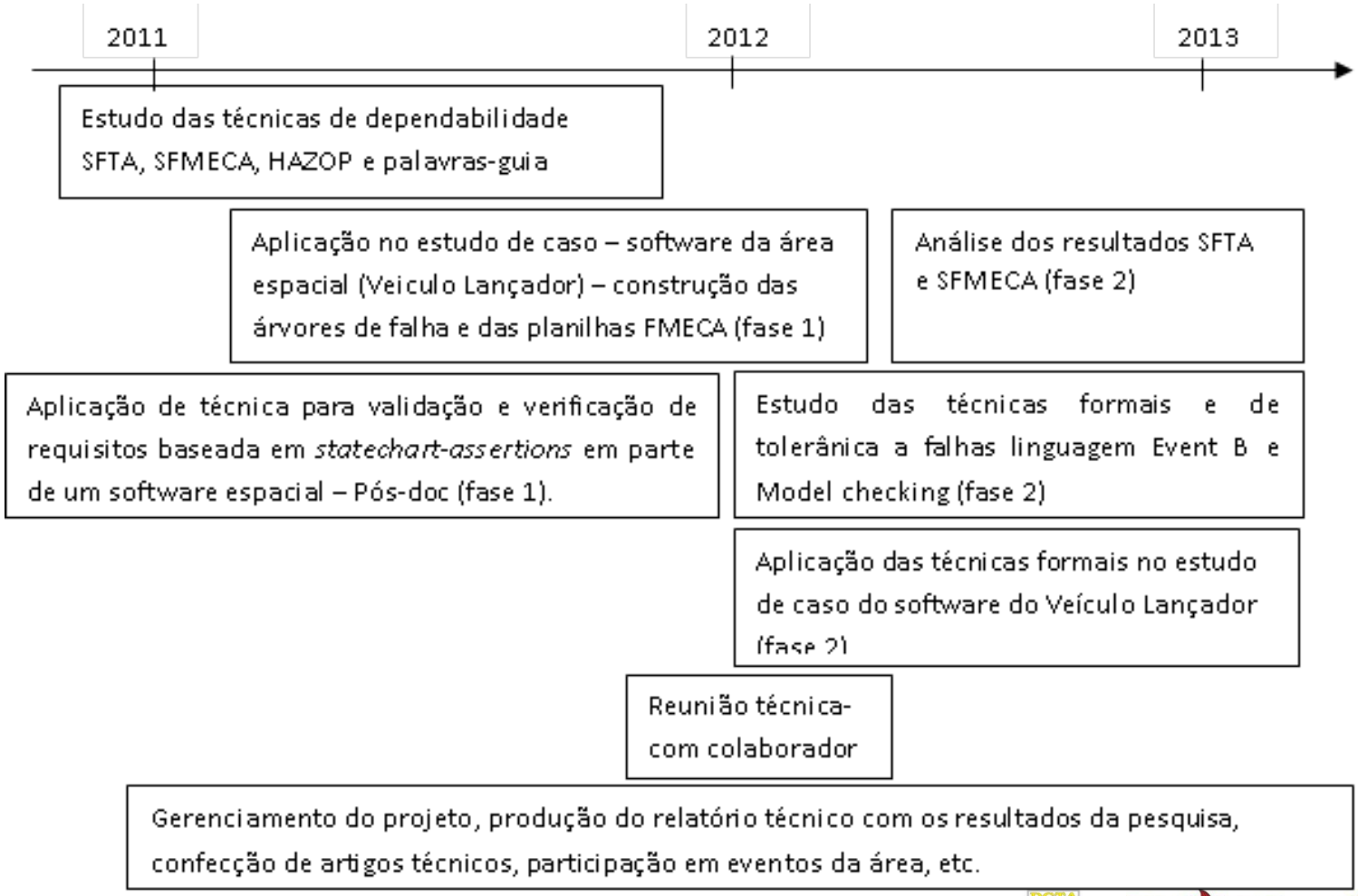
Objetivo Principal

- Capacitação na área de dependabilidade, verificação e validação de software espacial.

