Lessons from the Shuttle Independent Assessment

Dr. Tina L. Panontin
Chief Engineer, NASA Ames Research Center

RMC III, September 19, 2002

Outline

- Origin of the Shuttle Independent Assessment
- Shuttle Independent Assessment Team (SIAT)
- Assessment Structure
- Assessment Method
- General Results
- Example Findings
- Case Study: SSME LOX Pin Ejection
- Recommended Improvements to Current Methods
- Recommended Future Improvements

Shuttle Independent Assessment: Origin

- Two serious in-flight anomalies occurred on STS-93, in July 1999
  - Primary and back-up main engine controllers on separate engines drop offline when a wire arcs to a burred screw head.
  - Small fuel leak and subsequent premature MECO occur due to a pin ejected from engine post that penetrates three nozzle coolant lines.
- Several other incidents on prior flights or during maintenance procedures
- System design and redundancy successfully handled each anomaly or incident
- Increasing frequency of occurrence raised concerns over adequacy of operations and maintenance processes in light of projected extended life of Shuttle
- SIAT was formed by Dr. Henry McDonald, at the request of Mr. Rothenburg, then AA for Space Flight in September, 1999

Shuttle Independent Assessment Team

- Charter (September 7, 1999):
  - *"Dr. McDonald will lead an Independent Technical Team to review Space Shuttle systems and maintenance practices. The team will be comprised of NASA, contractor, and DOD personnel and will look at NASA practices, Shuttle anomalies and civilian and military experience."*
- Team Members:

Dr. H. McDonald	*ARC, Chairperson*
Dr. T. Panontin	*ARC, Technical Assistant*
L. Mederos	*ARC, Executive Secretary*
M. Conahan	*Aircraft Industry, Consultant*
RADM D. Eaton (ret)	*Naval Post Graduate School*
R. Ernst	*Naval Air Systems Command*
G. Hopson	*MSFC*
Dr. B. Kanki	*ARC*
Lt. Col. J. Lahoff	*USAF HQ Safety Center*
J. McKeown	*Naval Air Systems Command*
Dr. J. Newman	*LaRC*
R. Sackheim	*MSFC*
G. Slenski	*USAF Research Laboratories*
Col. R. Strauss	*USAF HQ Safety Center*
J. Young	*JSC*

Shuttle Independent Assessment Structure

- Assessment focused on four major sources of potential risk in complex systems (Haimes, 1998)
  - Hardware, including avionics, hydraulics, hypergols and APU's, propulsion, structures, and wiring
  - Software, including validation and verification of both ground and flight software
  - Human Factors, primarily in maintenance
  - Organizational or process issues, including risk assessment and management, problem reporting, and safety and mission assurance

Shuttle Independent Assessment Method

- Team meetings at Ames, Palmdale, Kennedy, Headquarters, and Johnson
- Team Site visits to Palmdale, Kennedy, Johnson
- Presentations from the Shuttle Program Office and Maintenance Organizations
- Subteam meetings and analyses
- Work force interviews at Palmdale, Kennedy and Marshall by support teams
- Numerous Tele- and Video-conferences
- Case studies used to illuminate potential issues

SIAT: General Results

- Shuttle is a complex system that operates in unforgiving flight environment
- System is still a "developmental" vehicle as opposed to an "operational" one
  - Still relatively few flights
  - Extensive maintenance, much of it highly specialized, some invasive
- Overall, Shuttle is a well-defended system
  - Dedicated, skilled workforce
  - Reliability, redundancy designed in
  - Vigilant, committed Agency

But, SIAT observed an erosion of defenses--a shift from rigorous execution of flight-critical processes

