PDQSAT UNIVERSITY SPACE MISSION: HAZARD ANALYSIS AND RISK ASSESSMENT OF THE OPERATION PHASE

Latin American STAMP Workshop 2024

Eng. Pedro Henrique Corrêa Picanço

Supervisors:

Dra. Maria Cecilia Pereira de Faria

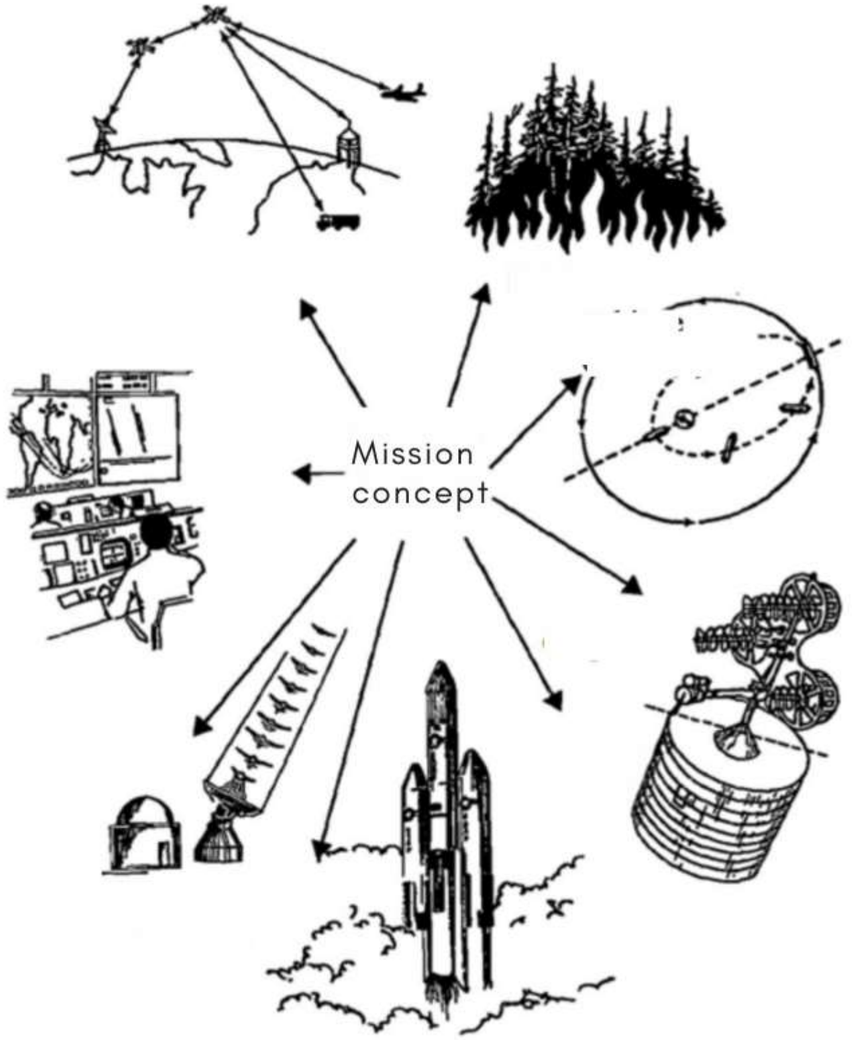
Eng. Carina Carla Aparecida Felipe da Silva

SPACE MISSION

HOW COMPLEX IS IT?