Objetivo específicos

- Desenvolver uma abordagem híbrida de V&V baseada em análise de dependabilidade e técnicas formais de V&V para aplicação em sistemas espaciais.
-Aplicar a abordagem desenvolvida em um estudo de caso (software de controle de voo de um lançador).
- Capacitação de recursos humanos (bolsistas CNPq) cuja absorção poderá ser feita no âmbito dos órgãos setoriais integrantes do Sistema Nacional de Desenvolvimento das Atividades Espaciais (SINDAE).

2- Cronograma



3- Custo total estimado/fonte de financiamento

Despesas de custeio: R$ 80.128,00

Despesas de capital: R$ 2.000,00

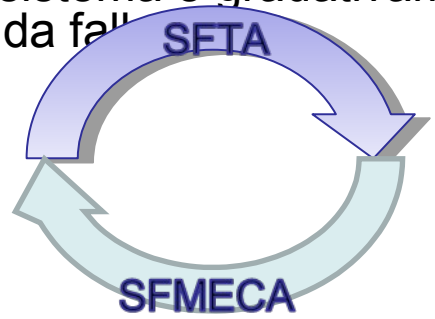
Concessão de bolsas DTI-B R$ 144.000,00

Processo CNPq/AEB/MCT 033/2010
559973/2010-1(Aprovado em 25/10/2010)

4- Abordagem adotada

Análise de Dependabilidade SFTA + SFMECA

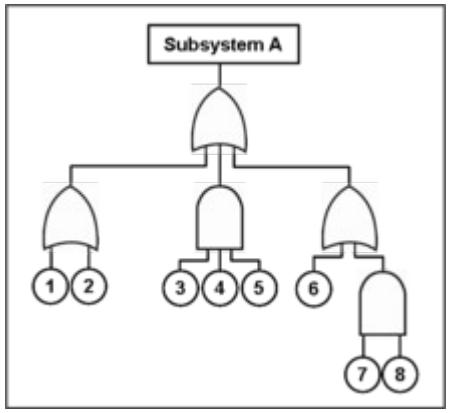
- Busca uma visão mais agregada do sistema iniciando seu exame pelas principais funcionalidades do sistema e gradativamente descendo até as subfuncionalidades até a raiz da fal



Tarefa 1: Mapeamento dos requisitos do software.
Tarefa 2: Construção das Árvores de Falha (SFTA) para cada potencial falha de requisito.
Tarefa 3: Aplicação da Análise de Modos de Falha, Efeitos e Criticalidade de software (SFMECA).
Tarefa 4: Recomendação de Provisões de Compensação .
Tarefa 5: Geração de requisitos não-funcionais para o Software.

4- Abordagem adotada

Análise de Dependabilidade: SFTA



Dedutiva (top down) tecnica focada em como os eventos normais do sistema podem conduzir a perigos.

Evento topo = perigo (falhas em requisitos de sistema para software)

Eventos básicos = conjunto de possiveis causas (falhas em requisitos de software)

4- Abordagem adotada

Análise de Dependabilidade: SFMECA

Indutiva (bottom-up) metodo usado para encontrar porblemas potenciais no sistema.

SFMECA é aplicada nos eventos basicos da SFTA, identificando potenciais modos de falha, consequencias, severidade e possiveis provisões de compensação.

