

IAA-99-IAA.6.1.01

PROCESS BASED MISSION ASSURANCE

J. Steven Newman

National Aeronautics and Space Administration (NASA)

Washington, DC 20546, USA

50th International Astronautical Congress
4-8 Oct 1999/Amsterdam, The Netherlands

For permission to copy or republish, contact the International Astronautical Federation
3-5 Rue Mario-Nikis, 75015 Paris, France

“PROCESS BASED MISSION ASSURANCE MODEL”

J. Steven Newman

National Aeronautics and Space Administration
Washington, DC 20546, USA

Abstract

This paper presents a model for management of mission success in complex high technology programs. Process Based Mission Assurance (PBMA) is defined as implementing those management and systems engineering processes necessary to manage inherent aerospace program risks and maximize the likelihood of mission success. The PBMA model is derived from extensive benchmarking of “best practices” in aerospace, electronics, and automotive manufacturing, reinforced by “empirical evidence” derived from evaluation of selected NASA programs. The model has been developed to be consistent with U.S. government performance-based contracting initiatives. The model provides a framework of high-level government expectations or “whats,” within which contractors have the flexibility to identify and implement their own process “hows.” The paper develops the hypothesis that regardless of contract form or procurement type, complex and demanding aerospace projects require a minimum set of processes necessary to assure safety, manage inherent aerospace program risks and maximize the likelihood of mission success. The paper develops the PBMA model centered on ten key elements, each element reflecting the themes of life-cycle risk management and defect/mishap prevention. The paper uses the PBMA template to evaluate

a broad range of ongoing NASA initiatives, identifying the individual approaches deployed to manage risks and achieve mission success.

Introduction

The PBMA model has been used as an evolutionary yardstick for evaluating NASA technology development and space program assurance process implementation. The model provides the basis to support development and accomplishment of assurance process requirements in new programs.

PBMA Model: Return-to-Basics Assurance Management

New Age Business Practices - an Eroding Sense of What Is Required

Government re-engineering and re-invention initiatives have succeeded in streamlining business practices at many Federal agencies. NASA has been at the forefront of this philosophical change with Administrator Daniel Goldin’s call for Better/Faster/Cheaper programs. While business and accounting practices are moving toward greater efficiency the programmatic results are a mixed bag. Noted successes include the acclaimed Mars Pathfinder mission which provided live video from the Martian surface 36 months and \$150M after program start. Noted failures have also include the \$71M Lewis spacecraft which was lost in orbit three days after launch, and burned up during re-entry a month later. While

Copyright © 1999 by the American Institute of Aeronautics and Astronautics Inc. No copyright is asserted in the United States under Title 17, U.S. Code. The US Government has royalty-free license to exercise all rights under the copyright claimed herein for Government purposes. All other rights are reserved by the copyright owner.

visionary, and in many ways necessary to lead change in the way NASA conducts business, the reality is that Better/Faster/Cheaper has often been left to interpretation by individual NASA program managers and their industry partners. Concurrently NASA procurement initiatives such as cooperative agreements, “announcements of opportunity” acquisitions, and performance-based contracts have focused on defining the “what,” allowing the contractor to develop the “how.” Thus traditional proscriptive assurance requirements such as NASA 5300.4 or Mil-Q 9858A have been eliminated in most new contracts. At the same time a wide perception gained favor that government assurance activities are redundant, or unnecessary and this has led to a series of initiatives designed to cut back or streamline surveillance and inspection approaches. Examples include reduction in Government Mandatory Inspection Points (GMIPs), as well as reduction in the government in-line approval role where contractors can demonstrate that their manufacturing processes are stable, capable and controlled. The reduction of government oversight and work process specification is being implemented, in-part, using the Single Process Initiative (SPI) to establish a single quality management system for multiple government customers at each contractor facility. It remains to be seen whether or not a single common process will adequately satisfy unique safety-critical and/or mission-critical assurance needs. Another element in this new business approach is pressure to diminish the NASA (government) role in design, design verification and test reviews as well as in forums established to resolve flight anomalies or mishaps.

