Space Informatics

Week 10: Safety and Reliability of Space System

Computer Science and Communications, University of Luxembourg

19 November 2019

Part 2

safety and reliability

objectives of the future lectures:

consider cyber-physical systems at a higher level

safety and reliability

objectives of the future lectures:

consider cyber-physical systems at a higher level

→ less code, more abstracted complex systems

safety and reliability

objectives of the future lectures:

consider cyber-physical systems at a higher level

→ less code, more abstracted complex systems

→ human reasoning

safety and reliability

overview of the future lectures (“to be presented” techniques):

→ for safety:

anticipate a dreaded event by identifying relations between causes and consequences

safety and reliability

overview of the future lectures (“to be presented” techniques):

→ for safety:

anticipate a dreaded event by identifying relations between causes and consequences

→ for reliability:

prove that pieces of code are correct

prove that a complex cyber physical system (e.g. a Cubesat) behaves as expected

safety

1. fault tree analysis, a powerful technique
2. fault trees 101
3. examples of gates and events
4. Fault tree analysis: a concrete case study
5. Fault trees events: unintended or maliciously provoked
6. Fault tree analysis: what is next?

fault tree analysis in a nutshell

- model cyber physical systems failure scenario

fault tree analysis in a nutshell

- model cyber physical systems failure scenario
- evaluate risks in order to find countermeasures

fault tree analysis

- H. A. Watson at Bell Telephone Laboratories (1961)
- at first, used by the U.S. Air Force
- shortly after, adopted by Boeing for their commercial flights
- Further developed and extended

fault tree analysis

- H. A. Watson at Bell Telephone Laboratories (1961)
- at first, used by the U.S. Air Force
- shortly after, adopted by Boeing for their commercial flights
- Further developed and extended
- still topical

fault tree analysis

- H. A. Watson at Bell Telephone Laboratories (1961)
- at first, used by the U.S. Air Force
- shortly after, adopted by Boeing for their commercial flights
- Further developed and extended
- still topical

Safety norms for
space systems,
ISO 26262
ISO 14620-1

fault tree analysis

- deductive method using *human reasoning*

fault tree analysis

- deductive method using *human reasoning*
- from a unique critical, failure event one must avoid (event of level 0, “root”)
- guess/determine direct causes of the event (events of level 1)

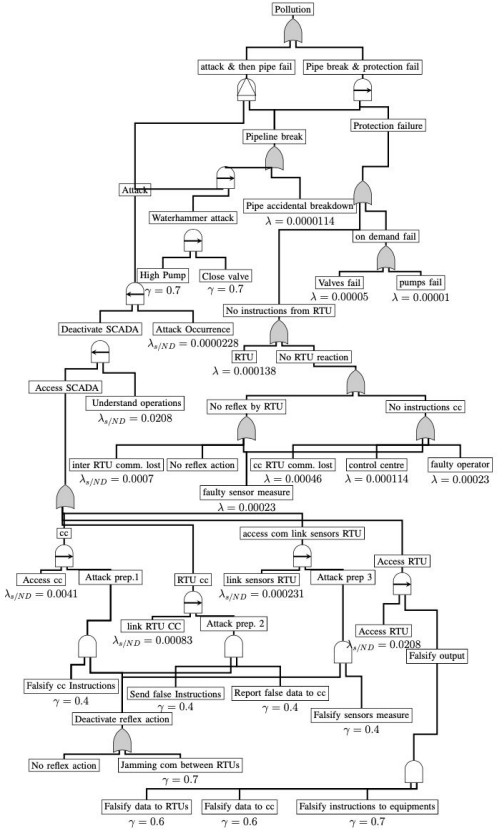
fault tree analysis

- deductive method using *human reasoning*
- from a unique critical, failure event one must avoid (event of level 0, “root”)
- guess/determine direct causes of the event (events of level 1)
- such that each cause (event) of level 1 is a consequence of causes (events) of level 2
- events can be combined together as necessary and sufficient conditions for the consequence to happen.

fault tree analysis

- deductive method using *human reasoning*
- from a unique critical, failure event one must avoid (event of level 0, “root”)
- guess/determine direct causes of the event (events of level 1)
- such that each cause (event) of level 1 is a consequence of causes (events) of level 2
- events can be combined together as necessary and sufficient conditions for the consequence to happen.
- … “unfold” causes and consequences until events at level XX are no longer decomposable (leaf)

fault tree analysis



looks like an inverted tree

1. fault tree analysis, a powerful technique
2. fault trees 101
3. examples of gates and events
4. Fault tree analysis: a concrete case study
5. Fault trees events: unintended or maliciously provoked
6. Fault tree analysis: what is next?

Fault trees structure

Simple structure; two types of elements

- **Logical gates**

The output of a logical gate at level N is a consequence of a combination of events of level N+1

Fault trees structure

Simple structure; two types of elements

- **Logical gates**

The output of a logical gate at level N is a consequence of a combination of events of level N+1

A gate is referred as a *parent*, while its input events are referred as its *children*

- indecomposable events: **leaves**

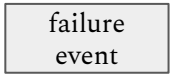
Leaves can be found at each level, however leaves have **no children.**

Logical gates

- combine different events together (input children)
- model goals, objectives (parents): *outputs whether the goal is achieved or not*

- AND gate: 
- OR gate: 
- SAND gate (sequential AND): 
- PAND gate (parallel AND): 
- ….

Failure events

- leaves of the tree (children) 

- indecomposable into smaller events: usually an expert opinion

- a timed system, a probabilistic system, a discrete system…
- a simple electrical component
- a basic human action

→ possibly eventually fails: its output becomes an input of its parent gate.

Examples of failure events

- Pressure control system failure: sensor disconnected; can we recover? Do we have sensors still working?

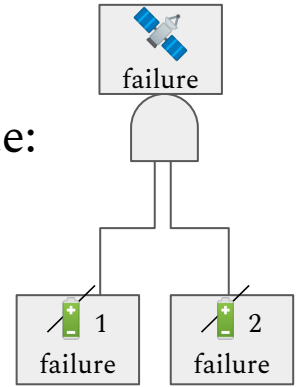
- Switch out of service: flawed component, fatality

- Communication system not responding: poor connectivity? possibility to recover?

1. fault tree analysis, a powerful technique
2. fault trees 101
3. examples of gates and events
4. Fault tree analysis: a concrete case study
5. Fault trees events: unintended or maliciously provoked
6. Fault tree analysis: what is next?

Gate: AND 1

AND gate:

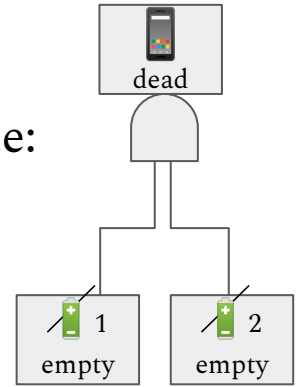


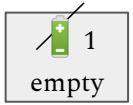
if 1 failure **and** 2 failure occur, then the gate is activated and the failure occurs (the objective).

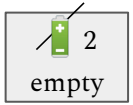
Battery failure: probability?

Gate: AND 2

AND gate:



if 

and 

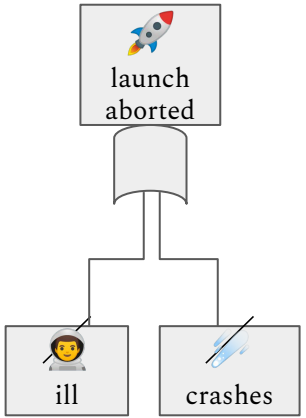
occur, then the gate is activated and 

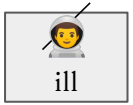
occurs.

Battery empty: mathematical equation to model the power consumption?

Gate: OR 1

OR gate:

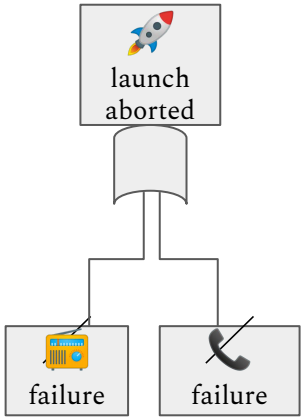


if  **or**  then the gate is activated and the 

Events: combination of probabilities and mathematical models?

Gate: OR 2

OR gate:



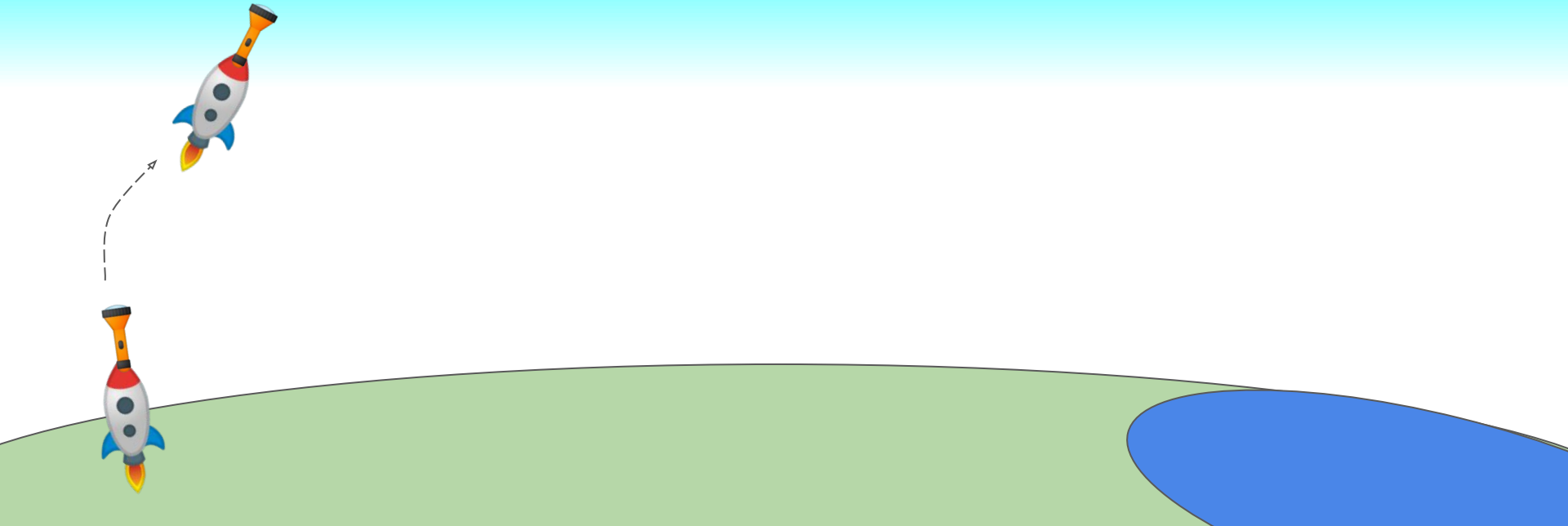
if failure **or** failure then the gate is activated and the launch aborted

Lost connection: issues with the component manufacturer?

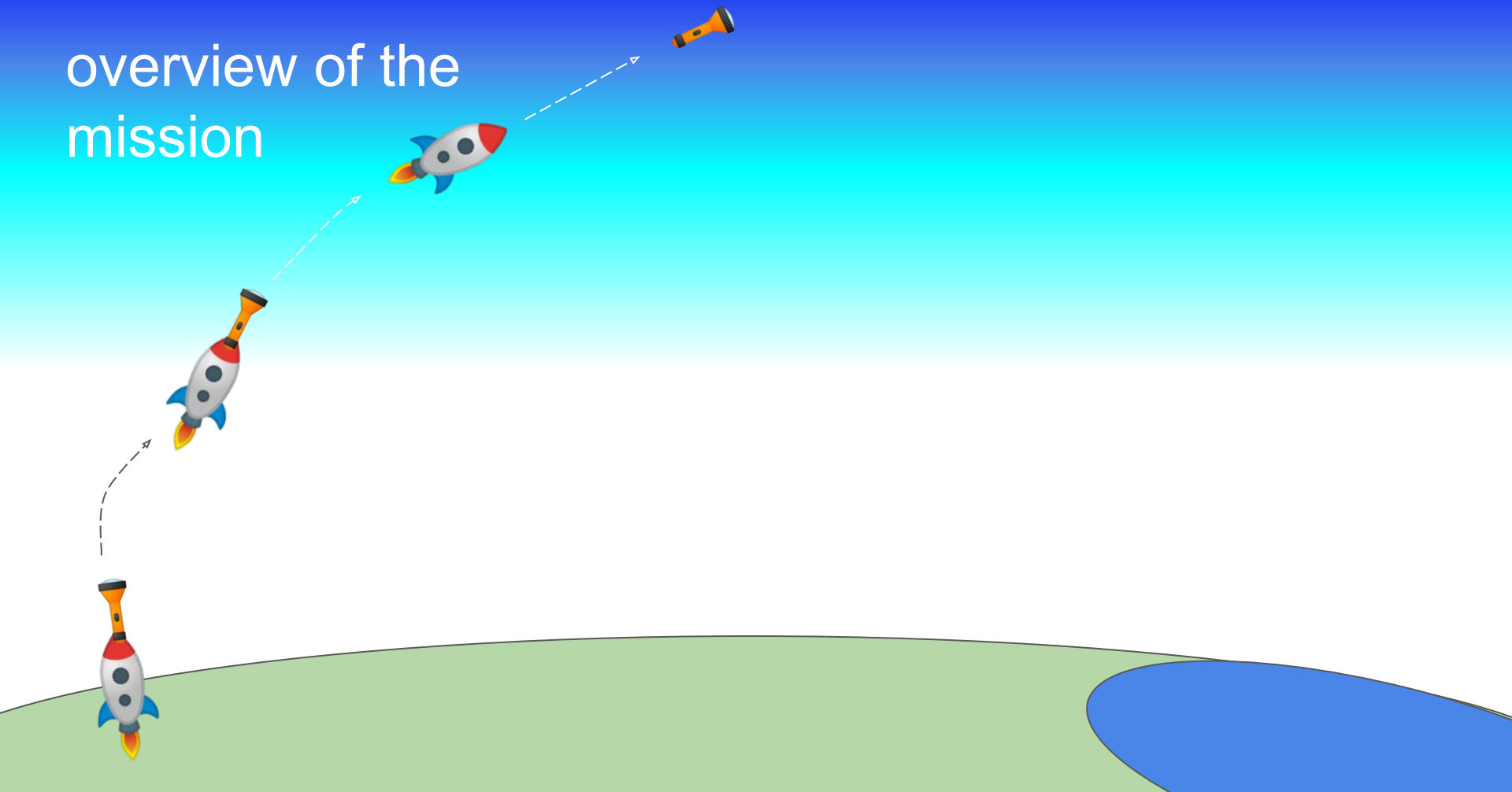
1. fault tree analysis, a powerful technique
2. fault trees 101
3. examples of gates and events
4. Fault tree analysis: a concrete case study
5. Fault trees events: unintended or maliciously provoked
6. Fault tree analysis: what is next?