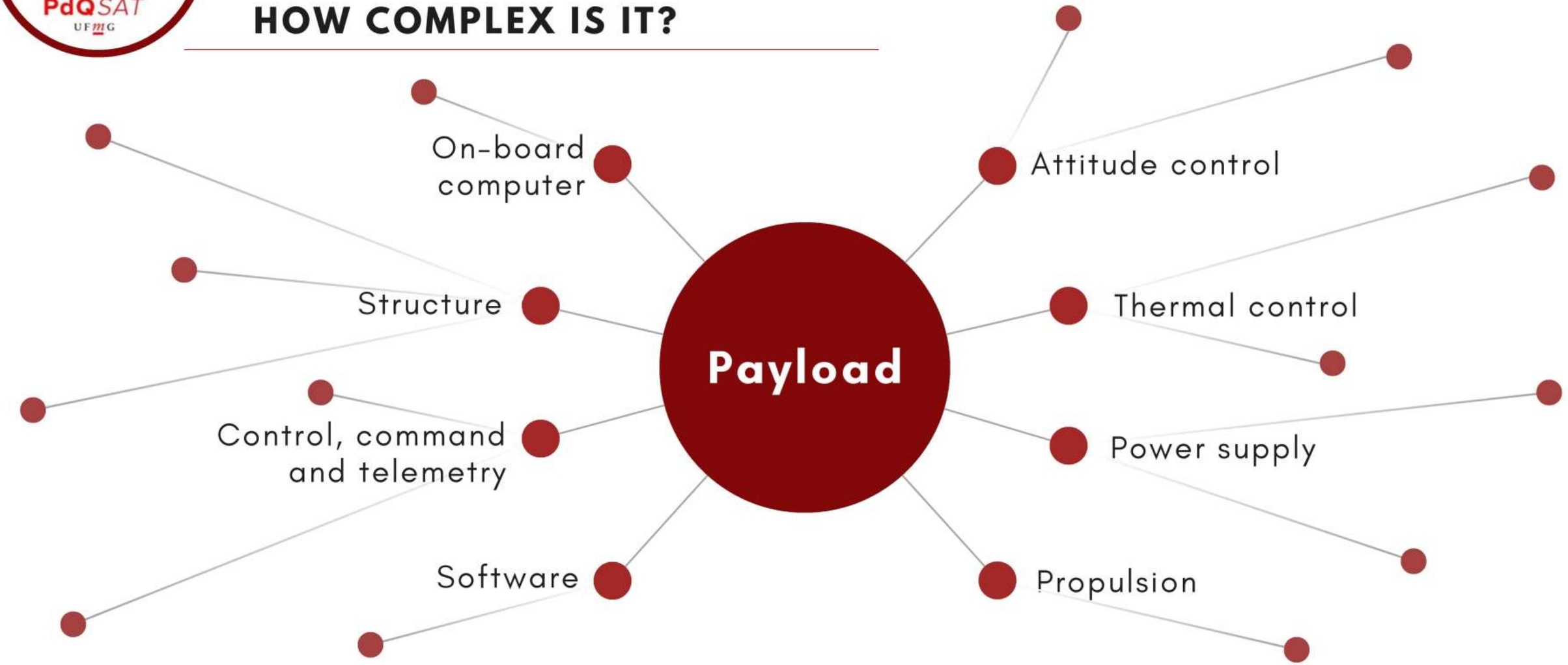
SYSTEM OF SYSTEMS

- Space mission's elements
- Complex interconnected systems
- High reliability



SPACE MISSION

HOW COMPLEX IS IT?

