



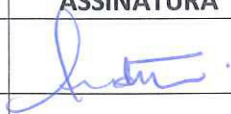
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO
INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS

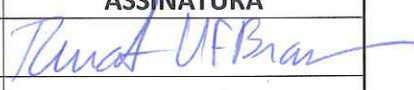
PROJETO:

EQUARS

Plano preliminar de segurança (safety) para a Missão EQUARS

DOCUMENTO: EQUARS-3300-PLN-001		ESTADO: APROVADO
DESCRIÇÃO: Descreve o plano a segurança (safety) para as atividades do satélite EQUARS.		
DATA: 05-09-2019	EDT: SEGURANÇA E MISSÃO (SAFETY)	PÁGINAS: 26

AUTORES			
NOME	DIVISÃO	DATA	ASSINATURA
Andreia Fatima Sorice Genaro	CGETE/SESEQ	24/9/19	

REVISORES			
NOME	DIVISÃO	DATA	ASSINATURA
P! Cristiane Mariano Zavati Silva	CGCEA	19/9/19	

APROVADO POR			
NOME	DIVISÃO	DATA	ASSINATURA
Leandro Toss Hoffmann	CGETE/DSS	19/09/2019	

REVISÕES				
REV.	DATA	N. PÁG. / MUDANÇAS	AUTOR	APROVADO POR

SUMÁRIO

1	INTRODUÇÃO.....	4
2	ESCOPO.....	4
3	DOCUMENTOS APLICÁVEIS E DE REFERÊNCIA	4
3.1	DOCUMENTOS APLICÁVEIS (DA)	4
3.2	DOCUMENTOS DE REFERÊNCIA (DR)	4
4	POLÍTICA DE SAFETY DA MISSÃO EQUARS	4
5	PLANO DE SAFETY DA MISSÃO EQUARS	5
5.1	ATIVIDADES DE SAFETY NO CICLO DE VIDA DO PROJETO	6
6	ENGENHARIA DE SEGURANÇA	8
7	ANÁLISES DE SEGURANÇA.....	9
7.1	ANÁLISE DE PERIGOS/CONDIÇÕES PERIGOSAS (HAZARD).....	9
7.1.1	Estrutura da análise de perigo para Missão EQUARS	9
7.1.2	Tarefa 1 – Definir o escopo, objetivos e o planejamento da análise de perigos	12
7.1.3	Tarefa 2 – Definir a baseline dos sistemas a serem analisados	15
7.1.4	Tarefa 3 – Identificar as manifestações de perigo	15
7.1.5	Tarefa 4 – Identificar e classificar os cenários de perigo.....	16
7.1.6	Tarefa 5 – Decidir se o perigo pode ser aceito	21
7.1.7	Tarefa 6 – Reduzir os Perigos	22
7.1.8	Tarefa 7 – Recomendar aceitação.....	23
7.1.9	Tarefa 8 – Rastrear e recomendar os perigos	23
7.1.10	Tarefa 9 – Aceitar os perigos	23
7.2	ANÁLISE PRELIMINAR DE RISCOS - APR	25
7.3	RELATÓRIO DOS RISCOS DAS ALTERNATIVAS SELECIONADAS	25
8	ATIVIDADES DE SAFETY PARA CONTRATAÇÃO DOS SUBSISTEMAS DO SATÉLITE EQUARS.....	25
9	ATIVIDADES DE SAFETY PARA ATIVIDADES DE AIT SATÉLITE EQUARS	25
10	PACOTE DE DADOS DE SAFETY	25
11	REVISÕES DE PROJETO	25

1 INTRODUÇÃO

O objetivo do documento é descrever o plano de segurança da Missão EQUARSEQUARS durante todo o ciclo de vida do projeto trazendo, de forma sucinta, as principais atividades que são necessárias para se garantir a implementação da política e dos requisitos de *safety* definidos para esta missão.

2 ESCOPO

Este plano de segurança define as atividades do programa de segurança da Missão EQUARSEQUARS a serem implementadas pela equipe responsável pela garantia de *safety* com o apoio da equipe técnica multidisciplinar do projeto para cada um dos segmentos (espacial, solo, lançador e aplicações) da Missão EQUARS. Este plano atende aos requisitos de *safety* estabelecidos no documento DA2.

3 DOCUMENTOS APLICÁVEIS E DE REFERÊNCIA

3.1 DOCUMENTOS APLICÁVEIS (DA)

- DA1 EQUARS-1140-PLN-001 Plano de gerenciamento de riscos
- DA2 EQUARS-3300-TS-001 EQUARS Preliminary Safety Requirements
- DA3 Plano de Safety para as atividades de contratação dos subsistemas do EQUARS (TBD-1)
- DA4 Plano de Safety para as atividades de AIT do EQUARS (TBD-2)

3.2 DOCUMENTOS DE REFERÊNCIA (DR)

- DR1 ECSS-Q-ST-40-02C Hazard analysis
- DR2 ECSS-Q-ST-20-07C Quality and safety assurance for space test centres
- DR3 ECSS-M-ST-80C Risk management
- DR4 – ECSS-Q-ST-40C Safety
- DR5 – EQUARS-3000-TS-001 – EQUARS Mission Assurance Preliminary Requirements

4 POLÍTICA DE SAFETY DA MISSÃO EQUARS

A Política de Safety da Missão EQUARS visa assegurar que os segmentos da missão não causem qualquer perigo ou dano, na seguinte ordem de prioridade:

- Vida humana;
- Meio ambiente;
- Propriedade pública ou privada (incluindo base de lançamento);
- Satélite e lançador;
- Equipamentos de suporte de solo e instalações

A Política de Safety da Missão EQUARS também visa à determinação e avaliação dos riscos associados às atividades do projeto; minimizar ou eliminar os riscos de segurança do projeto e assegurar a verificação das medidas de controle de segurança.

5 PLANO DE SAFETY DA MISSÃO EQUARS

O esforço na implementação do Plano de Safety para a Missão EQUARS exige o envolvimento de um grupo de pessoas de diversas áreas de conhecimento. Isso permite que os diferentes aspectos relacionados à segurança do projeto sejam identificados e avaliados.

A Figura 1 apresenta a organização da Missão EQUARS dentro da estrutura organizacional do INPE, onde se pode verificar que o SESEQ é um serviço da Coordenação Geral de Engenharia e Tecnologia Espaciais (CGETE). Equipe de Garantia de Missão e Safety para a Missão EQUARS destacando onde a equipe de Safety está inserida. A Figura 2, em complementação a Figura 1, apresenta todos os os grupos do SESEQ, onde pode-se observar que os grupos do SESEQ trabalham em uma estrutura matricial, estando todos no mesmo nível hierárquico. Na Figura 2 é possível verificar a posição do Grupo de Safety.

