Re: Saturn V

Source: http://sci.tech−archive.net/Archive/sci.space.history/2006−05/msg00663.html

- *From*: columbiaaccidentinvestigation@xxxxxxxxx
- *Date*: 24 May 2006 20:29:35 −0700

> "And losing seven astronauts in a Shuttle accident >wouldn't put a crimp in Shuttle flights if we were >rational about it."

When analyzing the safety of a space program the application of Murphy s Law, is should be the dominating rule. Calculating risks for vehicle or mission failure depends on the combined risks for the many components of the vehicle, all with varying degrees of criticality. A vehicles structural integrity, propulsion, guidance and navigation, all must function properly for a successful safe mission and return of astronauts. The practice of risk analysis is not just hypothetically and recklessly stating a failure rate, it is a methodical statistical approximation, based on careful examination of the elements comprising the vehicle.

Managing and understanding risks for better safety has a long history in many industries, but a great place to start for understanding risk management in our space program is the oral history interview with a Dr. Levine, or a visit to onlineethics.org where Roger Boisjoly can be found. Dr. levine and people like roger boisjoly are some of the many unsung heroes behind our space program, as they have spent their careers trying to maintain the highest levels of integrity in engineering and design, and must be respected.

http://www.jsc.nasa.gov/history/oral_histories/LevineJH/JHL_7−12−01−amended..pdf
Johnson Space Center Oral History Project
Oral History Transcript
Joseph H. Levine, Interviewed by Kevin M. Rusnak Houston Texas 12 June 2001

http://onlineethics.org/moral/boisjoly/RB−intro.html
Boisjoly, Roger M. 1987. Ethical Decisions −− Morton Thiokol and the Space Shuttle Challenger Disaster. American Society of Mechanical Engineers Annual Meetings

The failure mode and effect analysis was used to generate the number of components on the critical items list or (cil) for the space shuttle programs original design in order to meet many of the aerospace safety panels standards for manned space flight. An independent investigation conducted post challenger contained many recommendations including a new fmea for the space shuttle program.

http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19880010818_1988010818..pdf

This newly conducted fmea revised and increased the cil as can be seen in this report for the hydraulic system.

http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19800070348_1980070348..pdf

This following link shows a cil fmea on a et/orbiter lh2 recirculation valve

http://www.jsc.nasa.gov/news/columbia/nsts08399/book00/part3/031040502.pdf

But the shortcomings for calculating mission failure probabilities by using the fmea only are cited in the following paper.

Probabilistic Risk Analysis for the NASA Space Shuttle:
A Brief History and Current Work by Elisabeth Paté−Cornell, Stanford University,
and Robin Dillon, Virginia Tech Submitted for publication in
Reliability Engineering and System Safety April, 2000

The shuttle independent assessment team of 2000 refers to a safety practice in the airlines known as MEDA or the maintenance error decision aid. One of the ideas in the philosophy that statistical analysis has shown there are usually at least three to four contributing factors to maintenance errors, and most of the contributing factors are under the control of management, and therefore can be prevented. The consequences of human errors such as dives and catches cited in the siast 2000 were not reflected in the fmea, or the cil and therefore nasa mission managers were relying on failure probabilities that did not reflect reality.

Space Shuttle Independent Assesment Team
appendix human factors 91 par 3
Maintenance Error Decision Aid (MEDA)
The Maintenance Error Decision Aid (MEDA) process was developed as an aid to investigating the
causes of maintenance and inspection errors. Boeing, working with three of its customers, British
Airways, Continental Airlines, and United Airlines, developed and tested the MEDA process from 1992
through 1995. Since 1996, Boeing has provided MEDA implementation support to over 120 aircraft
maintenance and engineering organizations worldwide.

The MEDA philosophy is:
. Mechanics/engineers/inspectors do not make errors on purpose
. Errors are due to a series of related, contributing factors in
the mechanic/engineer/inspector s
work area
. Most of these contributing factors are under the control of
management and can, therefore, be
improved to prevent future, similar errors.
Contributing to maintenance errors are a wide range of factors
including 1) Information, 2)
Equipment/tools, 3) Aircraft design/configuration/parts, 4) Job/task,
5) Technical knowledge/skills, 6)
Individual factors, 7) Environment/facilities, 8) Organizational
factors, 9) Leadership/supervision, 10)
Communication. Existing data suggest that on average there are three to
four contributing factors per
maintenance error.

Now quantitative risk assessments (qra) s are not easy, and expensive, but are now the best way for a particular systems safety to be understood, and have realistic failure probabilities. This is done because the qra uses the Bayesian method for data collection, meaning new data is included as it becomes available as in tracking of the in flight anomalies, general maintenance and corrective actions for the space shuttle orbiters. The probable risk assessment guide for nasa written 2002, shows the progression of risk assessment methods for nasa.

http://www.ece.mtu.edu/faculty/rmkieckh/aero/NASA−PRAGUIDE.PDF

Murphy s Law should not be tested, and sometimes it takes the most bravery to overcome the pressures for success, and choose safety by not embarking on a mission that includes needless risks. It is the responsibility of those involved with design, manufacturing, maintenance, and use of space craft to ensure the safety of the astronauts. A civil society where the rule of law prevails (like ours), states that manslaughter charges can be filed against a person who disregards and does not correct a known safety problem, that results in death of another person. Florida legal precedent had been set by the ValuJet crash in the 90 s, and could easily apply to the launch space vehicles. The first priority of ANY private or government made expendable manned space vehicle is quality and safety, and with a reusable manned space vehicle it is quality, safety, reliability, and maintainability for we do not want to cause, or suffer a loss of crew. Trivializing death of another by anecdotes does not make it any more acceptable for life is precious, as anybody reading this will feel the same about their own life. Now when people haphazardly state failure conditions and scenarios that have not been met, and therefore declare something safe, a false sense of security starts to dominate simply because the accident has not happened yet. Designing and engineering a new space vehicle with ethical standards and practices means the making use of a quantitative risk assessment, for reaching failure probabilities with the most accurate method possible. But understanding the qra is just a tool for managing risks, and can only be as good as the data input, and the human decisions made from it, means that it in itself will not prevent another tragedy. Failure to eliminate design flaws, disregarding a no launch decision, and waiving launch protocols resulted in the death of the sts−51l crew, and loss challenger on Jan 28 1986. Simply put, if Roger Boisjoly s advice to not launch was listened to by mission managers, the challenger tragedy would not have happened and Murphy would not have won on jan 28, 1986.

.