overview of the mission

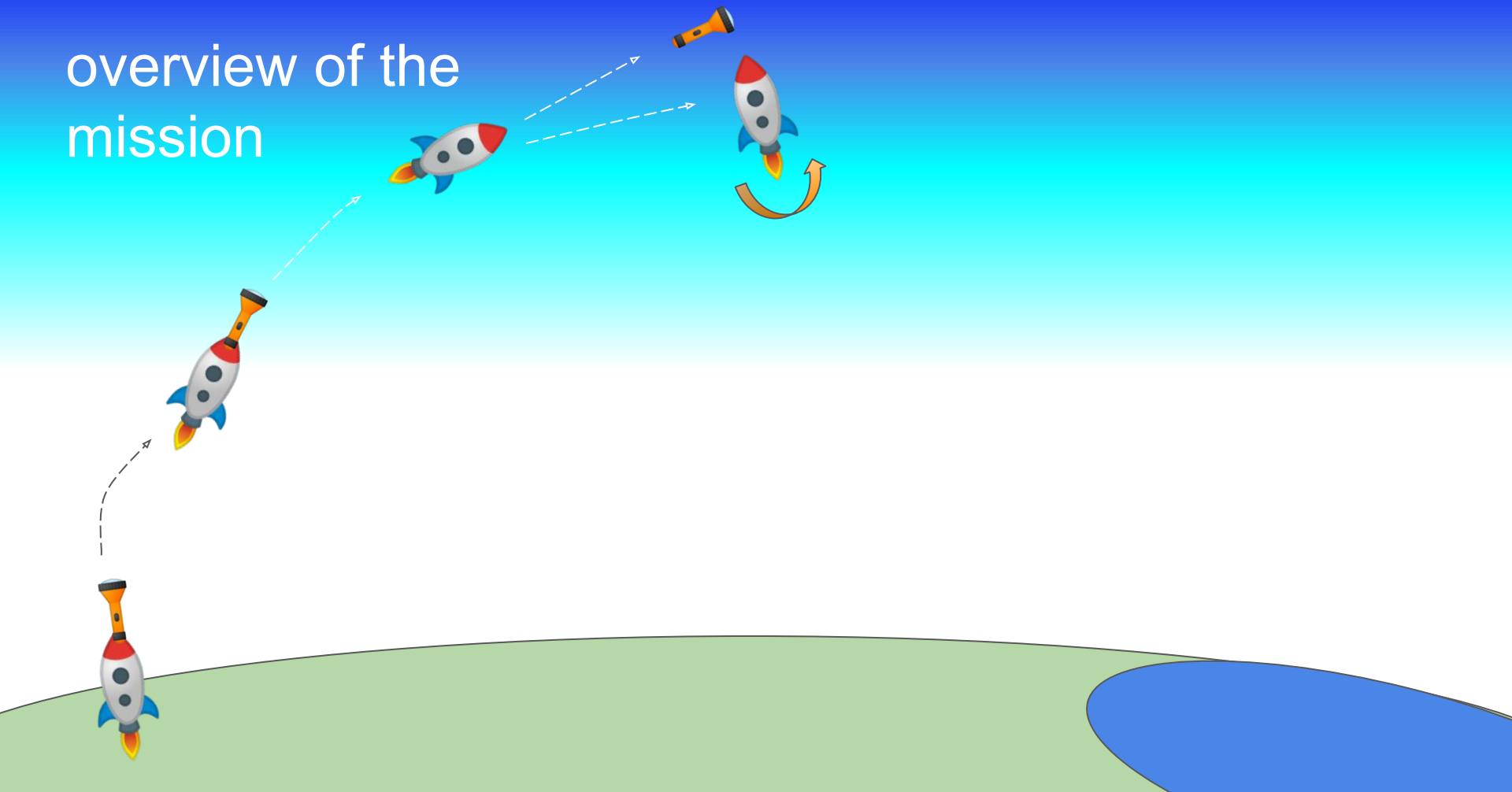
overview of the mission



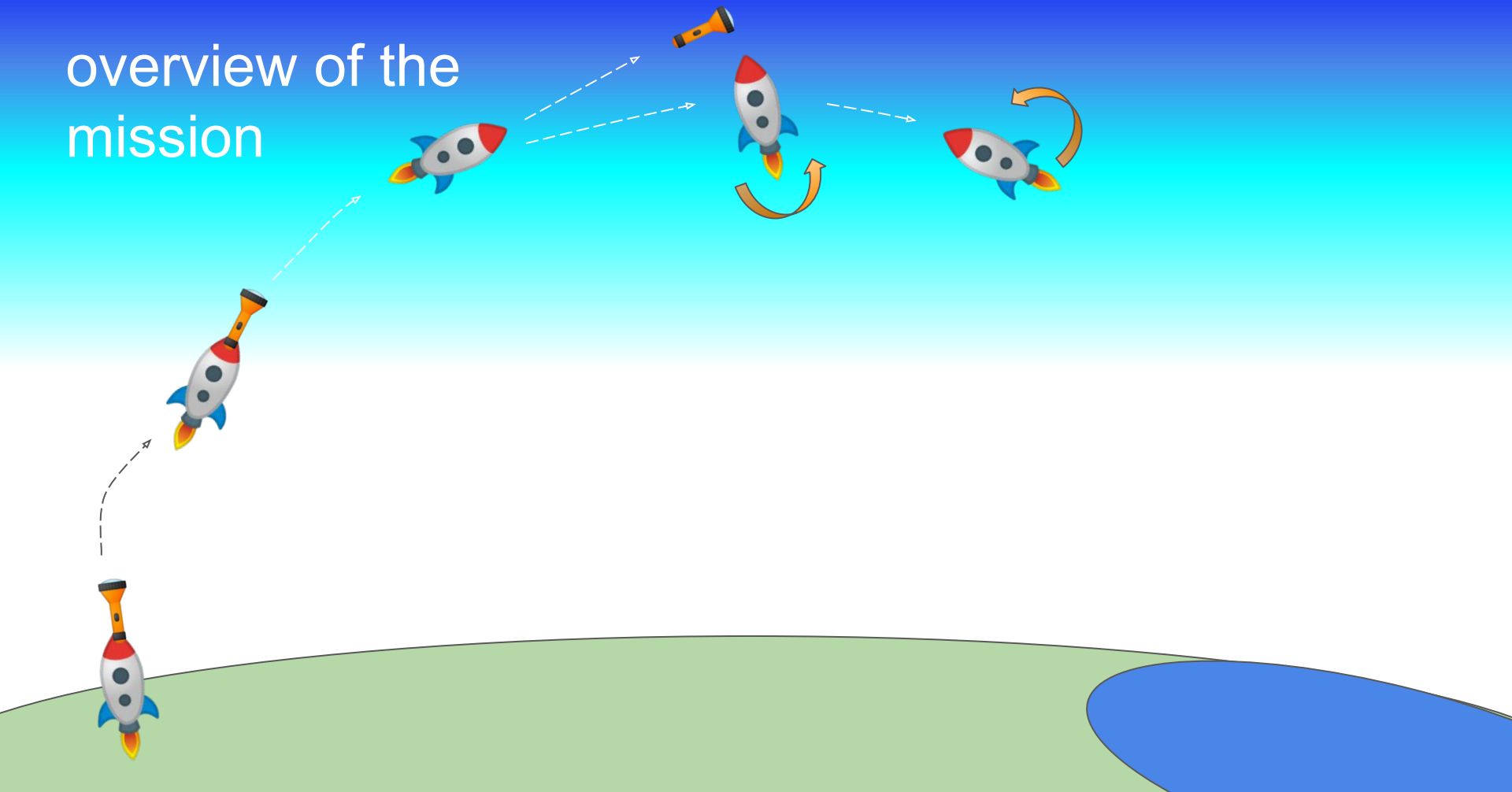
overview of the mission



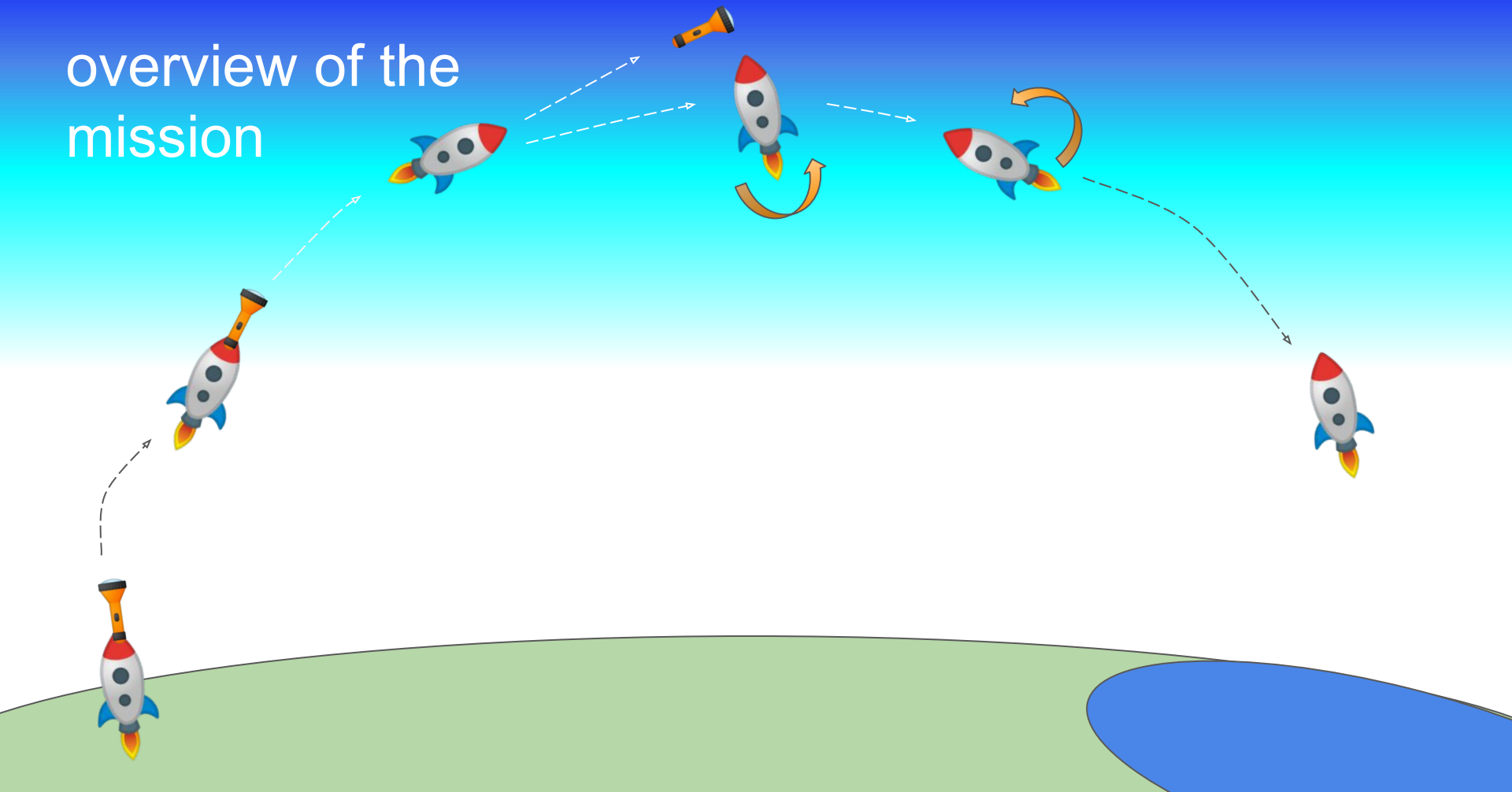
overview of the mission



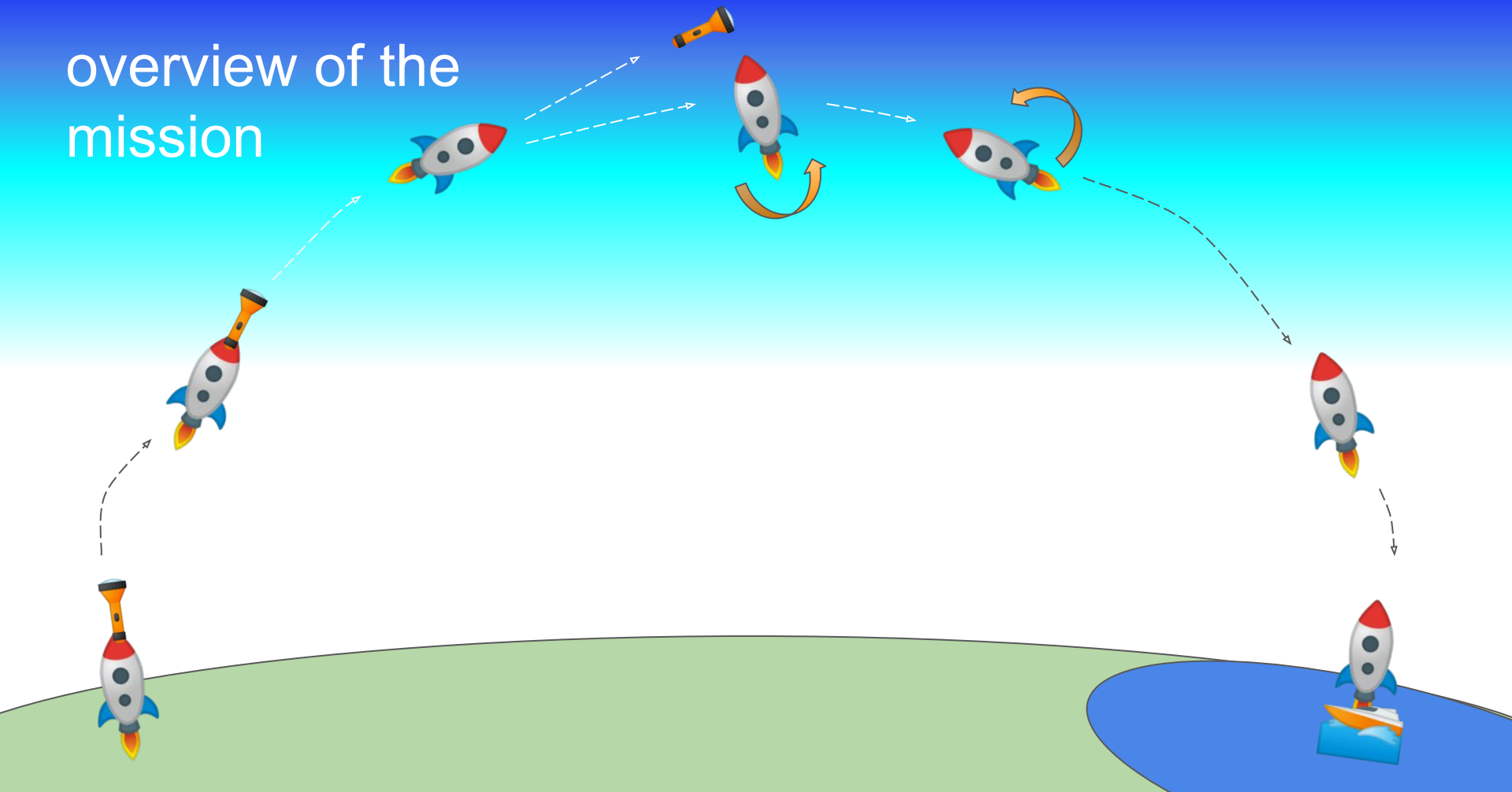
overview of the mission



overview of the mission



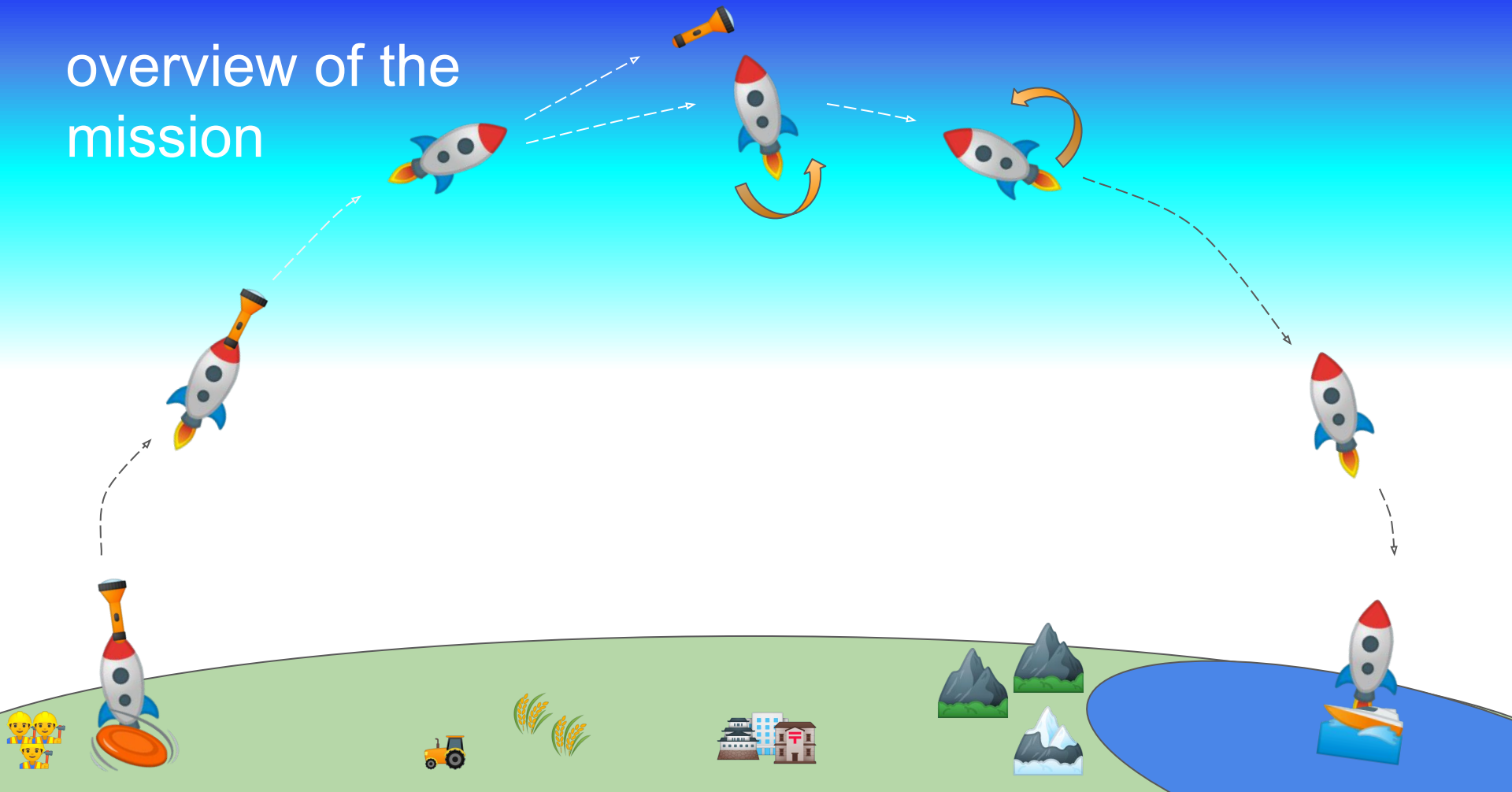
overview of the mission



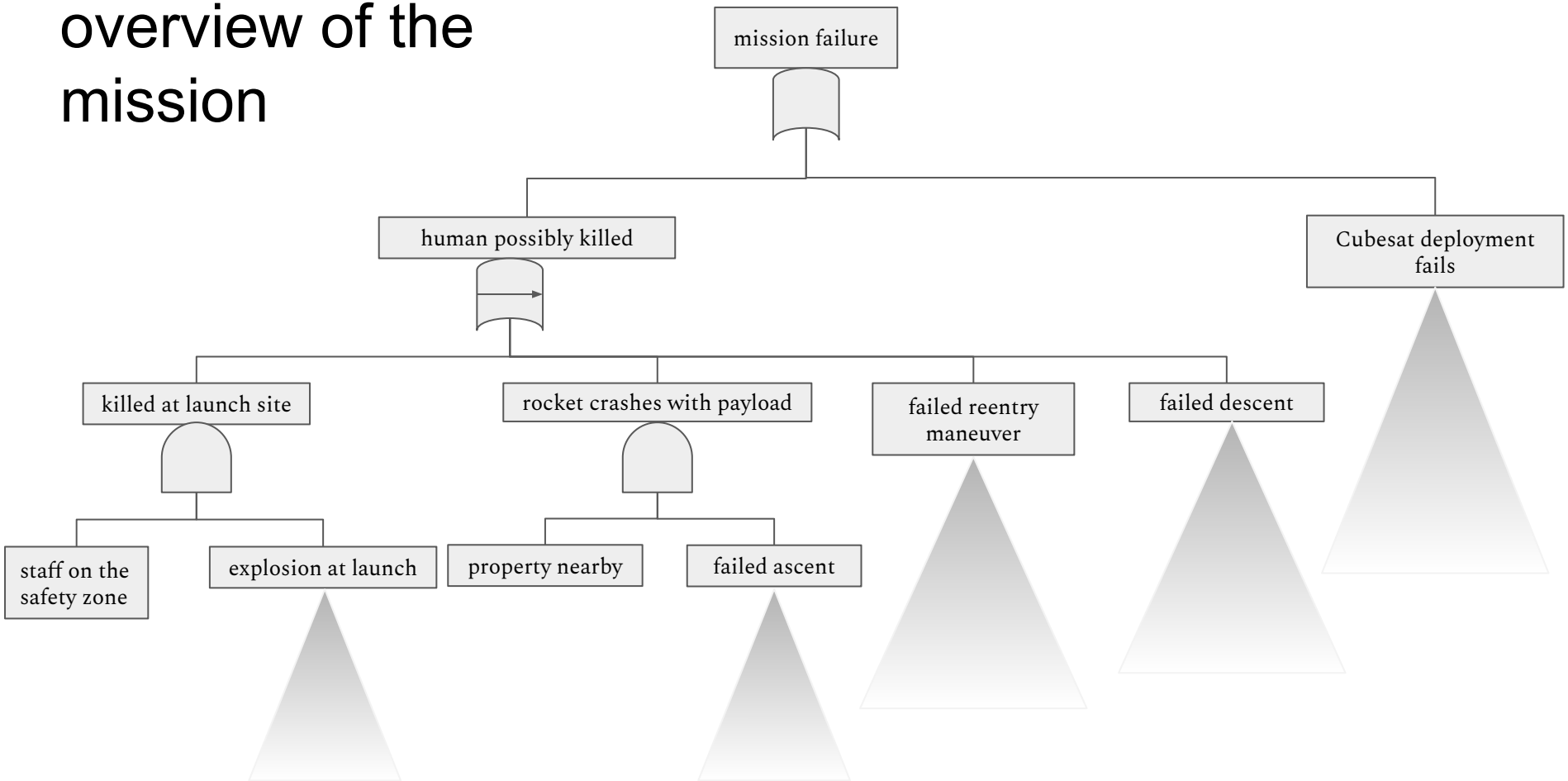
General objectives

- Critical: no human damages 💀
- High: no property destroyed on the ground 💰
- Medium: fail to put the payload in Low Earth Orbit (LEO)