Figura 1: Organização da Garantia da Missão dentro da estrutura organizacional do INPE

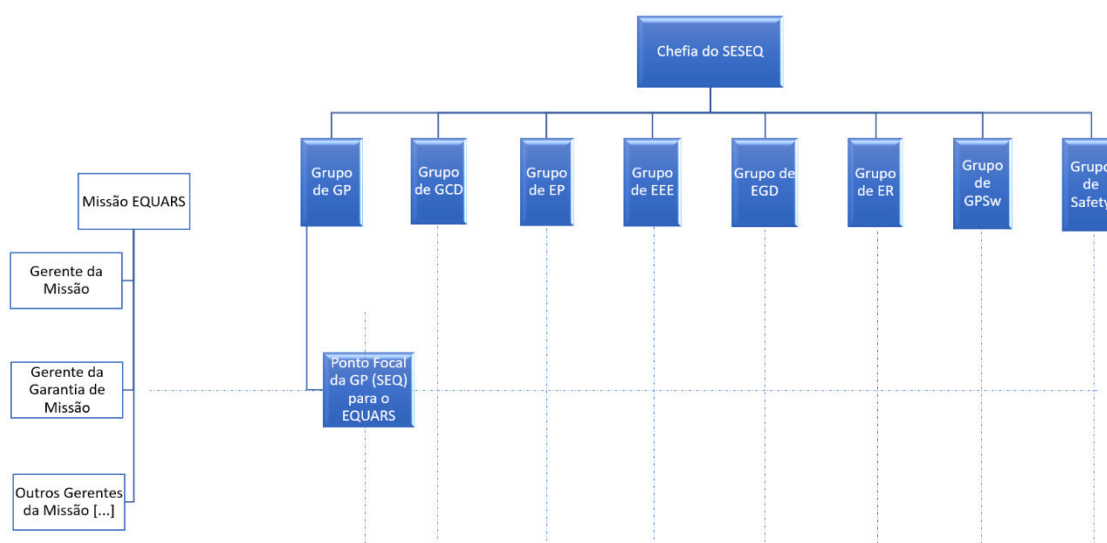


Figura 2: Hierarquia do SESEQ



Na Tabela 1 estão listados o papel e responsabilidades dos engenheiros de safety que irão atuar no projeto. Os profissionais envolvidos serão responsáveis por coletar todas as informações com apoio da equipe multidisciplinar do projeto com foco em identificar todos os perigos e riscos de safety para cada um dos segmentos da Missão EQUARS.

Cabe ressaltar que, o engenheiro de safety deve ter formação em engenharia de segurança para poder assinar os relatórios, conforme rege a legislação brasileira.

Tabela 1: Papel e responsabilidade do Engenheiro de Safety da Missão EQUARS

Papel	Responsabilidades
Engenheiro de Safety	Garantir que todas as condições perigosas (<i>hazards</i>) e riscos, relativos à Missão EQUARS foram devidamente identificados, avaliados, minimizados, controlados e aceitos durante as fases de projeto, desenvolvimento, produção e operações; Garantir a implementação da política de segurança da Missão EQUARS; Avaliar toda a documentação associada a safety dos subsistemas contratados e dar parecer técnico; Elaborar os relatórios de acompanhamento de safety os equipamentos e subsistemas; Participar de todas as revisões de projeto apresentando o status de toda documentação de safety associada à cada fase.

5.1 ATIVIDADES DE SAFETY NO CICLO DE VIDA DO PROJETO

Nesta sessão estão listadas as atividades de *safety* definidas para a Missão EQUARS e que foram adaptadas de DR4DR4DR4. A Tabela 2 consolida, para cada fase do ciclo de vida da Missão EQUARS, as atividades que precisam ser realizadas pela equipe de *safety* e quais os documentos serão gerados para evidenciar o cumprimento das atividades previstas.

Tabela 2: Atividades de safety durante o ciclo de vida da Missão EQUARS - Continua

Fase do projeto	Descrição da atividade	Evidência da implementação	Referência	Segmento(s) afetado(s)
Fase 0 Análise da Missão	1. Analisar os requisitos de segurança e lições aprendidas de missões anteriores ou de missões semelhantes; 2. Realizar análises preliminares de perigos de segurança do sistema proposto para apoiar nas análises de <i>trade-off</i> ; 3. Realizar análise dos riscos de segurança comparando com as alternativas; 4. Apoiar a avaliação definição missão.	1. Documento de requisitos preliminar em alto nível.	DA5	Segmento solo Segmento espacial
		2. APP – Análise Preliminar de Perigos para as opções de <i>trade-off</i> .	DR1	
		3. Relatório de análise de riscos de segurança para as alternativas.	TBD-3	
		4. Pacote com informações de segurança para a MDR	Não emitido	
Fase A Análise de Viabilidade	1. Realizar análises preliminares de perigos de segurança do sistema proposto atualizado para apoiar nas análises de <i>trade-off</i> ; 2. Identificar os requisitos de segurança específicos em nível de missão. 3. Identificar se existem funções críticas de segurança em nível de missão e elaborar as análises de perigos. 4. Elaborar o plano de segurança da missão. 5. Apoiar a PRR	1. Nova versão da APP – Análise Preliminar de Perigos para as opções de <i>trade-off</i> .	TBD-4	Segmento solo Segmento espacial
		2. Documento de Requisitos de safety de Missão do EQUARS.	Mission Assurance Preliminar requirements	
		3. Análise de perigo das funções críticas.	TBD-5	
		4. Plano de Segurança (<i>safety</i>) da Missão EQUARS.	Este documento	
		5. Pacote de dados de segurança para a PRR	Conjunto de documentos de safety PRR	
Fase B Definição preliminar do projeto	1. Realizar a análise de segurança para cada segmento da Missão EQUARS 2. Analisar os riscos de segurança das opções escolhidas que compõem os segmentos da Missão EQUARS	1. Análise de Perigo conforme DR1	7.3	Segmento solo Segmento espacial Segmento lançador Segmento aplicações
		2. Análise de Risco Preliminar da opção escolhida.	7.1	

Tabela 2: Conclusão

Fase do projeto	Descrição da atividade	Evidência da implementação	Referência	Segmento(s) afetado(s)
Fase C/D Definição detalhada do projeto, produção e ensaios de qualificação.	1. Análises de segurança em nível de subsistema (contratada) e de sistema (INPE) conforme sessão 7 do DR4DR4DR4; 2. Análise de segurança das operações com foco na identificação de planos de emergência e contingência, requisitos de treinamento e operações e desenvolvimento de procedimentos.	1a. Análise de Perigo conforme DR1.	7.3	Segmento solo Segmento espacial Segmento lançador Segmento aplicações
		1b. Relatórios de análise de segurança conforme Anexo D do documento DR4DR4DR4.	TBD-6	
		2a. Análise de Perigo conforme DR1.	7.3	
		2b. Relatórios de análise de segurança conforme Anexo D do documento DR4DR4DR4.	TBD-6	
Fase E Operação	1. Análises de segurança focada em possíveis mudanças operacionais que possam impactar a segurança.	1. Relatórios das análises de segurança das operações para cada segmento da Missão EQUARS.	TBD-7	Segmento solo Segmento espacial Segmento aplicações
Fase F Descarte	1. Análises de segurança focada em todas as operações de descarte e perigos associados.	1. Relatórios das análises de segurança para os segmentos da Missão EQUARS envolvidos nas operações de descarte.	TBD-8	Segmento solo Segmento espacial Segmento aplicações

NOTA: A geração de toda a documentação listada na terceira coluna da Tabela 2 é de responsabilidade do Engenheiro de Segurança responsável do projeto. Para análises em nível de missão o Engenheiro de Segurança designado para realizar as atividades previstas é um servidor do INPE com formação na área de segurança conforme requisitos da legislação brasileira (Lei nº 7.410, de 27 de novembro de 1985 – Planalto) e do CONFEA (Resolução nº 325 – Confea). No entanto, a responsabilidade pela geração de documentação de segurança em nível de subsistema é da empresa contratada pelo projeto, ou mesmo pelo próprio INPE, e os requisitos do Engenheiro de segurança responsável também precisam seguir às exigências supracitadas.

6 ENGENHARIA DE SEGURANÇA

As atividades de engenharia de segurança da missão EQUARS visa o atendimento dos requisitos de segurança previstos no documento DA2.

