Defense-in-Depth Inter Agency Workshop

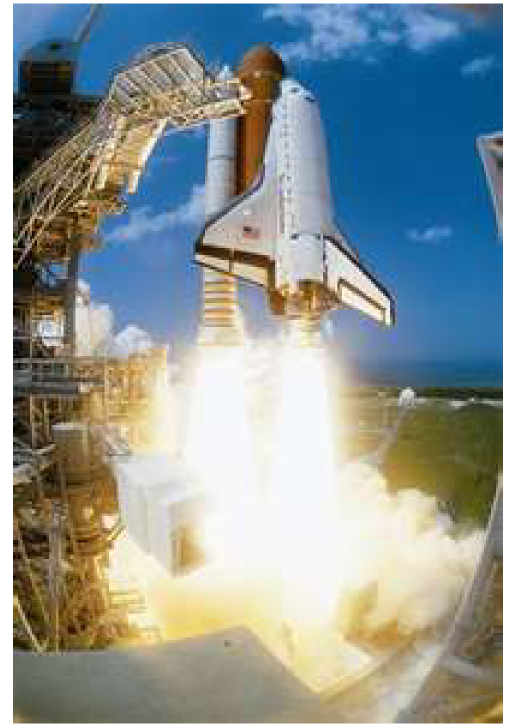
Designing on the edge

STEVE CASH

DIRECTOR MSFC SAFETY & MISSION ASSURANCE

AUGUST 26 2015

“Risky Business”

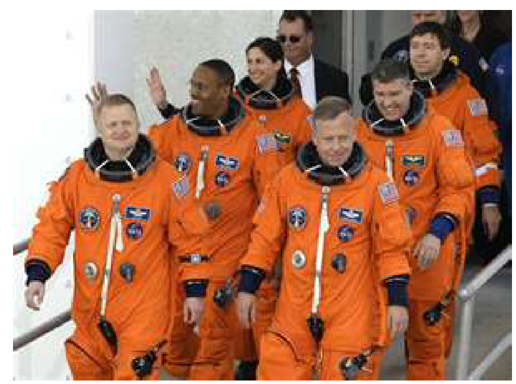


Space launch systems are inherently risky endeavor

- 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

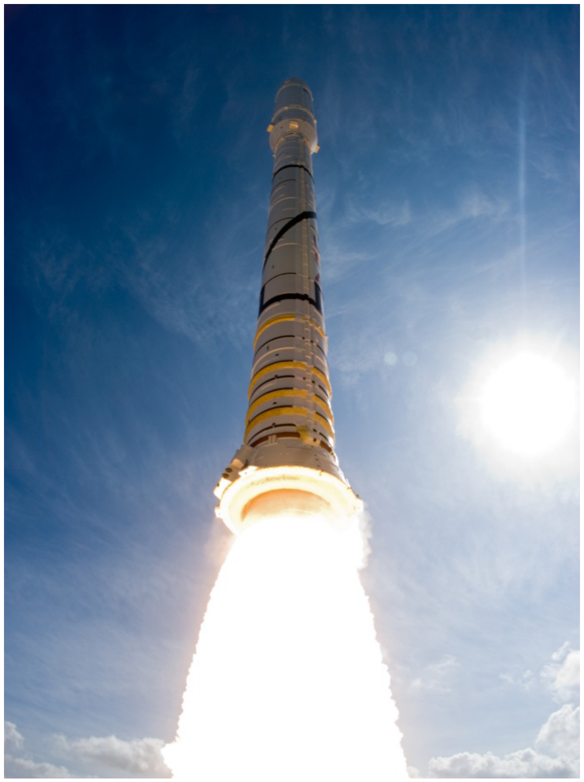
The launch vehicle’s basic mission is to deliver people and/or high dollar investments to orbit

- The consequences of failure are significant



Managing Risks

"Risk comes from not knowing what you`re doing"
Warren Buffett, 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