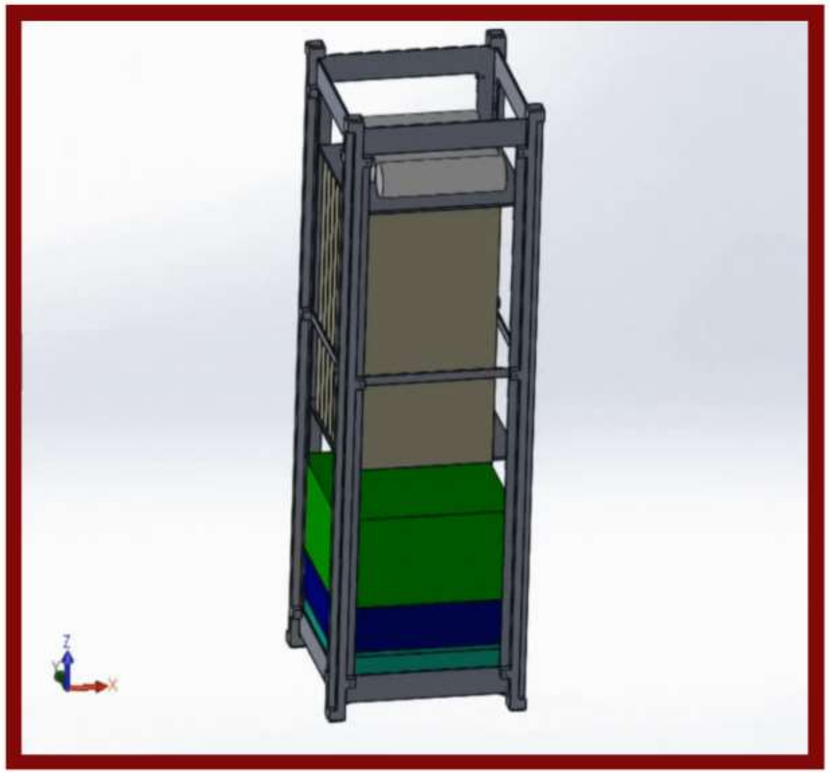


PDQSAT - PÃO DE QUEIJO SATÉLITE

UNIVERSITY SATELLITE

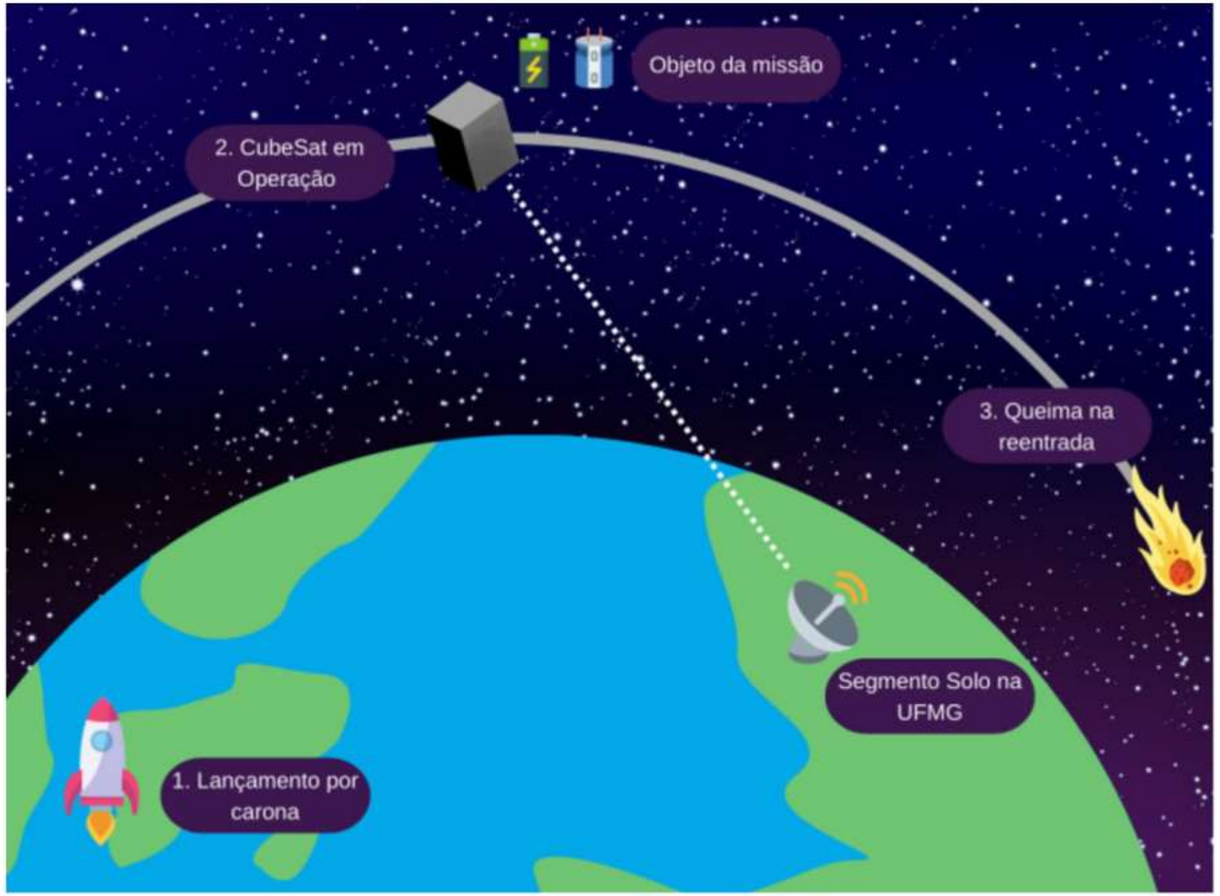
GOALS

- Characterize Li-S batteries and supercapacitor in hostile environment
- Qualify workforce in high-tech Engineering at UFMG
- Establishing Minas Gerais state in the Brazilian space scenario



PDQSAT - PÃO DE QUEIJO SATÉLITE

CONCEPT OF OPERATIONS



PHASES

- Hitchhiking rocket launch
- Minimum duration of 6 months in orbit
- Solo segment at UFMG
- Disposal by natural decay

WHY STPA?

- Previous work

  "APLICAÇÃO DE METODOLOGIAS DE ENGENHARIA DE SISTEMAS PARA O CICLO DE VIDA DO PDQSAT I - CUBESAT ACADÊMICO"

  Bruna Queiroz

- Based on Systems Theory and the STAMP approach

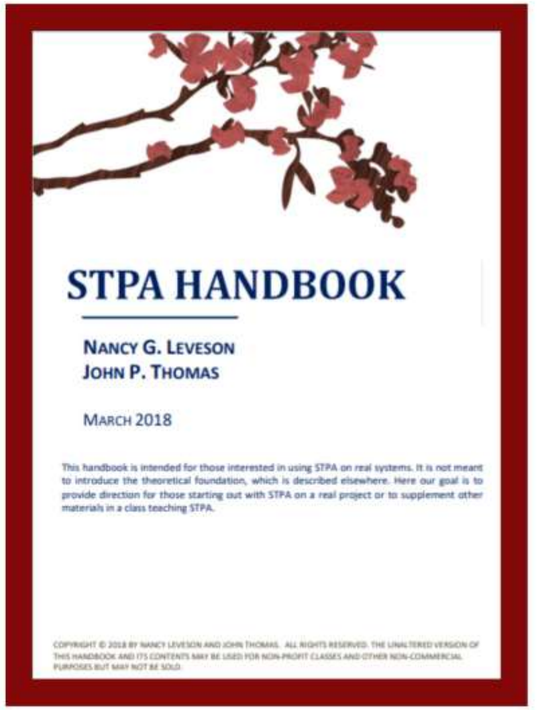
- Holistic view of problems as a whole and emerging properties

IMPORTANT DEFINITIONS

"A **loss** involves something of value to stakeholders. Losses may include a loss of mission, (...), loss or leak of sensitive information, or any other loss that is unacceptable to the stakeholders."