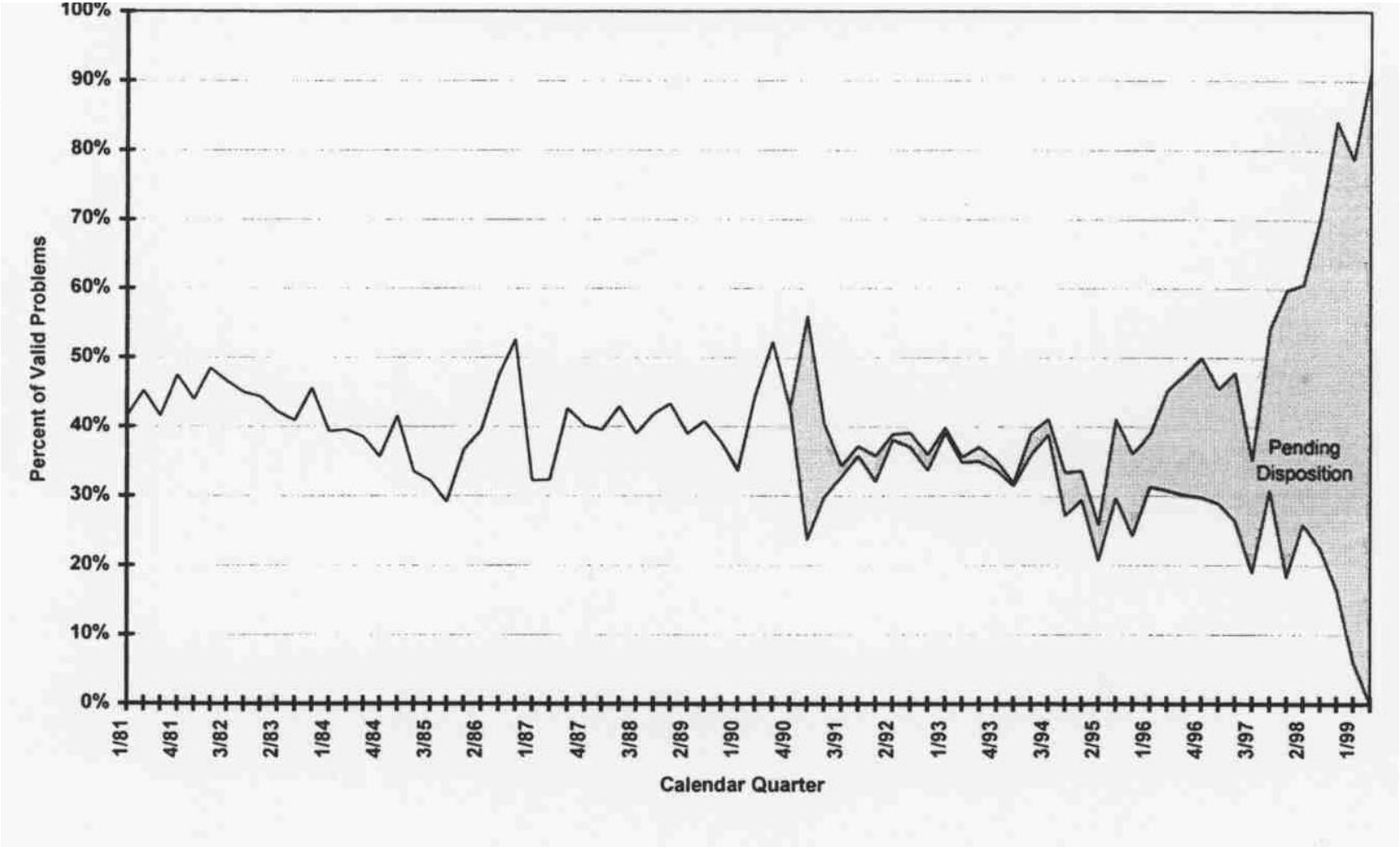
SIAT: General Results

- Assessment identified systemic issues that cross subsystems and work elements in addition to specific findings and recommendations
  - 8 systemic issues
  - 4 specific recommendations required for return-to-flight
  - 77 specific, longer-term recommendations
- Systemic issues describe erosion of key defensive practices:
  - Staff levels and stability
  - Communication
  - Risk awareness
  - System assurance
- Erosion of defenses found to be due to:
  - Reduction in resources and staffing
  - Shift toward “production-mode” since system is well-defended
  - Optimism engendered by long periods without major mishap

