Uma abordagem de MBSE para a missão Garatéa-L

Renan G. S. Menezes[1], Linélcio S. Paula[1], Emerson H. S. Oliveira[1], Luís E. V. Loures da Costa[1], Jonas B. Fulindi[1], Lucas Fonseca[2]
[1]Instituto Tecnológico de Aeronáutica (ITA), São José dos Campos/SP – Brasil
[2]CEO, Airvants – Brasil

***Resumo* – Este artigo apresenta os principais resultados da aplicação de uma abordagem *Agile System Engeneering* no estudo de caso da missão Garatéa-L (primeira missão lunar brasileira), utilizando MBSE e a linguagem descritiva de sistemas SysML. Dentro dos princípios dos métodos ágeis, foram realizados *Loop's* de projeto, processo de elicitação de requisitos, *Lab Meetings*, interação dinâmicas com os *stakeholders*. À partir da aplicação dessa abordagem foi possível desenvolver o Conceito de Operações da missão, abrangendo informações essenciais para o entendimento das necessidades dos *stakeholders*, e realizar a modelagem através do SysML. Os diagramas criados foram: *Use Cases*, Diagrama de Sequências "*White Box*" e Diagrama de Requisitos, e também foi realizada a análise de dependabilidade (*dependability*) e o estudo das alternativas da soluções (*trade studies*). Os resultados demonstram que a aplicação da abordagem ágil possibilita antecipar análises necessárias para o sucesso da missão e provê a rastreabilidade de requisitos em atendimento às necessidades dos *stakeholders*.**

***Palavras-Chave* – Garatéa-L, MBSE, SysML.**

I. INTRODUÇÃO

A abordagem ágil refere-se a um grupo de metodologias de desenvolvimento baseadas no processo interativo, em que os requisitos e as soluções evoluem por meio da colaboração entre equipes multifuncionais auto-organizadas [2].

Os métodos ágeis ou processos ágeis geralmente promovem um processo disciplinado de gerenciamento de projetos que incentiva inspeções frequentes e adaptação, uma filosofia de liderança que incentiva o trabalho em equipe, auto-organização e responsabilidade, um conjunto de melhores práticas de engenharia destinadas a permitir a entrega rápida de produtos de alta qualidade e uma abordagem de negócios que alinha o desenvolvimento com as necessidades do cliente e os objetivos da empresa [2].

O *International Council on Systems Engineering* (INCOSE) e o *Space Systems Working Group* (SSWG) iniciaram a investigação da aplicabilidade do MBSE (*Model-Based Systems Engineering*) para projetar CubeSats em 2011. O recente esforço do SSWG foi focado no desenvolvimento de um modelo de referência de *CubeSat* para ser usado pelos grupos de desenvolvimento das universidades [1].

O SysML (*Systems Modeling Language*) é comumente usado no MBSE, e é uma linguagem de modelagem gráfica desenvolvida pelo *Object Management Group* (OMG) com o propósito de ser utilizada na modelagem de uma ampla gama de problemas de engenharia. Não depende de nenhum método de engenharia de sistemas e destina-se a auxiliar vários métodos.

Renan G. S. Menezes, renang@ita.br; Linélcio S. Paula, linelcio@ita.br; Emerson H. S. Oliveira, emerson@ita.br; Luís E. V. Loures da Costa, loures@ita.br; Jonas B. Fulindi, fulindi@ita.br; Lucas Fonseca, fonseca.ldm@gmail.com.

É adequado para especificar requisitos, estrutura, comportamento, alocações e restrições nas propriedades do sistema para auxiliar em análises de engenharia [3].

II. MISSÃO GARATÉA-L

Garatéa vem do Tupi-Guarani "Busca Vidas" – A missão Garatéa-L [4] é primeira iniciativa brasileira de colocar uma sonda na órbita da Lua, essa missão visa responder algumas perguntas em relação ao entendimento da vida, olhando para o passado e tendo como perspectiva o futuro, para que se possa ter possíveis respostas da origem da vida, e em que condições ela tem potencial de existir. Sendo assim, essa missão tem um forte componente de Astrobiologia.