Conforme apresentado na Tabela 2, para cada fase do projeto da Missão EQUARS, um conjunto de documentos de segurança está previsto, tais como APR – Análise Preliminar de Riscos, Análises de

EQUARS	Plano preliminar de segurança (safety) para a Missão EQUARS	
--------	---	--

Perigos e *Safety Data Package*, tanto em nível de missão como em nível de sistema e subsistemas do segmento espacial, por exemplo.

As informações necessárias para realizar o levantamento de perigos e riscos de segurança geralmente incluem:

- a) Fluxo de atividades e/ou processos;
- b) Lay-outs, desenhos de máquinas;
- c) Lista de matérias-primas, subprodutos, produtos, efluentes, emissões, resíduos.
- d) Tarefas executadas com duração e frequência;
- e) Pessoal envolvido (normal, ocasional, manutenção);
- f) Treinamentos recebidos;
- g) Utilidades empregadas (ex: GN2, ar comprimido, etc.)
- h) Forma física das substâncias utilizadas;
- i) Requisitos de regulamentação e normas internas;
- j) Controle de usos;
- k) Planos de emergência existentes;
- l) Monitoramento;
- m) Inspeções de segurança e etc.

7 ANÁLISES DE SEGURANÇA

Para a Missão EQUARS está planejada a elaboração de diversas análises de segurança com o objetivo de atender as necessidades colocadas na Tabela 2 para cada um dos segmentos que compõem a Missão EQUARS nas diversas fases do projeto.

7.1 ANÁLISE DE PERIGOS/CONDIÇÕES PERIGOSAS (*HAZARD*)

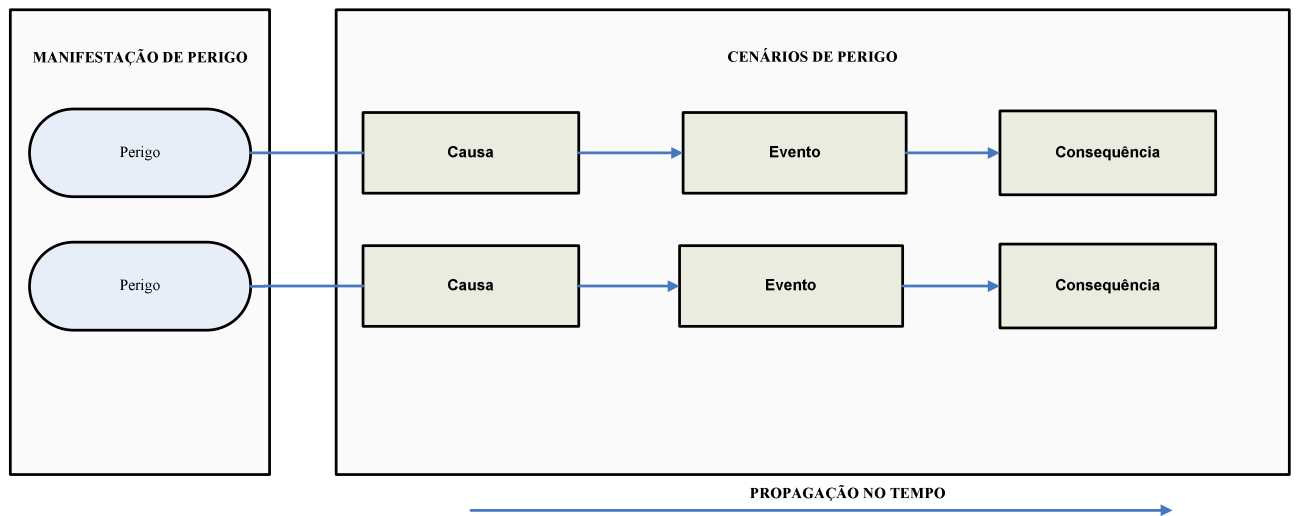
A análise de perigos/condições perigosas (*hazard*) é a principal análise de segurança determinística que auxilia os engenheiros e gerentes na inclusão de aspectos de segurança nas práticas de engenharia e no processo de tomada de decisão ao longo do ciclo de vida em projeto, construção, teste, operação, manutenção e descarte, juntamente com suas interfaces. A análise de perigos fornece informações essenciais para a avaliação do risco de segurança de um sistema.

7.1.1 Estrutura da análise de perigo para Missão EQUARS

Para a Missão EQUARS o modelo que será adotado para análise dos perigos dos segmentos obedece aos conceitos definidos no documento DR1, conforme esquematizado nas Figuras 3 a 6.

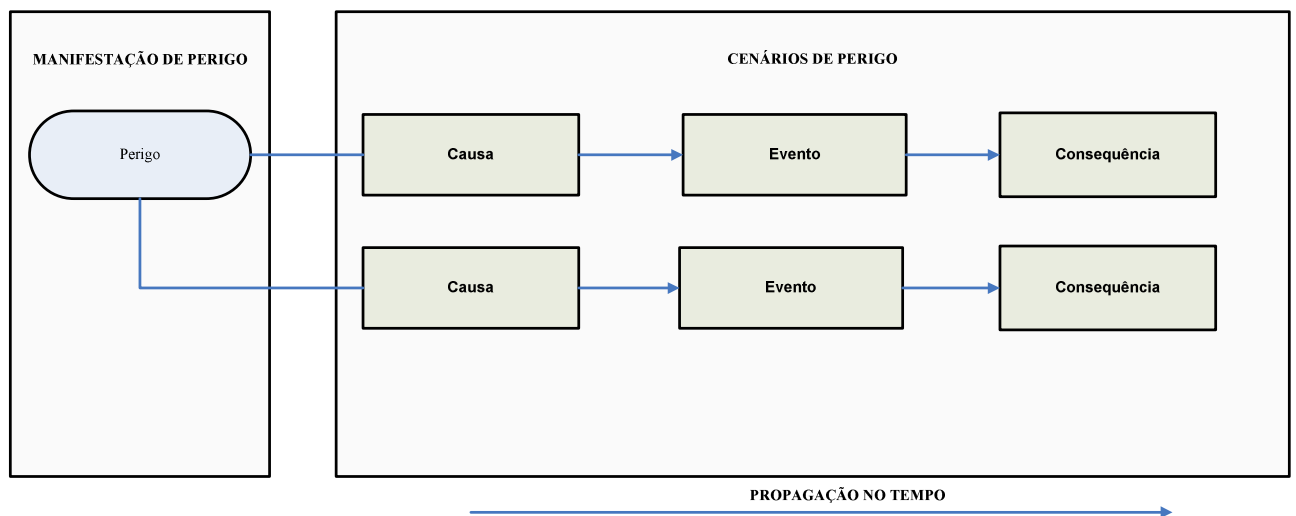
Os cenários de perigo refletem o comportamento do sistema para os perigos iniciados em termos de propagação das causas, eventos e consequências na segurança, conforme ilustrado na Figura 3.

A ocorrência de eventos está junto com os sintomas observáveis no sistema. As consequências de segurança são caracterizadas por sua severidade.

