Journal of System Safety
eEdition
A publication of the System Safety Society

President's Message
From the Editor's Desk
TBD
In the Spotlight:
Considering System Risks
Redundancy for Safety
Gains from Losses:
System Safety and Aging Systems
Tech Corner
Chapter News
Mark Your Calendar
About this Journal
Classifieds
Advertising in eJSS
Contact Us
Puzzle

Vol. 45, No. 3 • May-June 2009

Gains from Losses: System Safety Commentary on Accidents and Other Events

System Safety and Aging Systems

by John Livingston

Pages 1 | 2

One of the challenges for the space shuttle program is assessing the effectiveness of hazard controls and risk analysis based on flight performance. Each mission seems to have a new set of anomalies that must be given a thorough review before the next mission is to fly. For example, the space shuttle mission (STS-119) scheduled for February, 2009 was delayed to assess a hardware failure that occurred on the previous space shuttle mission (STS-126) in November, 2008.

A change in the flight performance of the system that maintains the pressure in the liquid hydrogen tank during ascent led to a post-flight system inspection that identified a failure of a poppet in one of the hydrogen flow control valves (FCVs) used in the system. The poppet was cracked and a small piece was missing [Ref. 1]. The fact that this was a first-time flight failure of this component was somewhat offset by the fact that the valve that experienced the material release was not the one in the inventory with the most flight exposure.

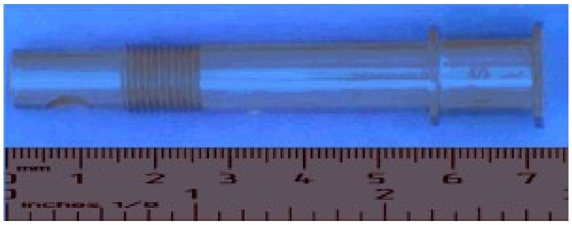

Figure 1 — GH2 Flow Control and Valve Poppet.

Figure 2 — STS-126 Valve Poppet Following Removal.

During space shuttle main engine (SSME) operation, gaseous hydrogen from the SSME's low-pressure fuel turbopump is fed back to the external tank (ET) liquid hydrogen tank to maintain proper tank pressure. The flow control valve operation is triggered by liquid hydrogen pressure transducers in the tank. When tank pressure decreases below 32 psia, the valve opens; when tank pressure increases to 33 psia, the valve closes [Ref. 2].

Such a failure of the poppet has two undesirable effects: The valve loses its ability to control the hydrogen flow (potential for increased system pressure), and debris is liberated into the system [Ref. 3].

High hydrogen flow into the ET liquid hydrogen tank could potentially lead to excessive pressure within the tank. The liquid hydrogen tank is protected from over-pressurization by a relief valve, but venting of hydrogen external to the vehicle during early ascent (less than 120 seconds of flight) has the potential for hydrogen ignition. It should be noted that the system has three FCVs and is designed to tolerate one FCV failed high without activation of the relief valve (initiating the venting). The nature of the failure does raise concerns about the potential for a common-cause failure mode that might affect more than one FCV poppet [Ref. 3].

The release of the debris could result in restricted flow or impacts to lines and other system components. Fortunately, analysis confirmed that even the release of the total poppet head would not restrict the flow to the point that the fuel tank pressure would fall below its lower limits. The main concern was the potential for debris to penetrate system lines, leading to over-pressurization of the ET intertank area or the Orbiter aft compartment. The release of hydrogen into those areas also had to be evaluated for the threat of a hydrogen-fed fire.

While the failure was quickly confirmed as fatigue related, the relationship of the contributing factors was not as clear. The leading theory for most probable cause was that an acoustic environment frequency mode was coupling with a structural poppet mode to induce the crack initiation and the resulting fracture of the poppet head [Ref. 3]. Analyses were undertaken to assess the contributing factors, including the potential for orbiter-to-orbiter variations in the acoustical environment characteristics. Although the three valves are in close proximity to each other, they are each fed by a hydrogen gas flow from a different SSME, which might also contribute to different "environmental" conditions.

> “The failure could not be explained by an obvious 'smoking gun' that made the failed poppet unique from other poppets in the flight hardware inventory.”

Nothing in the poppet's manufacturing history, material pedigree or general physical condition appeared to single it out from the other poppets. The failure could not be explained by an obvious "smoking gun" that made the failed poppet unique from other poppets in the flight hardware inventory.

Preliminary structural analyses bound the worst-case circumference for material loss to between 90 and 180 degrees. This raised the concern that a failure could result in the release of a fragment that was larger than that released on STS-126.

