Lost in Translation: The Case for Integrated Testing

November 2017

Aaron Young, QD35, Bastion Technologies Incorporated
Steven Novack, QD35, Bastion Technologies Incorporated

“The software did exactly what it was told to do. The reason it failed is that it was told to do the wrong thing.”

- The Coming Software Apocalypse, The Atlantic (Sept 2017)

Agenda

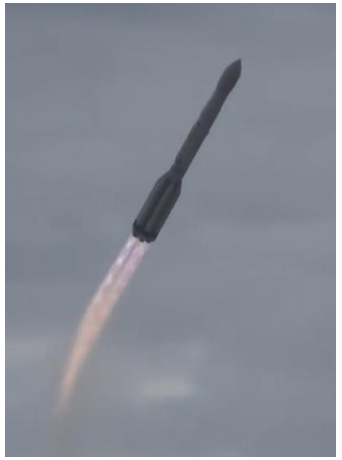
- Discuss the Genesis Accident as Lesson Learned Case Study
- Explain how errors can find their way through a program with a test plan that lacks an integrated test (i.e. *testing as you fly*).
- Demonstrate the benefits of performing an integrated test

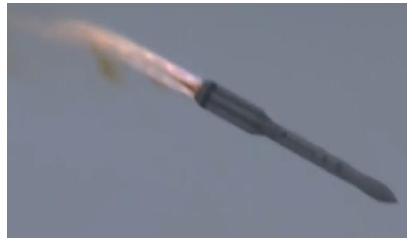
Known Polarity/Phasing Related Errors in Space Systems

System	Date	Error	Impact	Integrated test?
Chandra X-ray Telescope	1999	Sun sensor phasing error caught in post-integration testing.	Fixed prior to flight.	
Apollo LM	Ca. 1968	ICD and simulator models incorrect, driving descent engine gimbals in wrong direction.	Fixed prior to flight.	Yes
Delta Clipper (DCX)	1993	Sign error in control loop caught during integrated closed-loop suspended pendulum test.	Fixed prior to flight.	Yes
Galileo Spacecraft Probe	1995	High G and low G g-switches cross-wired.	Parachute deployed at wrong altitude but mission still successful.	
TOMS-EP	1996	Sun sensors cross-wired. Polarity on magneto-torquers reversed.	Fixed in software after launch.	
TIMED	2001	Sun sensors were mounted 90 degrees off. Polarity on magneto-torquers reversed.	Fixed in software after launch.	
Genesis	2004	G-switch installed backwards due to design error. Centrifuge test cancelled in favor of inspection.	Parachute failed to deploy. Spacecraft was destroyed.	
TERRIERS	1999	Sign flip in magneto-torquer command due to unknown cause.	Spacecraft lost.	
Proton	2013	Yaw rate gyro was installed incorrectly.	Crashed near launch pad.	

Eight known US errors in recent history (since 1986) out of less than 1000 launches (Greater than 1 in 125).