Figura 3: Perigos e Cenários de Perigos

Fonte: Adaptado de DR1

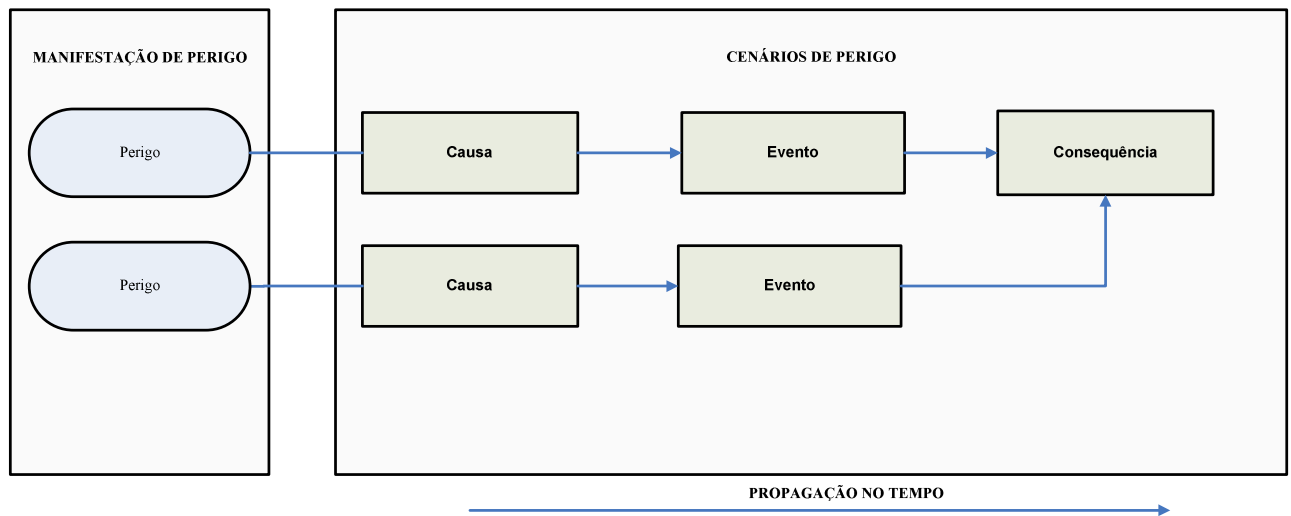
O conjunto de cenários de perigo oriundos da mesma manifestação de perigo é agrupado em uma árvore de perigo, conforme ilustrado na Figura 4.

Figura 4: Árvore de Perigos

Fonte: Adaptado de DR1

O conjunto de cenários de perigos que levam à mesma consequência de segurança é agrupado em uma árvore de consequências, conforme ilustrado na Figura 5.

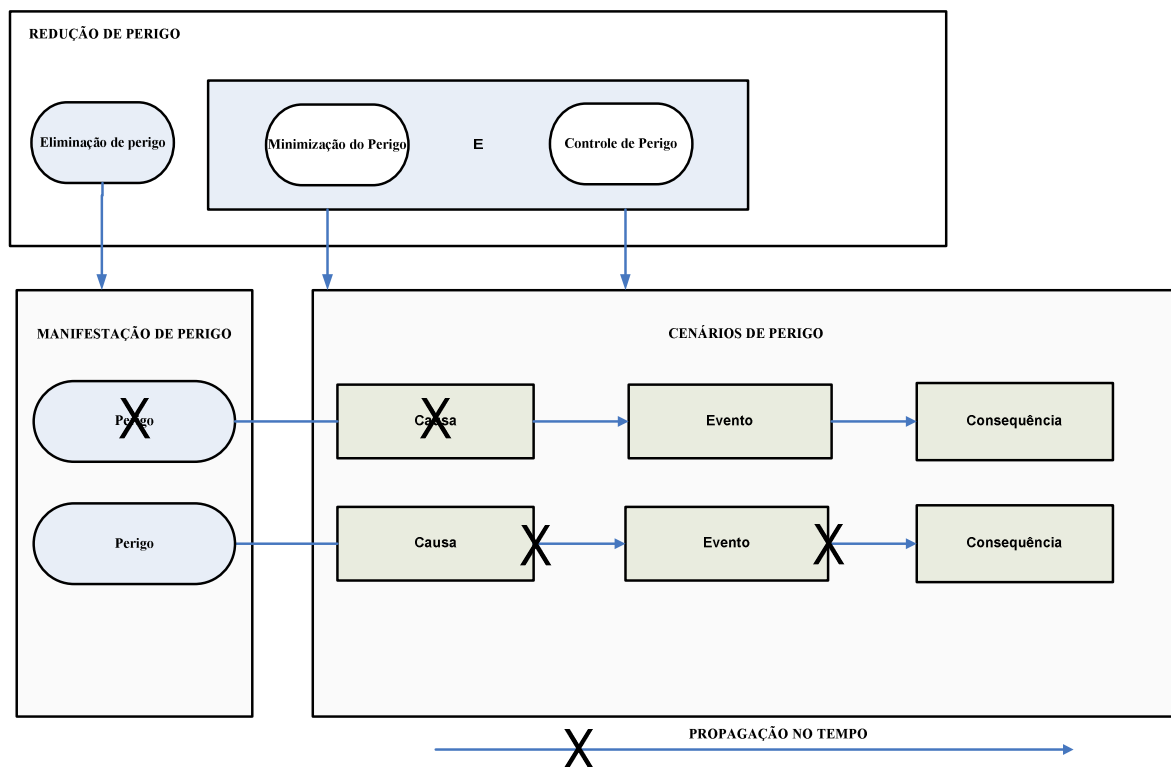
Figura 5: Árvore de Consequência de Perigo



Fonte: Adaptado de DR1

Os perigos são reduzidos eliminando-os ou, se isso não for possível, minimizando-os e controlando-os, conforme apresentado na Figura 6.