Risk Awareness: Findings

- Failure Mode and Effects Analysis / Critical Items List (FMEA/CIL) not updated with problem occurrence/recurrence, aging, wear, or new assessment information
- Large number of waivers and exceptions for flight (~330 CIL waivers for STS-93)
- Increased tendency to accept risk without sufficient scrutiny because of prior success
- Increased number of Standard Repairs (200 of ~500 on SSME CRIT1 items) and Fair Wear & Tear allowances that reduce problem visibility
- Weaknesses in reporting requirements and procedures that can allow problems to go unreported or reported without sufficient accuracy and emphasis
- Antiquated Problem Reporting And Corrective Action (PRACA) database that lacks adequate tracking/trending methods and inhibits decision support

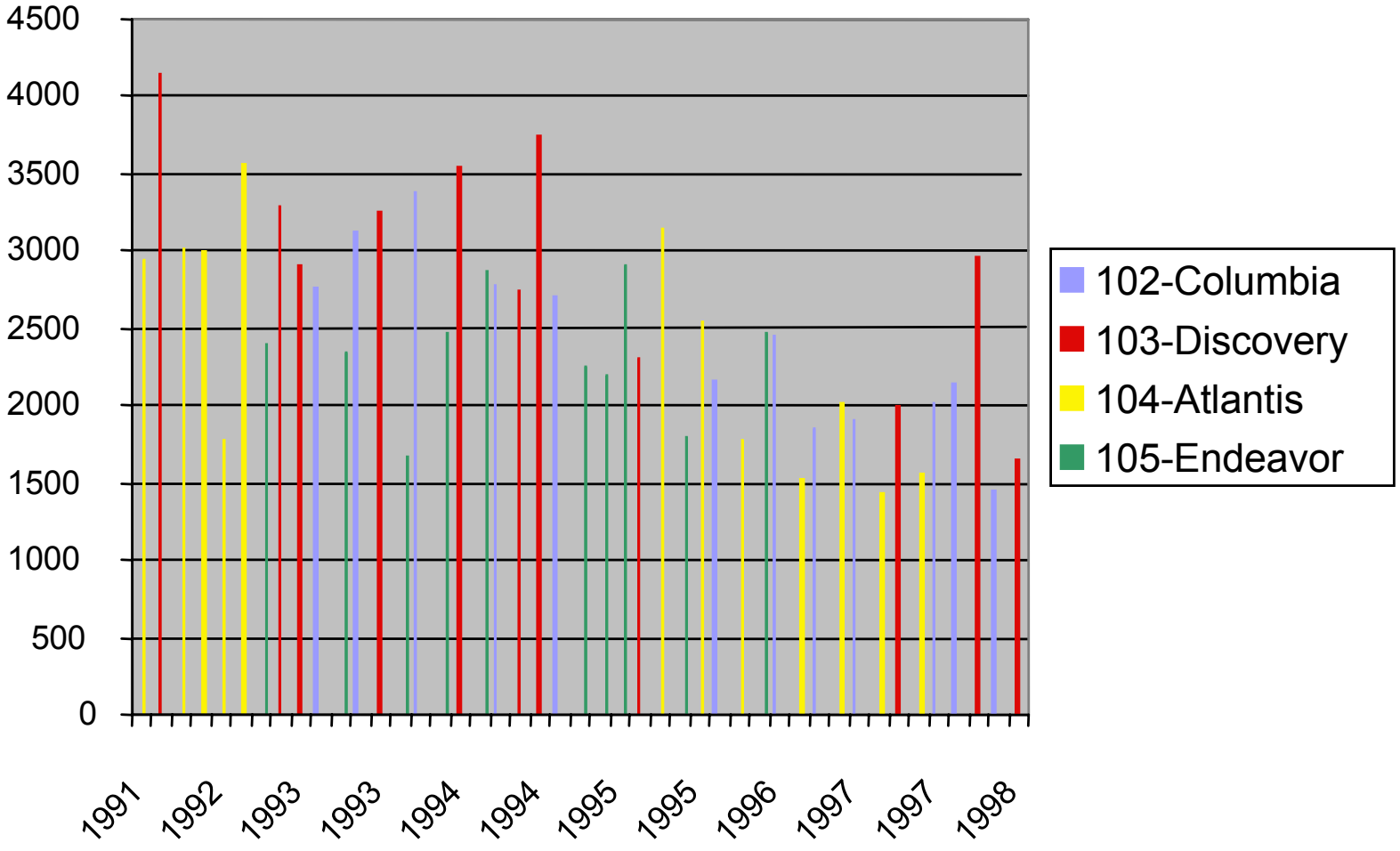
Valid Problems vs. Pending Disposition



System Assurance: Findings

- Moving to ‘insight’, self inspection
- Large reductions in Mandatory Inspections Points
- Violation of fly as test, test as you fly philosophy
- Increased reliance on redundancy and abort modes
- Compromised redundancy (76 areas, 300+ circuits, 6 areas loss of all main engines)
- Potential complacency in problem reporting and investigation
- Move toward repair implementation without engineering oversight