Proton 2013 Failure

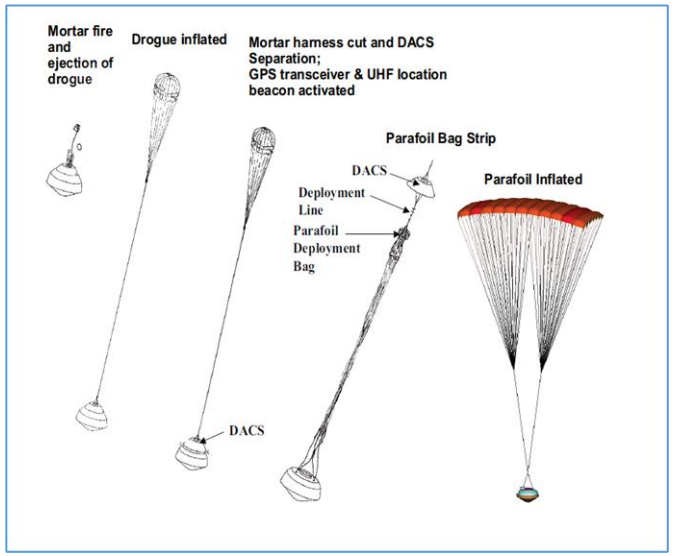




Agenda

- Genesis was the fifth in NASA's series of Discovery missions, and the first U.S. mission since Apollo to return extraterrestrial material to Earth for study.
  - The purpose of the mission was to collect samples of solar wind and return them to Earth.
- Launched August 8, 2001, Genesis was positioned approximately one million miles from the Earth orbiting the Earth-Sun libration point L1 which is outside Earth's magnetosphere.
  - It remained in a libration point orbit for 28 months. The capsule lid was closed on April 1, 2004 and the spacecraft returned for a daytime Earth entry.
- On September 8, 2004, entry occurred on time and at the nominal location to support a landing as designed.
  - Operation of the spacecraft appeared nominal until the expected deployment of the drogue parachute at approximately 108,000 ft (33 km) altitude. No drogue or parachute was observed, and the SRC impacted the desert floor at 9:58:52 MDT.

Intended Outcome



Actual Outcome

Genesis Accident – Sequence of Events

- Investigation into the accident determined that the Genesis Project had a number of interrelated issues that led to the inversion of the G-switch sensors (the proximate cause that resulted in the drogue parachute deployment mishap).
    - Equipment used on the Genesis project was based on heritage equipment, but during development, it was recognized that more functionality was required than was available from the heritage equipment, upon which its proposed design had been based, thus requiring adjustments to the design.
    - As part of the redesign, the G-switch sensor was also moved from the timer card to the relay card, since it was mounted on shock isolators and would help avoid an unintended triggering due to buffeting during the early entry or inadvertent shifting of the relay positions which concerned the designers.
    - The new design was recognized as a break with the heritage design, but this was not effectively communicated through the project personnel. Many engineers believed that the pyro initiation aspects of the design maintained their heritage.

Lessons Learned

- Root cause analysis identified the following items leading to accident:
  - Genesis Project Management and Systems Engineering did not perform due diligence with regard to reviewing briefing materials.
    - A centrifuge test to verify the directionality of the G-switch sensors had been planned, but was deleted in favor of drawing inspections.
      - The acceleration is generated by the rotary motion of a cantilever arm. The test object is installed on the mounting table at one end of the arm, and the acceleration of the test object is controlled by the rotating speed.
      - The measurement signals are monitored and recorded in the measurement room via measurement rack at the center of the rotation.

    - The only documentation indicating that Genesis Project Management or Systems Engineering had been informed of a centrifuge test deletion was a single bullet presented at two management reviews that read, *"SRC AU 3-g test approach validated; moved to unit test; separate test not required."*
      - Project Management and Systems Engineering believed that a quick-lift test had functionally and adequately replaced the centrifuge test.
      - No one above the SRC-AU Team reviewed the test plan or results, which contributed to the belief that the quick-lift test had functionally replaced the centrifuge test. This was because Systems Engineering was not required to review subsystem test procedures or verification results.
      - No documentation of the change in verification methods was generated in the form of a Change Request or Technical Memorandum. Had this been done it would have resulted in a critical assessment of the change.
    - No one recalled any discussion occurring regarding the bullet.
    - Project Management and Systems Engineering assumed that a functional replacement for a centrifuge test was to occur that would determine G-switch sensor orientation.

Lessons Learned (cont.)

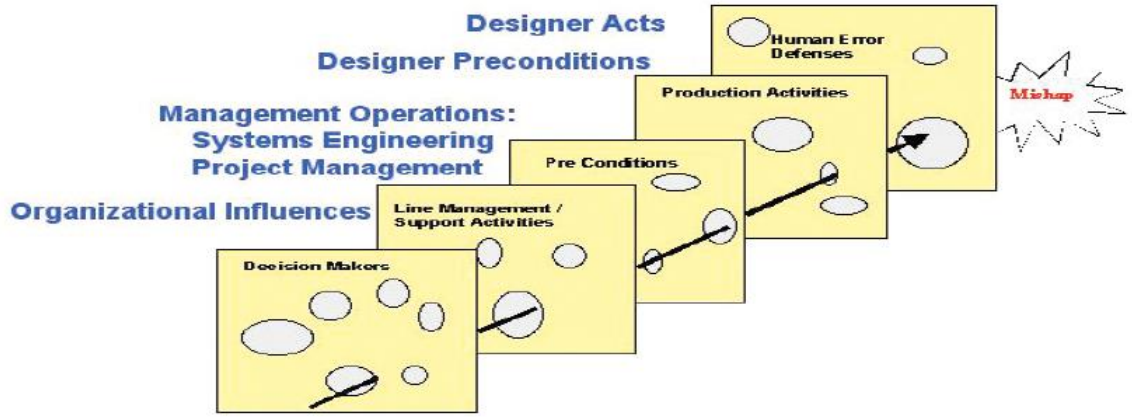
- Root cause analysis identified the following among the items leading to accident:
  - Faster, Better, Cheaper (FBC) philosophy: Cost-capped mission with threat of cancellation if overrun.
    - As proposed, selected, and confirmed on Genesis, the FBC philosophy had the following effects:

