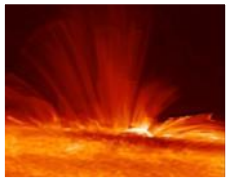
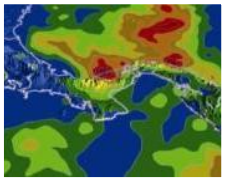
An Unswerving Focus on Safety

Steve Cash
3/9/2016

marshall


“Risky Business”

Space launch systems are inherently risky endeavors

- It takes a tremendous amount of energy to get to orbit
- Highly energetic systems must be designed, manufactured, assembled, and operated
- Launch environments are harsh
- Desire for high-performance often results in very complex designs with low margins
- Production rates are relatively low, yet often complex

The launch vehicle’s basic mission is to deliver people and/or high dollar investments to orbit

- The consequences of failure are significant

Managing Risks

"*Risk comes from not knowing what you`re doing.*"
Warren Buffett 1930- , American Investment Entrepreneur

Managing a "risky business" warrants careful attention to:

- identifying and characterizing risks
- mitigating risks to "acceptable levels"
- verifying the desired mitigations are in place
- monitoring performance to assure mitigations perform as expected over time

"*Know Your Risks*"

- **Identifying and characterizing the safety and mission success risks** associated with a space launch system **is no simple task.**

- There are many sources of these risks, spanning from:
  - the harsh environments they operate in
  - design complexities driven by needs for high-performance
  - complex interactions within the system and its external interfaces
  - hardware failure mechanisms
  - reliance on software to fly the vehicle
  - low manufacturing production rates coupled with the need for high-quality products

Tools Used to Help Identify and Mitigate Risks

- **There are many sources of safety & mission success risks**
  - How can we assure they are identified in a timely manner, mitigated to "acceptable levels"….and assure that the mitigations are satisfactorily incorporated into the design and into the production of each flight unit?

- **Use tools that can help:**
  - assure that risks are systematically identified throughout the life cycle
  - provide a means to allocate risk mitigations to the design, manufacturing, assembly, transportation, and operations
  - provide a means to verify that these risk mitigations are in place
  - characterize and allow formal acceptance of residual risks

- **The primary tools that have been used to accomplish this objective are Hazard Analysis and FMEA/CIL**
  - **Probabilistic Risk Assessment (PRA)**

Hazard Analysis

- Hazard Analysis (HA) is a "**top down**," systematic, qualitative safety risk assessment tool.
  - MSFC has historically used a Fault Tree Analysis to drive its Hazard Analysis
  - Causes which could lead to this undesired end state are identified
  - Controls and verification requirements are identified
  - A "qualitative risk assessment" is performed (*using the Program's Risk Matrix*) to characterize each cause's residual risk
  - All of the above are captured in Hazard Reports, which allows formal communication and acceptance of risks

Failure Modes and Effects Analysis (FMEA)

- Failure Modes & Effects Analysis (FMEA) is used to identify and document the **credible failure modes and causes** of each hardware item of a system.
- **“Bottoms-up” analysis**, which begins with the component/item and analyzes all possible failure modes and their associated effects that result on the function, system, crew, and vehicle.
- A FMEA also documents **the worst-case effect of failures** for each mission phase and assigns a “criticality” per the applicable Program’s FMEA/CIL methodology.

Critical Items List (CIL)

- A CIL is created for "**critical" failure modes** which were identified by the FMEA
  - **Failure modes which could result in loss of life, loss of the vehicle, or the mission.**
- CIL "**Retention Rationale**" is developed and documented for the CIL's failure causes in order to **reduce the likelihood** of critical failure mode occurrence by means of applying design controls, inspections, and tests.

SLS Innovation

- In-line Assessment (ILA) and Risk Based Approach (RBA)
- ILA and RBA are a MSFC S&MA Innovation to government quality assurance processes, helping to streamline the process without loss of technical rigor.
- ILA and RBA utilize MSFC lessons learned from the Shuttle and ARES programs.
  -- ILA differs from Government Mandatory Inspection (GMI). Assurance of a single process versus a single inspection point.
    - More effective QA of critical and complex processes.
    - QA personnel embedded with team – no waiting for a S&MA rep
    - Innovative use of electronic databases and communication links to report and correct issues.
    - ILA – varying frequency / sampling - not mandatory

ILA and RBA

- **RBA (Risk Based Assessment**) – differs from previous ("one size fits all") QA verification strategies. Determines most appropriate government inspections method (GMI vs. ILA) - uses technical and quality risk based screening questions and common risk ranking.
  - Identifies fabrication/assembly and inspection processes with greatest safety and quality risk.
  - More selective use of GMI and accomplish more efficiently
  - Identifies those safety/mission critical inspections for ILA.
  - Identifies, characterizes, and communicates quality assurance risks in a common manner across all SLS Elements.
- **Pilot Results** – demonstrate concept and effectiveness:
  - Much more effective use of Government QA personnel-engaged and contributing.
  - Reduces impact to contractor production schedules.
  - Positive feedback from Contractors
  - Solids: Pilot on test motors (DM2, DM3, QM1), now operational (TVC and other refurbishment processes)
  - Liquids: Multiple supplier components assessed including liner welds and valves.
  - Other SLS Elements engaged in implementing.
- Commercial Crew (and others) S&MA assessing use of ILA and RBA.