No Garatéa-L será embarcado um *Payload* com diversas colônias de microrganismos vivos e moléculas de interesse biológico, que serão expostas à radiação espacial por seis meses, com o objetivo de verificar quais efeitos o ambiente espacial fora da proteção da atmosfera e do campo magnético terrestre causarão nesses microrganismos, e como eles se comportarão nesse ambiente inóspito [7].

III. MEDOTOLOGIA

A engenharia de sistemas baseada em modelos (MBSE) é a aplicação formal da modelagem para suportar os requisitos do sistema, projeto, análise, verificação e atividades de validação, onde um modelo é uma representação de algo, sendo que ele não captura todos os atributos da coisa representada, mas apenas aqueles que parecem relevantes [2].

A missão Garatéa-L foi modelada de acordo com os conceitos de engenharia de sistemas ágeis, utilizando MBSE e a linguagem SysML.

IV. RESULTADOS

A. Conceito de operações

O Conceito de Operações é um documento utilizado para traduzir as expectativas dos *stakeholders* em requisitos de sistemas, ele tem como propósito descrever as características do sistema em ambiente operacional, ajudando usuários, clientes e gestores a entenderem os objetivos do sistema e o seu funcionamento.

Na Fig. 1 é apresentado o diagrama de contexto [5] para a missão Garatéa-L. O objetivo desse diagrama é apresentar uma visão inicial da missão e de como as partes interessadas se relacionam com o sistema de interesse.

Dentre as partes interessadas pode-se destacar a Comunidade Científica como o principal *stakeholder* da missão Garatéa-L. Ela poderá se beneficiar dos resultados obtidos pela missão, melhorando seu entendimento sobre a origem da vida humana na terra e sobre como ela reagiria em viagens do tipo *deep space*.

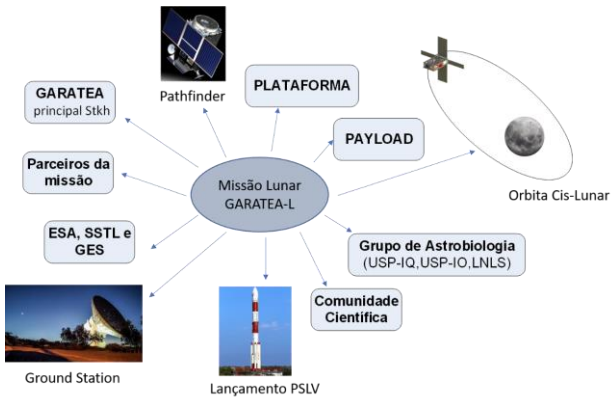

Fig. 1. Diagrama de contexto

B. Funções de sistema

Funções de sistema são declarações do que o sistema faz, essas funções devem ser relacionadas com os requisitos de *stakeholders*, mais especificamente, elas podem ser derivadas desses requisitos, e geralmente são mais qualitativas. Na Fig. 2 foram modeladas as funções do sistema através do diagrama de *Use Cases.*