Figura 6: Redução de Perigos

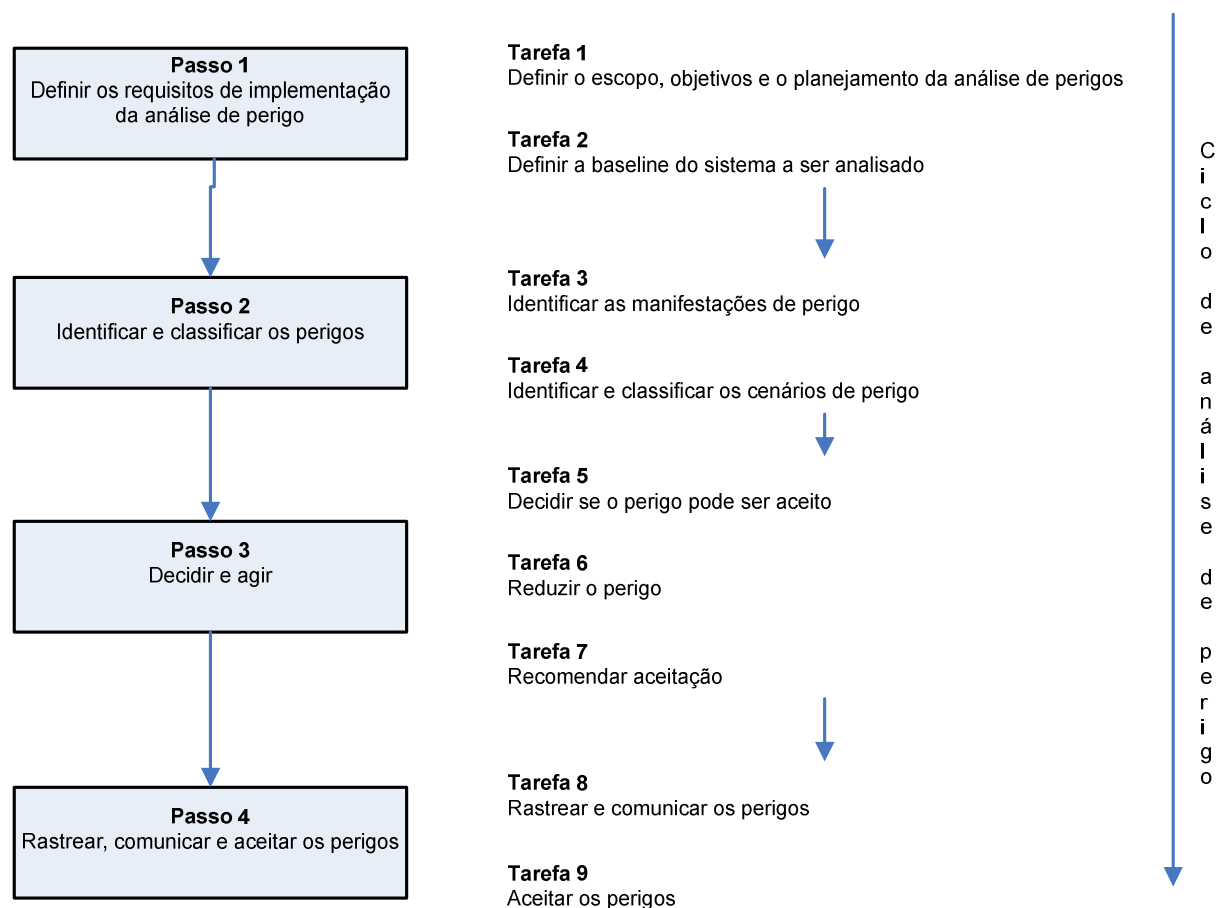


Remover ou alterar os perigos, eliminação de evento ou interrupção do evento

Fonte: Adaptado de DR1

Para realizar as análises de perigo da Missão EQUARS serão realizados quatro passos principais e nove atividades relacionadas. A Figura 7 apresenta, de forma simplificada, o processo de análise de perigos.

Figura 7: As nove atividades relacionadas com os quatro passos do processo de análise de perigo



Fonte: Adaptado de DR1

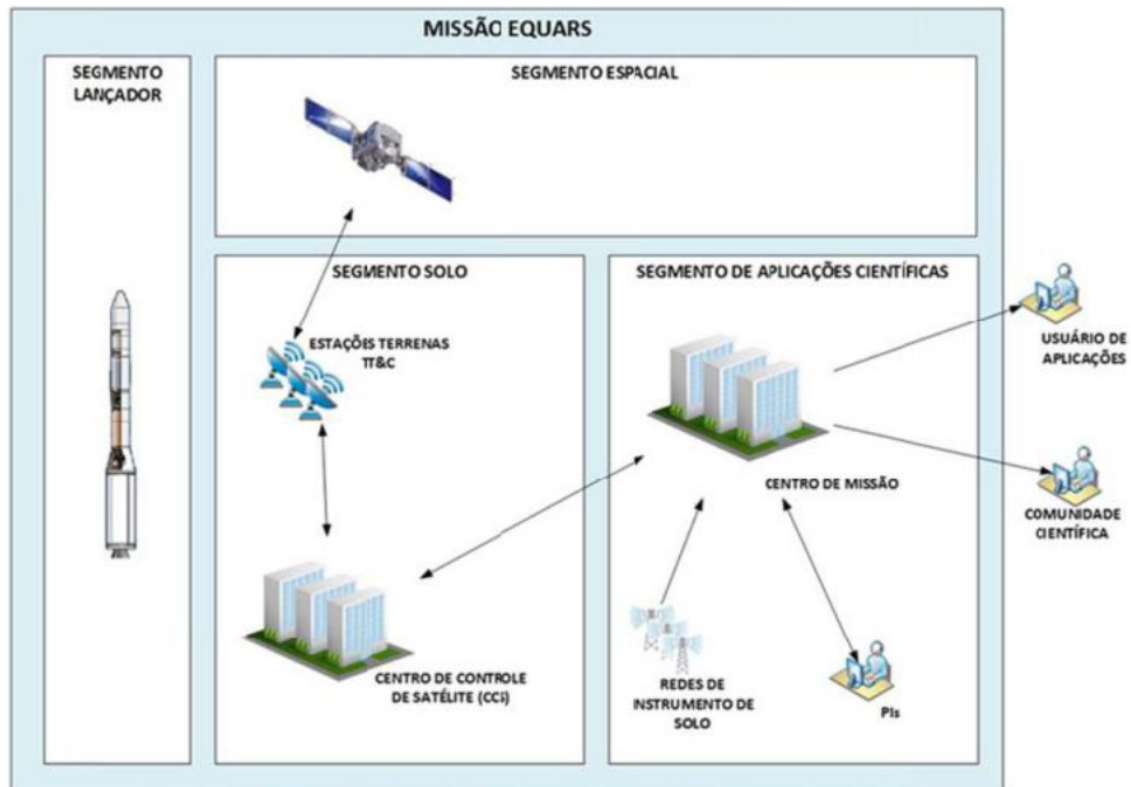
7.1.2 Tarefa 1 – Definir o escopo, objetivos e o planejamento da análise de perigos

Para se avaliar os perigos envolvidos na Missão EQUARS será necessário analisar os perigos para todos os segmentos envolvidos.

- Segmento Espacial: Satélite;
- Segmento Solo: Estações terrenas, Centro de controle;
- Segmento de aplicações científicas: Centro de Missão, PI's, Usuários, Comunidade Científica;
- Segmento lançador: Foguete.

A Figura 8 ilustra a concepção geral da Missão EQUARS mostrando, de forma lúdica, como se relacionam cada um dos segmentos.

Figura 8: Concepção Geral da Missão EQUARS



Fonte: Slide apresentação MDR (Silva, M.B. 2017)

Para as análises de perigo da Missão EQUARS será utilizado o esquema de pontuação de severidade de perigo conforme apresentado na Tabela 3.

Tabela 3: Esquema de pontuação de severidade de perigo

Categoria	Pontuação	Severidade	Severidade da consequência de segurança
I	4	Catastrófico	- Perda de vida, risco de vida, lesão permanente ou doença ocupacional; - Perda de instalações do local de lançamento ou perda do sistema; - Efeitos ambientais prejudiciais graves.
II	3	Crítico	- Lesão temporária, mas que não ameaça a vida; - Danos maiores aos sistemas de voo ou danos maior as instalações de solo; - Danos maiores à propriedades públicas e privadas; - Efeitos ambientais prejudiciais maiores
III	2	Marginal	- Lesão, incapacidade ou doença ocupacional menor; - Dano menor ao sistema e/ou ao meio ambiente.
IV	1	Insignificante	- Menos que uma lesão, incapacidade ou doença ocupacional menor; - Menos que um dano menor ao sistema e/ou ao meio ambiente.

Fonte: Adaptado de DR1

Além da gravidade, a probabilidade do evento perigoso também é considerada, uma vez que tendo em conta o resultado do gerenciamento de perigos. Por exemplo, um perigo identificado como catastrófico pode ter probabilidade extremamente baixa de ocorrer. De acordo DR3, a probabilidade de um evento pode ser classificada em cinco categorias. Um resumo da probabilidade do esquema de pontuação extraído de RD3 é mostrado na Tabela 4.

