System Safety and Quality Assurance Important Partners in Program Success.

Tennessee Valley Chapter
International System Safety Society

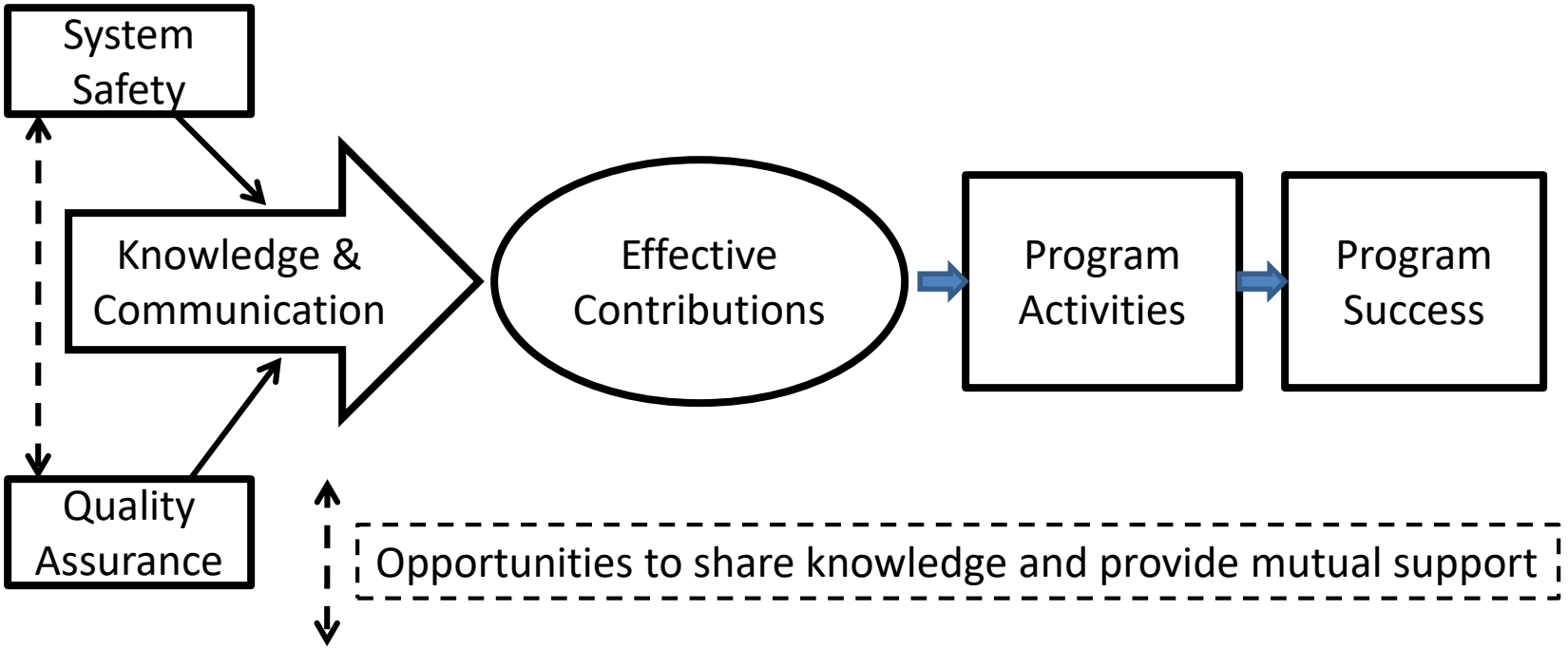
John Livingston

Talking Points

- Background
- Relationships of Assurance functions
- Quality Assurance
- System Safety
- Examples of Common Interest (opportunities missed and utilized)
- Conclusions

Needed for Success

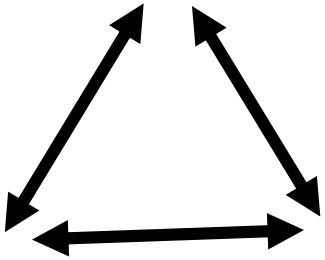
- While Program(or Project) management has the responsibility for the program's success, System Safety and Quality Assurance provide key support functions which depend on Knowledge and Communication for effective contributions to program success