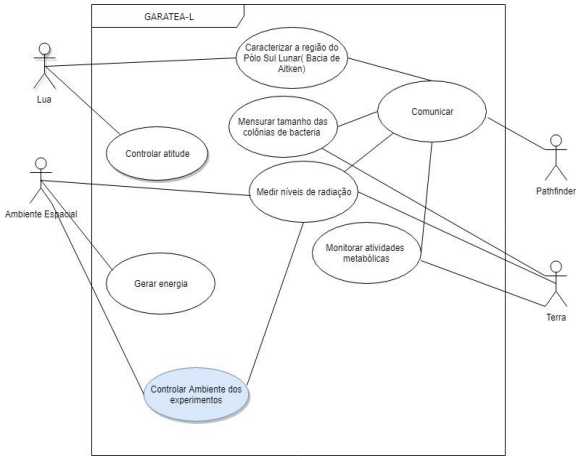

Fig. 2. *Use Cases* funções do sistema

Com a modelagem dos *Use Cases* é possível perceber as relações existentes na fronteira entre as funções de sistema e os atores envolvidos. A partir dessa identificação e correlação com os atores é possível criar outros diagramas e fazer análises. Como, por exemplo, o diagrama de sequência que permite uma análise de cenários, ou o diagrama de blocos, composto de portas e interfaces, que demonstra o fluxo de informações entre as interfaces. Esses diagramas ajudam no entendimento de como o sistema deve funcionar, além de auxiliar na identificação de requisitos de sistemas e interfaces.

C. Análise de dependabilidade

Dependabilidade (*Dependability*) é um termo coletivo usado para descrever o desempenho da disponibilidade e seus fatores de influência: confiabilidade, mantenabilidade e suporte logístico de manutenção. A dependabilidade é usada para descrições genéricas, sem expressão quantitativa [6].

Nesta abordagem de Engenharia de Sistemas Ágil foram utilizadas as ferramentas FMECA e FTA.

FMECA (*Failure Mode, Effects and Criticality Analysis*) é uma ferramenta adequada para levantamento de riscos do tipo técnico. Através dela é possível identificar panes (falhas) potenciais e seus efeitos, antecipando problemas de interface do sistema [6].

Os critérios para gerar a pontuação de cada caso de falha são apresentados nas Tabelas I e II.

TABELA I. CRITÉRIOS DA FMECA

OCORRÊNCIA (O)	CRITICIDADE (S)	DETETABILIDADE (D)
IMPROVÁVEL = 1	APENAS PERCEPTÍVEL = 1	ALTA = 1
MUITO PEQUENA =2	POUCA IMPORTÂNCIA = 2	MODERADA = 2
MODERADA = 3	MODERADAMENTE GRAVE = 3	MÉDIA = 3
ALTA = 4	GRAVE = 4	PEQUENA = 4
ALARMANTE = 5	EXTREMAMENTE GRAVE = 5	IMPROVÁVEL = 5

TABELA II. RPN (*RISK PRIORITY NUMBER*) = O x S x D

RISCO (RPN)
BAIXO (1 a 12)
MÉDIO (13 a 60)
ALTO (61 a 125)

Após definir os critérios, foi realizado o processo com a ferramenta FMECA. Na Tabela III a seguir é possível observar que o modo de falha e respectivamente os casos de falha com maior RPN (*Risk Priority Number*) foram: **Modo de Falha** – Sistema de processamento; **Casos de falha** – O software não funciona e o hardware não funciona.

TABELA III. FMECA

FMEA/FMECA SIMPLIFICADA - para use case "Controlar o ambiente dos experimentos"

ITEM	Modo de Falha	Caso de Falha	EFEITOS	S	D	O	RPN
1	Sensores de monitoramento do ambiente	Sensor de temperatura não funciona	Perda do monitoramento e controle de	4	1	2	8
		Sensor de pressão não funciona	Perda do monitoramento e controle de	4	1	2	8
		Sensor de umidade não funciona	Perda do monitoramento e controle de	4	1	2	8
		Sensor de radiação não funciona	Perda do monitoramento de radiação	4	1	1	4
		Sensor de Luminosidade não funciona	Perda do monitoramento e controle de	4	1	2	8
		Sensor de oxigênio não funciona	Perda do monitoramento e controle de	4	1	4	16
2	Atuadores do controle ambiental	Atuador do controle de temperatura não funciona	Perda do controle de temperatura	4	2	2	16
		Atuador do controle de pressão não funciona	Perda do controle de pressão	4	2	3	24
		Atuador do controle de umidade não funciona	Perda do controle de umidade	4	2	3	24
		Atuador do controle de Luminosidade não funciona	Perda do controle de luminosidade	4	2	2	16
		Atuador do controle de oxigênio não funciona	Perda do controle de oxigenio	4	2	3	24
3	Sistema de processamento	O software não funciona	Perda do controle do ambiente	4	4	4	64
		O hardware não funciona	Perda do controle do ambiente	4	2	3	24
4	Estrutura Mecânica do Payload	Hemerticidade não funciona	Perda do controle do ambiente	4	2	2	16
5	Especificação projeto do Controle ambiental	Erro de especificação dos parâmetros ambientais	Perda parcial do controle ambiental	3	1	2	6
		Erro de especificação de componentes	Perda parcial do controle ambiental	3	1	2	6

