18th International Conference on Space Operations, Montreal, Canada, 26 - 30 May 2025.

SpaceOps-2025, ID # 360

Expect the best, plan for the worst: the Stop OCM Burn FDIR implementation during Copernicus Sentinel-1B de-orbit campaign

P. Sintes Arroyo[a*], C. Gison[b], A. L. O'Connell[c]

[a] Sentinel-1 Flight Control Team, Copernicus Operations Support Services (COP-2) for ESA, Serco Services GmbH, Lise-Meitner-Straße 10, 64293 Darmstadt, Germany, pol.sintes@serco-eu.com
[b] Sentinel-1 Flight Control Team, Copernicus Operations Support Services (COP-2) for ESA, Serco Services GmbH, Lise-Meitner-Straße 10, 64293 Darmstadt, Germany, camilla.gison@serco-eu.com
[c] Sentinel-1 Flight Control Team (OPS-OEN), ESA-European Space Operations Center, Robert-Bosch-Straße 5, 64293 Darmstadt, Germany, Alistair.O'Connell@esa.int
[*] Corresponding Author

Abstract

The Sentinel-1B de-orbiting campaign represented a first for the Copernicus family of satellites when it comes to End of Life (EOL) operations. To deal with the uncertainties such a long and demanding campaign entailed, the Flight Control Team (FCT) at ESOC assessed the feasibility of interrupting an Orbit Control Manoeuvre (OCM) burn based on Reaction Wheel (RW) Speeds and/or Tank Pressure readings due to the potential loss of S/C attitude control during the fuel depletion phase. However, in the de-orbiting phase, after a RW overspeed triggered a Safe Mode during an OCM burn, it was realized that based on the approach for the fuel depletion phase, the preliminary FDIR design could potentially be adapted to stop an ongoing OCM burn sequence for this phase too and prevent further entry to Safe Mode in similar anomaly cases, especially in OCMs where multiple thrusters are operated in open loop and thrust imbalance may occur.

This paper describes the design and validation steps that led to the safe and robust implementation of this FDIR (Fault Detection, Isolation and Recovery) on Sentinel-1B and presents the results and operational benefits obtained by this approach for potential use in other missions: its application proved to be effective to minimize satellite outages and recovery times during the Sentinel-1B de-orbiting and will be re-used for other Sentinel-1 spacecraft during critical mission phases such as deorbiting or commissioning, but may also be applied during routine operations to reduce or completely avoid loss of payload operations, thus maximising the science data return.

Keywords: Sentinel-1, de-orbiting, FDIR, Manoeuvre

Acronyms/Abbreviations

ARB	=	Anomaly Review Board
ASW	=	Avionics Software (ASW)
CAM	=	Collision Avoidance Manoeuvre
COP-2	=	Copernicus FOS Operations Support Service Contract
C-SAR	=	C-Band Synthetic Aperture Radar
EAS	=	Event Action Service
EOL	=	End of Life
ESA	=	European Space Agency
ESOC	=	European Space Operations Centre
FCT	=	Flight Control Team
FDIR	=	Fault, Detection, Isolation and Recovery
HK	=	Housekeeping
IP	=	In-Plane
MDS	=	Monitoring Data Set
MI	=	Monitoring Item
OBCP	=	On-board Control Procedure
OCM	=	Orbit Control Manoeuvre
OMS	=	On-board Monitoring Service
OOP	=	Out-of-Plane

PUS	=	Packet Utilisation Standard
RCT	=	Reaction Control Thruster
RW	=	Reaction Wheel
S/C	=	Spacecraft
SOM	=	Spacecraft Operations Manager
SOE	=	Spacecraft Operations Engineer
SSID	=	Sub-Schedule Identifier
TPF	=	Task Parameter File
USM	=	Ultimate Safe Mode

1. Background

Sentinel-1B was launched on 25 April 2016 as the second satellite of the Sentinel-1 constellation, the first of the European Union's Copernicus Sentinels program, operated by ESA on behalf of the European Union and funded by the European Union and ESA.

For more than five years, it produced valuable high-resolution radar images used across a wide range of applications. However, on 23 December 2021, a major failure in the Platform power supply to the C-SAR Instrument unexpectedly terminated the mission before its planned end date [1].

Following several unsuccessful attempts to restore power to the satellite's payload, ESA declared the mission finished on 3 August 2022. At the same time, since the satellite's platform operational capabilities were unaffected by the power failure, ESA and Industry began preparing for its controlled de-orbit and passivation [2]. This de-orbit was the first such end-of-life operation of the Copernicus program and will serve as a reference for future de-orbit campaigns.

The de-orbiting campaign planning commenced immediately after the mission was declared finished, aiming at lowering the Spacecraft (S/C) 's altitude as much as possible following the latest (at the time) ESA Space Debris Mitigation [3] guidelines.

1.1 Sentinel -1B Propulsion System

The de-orbit plan was devised to utilize the Sentinel-1B propulsion system in a smart and innovative way. To give context, the Sentinel-1B propulsion system (see Figure 1) consists of two redundant branches, each with seven 1 Newton RCTs:

- RCT 1 – In-Plane retrograde manoeuvres (lowering the orbit)
- RCT 2 – In-Plane prograde manoeuvres (raising the orbit)
- RCT 3 – Out-of-Plane manoeuvres (orbit inclination correction)
- RCT 4, 5, 6, 7 – Attitude control after launcher separation and in Safe Mode

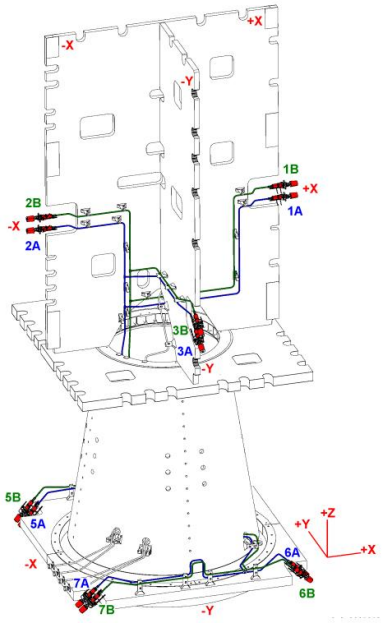


Fig 1. Sentinel-1B RCT configuration

The plan was devised to utilize the four RCTs located on the -Z panel (RCTs 4, 5, 6, and 7), previously used

only for attitude control during the initial post-launch phase or in USM - a last-resort mode activated in case of major anomalies, relying on separate onboard hardware and software.

These RCTs were selected because the usual IP thrusters (RCT 1 and 2 main and redundant) used for orbit maintenance could only be fired one at a time and the achievable Delta-V was severely limited due to thrust plume impingement [4]. ESA's goal was to complete the de-orbit campaign as quickly as possible to focus resources on launching future Sentinel-1 satellites.

1.2 Key milestones in defining the new FDIR concept

The first de-orbit manoeuvres were conducted using RCT1 in February 2023, as these OCMs had already been tested and used for orbit maintenance since launch. Simultaneously, the design and validation of new manoeuvres utilizing the -Z RCTs were carried out. This required slewing the spacecraft to align the -Z RCTs with the direction of flight. The first de-orbit manoeuvres of this type were successfully executed in April 2023. The objective was to complete the de-orbit campaign by the end of 2023, depleting the remaining onboard fuel and reaching a target orbit that would ensure atmospheric re-entry within twenty-five years.