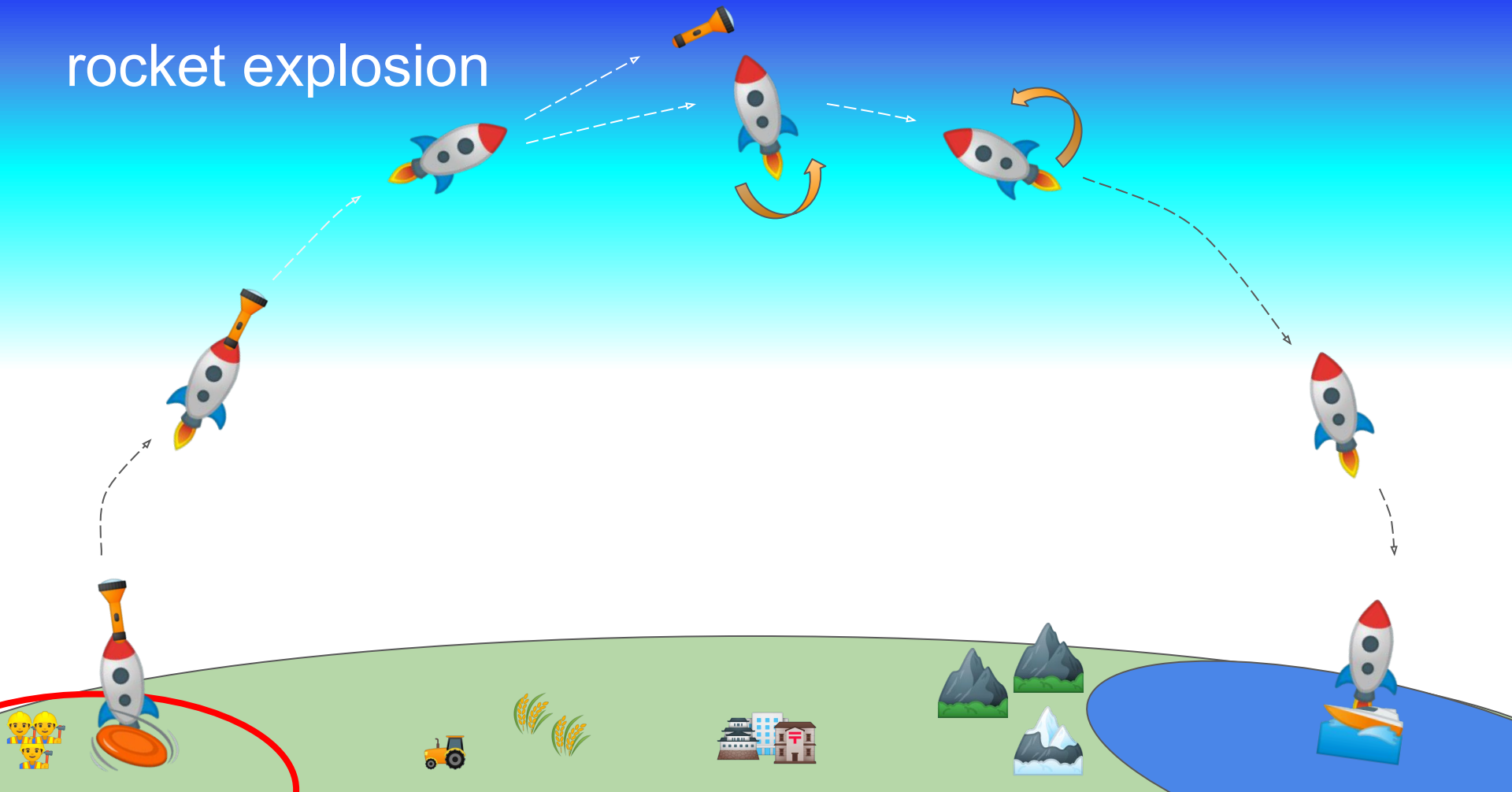
overview of the mission



overview of the mission



rocket explosion

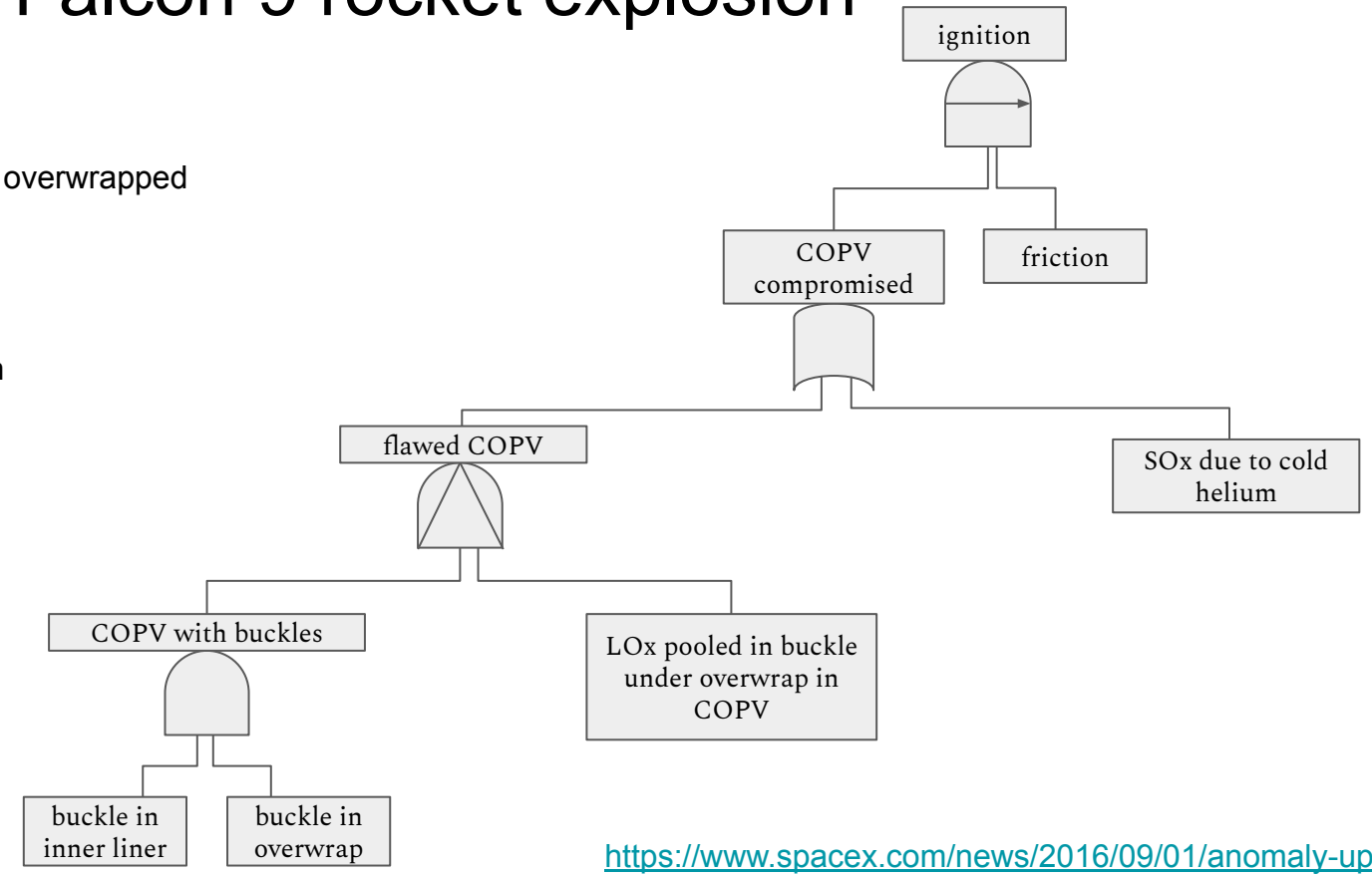


SpaceX Falcon 9 rocket explosion

COPV: composite overwrapped pressure vessel

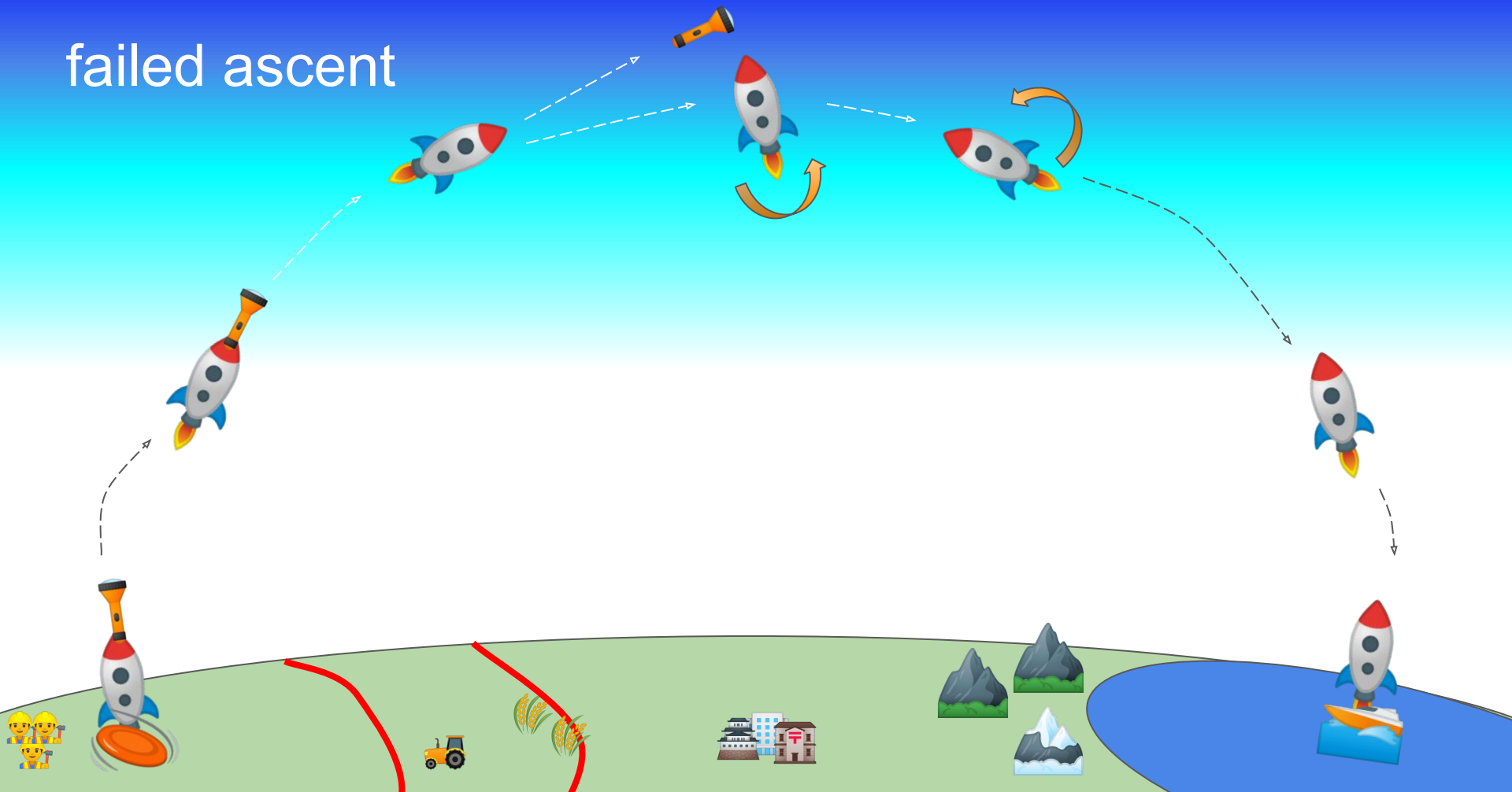
SOx: solid oxygen

LOx: liquid oxygen

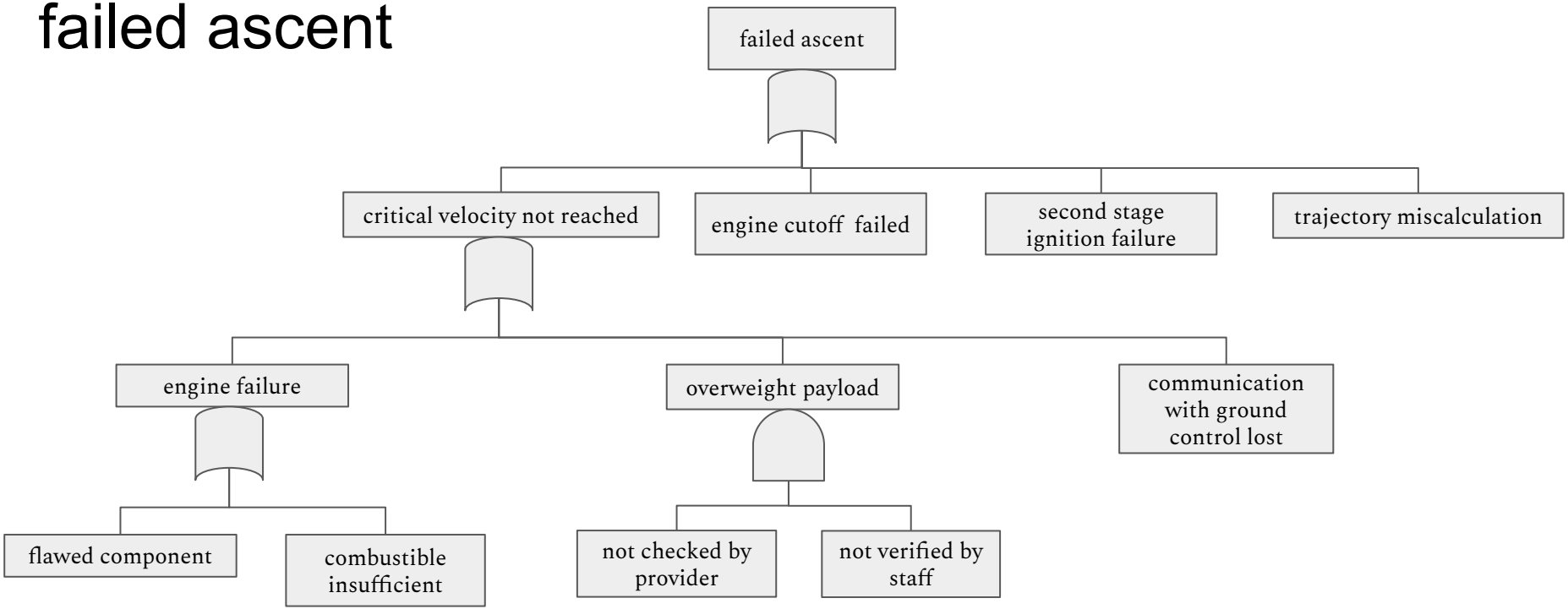


https://www.spacex.com/news/2016/09/01/anomaly-updates

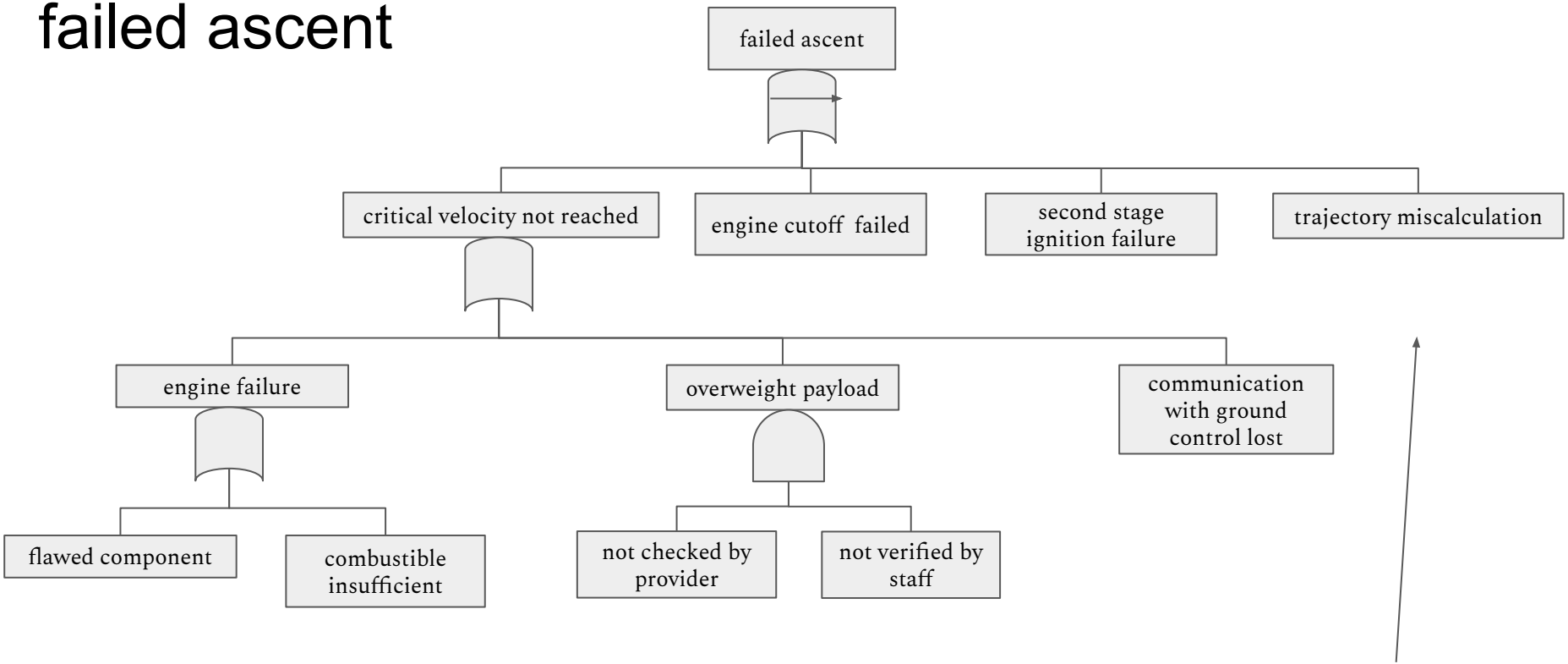
failed ascent