System Safety and Mission Assurance

SYSTEM SAFETY REQUIRES THE SUPPORT OF AND INTERACTION WITH THE OTHER ASSURANCE FUNCTIONS

SYSTEM SAFETY
- Hazard detection & mitigation



RELIABILITY
- Hazard Causes
- Probability Analyses

QUALITY
- Process Controls
- Verification Activities

The Reliability and Quality Assurance efforts provide:

» Important elements of the total system safety effort

» Cross-checks for completeness & practicality

Reliability

- Reliability analysts provide key support in the development of hazard Analysis and event probability information.
- Their knowledge and understanding of the hardware characteristics and operations support the identification and solution of potential Safety risk issues are:
  - Properly Identified in the Failure Modes and Effects Analysis (FMEA) & other Risk Assessments
  - The appropriate reflection of Reliability Assessments information is appropriately reflected in hazard causes and controls.

Quality Assurance and Quality Management Systems

Quality Assurance - “The planned and systematic activities implemented in a quality system so that quality requirements for a product or service will be fulfilled.“ (American Society for Quality (ASQ))

Quality Assurance are the activities and management processes that are done to ensure that the products and services the project delivers are at the required quality level.

- Process driven
- Focused on the development of the product or delivery of the service.

A quality management system (QMS) is a formalized system that documents the processes, procedures, and responsibilities for achieving quality policies and objectives. SO 9001 is the international standard that specifies requirements for a quality management system.

Quality Assurance

A standard set of Quality System elements are listed below Most major companies and government agencies are certified to ISO 9001 and AS9100 with audits by audited by a registrar and internal reviews.

- **Program/Project Planning**
- **Receiving, In-process and Final Inspection**
- **Product Identification and Traceability**
- **Inspection and Testing Status**
- **Corrective and Preventive Action**
- **Non Conforming Material Control**
- **Training**
- **Handling, Storage, Packaging, Preservation, & Delivery**
- **Contract Review**
- **Purchased Material Control**
- **Design Control**
- **Control of Records**
- **Document and Data Control**
- **Calibration and Tool Control**
- **Fabrication and Process Control**
- **Infrastructure and Work Environment**

Typical Quality Assurance Activities

Quality Engineer (Project)

- Participate in Technical Interchange Meetings, Milestone reviews, and Audits.
- Establish the Quality Plan.
- Evaluate change requests, deviations and waivers and other related document changes.
- Perform drawing reviews per Quality Plan and organizational requirements
- Provide appropriate quality requirements for procurements per organizational requirements
- Assess in-house fabrication work requests and provide quality requirements and identify inspection points. (work with program System Safety (Hazard Reports) and Reliability (Failure Modes and Effects Analysis (FMEA), Critical Items List (CILs), or a Failure Mode, Effects and criticality Analysis (FMECA)
- Support Operational Readiness Reviews, Operational Inspection Reviews, and or Test Readiness Reviews (ORRs/ORIs/ TRRs).
- Provide letters of delegation (LOD).
- Participate in Material Review Board (MRB) activities.
- Participate in the Acceptance Data Package review

- For Government QA Efforts - Establish Government Mandatory Inspection Points (GMIPs)

Quality Assurance Management

- In recent years carefully structured and detailed quality assurance and management programs have been developed. AS9001 and AS9100 are quality management standards.
- AS9100 is structured to align with ISO 9001:2008, but it also provides additional provisions for regulatory compliance and several aerospace-sector specific requirements. Beside a general discussion of the relationships with reliability, maintainability and safety efforts, there are a number of the quality program requirements that directly interface with program safety and system safety efforts.

  From the hardware standpoint,

  – there are requirements for design verification and validation,
  – inspection and testing requirements,
  – and control of production and operational processes.

  From the programmatic side,

  – there are requirements for configuration management (including process changes, product documentation including the disposition of non conforming products and audit functions);
  – definition of quality program methods and techniques; and corrective action activities including data collecting, analysis, investigation and resolution documentation.

