National Aeronautics and Space Administration

NASA Engineering and Safety Center Technical Bulletin No. 24-05

Key Considerations When Developing Avionics for Safety-Critical Systems

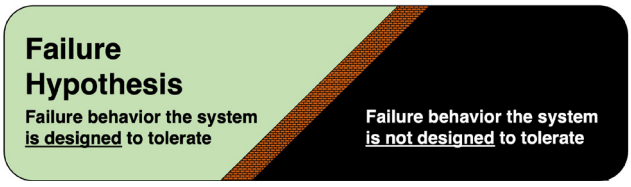
Multiple human spaceflight programs are underway at NASA including Orion, Space Launch System, Gateway, Human Landing System, and EVA and Lunar Surface Mobility programs. Achieving success in these programs requires NASA to collaborate with a variety of commercial partners, including both new spaceflight companies and robotic spaceflight companies pursuing crewed spaceflight for the first time. It is not always clear to these organizations how to show their systems are safe for human spaceflight. This is particularly true for avionics systems, which are responsible for performing some of a crewed spacecraft's most critical functions. NASA recently published guidance describing how to show the design of an avionic system meets safety requirements for crewed missions [1].

Background

The avionics in a crewed spacecraft perform many safety-critical functions, including controlling the position and attitude of the spacecraft, activating onboard abort systems, and firing pyrotechnics. The incorrect operation of any of these functions can be catastrophic, causing loss of the crew. NASA's human-rating requirements describe the need for "additional rigor and scrutiny" when designing safety-critical systems beyond that done for uncrewed spacecraft [2]. Unfortunately, it is not always clear how to interpret this guidance and show an avionics architecture is sufficiently safe. To address this problem, NASA recently published NASA/TM−20240009366 [1]. It outlines best practices for designing safety-critical avionics, as well as describes key artifacts or evidence NASA needs to assess the safety of an avionics architecture.

Failure Hypothesis

One of the most important steps to designing an avionics architecture for crewed spacecraft is specification of the failure hypothesis (FH). In short, the FH summarizes any assumptions the designers make about the type, number, and persistence of component failures (e.g., of onboard computers, network switches). It divides the space of all possible failures into two parts – failures the system is designed to tolerate and failures it is not.



The Failure Hypothesis splits the space of all possible failures into two parts.

One key part of the FH is a description of failure modes the system can tolerate – i.e., the behavior exhibited by a failed component. Failure modes are categorized using a failure model. A typical failure model for avionics splits failures into two broad categories:

- Value failures, where data produced by a component is missing (i.e., an omissive failure) or incorrect (i.e., a transmissive failure).
- Timing failures, where data is produced by a component at the wrong time.

Timing failures can be further divided into many sub-categories, including:

- Inadvertent activation, where data is produced by a component without the necessary preconditions.
- Out-of-order failures, where data is produced by a component in an incorrect sequence.
- Marginal timing failures, where data is produced by a component slightly too early or late.

In addition to occurring when data is produced by a component, these failure modes can also occur when data enters a component (e.g., a faulty component can corrupt a message it receives). Moreover, all failure modes can manifest in one of two ways:

- Symmetrically, where all observers see the same faulty behavior.
- Asymmetrically, where some observers see different faulty behavior.

Importantly, NASA's human-rating process requires that each of these failure modes be mitigated if it can result in catastrophic effects[2]. Any exceptions must be explicitly documented and strongly justified.

In addition to specifying the failure modes a system can tolerate, the FH must specify any limiting assumptions about the relative arrival times of permanent failures and radiation-induced upsets/errors or the ability for ground operator to intervene to safe the system or take recovery actions.

For more information on specifying a FH and other artifacts needed to evaluate the safety of an avionics architecture for human spaceflight, see the full report [1].

References

1. R. F. Hodson, A. Loveless, W. Torres-Pomales, and P. S. Miner, "Failure-Tolerant Avionics for Crewed Space Systems: Recommended Best Practices," National Aeronautics and Space Administration, NASA/TM−20240009366, Jul. 2024.
2. "Human-Rating Requirements for Space Systems," National Aeronautics and Space Administration, NPR 8705.2C, Jul. 2017.

For more information, contact Robert F. Hodson robert.f.hodson@nasa.gov. nesc.nasa.gov
10/30/24 DOC ID: 20240013463