With this timeline in mind and the -Z RCT manoeuvres working successfully, the FCT at ESOC, composed by ESA staff and the COP-2 Service Contract, began planning the final fuel depletion manoeuvres. These manoeuvres posed a significant challenge, as accurately determining the remaining fuel was difficult. The fuel estimation was based on tank pressure readings, which could only predict the pressure at end-of-life to within approximately 5Kg uncertainty on the remaining fuel.

During the final manoeuvres, fuel exhaustion could occur at different times through the four RCTs due to the different pipework length of each RCT and the final thrust from each RCT was expected to be intermittent. This could create a torque on the spacecraft, potentially causing large attitude disturbances and triggering a Safe Mode. To mitigate this risk, the FCT explored different solutions. The chosen approach involved implementing a new FDIR action. This action would automatically stop an ongoing manoeuvre if the tank pressure suddenly dropped to a value significantly less than the lowest predicted fuel depletion pressure. Additionally, since the tank pressure fuel depletion value had some uncertainty, the FDIR was further updated to halt manoeuvres if reaction wheel (RW) speeds were exceeded. These thresholds were set within the Safe Mode limits to prevent escalation.
However, soon after the first FDIR design was validated, unexpected RCT degradation was observed a few months after initiating the -Z RCT manoeuvres. The degradation was closely monitored by teams at ESOC, the Sentinel-1 Project, and Industry partners.

Then, in July 2023, further degradation triggered a Safe Mode event. For Sentinel-1 an escalation to Safe Mode, even though the S/C stays in a stable state, has a major drawback: the satellite enters a mode in which performing manoeuvres is not possible due to the AOCS hardware in use. Bringing the system back to a status in which it is possible to manoeuvre requires typically one complete working day and the involvement of many resources. This has the double effect of slowing down or completely stopping ongoing activities, like the deorbiting campaign at the time of the triggering, but most importantly poses a risk in case a sudden CAM needs to be executed.

Investigations revealed that the degradation was uneven among thrusters, creating an RCT imbalance similar to what had been anticipated for the fuel depletion phase.

Recognizing this, the FCT quickly realized that the previously designed FDIR could also be deployed during the de-orbit phase to prevent mission interruptions. By implementing the FDIR earlier, the team could continue the de-orbit campaign as planned, minimizing the risk of Safe Mode triggering and lengthy recoveries. Further modifications to the original FDIR were necessary to include the option of halting manoeuvres if certain attitude disturbances were reached.

2. Stop Burn FDIR: Design

Before presenting the design of the new FDIR mechanism, it is essential to review two of the key concepts that make Sentinel-1 on-board autonomy possible and were fundamental for the implementation of the new operational approach: the On-board queue management and the FDIR mechanism implemented in SW.

2.1 On-board queue management

Sentinel-1 manages most of its routine operations making extensive use of its capability to store commands on-board up to 8 days in advance. These commands are saved in two on-board queues: the Time-Tagged queue and the Position-Tagged queue. However, due to the variety of operations that can be uplinked on board for future execution, Sentinel-1 exploits the ASW possibility of dividing the commands in Sub-Schedule Identifiers (SSID). Following a mission convention, each type of operation or subsystem is assigned a unique SSID: this allows the software to act on specific commands (i.e., delete, move, disable execution, etc) identified by their SSID without affecting all the stored operations related to other subsystems. The commands to perform OCMs, which are generated by Flight Dynamics (FD) and disseminated to the FCT via a Task Parameter File (TPF), are uplinked on-board as Time-tagged commands and identified with a unique SSID.

2.2 SW FDIR concept

Sentinel-1 FDIR logic, upon a fault detection, proceeds hierarchically to isolate the issue performing a series of recovery actions increasing in severity: from an autonomous on-line recovery, to a complete unit swap, to a central software restart (each restart progressing through the available satellite Safe Modes). This mechanism is distributed across the S/C in a mixture of Software and Hardware monitors and allows Sentinel-1 to achieve a robust on-board autonomy. The Avionics subsystem, which is the on-board controlling system where the Avionics Software (ASW) resides, directs the FDIR mechanism by the interaction of a set of ECSS Packet Utilization Standard services [5], as described in Figure 2.

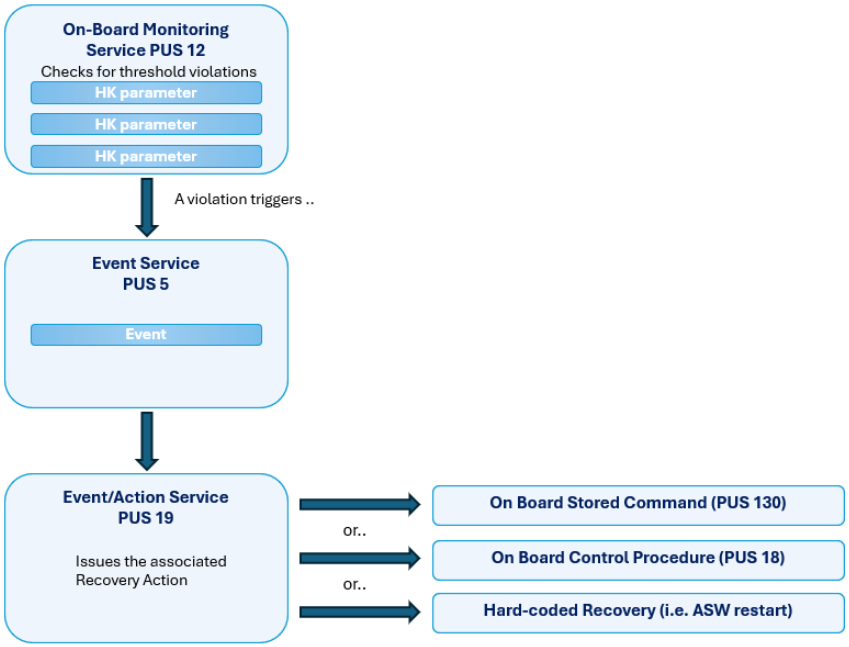


Fig 2: Broad scheme of Sentinel-1 Software FDIR and PUS services interrelations

The spacecraft's onboard systems continuously collect, process, and use diagnostic data to ensure safe operations and effective fault management: in fact, the starting point of Sentinel-1 FDIR process is the acquisition of defined Housekeeping (HK) parameters at regular time intervals computed by the various ASW Applications (software configuration items, each one in charge of a specific data pool of parameters). After this point, the interaction between PUS services takes place:

- PUS Service 12 - On Board Monitoring Service (OMS): a set of limits are applied upon the acquired HK parameters, and the purpose of OMS is to check that the defined thresholds are not violated. The OMS is made up of Monitoring Data Sets (MDS), each one related to a subsystem or operation mode. Each MDS has a defined number of Monitoring Items (MI), that can be considered specific checks on a single parameter. The monitors can be enabled or disabled at item, data set or whole Service 12 level.
- PUS 5 Service – Event Reporting Service (ERS): when a violation of a monitoring is detected, this is notified by Service 12 and a related Event with information on the anomalous condition and severity is raised by Service 5.
- PUS 19 Service – Event Action Service (EAS): when an event is detected, the EAS allows the S/C to perform an autonomous recovery action associated with the event. Up to three different levels of recovery actions can be defined per event. A recovery action can be the execution of a simple command, stored in the On-Board Command Database (OBCD) and handled by customised PUS Service 130; a series of commands that make up an On Board Control Procedure (OBCP), responsibility of PUS Service 18; ultimately, a recovery hard-coded in the software (like an ASW restart).

