Bryant, Larry W.
Situational Awareness: a Cornerstone of Operational Excellence in Space
Journal of Aerospace Technology and Management, vol. 7, núm. 2, 2015, pp. 141-142
Instituto de Aeronáutica e Espaço
São Paulo, Brasil

Situational Awareness: a Cornerstone of Operational Excellence in Space

Larry W. Bryant[1]

Operating in space is, at best, a risky business. Given that it is fraught with peril, the goal of operational excellence is not just a nice-to-have objective; it becomes a mandatory, albeit unwritten, requirement. Does this mean we have to command our spacecraft flawlessly or that every maneuver imparts an exactly predictable amount of delta-V? Obviously not, but it does mean striving to be error free in commanding and trying to reduce the variance of our maneuvers as much as possible. It is an attitude in our behavior as much as it is an exactitude in our performance. A number of factors, training, experience, education, and so forth, contribute to our behavior and performance, but the one that provides the essential foundation is maintenance of situational awareness.

Situational awareness is woven into the very fabric of operational excellence. By recognizing the similarities and differences between situations for which you have trained and those you have not, you are able to deal with new operational challenges. Being aware of your spacecraft state as well as its future state may well help you avoid a catastrophic commanding error. As an example, consider that you are about to send an innocuous command to your spacecraft for one of its instruments. You can tell from telemetry that the instrument's sequence engine (portion of memory dedicated to sequences for this instrument) is empty with nothing executing at the time. However, a check of your spacecraft sequence of events alerts you to the fact that, in the time it takes for your command to reach the spacecraft (a light time), a different sequence to ramp up the voltage in the instrument will begin to execute in that sequence engine. Both sequences occupying the same engine will cause a sequence collision. A collision usually results in a safe mode entry which, under the right conditions, can have unintended and undesirable consequences. Fortunately, by maintaining situational awareness and checking the sequence of events, you can delay your command until the sequence engine is actually empty, avoiding a sequence collision and perhaps significantly grave consequences. In addition to understanding current and future states of the spacecraft, it is essential to understand and communicate about the interactions of flight and ground states and systems.

The interactions of the attitude control and navigation teams supporting a spacecraft intended to orbit another planet provide an excellent case study of the need to maintain situational awareness of interactions and what can happen when you do not. The navigation team is responsible for determining the spacecraft trajectory, designing maneuvers to maintain its course and inserting it into an orbit around the planet. A major input to their calculations comes from the tracking data they receive. This includes range information, Doppler data and delta-differenced one-way ranging (DDOR) to name a few. However, there are forces at work on the spacecraft that are hard to model with just radiometric data, such as non-gravitational forces and the forces caused by angular momentum desaturation maneuvers. Fortunately, these can be determined by the attitude control system (ACS) and passed on to the navigation team. The navigation team would normally enter these as inputs to their software and model their effects. This permits calculation of the trajectory with greater certainty. There are a couple of caveats though — the units must be known and the format must be readable by the navigation software. These are controlled by an interface specification between the two teams. In the situation we are considering, these were specified, but the specification was not followed, a fact not discovered until a mishap investigation was conducted.

How could situational awareness have helped avoid the catastrophe that occurred? It turns out there were numerous opportunities for the navigation team to be involved in reviewing and testing the interfaces and thus maintaining their situational awareness. A discrepancy between the delta-Vs expected by the navigation team and those produced by the ACS tools was only identified in an e-mail some five months before the scheduled orbit insertion and the navigation team failed to write an official anomaly report to document the discrepancy and its resolution. The situation did not become any clearer when the navigation team identified errors in the

small forces impulse data. There were several informal e-mail messages back and forth between the navigation team and the spacecraft team in an attempt to resolve the errors; however, a formal anomaly report was not written and the investigation was never completed.

It was also found later that some members of the spacecraft team had little understanding that the estimated delta-Vs derived from the small forces impulse data were a direct input to the orbit determination process and that the spacecraft trajectory was sensitive to very small (millimeters per second) velocity errors. Navigation team members were also largely unfamiliar with many of the relevant properties of the spacecraft. Without this understanding, the navigation team incorrectly assumed that the delta-V component uncertainties were small, spherically distributed, and uncorrelated. Contrary to established practice, the project did not require an update to the navigation accuracy analysis prior to launch to represent the true spacecraft design and operational expectations. This sequence of events points to ample opportunities to communicate and improve situational awareness and resolve the discrepancy that ultimately resulted in a periapsis altitude of approximately 60 km *versus* the targeted 160 km. As a result, the spacecraft was presumed to have taken up permanent residence on the planet's surface. Not only is communication between teams essential for situational awareness but also an understanding of the way a spacecraft performance evolves as process and configuration changes are made. Perhaps a better understanding of this aspect of situational awareness can be seen by examining an event where it could have prevented the loss of a spacecraft.

The spacecraft we are considering has two processors that operate in parallel with one in control. During a safe mode recovery, it was discovered that the high gain antenna (HGA) had moved through an area that was thought to be obstructed. In the process of testing this obstruction, several parameters were modified including the contingency mode HGA elevation angle. Identical values were subsequently stored in both processors. A few days later, the non-controlling processor entered contingency mode (an intermediate response to a perceived anomaly prior to entering safe mode). Due to a lack of telemetry, the ground was not aware that the non-controlling processor had entered contingency mode and was no longer executing sequences or accepting commands from the ground. Commands were sent to both sides of the spacecraft to configure it for normal mapping, including the contingency mode HGA elevation angle. The new values, now loaded in only one processor, differed by 0.00011 degrees from what had been stored in both processors, insignificant as far as performance was concerned. A subsequent memory readout showed the difference between the two processor's parameter values and about six months later, a follow-up memory readout revealed six additional miscompares between the two processors. In an effort to improve configuration control over the two processor memories, it was decided to upload correct values to both processor memories.

Because only two parameters had special commands that had been tested and used before (including the HGA elevation parameter), it was decided to use a general memory load command for the process. However, the command for the HGA elevation command was sent to the wrong starting address. Consequently, not only was the HGA elevation wrong but also the solar array gimbal soft stop enable flags used to prevent the solar array from driving into the hard stop (in an adjacent memory word) were corrupted. The memory load was built and tested in the test bed prior to sending it to the spacecraft, but a functional test was not included in the testing. What this means is they tested that the parameters were loaded in the memory locations specified but not that the spacecraft performed as expected when these parameters were used. Thus, the file lays dormant until the next entry into contingency mode.

Contingency mode was entered about five months after the file load and numerous alarms were observed. The indications were that the solar array gimbals were the problem and they had swapped to the alternate set of gimbals. The spacecraft subsequently went to an orientation that pointed the HGA away from Earth and placed one of its batteries in direct view of the sun. The end result was an inability to communicate with the Earth and a discharge of the battery, estimated to take several orbits. Once the chain of events was set in place, the conditions were such that recovery of the spacecraft was very unlikely. However, if the flight team had been aware of the situation that the HGA parameters did not need to be updated, *i.e.* even though the parameters were in disagreement, the difference was negligible, the resultant memory corruption could have been avoided and the spacecraft would not have been lost.

The conditions discussed above show the breadth to which the flight team must be aware of the situation surrounding current operations as well as the spacecraft environment and state. Maintenance of situational awareness could have prevented the loss of a number of spacecraft. Fortunately, not all lapses in situational awareness lead to the demise of a spacecraft, but clearly a cornerstone of operational excellence is situational awareness.