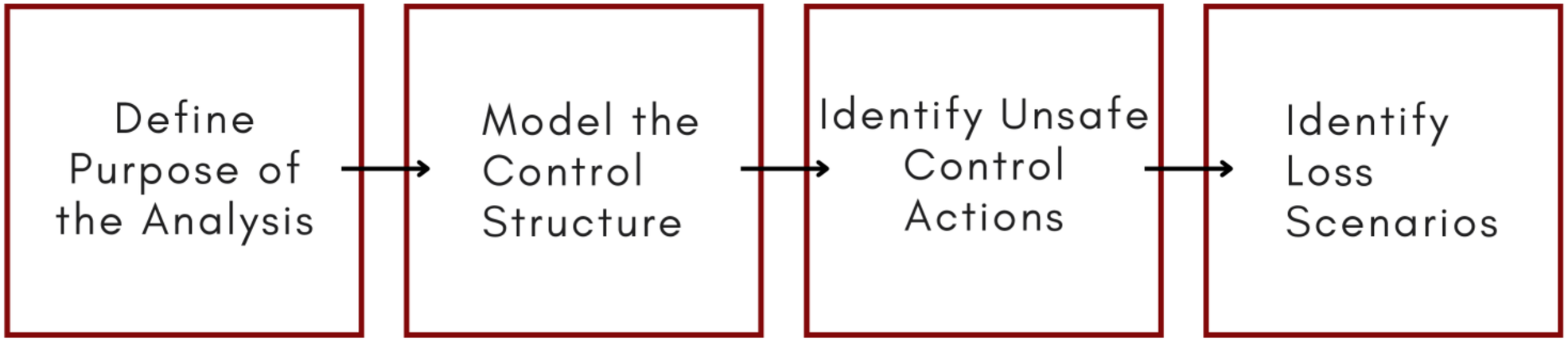
"A **hazard** is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss."

"**Risk** is an uncertain event or condition, that if it occurs, has a positive or negative effect on a project's objective." (PMBOK, 2005).



SYSTEMS THEORETIC PROCESS ANALYSIS (STPA)