    1. Maximal science scope and focus on payload issues at the expense of the spacecraft, SRC, and ground systems.
    2. Low schedule and dollar reserves leading to significant adverse pressure on decision making.
    3. Focus on a low-risk implementation led to a reliance on heritage hardware which gave a false sense that mission risk was controlled and allowed the risks associated with the lower standards for heritage to go unrecognized.
    4. Very lean Systems Engineering team with heavy un-checked reliance on the subsystems teams for requirements and verification functions.

Estimating Risk from Human Errors

- The risk of human error is one of the primary risk drivers in any aerospace program. As a result, testing is in place that serves to catch these errors and rectify them prior to an accident occurring.

- However, developing any integrated system requires individuals from different individuals and/or organizations to collaborate. As a result, a lack of specification in procedures during development can result in a misinterpretation that leads to an error occurring.



Human Failure Event (HFE) Development

- The human failures are evaluated at a qualitative level first to determine likelihood. For events that don't screen, they are subjected to detailed quantitative analysis using the SPAR-H (Standardized Plant Analysis Risk Model Human Reliability Analysis [HRA]) method.

- The SPAR-H method was utilized to develop an Human Error Probability (HEP) for each HFE.
  - SPAR-H analyzes characteristics (Performance Shaping Factors [PSFs]) that affect an individuals ability to make a decision.
  - PSFs represent multiplying factors that are applied on baseline HEP value (1E-03).

Sample HFE Quantification

Performance Shaping Factors	PSF Level	Multiplier
Cognitive/Execution	Execution	1.00E-03
Available Time	Nominal	1
Stress	Nominal	1
Complexity	High	5
Experience/Training	Nominal	1
Procedures	Nominal	1
Ergonomics/HMI	Good	0.5
Fitness for Duty	Nominal	1
Work Processes	Nominal	1
HEP	-	2.50E-03

Recovery Actions – Benefits of an Integrated Test

- Testing or checks can serve as recovery actions to reduce the likelihood of an error occurring.

- A recovery action is defined as an action performed by personnel that serves to prevent or mitigate an error.
  - Human Reliability Analysis (HRA) methods (i.e. SPAR-H) are used in a similar manner to modeling a regular HFE.
  - The event consists of two distinct phases: 1) diagnosis/cognitive phase, and 2) execution

