Integrating Safety and Mission Assurance in Design

Chris Cianciola
Kenneth Crane
Agenda

- Leveraging Lessons Learned
- Integrating Safety and Mission Assurance (S&MA) into design
- Lean, Kaizen, and Six Sigma Practices in Design and Development
  - Ares I-X
  - Ares I
Leveraging Lessons Learned

- Flying with Launch Abort System / In-line Configuration
  - Improving chances for escape in emergencies
  - Reducing ascent debris damage threat

- Using heritage hardware
  - Apollo-derived J-2 engine
  - Shuttle solid rocket boosters

- Upgrading to new hardware where appropriate (e.g. avionics)

- Using weight-saving measures from ET development
S&MA Process Changes – Resources

- S&MA organization elevated from "Office" to "Directorate" level
- Civil Servant staffing increased from 102 in 2002 to 156 in 2006
- Project resources still negotiated with the programs and projects – but S&MA given real appeal authority to address shortfalls
- Resources provided for S&MA Technical Authority, Chief S&MA and others
- S&MA grade structure brought closer to parity with engineering
- New S&MA Vision created and communicated
  - S&MA unique discipline expertise
  - S&MA's role of being part of the effort to find solutions
  - Early S&MA involvement leads to improved quality, safety, and reliability of the design
- Center Director actively championed the rotation of some of the Center's best engineers into S&MA
Agency further transitioning to HQ direct funding for S&MA managers designated as part of the technical authority

S&MA Technical Authority (TA) currently being defined and institutionalized

- Will create a healthy balance between S&MA TA, Engineer TA, and Program/Project Management authority
- S&MA TA will have a seat at every level of management - Level 4 through Level 1
- Will provide S&MA with the authority to assure S&MA requirements are properly implemented in all programs and projects
S&MA Process Changes – Discipline Expertise

- All S&MA personnel required to select an S&MA discipline as the primary area of expertise
- Professional Development Roadmaps (PDRMs) created to identify and list courses, knowledge and the experience necessary to be qualified at the various levels of S&MA discipline development
- Discipline Champions established to train and mentor S&MA personnel in their efforts to develop
- Mandatory Discipline working groups established to provide a forum for discipline development and knowledge sharing - run by Discipline Champions
Performed Failure Mode Effect Analysis (FMEA) on design of Pressurization Control Panel

- **Situation:** A proposal was made to reduce the total number of solenoid control valves that control both the J-2X upper stage engine's LH₂ and LO₂ prevalves and recirculation valves to reduce overall cost and weight while increasing the overall system reliability.
- A formal reliability trade study was requested to quantify the impact on reliability compared to the baseline design.
- The study team examined 4 alternative valve designs that were more fault tolerant.
- **Conclusion:** Design alternative 4 was selected because it provided the highest overall system reliability.
S&MA Value Added – Integrated System Failure Analysis

**Physical timeline**

- **Initiator occurs**
- **Fault development**
- **Functional fault**
- **Explosion occurs**
- **Blast wave forms**
- **Critical Overpressure**

**Treq depends on LAS thrust capability**

**Response timeline**

- **Precursor detected**
- **Escape system activated**
- **CEV generates escape thrust**
- **Safe distance achieved**

Time required for safe overpressure
Integrated System Failure Analysis
Failure Event to Initial Failure Environment

Initiator

Fault

Fault-to-threat development time

Off-nominal time

USE Uncontained Start Failure

- Excessive gas spin flow
- Excessive propellant flow to engine
- Combustion chamber pressure increases
- Engine ruptures locally, explodes & fragments
- Structural tank failure
- Propellant mixes
- Explosion occurs

Decision to abort

Threat/hazardous environment

Initiator-to-fault development time

Warning time + LAS activation

National Aeronautics and Space Administration
S&MA Value Added – System Safety

- Recommended move of pressurization line out of the First Stage cable tray to reduce risk to LSC and avionics
- Influenced common bulkhead monitoring
- Influenced valve design for LH₂ and LO₂ pressurization to maintain fault tolerance
- Opened issue for mitigation of overboard GO₂ venting
S&MA Value Added – Up-Front Quality Involvement