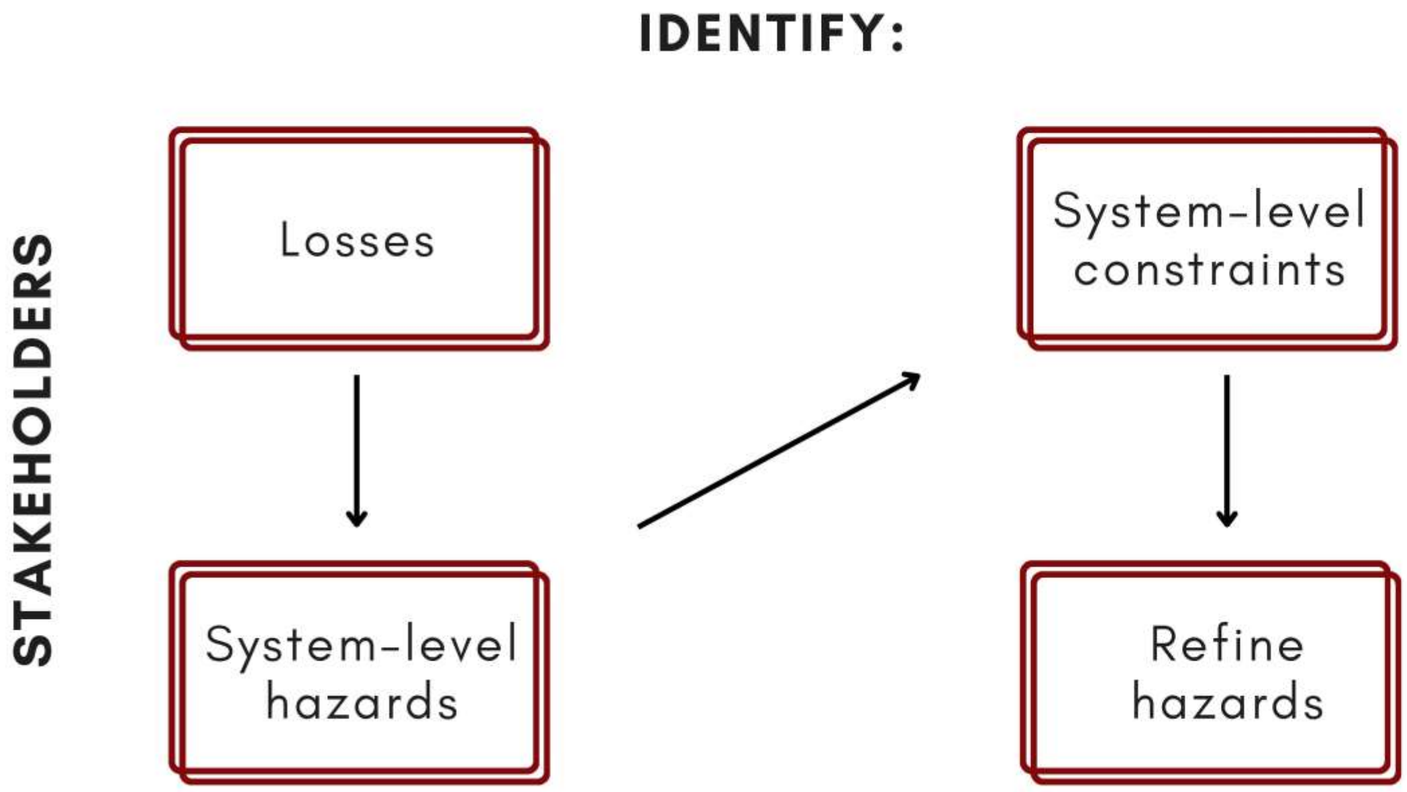
MAIN STEPS



STPA

STEP 1

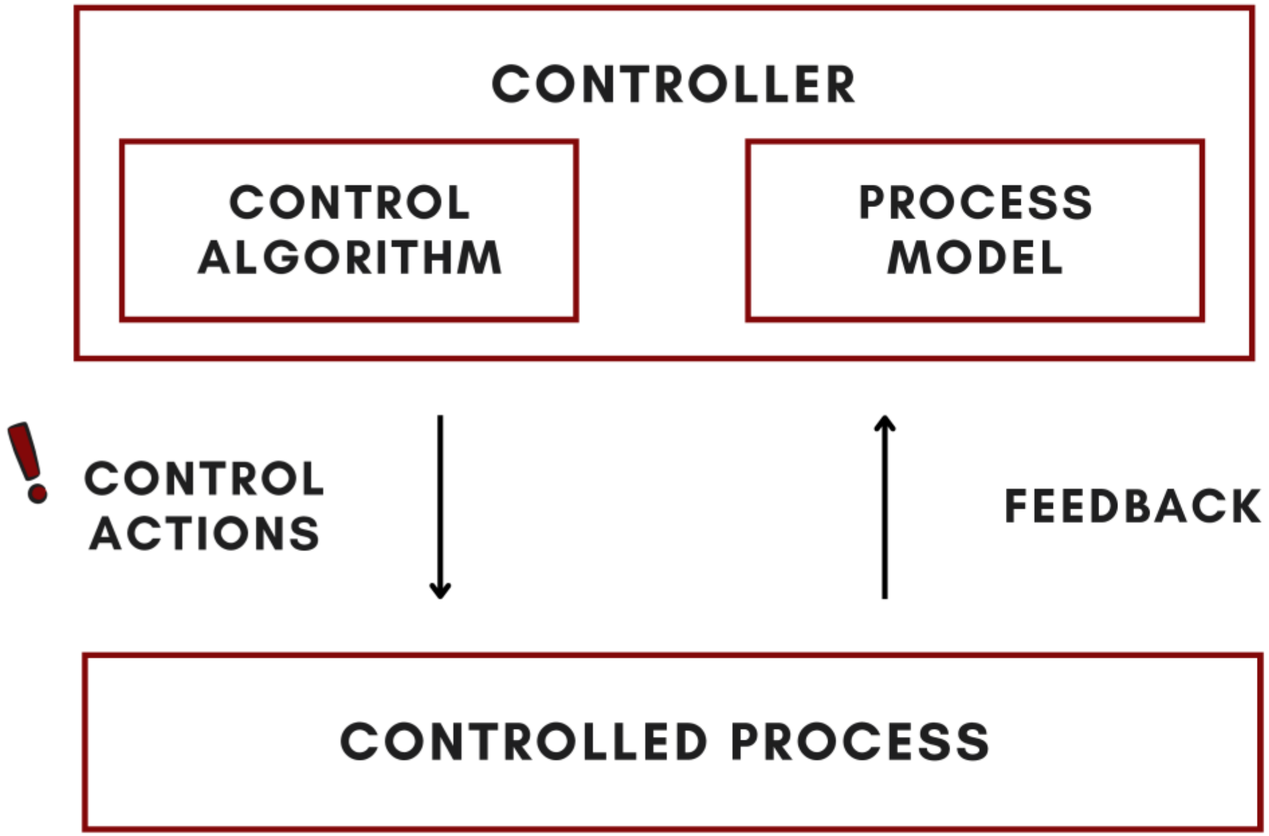
Define Purpose of the Analysis

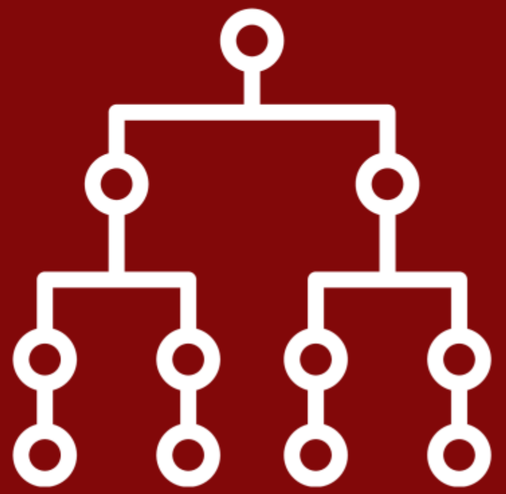


STPA

STEP 2

Model the Control Structure - *control loop*





STPA

STEP 3

Identify Unsafe Control Actions

CONTROL ACTION	CONTEXT	DO NOT PROVIDE ACTION CAUSES HAZARD	PROVIDE ACTION CAUSES HAZARD	TOO EARLY, TOO LATE, OUT OF ORDER	FINISHED TOO SOON, APPLIED FOR TOO LONG