The FDIR structure is set in the S/C design phase and should not be modified during routine operations. However, it is understood that during the mission lifetime operational scenarios may change and problems can arise at any time. For this reason, each of the aforementioned PUS Services also provides Spare items or sections dedicated to user customisation to cater for new anomalies handling or different ground needs.

2.3 The Stop Burn FDIR design

The default FDIR mechanism to cope with attitude disturbances or RW overspeed during manoeuvres for Sentinel-1 is based on a subset of MIs enabled only when the S/C is in OCM mode. Limits are checked for Overspeed of the 4 RWs, attitude errors and attitude rate errors on all axes (Table 1). Upon violation of one of the thresholds, an Event is raised to which Service 19 associates a hard-coded recovery that triggers a transition to Safe Mode. The whole FDIR mechanism is described in Figure 3.

Table 1. Current FDIR thresholds for Safe Mode escalation in OCM

MDS / MI	Description	Safe Mode Threshold
MDS 34 MI 5-9-13-17	RW Overspeed (RW 1-2-3-4)	+/- 385 rad/s
MDS 36 MI 1-2-3	Attitude Error (X-Y-Z)	+/- 0.1 rad
MDS 36 MI 4-5-6	Attitude Rate Error (X-Y-Z)	+/- 0.01 rad/s

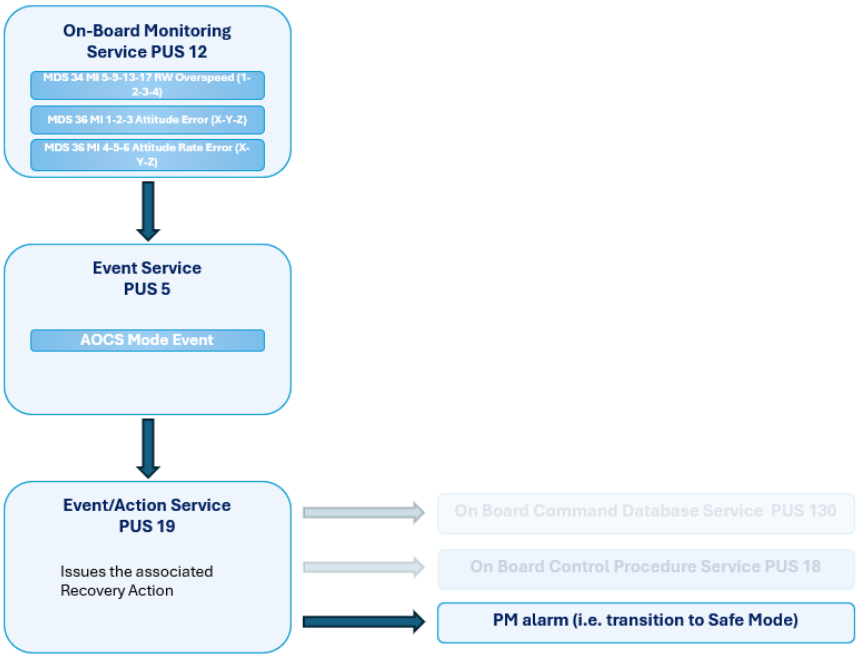


Fig. 3: Default FDIR mechanism in case of RW Overspeed, Attitude Error or Attitude Rate Error breaches

The new FDIR was designed taking the existing one as a starting point and developed according to the following drivers:

- The FDIR should allow the Spacecraft to remain in Standby Mission Mode with Pitched Attitude and capable to perform Collision Avoidance Manoeuvres (CAM)
- The FDIR should prevent escalation to Safe Mode
- The FDIR should be based on existing monitoring definitions but be defined using spare monitoring items, adjusting the limits within the existing MI limits (in case the FDIR is not successful the existing FDIR will guarantee the safety of the Spacecraft)
- The FDIR should prevent the execution of any further OCMs already uplinked into the On-board Time-tagged queue
- The FDIR should be designed to handle failures on both main and redundant RCT branches.

The new devised FDIR logic, from here on referred to as “Stop Burn FDIR”, was then the following (Figure 4):

1) New dedicated Spare Monitoring Items were configured to monitor RW Overspeed, Attitude Errors and Attitude Rate Errors, belonging to the data sets enabled during OCM executions (MDS 34 and 36).

2) In case these new monitors’ limits are breached, a new Spare Error Handler is raised, configured to trigger the execution of a new OBCP.

3) The spare OBCP will execute the following commands:
   a) Stop the RCT Actuation
   b) Disable the execution of commands with OCM SSID
      i. All the Time-tagged commands related to OCMs will not be executed
   c) Switch off RCT drivers
   d) Switch off RCT-A
   e) Switch off RCT-B

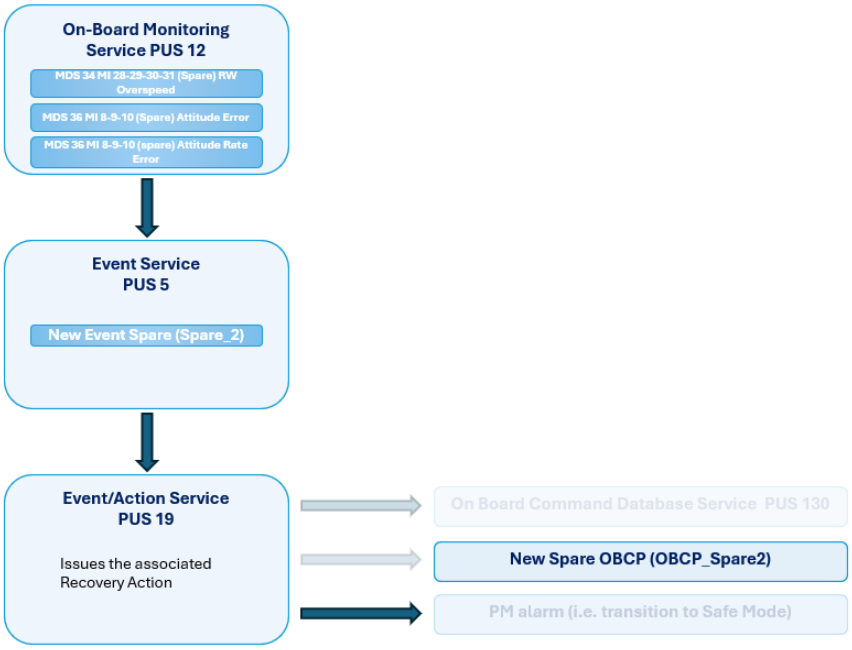


Fig. 4: New FDIR mechanism to stop an ongoing Burn

Thanks to this design, the FDIR could be easily activated or deactivated according to the circumstances: for example, when manoeuvres that could impact the S/C safety had to be executed, like a CAM, the FDIR could be bypassed by simply disabling the newly defined monitoring.