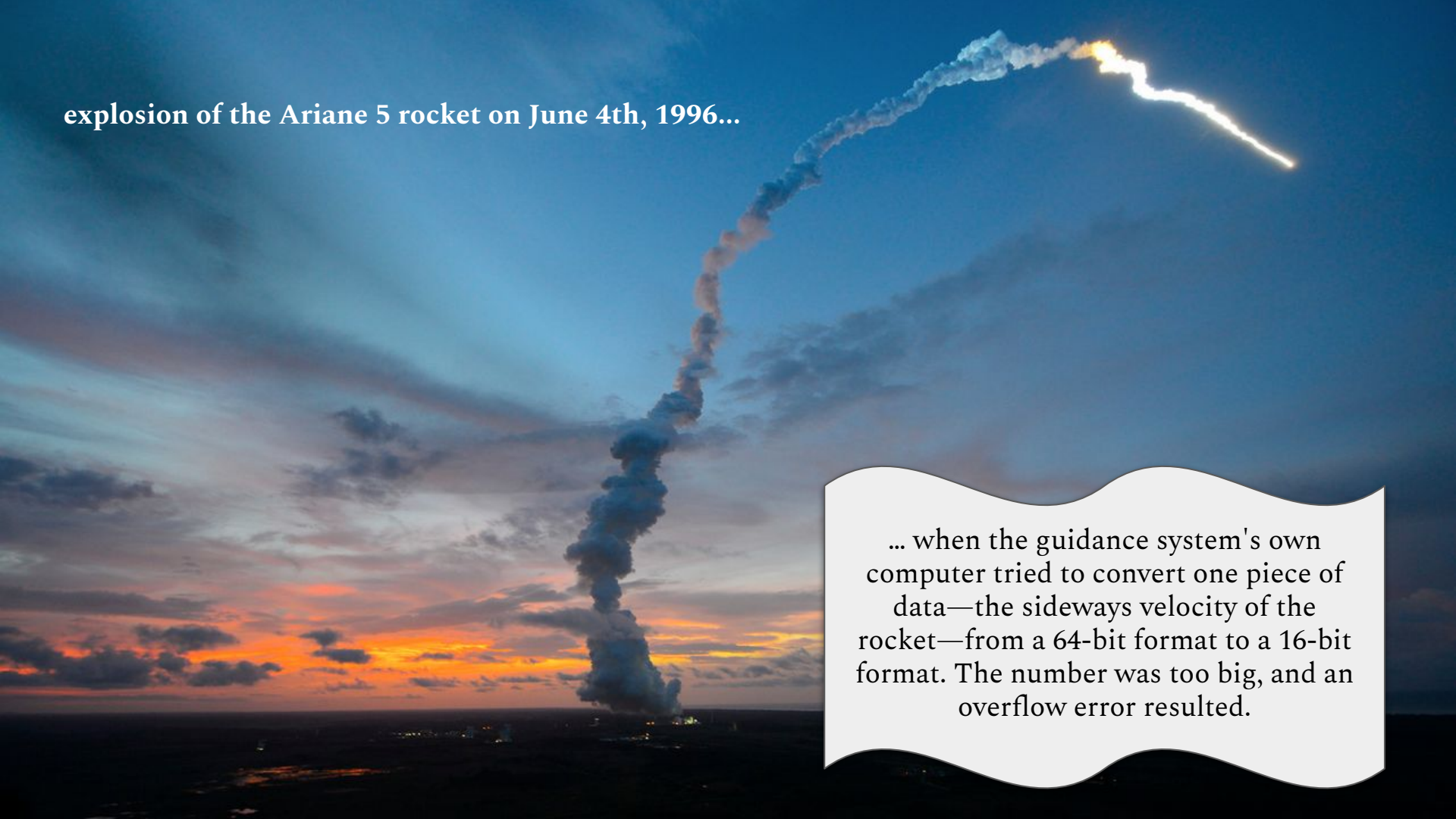
failed ascent



failed ascent



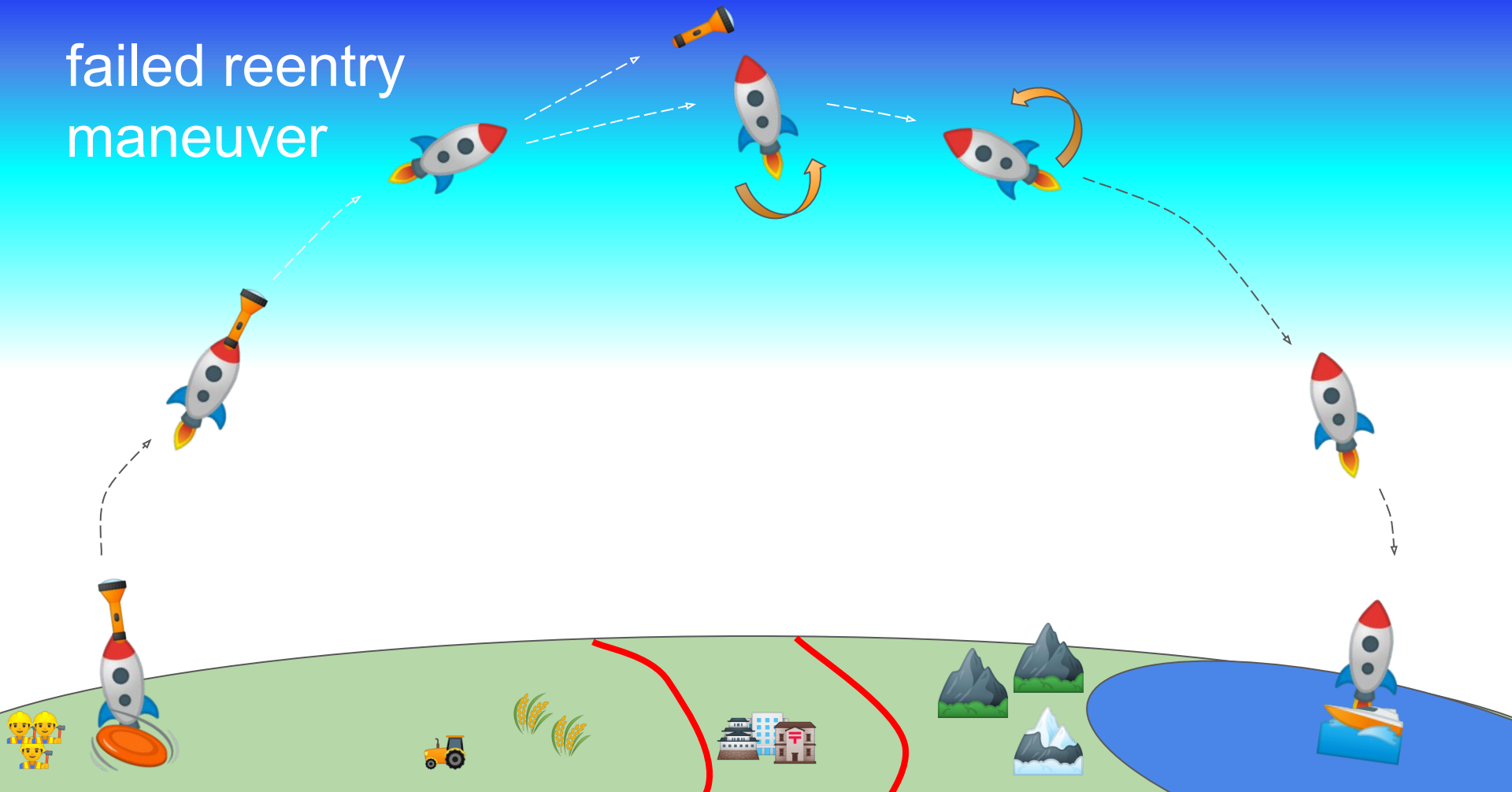
E.g., Ariane 5 failed due to a software vulnerability.



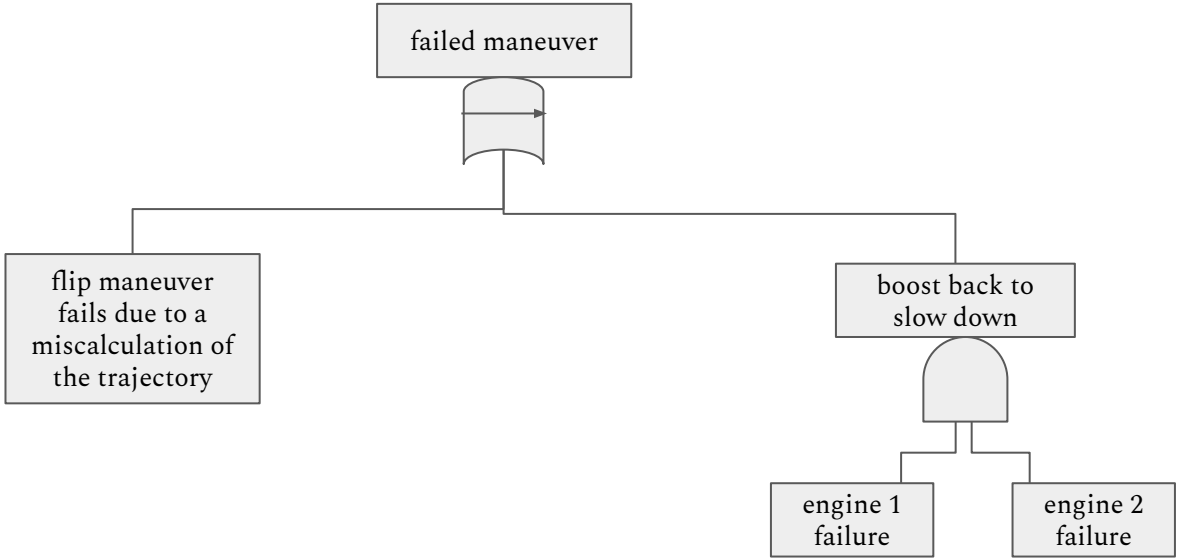
explosion of the Ariane 5 rocket on June 4th, 1996...

... when the guidance system's own computer tried to convert one piece of data—the sideways velocity of the rocket—from a 64-bit format to a 16-bit format. The number was too big, and an overflow error resulted.