UCA - N: <Source> + <Type> + <Control Action> + <Context> + <Consequence> + [Hazard Tracking]

STPA

STEP 4

Identify Loss Scenarios

- UCA - Unsafe Control Action
- Controller problem
- Problem between controller and controlled process
- Problem in the controlled process
- Controller process model problem

RISK ASSESSMENT

Risk Acceptance Matrix

- Matrix Size
- Severity and possibility ruler
- Selection of risks into levels

RISCOS

LOSSES DEFINED FOR THE MISSION

ID	Loss Description
L1	Financial Loss
L2	Knowledge Loss
L3	Missed Deadline
L4	Satellite-Ground System Loss
L5	Experiment Quality Loss
L6	Situational Awareness Loss

Mission financial budget

Documentation; data; mission goal

Opportunities

Structures

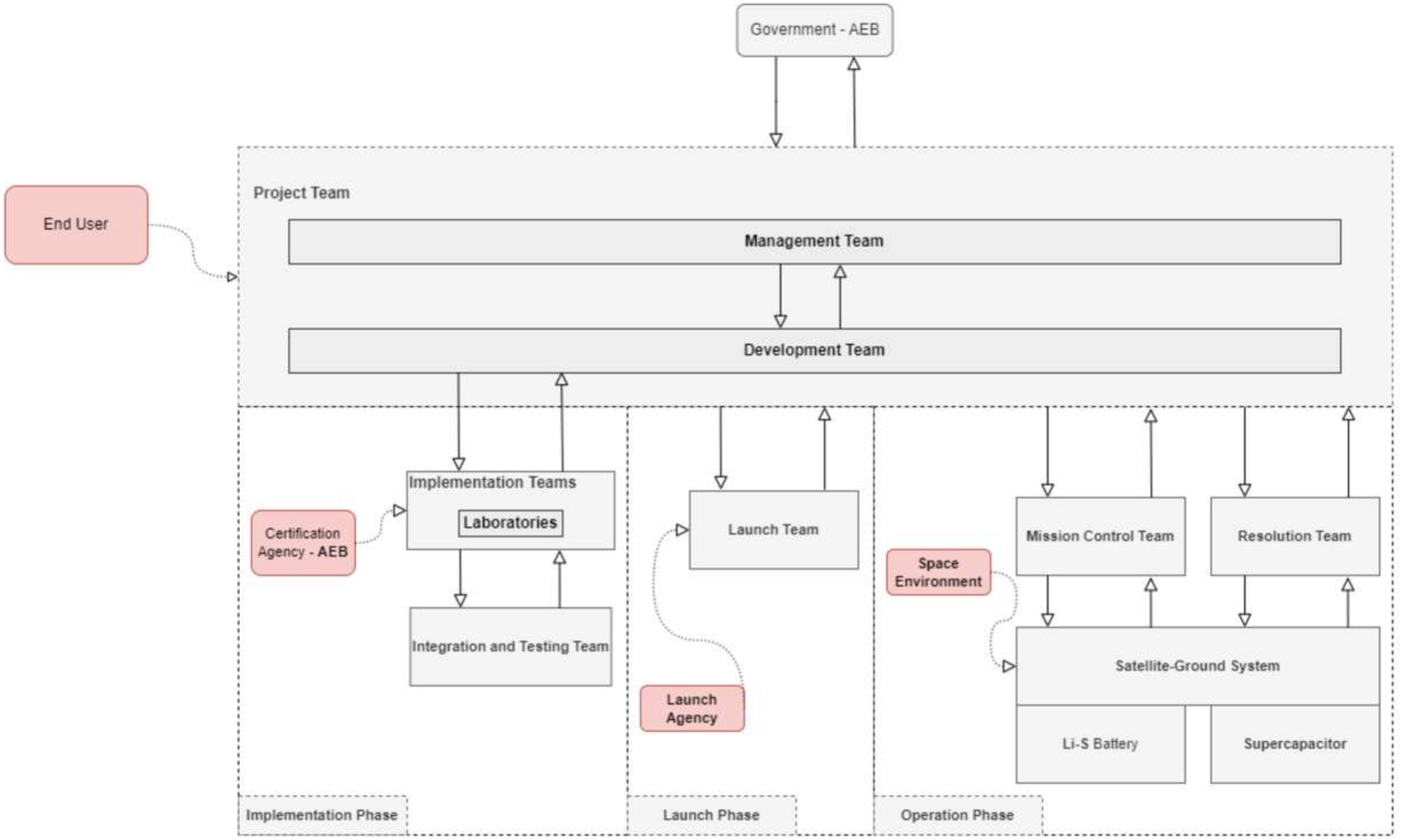
Batteries; supercapacitor

Satellite; comunication; information

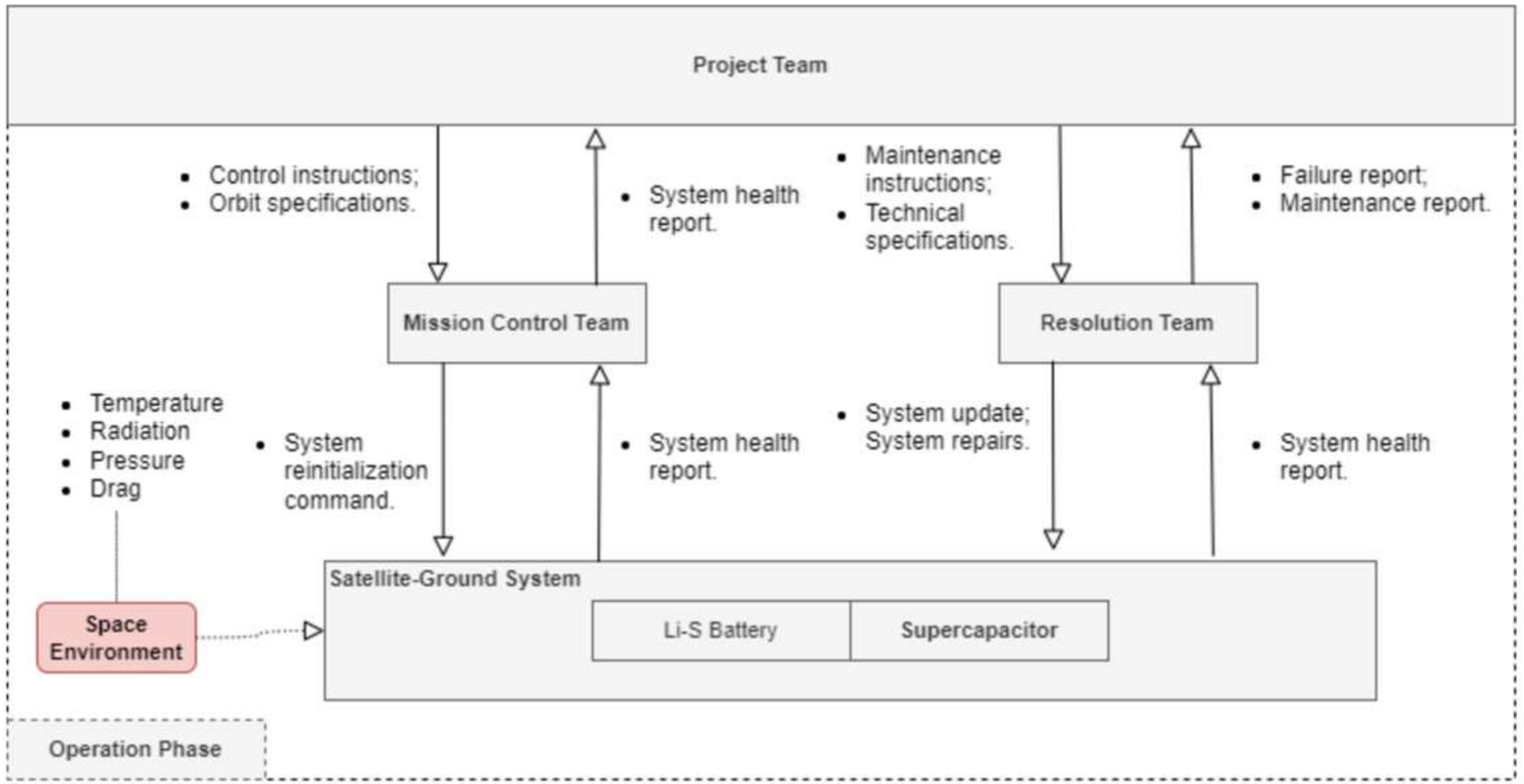
HAZARDS TRACKED

ID	Hazard Description	Related losses
H-1	Communication efficiency for the mission is compromised	L1, L2, L4, L5, L6.
H-2	The system is operating without power supply	L1, L2, L4, L5.
H-3	The system does not have adequate situational awareness	L2, L3, L4, L5, L6.
H-4	The system is not configured to accomplish the mission	L1, L2, L3, L4, L5, L6.
H-5	The system is not configured to maintain the quality of experiments	L2, L3, L5.