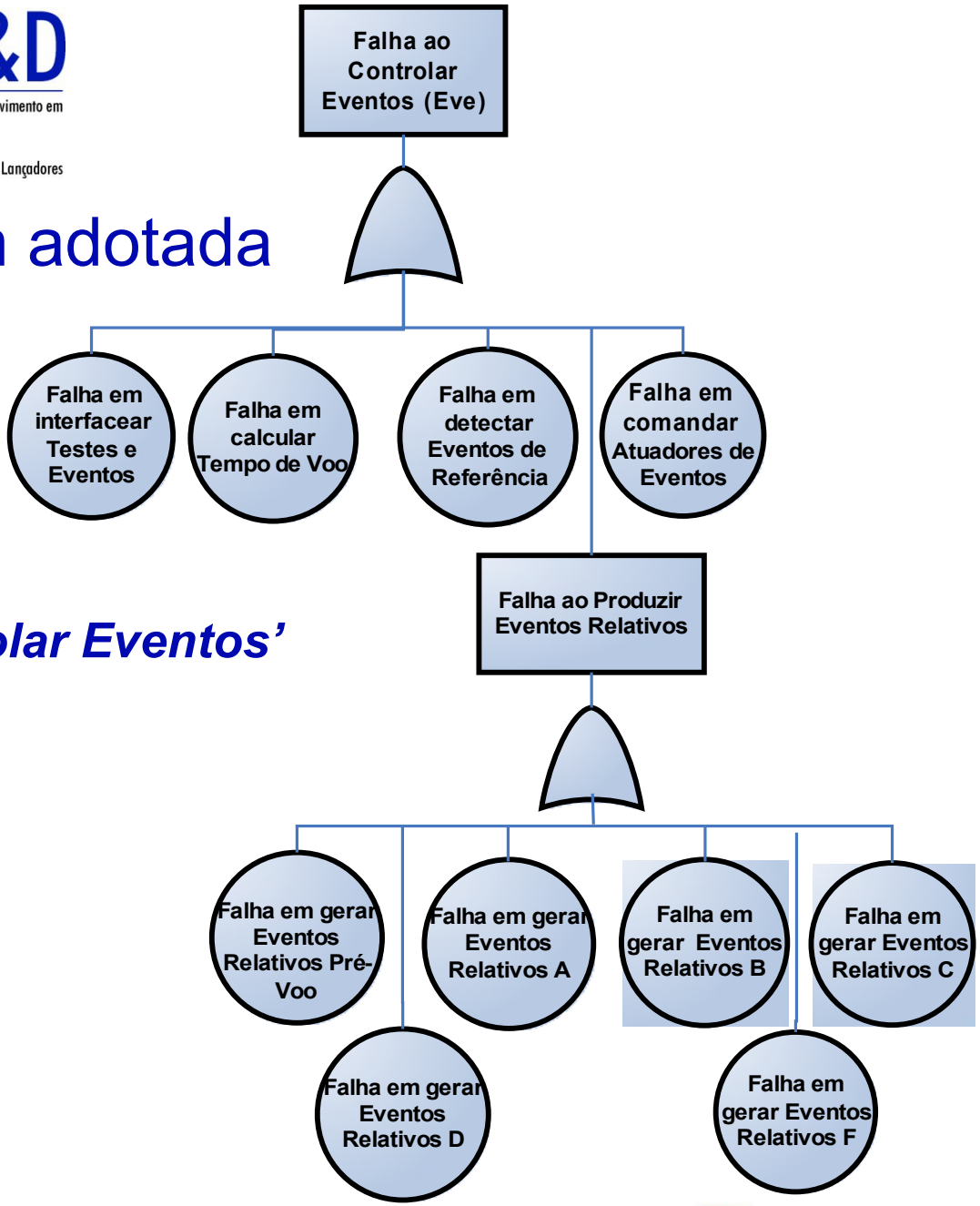
POTENTIAL
FAILURE MODE AND EFFECTS ANALYSIS
Front Door L.H.