Tabela 4: Esquema de pontuação de probabilidade

Categoria	Pontuação	Probabilidade	Probabilidade de ocorrência
A	5	Máxima	Certo de ocorrer, vai ocorrer uma ou mais vezes por projeto
B	4	Alta	Ocorrerá com frequência , cerca de 1 em cada 10 projetos
C	3	Média	Ocorrerá às vezes , cerca de 1 em 100 projetos
D	2	Baixa	Raramente ocorrem, cerca de 1 em 1000 projetos
E	1	Mínimo	Quase nunca irá ocorrer, 1 em 10000 ou mais

Fonte: Adaptado de RD3

Ao se combinar a gravidade e a probabilidade (pontuação de gravidade x pontuação de probabilidade), o índice de risco de um evento perigoso pode ser determinado, conforme ilustra a Matriz Severidade e Probabilidade, mostrado na Tabela 5.

Tabela 5: Tabela de índice de risco

		Índice de risco			
Probabilidade	A (5)	5	10	15	20
	B (4)	4	8	12	16
	C (3)	3	6	9	12
	D (2)	2	4	6	8
	E (1)	1	2	3	4
		IV (1)	III (2)	II (3)	I (4)
Severidade					

Fonte: Adaptado de RD3

A Tabela 5 é destacada em verde, amarelo e vermelho para representar a gravidade do risco. Riscos em destacados em verde são, em geral, considerados aceitáveis, os riscos destacados em amarelo exigem atenção por meio de treinamento, procedimentos de monitoramento ou melhoria de projeto. No entanto, os riscos destacados em vermelho são inaceitáveis. A Tabela 6 apresenta propostas de ações para cada classificação de risco encontrada.

Tabela 6: Tabela de gerenciamento de risco

Índice de risco	Magnitude do risco	Proposta de ações
AI, AIII, BI	Risco muito alto	Risco inaceitável: implementar os novos processos para a equipe. Buscar atenção no nível adequado de gerenciamento, conforme definido no plano de gerenciamento de risco.
AIII, BII, CI	Risco alto	Risco inaceitável: Ver o item anterior.
AIV, BIII, CII, DI	Risco médio	Risco inaceitável: gerenciar de forma agressiva. Buscar atenção no nível adequado de gerenciamento, conforme definido no plano de gerenciamento de risco.
BIV, CIII, DII, EI	Baixo risco	Risco aceitável: controlar e monitorar. Buscar atenção do responsável pelo gerenciamento do pacote de trabalho.
CIV, DIV, DIII, EIV, EIII, EII	Risco muito baixo	Risco aceitável: ver o item anterior.

Fonte : Adaptado de DR3

7.1.3 Tarefa 2 – Definir a *baseline* dos sistemas a serem analisados

A Tarefa 2 se aplica aos segmentos da Missão EQUARS e que foram listados em 6.1.2 e representados na Figura 2.

Para execução deste plano será necessário executar o procedimento listado abaixo:

- Definir e descrever o projeto e/ou a operação sujeitos à análise de perigo;
- Revisar a *baseline* de sistema para cada ciclo de análise de perigo com o nível de detalhe disponível para a fase do projeto em que serão analisados.

7.1.4 Tarefa 3 – Identificar as manifestações de perigo

O escopo deste plano contempla todos os segmentos da Missão EQUARS e que foram listados em 6.1.2 e representados na Figura 2.

Os perigos que se manifestam no sistema ocorrem por meio de eventos iniciais, ou seja, existe um evento que inicia a causa, havendo assim a necessidade de se identificar como os perigos se manifestam para os sistemas que compoem os segmentos da Missão EQUARS.

Os perigos genéricos associados com qualquer um dos segmentos durante sua operação em solo e em órbita serão registrados na **Planilha de Perigos Genéricos durante Operações em Solo e em Órbita**, conforme modelo apresentando na Figura 9.

Figura 9: Modelo de Planilha de Perigos Genéricos durante Operações em Solo e em Órbita

MATRIZ DE PERIGO			
Sistema:		Segmento:	
Perigos Genéricos		Operação em Solo	Operação em Órbita
Elétrico			
Químico			
Mecânico			
Térmico			
X = Aplicável - = Não Aplicável			

Fonte: A autora

EQUARS	Plano preliminar de segurança (safety) para a Missão EQUARS	
--------	---	--

As manifestações de perigos que tem relação com operação no solo ou em órbita serão registradas na ***Lista de Manifestação de Perigo***, conforme modelo apresentando na Figura 10.

Figura 10: Modelo de Lista de Manifestação de Perigo

Fase da Missão	Manifestação de Perigo <i>Evento</i>	Equipamento Subsistema Sistema	Descrição da Manifestação de perigo
Somente em Solo	1		
	2		
	3		
	...		
Somente em órbita	1		
	2		
	3		
	...		
Em solo e em voo	1		
	2		
	3		
	...		

Fonte: A autora

7.1.5 Tarefa 4 – Identificar e classificar os cenários de perigo

As consequências dos perigos variam dependendo da severidade do evento. O mesmo perigo pode ter consequências diferentes, dependendo de vários fatores, como condições ambientais, limites de segurança predefinidos, funções e limitação dos dispositivos de segurança, duração dos eventos e a rapidez com que as causas do evento são corrigidas. Da mesma forma, consequências idênticas podem resultar de diferentes eventos de perigo.

Para a Missão EQUARS, os cenários dos perigos potenciais serão elencados na ***Tabela resumida da análise de perigo***, conforme modelo apresentado na Figura 11.

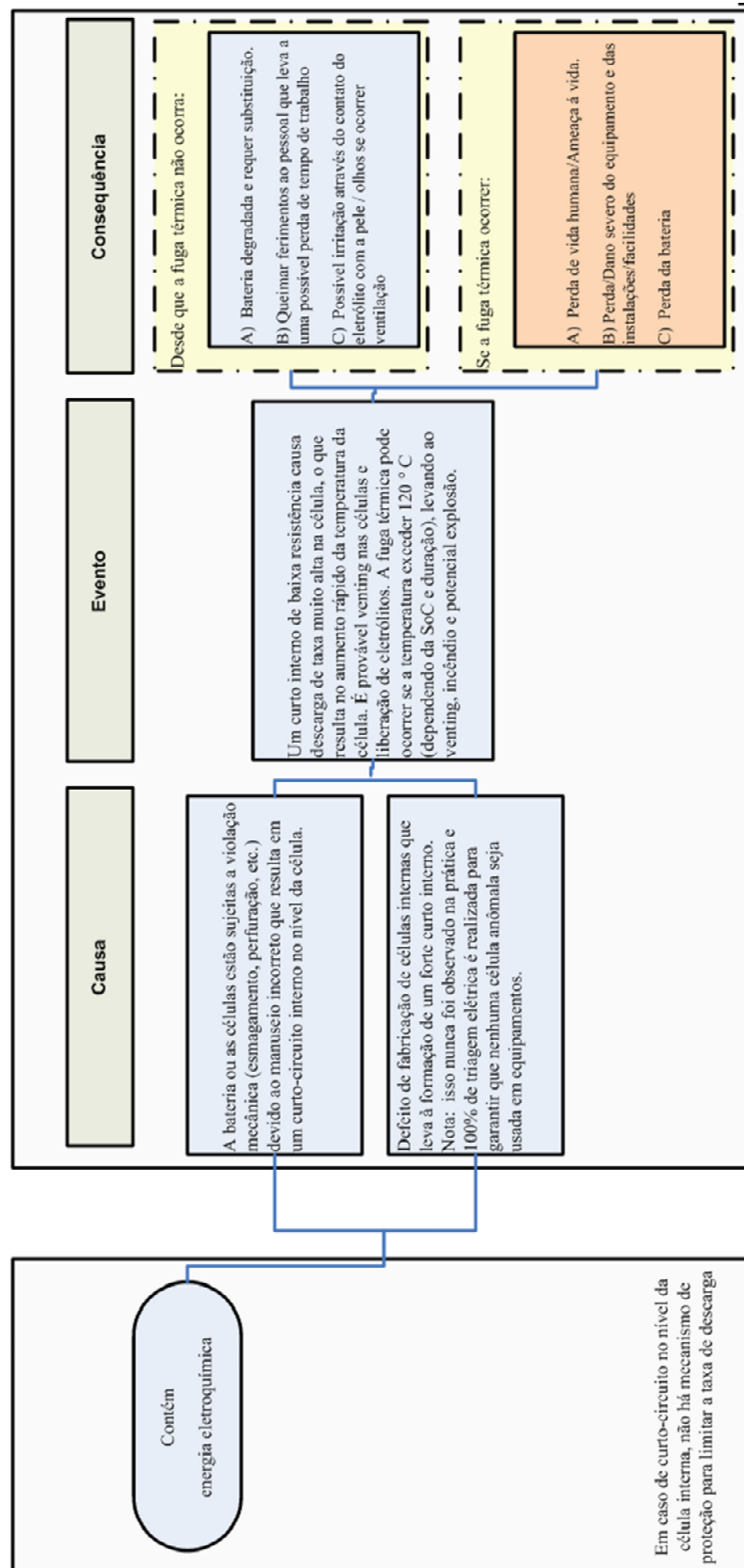
Figura 11: Modelo da Tabela Resumida da Análise de Perigo