Após fazer a FMECA e registrar os modos de falhas, seus respectivos casos de falhas e seu nível de criticidade através do RPN, foi realizada a avaliação de segurança e o resultado registrado em uma tabela com recomendações de ações com o objetivo de mitigar, eliminar ou monitorar o potencial modo de falha e seus respectivos casos de falha. A Tabela IV apresenta as ações a serem executadas.

TABELA IV. AVALIAÇÃO DE SEGURANÇA

Id	Modulo de Falha	Descrição do Risco	RPN	Ações	Prioridade
1	Sistema de processamento	O software não funciona	64	Detalhar utilizando FTA e para os eventos básicos fazer nova tabela de ações específicas	1
2		O hardware não funciona	24	Detalhar utilizando FTA e para os eventos básicos fazer nova tabela de ações específicas	2

A FTA (*Fault Tree Analysis*) é uma técnica gráfica cujo objetivo é identificar combinações de falhas nos componentes de um sistema ou equipamento, que podem levar à ocorrência

de pane no item avaliado. Nas análises de riscos, em particular, permite identificar as falhas isoladas ou conjuntas, que podem levar a panes críticas [6].

Diferentemente da FMECA, que é válida para todo o sistema, cada FTA vale apenas para um modo de falha ou caso de falha do sistema.

Para nosso estudo de caso foram extraídos da FMECA os casos de falhas com o maior RPN. No processo de análise por FTA, colocamos cada caso de falha escolhido como evento topo na FTA e assim detalhamos as possíveis combinações até chegar ao nível de eventos básicos (iniciantes) que levam ao evento topo. Nas Fig. 3 e Fig. 4 são apresentadas as árvores de falha para o "hardware não funciona" e "software não funciona" respectivamente.

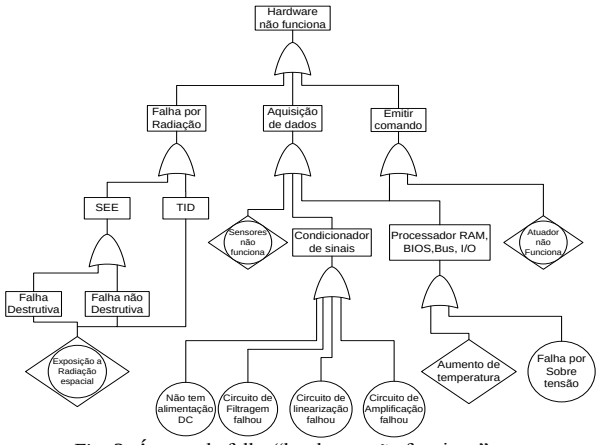

Fig. 3. Árvore de falha "hardware não funciona"