Silver Bullet Assurance Thinking

The period of New Age procurement and acquisition has been coupled with “Silver Bullet” assurance thinking, the belief that heavy emphasis on one or more tools in the

assurance process inventory will necessarily lead to success. Examples include:

- Integrated Product Teams
- Advanced Quality practices
- Risk Management
- Key Characteristics management

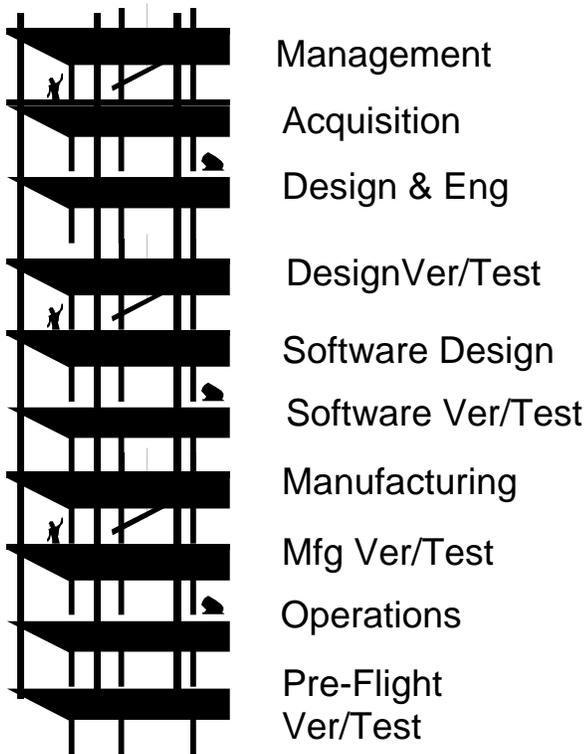
Indeed, all of these items are key elements in the “solution set” of things which must be done but no single assurance tool or activity (i.e., silver bullets) allows you to achieve mission success. While risk management thinking is offered as a backbone philosophy, no one discipline (e.g., formal risk management) is put forward as the key to success. The PBMA approach underscores the need for complete, thorough, across the board assurance process implementation.

Old Testament Rules & Consequences: A Risky Business

Going into space, or flying at hypersonic speeds at the edge of space are “Old Testament” endeavors (follow the rules or suffer the consequences). One must follow the rules of complete, thorough, time-tested systems engineering and management discipline. Cutting corners will expose the program to risks greater than those already inherent in aerospace programs. The most reliable launch system (Space Shuttle) has experienced an approximate 1 % failure rate. Expendable launch vehicles (ELV’s) have historically failed approximately 5% of the time. To put the discussion into a proper risk perspective, consider the following. The ELV failure probability is on the order of 100 times higher than probability of death for participants in high risk sports such as scuba diving, mountaineering and boxing, and is 200 times more likely than death in a skydiving mishap (U.S. Hang Gliding Association and National Safety Council statistics). NASA obviously wants and needs to drive space flight failure probabilities down as far as possible:

protecting the public, protecting the lives of our astronauts and employees, and helping our unique one-of-a-kind payloads to reach their destinations.

The inherent risk in achieving orbit is mitigated in the commercial communication satellite business model through purchasing insurance. The model works. However, insurance does not provide similar satisfaction when NASA loses a high-value scientific payload or a human life.



PBMA Elements

The PBMA Model

The PBMA model consists of the ten basic assurance process elements depicted in the “framework” graphic shown above. The PBMA elements parallel a typical project life-

cycle reflecting the importance of life-cycle assurance thinking. The backbone of the PBMA approach is risk management thinking and the recurrent use of the risk management discipline: identification and analysis of failure modes, hazards, sources of variation, etc.), planning for control & mitigation of potential failure mechanisms, 3) documentation, review and tracking of identified risks. “Eyes-open,” program acceptance, of residual risks is an element in informed management decision making.

Embedded Risk Management Thinking and Behavior



How can it fail? Could someone get hurt? How likely would that be? Can we prevent that from happening? OK,...let’s redesign or do something to make this less likely. By the way, keep tabs on this until we find a solution. And finally, we are going to get an outside group of experts to look at our project to see if we are really as good as we think we are.