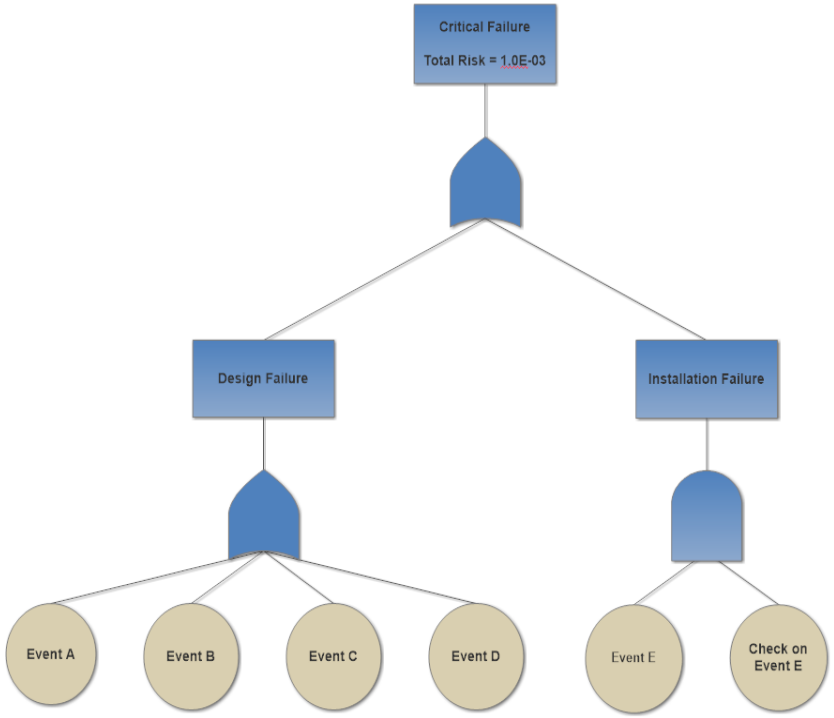
- An integrated test would serve as a check, not only on the human actions to ensure they were performed correctly, but on the entire system to check that the components are functioning accordingly.

Recovery Actions – Benefits of an Integrated Test (cont.)

- The following illustration demonstrates the effect of a recovery action on system risk with two cases.
  - The one on the left represents a case with no recovery action in place.
  - The example on the right includes the recovery action to demonstrate the effect.

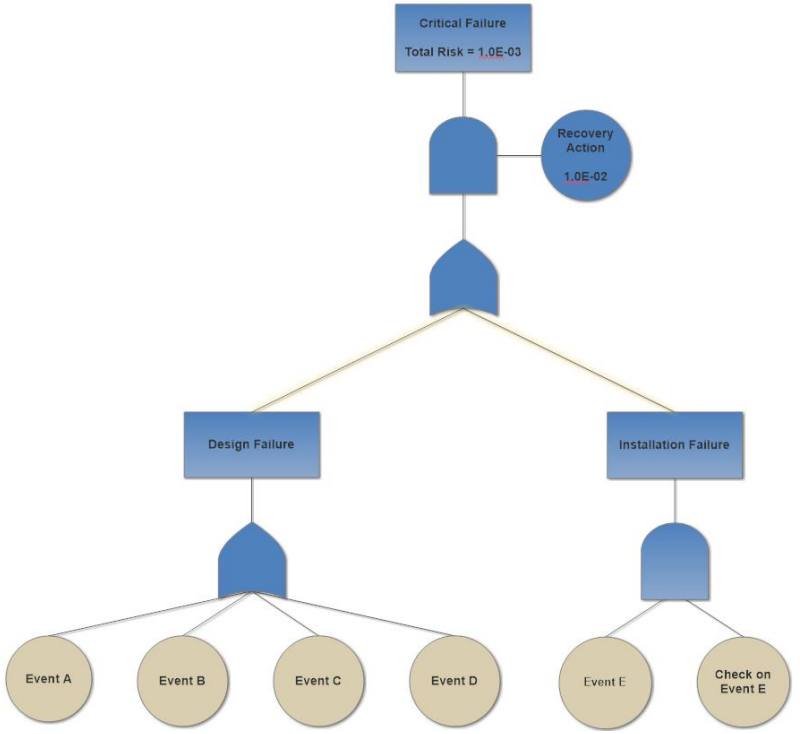
Case 1 (w/ No Recovery Action):

Risk = 1.0E-03 (1 in 1000)



Case 2 (w/ Recovery Action):

Risk = 1.0E-3 x 1E-02 = 1.0E-05 (1 in 100,000)



Summary

- The increase in complexity of systems and multiple individuals/organizations collaborating presents opportunities for additional errors to occur in the integrated design.
  - Confidence in heritage design or budgetary and/or schedule pressures present challenges that can result in eliminating or reducing critical testing.

- Performing an integrated test or “testing as you fly” adheres to best practices as shown by past programs and current spacecraft and launch vehicles.
  - Effective testing can result in a significant risk reduction of the design by orders of magnitude.
  - An integrated test eliminates gaps in a testing program that only tests components individually or when a subset of components in an integrated design.