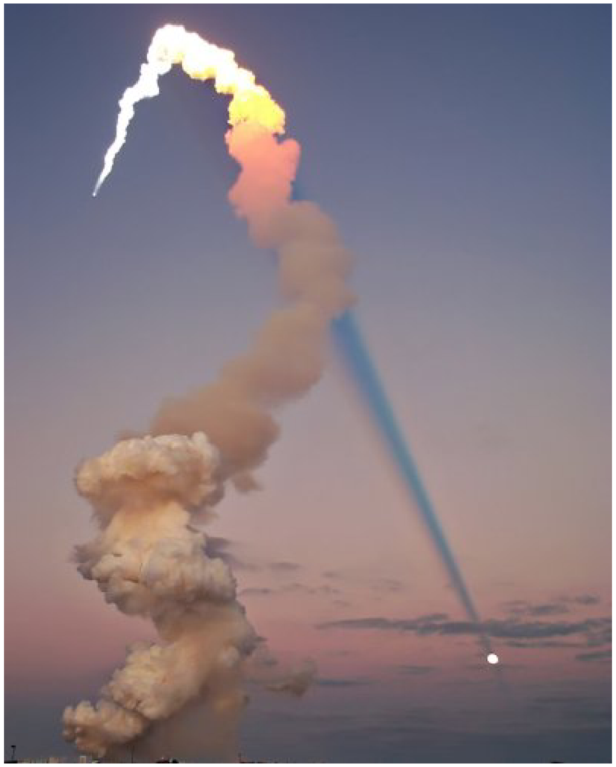
"A ship in harbor is safe - but that is not what ships are for"
-John A. Shedd, *Salt from My Attic*

“*Know Your Risks*”

- Identifying and characterizing the safety & mission success risks associated with a space launch systems is no simple tasks

- 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

- The next 3 charts provide just a top-level snapshot of some of these risks



Example sources of Launch Vehicle Safety & Mission Success Risks

- **Natural and Induced Environments (ground and ascent winds, lightning, hail, aerodynamics, vibrations, acoustics, shock, accelerations, thermal, EMI, etc)**
  - Uncertainty that the environments or loads have been properly characterized/modeled and validated
    - e.g., STS-1 Ignition Overpressure
  - Inadequate ground and/or flight testing to validate predicted environments and loads

- **System interactions**
  - Failure to fully understand and mitigate potential system interactions
    - MPS interactions between propellant stages/tanks and engines
      - *pre-press/ press cycles, chill down, Ullage collapse, propellant quality, contamination, cavitations, etc*
    - Hazardous accumulations of gases/liquids in compartments and in proximity to the vehicle/launch complex
    - Vehicle-to-launch pad interactions
      - Liftoff clearances, umbilicals/mechanisms re-contacts, liftoff acoustics, IOP, etc)
    - Plume heating / recirculation flows
    - Separation/staging events
    - Thrust oscillations
    - EMI (lightning, avionics EMI, RF energy, etc.)
    - Debris
    - Controllability (e.g., dynamic response, OML sensitivities, slosh, TVC capabilities/response rates, etc)
    - Abort'ability (e.g., potential abort environments, abort system capability, abort triggers, etc)
    - etc
  - Lack of, or inadequate integrated testing with hardware and software
  - Lack of, or inadequate integrated system-level qualification/acceptance tests & checkout

Example sources of Launch Vehicle Safety & Mission Success Risks

- **Hardware Failures**
  - Not understanding the various hardware failure modes, their effects and their failure causes
    - Failure of systems, subsystems, components or parts to function when required
    - Inadvertent activation systems, subsystems, components mechanisms, or parts when undesired (e.g., pyrotechnic inhibits)
  - Inadequate design mitigation of critical failure modes
    - Inadequate failure tolerance or FDIR; use of low reliability parts; inadequate design & construction STD's (e.g., structural strength, fracture control, material selections, etc); etc
  - Poor hardware quality
  - Exposing hardware to environments/loads outside its design limits
    - Inadequate design for max expected environments/loads
    - Inadequate understanding of the various environments/loads that critical hardware will be subjected
    - Inadequate qualification program to account for all applicable environments/loads and their variability/uncertainties
      - Environments are a potential "common cause failure" mechanism

- **Software Anomalies**
  - Failure of hardware designers to properly communicate their needs (requirements) to S/W developers
  - Failure to code the S/W properly
  - Inadequate verification testing of the S/W and the integrated S/W and H/W system