Lista de Cenário de Perigo (em órbita)					
Case #	Manifestação do Perigo	Causa-Eventos-Consequência	Severidade da Consequência	Sintomas Observáveis	Propagação e tempo de reação
1					
2					
3					
...					
Lista de Cenário de Perigo (em solo)					
Case #	Manifestação do Perigo	Causa-Eventos-Consequência	Severidade da Consequência	Sintomas Observáveis	Propagação e tempo de reação
1					
2					
3					
...					
Lista de Cenário de Perigo (em solo e em órbita)					
Case #	Manifestação do Perigo	Causa-Eventos-Consequência	Severidade da Consequência	Sintomas Observáveis	Propagação e tempo de reação
1					
2					
3					
...					

Fonte: Adaptado de DR1

Para cada *case* da análise de perigo relacionado com equipamento/sistema/subsistema que compõem os segmentos da Missão EQUARS, uma árvore de Perigo será construída, conforme modelo apresentado na Figura 12.

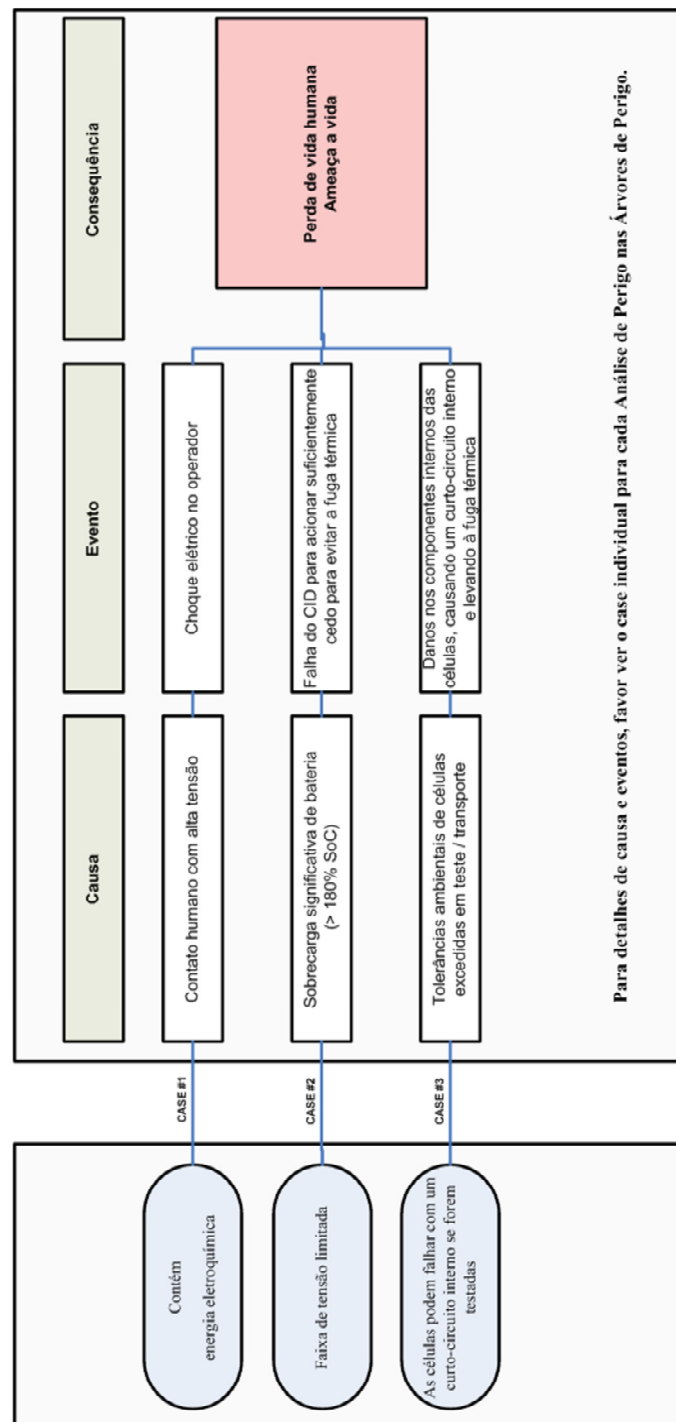
Figura 12: Exemplo de Árvore de Perigo



Fonte: A autora

Com base no estudo das consequências de todas as árvores de falhas construídas para cada *case* identificado torna-se possível categorizar todas as consequências potenciais de perigos. Diferentes *cases* podem ter consequências iguais e para se visualizar este relacionamento entre os *cases* com uma consequência específica, a **Árvore de Consequências** é construída. A Figura 13 apresenta um modelo que será utilizado para analisar as consequências dos perigos para a Missão EQUARS.

Figura 13: Exemplo de Árvore de Consequências



Fonte: A autora

7.1.5.1 Informações sobre propagação de tempo

Como parte da análise de perigo da Missão EQUARS é necessário realizar o levantamento de informações sobre o tempo de propagação (P_{time}) e o tempo de reação (R_{time}) para cada *case*. O P_{time} pode ser entendido como sendo o tempo entre a ocorrência do evento iniciador (causa) e a ocorrência da consequência, enquanto que o R_{time} é o tempo disponível para ações de mitigação após a detecção da ocorrência do evento iniciador (causa). A Figura 14 apresenta o modelo da planilha que a equipe de segurança de sistemas do EQUARS irá utilizar para registrar os dados de P_{time} e R_{time} para cada *case* estudado na análise de perigos.

Figura 14: Modelo da planilha de tempos de reação e propagação dos perigos

Case	Título	Tempo de propagação e reação	Comentários
		P_{time} R_{time}	
		P_{time} R_{time}	
		P_{time} R_{time}	
		P_{time} R_{time}	
		P_{time} R_{time}	
		P_{time} R_{time}	

Fonte: A autora

7.1.5.2 Severidade do Perigo

Todas as consequências que forem identificadas por meio da Árvore de Consequências (Figura 13) precisam ter a sua severidade pontuada, utilizando como referência a Tabela 3. As informações oriundas deste trabalho são organizadas em uma planilha, conforme mostrado na Figura 15.

