Feared Events in the world of Active Debris Removal and In-Orbit Servicing

Robin Biesbroek

24/08/2021

Objective of this presentation

To show you plenty of things that could go wrong in an ADRIOS type of mission….

"….so you can avoid (mitigate) these events by design and requirements

"Think negative……to achieve the positive

Risks

Examples: objective is to get a box safely to a ship, using a truck

Typical requirements related to fastening the box on to the truck, rope security to lift the box on to the ship, etc.

https://www.youtube.com/watch?v=kK11q3Zj4sw

What is a good system?

Needless to say it shall do what it's supposed to do

But a REALLY good system also knows how to handle non-nominal events, failures etc. and even better: unforeseen events

- AOCS (attitude and Orbit Control System) fails and one side facing the Sun for a week, instead of bbq mode
- Landing outside of intended landing ellipse (Apollo 11!)
- Failure during transfer and still able to get humans safely back (Apollo 13!)
- Launcher malfunction and still be able to reach final orbit (ARTEMIS)
- Etc…

So how does this work in reality

Project completely ignores risk and starts to design

- At the end of the design, some risk person is asked to evaluate the risk, make a severity-likelihood matrix etc.

- During final review, risk person points out an issue in the design which could lead to failure under certain conditions

- Project manager says “Oh s*&#”

- Issue is hidden and we build or launch it anyway, or an expensive change happens

Why do we ignore and go on?

Typically: no time and/or budget to solve it

It IS a valid point

On plenty of occasions a possible failure mode is discovered shortly before launch. In many cases, the project decides to launch anyway (with possible adopted operational procedures to minimize the risk of the failure mode to happen)

But: if we had found this mistake earlier on in the project, it is likely we could have solved the issue within the budget

..and this is why we do phase 0 studies in ESA! Sometimes several for one project, as the cost is minimal compared to the total project cost

Example: Exomars

6.3 EDM Failure Root Causes Analysis Summary

The high dynamic phenomenon experienced during the parachute deployment phase was not due to the failure of a specific subsystem or component but rather due to a natural phenomenon caused by a combination of various parameters, which were not properly predicted/expected before flight.

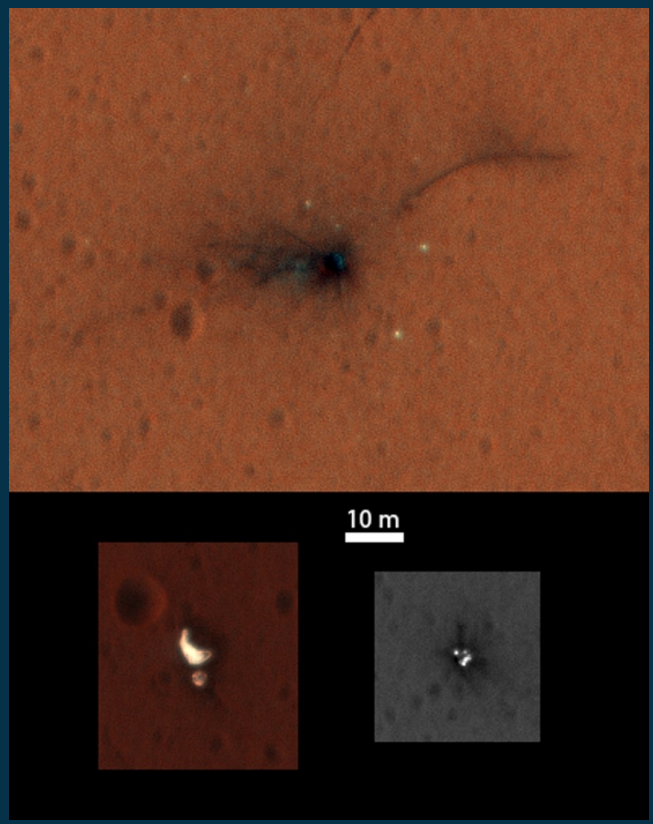
On the basis of the outcome of the investigations performed, the SIB members identified four main root causes that led to the Schiaparelli failure:

- Insufficient conservative modelling of the parachute dynamics which led to expect much lower dynamics than observed in flight;
- Inadequate persistence time of the IMU saturation flag and inadequate handling of IMU saturation by the GNC;
- Insufficient approach to FDIR and design robustness;
- Mishap in management of subcontrac[illegible]nd acceptance of hardware, (the persistence of IMU saturation time was not recorded[illegible]eptance and instead believed to be 15 ms).

Recommendation 02- An overview and verification plan of all sub models and their parameters shall be established.