2.4 Challenges of the definition

The flexibility provided by the ASW and described in Section 2.2 offered the perfect opportunity to modify the FDIR logic to suit the spacecraft's new needs and therefore the operational concept could be implemented by the FCT with the collaboration of the Satellite manufacturer. However, the definition of the Stop Burn FDIR was not free from challenges for the FCT:

1) Not all the commands needed for the new OBCP were present in the OBCD: as TCs from a to e were not planned to be part of the Database of commands on-board, the ASW required a patch to add them as Spare TCs available for on-board usage.

2) The usage of Spare items (MIs, Events, OBCPs, TCs..) relies on having a clear picture of the current status of the on-board software and available resources: before starting the design of the Stop Burn FDIR, it was crucial to understand how many Spare monitoring items, Spare Events, Spare OBCPs and Spare commands were already employed for other operational needs during the mission's lifetime and how many were available for the FCT to use. This could be easily achieved thanks to the well-documented history of operations on the satellite, whose details are all tracked in Special Operation Requests (SOR) and the Mission History Log (a repository of the full story of the mission since its beginnings).

3) Implementing new operational concepts in a flying mission requires careful handling. Any activity introduced while in flight must be thoroughly validated to ensure the safety of the mission. Moreover, in this particular case, given the triggering of the Safe Mode in July 2023, the new monitoring thresholds needed to be finetuned, making the design of the Stop Burn FDIR an iterative process, where the simulations executed were used to refine the FDIR definition. All the actions performed to confirm the reliability of the new FDIR and the study of the

appropriate limits are described in the next Section.

3. Stop Burn FDIR: On-Ground Validation

A series of tests were performed by the FCT using the ESOC S/C simulator to validate the design of the FDIR. These were used for two main purposes:

- To validate the correct triggering of the new FDIR.
- To determine suitable thresholds for the new Service 12 monitoring parameters.

The ESOC S/C simulator has already proven to be a realistic environment for testing attitude disturbances on the spacecraft, which makes the simulation results reliable.

As seen in Section 2, the FDIR concept was to utilize the same parameters as in Table 1 with adjusted thresholds. These new thresholds had the following requirements:

- They should be within the Safe Mode thresholds to prevent escalation to Safe Mode.
- They should not be so low that they would trigger during nominal manoeuvre disturbances (these thresholds can be deduced from flight data).
- They should cope with a range of RCT imbalances to the maximum extent possible without triggering a Safe Mode.

As an initial starting point for simulations, the following thresholds were used:

Table 2. Initial FDIR thresholds for Stop Burn

MDS / MI	Description	Stop Burn Threshold
MDS 34 MI 28-29-30-31	RW Overspeed (RW 1-2-3-4)	+/- 250 rad/s

The following process was used to mimic the starting conditions of a de-orbit manoeuvre in the ESOC simulator:

- Load a simulator breakpoint in nominal science attitude and replicate the current attitude and S/C configuration.
- Turn off payloads.
- Set a -90-degree pitch attitude so the -Z RCT can be used to lower the orbit.
- Update the RCT scale factor with current degradation values (see Table 3).
- Set the S/C in OCM Mode with RCT A branch ON.
- Apply the RAM patch to include the Stop Burn FDIR.
- Save the breakpoint for reuse in different test cases.

Table 3. RCT Degradation values during Safe Mode anomaly

RCT	Force
RCT 4A	0.57 N
RCT 5A	0.56 N
RCT 6A	0.47 N
RCT 7A	0.58 N

3.1 Initial simulation

The initial simulation mimicked the burn that caused the Safe Mode escalation in July 2023. The objective was to verify the correct behaviour of the simulator in comparison with real flight data, the correct execution of the FDIR with the initial Service 12 thresholds and to determine if the Safe Mode could have been prevented.

A 700-second RCT burn was initiated in the simulator (see Figure 5). After 389 seconds, the new RW2 overspeed threshold was reached, and the burn actuation successfully stopped by the Stop Burn FDIR. Further Observations:

- Attitude disturbances before the FDIR triggered were very similar to the real behaviour of the spacecraft during the Safe Mode event
- RW2 overspeed was the first threshold to be violated.
- Spare OBCP triggered successfully after the Service 12 monitoring violation, halting the burn, switching off the RCTs, and disabling further manoeuvre TCs onboard (see Figure 6).
- RW speed continued increasing after the burn stopped, as expected, but the SC recovered before reaching the Safe Mode threshold, successfully preventing escalation.