Quality Engineering

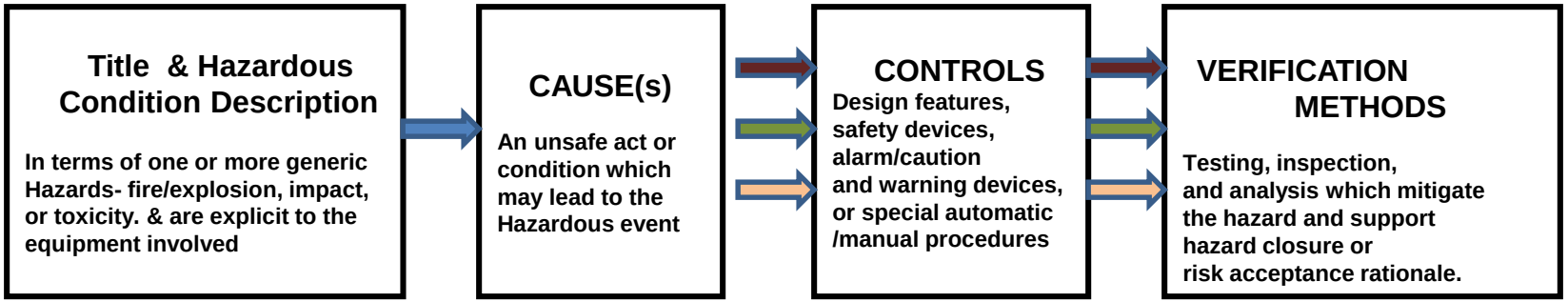
- Quality engineering is important in assuring that proposed inspections and other verification efforts are doable and practical.
- Early identification of troublesome implementations, generally lead to more and better verification (or even improved controls) solutions.
- Getting team agreement on the “safety critical” inspections is a key step in keeping the hazard control verification actions properly focused.

Critical Processes

- In complex systems, there will be many processes that are critical to the safety and mission success of the program.
- They exist at every phase of the program life cycle and are influenced by many contributing factors.
- To assure safe operation, hardware has to be created from specific materials in carefully controlled processes.
- Many of the process control activities that were instituted to meet quality assurance standards were also important hazard control verification activities.

System Safety Product Contributions

Key Hazard Assessment Elements



Data Sources:

Causes
- Fault Trees
- FMEA/CIL
- Operations
  - Program
  - Other (Lessons Learned)

Controls
- Design
  - Hardware & Materials
  - Processes
    - Plant
    - Operational

Verification
- Testing
- Inspections
- Simulations

Tracked by:

Program Activities: Change Requests & Related Boards, Milestone Reviews (SRR, PDR, CDR ,DCR)
Engineering Activities: Working Groups, Issues meetings, technology & system tests
Assurance Activities: Office Level (Local), Program, Agency & Outside

Examples of Common Interest

Opportunities Missed (Examples 1 and 2)

- Hubble Space Telescope
- Tethered Satellite System

Common Interest utilized (Example 3)

- Space Shuttle Main Engines

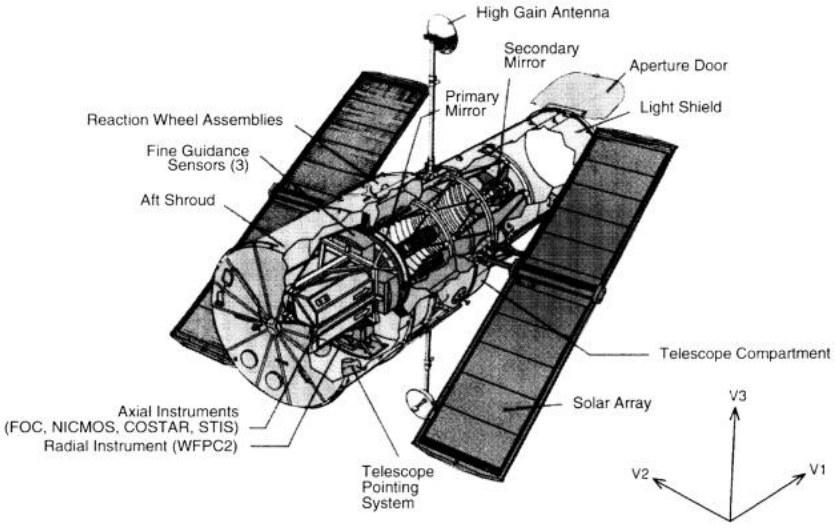
Example 1 – Hubble Space Telescope

- After many years of promoting by astronomers, design on a space based telescope begin in the early 1970's. Preliminary design studies were undertaken in 1972 lasting until 1977. Budget issues led to the reduction in the size of the primary mirror from the planned 3 m. to the 2.4 m. that was flown.
- The Hubble Space Telescope (HST) was first scheduled for launch in 1983, but it was not really to launch until early 1986. The stand down after the tragic loss of the shuttle Challenger in January of 1986, delayed the launch by 4 more years. It was finally launched on April 24, 1990 as Part of the STS-31 Mission.