The main weakness of the adopted decision logic was the fact that the FDIR focussed on RDA failures. Insufficient general "what if" analysis and Worst Case analysis were performed for the characterization of this critical phase. The fact that the system was Zero Failure Tolerant does not justify an over simplistic approach with no possibility of recovery from anomalies (even with degraded performance). In particular, partially redundant data were available on board.

EXOMARS 2016 - Schiaparelli Anomaly Inquiry
Reference: DG-I/2017/546/TTN
Date 18/05/2017 Issue 1 Rev 0
Page 21



Start designing well!

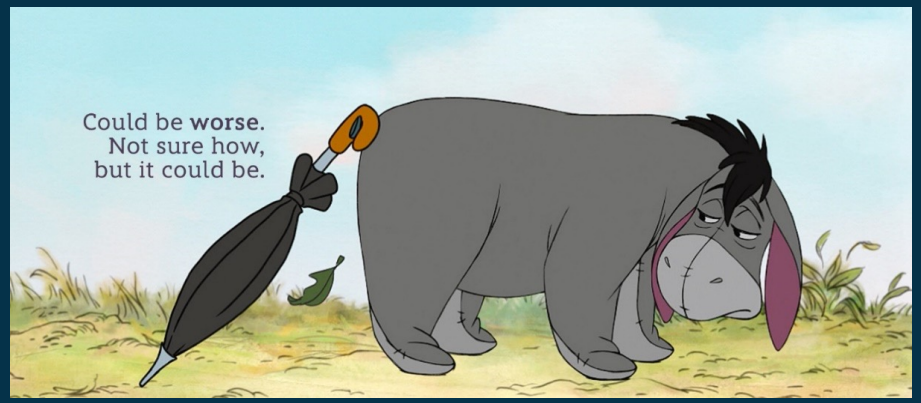
Start evaluating the challenges of the design / the mission right from the beginning. Think ‘what if?’

Don’t do it alone; have it reviewed, do it concurrently

- Plenty of tools to help you, such as the CFDA (Catalogue of Failure Data for Safety and Dependability Analysis)

