National Aeronautics and Space Administration

NASA Engineering and Safety Center Technical Bulletin No. 23-02

Safety Considerations when Repurposing Commercially Available Flight Termination Systems from Uncrewed to Crewed Launch Vehicles

Both uncrewed and crewed launch vehicles (LV) require Flight Termination Systems (FTS) for Range Safety to protect the public and ground assets in the event of a LV failure. Flight crew safety in this context is an added consideration for human spaceflight. The FTS is an electroexplosive system that activates destruct charges to rupture propellant tanks and shut down engines during flight termination. Commercially available FTS units have been developed for uncrewed applications and are now being repurposed to crewed applications. A consequence of using these systems is that they are designed for public and ground crew safety, though inadequate for flight crew safety. Missing are Human Space Flight (HSF) design controls for inadvertent activation during crewed ascent and protection for crew emergency abort.

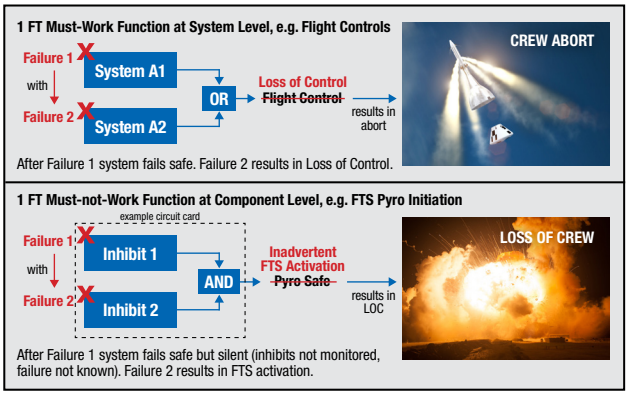
Background

The pyrotechnic initiation circuits, and software for autonomous FTS, in commercial uncrewed FTS are designed to prevent "failure-to-operate" (i.e., must-terminate) during the flight phase but lack standard protections found in crewed system to prevent inadvertent fire because they were designed to Space Force (SF) Range requirements without consideration to NASA crew safety requirements. The FTS is a fail-destruct system (i.e., as opposed to fail-safe), so in the case of crewed flight, inadvertent fire of the FTS system would circumvent the emergency escape system designed to allow crew survival. For this reason, NASA standards require the design to be two-fault tolerant to inadvertent fire when that failure mode leads directly to loss of crew (catastrophic hazard). While the prevention of failure-to-operate can be met with redundant strings, prevention of an inadvertent terminate relies on protection within the unit/string, meaning inadvertent fire controls must be included within each unit. System-level redundancy cannot address this hazard. In addition, there are other requirements levied for crewed missions during the ascent that the SF Range only requires to be active when ground crews are in and around the LV during prelaunch operations.

Best Practices for Crewed FTS Designs

Design features employed by both the military and NASA to prevent inadvertent fire are shown in the table below, while must-work versus must-not-work fault tolerance considerations for crewed vehicles are shown in the figure below.

Human Rated Design Features Checklist to Prevent Inadvertent Fire
Arm only when fire is imminent
Two-fault tolerance to Inadvertent Fire by inspection
Physical design separation and independence of FT strings
Isolation from other systems
Inhibit protections and monitoring
Independent monitoring of software functions
Activation margin controls internal to firing circuit



While these are common hazard controls for HSF safety and are employed both by NASA and the SF Range, there is a difference between how and when the organizations apply these requirements. For example, the SF Range also requires an FTS arm switch, but allows it to be resident in ground service equipment and eliminated when ground crews clear the launch site. This hazard control approach is effective for ground crew but not flight crew. Similarly, the SF Range requires monitoring of safety inhibits, but only those inhibits engaged while on the ground. The range does not require the in-flight inhibits (fire command) to be monitored since an inadvertent FTS activation in flight threatens neither the public nor the launch-site ground crew, which is the focus of their requirements.

Summary

The SF Range Safety requirements are not an alternate for NASA's crew safety requirements. As in the case for the Space Shuttle and other NASA programs, both SF Range and NASA crew safety requirements sets can and should be met to afford the flight crew a level of hazard control on par with what has traditionally been afforded NASA flight crews and what is required by the range for ground crews.

Definitions

Arm: In the electrical firing circuit, the arm inhibit is upstream of the serial fire inhibits. The fire command provides the final application of power to the electroexplosive device. The electrical circuit arm is the preliminary state which must be transitioned just prior to firing pyrotechnics. It is the final application of power to the last remaining fire inhibits prior to firing pyrotechnics, as well as the powering up of the control logic (inhibit field effect transistor gate drive and decisional logic) that services those final terminate/fire inhibits. Ideally this function is physically located in a separate assembly.

Two-Fault Tolerance: Required for explosive systems (e.g. FTS, which is fail-destruct) due to the potential of circumventing crew survival emergency systems. NASA legacy fault tolerance requirement for catastrophic hazard without use of emergency systems applies to the FTS case.

References

1. JSC 62809 Human-rated Spacecraft Pyrotechnic Specification
2. LLIS 30602 NASA's Entry into Commercial Space – DDT&E Lessons Learned, ntrs.nasa.gov/citations/20210023013
3. NESC Technical Bulletin TB 20-01, Latching Safety-Critical Signals in Pyrotechnic Circuits. www.nasa.gov/nesc/technicalbulletins
4. Design Development Test and Evaluation (DDT&E) Considerations for Safe and Reliable Human Rated Spacecraft Systems, NASA/TM-2008-215126/Vols I & II. ntrs.nasa.gov/citations/20080019635 ntrs.nasa.gov/citations/20080019636

For information, contact thomas.k.evans@nasa.gov, christopher.j.iannello@nasa.gov or robert.f.hodson@nasa.gov