System: 1 - Automobile
Subsystem: 2 - Closures
X Component: 3 - Front Door L.H.
Model Year(s)/Vehicle(s): 199X/Lion 4dr/Wagon
Core Team: A. Tate Body Engrg, J. Smith - QC, R. James - Production, J. Jones - Maintenance
Process Responsibility: Body Engineering
Key Date: 3/31/2003
FMEA Number: 1450
Page 1 of 1
Prepared By: J. Ford - X6521 - Assy Ops
FMEA Date (Orig.): 3/10/2003 (Rev): 3/21/2003

Item / Process Function/Requirements	Potential Failure Mode	Potential Effect(s) of Failure	Sev	Class	Potential Cause(s)/Mechanism(s) of Failure	Occur	Current Process Controls Prevention	Current Process Controls Detection	Detec	RPN	Recommended Action(s)	Responsibility & Target Completion Date	Actions Taken	Actions Taken	Sev	Occur	Det	RPN
3 - Front Door L.H.																		
Manual application of wax inside door. To cover inner door, lower surfaces at minimum wax thickness to retard corrosion.	Insufficient wax coverage over specified surface.	Deteriorated life of door leading to: - Unsatisfactory appearance due to rust through paint over time. - Impaired function of interior door hardware.	7		Manually inserted spray head not inserted far enough.	8		Visual check each hour - 1shirt for film thickness (depth meter) and coverage.	5	280	Add positive depth stop to sprayer.		Stop added, sprayer checked on line.		7	2	5	70
					Spray head clogged - Viscosity too high - Temperature too low - Pressure too low.	5		Test spray pattern at start-up and after idle periods, and preventive maintenance program to clean heads.	3	105					7	1	3	21
					Spray head deformed due to impact.	2		Preventive maintenance program to maintain heads.	2	28					7	2	2	28
					Spray time insufficient.	8		Operator instructions and lot sampling (10 doors/shift) to check for coverage of critical areas.	7	392					7	1	7	49