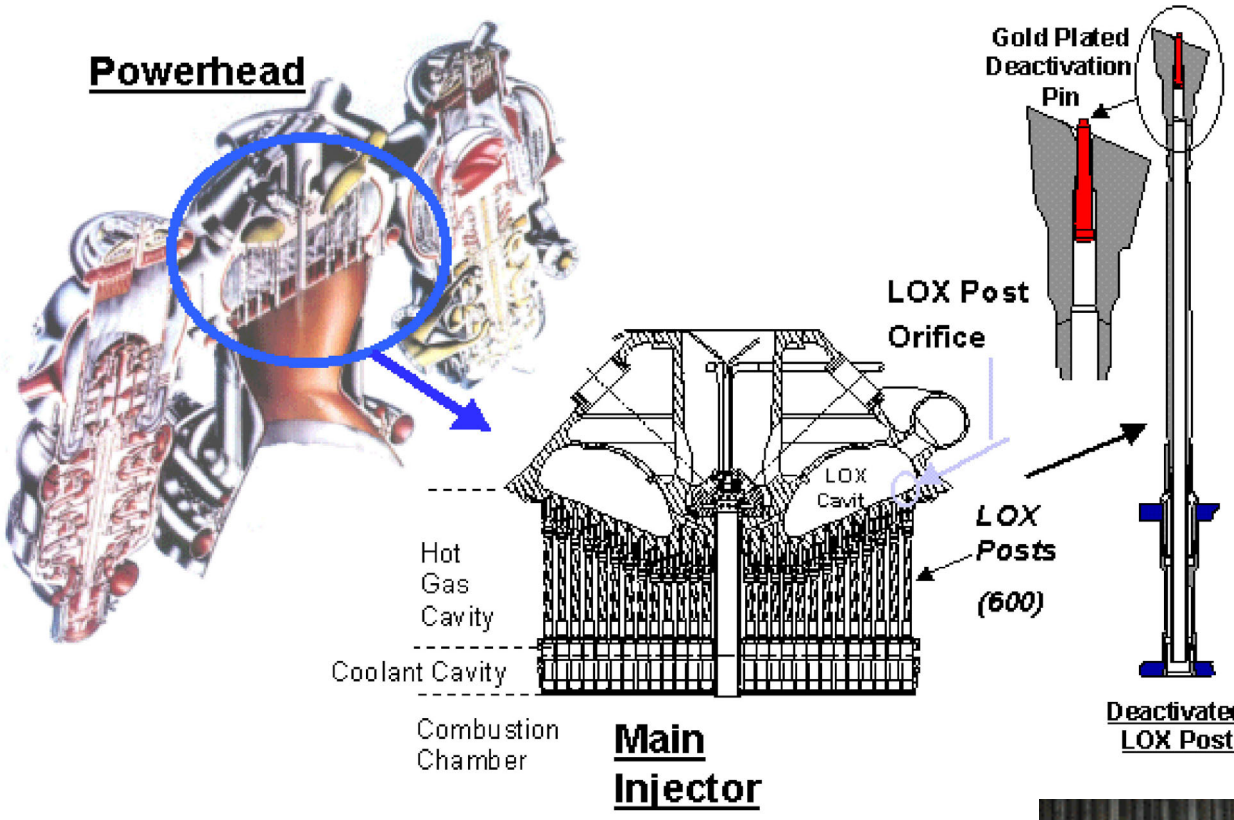
PRACA: Declining PR Count



Case Study: SSME LOX Pin

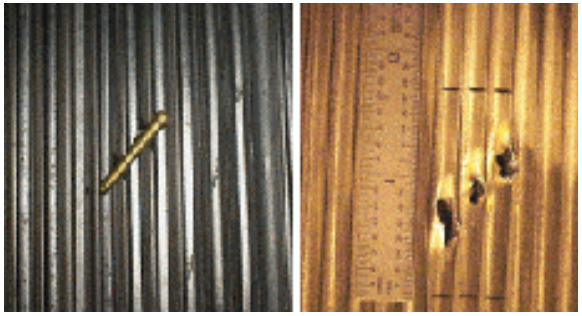
- 600+ LOX Main Engine Injectors are CRIT 1 components that are manufacturing or fatigue life limited (cracking results)
  - Cracked LOX Post could allow combustion within injector head and cause main engine failure
  - Repair consists of pin (1 inch long, 0.1 inch dia.) friction-fitted into post to deactivate injector by blocking LOX flow
  - After pin insertion, vacuum leak checks and engine firing (green run) verify repair
- Pin Ejection IFA on STS-93
  - 2 LOX posts deactivated with standard pin repair
  - 1 deactivation pin ejected upon engine start
  - 3 of 1080 SSME nozzle coolant tubes ruptured
  - 4.5 lbs/sec leak of H_2 (visible on take-off)
  - Premature MECO (0.15 seconds early) and 16 ft/sec underspeed