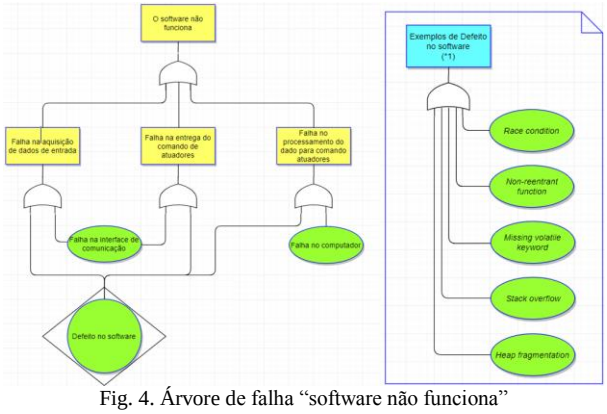

Fig. 4. Árvore de falha "software não funciona"

Após a análise através da FTA, a estratégia adotada é reavaliar a segurança, gerando uma tabela de ações (Tabela V), agora colocando como possíveis riscos os eventos básicos resultantes das FTA's, e propondo as ações de mitigação dos riscos potenciais.

TABELA V. AVALIAÇÃO DE SEGURANÇA ESPECÍFICA

Id	Modulo de Falha	Descrição do Risco	RPN	Ações	Prioridade
1	O software não funciona	Defeito no software	**64**	• Adotar práticas e conceitos de engenharia de sistemas que contribuam com o processo de desenvolvimento de projetos de software • Fazer Verificação e Validação do produto software • Fazer revisão de projeto	**1**
		Falha na interface de comunicação	**64**	• Adotar práticas e conceitos de engenharia de sistemas que contribuam com o processo de desenvolvimento de projetos de software • Fazer Verificação e Validação do produto software • Fazer Verificação e Validação de integração dos equipamentos • Fazer revisão de projeto	**1**
		Falha no computador	**64**	• Fazer Verificação e Validação do produto software • Fazer Verificação e Validação das funções do computador • Implementar redundância do computador • Fazer revisão de projeto	**1**
2	O hardware não funciona	Exposição à Radiação espacial	**24**	• Fazer análise do fluxo de partículas e níveis de energia na órbita da missão. • Fazer análise da tolerância à radiação dos componentes selecionados à missão • Fazer teste de radiação em alguns componentes • Fazer o estudo de blindagem para os componentes • Fazer o estudo de redundância para os componentes e sistemas	**2**
		Não tem alimentação DC		• Fazer testes funcionais • Verificar conexão dos cabos • Verificar painéis solares e bateria • Verificar montagem e integração	**2**
		Circuito de Filtragem falhou		• Fazer testes funcional • Fazer revisão de projeto	**2**
		Circuito de linearização falhou		• Fazer testes funcionais • Fazer revisão de projeto	**2**
		Circuito de Amplificação falhou		• Fazer testes funcionais • Fazer estudo de interferência eletromagnética	**2**
		Aumento de temperatura		• Fazer estudo térmico da missão • Fazer estudo da dissipação de calor • Fazer revisão de projeto	**2**
		Falha por sobre tensão		• Fazer proteção do circuito contra picos de tensão • Fazer revisão de projeto	**2**
		Atuador não funciona		• Fazer testes funcionais • Fazer testes ambientais • Fazer inspeção de montagem e integração • Fazer revisão de projeto	**2**

D. Trade studies

O objetivo dessa análise é estudar algumas alternativas de arquiteturas disponíveis no mercado que possam atender as necessidades do projeto, observando os requisitos até aqui mapeados através de todo o processo ágil utilizado no MBSE [2]. Para esta análise foi escolhido como função chave do sistema: "Estudar a resposta à radiação em uma cultura de bactérias (Extremophile) na região cis-lunar e recobrar seu crescimento simulando condições terrestres".

As soluções candidatas foram selecionadas nos primeiros *Loop's* de desenvolvimento de projeto de acordo com a metodologia Ágil. Nesta análise foi considerada a possibilidade da utilização de um CubeSat 3U com a alocação dos experimentos (*Payload*) no volume de 1,5U's, e a alocação da plataforma no volume restante de 1,5U's. Outras avaliações sistemáticas deverão ser consideradas posteriormente de acordo com maturidade do projeto, de acordo com surgimento de novos requisitos dos *stakeholders* e modificação dos requisitos já existentes.