Risk management serves as a philosophy, a “way of thinking”, or mental discipline as well as a formal tool within the PBMA model. Complex aerospace systems require special care. The laws of physics demand certain rigor and thoroughness in design, manufacturing and operations, regardless of contract vehicle. Even (or especially) Faster/Better/Cheaper

programs should adhere to the PBMA framework, achieving economies through innovative implementation of the philosophy which allows (program and contractor) management flexibility in implementing “best practices” and processes within the PBMA framework. The processes encompassed in the PBMA model (and its risk containment philosophy), while not guaranteeing mission success will provide the best chance for a program to succeed. Failure to implement documented assurance processes or failure of people within good processes will always remain as possible sources of program failure. Consequently, management vigilance, leadership, and visibility into process implementation (management assurance activities) is essential. As discussed below, management assurance processes serve as the glue that binds together and provides discipline for overall PBMA implementation.

Ultimately the validation of the PBMA life-cycle assurance approach is in the results achieved by smart, serious, successful program managers who indeed choose to implement multiple processes in each of the PBMA areas.

PBMA Overview

Table 1 provides a summary of “best practice” risk identification and risk control/mitigation processes within each of the PBMA elements. A brief narrative for each element is provided in the following paragraphs.

Management Assurance Processes

A documented and vocal top level management commitment to mission assurance and risk management is a necessary first step leading to establishment of management assurance processes including policies, procedures and documented requirements. Other key concepts include development of an assurance management strategy and implementation of assurance plans including a formal risk

management plan. Management risk control concepts include audits to verify program and contractor assurance process implementation, assurance control boards, independent assessment, and formal management assurance reviews. Complex risk management issues invariably benefit from an informed and knowledgeable second opinion. Independent assessments are also applicable to design, engineering, manufacturing and operational activities.

Acquisition Assurance Processes

The procurement/acquisition process sets the stage for mission success ...or failure. Acquisition teams must be staffed with knowledgeable, experienced personnel from the right mix of functional disciplines including safety and mission assurance. The discipline of risk management must be inserted in the earliest project formulation activity. NASA has initiated a “Risk-Based Acquisition Management” (R-BAM) program intended to integrate risk management thinking throughout the acquisition process. This initiative will require changes to the NASA FAR supplement to include risk management as a mandatory acquisition planning element, and inclusion in mission suitability criteria for source evaluation boards. Risk Management will also be included as a technical element in award fee determination and serve as a core factor in contract surveillance planning.

Design & Engineering (D&E) Assurance Processes

D&E assurance processes emerge from systems thinking. Best practices include concurrent development of manufacturing, test, and assembly processes, and process controls. Other D&E assurance concepts include use of cross-functional teams, key product characteristic (KPC) identification and control, robust design (minimum set of KPC’s). D&E risks are further mitigated through use of computer-aided manufacturing and design tools

which can simultaneously provide multiple access, communication and configuration management. Design simplification (part count reduction and simplification), and use of proven technology and/or commercial off-the-shelf systems and sub-systems can control risk. D&E risk identification tools include first and foremost Failure Modes and Effects Analysis (FMEA). Successful programs extensively employ FMEA and other structured logic techniques (e.g. fault trees, Fishbone or Ishakawa Diagrams, etc.). to provide insight into how a product, process, machine, activity, or operation could fail, and the consequences of various “failure modes”. Design margin and design conservatism provide a further means to mitigate risks associated with unknown errors which inevitably exist in modeling complex systems and expected environments.

D&E Verification & Test Assurance Processes

Design verification is a critical assurance activity which is typically accomplished through test (the preferred method), analysis, similarity (heritage), modeling, or through a combination of these approaches. D&E verification relies on the fidelity of the test equipment/test scenario, the applicability and assumptions contained in analyses and models, the absence of unknown synergistic effects, applicability of component testing data and the ability to accurately define and simulate complex environments. All of the programs surveyed in this paper devoted significant attention and resources to design verification and testing.