Pin Ejection IFA on STS-93



Powerhead, Main Injector and Liquid Oxygen Post Details

Ruptured Tubes

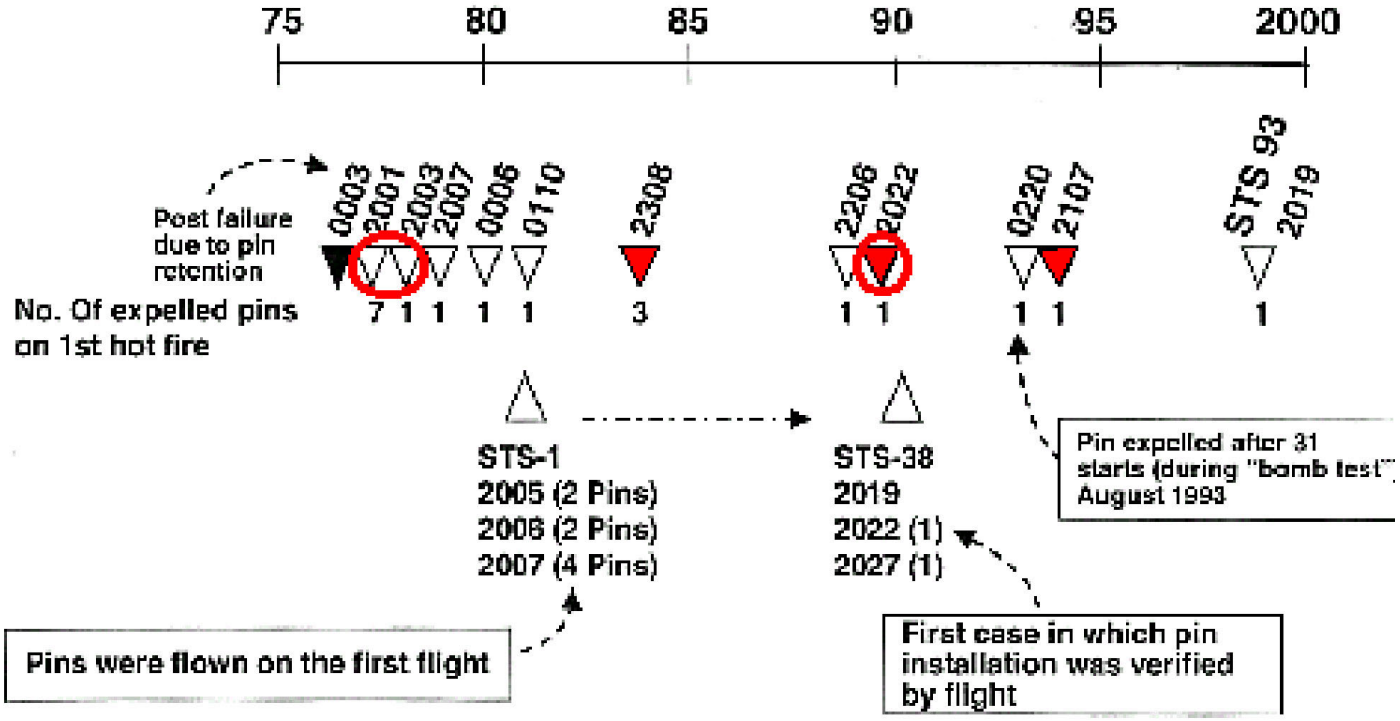


SSME LOX Pin Case: Analysis

- 212 pin repairs have been implemented over course of Program
- 19 of 20 pin loss events occurred during green runs with no damage
- On STS-38 (1990), pinned injector first successfully flown without 'green run.'
- Practice repeated 5 more times with 9 pins and without incident till STS-93.
- Damaged LOX post deactivation historically treated as a standard repair, although repaired LOX post is a CRIT 1R item
- Standard repair allowed optional PRACA data entry, confused CRIT level
- 'Fly as you test, test as you fly' was violated
- Process migration until green run and flight became interchangeable

- ***The real risk was unsuspected***
  - ***One in ten probability of ejection during first hot-fire unknown***
  - ***Potential consequence of pin ejection unrealized in past occurrences (pin ejection is benign)***

Intermittent Reporting of Pin Ejection



Reported in PRACA

Listed on 1994 PR (for 2107) as previous occurrences

Recommended Improvements to Current Processes

- Analyze data bases such as PRACA (when possible); improve probability assumptions; find correlating factors
- Use observed event frequencies, loads, and update FMEA/CIL
- Use quantitative risk assessments and other reliability engineering techniques when possible to aid decision making
- Assess number of concurrent/sequential errors required for events of various criticalities with attention to potential single point failures, especially human ones
- Question assumptions and changes to processes
- Consider system redundancy as last defense

Future Improvements

- New methods for health assessment, and fault detection and correction to minimize need for invasive maintenance
- Methods for modeling, identifying, and assessing organizational and human risks
- Ability to measure/trend adherence to critical processes and procedures
- Predictive rather than descriptive tools for risk assessment
- Ability to address outliers in statistical samples--catastrophic but very rare occurrences
- Improved anomaly and mishap investigation, analysis, and categorization and conduct Agency/industry-wide trending