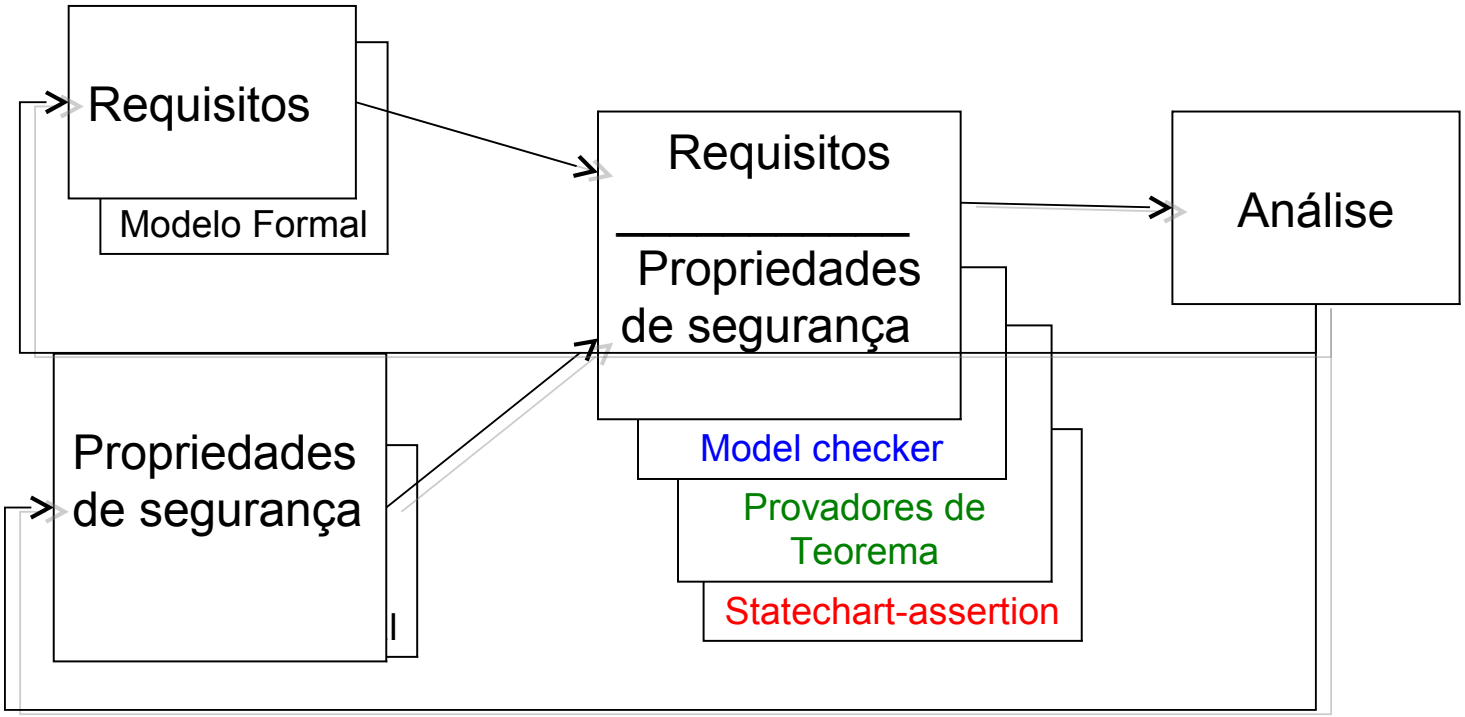
4- Abordagem adotada

SFTA, *'Controlar Eventos'*



4- Abordagem adotada

Abordagem Formal com enfoque em Dependabilidade

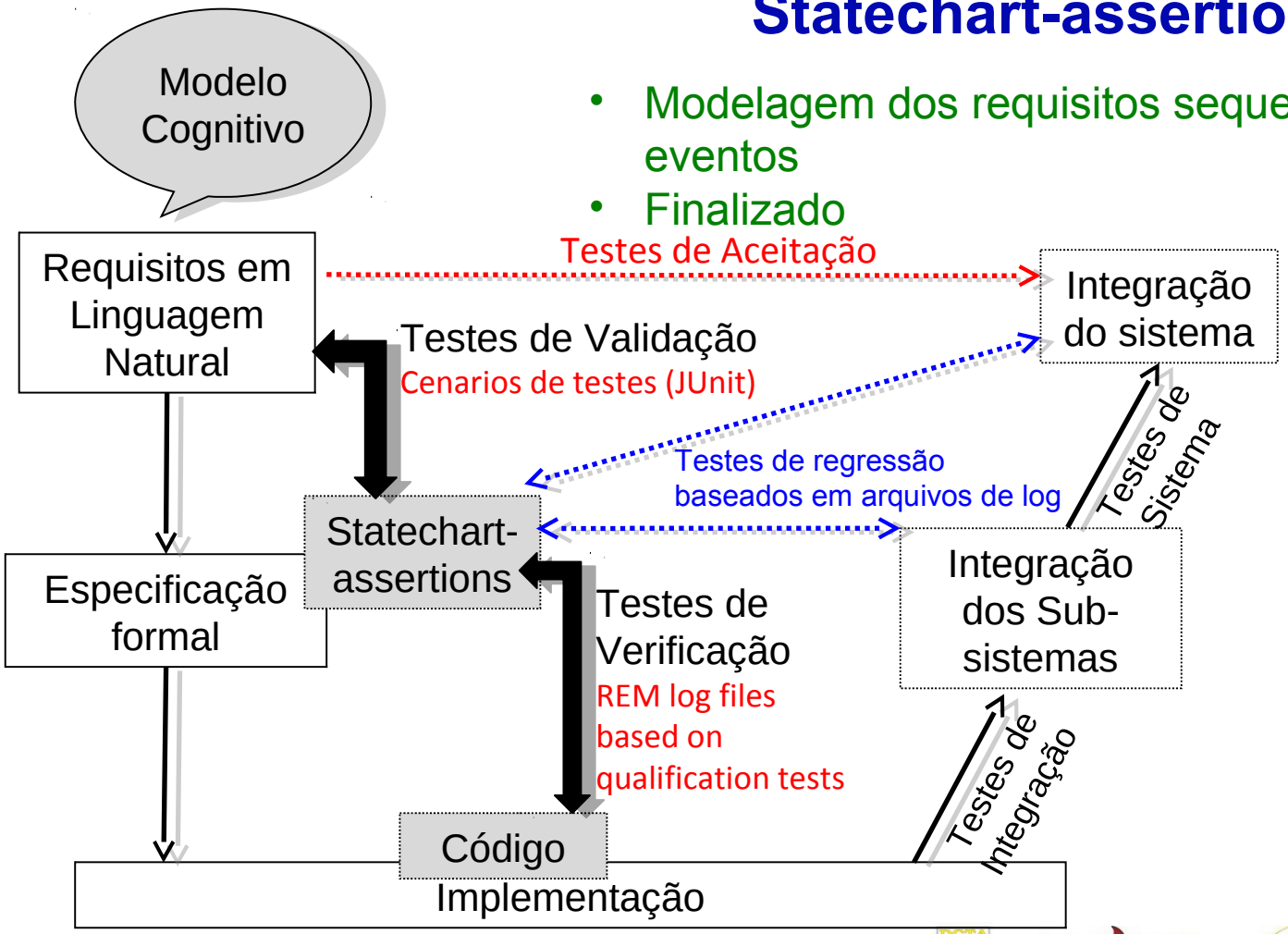


