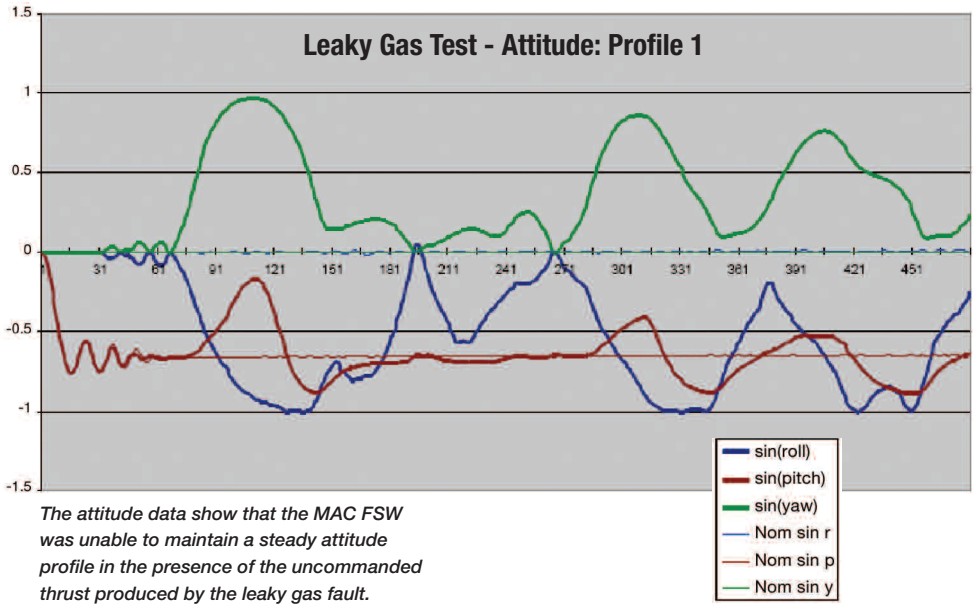
Empirical Assurance of Embedded Software Using Realistic Simulated Failure Modes

Ken Chen, *Johnson Space Center*
Ted Bennett, *Triakis Inc.*

We have created a virtual system integration laboratory (VSIL) simulation of the Johnson Space Center Mini-AERCam nanosatellite from project documentation to explore the concept of failure mode effects testing.



The attitude data show that the MAC FSW was unable to maintain a steady attitude profile in the presence of the uncommanded thrust produced by the leaky gas fault.

The Mini-AERCam VSIL supports the execution and test of flight software without the need for external test equipment or other hardware. As such, it provides an ideal tool for software quality assurance (SQA) groups to improve their effectiveness by conducting software testing rather than relying exclusively on analysis tools and process monitoring. This domain has historically been inaccessible to them due to the high cost of procuring their own system integration lab (SIL), and limited availability of project-level SILs for their use.

With the opening of the flight software (FSW) testing domain to SQA teams using a VSIL, some of the unique capabilities of this virtual environment may be applied to ease, complement, or supplant laborious analysis activities such as failure modes and effects analysis (FMEA). Failure modes may be modeled as intrinsic characteristics of parts within the virtual environment that can be manifested as desired during the execution of test scenarios. We refer to these as "enhanced" failure modes because they are generally difficult or cost-prohibitive to produce in a hardware SIL, but readily achievable in a virtual environment simulator.

Invoking failures in simulated parts during test most closely mimics how the FSW would encounter such an event in an operational setting. Observing/measuring the behavior of the FSW and system in response to a failure condition is the surest way to verify conformance to a requirement. This ability confers less need for reliance on analysis, and more flexibility and realism in the evaluation of the effects of failure modes. For this effort, our selection of failure modes was drawn from the list of those analyzed as part of the safety and mission assurance team's Mini-AERCam FMEA activity.

The engineering team may use this tool to test the requirements and design as they are being developed to probe for weaknesses, inconsistencies, completeness, etc. Testing the system requirements and design early on leads to improved robustness and fewer downstream design changes, thereby reducing risk, costs, and negative schedule impact. Having the system design simulated helps eliminate errors in understanding due to ambiguities and misinterpretation of written specifications among engineering team members and between the design authority and contractors.