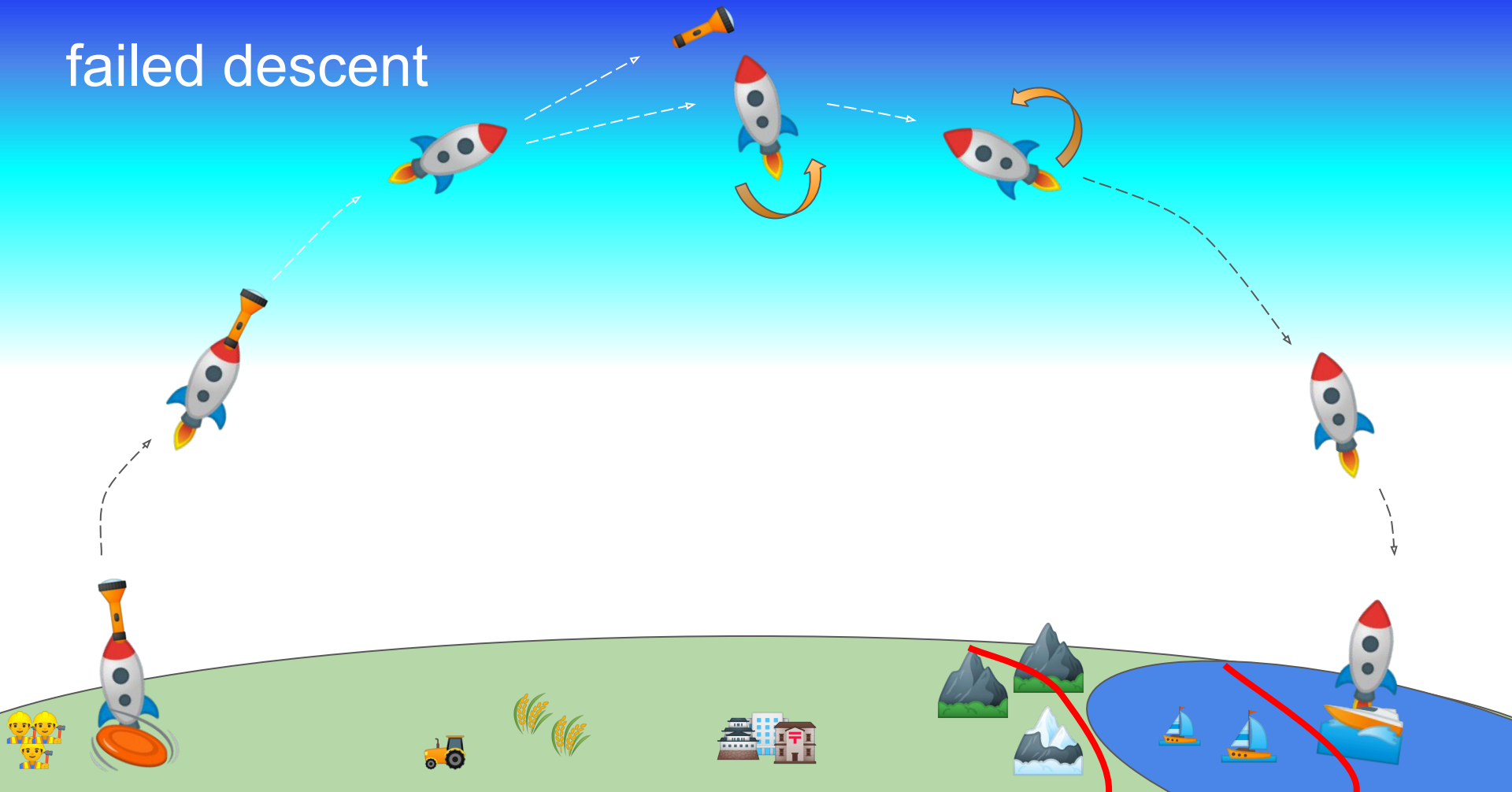
failed reentry maneuver



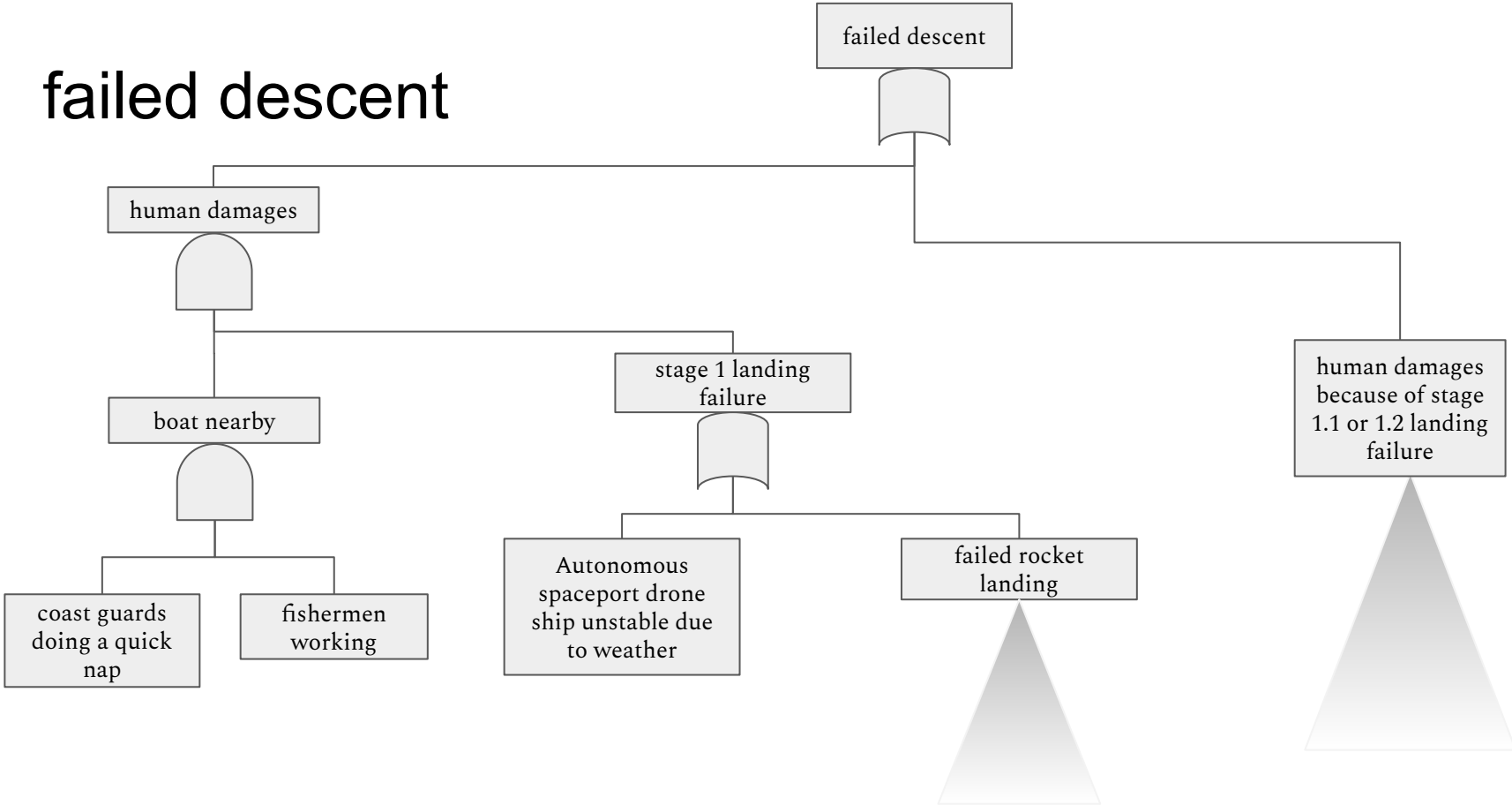
failed reentry maneuver



failed descent



failed descent

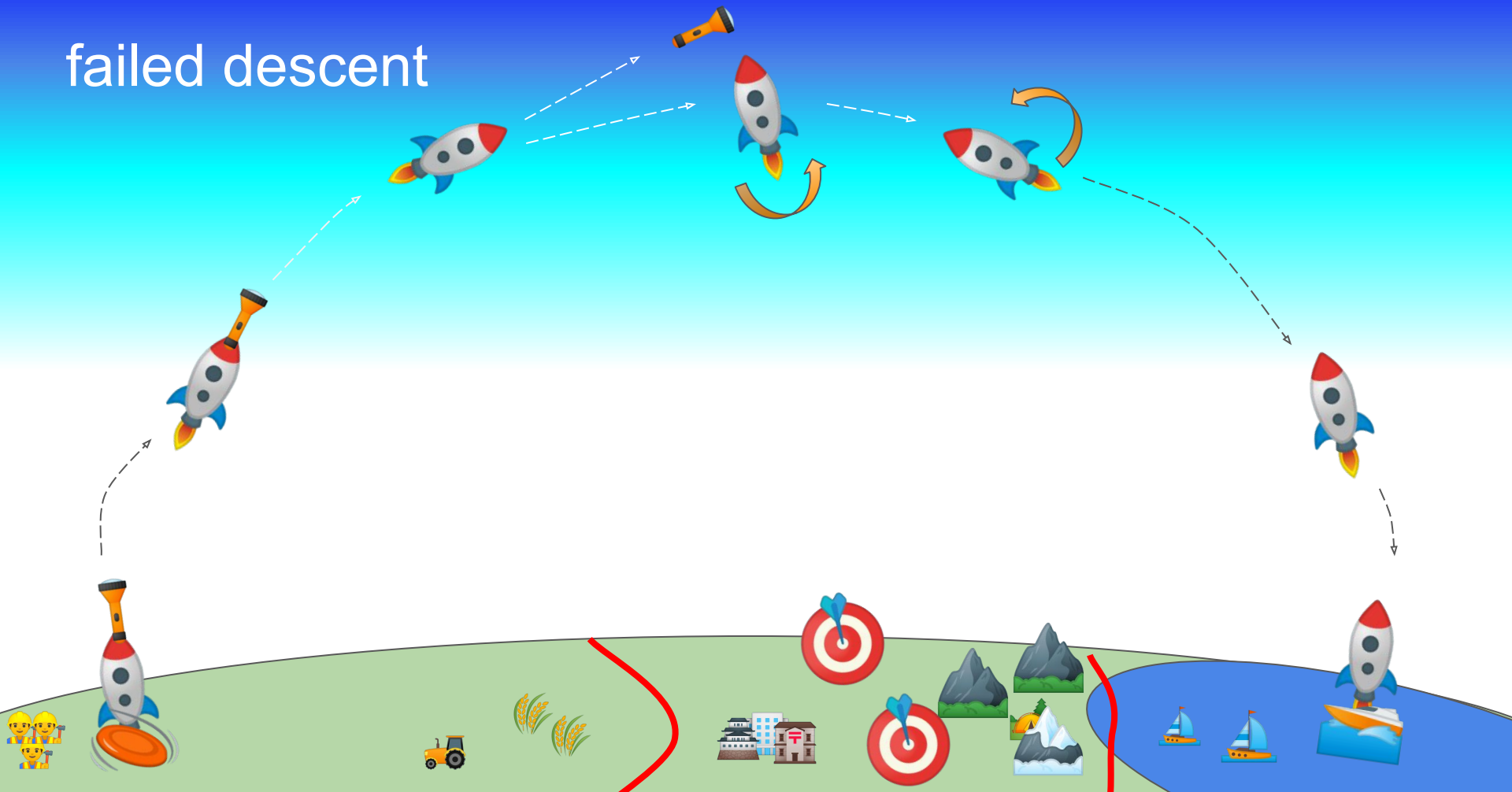


Reassembling sub-trees

Provides flexibility in the design process of fault-trees.

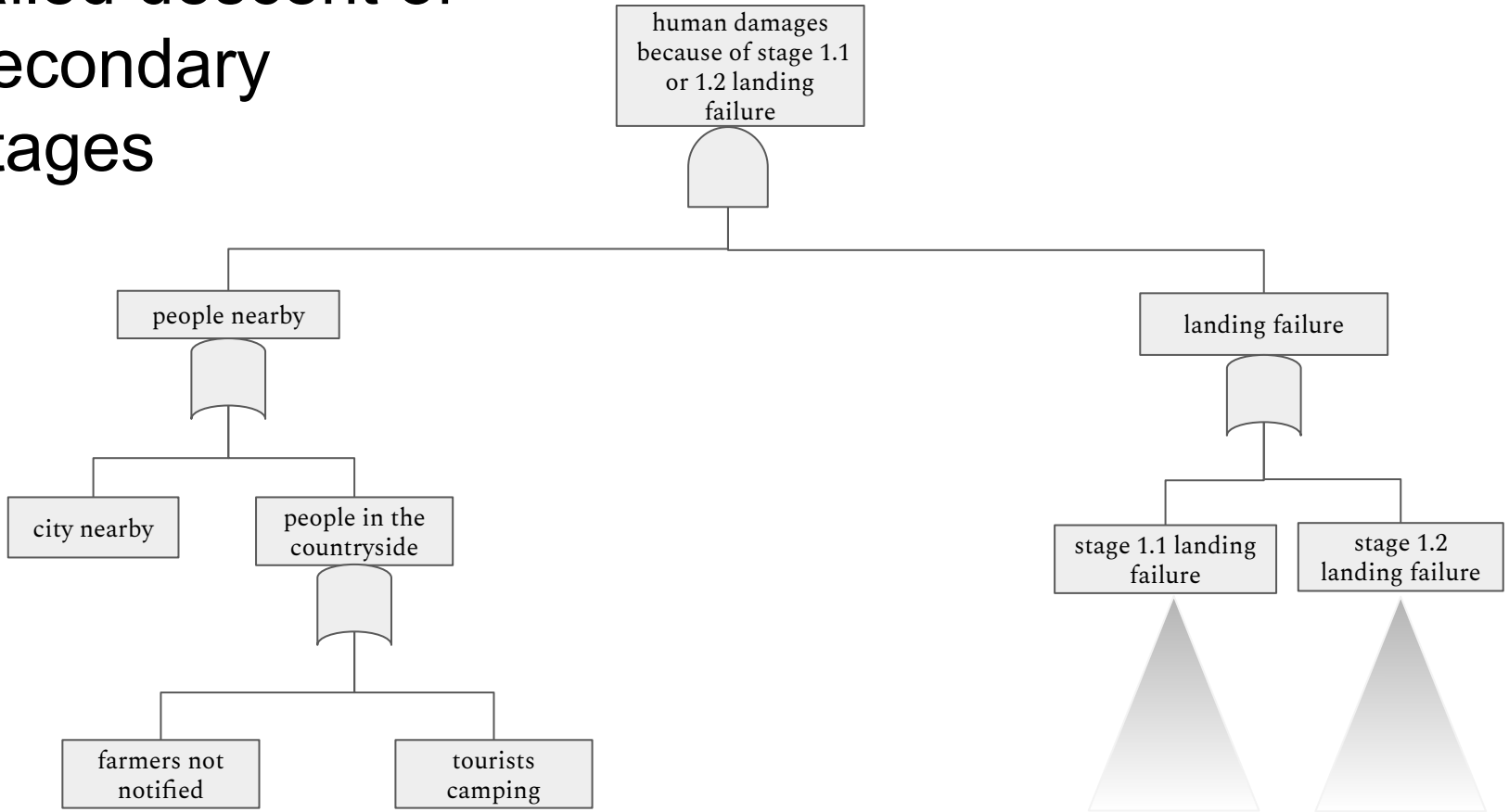
Question: **How does Falcon Heavy compare to Falcon 9?**