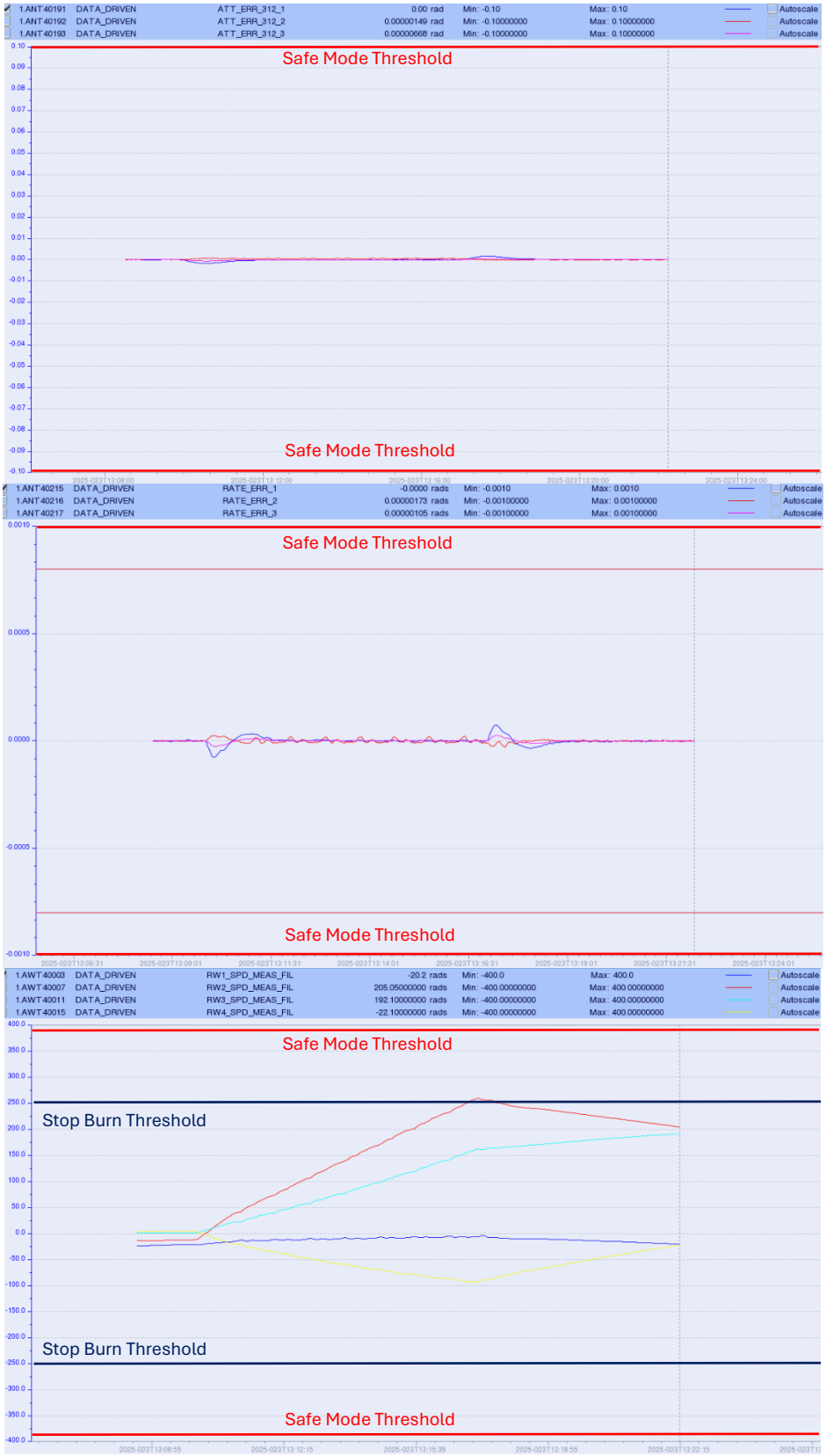


Fig. 5. Attitude Error, Attitude Rate Error and RW Speed for Safe Mode case

Note that the calibration for the attitude rate error is capped at +/- 0.0008192 rad/s. Therefore, plotting this parameter provides limited insight into whether it would exceed the Safe Mode threshold of +/-0.001 rad/s. For this reason, the attitude rate error will not be plotted in further simulation results. However, the spacecraft FDIR

will continue to monitor this value, and if it is violated, a Safe Mode event will still be triggered.

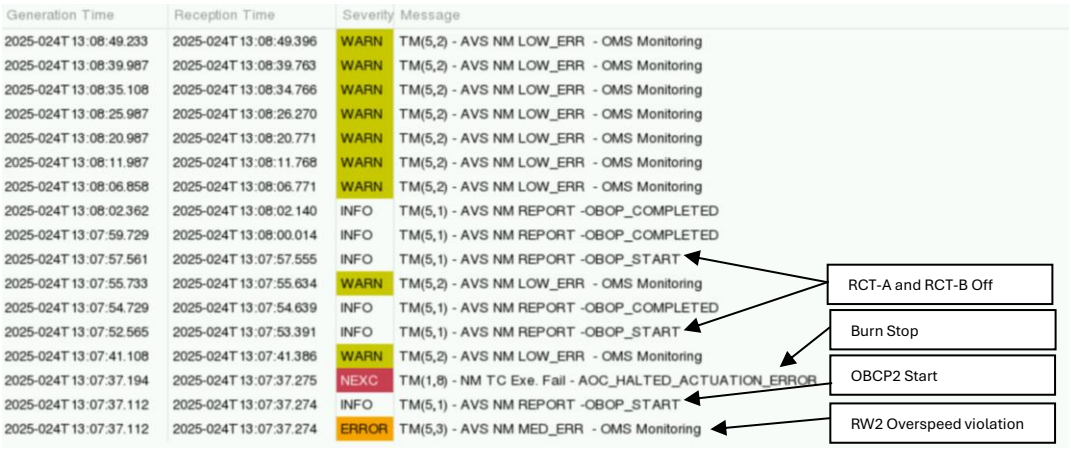


Fig. 6. List of On-board events generated during the FDIR triggering

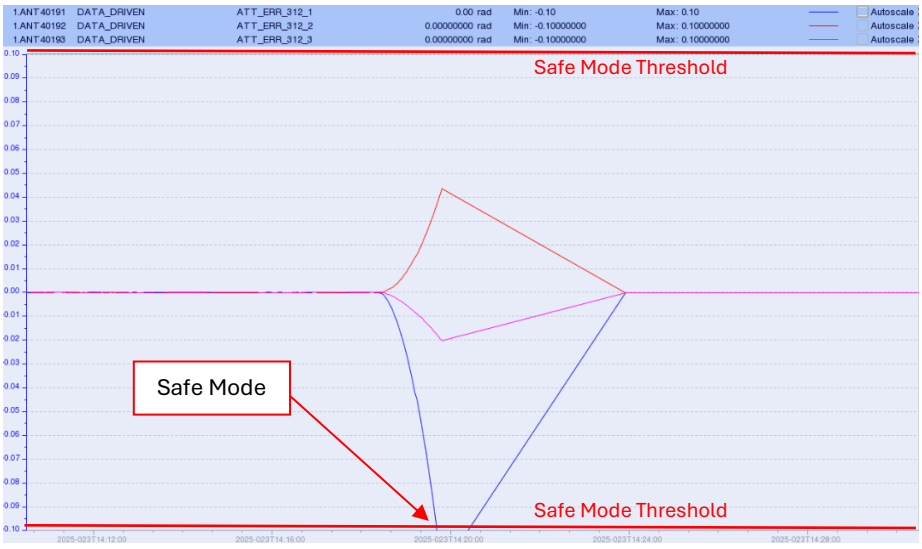
Once the initial simulation proved the concept, a series of simulations were performed to test further RCT degradation scenarios.

3.2 Further simulations

Since RCT degradation was unpredictable, additional simulations tested worst-case scenarios. In these cases, an RCT was completely failed to simulate greater imbalances and a 700-second RCT burn was initiated.
The first simulations focused on RCT6A, as it degraded fastest and caused the July 2023 Safe Mode. The simulator was adjusted to set RCT6A as failed (0 N).

Table 4. RCT Scale Factor for RCT6A failure simulations

RCT	Force
RCT 4A	0.57 N
RCT 5A	0.56 N
RCT 6A	0.00 N
RCT 7A	0.58 N



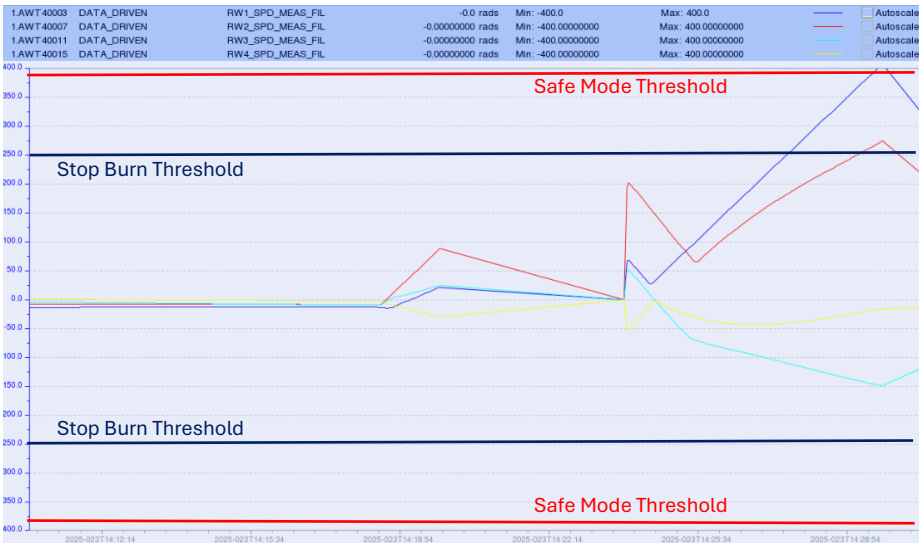


Fig. 7. Attitude Error and RW Speed for initial RCT6 failure simulation

The results of the initial simulation (see Figure 7) were that FDIR did not trigger, but Safe Mode escalation was observed. The Safe Mode was caused by an attitude error threshold violation rather than an RW overspeed. This was the reason why the FDIR design was expanded to include attitude error and rate error monitoring across all three axes (as seen in Section 2).