Manufacturing Assurance Processes

Key manufacturing and production assurance (risk control) concepts include establishing and quantitatively demonstrating critical process capability, stability, and control. Formal process certification approaches can achieve all three objectives. Process FMEA and process proofing activities can serve to identify process risks. The use of process fail-safing can then

provide controls or mitigation for existing process failure modes. Innovative process surveillance and inspection activity, such as the Space Shuttle Structured Surveillance Program, can provide the necessary levels of risk control for flight critical production activities.

Manufacturing Verification & Test Assurance Processes

Typically, manufacturing and production processes include thousands of potential failure modes. Examples include defects in raw materials, lack of workmanship discipline, and improper transportation or handling of assembled components, to mention only a few. Testing assurance activities must span the entire build process. The criticality of the production activity, the demonstrated process capability, and stability all help determine how and when to conduct production testing. Post production tests provide a way of identifying system assembly problems which may appear at interfaces between (previously tested) sub-systems and components.

Software Design Assurance Processes

Configuration management is a central software assurance activity. A senior systems engineer once described the problem with software management as “people who are used to managing fixed things (mechanical/electrical hardware elements) are confronted with managing software ... a product that wants to change every second.” Formal software safety analysis, software hazards analysis, software risk management, and software quality control planning form a minimum baseline assurance approach for software performing flight critical (life critical) functions. Software design simplification and the use of proven (heritage) software, when applied properly, can further reduce mission risk.

Software Verification & Test

The old adage ..“test what you fly and fly what you test” is enduring. The use of the flight vehicle as the ground-based software test-bed is a clearly preferred practice. The use of flight simulators or simulation laboratories is a second choice. Independent verification and validation of critical software is always a best practice. The testing approach must necessarily reflect the software maturity, heritage and application.

Operations Assurance Processes

System safety planning which incorporates hazard analysis, control and mitigation is a fundamental operations assurance activity. Operations FMEA and Operations Readiness Reviews are other important risk identification and control methodologies. Contingency and emergency preparedness planning are essential risk control measures.

Pre-Flight Verification & Test

Pre-flight verification and test includes the final testing and checkout of flight hardware along with the formal reviews which precede flight operations. Assurance activities include pressure system and propellant leak testing, control system functional testing, hydraulic system tests, and composite electrical systems tests. Operations verification reviews include launch readiness or flight readiness reviews close to the day of launch, typically preceded by a series of daily reviews during the week prior to operations. Other management reviews may be conducted in prior weeks. Each forum typically identifies current flight system issues, identifies planned disposition or corrective action and tracks closure or resolution.

If you are serious about success...and an insurance settlement is unsatisfactory.... You have to do it all

Assurance as Insurance

The PBMA elements can be considered equivalent to a basic insurance policy for any program in which the cost and effects of failure can not be satisfactorily addressed through an insurance settlement or a budget augmentation. This potentially includes timing-critical planetary exploration missions, multiple, inter-dependent space platform launches, space station re-supply missions, and one-of-a-kind planetary explorers or great observatories. NASA high-value assets are invariably linked to teams of scientists and investigators who have worked for years to develop and build their specialized instruments and ground based command/control and data management infrastructure. Assurance processes must be implemented in every major system supporting these critical missions including the launch vehicle, spacecraft bus, payload (instruments) and critical ground support equipment.