failed descent

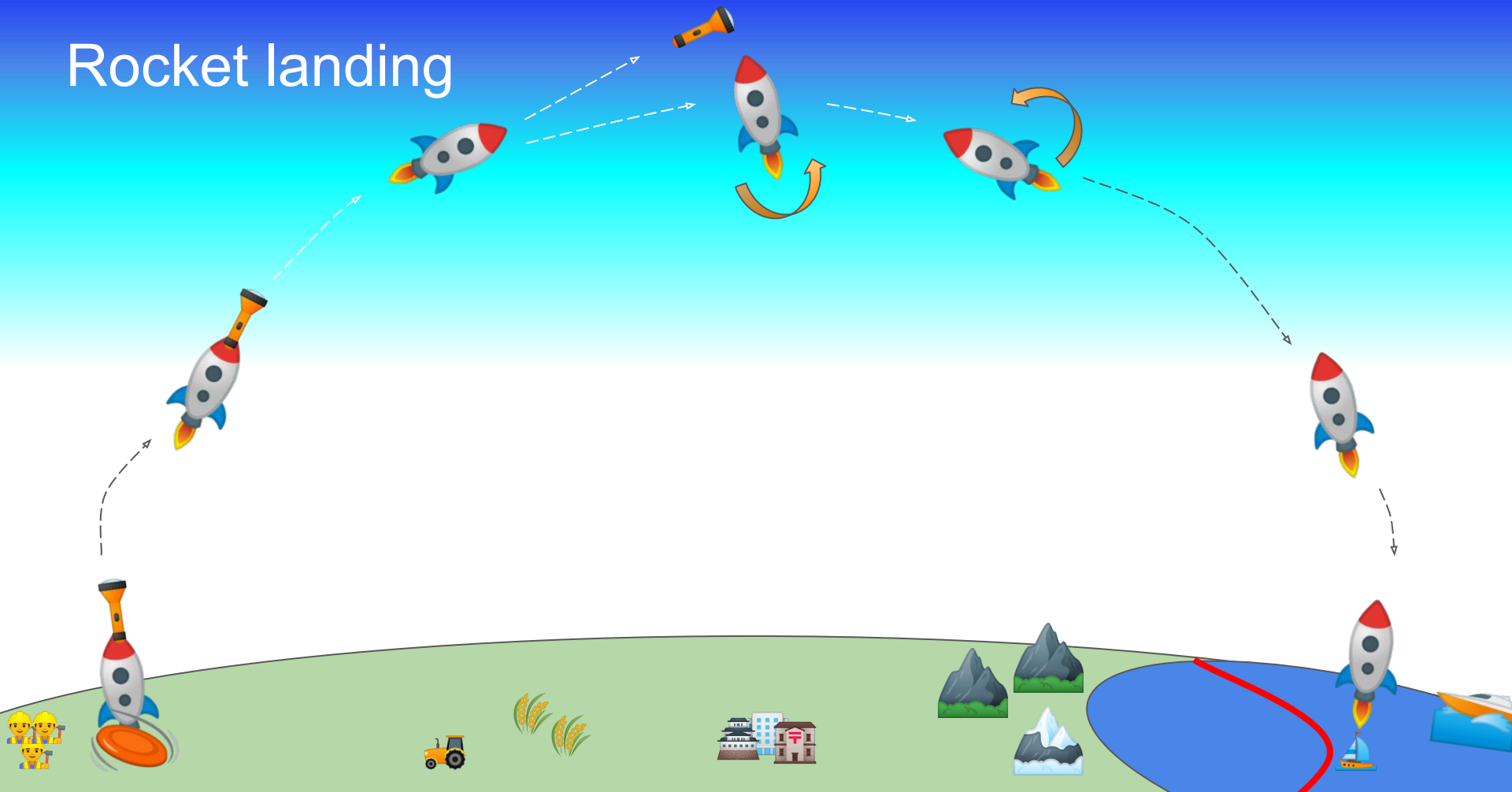


failed descent of secondary stages

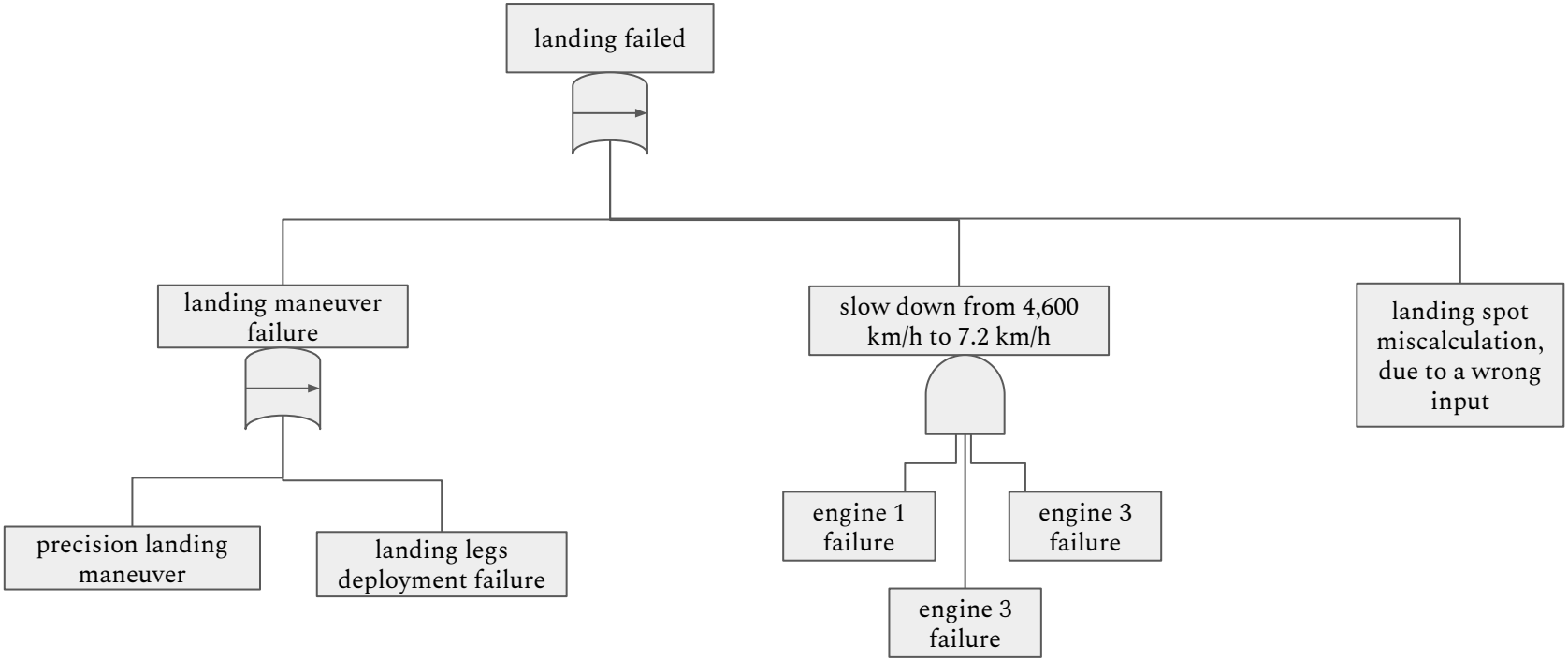
Note that tree for stage 1 **landing failure** may be reused for stages 1.1 and 1.2.



Rocket landing

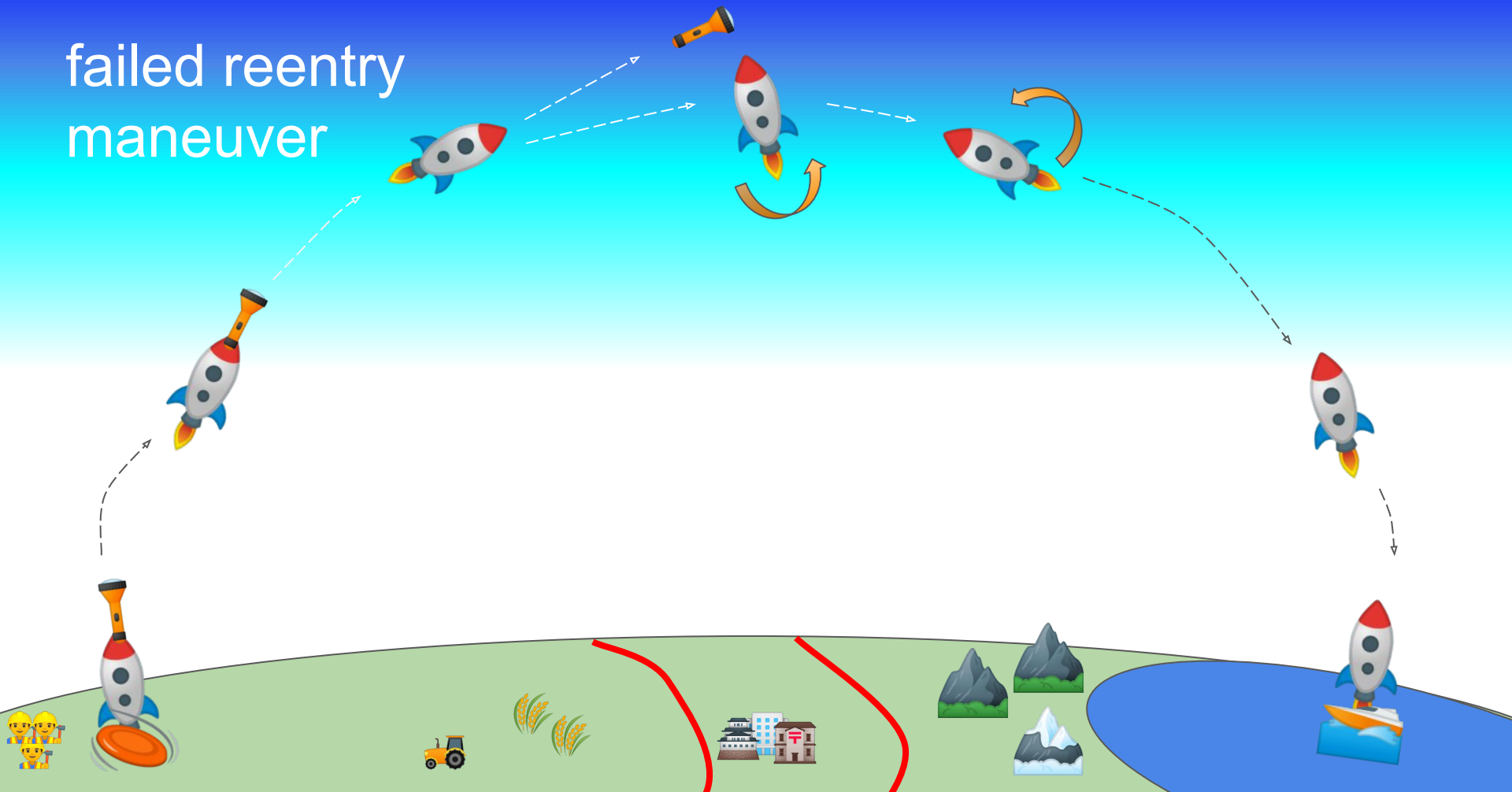


Rocket landing

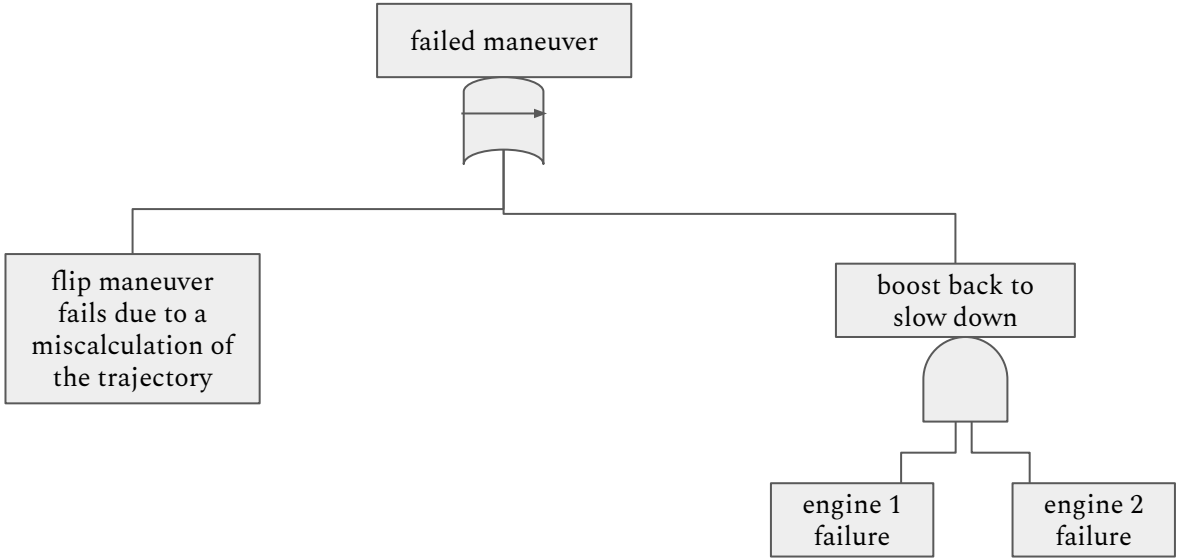


1. fault tree analysis, a powerful technique
2. fault trees 101
3. examples of gates and events
4. Fault tree analysis: a concrete case study
5. Fault trees events: unintended or maliciously provoked
6. Fault tree analysis: what is next?