To assess particle impact concerns, engineering analyses were performed in parallel with related additional testing. A flow field and particle trajectory analysis was performed. Initial analysis results revealed areas of marginal structural capability of withstanding an STS-126-sized piece, which led to additional efforts to develop a more refined analysis. In addition, impact testing was conducted at several different NASA centers to verify the analysis results.

Initial inspection of the FCVs in the flight inventory identified only one FCV with a very fine crack. The FCV had flown 16 times on two different orbiters, in three different system locations. Inspection of the crack structure revealed that at least one flight was flown with the crack condition. A fracture induced in the cracked poppet resulted in surface failure similar to the STS-126 failure [Ref. 3].

The initial inspections were done with a SEM (scanning electron microscope), which provided extremely high resolution, but further investigation of the technique disclosed that surface conditions, including marks from the machining process used in the valve manufacturing, could mask small cracks in the valve poppets [Ref. 4].

Because of the concerns about the SEM limitations, eddy current inspections were initiated. Eddy current is a non-destructive evaluation (NDE) method that uses electromagnetism properties for conducting examinations. It is most effective in detecting surface and near-surface defects. The eddy current test identified several other FCVs with small cracks and greatly aided the selection of candidate STS-119 FCVs that were "low" flight-time items without detectable cracks [Ref. 5].

next page »

Journal of System Safety
eEdition
A publication of the System Safety Society

Vol. 45, No. 3 • May-June 2009

Gains from Losses: System Safety Commentary on Accidents and Other Events

System Safety and Aging Systems

by John Livingston

Pages 1 | 2

To assure that a similar hazard potential did not exist for the External Tank LOX tank pressurization system, its design and operational history were reviewed. While oxygen system (GO2) flow control valves had a similar exposure to environmentally induced high cycle fatigue, there was at least one key design difference. The GO2 poppet material is Monel, which is more ductile and tougher than GH2 poppet material [Ref. 3].

The final rationale behind the decision to launch STS-119 was based on the confidence that the eddy current testing would reveal any signs of cracking in the FCV valves (down to very small indications), and that crack growth/propagation analysis tools had concluded that the cracks below the detection level would not propagate to failure within the span of a single-flight operation [Ref. 5].

The STS-119 was successfully launched on March 15, 2009. Main fuel system performance during ascent indicated nominal hydrogen flow control valve performance. Within a few days after the orbiter's return, the hydrogen flow control valves were removed and inspected. No cracks were found in the initial inspection.

The shuttle program now has to address the longer-term use issue. Should the FCVs be redesigned to address the current design shortcomings? How quickly can that be done? The program has less than two years left. While picking the "best" hydrogen flow control valves may address the probability of debris being generated, it does not address the other component of risk — the effect. There are some members of the program team who continue to push for installation of special "doubler" plates to re-enforce the first 90-degree bend in the hydrogen piping, which is in the direct path of any released FCV debris. The objective is to increase the elbow's resistance to penetration by the debris (reducing the potential for line failure [leakage]). The challenge is to develop a design that is both effective and non-intrusive.

Understanding the effects of "aging" systems is not just a space shuttle program concern, nor even just a NASA agency-level effort. Concerns about military and commercial aircraft aging issues have grown during the past few years as many different aircraft have been subjected to extended operational lives.

The U.S. Air Force has done a number of studies on the challenges of operating aging aircraft in an operational force. In 1997, the National Research Council Committee on Aging of U.S. Air Force Aircraft issued a report that addressed the threat of structural deterioration of U.S. Air Force aircraft. Among its many conclusions and recommendations, it noted that "the inexorable increase in the number of fatigue-critical areas safe-rack-growth-designed structure and the potential for missing new areas as they develop" requires improvements in analysis techniques, supporting testing and "to improve NDE techniques that are sensitive enough to detect small cracks in multilayered and hidden structures to support safety inspections" [Ref. 6].

> “Before or after an anomaly is identified, it is important that the system safety analyst understands the strengths and limitations of any inspection technique. While the inspection equipment pedigree might be impressive, it is the results that count.