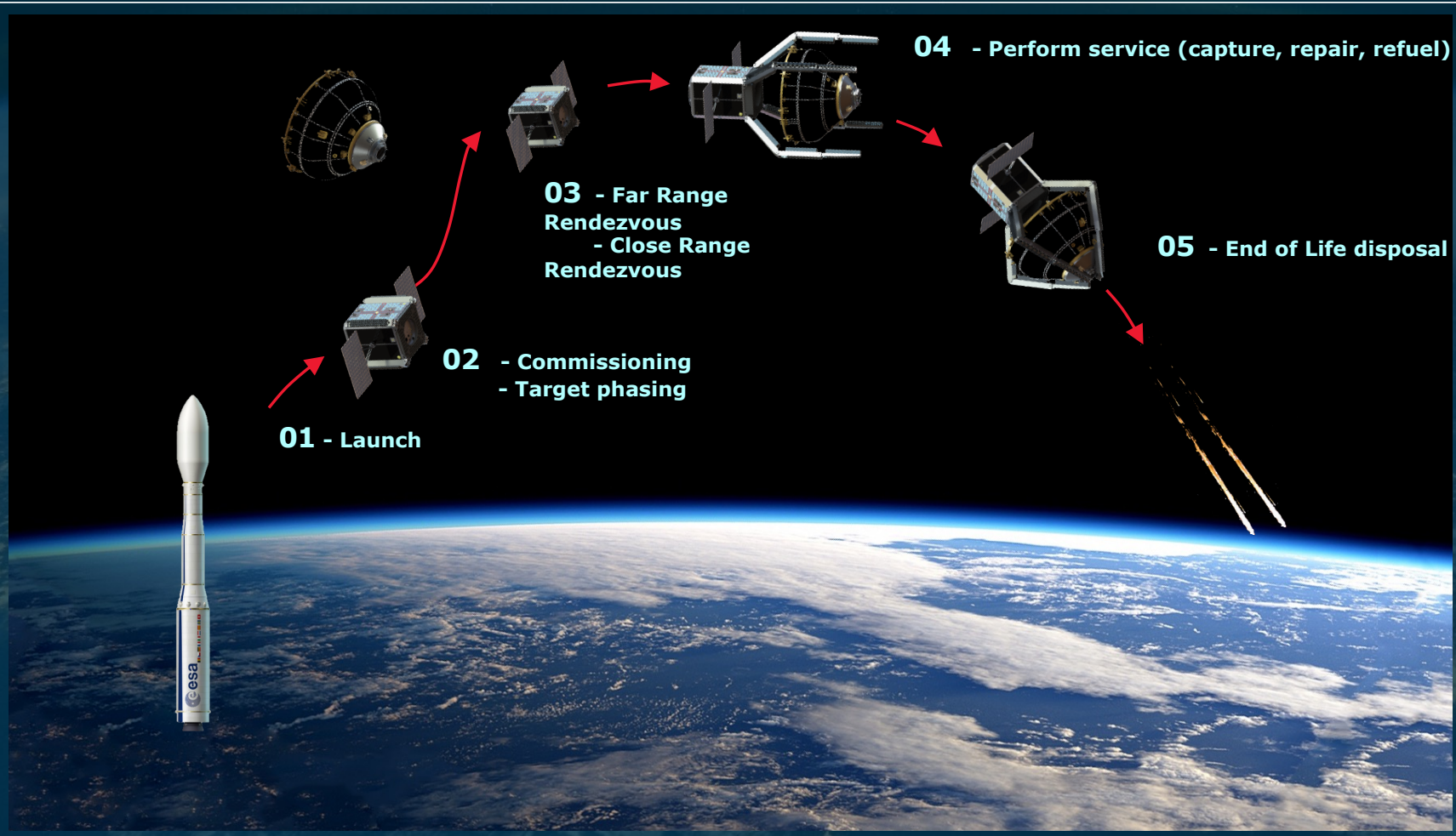
We hate people that sound pessimistic

We prefer to ignore them



But let’s take it positively, and ensure that “what if this or that fails?” are risks that are mitigated during the design.

Simple CONOPS (= how e.g. a space segment is used)



Launch feared events

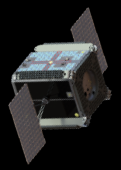
Typically no different from other types of mission

What if untimely deployment of capture system?
(e.g. net)

Large capture/docking service may lead to tanks mounted 90° w.r.t. launch direction -> vibration loads different than 'usual'

01 - Launch

Commissioning and phasing feared events



02 - Commissioning
- Target phasing

LEOP typically no different from other types of mission

During commissioning several capture and GNC systems could be tested, e.g. deployment of robot arm, robot arm connects to drill stored on the spacecraft, etc.

What if capture or service device does not deploy or correctly retracts?

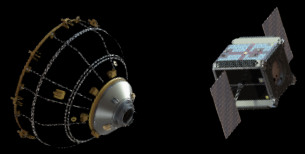
What if any of the (close proximity) sensors fail?

What if any service device (screwdriver, claw etc.) cannot be captured by the arm?

How can we test anything related to confirmation of successful capture

Phasing: what if we share a launch and the launcher leaves the servicer in an orbit plane quite different from the target's orbit plane?

Close approach feared events

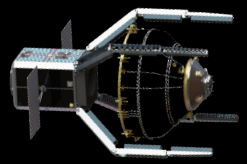


03 - Far Range Rendezvous
- Close Range Rendezvous

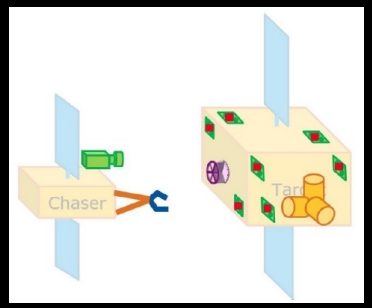
In case of uncontrolled target: what if the motion of the target is different than predicted (e.g. faster rotation?)
What if the colour of the target is different from simulations/tests?
What if there is a OBC reset/failure during close approach?
What if there is a safe mode in a hold point and no recovery for a long time (e.g. one week)? Collision possible?
What if the target state is not as predicted? (e.g. loose cables?)
What if target is blocking communications line of sight?
What if RF interference between target and servicer?

In all cases…collision and possible creation of extra debris needs to be avoided!