  Its operation has included Space Shuttle service missions (4 were conducted), but the HST has no active de-orbit system. A study by NASA Orbital Debris Program Office predicted the HST would re-enter about 2020 with an estimated 26,000 pounds of the spacecraft making it to the ground in footprint stretching over 755 miles

  The analysis suggests that the risk posed to the human population in the year 2020 is 1:250 – a risk that exceeds the risk of 1:10,000 cited in a NASA Safety Standard for reentry debris strike risk. (A later studies placed the Hubble risk at 1/700)

Example 1 – Hubble Space Telescope



The Hubble Space Telescope measures 13.1 m (43.5 ft) in length, 4.27 m (14.0 ft) in diameter, and weighs 11,000 kg (25,500 lb)

The primary mirror of the Hubble telescope measures 2.4 m (8 ft) in diameter and weighs about 826 kg (1820 lbs).

The Spherical Aberration Problem

- The first images from the HST were marred by an optical defect called spherical aberration which limited the image quality.
- An investigation commission found that a reflective null corrector, a testing device used to achieve a properly shaped non-spherical mirror, had been incorrectly assembled—one lens was out of position by 1.3 mm (0.051 in). (The experts had failed to properly re-configure from a test set-up)
- During the initial grinding and polishing of the mirror, the contractor (Perkin-Elmer) analyzed its surface with two conventional refractive null correctors. However, for the final manufacturing step (figuring), they switched to a custom-built reflective null corrector, designed explicitly to meet very strict tolerances which resulted in the mirror being ground very precisely but to the wrong shape.
- The commission blamed both Perkin-Elmer(PE) and NASA
  - Perkin-Elmer
    - Did not review or supervise the mirror construction adequately,
    - Did not assign its best optical scientists to the project
    - Did not involve the optical designers in the construction and verification of the mirror.
  - NASA was criticized for
    - not picking up on the quality control shortcomings - relying totally on test results from a single instrument and not having an end-to-end test of the final optical system.
  - **Not acknowledged was the "off-limits" PE Metrology Area which had no NASA oversight**
- Happy Ending - The fact that the mirror had been ground so precisely to the wrong shape led to the design of new optical components for the science experiments with exactly the same error but in the opposite sense, which were added to the HST during maintenance missions

Example 2 -Tethered Satellite

Mission 1

Tethered Satellite First Mission

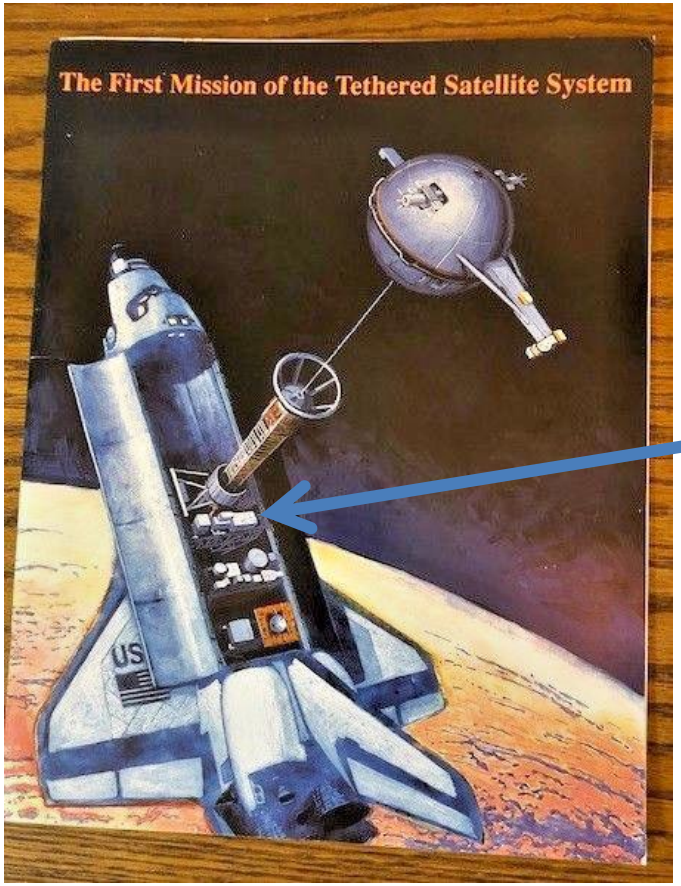
The first Tethered Satellite System mission (TSS-1) was flown on the STS-46 (July 31 to August 8, 1992). The Tethered Satellite was developed by the Italian space agency