In March, 2006, the FAA issued a fact sheet that gave an overview of its Aging Airplane Program. The FAA program was initiated after the 1988 Aloha Airlines accident to address airplanes being operated beyond original design service goals,

President's Message
From the Editor's Desk
TBD
In the Spotlight:
Considering System Risks
Redundancy for Safety
Gains from Losses:
System Safety and Aging Systems
Tech Corner
Chapter News
Mark Your Calendar
About this Journal
Classifieds
Advertising in *eJSS*
Contact Us
Puzzle

and the fact that original maintenance plans were not required to address potential age-related issues. The program has been updated and expanded in a series of responses to the Aging Airplane Safety Act of 1991, the 1996 TWA 800 accident and the 1998 Swiss Air accident [Ref. 7].

impressive, it is the results that count.
”

In addition to the problems caused by aging aircraft structures, other major systems were also exhibiting the effects of extended operation. In October,1998, the FAA began the Aging Transport Non-Structural Systems program, modeled after the aging structures program.

One measure of the extent of the problem is the fact that the FAA has issued more than 700 Airworthiness Directives (ADs) to address specific safety concerns or "unsafe conditions" on specific airplane types since 1990. Areas addressed include airplane structural issues (540), fuel tank safety issues (85) and wiring safety issues (110) [Ref. 7].

Separately, the FAA has promoted safety measures through general rule-making that addresses the aging aircraft structure and wiring concerns:

- Repair Assessment Program Rule (RAP) — April 19, 2000
- Fuel Tank Safety Rule (FTS) — April 19, 2001
- Aging Airplane Safety Rule (AASR) — January 25, 2005
- Enhanced Airworthiness Program for Airplane Systems (EAPAS) — September 22, 2005
- Widespread Fatigue Damage (WFD) — April 18, 2006

The FAA program continues to develop with new requirements and rules. A new rule issued in December, 2007, requires holders of design approvals to give aircraft operators access to damage tolerance data for repairs and alterations to fatigue-critical airplane structure [Ref. 8].

Finally, one online source of information for the different studies on aircraft aging is the annual Aircraft Aging Conference, now in its 12th year. Papers (and presentations) from the 2008 conference can be found at http://www.aaproceedings.utcdayton.com/. The range of papers and the organization involved are quite impressive.

What does all of this mean to a system safety analyst supporting a program with an extended operational life? First, the system safety analyst must keep in close touch with the performance of the hardware in the field. It is also important to be in constant communication with the reliability analysis team. The analyst needs a clear understanding of the hardware's expected life, as well as any analysis and/or testing done to support extensions of the system's operational life.

Before or after an anomaly is identified, it is important that the system safety analyst understands the strengths and limitations of any inspection technique. While the inspection equipment pedigree might be impressive, it is the results that count.

The recent NASA experience with the STS-126 flow control valve poppets and the general experience with aging DoD and commercial aircraft have re-enforced the need for increased vigilance in the operation of aging hardware. There is a need for better information gathered by increased numbers of inspections and the use of improved inspection techniques to identify developing conditions. There is also a need for analyses that address the potential safety issues with aging systems.

Hazard analysis and any related risk assessments should never be allowed to become stagnant. System operations can reveal unanticipated hazard causes and unexpected shortcomings in hazard controls and/or associated verifications of hazard control functions or activities.

The system safety analyst must also be wary of temporary or emergency design "fixes" that tend to become permanent. Managers of programs in the final stages of a system's life-cycle are generally reluctant to make extensive (or expensive) design changes to address root causes. They are more likely to utilize expanded analysis and increased hardware inspections to address aging hardware issues.

References:

1. NASA Summary Sheet. "Gaseous Hydrogen Flow Control Valves," National Aeronautics Space Administration, Washington, DC, February 2009.
2. Shuttle Reference Manual. National Aeronautics Space Administration, Washington, DC, 1988.
3. Bergin, Chris. "Understanding the Threats — FCV Flight Rationale Effort Outlined," NASA Spaceflight.com Web page (http://www.nasaspaceflight.com), Feb. 5, 2009.
4. "Examiner Exclusive 2: NASA Pressure Builds with Critical Valve Problems Dating Back to 1992," http://www.insideksc.com, Feb. 7, 2009.
5. Bergin, Chris. "FRR Clears STS-119 for March 11, Pending SRB Resolution," NASA Spaceflight.com Web page (http://www.nasaspaceflight.com), March 6, 2009.
6. Committee on Aging of U.S. Air Force Aircraft, Commission on Engineering and Technical Systems. "Aging of U.S. Air Force Aircraft: Final Report," National Research Council, National Academy of Sciences, Washington, DC, 1997.
7. FAA Fact Sheet. "FAA's Aging Airplane Program," Federal Aviation administration, Washington,

DC, March 29, 2006.
8. Schneider, Greg. "New Part 26 DAH Rule, Damage Tolerance Data for Repairs and Alterations," DAH Familiarization Briefing for Part 26 DAH Rule (AASR), Cologne, Germany, Dec. 14, 2007.

« previous page