Table 1 Process Based Mission Assurance Model

Assurance Process	Risk Identification Processes		Risk Control & Mitigation Processes	
Management	<ul style="list-style-type: none"> - Management reviews - Self audit - ISO certification audit - Independent assessment - Performance metrics 		<ul style="list-style-type: none"> - Documented management & administrative processes (ISO 9001) - Top level assurance requirements documents - Assurance Planning - Risk Management Planning - Configuration control - Control Boards 	<ul style="list-style-type: none"> - Program Commitment Agreements - Independent Assessment (Informed, knowledgeable second opinions) - Management Review - Audit - Adequate staffing, - Proper skill mix - Training,
Acquisition	<ul style="list-style-type: none"> - Evaluation of past performance - Pre-Award Audit - Thorough and complete RFP - Procurement risk assessment 		<ul style="list-style-type: none"> - Risk Based Acquisition Management (R-BAM) - Knowledgeable, skill-balanced acquisition team - Clear documented policies - Clear assurance policy requirements 	
Design & Engineering	<ul style="list-style-type: none"> - Concurrent Eng. - FMEA - Fault Tree Analysis - PRA - KPC Analysis 	<ul style="list-style-type: none"> - DFA/DFM analysis 	<ul style="list-style-type: none"> - Factors of Safety - A-Basis allowable design - Robust design - Mature (proven) design - Simplified design 	<ul style="list-style-type: none"> - Buildable design - Testable Design - Fault tolerant design - Inspectable design
Design Verification & Test	<ul style="list-style-type: none"> - Test (Coupon, sub-system, system) - Simulation - Analysis - Test articles 	<ul style="list-style-type: none"> - Independent engineering analysis - Independent analytical modeling 	<ul style="list-style-type: none"> - Design Reviews (PDR, CDR, DCR) - Independent Assessment (informed, knowledgeable second opinions) 	Removes ignorance about synergistic and integrated system failure modes

FMEA-Failure Modes & Effects Analysis	PDR – Preliminary Design Review	RFP – Request for Proposal	ISO – International Standards Org.
PRA-Probabilistic Risk Assessment	CDR – Critical Design Review	DFA/DFM – Design for Assembly/Design for Maintainability	S/W – Software
KPC – Key Product (Process) Characteristics	DCR – Design Certification Review		Q/A – Quality Assurance

Table 1 (continued) Process Based Mission Assurance Model

Assurance Process	Risk Identification Processes		Risk Control & Mitigation Processes	
Software Design	- S/W Hazards Analysis - S/W FMEA	- Software Safety Anal. - S/W Fault Tree Anal.	- Design Requirements - Design Planning - Configuration Control	- S/W QA Plan - Milestone Reviews
Software Verification & Test	- Formal Test Plan - Requirements Verification and Management Plan - Independent Verification & Validation - Flight Simulation (Fly the s/w) Laboratory		- Integrated Software/Hardware Testing - Subroutine level testing - “Formal Methods Inspection” - Technical Review Boards	
Manufacturing	- Process FMEA - Key Characteristic Identification - Statistical Process Control - Variability analysis - Supply chain audit		- Work Control Processes - Work Review Processes - Change Control Processes - Process fail-safing - Process Certification - Electronic data sharing, - Early supplier involv.	- Self Audit - Supply chain audit - ISO Cert. Req. Suppliers - Surveillance & inspection
Manufacturing Verification & Test	- Production Verification Testing (Pressure vessel proof testing, structural static loads, end-to-end electronic check-out) - Acceptance Testing		- Hardware pedigree (non-conformance) review - Independent Assessment - Hardware Build Reviews	
Operations	- Hazard analysis - System Safety Analysis - Grd. Trans. FMEA - Move/Lift/FMEA	- Range Safety Risk and Hazards Analyses - Env. Impact Ass. - Orbital Debris Risk Eval.	- Operational Read. Reviews - Emergency Prep. Planning - Contingency Planning - Operations Simulation - Flight Termination Sys.	- Independent Assessment - Certificate of Flight Readiness - Flight Read Reviews
Pre-Flight Verification & Test	- Flight software operational verification testing - Composite System Tests		- Wet Tanking Demonstration Test	

FMEA-Failure Modes & Effects Analysis PRA-Probabilistic Risk Assessment KPC – Key Product (Process) Characteristics	PDR – Preliminary Design Review CDR – Critical Design Review DCR – Design Certification Review	RFP – Request for Proposal DFA/DFM – Design for Assembly/Design for Maintainability	ISO – International Standards Org. S/W – Software Q/A – Quality Assurance
---	--	--	---

Validation Test Cases for the PBMA Model

The best practices and examples shown in Tables 1 have been derived from the five major NASA program areas described below:

Space Shuttle Super Lightweight Tank (SLWT): a human-rated launch system and the pioneering use of 2195 aluminum-lithium in a major structural application (Lockheed-Martin Michoud Assembly Facility).