Figura 15: Severidade das Categorias de Consequências identificadas

Consequência	Pontuação da Severidade

Fonte: A autora

7.1.5.3 Probabilidade do Perigo

Para compilar o “Índice de Risco” de um *case* da análise de perigo, o ideal é que a probabilidade de cada *case* seja considerada com base em experiências/eventos passados para que seja possível permitir a pontuação com certa precisão. Para a Missão EQUARS vai se tentar utilizar dados de lições aprendidas oriundas de outros projetos de satélites do INPE. As pontuações da probabilidade são baseadas naqueles definidos na Tabela 4.

A Figura 16 apresenta o modelo da planilha que será utilizada para apresentar um resumo da pontuação de probabilidade para cada *case* da análise de perigo identificado.

Figura 16: Resumo da pontuação da probabilidade

Case	Título	Probabilidade	Comentários

Fonte: A autora

7.1.6 Tarefa 5 – Decidir se o perigo pode ser aceito

A severidade e a probabilidade de cada *case* da análise de perigo e o índice de risco resultante (produto da classificação de severidade e da classificação da probabilidade) serão avaliados e resumidos em uma planilha, conforme modelo apresentado na Figura 17.

Figura 17: Resumo do Índice de Risco e Pontuação de Aceitação

Case	Título	Severidade (1 a 4)	Probabilidade (1 a 5)	Índice de Risco (1 a 20)	Magnetude do Risco	Aceitação

Fonte: A autora

EQUARS	Plano preliminar de segurança (safety) para a Missão EQUARS	
--------	---	--

7.1.8 Tarefa 7 – Recomendar aceitação

A tabela contendo as informações sobre Redução de Risco e Índice de Risco Revisado (Figura 17) será submetida ao gerente da Missão EQUARS para se analisar. Nesta tabela os perigos não resolvidos também estarão identificados para ações futuras. A equipe de segurança de sistemas espaciais fornece então as justificativas e os dados de apoio para resolução e aceitação dos perigos.

7.1.9 Tarefa 8 – Rastrear e recomendar os perigos

A equipe de segurança de sistema da Missão EQUARS manterá um banco de dados (**TBD**) onde poderá avaliar e revisar periodicamente todos os perigos identificados e atualizar os resultados após cada iteração do processo de análise de perigos.

Também apoiará na identificação das mudanças nos riscos existentes e, quando necessário, iniciará uma nova análise de perigos.

Faz parte do plano de segurança da Missão EQUARS verificar o desempenho e o efeito das atividades de redução de perigos, assim como identificar e comunicar a evolução dos perigos ao longo do ciclo de vida do projeto.

7.1.10 Tarefa 9 – Aceitar os perigos

Todos os perigos identificados serão encaminhados para aceitação formal pela gerência da Missão EQUARS. A apresentação final de cada *case* das análises de perigos será feita por meio da **Folha de Resumo dos Perigos**, conforme modelo apresentado na Figura 19.

Figura 19: Folha de Resumo dos Perigos

DESCRIÇÃO DE PERIGO E MAGNITUDE DO RISCO DE SEGURANÇA								
Case Nº		Título de Cenário de Perigo:						
Manifestação de Perigo				Causa				
Eventos				Consequência de Segurança				
Severidade (S)				Probabilidade (P)				
Insignificante	Marginal	Crítico	Catastrófico	Mínima	Baixa	Média	Alta	Máxima
IV(1)	III(2)	II(3)	I(4)	E(1)	D(2)	C(3)	B(4)	A(5)
Índice de Risco (R = S x P)								
Magnitude do Risco ¹								
DECISÃO E AÇÃO DE RISCO DE PERIGO E SEGURANÇA								
Mais mitigação é requerida? ²								
Abordagem de redução de risco				Eliminação/Minimização/Controle/Não aplicável				
Medidas de redução de perigo (recomendações Gerais)						Status		
Severidade Revisada (S)				Probabilidade Revisada (P)				
Índice de Risco Revisado (R = S x P)								
Magnitude do Risco Revisada ¹								

Legenda: ¹ Baseado na Tabela 5

² Baseado na Tabela 6

Fonte: Adaptado de DR1

7.2 ANÁLISE PRELIMINAR DE RISCOS - APR

A metodologia para realizar uma análise preliminar de riscos para a Missão EQUARS é a mesma que está definida no documento DR4.

A equipe de safety do projeto EQUARS executa a atividade de levantamento dos riscos preliminares de safety e insere as informações nos campos apropriados e disponibilizados pela ferramenta *Simple Risk*, disponível em <https://f100.ete.inpe.br>.

Por meio de reuniões semanais ou quinzenais os riscos identificados são revisitados e o status de implementação de ações pelos responsáveis em gerenciar tais riscos são atualizados.

7.3 RELATÓRIO DOS RISCOS DAS ALTERNATIVAS SELECIONADAS

Assim que as alternativas forem definidas a equipe de safety elaborará um relatório das condições perigosas (hazard) e dos riscos de segurança associados identificados e que afetam tais alternativas.

8 ATIVIDADES DE SAFETY PARA CONTRATAÇÃO DOS SUBSISTEMAS DO SATÉLITE EQUARS

Especificamente quando se tratar dos contratos industriais de fornecimento de subsistemas do satélite EQUARS, o plano de safety a ser seguido é o definido em DA3 (TBD-1).

9 ATIVIDADES DE SAFETY PARA ATIVIDADES DE AIT SATÉLITE EQUARS

Especificamente quando se tratar das atividades de AIT do satélite EQUARS, o plano de safety a ser seguido é o definido em DA4 (TBD-2).

10 PACOTE DE DADOS DE SAFETY

Para cada fase da Missão EQUARS (ex: Fase B, Fase C/D) um conjunto de documentos, doravante *Safety Data Package* será entregue para cada um dos segmentos da Missão EQUARS.

Este *Safety Data Package* compõe pelo menos os seguintes documentos:

- Formulários das Análises Preliminares de Perigos;
- Relatório de análise de perigos;
- Formulários do levantamento dos riscos de segurança;
- Relatórios de análise dos riscos de segurança;
- Análise de perigos das funções críticas identificadas;

11 REVISÕES DE PROJETO

A equipe de safety participará de todas as revisões de projeto da Missão EQUARS pontuando as questões de safety identificadas durante todo o ciclo de vida.

EQUARS	Plano preliminar de segurança (safety) para a Missão EQUARS	
--------	---	--

LISTA DE ITENS <i>TO BE DEFINED</i>		
ID	DESCRIÇÃO	STATUS
TBD-1	Plano de safety para atividades de contratação dos subsistemas do EQUARS. Somente é possível durante a fase de contratação, quando já se conhece detalhes do item a ser adquirido.	Não iniciado
TBD-2	Plano de safety para atividades de AIT do EQUARS. Documento deverá ser preparado para a PDR.	Não iniciado
TBD-3	Relatório de análise de riscos de segurança para as alternativas. Será finalizado até a conclusão da PRR.	Em andamento
TBD-4	Análise preliminar dos perigos para as opções de trade-off.	Em andamento
TBD-5	Análise de perigo das funções críticas	Não iniciado
TBD-6	Documentos a serem entregues na Fase C/D	Não iniciado
TBD-7	Documentos a serem entregues na Fase E	Não iniciado
TBD-8	Documentos a serem entregues na Fase F	Não iniciado
LISTA DE ITENS <i>TO BE CONFIRMED</i>		
ID	DESCRIÇÃO	STATUS