Para avaliar o desempenho das soluções candidatas, foram definidos os critérios para o estudo e registrados na Tabela VI, juntamente com os resultados obtidos.

TABELA VI. CRITÉRIOS PARA AVALIAÇÃO DE DESEMPENHO E SEUS RESULTADOS

	Estudo de critérios			
SOLUÇÃO	Custo	Volume	Potência	Dependabilidade
	Custo Recorrente, Desenvolvimento, Lançamento e Operação. 1.000.000/Kg da SSTL	Capacidade de Volume para embarcar Experimentos, controle de atitude e controle de ambiente. O experimento precisa de no mínimo 1,5U.	Capacidade de geração de energia. Mais energia possibilita melhor controle de atitude e margem de operação.	Equipamento com herança em operação em condições ambientais agressivas com radiação ionizante. Mais equipamentos aumenta a dependabilidade. Considerando a Herança de projetos da NASA
	Kg	U para Payload	Watts	Quantidade
6U Deployable	10	2	9	6
6U	9	2	5	5
3U	4	1,5	2	2

Para poder medir a efetividade das soluções candidatas, e chegar numa pontuação final e, definir qual solução é a mais adequada, foram definidos pesos aos critérios para realizar a análise final e chegar ao resultado. Na Tabela VII é apresentadata a medida de efetividade para as soluções.

TABELA VII. MEDIDA DE EFETIVIDADE

SOLUÇÃO	**CRITÉRIOS E PESOS**			
	Custo	**Volume**	**Potência**	**Dependabilidade**
	0,50	**0,20**	**0,10**	**0,20**
6U Deployable	0,00	10,00	10,00	0,00
6U	1,67	10,00	4,29	2,50
3U	10,00	0,00	0,00	10,00

A Tabela VIII apresenta a pontuação final para a solução mais adequada de acordo com os pesos estabelecidos para cada critério.

TABELA VIII. PONTUAÇÃO FINAL

SOLUÇÃO	PONTUAÇÃO
6U Deployable	3
6U	3,762
3U	7

A solução vencedora atendendo aos critérios estabelecidos foi a arquitetura 3U's, conforme destacado em cinza.

E. Funções de subsistema

Existem duas abordagens viáveis para o desdobramento de sistema em subsistemas. A primeira abordagem é a "*Bottom up*", onde o sistema é composto a partir da definição dos componentes. E a segunda, a qual foi utilizada para realizar a modelagem deste trabalho é a "*Top down*". Nesta abordagem os *Use Cases* do sistema são decompostos com a relação "*include*", juntamente com as funções relevantes do sistema, de modo que cada uma delas são atribuídas a um subsistema como na Fig. 5.