X-33 Advanced Technology Demonstrator: a prototype single-stage-to-orbit, space plane (Lockheed-Martin Skunkworks) developed under a cooperative agreement with minimal government-imposed safety and mission assurance requirements. This non-traditional “better, faster, cheaper” project is funded at approximately \$1.2 Billion.

X-34 Technology Test-bed Demonstrator: (Orbital Sciences): a reusable space plane prototype being developed under a firm fixed price contract (approximately \$70 million); incorporates few government-imposed safety and mission assurance requirements.

Space Shuttle Ground Operations: (United Space Alliance or USA): this contract represents a “first time” contracting-out of safety critical functions previously directly managed/approved by NASA civil service personnel.

NASA Expendable Launch Vehicle (ELV): launch service contracts which incorporate government (assurance) approval and insight roles but leave primary assurance process implementation with the contractor.

Comparative Observations

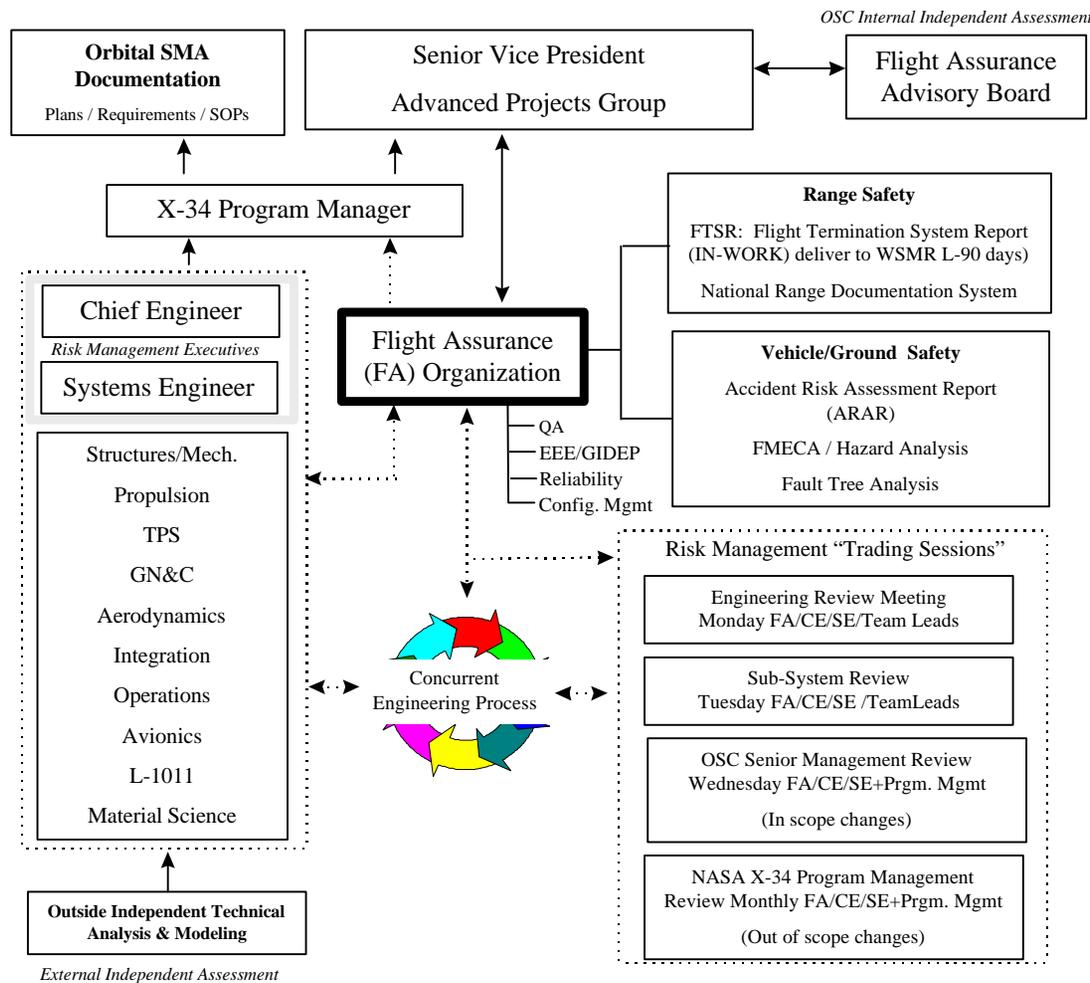
All of the reviewed programs contain basic aerospace risk management and program assurance processes, including extensive planning for mission success, as well as formal and informal risk management approaches. Each NASA managed program conducted some form of risk management, (i.e., risk identification & analysis, planning for risk control and/or mitigation, documentation an tracking of control & mitigation) throughout the project life-cycle. All programs incorporated design margin / redundancy / fail-safing and heavy emphasis on systems thinking. Each program employed FMEA / hazard analysis /fault tree, etc. Each program employed risk review / documentation & tracking. Each program employed independent assessment, as well as planning, practice and training for operational scenarios where things go wrong. Many of the operational and design risk identification and mitigation processes were mandated by the US military range requirements. Most of the programs continue to reflect fundamental Mil-Q 9858A thinking.