After testing various thresholds, the optimal values were determined to be 1/10 of the current Safe Mode thresholds:

Table 5. RCT 6A Failure simulations for different Attitude FDIR thresholds

RCT 6A Failure simulations	**Attitude Error**	**Att. Rate Error**	**Outcome**
Safe Mode Thresholds	+/- 0.1 rad	+/- 0.01 rad	**Failure**
½ Safe Mode Thresholds	+/- 0.05 rad	+/- 0.005 rad	**Failure**
⅕ Safe Mode Thresholds	+/- 0.02 rad	+/- 0.002 rad	**Failure**
$\frac{1}{10}$ Safe Mode Thresholds	+/- 0.01 rad	+/- 0.001 rad	**Success**

The RW overspeed threshold is not reached and could be left unchanged.

Table 6. Updated Stop Burn FDIR thresholds

MDS / MI	**Description**	**Stop Burn Threshold**
MDS 34 MI 28-29-30-31	RW Overspeed (RW 1-2-3-4)	+/- 250 rad/s
MDS 36 MI 8-9-10	Attitude Error (X-Y-Z)	+/- 0.01 rad
MDS 36 MI 11-12-13	Attitude Rate Error (X-Y-Z)	+/- 0.001 rad/s

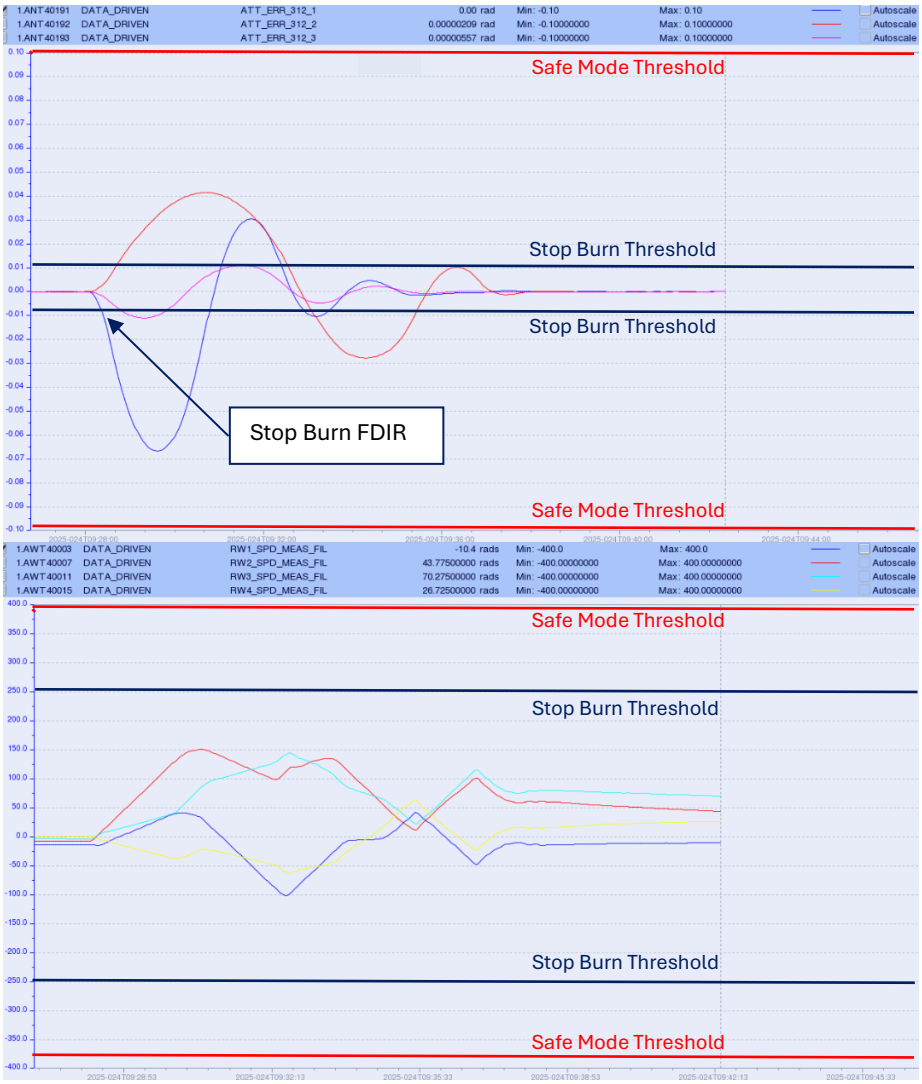


Fig. 8. Attitude Error and RW Speed for RCT6A failure simulation with updated FDIR thresholds

The new thresholds were low enough to prevent Safe Mode but high enough to avoid interference with nominal manoeuvres (see Figure 8). Attitude error limits have a margin of approx. 3 times compared to nominal in-flight RCT-A burns. The attitude rate limits have a margin of more than 5 times compared to in-flight nominal RCT-A burns (see Figure 9).

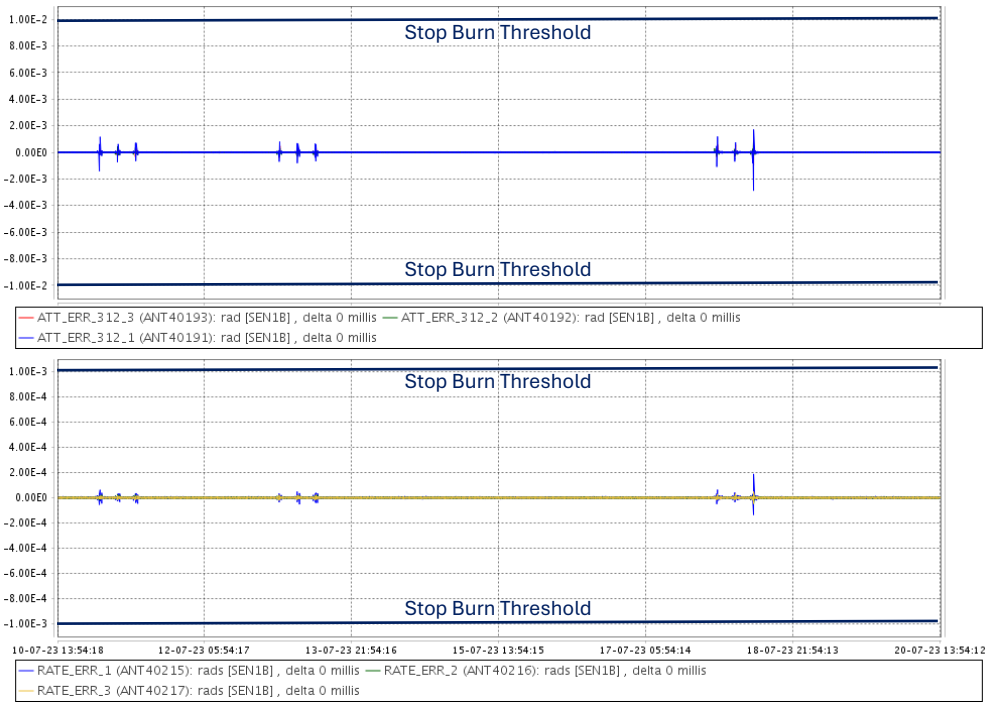


Fig. 9. Stop Burn FDIR thresholds vs real OCM attitude disturbances

With the new thresholds, simulations were conducted for complete failures of additional RCTs. The following results were obtained:

Table 7. RCT Failure simulation results

Sim #	RCT Thrust				FDIR start (sec)	Safe Mode
	4A	5A	6A	7A		
1	0.57	0.56	0	0.58	29	No
2	0	0.56	0.47	0.58	29	No
3	0.57	0	0.47	0.58	30	No
4	0.57	0.56	0.47	0	24	No

The simulations confirmed that the updated thresholds effectively prevented Safe Mode escalation in worst-case scenarios. FDIR is always triggered by the Attitude Error in the X axis 20-30 seconds after the start of the burn. Double RCT failure simulations were not performed (the FDIR was designed to cope with only a single RCT failure).