Example sources of Launch Vehicle Safety & Mission Success Risks

- **Product Quality**
  - Failure to build the system in accordance with designer expectations…and the analyzed and qualified configuration (i.e., the *as-built product does not equal the as-designed*)
    - Inadequate or ambiguous drawings / specifications
    - Potential variability in manufacturing and assembly processes
      - Lack of well defined and controlled manufacturing / assembly procedures
      - Production equipment variability
      - Technician/Inspector variability
  - Poor workmanship
    - Inadequate acceptance criteria
    - Inadequate Technician/Inspector training
    - Inadequate or defective inspection equipment
  - Inadequate manufacturing and environmental control
    - Examples might include contamination, corrosion, excessive temperatures or humidity, etc
  - Use of defective, substitute, or counterfeit materials or parts
  - Failure to account for material or part variability
    - Supplier variability, inadequate acceptance testing/screening, etc
  - Failure to detect nonconformities or process departures during manufacturing, assembly, transportation and/or handling
  - Failure to detect problems during qualification/acceptance testing or integrated system checkout
  - Inadequate, or lack of adequate engineering assessments of identified nonconformities, process departures, qualification/acceptance test or checkout problems,

NASA's general approach to "Defense In Depth"

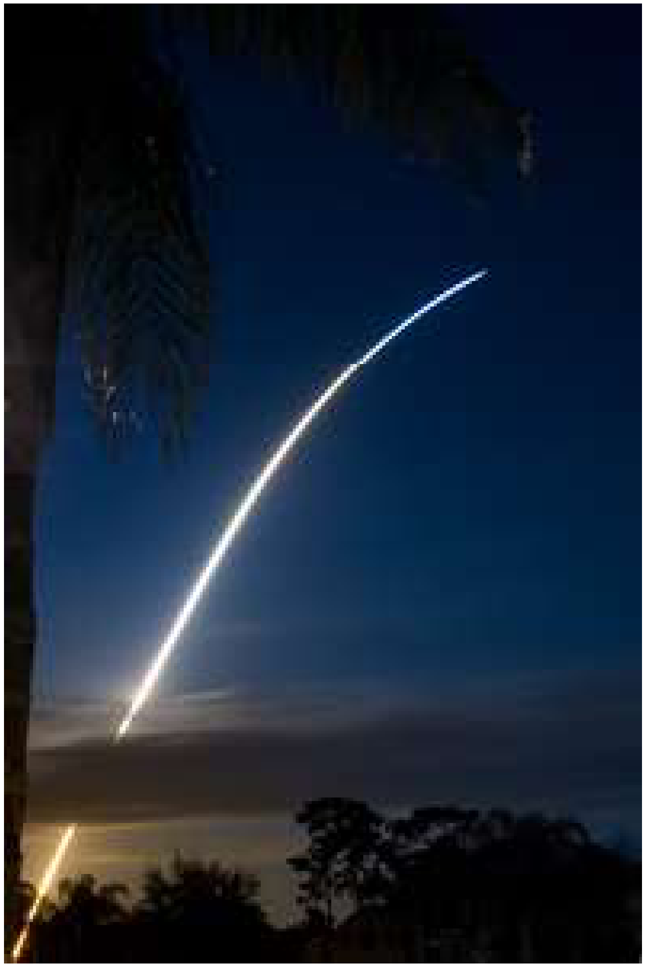
- **Design, Manufacture & Test to enable safety & mission success**
  - Design to tolerate failures and have high reliability
  - Implement NASA Standards in design and processes (e.g., Safety Factors, Fracture Control, Parts Selection, EMI, Contamination Control, etc.)
  - Perform qualitative and quantitative safety & mission success analyses to identify and mitigate risks
    - Hazard Analyses
    - Failure Modes & Effects Analyses
    - Reliability Predictions
    - Probabilistic Risk Analyses (PRA)
  - Perform Government Mandatory Inspections (GMIP's) and In-Plant Surveillance
  - Inline assessments /Risk Based Assessments
  - Test what you Fly philosophy
  - Conduct Acceptance & Qualification Testing (Challenger PVM-1 Flaw testing)
  - Dissenting Opinion Process
  - Launch Commit Criteria
  - Conduct formal reviews at milestones (SRR, SDR, PDR, CDR, DCR, Acceptance, Test Readiness, Flight Readiness)
  - Perform Post-Flight Assessments