Assurance Process Mapping

The broad dispersion of assurance activity across a program (...a good thing) often makes it difficult to find a single individual who has knowledge or understanding of assurance process implementation. Assurance process mapping has helped NASA management achieve a better understanding of how sometimes complex administrative models support the implementation of assurance activities. An example from the X-34 program is provided below.

Top Level Assurance Process Map for the X-34 Project

An assurance-centric picture of who is doing what to keep it safe, manage risk and make it work allows all levels of management and every player in the project to see how assurance activities fit together. Lower level process maps were also assembled showing relationships with: 1) assurance function providers established through task agreements, 2) OSC suppliers, and 3) government agencies responsible for surveillance and insight.



The X-34 Example

- Independent Flight Assurance (FA) manager reporting direct to senior management
- Independent Review Function (Flight Assurance Advisory Board)
- "Hard-lined" assurance responsibilities of FA manager identified
 - Range Safety
 - Flight Safety
 - Ground Safety
- FA access and participation in programmatic risk management and concurrent engineering forums

Conclusion

Planning for and implementing the ten assurance elements described in this paper is essential to the success of any NASA (or other serious) aerospace undertaking. The ten PBMA elements should be considered a necessary starting point on the road to mission success.



Consistent with performance-based contracting philosophy, the implementation “how,” is not explicitly prescribed. The depth and extent of implementation within each PBMA element must be defined by program risk managers. Ignoring any element in the PBMA model is to assume unreasonable risk.

Better/Faster/Cheaper (BFC) does indeed require better, more rigorous, more complete risk management thinking which is the underpinning of the PBMA model. As greater freedom and greater responsibility shifts to the contractor to do the job right, (exercising assurance discipline and critical process control) it is important to reaffirm NASA expectations for comprehensive assurance process implementation throughout the program/project life-cycle. The PBMA model provides a framework to achieve that goal.

References

1. “Space Shuttle Super Lightweight Tank – Independent Assessment of Risk Management Activities,” NASA Headquarters, Office of Safety & Mission Assurance, SLWT, December 12, 1997.
2. X-33 Safety & Mission Assurance Review, NASA Headquarters, Office of Safety & Mission Assurance, March 5, 1998.
3. X-34 Safety & Mission Assurance Review, NASA Headquarters, Office of Safety & Mission Assurance, June 17, 1998.
4. “Process Readiness Review, Space Shuttle Program, Space Flight Operations Contract (SFOC), United Space Alliance, An Independent Assessment of SFOC/ USA-Ground Operations, NASA/SFOC Flight Operations, and NASA/KSC Safety & Mission Assurance,” NASA Headquarters, Office of Safety & Mission Assurance, October 27, 1998.
5. “Space Shuttle Ground Operations Independent Review of United Space Alliance Strategic Initiative Implementation, - *Process Modernization and Re-Engineering*,” NASA Headquarters, Office of Safety & Mission Assurance, April 19, 1999.
6. “Life Cycle Risk Management Elements for NASA Programs, A Program Manager’s Guide to Faster / Better & Cheaper,” J. Steven Newman, Senior Technical Advisor, Office of Safety & Mission Assurance, National Aeronautics & Space Administration, June 1997.