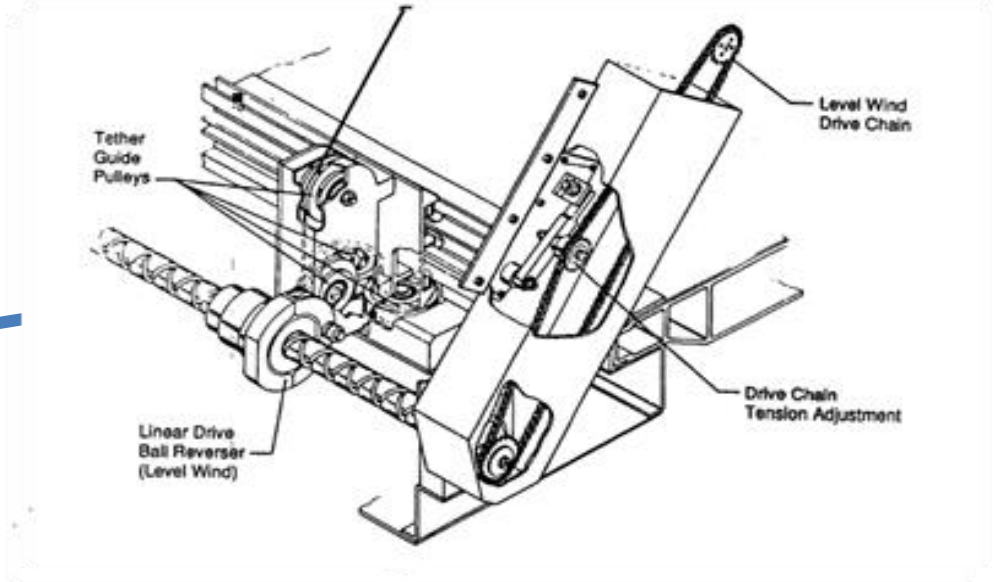
- Weight =515kg (1,139 pound),
- 1.5m (5 foot) diameter
- Deployed from the shuttle cargo bay the Shuttle cargo bay while attached to a 20-km (12.5-mile) long tether

The deployment system and the tether (a Kevlar covered copper cable) was developed and manufactured under a NASA contract

TSS-1 was a 31 hour mission to explore the dynamics and electricity-generating capacity of the tether system

TSS





The Level Wind Mechanism

Mission 1 Issues

- Unfortunately several problems developed during the deployment and the satellite only reached a maximum distance of 265 meters (860 feet) not 20 km from the Atlantis
- During the abnormal operations, the deployment system became jammed with the tether unable to move either in or out.
- Attempts made over the next several days to clear the jam and complete the deployment failed
- Finally the crew was able to retrieve the satellite and safety stow it for the return to Earth

Jamming of the Level Wind Mechanism

The most serious of the three problems identified was the mechanical interference between a bolt and the level wind mechanism which caused the jamming of the level wind mechanism.

- The protruding bolt was part of a modification kit installed late the TSS-1 processing flow at the launch site after completion of the deplorer systems level testing
- The modification was required to overcome structural negative margins of safety that were discovered a mission level loads verification analysis near the planned launch date

The investigation Board cited three lessons learned from the TSS-1 events:

- "The Spacelab carrier-to-TSS-1 structural loads analyses should have discovered the structural problem earlier
- Flight hardware changes late in the project cycle are a risk
- And ground testing should fully explore the dimensions of the expected flight environment."

Missed Deficiencies

While not specifically identified in the report, the deficiencies noted in the system engineering efforts apparently were also present in the system safety assessments.

