National Aeronautics and Space Administration

Goddard Space Flight Center
Greenbelt, MD 20771

September 2, 2021

Reply to Attn of: 300 300-STM-1014

TO: Distribution

FROM: GSFC Council of Chiefs

SUBJECT: GSFC Technical Memorandum - GSFC application of lessons learned from the ICESat-2 missed risk mitigation maneuver close call

On July 3, 2020, the Ice, Cloud and land Elevation Satellite-2 (ICESat-2) mission failed to execute a Risk Mitigation Maneuver (RMM) planned at 22:16:13 UTC to mitigate conjunction with Russian SL-3 Rocket Body with time of closest approach (TCA) on July 4, 2020 at 15:12:05 UTC. The sequence of events was as follows:

- Nominal Weekly Schedule Planned and uploaded
- Conjunction High Interest Event identified, RMM warranted and planned
- Incorrect Maneuver Timeline (MTL) automatically ingested and used for science activity planning
  - No detection incorrect maneuver timeline used
  - No detection RMM and instrument activity scheduled at same time
- Instrument Activity remained scheduled during RMM Activities preventing RMM to execute

The Earth Science Mission Operations (ESMO) project performed a thorough analysis to determine root cause, and corrective actions to prevent recurrence on future ICESat-2 operations. While many of the problems were very specific to the ICESat-2 mission operations processes and unique constraints, an independent review team and senior Safety and Mission Assurance staff took a focused look at the applicability across all of GSFC mission operations to identify the broad lessons learned, and subsequently, the GSFC Council of Chiefs reviewed for broad applicability across the Center and to some extent the Agency. The lessons learned are summarized as follows:

1. <u>Beware of manual processes needed to perform critical functions in mission operations.</u>
   a. Add some level of automation into the manual review process, e.g., developing tools to check the flight rules and constraints. Good examples are SSMO missions that use scripts to review the Delta-V loads.
   b. Consider having severity constraints (critical warnings) that do not allow mission planning (or other) products to be generated until the constraint or

failure is resolved.

c. Add an additional review for steps that can only be accomplished manually.

d. Operational procedures should verify contents of all input data and command loads.

e. Mission Systems Engineers & Operations Assurance Engineers should not presume sufficient verification of inputs to important ground system software is occurring.

2. <u>For infrequent critical commands, regularly practice the implementation process to ensure that the team maintains familiarity with implementation.</u>
    a. Schedule periodic operational procedure reviews, walk-throughs, or training. Conducting reviews or training may: a) remind operators of procedural subtleties; b) indicate that procedural documentation needs to be updated to reflect current operations; or c) provide opportunities for operators to identify process improvements.

3. <u>Plan and exercise before launch all planned operational scenarios that do not involve an anomalous spacecraft --including infrequent and/or contingency scenarios like debris avoidance maneuvers.</u>
    a. Low-Earth Orbiting (LEO) spacecraft being developed should include executing debris avoidance maneuvers in their operations concept and exercise that process before launch. The process of planning and executing an ICESat-2 RMM was not exercised before launch. Even more generally, the process of generating a `split' command load (interrupting the nominal command load to insert an activity like an RMM) was not exercised before launch. This, paired with the lack of planning laser conjunction avoidance before launch, means a significant portion of the RMM activities had to be developed ad-hoc after launch.

4. <u>Apply best practices, such as those defined in GOLD Rules that are still applicable in phase E:</u>
    a. (3.04) Apply independent software testing to the phase E software sustaining engineering process. One of the validation tools developed by the mission in response to this Close Call was developed and tested by the same person. This increases the likelihood of an error existing in the deployed code. In fact, this was experienced by the mission; the tool was deployed with an uncaught defect. Fortunately, the defect did not cause another anomaly or Close Call.
    b. (3.10) In Phase-E, conduct tests or re-tests of critical events using available simulation and flatsat resources. Risk mitigation maneuvers need to be identified as either critical operations and or day-in-the-life focused on spacecraft.
    c. (1.14) Perform critical events such as maneuvers only within telemetry and command capability. Hence, passes should be scheduled during critical operations (e.g., RMMs or other orbital maneuvers). The ICESat-2 operations team did not schedule a pass to occur during the RMM and therefore did not know immediately that the RMM had failed to execute. Due to the time-

consuming nature of the ICESat-2 RMM process, insufficient time existed to attempt a second RMM. But for other, more agile missions, quickly determining that a maneuver did not execute may have allowed for another RMM attempt.