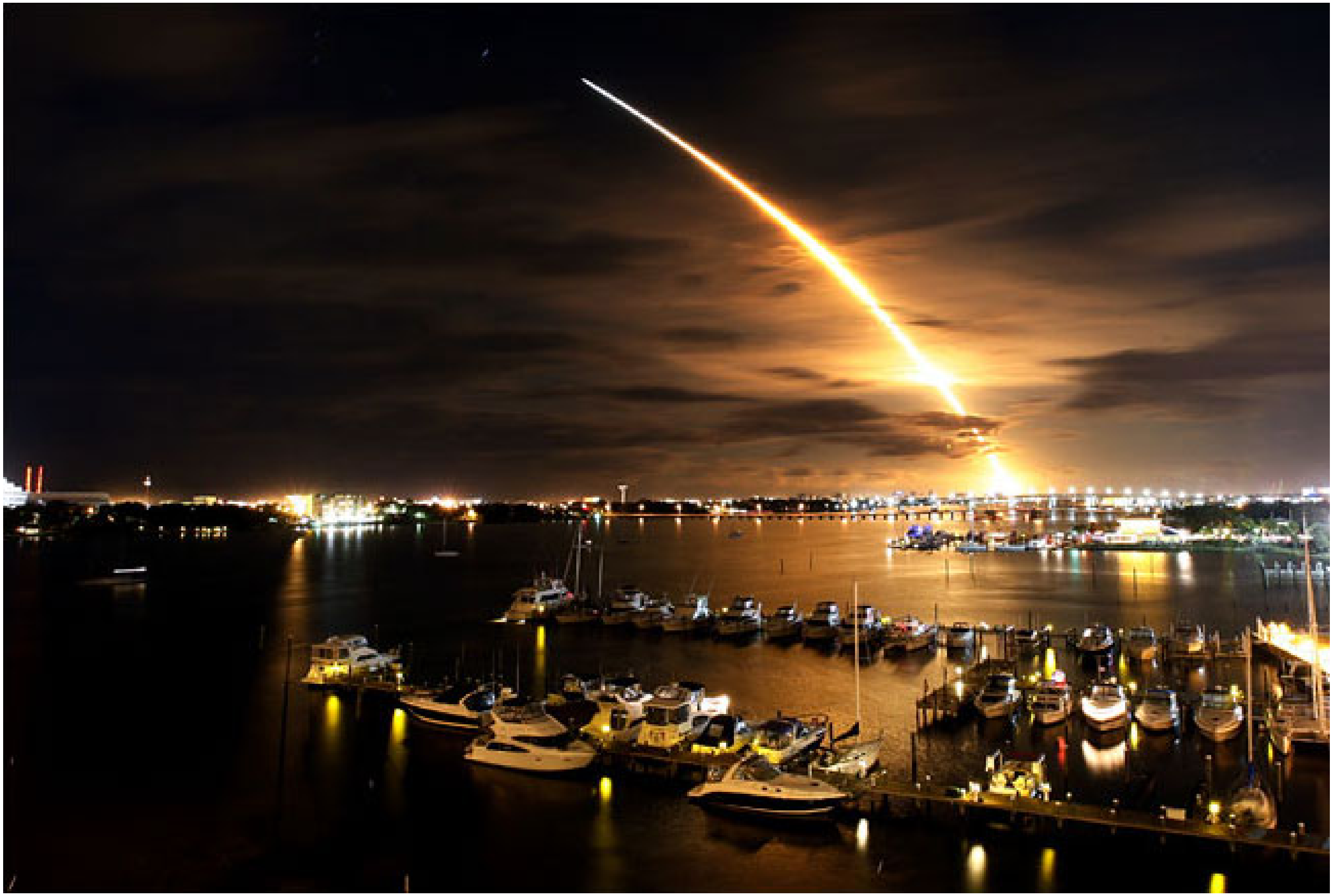
- **Provide ability to abort the mission and get the flight crew off the vehicle**
  - Required by NASA's NPR 8705.2 (*NASA's Human-rating Requirements*) for new crewed space systems