mellhorias/correções

4- Abordagem adotada

Verificação e Validação usando Statechart-assertions

- Modelagem dos requisitos sequencia de eventos
- Finalizado

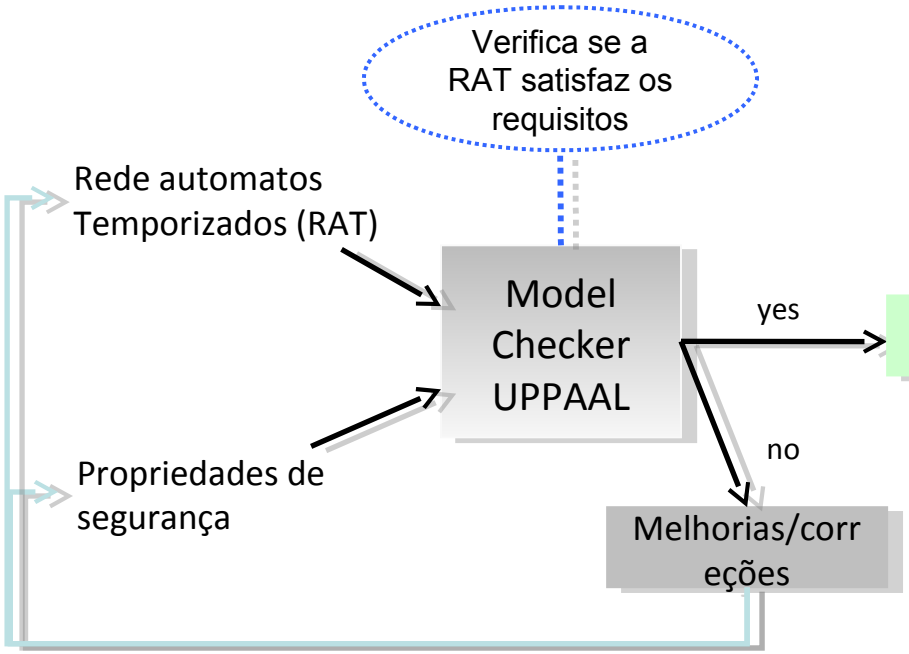


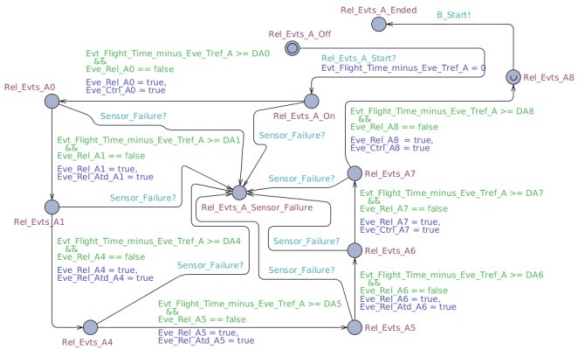