- Manufacturing layout
- Robotic welding tool procurement/acceptance
- Manufacturing Execution System
- Drawing Review
- Phased array ultrasonic weld inspection
- Workmanship Standards
- Process FMEA for TPS (in work)
- S&MA actively engaged in the process
S&MA Today

- Receiving respect for technical expertise
- Becoming an organization where NASA’s best and brightest want to work
- Bringing unique engineering expertise to the table in support of programs and projects
  - Programs see us as a must-have – not a forced-to-have group – and programs request S&MA support beginning with program formulation
  - S&MA can help make systems safer and more reliable; early recognition of vulnerabilities results in fewer re-design efforts
- Actively training and developing its people
- Not only identifying issues, but also helps identify solutions
- Rewarding and acknowledging superior performance
Testing Strategy

- "Test as you fly" strategy
- Ground, flight, and orbital tests
- Ares I-X
  - April 2009
  - Suborbital flight test
  - Combination of operational and mockup hardware
  - Demonstrate ability to control Ares I vehicle

- Additional Ares tests
  - Ares I-Y: First flight of five-segment RSRB
  - Orion 1: First flight of J-2X and Orion
  - 2015: First crewed flight to International Space Station
  - 2018: First flight of Ares V
Ares I-X Mission Overview

- Demonstrate the ascent flight control system
- Characterize and mitigating the roll torque due to first stage motor performance for a vehicle dynamically similar to the operational vehicle
- Demonstrate nominal first and upper stage separation and clearances
- Test the First Stage parachute recovery system and separation/entry dynamics
- Validate assembly and processing flow, as well as launch and recovery operations
Meetings conducted for each vehicle element to incorporate an additional 60 days of schedule margin.

- Events consisted of identifying the following activities:
  - The current state
  - The ideal state
  - A realistic future/target state
  - Assumptions, decisions, and/or actions to be taken to achieve the future state
  - Meeting outputs

- Assuming 60-day change could be made, Ares I-X MMO managing to the earlier launch date.
Identified management need for Lean processes:

- Different parts of Ares I-X organization had conflicting notions of safety conservatisms in flight test
- Resolution: Combined all Ares I-X activities under one Mission Management Office (MMO) under the Constellation Program
- Lean activities also reduced number of review boards by 60%
Lean Event Results

**First Stage**
- **Actions:** Changed hardware delivery schedule, pre-drilled some hardware for quicker assembly, and deferred avionics testing until the hardware reached Kennedy Space Center (KSC)
- **Result:** Reduced amount of touch-labor time by as much as 4 to 30 days, depending on hardware

**Avionics**
- **Actions:** Established hard deadlines for delayed items; condensed and reduced number of check points; verified work on-site at KSC; and rescheduled delivery of some components
- **Result:** Met 60-day goal

**Roll Control System**
- **Action:** Procured support hardware prior to the element’s Critical Design Review (CDR)
- **Result:** Met 60-day goal

**Upper Stage Simulator / Command Module / Launch Abort System Simulators**
- **Actions:** Streamlined procurement process with United Space Alliance (USA) by reducing the legal review time from 42 to 28 days; reordered activities on the launch pad, reducing pad flow from 7.5 days to 5.5 days
- **Result:** Met 60-day goal

**Ground Systems / Ground Operations**
- **Actions:** Streamlined procurement process with United Space Alliance (USA) by reducing the legal review time from 42 to 28 days; reordered activities on the launch pad, reducing pad flow from 7.5 days to 5.5 days
- **Result:** Met 60-day goal

**Systems Engineering & Integration**
- **Actions:** Streamlined (reduced number of) review cycles for Integrated Design and Analysis Development Flight Instrumentation, and Assembly Integration and Test
- **Result:** Met 60-day goal
Leadership commitment

- Ares Projects Office (APO) leaders visited Boeing to learn about 787's market share improvement through lean practices.
- APO leaders requested in-house training for all managers on Lean and Kaizen.
Lean and Kaizen Success Stories

♦ **Lean success stories**
  - Integrated Safety & Mission Assurance earlier in design process
  - Developing and improving manufacturing processes for Ares I Upper Stage
  - Improved communications between vehicle element offices
  - Trained Contracting Officer’s Technical Representatives on value stream mapping