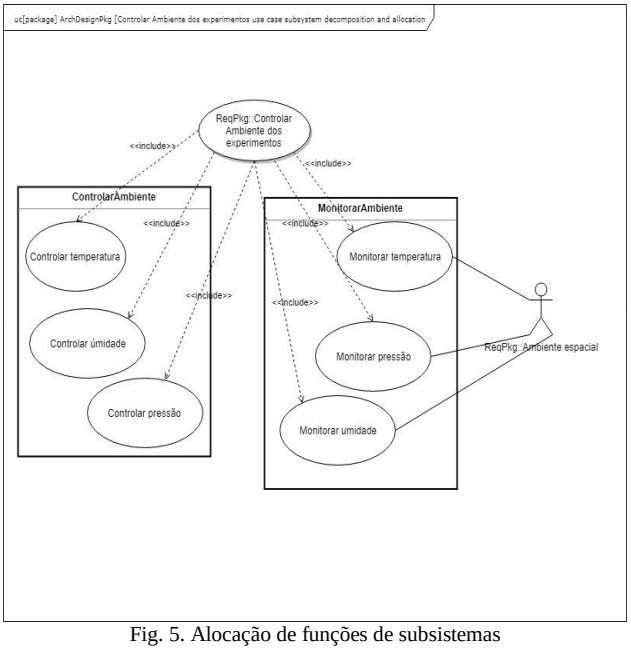

Fig. 5. Alocação de funções de subsistemas

Após ter-se definido quais são os subsistemas que estão incluidos no sistema, foi realizado um desdobramento do subsistema "Monitorar Ambiente", e feita sua representação através de *Use Cases* (Fig. 6), a fim de entender as relações entre os atores e as funções desse subsistema. O objetivo era deixar claro essas interações para a criação do diagrama de sequência de um cenário "*White Box*".

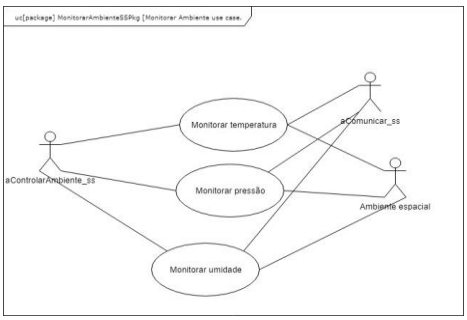

Fig. 6. Desdobramento de requisitos de subsistemas

Os cenários representados por "*Black Box*" estão entre os principais produtos de trabalho para análise de *Use Cases* em nível de sistema. O conceito de "*Black Box*" não significa que o sistema não seja acessível; ele quer apenas dizer que não é considerada a estrutura interna ou o funcionamento interno do sistema. Há a possibilidade de caracterizar a natureza da entrada, o controle de saída e as transformações de dados realizadas pelo sistema, mas não se pode dizer como essas transformações foram realizadas ou quais partes internas desempenharam papéis nessas transformações [2].

No entanto, quando saimos do cenário "*Black Box*" e entramos em um cenário "*White Box*", podemos ver essas partes internas ao nível de subsistema, e mapear as interações entre os subsistemas que executam essas interações. O comportamento dentro dos subsistemas é agora o nível da "*Black Box*", acarretando que as interações entre os subsistemas estão mais claras.

Cada vez que um fluxo de informação ou um evento no diagrama de sequência é gerado, estão sendo criadas e alocadas as funções para esses subsistemas, refinando suas interfaces e alocando indiretamente requisitos. Na Fig. 7 tem-se um exemplo de diagrama de sequência, que representa a função do subsistema "Monitorar Ambiente".

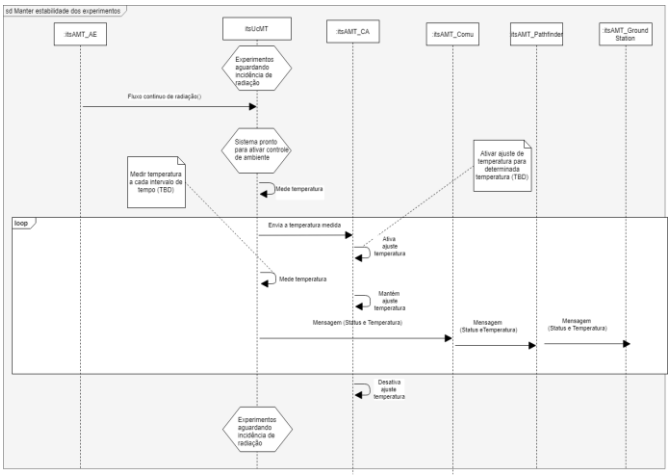

Fig. 7. Diagrama de sequência "*White Box*"

F. Diagrama de requisitos

Os subsistemas são geralmente compostos de elementos de várias disciplinas de engenharia, incluindo software, hardware, mecânica, térmica entre outras. Após se realizar toda a modelagem, fazendo a identificação das funções a nível de sistema e subsistemas, foi criado um diagrama de requisitos representado na Fig. 8. Esse diagrama ilustra o relacionamento dos requisitos em nível de sistema com os requisitos em nível de subsistema. Com esses requisitos bem definidos é possível alocar os mesmos para as diversas áreas de engenharia para que cada especialidade possa continuar a etapa de desenvolvimento do projeto. Através dessa modelagem é possível perceber se não há porventura, alguns requisitos faltando, em excesso, ou duplicados. Ela possibilita também a rastreabilidade, mantendo esses requisitos organizados, e melhorando a compreensão do sistema.