The ESOC simulations were analysed by both Industry and Project teams, and the results were confirmed to be satisfactory.

4. Stop Burn FDIR: Upload, Activation and Results

After the successful validation of the FDIR and the definition of the monitoring thresholds, the Stop Burn FDIR could be uploaded on board. A Special Operation Request was created for this activity and applied to the S/C in September 2023.

During the deorbiting campaign, the RCTs continued to degrade in an unpredictable way, with different performances from burn to burn. It was only a matter of time until the Stop Burn FDIR was activated during one of the orbit-lowering manoeuvres.

The first time that the Stop Burn FDIR triggered was on 12 October 2023. At that point in the deorbit, the RCT propulsion had already been switched to the redundant branch after the Safe Mode in July 2023 and batches of 4 manoeuvres were performed twice per week with burn durations of around 380 sec.

The FDIR triggered in the 2nd manoeuvre of that batch, with the burn starting at 04:57:57 UTC. The FDIR triggered 236 sec after, at 05:01:51 UTC, halfway through the manoeuvre.

The FDIR was triggered by the Attitude Error violation on the X axis (roll axis). The events that triggered afterwards match the ones received during the validation in the simulator (Table 8).

Table 8: On-Board Events after the Stop Burn FDIR on 12/10/2023

DateTime	Event Packet	Severity
2023-10-12 05:01:51.769	TM(5,3) - AVS NM MED_ERR - OMS Monitoring	Error
2023-10-12 05:01:51.773	TM(5,1) - AVS NM REPORT -OBCP_START	Nominal
2023-10-12 05:01:51.855	TM(1,8) - NM TC Exe. Fail - AOC_HALTED_ACTUATION_ERROR	
2023-10-12 05:02:07.105	TM(5,1) - AVS NM REPORT -OBCP_START	Nominal
2023-10-12 05:02:09.265	TM(5,1) - AVS NM REPORT -OBCP_COMPLETED	Nominal
2023-10-12 05:02:12.230	TM(5,1) - AVS NM REPORT -OBCP_START	Nominal
2023-10-12 05:02:14.394	TM(5,1) - AVS NM REPORT -OBCP_COMPLETED	Nominal
2023-10-12 05:02:17.019	TM(5,1) - AVS NM REPORT -OBCP_COMPLETED	Nominal

The following plots give the attitude and RW performance during that burn. As can be seen from Figure 10, the FDIR prevented an escalation to Safe Mode.

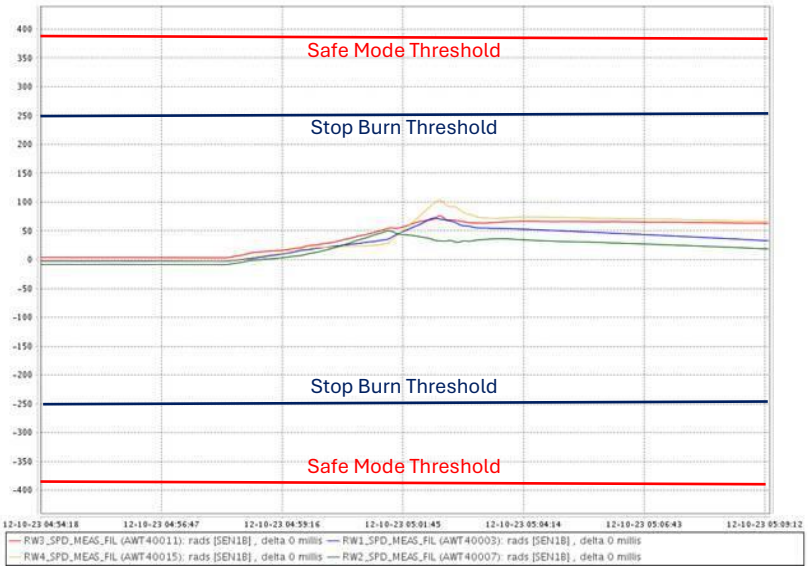


Fig.10. Attitude Error, Attitude Rate Error and RW Speed behaviour during the Stop Burn FDIR on 12/10/2023

An account on all the cases in which the Stop Burn mechanism was triggered and therefore prevented a Safe Mode can be found in Table 9.

Table 9: Summary of Stop Burn FDIR triggering events

Date	Monitoring breached	RCT branch	FDIR start (sec after burn start)	Safe Mode
12/10/2023	Attitude Error (X)	B	236	No
26/10/2023	Attitude Error (X)	A	188	No
31/10/2023	Attitude Error (X)	A	134	No
12/12/2023	Attitude Error (X)	A	110	No

The last Pitch Slew OCM was performed 29th February 2024, when the SC reached the 25 years re-entry point. After that, the FCT could start preparing the passivation activities, which were completed on 12th September 2024 [6].

5. Conclusions

Even if designed as a safety measure, the Stop Burn FDIR proved to be successful in all cases: no more Safe Modes due to attitude disturbances or RW overspeed were triggered since the FDIR was applied. This allowed the Sentinel-1B de-orbit campaign to continue without safe mode interruptions and lower the SC orbit as much as possible despite the unpredictable performances of the 4 -Z RCTs.

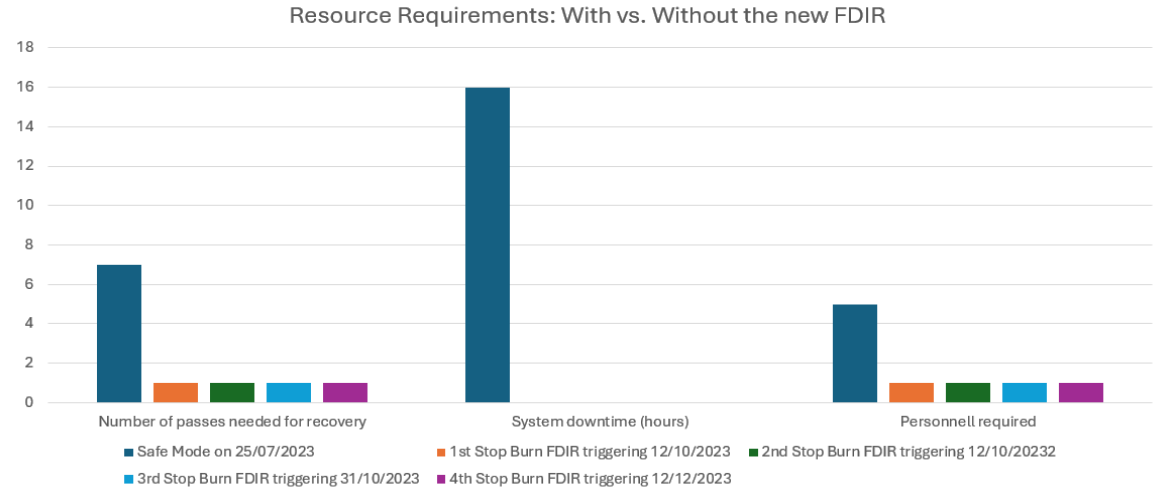


Fig. 11: Comparison of resources requirements to recover the S/C with and without the Stop Burn FDIR