- The report did not acknowledge any concerns being raised by the system safety team or the safety and mission assurance organization (safety, reliability & quality assurance)
- No documentation was cited that would indicate an integrated system level design and operational safety assessment was preformed for the modification

<u>True integration is more than assembling the pieces of individual design assessments. For any "last minute" modification there needs to be a thorough evaluation of the total system configuration and operation versus the modification as implemented.</u>

Example 3 - Space Shuttle Main Engine (SSME) Enhancements

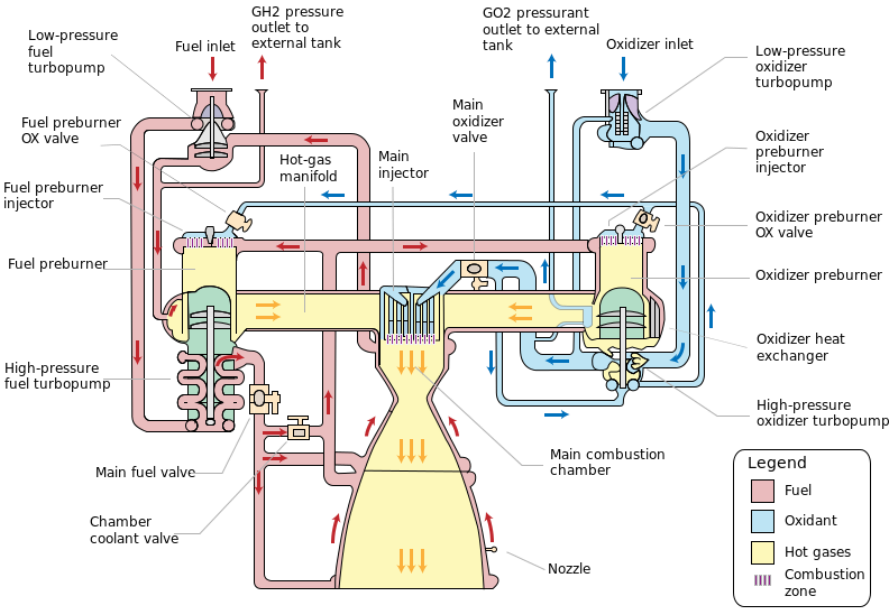
Program, Engineering, Safety, Reliability and Quality Assurance working together

Space Shuttle Main Engine (SSME) Enhancements

Space Shuttle Main Engines(3 per Vehicle)
Propellants O2/H2
Rated power level (RPL) 469,448 lb
Nominal power level (104.5% RPL) 490,847 lb
Full power level (109% RPL) 512,271 lb
Chamber pressure (109% RPL) 2,994 psia
Specific impulse at altitude 452 sec
Throttle range (% RPL) 67 to 109
Gimbal range +/- 11°
Weight 7,748 lb

NASA increased the reliability and safety of Shuttle flights through a series of enhancements to the Space Shuttle Main Engines. Modifications included new high-pressure fuel and oxidizer turbopumps, a two-duct powerhead, a single-coil heat exchanger and a large-throat main combustion chamber

Single-Coil Heat Exchanger



- The Shuttle's engines supply pressure to the external tank, which in turn provides propellants to the engines. This pressure is produced by the engine's heat exchanger, a 40-foot-long (12-meter) piece of coiled stainless steel alloy tubing. the original heat exchanger had seven welds.
- The newly designed exchanger was a continuous piece of stainless steel alloy. The design eliminated all seven criticality 1 (loss of crew and vehicle if they failed) welds. Also the increased thickness of the redesigned heat exchanger reduced wear on the tube and lessened the chances of damage. It also reduced maintenance and post-flight inspections.

Conclusions

- Even robust systems require appropriate quality assurance efforts to meet performance expectations.
- For complex systems that operate in challenging environments with limited “safety” margins, a vigorous quality assurance program is also a critical component of the program safety effort.
- History and "common sense" sustain the proposition that programs which have well integrated quality and safety efforts will fare better that those with assurance efforts limited to individual discipline responsibilities.

References

- **Teamwork - A Key Component in Aerospace Flight Safety Efforts By John M. Livingston and Jon C. Wetherholt, ISSAA Conference**
- **System Safety and Quality Assurance - a Valuable Partnership for Program Success, John Livingston System Safety Journal**
- **Non-Sensitive material from Quality Assurance Charts, SLaTS Course (2012)**
- **The Hubble Space Telescope optical systems failure report, National Aeronautics and Space Administration, [1990] Series: NASA technical memorandum, 103443.**
- **NASA TM 108704 -Tethered Satellite System Contingency Investigation Board Final Report**
- **Space Shuttle Main Engine (SSME) Enhancements, NASA FactsFS-2002-03-60-MSFC March 2002**