National Aeronautics and Space Administration

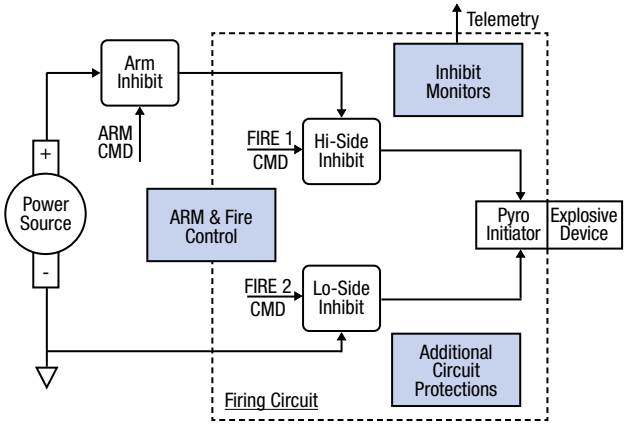
NASA Engineering and Safety Center Technical Bulletin No. 23-01

Including Key Design Features in Safety-Critical Pyrotechnic Firing Circuits

Pyrotechnic systems often fall into a unique category in that inadvertent activation of these systems resulting from a fault and/or lack of safe margins can lead directly to loss of crew. For example, untimely activation of pyrotechnics used for a flight termination system could override an abort capability. Over the years, NASA and the military have learned lessons about safe pyrotechnic circuit design and test, many of which are codified [1][2][3][4]. However, with NASA's recent efforts to move toward a development model that leans more heavily on Commercial Partners, these requirements have not always been directly levied on projects, and in some cases have been misinterpreted. This bulletin describes key safety features of pyrotechnic firing circuit design and provides rationale for inclusion of each feature.

Background

The diagram below shows a simplified best-practices firing circuit depicting multiple inhibits, monitoring, and other protections.



Notional Pyrotechnics Firing Circuit

Recommendations/Best Practices for Key Safety Features

1. **Two-Fault Tolerance** - Human space flight (HSF) systems should include sufficient inhibits to provide protection against inadvertent activation such that no two faults can result in loss of crew. Two-fault tolerance is required to prevent failure modes from defeating not only system level redundancies designed to enable mission completion, but also emergency systems designed to respond to catastrophic events in progress and enable crew survival. Two-fault tolerance is the front line of protection and can often be implemented with minimal hardware impact. For context, in recent HSF systems with a "fail-destruct" design, i.e., one-fault tolerant, "inadvertent activation" failures were not classified as unique, allowing the system to be only single-fault tolerant to inadvertent fire. Nonetheless, these systems were compliant with requirements for one-fault tolerant, fail-safe systems. For a fail-destruct system design, this meant direct loss of crew events could occur after a second failure. Whereas in two-fault tolerant systems, after the second failure there is still an emergency system (i.e., abort) designed to allow crew survival.
2. **Arm Only When Firing** - Arm the firing circuit only when firing is imminent. This is effectively design guidance for the first in the series shown in the diagram and ensures the firing circuit in the dashed box remains deenergized unless and until firing is intended. As context, in recent programs this arm inhibit function has not been implemented as the conventional successive application of power. Instead, it has been allowed to reside within ground service equipment as a ground crew safety feature or controlled via software with the firing output energized up to the final inhibits, i.e., power always applied up to the Hi-Side Inhibit in the diagram and ready-to-fire, regardless of intent. By using the staged application of power, we can use the precursor arm state as proof positive of a potential impending fire.
3. **Inhibit Monitors** - Monitoring circuits are critical to having insight into the health of inhibits that prevent inadvertent activation. Without these circuits the system's fault tolerance cannot be fully verified on the configured system. Traditionally, to qualify as a safety-critical inhibit, the state of that inhibit must be monitored.
4. **Fault Containment Regions** - To the extent possible both electrical and physical isolation are needed to contain faults. Fault containment regions (FCRs) should be designed in. The power and arming system should reside in separate FCRs. The hi-side and lo-side paths including control logic should also be isolated to prevent fault propagation and cascading or common-mode faults.
5. **Know Your Margins** - Margins on signals should be verified by test or analysis to ensure spurious noise will not initiate the pyrotechnics. On the firing lines, 16.5dB of margin to the no-fire limit of the initiator is required for human-rated system, and 6dB margin is required on control paths to firing circuits.

There are other recommended protections, tests, and procedures described in JSC 62809 that increase safety and mitigate inadvertent activation of pyrotechnic systems. For crewed programs and projects requiring safety critical pyrotechnics, the key electrical firing circuit design principles and hazard controls documented in JSC 62809 should be levied as a requirement.

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.

NESC tech bulletin