People


January 16, 2003 STS-107
COLUMBIA
HI DAD
By Lara
Israel
BY Tal
Ramon
I LAN
Tal Ramon
I Love
ABA
Dad
HUSBAND
STS 107
BROWN CLARK CHAWLA ANDERSON RAMON

People

- **People are your most Important Resource** to assure Flight Safety And Mission Success. Value them.
- **Open Communication Should Be the Standard** that is embraced by the Highest Management to the Line Supervisor. Never tolerate Retribution for Speaking Up. If the King Has No Clothes, Tell Him.
- **Beware of Normalization of Deviance.**
- **Be Willing to Make a Decision.**

- **All Flight Rationale Should Contain These Elements** (Pocketing)

- Solid Technical Understanding
- Condition Relative to Experience Base
- Bounding Case Established
- Self-Limiting Aspect
- Margins Understood
- Assessment Based on Data, Testing, and Analysis
- Interactions with Other Elements/Conditions Addressed

Stay Humble – You are never as smart as you think you are

- **Invest early in good, multi-disciplined, structured brainstorming** about possible failure modes for each component. (FMEA/CIL and Hazards Analysis are great, established tools for doing this!) It will pay off.
- **Launch vehicles operate on the edge of technical feasibility and in a regime frequently beyond your engineering intuition. Pocketing**
- **Margin and fault tolerance** are essential when you design on the edge.
- **Test what you fly and fly what you test**. Test at the corners of the Box. (Challenger)
- **Resist Cutting Test Because of Budget Issues**.

Communications and Making Good Decisions

- **Always seek out dissenting opinions. Beware of Group Think.**
- **Listen to your hardware**. It is always talking to you. (External Tank (Inter tank Popcorn)
- **Major decision meetings** (Flight Readiness Reviews, Critical Design Reviews) need to be held face-to-face.
- **Reward people for speaking up.**

Communications and Making Good Decisions

- All Models are Wrong, Some are useful.Challenge analyses, **especially** from models that are not anchored with actual empirical data. Have a good understanding of the assumptions in the models.

- **Listen** with an open mind. When you focus on the end answer, you tend to hear things only with an ear to confirm what you want that end answer to be **(Confirmation bias).**

- **Cheating Gravity is hard to do.** You do the best you can and make the best decisions that you possibly can, and sometimes you'll be wrong. Margin and fault tolerance. (STS-78 PSA)

- It is always better to *determine* the condition of a suspect component (via direct measurement or observation) than it is to *infer* its condition via indirect measurement or observation or, worse yet, analysis. (Columbia wing on-orbit)

Communications and Making Good Decisions

- Both Columbia and Challenger were brought down by **known problems** that were being managed, not by somebody missing something or some new failure mode. You must critically challenge MRs, problem reports, etc., and get them right!

- Guard against compartmentalization. **Don’t be a bystander** and assume that somebody else who knows a lot more about the subject isn’t worried about the question in your mind. Sometimes the sponsors are engaging in wishful thinking. **Be courageous** and ask what you think is the obvious question. Don’t Check Your Brain at the Door.

Communications and Making Good Decisions

- When a technical matter is presented to you for decision, play it back to presenters in your own words.

- **Risk tolerance goes way up as a deadline or milestone approaches. Guard against it. Someone's life may be depending on it.**

- **Know your team.** Be there for them. Things at home affect how decisions are made.

Communications and Making Good Decisions

- **You're never as smart as you think you are**. If a team member (analyst, subsystem manager, chief engineer, etc.) habitually comes across as dead sure on technical matters, then they haven't learned this lesson yet. (Nozzle Pocketing)

- **Cost and schedule pressures are always present and real**, but don't let them box you into thinking that stand-down is not a real option. It is. Don't say, "Well, we have to do it this way or we can't fly." Sometimes you indeed **can't** fly.

- **Make sure your team is willing to speak up** and challenge technical presentations, no matter who is presenting. Speaking up is tough. (STS-112 FRR)

People


January 16, 2003 STS-107
COLUMBIA
HI DAD
By Lara
Israel
I
LAN
BY Tal
Ramon
Tal Ramon
I Love
ABA
Dad
BROWN CLARK CHAWLA ANDERSON
HUSBAND
STS 107