Apoio

4- Abordagem adotada

Modelagem e Verificação usando Model-checker

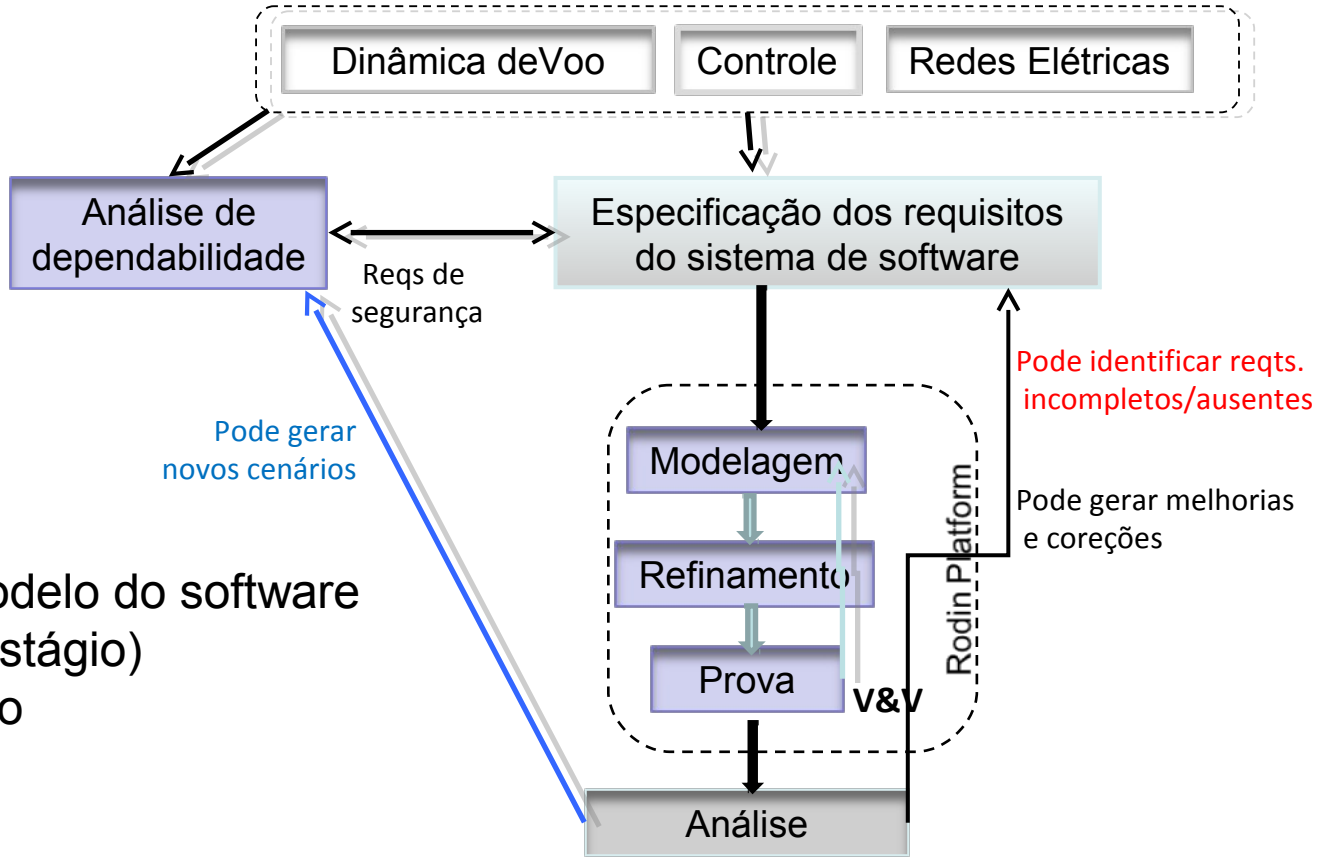
- Criação do modelo da sequencia de eventos de voo e dos sensores
- Em andamento