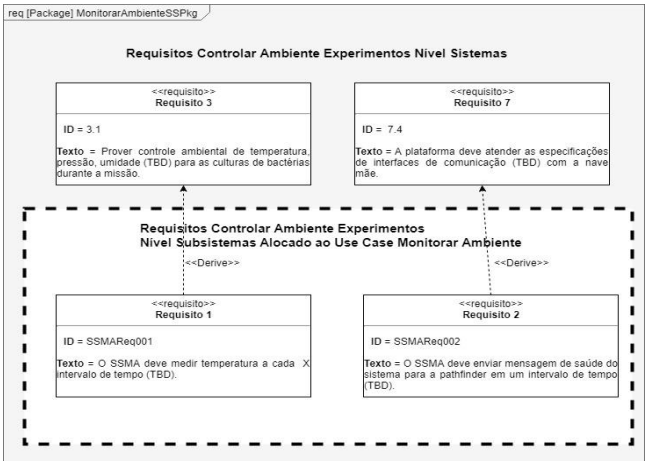

Fig. 8. Diagrama de requisitos

V. CONCLUSÃO

Os resultados demonstram que a aplicação da abordagem de MBSE ágil agrega mais desempenho e dinâmica aos times de desenvolvimento de sistemas espaciais, através dos *Loop's* de projeto, possibilita sistematizar o processo através da modelagem lógica das análises que definem o sistema, e auxilia na rastreabilidade de requisitos de forma a manter o alinhamento com as necessidades dos *stakeholders*.

Dentro dos princípios da Engenharia de Sistemas Ágil, o uso do SysML como linguagem descritiva de sistemas para geração dos diagramas auxiliou na convergência de entendimento entre todos os *stakeholders*, diminuindo o tempo de análise comumente orientada a documentos, mitigando dúvidas e aumentando a probabilidade de compreensão sobre as funções e requisitos do sistema.

O trabalho não se esgota neste artigo, mas sim evolui gradativamente conforme os *Loop's* de projetos forem acontecendo até convergir para o estudo final que atenda às expectativas dos *stakeholders*.

REFERÊNCIAS

[1] D. Kaslow, B. Ayres, M. Chonoles, S. Gasster, L. Hart, C. Massa, R. Yntema, and B. Shiotani. "Developing a CubeSat Model-Based Systems Engineering (MBSE) Reference Model – Interim Status #2." Proceedings of IEEE Aerospace Conference. Big Sky, MT. 2014.

[2] Douglass, Bruce Powel, Agile Systems Engineering-Morgan Kaufmann, 2016.

[3] S. Friedenthal, A. Moore, and R. Steiner, A Practical Guide to SysML: The Systems Modeling Language, 3rd ed. Morgan Kaufmann, 2015.

[4] FONSECA, L.; NOGUEIRA, S. Manifesto da missão lunar brasileira. São Paulo, Brasil, 2016.

[5] Larson, W; Kirkpatrick, D; Sellers, J.; Thomas, D.; Verma, D. Applied space systems engineering. The McGraw-Hill Companies. United States, 2009.

[6] I.A. Azevedo, "EA-160 Confiabilidade de components e sistemas, tech. report, Divisão de Engenharia Eletrônica, ITA,2015.

[7] Galante, D.; Rodrigues, F. Astrobiology experiment: probing the resilience of molecular biosignatures to the space environment. Campinas, Brasil.