Summarising, the new FDIR concept proved to be beneficial in three different areas (Figure 11):

1) Number of passes needed for the recovery: to bring back the S/C to its operative state after a Safe Mode, many activities must be executed at System and Subsystem level. For a LEO satellite like Sentinel-1B, this means fitting the recovery activities in short (approx. 10 minutes) commanding passes, delaying and extending the recovery process. In the cases where the Stop Burn FDIR triggered, only one commanding pass was needed (no recovery actions to be performed, only clean-up operations after the triggering of the FDIR).
2) Hours of system unavailability: escalation to Safe Mode, as seen in Section 1, implies a fall back to an operative mode in which the S/C is not capable of performing manoeuvres.
The long recovery activities required to restore the nominal status protracts the period during which the S/C remains non-manoeuvrable, exposing it to the risk of not performing a CAM in case of a sudden collision warning. Thanks to the Stop Burn FDIR the S/C stays OCM-capable also in case of FDIR triggering.

Moreover, for a satellite in its routine phase, a Safe Mode escalation implies also the switch-off of the payload, leading to a significant loss of mission data. With the Stop Burn FDIR, all the payload operations remain safe for execution (note that this was not the case for Sentinel-1B, the payload was non-operational at the time of the events, but is an added advantage of this design), minimising almost to zero the impact of a non-smooth OCM execution on the science mission.

3) Number of personnel required to perform the recovery: recovery from a Safe mode escalation is an all-hands-on-deck effort. The Spacecraft Operations Manager (SOM), the on-call Spacecraft Operations Engineer (SOE), a supporting SOE and a Spacecraft Controller (Spacon) are the minimum number of personnel required to ensure that the steps of the recovery are completed in a precise and timely manner. Thanks to the Stop Burn FDIR, only one person, the SOE on-call, was required to perform the clean-up activities the times this triggered. This allowed ESA to accomplish its goal to complete the campaign successfully while focusing the other resources on the preparation and launch of future Sentinel-1 satellites.

This approach brings several non-quantifiable benefits, too. Recovering the S/C from a Safe Mode is a long operation performed in many steps and involves activities that meddle with vital parts of the satellite. Hence, the risk introduced by performing a long recovery like this one is greater than the risk introduced by clean-up activities after the triggering of the Stop Burn FDIR (i.e., unexpected behaviour of the Spacecraft, possibility of human errors, etc.). Furthermore, the time needed to perform investigations, Anomaly Review Board (ARB) meetings, implement a recovery strategy after a Safe Mode event is not taken into account in the calculation but must be considered when reviewing the advantages of the new design: the recovery process could span several days, adding up to the system unavailability time and to the number of resources solely allocated to investigation and recovery (hence removed from other activities).

Despite the challenges, the team gained invaluable insights into the spacecraft's capabilities and limitations, which will provide benefits for future Sentinel-1 operations. A very similar approach has been applied during the Orbit Acquisition phase of the latest addition to the Sentinel-1 constellation, Sentinel-1C, launched in December 2024 [7]. The implementation of the same FDIR logic, with the appropriate modifications, ensured plenty of margin for safe usage of -Z RCT thrusters, that can be used to reach the target orbit for the acquisition phase in a faster way, without falling back to Safe Modes in case of -Z RCT misbehaviour.

Given the similarities of the Sentinel-1 spacecraft, this approach could be repurposed for the future critical mission phases, such as the de-orbiting campaign of Sentinel-1A or the Orbit Acquisition phase of Sentinel-1D. Moreover, as hinted at in point 2 and inferable from Figure 11 also a spacecraft in routine operations could benefit from a similar FDIR logic: the new concept applied to risky manoeuvres in routine operations could reduce or completely avoid loss of payload availability, thus maximising the science data return. An effective FDIR can avoid system downtime caused by anomaly triggering, safe mode escalation and lengthy recovery operations, that would in this case also involve Payload recovery operations, extending the time required to make the satellite operative again and producing science.

Lastly, the new logic was devised starting from basic PUS services concepts, which have the great advantage of being common, coherent and implementation independent for all the missions applying the same standards, that are with each new version contributing to a harmonisation of procedures and operational strategies [8]. Therefore, the same logic could be re-used for critical operation phases of other missions adopting PUS, with the necessary modifications. Sentinel-1B was the first satellite of the Copernicus family to be deorbited and, just as it was for its LEOP [9], can serve as a reference point for the new phase of Sentinel missions, in which older generations are gradually being phased out and replaced with the more advanced models, ensuring continuity and

technological evolution in Earth Observation.

Acknowledgements

The authors would like to thank the Sentinel-1 Project, Mission Management, Post-Launch Support Office, Industry Partners, and ESOC Sentinel-1 FCT for the collaboration on the Stop Burn FDIR design and the work behind this paper. Spacecraft operations' success can only be achieved thanks to collaboration between teams working together towards a common goal.

Disclaimer

The views expressed herein can in no way be taken to reflect the official opinion of the European Space Agency or the European Union.

References

[1] Sentinel-1b In-Flight Anomaly Summary Report, https://sentinel.esa.int/documents/247904/4819394/Sentinel-1B+In-Flight+Anomaly+Summary+Report.pdf, ESA Repository

[2] Mission ends for Copernicus Sentinel-1B satellite, https://www.esa.int/Applications/Observing_the_Earth/Copernicus/Sentinel-1/Mission_ends_for_Copernicus_Sentinel-1B_satellite, ESA Webpage

[3] Space Debris Mitigation Policy for Agency Projects, ESA/ADMIN/IPOL(2014)2, 28 March 2014.

[4] Serrano, M. M., Catania, M., Sánchez, J., Vasconcelos, A., Kuijper, D., & Marc, X. Sentinel-1A flight dynamics LEOP operational experience. International Symposium on Space Flight Dynamics Symposium on plume impingement. October 2015.

[5] ECSS-E-ST-70-41A (Space engineering – Ground systems and operations – Telemetry and telecommand packet utilisation), 30 January 2003

[6] Thomas Ormston et al. "Sentinel-1B End-Of-Life Operations" SpaceOps 2025 Conference. May 2025.

[7] Double win for Europe: Sentinel-1C and Vega-C take to the skies, https://www.esa.int/Applications/Observing_the_Earth/Copernicus/Sentinel-1/Double_win_for_Europe_Sentinel-1C_and_Vega-C_take_to_the_skies , ESA Webpage

[8] Ignacio Clerigo, Andrea Accomazzo, Peter Collins, Nic Mardle, Elsa Montagnon, Jose-M Morales-Santiago and Ignacio Tanco. "One Standard to Rule Them All: the Tailoring of PUS-C for Future ESA Missions," AIAA 2018-2399. 2018 SpaceOps Conference. May 2018.

[9] Ian Shurmer. "The Sentinel-1A LEOP: Paving the Way for the Sentinels LEOP Preparation and Execution," AIAA 2016-2457. SpaceOps 2016 Conference. May 2016.