4- Abordagem adotada

Modelagem e Verificação usando Provadores de Teoremas



- Criação do modelo do software de bordo (1º estágio)
- Em andamento

5- Sumário dos Resultados obtidos até o momento

- **SFTA - Produção de 6 Árvores de Falhas** (Eventos topo)
  - 16 eventos intermediários e 82 eventos básicos.

- **SFMECA: Produção de 34 Análises de Falha** (Eventos base)
  - 24 análises referentes ao requisito 'Controlar Voo'
  - 10 análises referentes ao requisito 'Controlar Eventos'

- **Modelos formais dos requisitos (statechart-assertions)**
  - 44 requisitos formalmente especificados e validados.
  - 220 testes de validação.
  - 176 testes de verificação.
  - Aplicação de outras duas técnicas formais em andamento.

6- Perspectivas futuras /desafios a serem vencidos

- Estudo de uma abordagem quantitativa para SFTA.
- Priorizar as provisões de compensação mais criticas (código ou modelos formais verificáveis).
- Gerar requisitos de segurança advindos da análise de dependabilidade.
- Análise comparativa dos resultados.
- Definição de processo/metodologia/técnica mais adequada em função do tipo de sistema a ser desenvolvido.

7- Agradecimentos

✓ AEB – Agência Espacial Brasileira

✓ IAE – Instituto de Aeronáutica e Espaço

✓ CNPq - Conselho Nacional de Desenvolvimento Científico e Tecnológico.

Referências

ECSS-Q-80-03 (Draft 01/03/2006) - Space Product Assurance: Methods and techniques to support the assessment of software dependability and safety, Noordwijk, 2006;

ECSS-Q-ST-30-02C (06/03/2009) - Space Product Assurance: Failure modes, effects (and criticality) analysis (FMEA/FMECA), Noordwijk, 2009;

JPL D-28444 (Rev.#0 02/05/2005) - Software Fault Analysis Handbook (Software Fault Tree Analysis (SFTA) & Software Failure Modes, Effects and Criticality Analysis (SFMECA));

NASA Software Safety Guidebook, NASA TECHNICAL STANDARD, March, 2004 http://www.hq.nasa.gov/office/codeq/doctree/871913.htm.

Referências

D. Drusinsky, Modeling and Verification Using UML Statecharts – A Working Guide to Reactive System Design, Runtime Monitoring and Execution-based Model Checking, Burlington, Mass.: Elsevier, 2006..

P. Berander and P. J nsson, “A goal question metric based approach for efficient measurement framework definition,” Proc. ACM/IEEE Int. Symposium on Empirical Softw. Eng., Rio de Janeiro, Brazil, Sept. 2006, pp. 316-325.

F. Schneider, S.M. Easterbrook, J.R Callahan, and, G.J. Holzmann, “Validating requirements for fault tolerant systems using model checking”, In Proceedings of 3rd International Conference on Requirements Engineering (ICRE'98), 1998.

B. Berard, M. Bidoit, A. Finkel, F. Laroussinie, A. Petit, L. Petrucci, Ph. Schnoebelen and P. McKenzie, *System and Software Verification: Model-Checking Techniques and Tools*, Springer-Verlag Berlin Heidelberg, 2001, pp. 39-58

Event-B and the Rodin Platform. http://www.event-b.org/index.html. Accessed 27 Jan. 2012 .

Contatos

Carlos Lahoz
lahozchnl@iae.cta.br

Miriam Alves
miriammcba@iae.cta.br

Martha Addala
marthamada@iae.cta.br