CONTROL STRUCTURE



OPERATION PHASE



HAZARDS TRACKED

Ação de Controle	Contexto	Não prover ação causa perigo	Prover ação causa perigo	Cedo demais, tarde demais, fora de ordem	Finalizado cedo demais, aplicado por tempo demais
Reinicialização do sistema em órbita	**Fase de lançamento**	Não há perigo	Não há perigo	Não há perigo	Não há perigo
	Fase de inicialização do satélite em órbita	UCA-1: O time de controle não prover a reinicialização do sistema em órbita durante a fase de inicialização do satélite em órbita resulta em satélite não ser capaz de completar a inicialização. **H-1, H-3, H-4, H-5**	UCA-2: O time de controle prover a reinicialização do sistema em órbita durante a fase de inicialização do satélite em órbita resulta em satélite não ser capaz de completar a inicialização. **H-1, H-2, H-3, H-4, H-5**	Não há perigo	Não há perigo
	Fase de operação do satélite em órbita	UCA-3: O time de controle não prover a reinicialização do sistema em órbita durante a fase de operação do satélite em órbita resulta em satélite não ser capaz de completar a operação. **H-1, H-2, H-3, H-4, H-5**	UCA-4: O time de controle prover a reinicialização do sistema em órbita durante a fase de operação do satélite em órbita resulta em satélite perder dados de operação. **H-5**	Não há perigo	Não há perigo
	Fase de reentrada	Não há perigo	Não há perigo	Não há perigo	Não há perigo

- Tracking
- Easy to understand

HAZARDS TRACKED

UCA-1: The control team **not** providing for the in-orbit system reset during the in-orbit satellite initialization phase results in the satellite not being able to complete the initialization. **H-1, H-3, H-4, H-5.**

LOSS SCENARIOS

- 145 different loss scenarios

UCA	Problema no Controlador	Problema Entre Controlador e Modelo Controlado	Problema no Modelo Controlado	Problema no Modelo de Processo do Controlador
UCA-15: O time de resolução prover os reparos do sistema de forma errada durante a fase de inicialização do satélite em órbita resulta no não recebimento dos dados de housekeeping ou na leitura errada dos dados de housekeeping. H-1, H-3, H-4, H-5	Cenário 58 para UCA-15: O time de resolução prover os reparos do sistema de forma errada durante a fase de inicialização do satélite em órbita resulta no não recebimento dos dados de housekeeping ou na leitura errada dos dados de housekeeping [UCA-15] porque o time de resolução não possui o conhecimento de reparo da antena.	Cenário 59 para UCA-15: O time de resolução prover os reparos do sistema de forma errada durante a fase de inicialização do satélite em órbita resulta no não recebimento dos dados de housekeeping ou na leitura errada dos dados de housekeeping [UCA-15] porque o tempo foi reduzido demais para reparo adequado para funcionalidade do sistema, nesta etapa.	Cenário 60 para UCA-15: O time de resolução prover os reparos do sistema de forma errada durante a fase de inicialização do satélite em órbita resulta no não recebimento dos dados de housekeeping ou na leitura errada dos dados de housekeeping [UCA-15] porque o time de resolução não possui o as ferramentas necessárias para reparo.	Cenário 61 para UCA-15: O time de resolução prover os reparos do sistema de forma errada durante a fase de inicialização do satélite em órbita resulta no não recebimento dos dados de housekeeping ou na leitura errada dos dados de housekeeping [UCA-15] porque o sitema antena-painel de controle apresenta notificação errada de problemas da antena.

- Research on weaknesses
- Understand the situations

LOSS SCENARIOS

Scenario 58 for UCA-15: The resolution team incorrectly providing system repairs during the initialization phase of the satellite in orbit results in housekeeping data not being received or housekeeping data being read incorrectly **[UCA-15]** because the resolution team does not have the knowledge to repair the system.

RISK ASSESSMENT

- 145 loss scenarios
- Risk level
- Hazard exposure
- Hazard leading to an accident

Possibility		Description of possibility criteria
Numeric	Descriptive	
1	UNLIKELY	Unlikely to happen
2	POSSIBLE	May happen once
3	LIKELY	Likely to happen one or more times

Severity		Description of severity criteria
Numeric	Descriptive	
1	LOW	Risks have minor consequences
2	MEDIUM	Risks have short- and medium-term reversible consequences with viable costs
3	HIGH	Risks have irreversible consequences or unviable costs

	Severity		
Possibility	LOW 1	MEDIUM 2	HIGH 3
UNLIKELY 1	1	2	3
POSSIBLE 2	2	4	6
LIKELY 3	3	6	9

RISK ASSESSMENT

Scenario	Severity	Possibility	Risk
C51	HIGH	LIKELY	9
C52	HIGH	UNLIKELY	3
C53	HIGH	POSSIBLE	6
C54	HIGH	UNLIKELY	3
C55	HIGH	LIKELY	9
C56	HIGH	UNLIKELY	3
C57	HIGH	POSSIBLE	6
C58	HIGH	POSSIBLE	6
C59	HIGH	POSSIBLE	6
C60	HIGH	UNLIKELY	3
C61	HIGH	UNLIKELY	3

Scenario Count	Risk Level
14	1
29	2
46	3
16	4
38	6
2	9

MISSION IMPACT

- Holistic view of the mission
- Prioritization in project decisions
- Risks divided into levels
- Mitigation of losses as a focus of action
- Actuators for mitigation
- Continuous process of improvement

PDQSAT UNIVERSITY SPACE MISSION: HAZARD ANALYSIS AND RISK ASSESSMENT OF THE OPERATION PHASE

Eng. Pedro Henrique Corrêa Picanço

/pedropicanco

Tel: (91) 98947-3797

E-mail: pedrohcpicanco@gmail.com