Service feared events



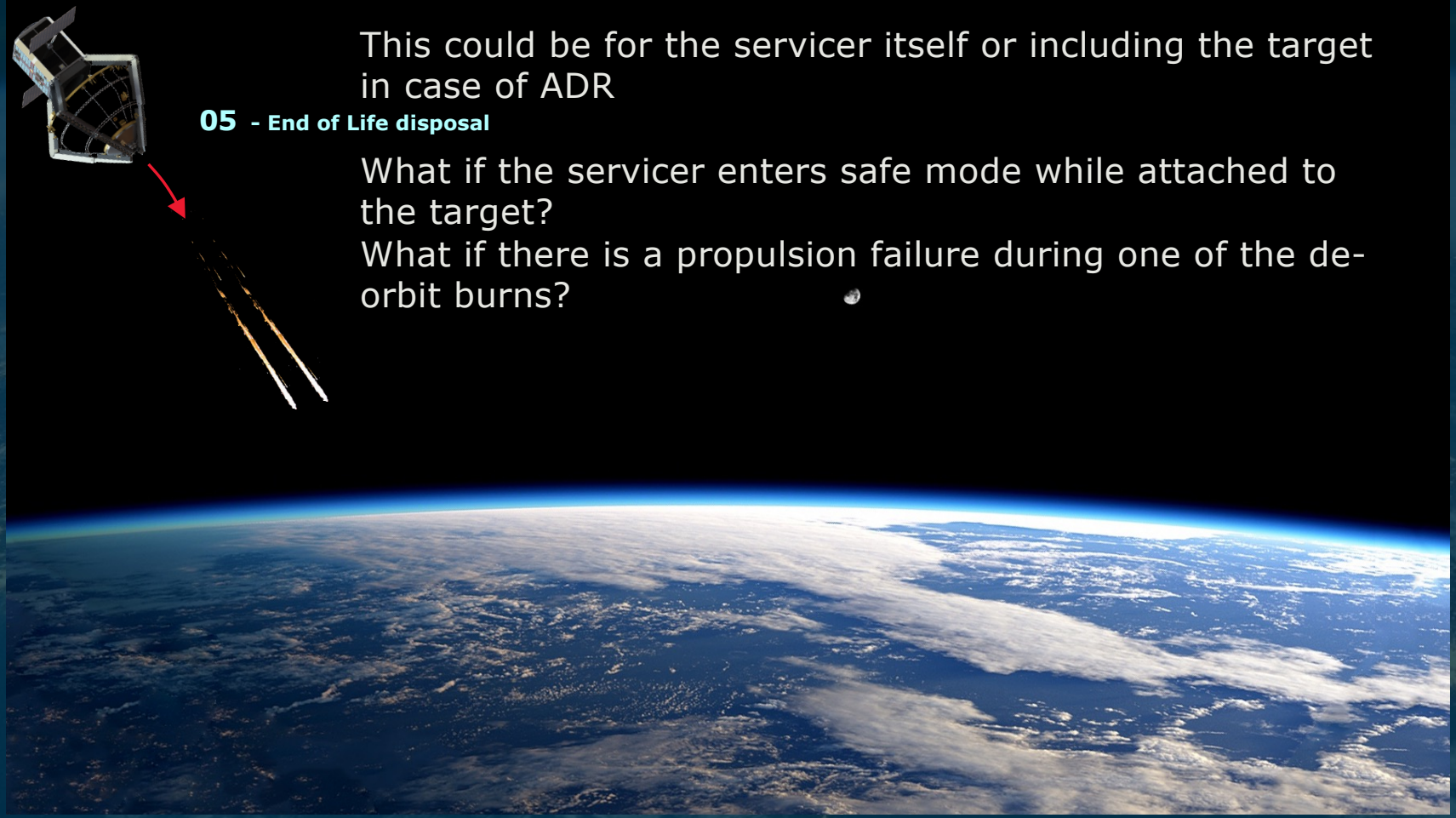
04 - Perform service (capture, repair, refuel)



Strongly dependent on service types but some examples:

What if no confirmation on capture/docking/berthing?
What if uncontrolled shocks are too large for mechanisms to withstand?
What if continuous fatigue too large for the capture/berthing interface?
What if there is a hand-over of ground-station during capture/berthing?
What if an item breaks off?
What if simulations of touching the target and/or post-capture stabilisation are different from real life?
What if there is a failure in the capture/berthing system?
What if plume impingement on target?
What if sensors to detect separation fail?
What if the separation fails?

End of life feared events



05 - End of Life disposal

This could be for the servicer itself or including the target in case of ADR

What if the servicer enters safe mode while attached to the target?

What if there is a propulsion failure during one of the de-orbit burns?

Plenty of mitigations

Fail safe trajectories

Design for some CAM's

Time operations well (G/S, light conditions)

Design with large margins (target not entirely the same as in simulations, colours different, motion different, etc.)

Extra mechanism to obtain 'firm' grip?

Thruster layout avoiding plume impingement

Requirements on maximum collision impact (but how to verify?)

Redundant control

Etc.

Etc.

Bottom line

Some examples were given here in ‘cowboy style’ (eventually compliance with ECSS is recommended!)

Many more exist..

Start designing well!

Flip through each function in the spacecraft and ask what can go wrong

Find solutions to mitigate the risk and link requirements to force the solution into that direction

Do this early in the project design phase!