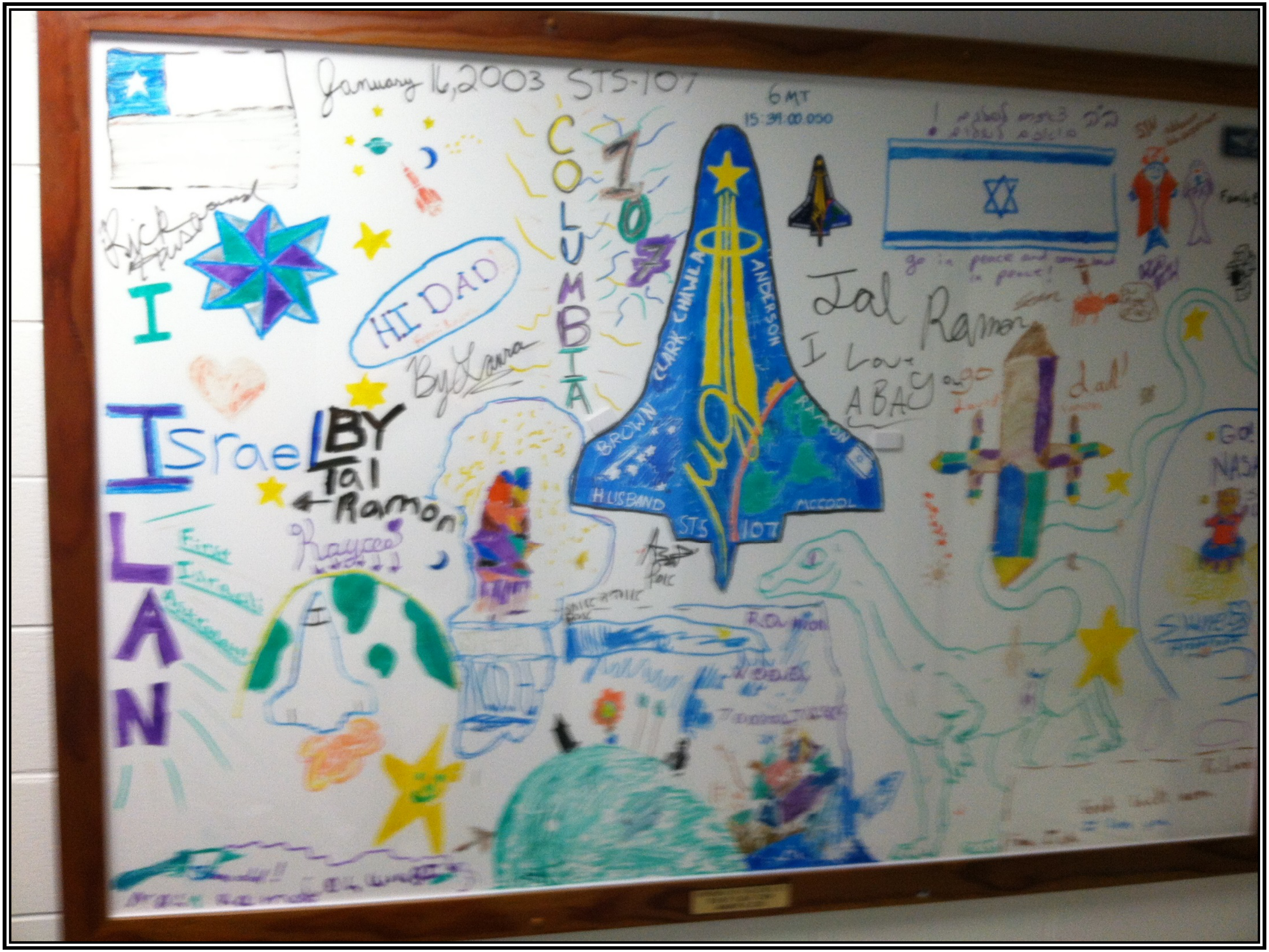
- **Protect the Public and the Range in case of a very serious anomaly**
  - Include means to monitor and track the vehicle by Range Safety
  - Include Flight Termination Systems
  - Ability to destruct the vehicle if necessary to protect the public and the Range

Conclusions

- **Spaceflight is an inherently risky endeavor**
- **A launch vehicle's basic mission is to deliver people and/or high dollar investments to orbit**
  - The consequences of failure are significant
- **A formal, systematic approach to identifying and mitigating safety risks, closed-loop verifying implementation of risk mitigations, and characterizing the residual risks is needed**
- **Formal acceptance of residual risks is warranted**
- **NASA's historical tools (HA, FMEA/CIL and PRA) provided mechanisms to accomplish the above**







January 16, 2003 STS-107
GMT
15:39:00.000
COLUMBIA
107
HI DAD
By Laura
I
Israel
ILAN
BY
Tal
Ramon
Kaycee
BROWN
CLARK
CHAWLA
ANDERSON
RAMON
HUSBAND
McCOOL
STS
107
Tal
Ramon
I Love
ABBA
go in peace and come back in peace!
Go
NASA