failed reentry maneuver

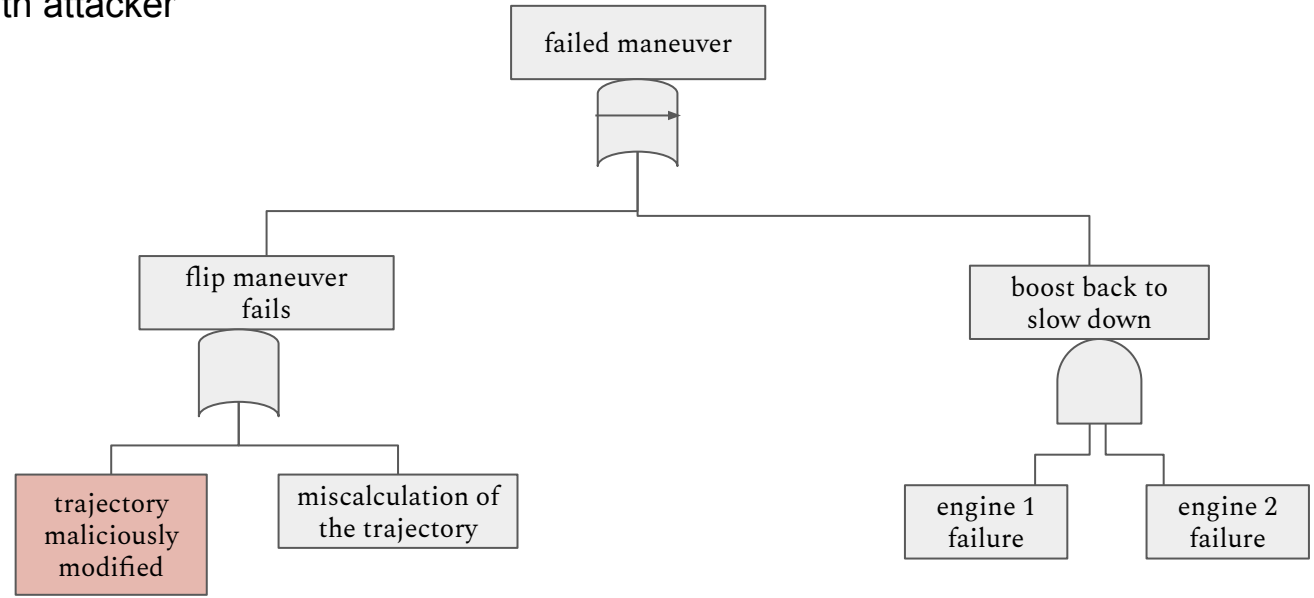


failed reentry maneuver

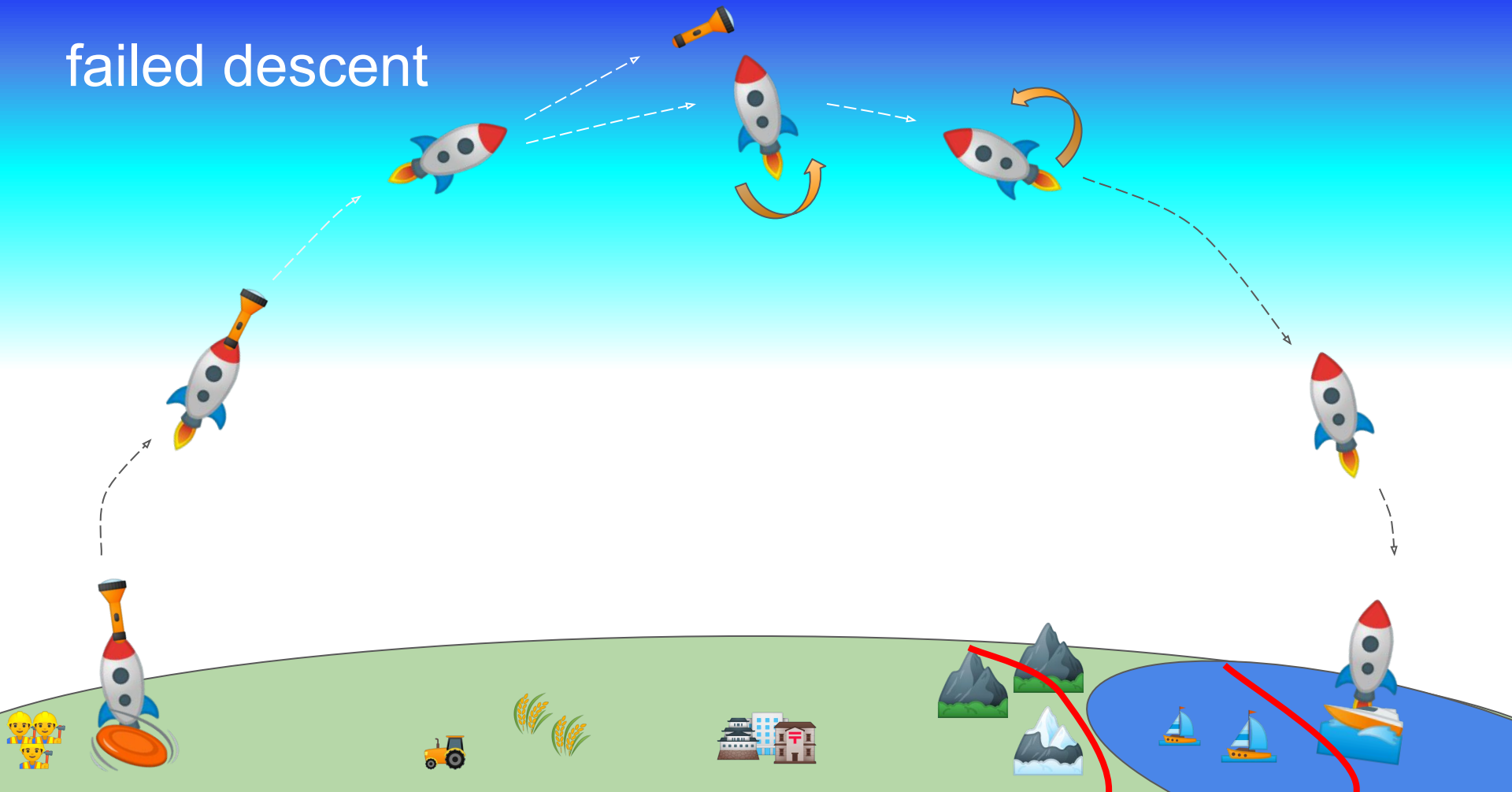


failed reentry maneuver

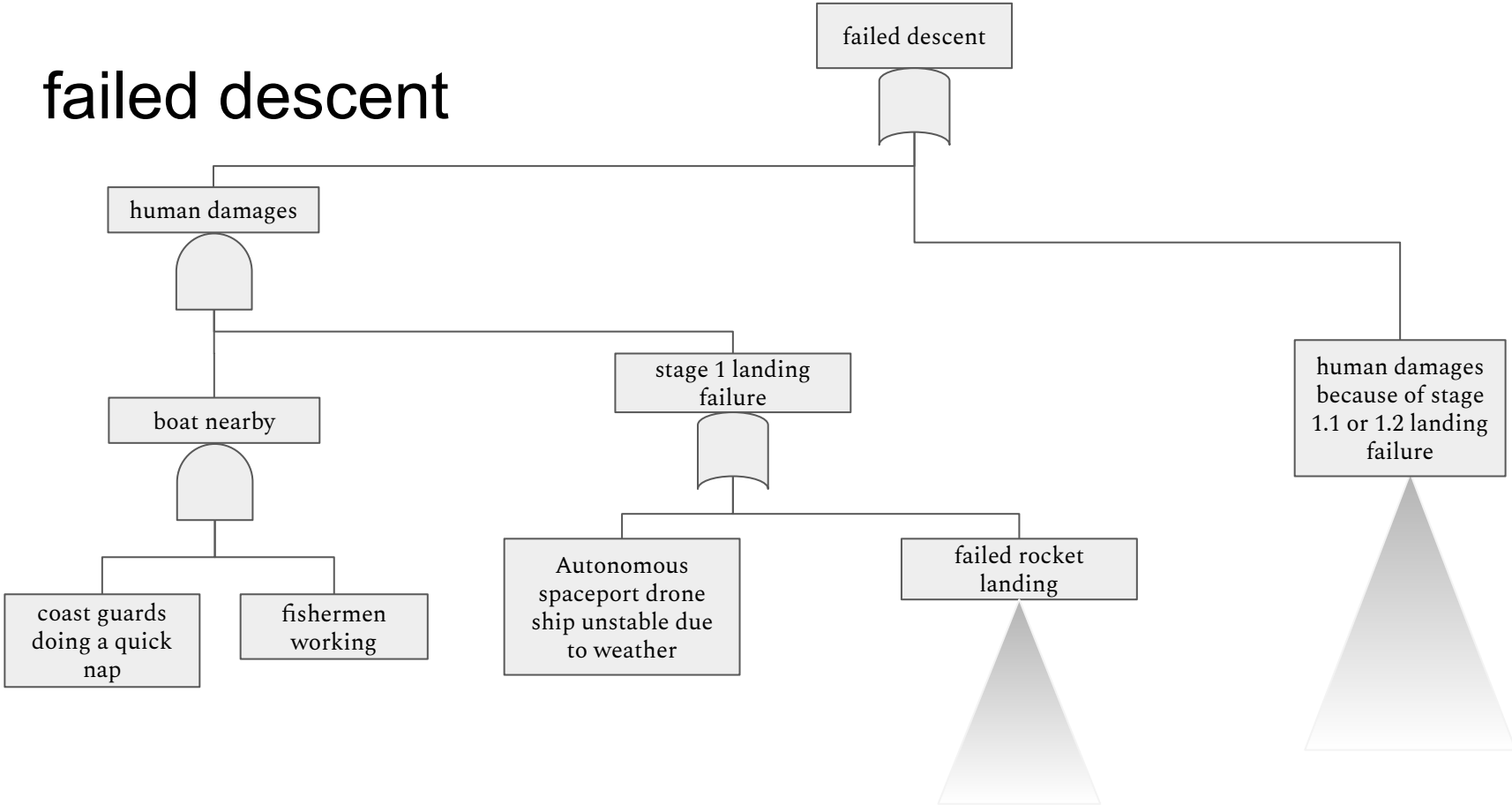
version with attacker



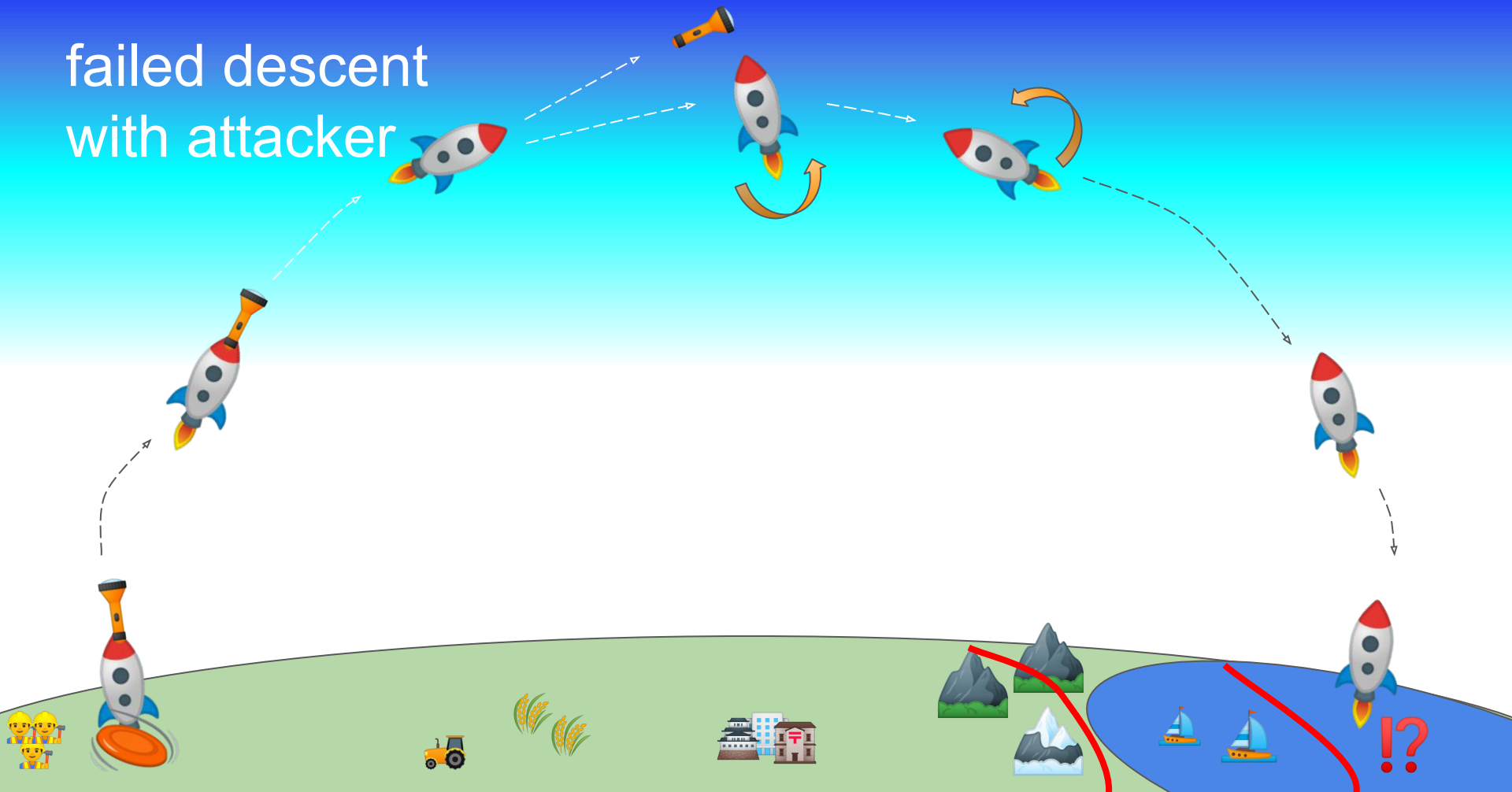
failed descent



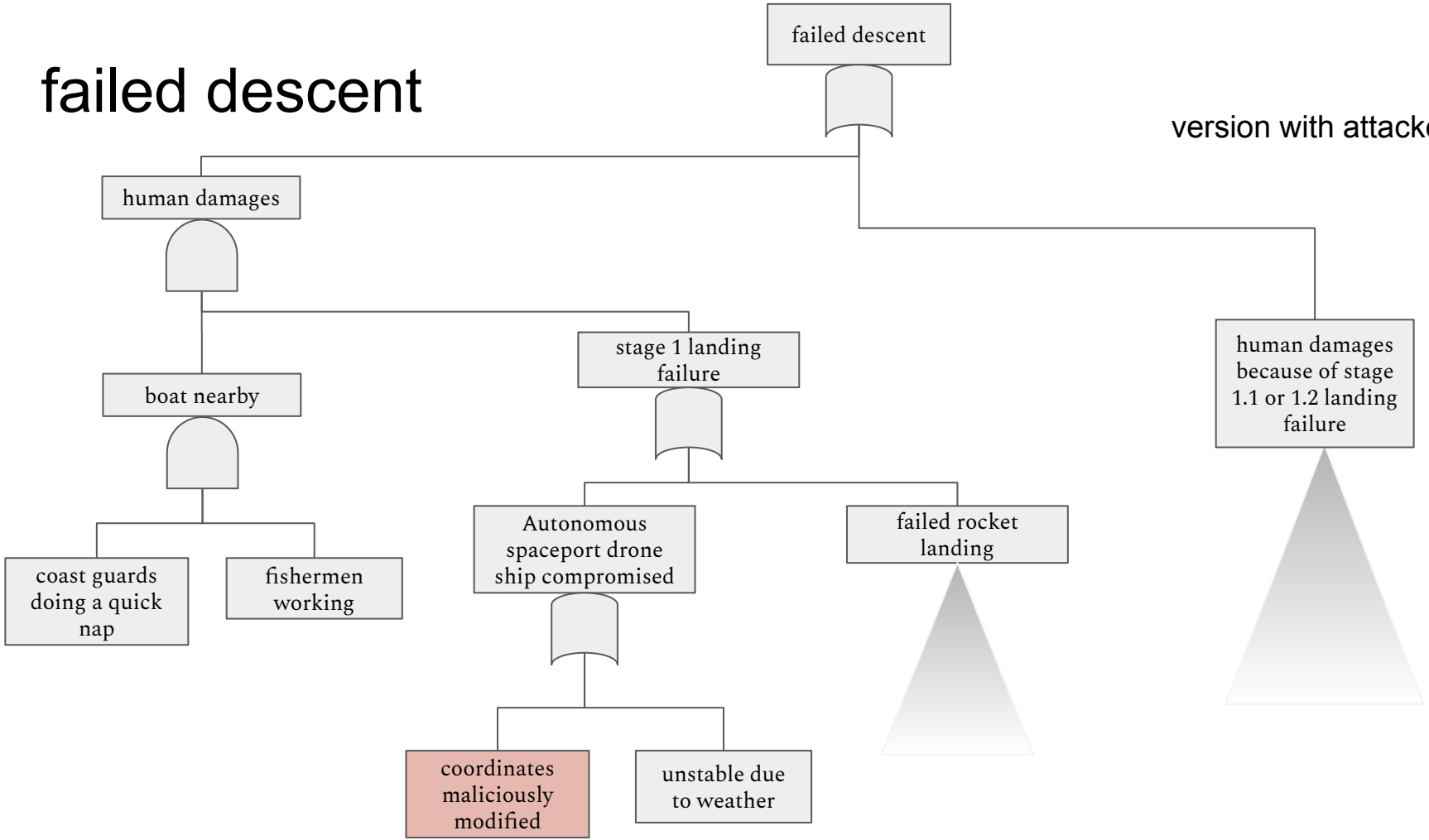
failed descent



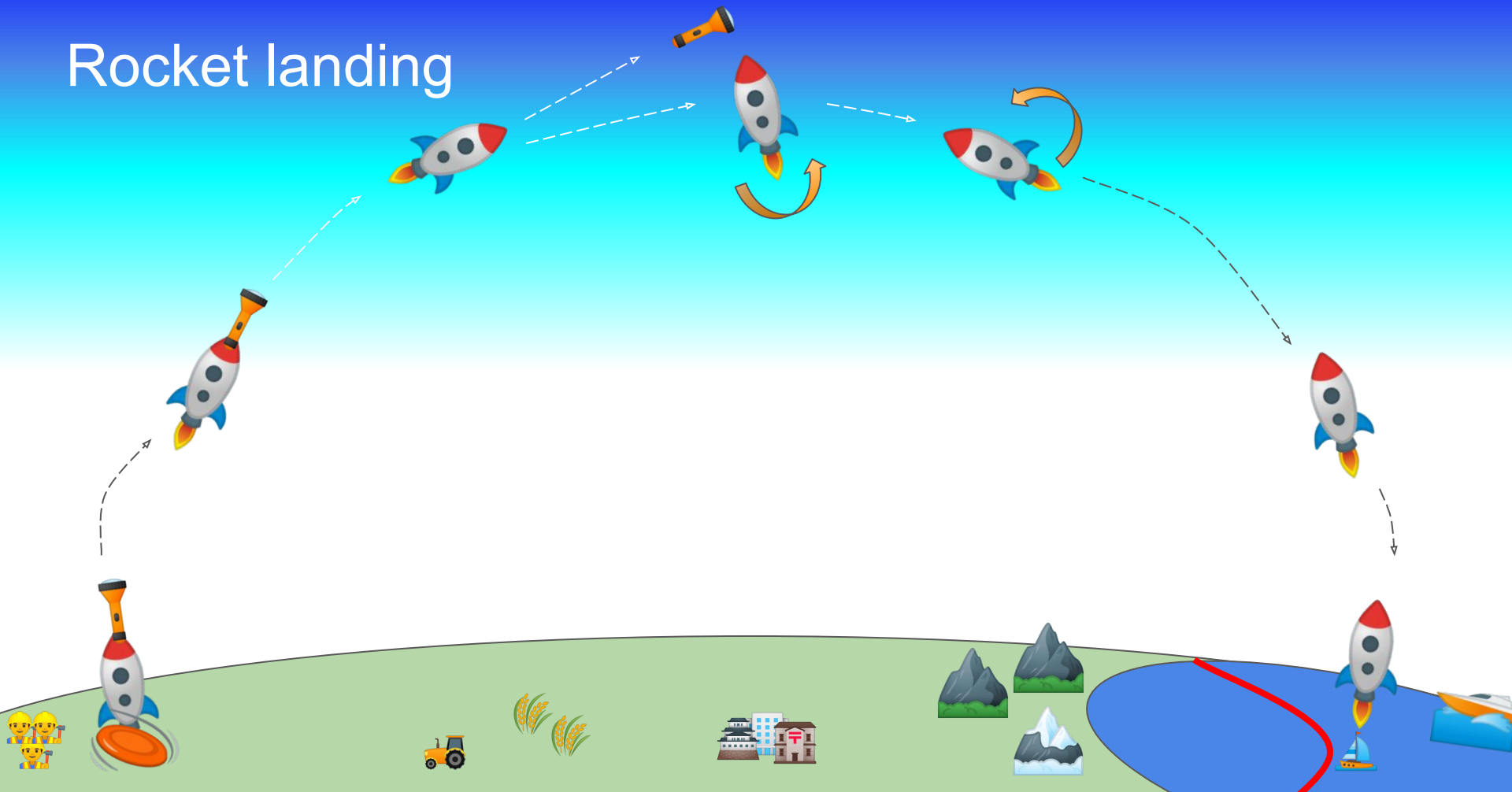
failed descent with attacker



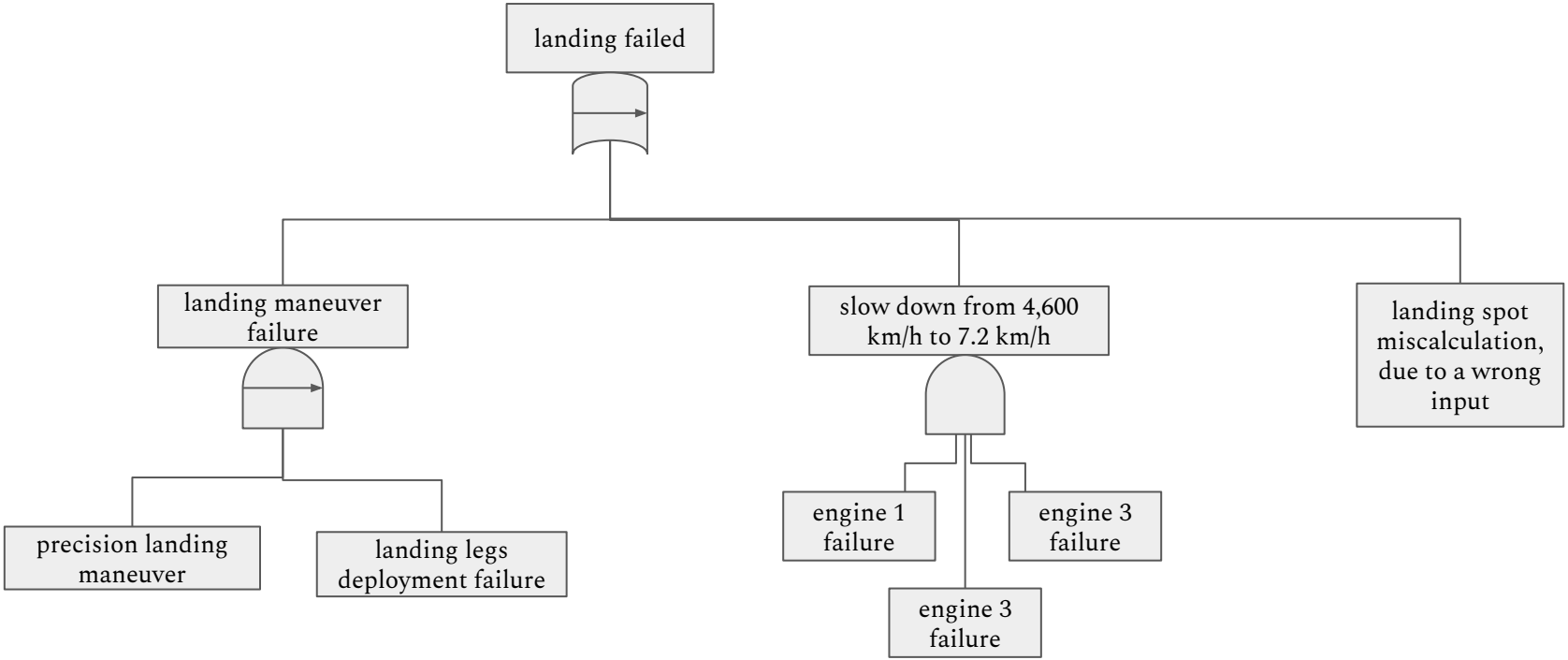
failed descent



Rocket landing

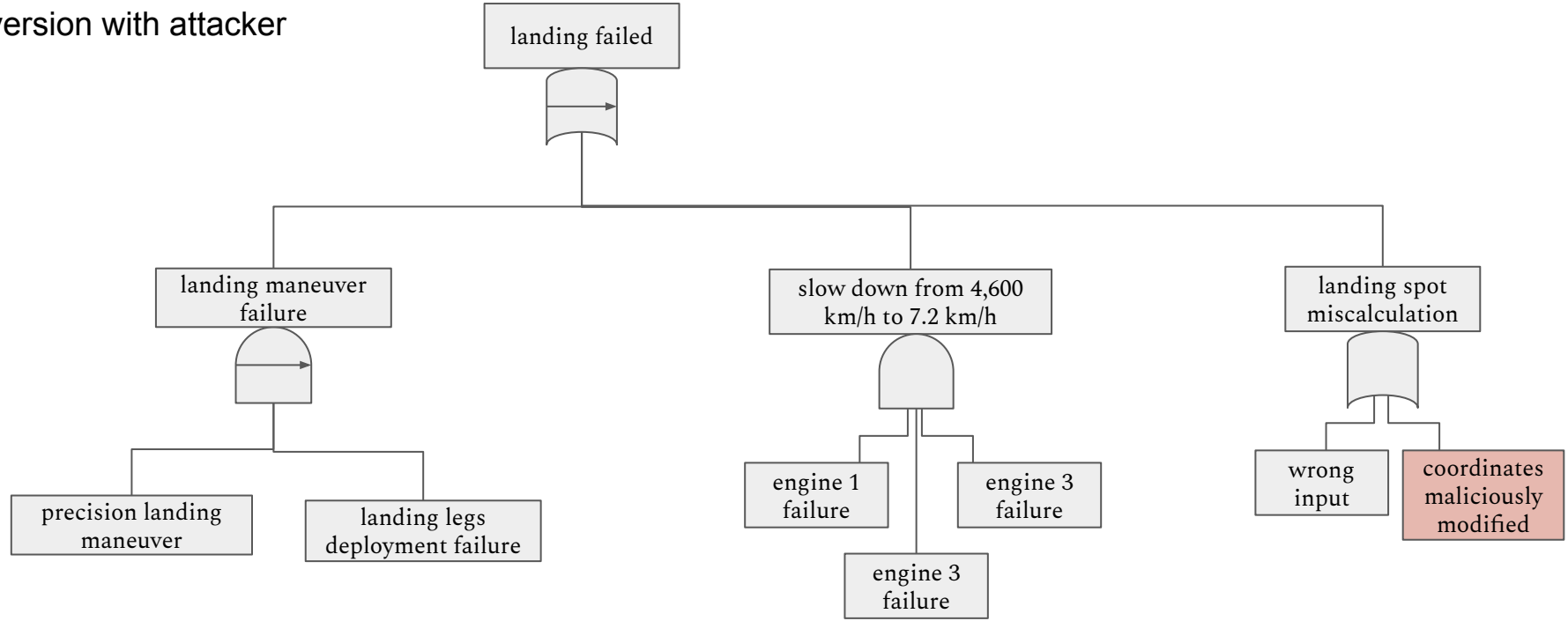


Rocket landing

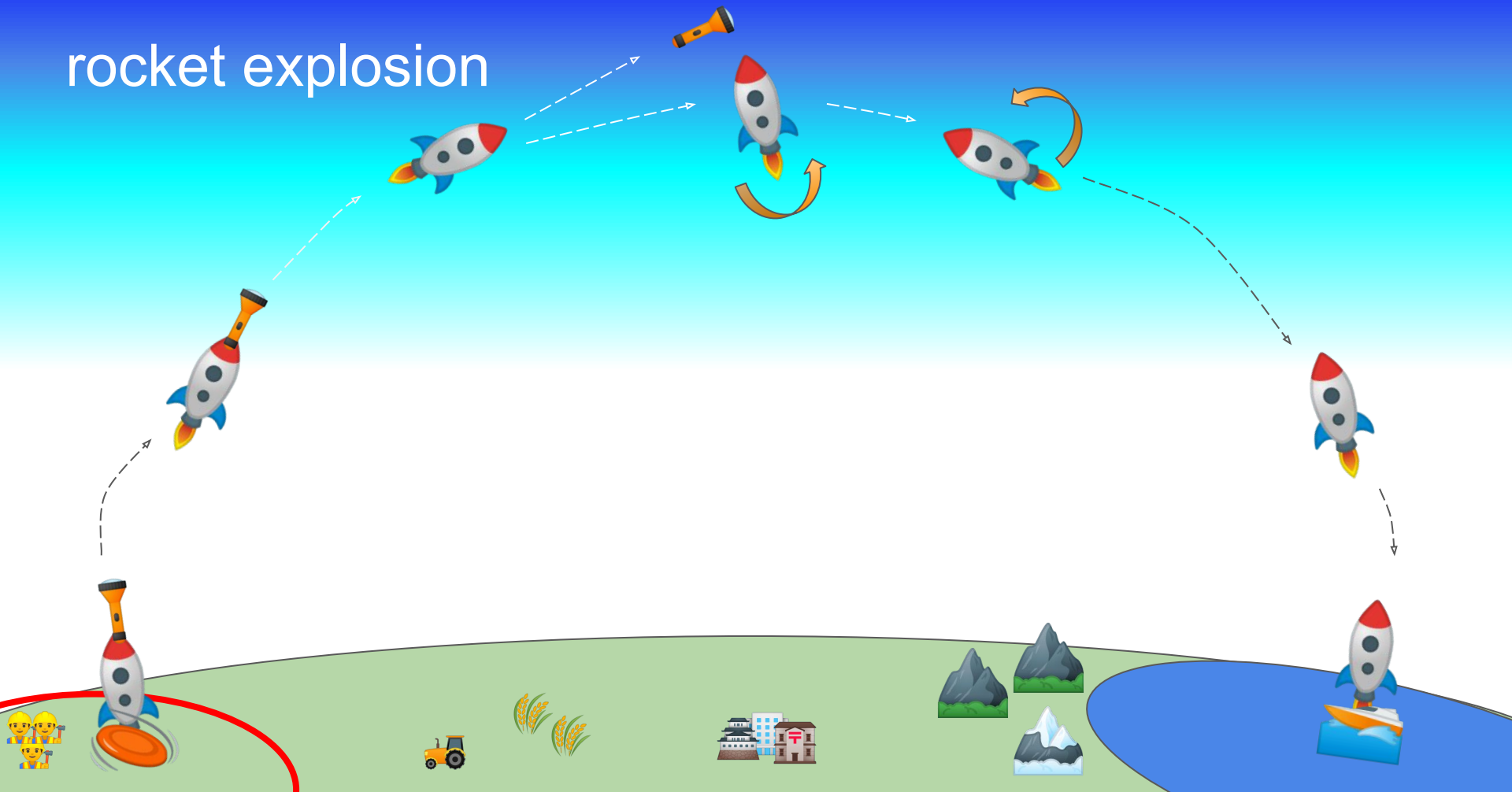


Rocket landing

version with attacker



rocket explosion

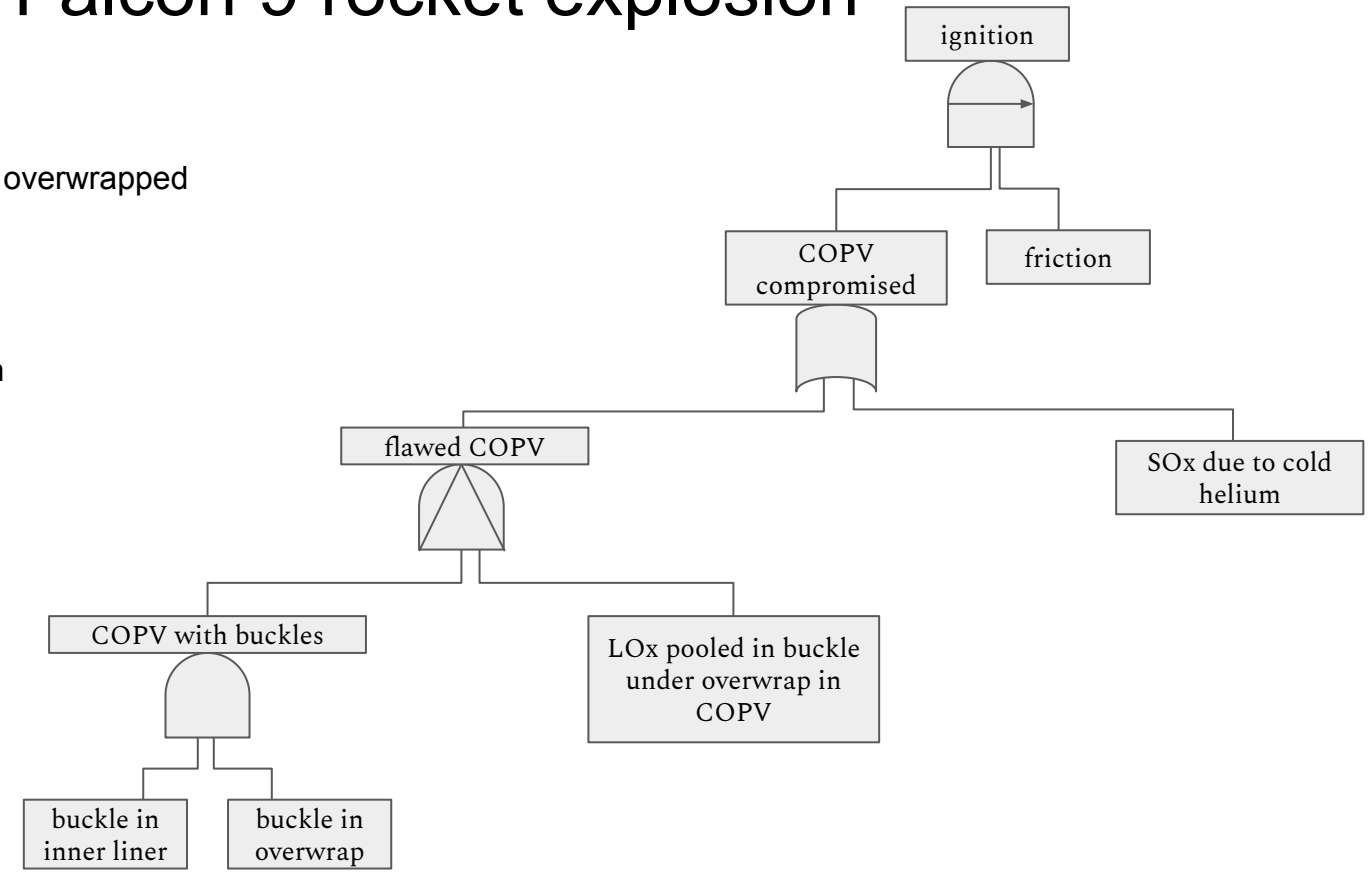


SpaceX Falcon 9 rocket explosion

COPV: composite overwrapped pressure vessel

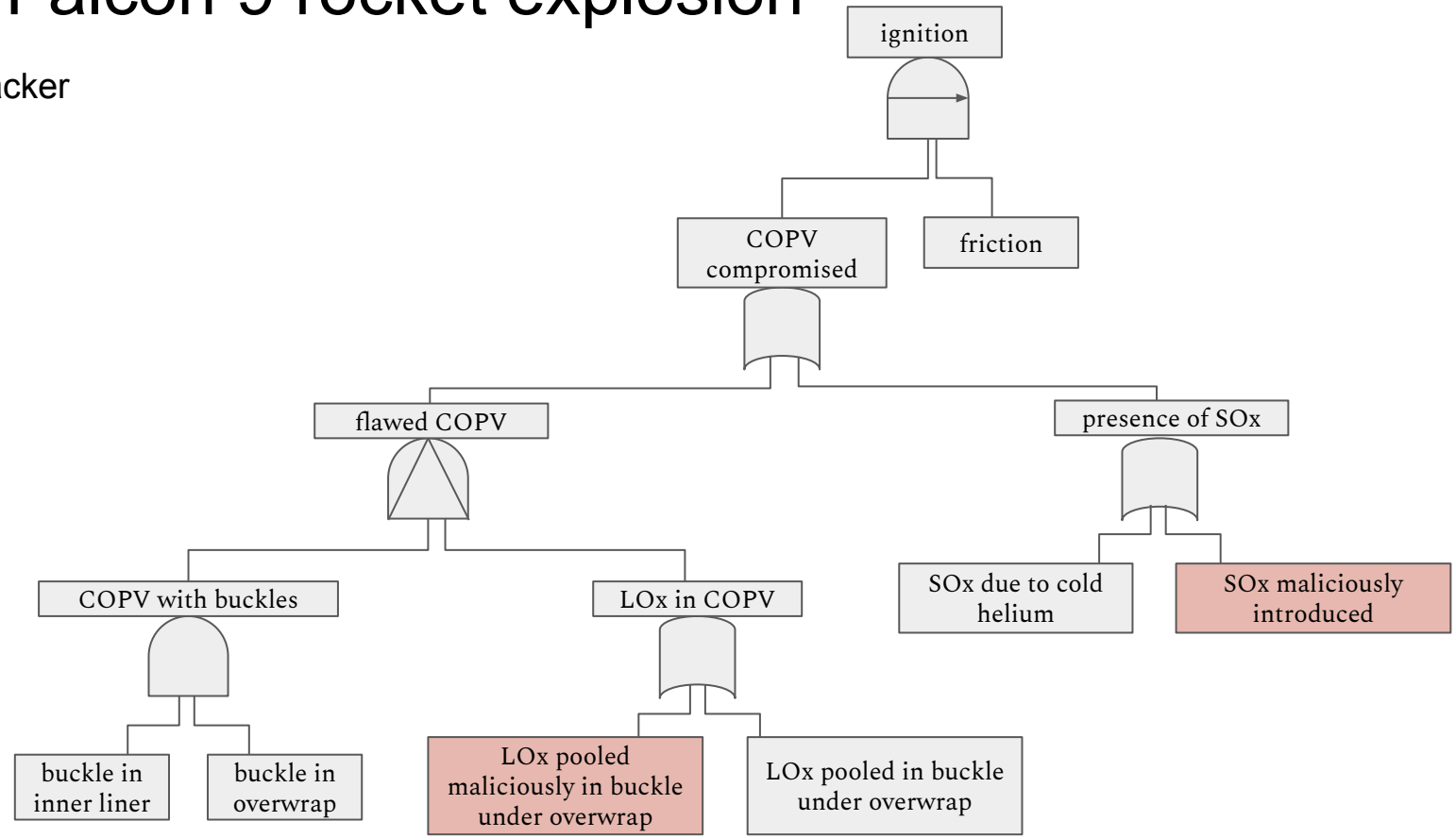
SOx: solid oxygen

LOx: liquid oxygen



SpaceX Falcon 9 rocket explosion

version with attacker



Attackers profiles

enable/disable attacks based on parameters

	no skill	medium skills	highly skilled
no budget			
medium budget			
high budget			

Attackers profiles

enable/disable attacks based on parameters

	no skill	medium skills	highly skilled
no budget			
medium budget			
high budget			

is the attack possible or not?
1 or 0
enable or disable

Attackers profiles

enable/disable attacks based on parameters

	no skill	medium skills	highly skilled
no budget			
medium budget			
high budget			

affects the probability of an attack to be successful

Attackers profiles

enable/disable attacks based on parameters

	no skill	medium skills	highly skilled
no budget			
medium budget			
high budget			

affects parameters defining the success of an attack
e.g. time, cost, damages

1. fault tree analysis, a powerful technique
2. fault trees 101
3. examples of gates and events
4. Fault tree analysis: a concrete case study
5. Fault trees events: unintended or maliciously provoked
6. Fault tree analysis: what comes next?

Problems we can substantiate:

Question: Do Falcon 9 missions pose less of a risk to humans than conventional missions?

Answer: Yes (by the semantics).

Question: But how much so?

Method: Assign sensible probabilities to periodic events,

and enable/disable attacks according to attacker profiles.

Further risk assessment questions.

Risk assessment questions addressed by reassembling sub-trees:

1. damage to 3rd-party property?

2. damage to assets of business (SpaceX)?

3. cost of failing to deliver payload?