♦ **Kaizen process improvement success stories**
  - Improved the workforce planning process
  - Reduced the length of project integration meetings
  - Improved APO’s risk management process
  - Improved requirements change, trade study, and design review processes

♦ **Kaizen new process development success stories**
  - Optimizing the ground support equipment flow for handling the Ares I Upper Stage
  - Merging the manufacturing flows at the Michoud Assembly Facility
  - Resolving differences in welding and manufacturing processes between NASA and the Upper Stage prime contractor (Boeing)
  - Optimizing the cleaning and corrosion protection processes
  - Automating task description sheets
Ares Six Sigma Practices

- **Ares I Upper Stage Friction Stir Welding Tool**
  - Uses high rotational speed and frictional heat to crush, "stir" together, and forge a bond between two metal alloys.
  - At the end of the weld, the single-piece pin tool is retracted and leaves a "keyhole".
  - To overcome these drawbacks, a Marshall Center welding engineer helped design an automatic retractable pin tool to prevent keyholes.
  - Manufacturing and assembly team applied Six Sigma processes to design an experiment to find the optimum machine settings for ensuring a nominal weld.
  - The analysis developed a set of values for determining the proper settings for welds, as well as determining the effectiveness of a weld if the settings are known but off-nominal.
  - **Result**: Unprecedented level of accuracy and minimization of weld stress.
Ares Team Norms and
S&MA Team Messages

Ares Projects Office Team Norms

- **Treat others with dignity and respect**
- **Make sure your people have the tools they need to be successful**
- **At the end of the day, make sure that everyone's hard work is acknowledged**

**HAVE FUN**
Once in a career opportunity!
We are running a marathon, not a sprint — not in 24/7 emergency mode all the time.

**RESPECT OUR FAMILIES AND OURSELVES - HEALTHY BALANCE BETWEEN WORK AND FAMILY IS ESSENTIAL**

**INTEGRITY IS EXPECTED**
"Look each other straight in the eye, tell the truth, full disclosure"

**TEAMWORK IS ESSENTIAL**
"Our" instead of "my". "We" instead of "I". "Us" rather than "me... we're all important"

**INTEGRATION AMONG THE PROJECT AND WITH PARTNER ORGANIZATIONS (E.G., ENGINEERING, S&MA, OTHER CENTERS, PROGRAM PROJECTS) IS ESSENTIAL**
Communicate, communicate, communicate with each other.
Don't wait on someone else to initiate

**BELIEVE THE BEST ABOUT EACH OTHER (ASSUME NO MALICIOUS INTENT)**

**CONSTRUCTIVE CONFLICT LEADING TO DECISIONS (CLCLOSURE) AND ONCE MADE DON'T CARRY IT PERSONALLY IF IT DID NOT GO YOUR WAY**

**WE WILL HOLD EACH OTHER ACCOUNTABLE AND MEET OUR COMMITMENTS**
Our ultimate commitment is a safe, reliable, affordable delivery of Orion to orbit

**FAILURE IS ACCEPTABLE DURING DEVELOPMENT**
We are willing to take calculated risks to further our knowledge

**EARLY IDENTIFICATION AND HIGHLIGHT OF ISSUES.**

National Aeronautics and Space Administration

7442.21
S&MA in Ares Design – Summary

- Providing more resources to support Ares design work
- Making S&MA more independent for objective assessments
- Improving discipline expertise as well as training and mentoring opportunities for new employees
- Adding value through Failure Mode Effect Analyses (FMEAs)
- Using the Ares quantitative safety and reliability requirement to enforce the “Design for reliability and safety” paradigm shift
- Improving system safety by using a functional analysis system approach to model and understand integrated system failures similar to the Shuttle foam problem.
- Improving design reliability by using Probabilistic engineering physics-based modeling
- Evaluating and understating design uncertainty and design margins using probabilistic engineering techniques
- Getting involved in quality up front using Lean, Six Sigma, and Kaizen practices
- Receiving respect for technical expertise
- Becoming an organization where NASA’s best and brightest want to work
- Bringing unique engineering expertise to the table in support of programs and projects
Questions?

www.nasa.gov/ares