5. Utilize and maintain a certain level of redundancy in terms of knowledge and personnel availability within the flight operation team for reviews and verification activities.
    a. Currently, resource-constrained missions may have software that only one person is qualified to maintain preventing defect fixes in that software when that person is unavailable. This was experienced by the ICESat-2 mission, preventing a validation tool software defect from being fixed until the developer in question returned to work from leave.
    b. Missions should not rely solely on a mission director to have a spacecraft-level purview. Based on the designed mission architecture and possibly inattention in early reviews, ICESat-2 operations are more `stove-piped' than other missions; as a result the mission director must provide the system-level oversight. The operations team should bear responsibility for spacecraft health, with a sufficient system-level purview. During the Command Authorization Meeting (CAM), the operator error that led to the violation of the operational constraint was not noticed. This, and other system-level issues, are more easily missed when insufficient systems-level oversight exists.

6. Do not skip planned system checkout activities during commissioning
    a. To decrease the likelihood that similar Close Calls result in the destruction of NASA missions, spacecraft should exercise systems that are needed to successfully conduct avoidance maneuvers, such as the propulsion system. Checkout of such systems ensures they are available and operational for use in avoidance activities. Historically, not all GSFC missions have followed this guidance. Fortunately, the ICESat-2 Failed RMM Close Call did not result in a collision. The development of a GOLD Rule should be considered to provide a uniform process to complete key checkout activities.

7. Design recommendations
    a. Permit only one individual to command changes to the ACS mode, with a backup only when circumstances prevent this individual from performing the required function. Allowing more than one entity to command changes to the ACS mode increases the likelihood of an operational error. This lesson learned has been shared by the RST Software and Mission Operations Assurance Engineer with the RST mission. The current path forward for the execution of RST momentum unloads decreases the number of times such ACS commanding conflicts could occur.
    b. Design spacecraft and spacecraft Concepts of Operations to accommodate multiple options (primary and secondary) for debris avoidance maneuvers. In addition to posigrade avoidance maneuvers, spacecraft should be designed in a manner to allow the option of retrograde maneuvers. Missions should also

consider including the use of pre-loaded maneuver sequences which could decrease the time needed to conduct avoidance maneuvers and that would increase the chance a maneuver could be re-attempted if needed.

8. Develop an Orbital Collision Avoidance Plan (OCAP) per the new NID NASA Interim Directive (NID) 7120.132.
   a. NID 7120.123 establishes minimum collision avoidance requirements and associated operational protocols for NASA space flight programs, projects, and vehicles to protect the space environment and minimize the risk of collisions.

9. Make sure all operational constraints are documented.
   a. A verification should be performed and crosschecked that the constraints document is complete. The ICESat-2 RMM Investigation identified a situation in which a specific constraint (e.g., preventing science operational commands within a critical maneuver) was not adequately documented in the formal documentation of such mission-specific constraints. As a result, none of the operational procedures had checks in place (and tested during preflight) to ensure specific constraints such as the one described above were not violated..
   b. Ensure all operational constraints are aligned with formal operational procedures.

10. The Center and Agency should approach missions in operation with the same level of attention as with missions in development
    a. The Center should apply the same level of importance and resources toward missions in operation as to those in development.

These lessons lead to recommendations that come into play at multiple points in the mission lifecycle, extending back to early development of concepts of operation, so they should be considered by mission designers, systems engineers, and mission operations individuals.

If there are any questions on these, or a desire to schedule a briefing, feel free to contact Jesse Leitner at jesse.leitner@nasa.gov.

Jesse Leitner Digitally signed by Jesse Leitner
Date: 2021.09.13 08:03:02
-04'00'

Dr. Jesse A. Leitner
Chief Engineer
Safety and Mission Assurance

TRISTRAM HYDE Digitally signed by TRISTRAM HYDE
Date: 2021.09.03 21:25:22 -04'00'

Tristram T. Hyde
Chief Engineer
Goddard Space Flight Center

JAMES GARVIN Digitally signed by JAMES GARVIN
Date: 2021.09.04 08:45:01 -04'00'

Jim Garvin
Chief Scientist
Goddard Space Flight Center

Peter Hughes Digitally signed by Peter Hughes
Date: 2021.09.12 23:36:57 -04'00'

Peter Hughes
Chief Technologist,
Goddard Space Flight Center

TIMOTHY TRENKLE Digitally signed by TIMOTHY TRENKLE
Date: 2021.09.06 08:45:29 -04'00'

Tim Trenkle
Senior ETD Engineer,
Engineering and Technology Directorate

Distribution:

100/D. Andrucyk
100/A. Kinney
300/All
400/Program and Project Managers

500/D. Mitchell
500/T. Hyde
500/T. Trenkle
600/M. Clampin
800/D. Pierce