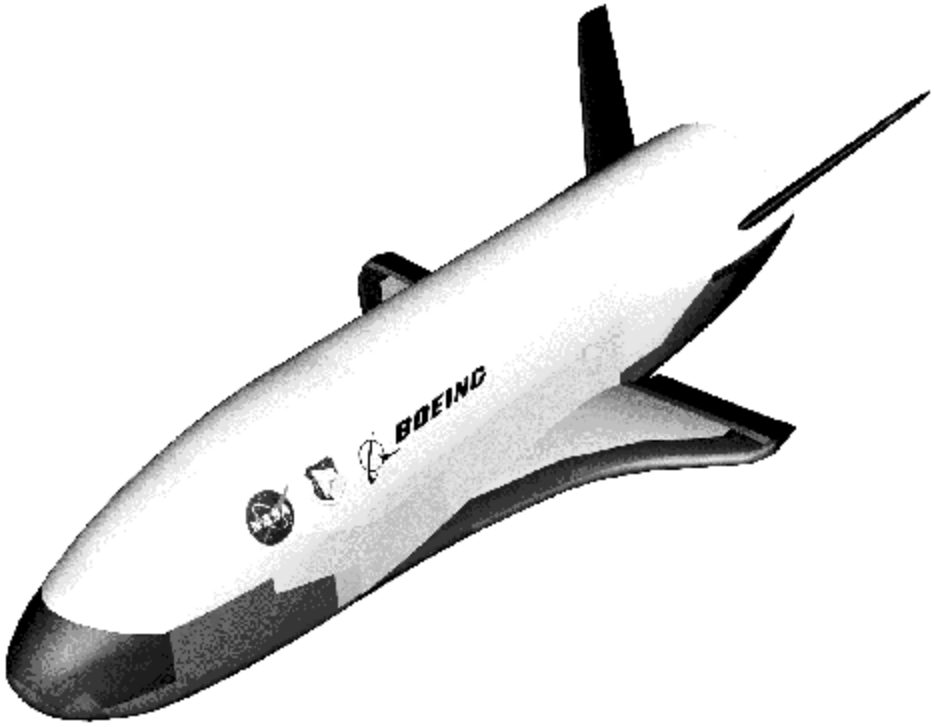
Independent Assessment of X-37 Safety & Mission Assurance Processes and Design Features



NASA Headquarters
Office of Safety & Mission Assurance
June 18, 2001

Executive Summary

Background

The safety and mission assurance (SMA) management processes for the X-37 program, were reviewed by the NASA Headquarters Office of Safety and Mission Assurance (OSMA) during the January - March 2001 time period. The review process included document examination, structured telephone interviews with key process owners, and an onsite review at Boeing, Seal Beach on January 31 - February 2, 2001. Knowledge derived from reviews, examination of process documentation, obtaining objective evidence of process implementation, establishing confidence in reliability and expected casualty (Ec) analyses, and participation in flight/operational readiness review process will provide the basis for NASA AA/SMA endorsement decisions concerning:

- Signature on flight or operational readiness documents (e.g. CoFR)
- Third-party indemnification endorsement/non-concurrence

This review fulfills, in part, the government management responsibilities to assure public safety, exercise care in management of financial resources, and promote the likelihood of achieving mission success.

The X-37 program is managed by the NASA Marshall Space Flight Center (MSFC) and conducted by Boeing. Formulated as a cooperative agreement, NASA is not only the sponsor but also a risk-sharing partner in the program. As the X-37 industry partner, Boeing has requested that NASA grant indemnification against any third-party lawsuits that may result from the operation of the X-37 vehicle. In order to qualify for indemnification, the developer (contractor/industry partner) must establish, by law (Section 435 of Public Law106-74), to NASA's satisfaction, compliance with NASA-prescribed safety procedures and practices. At present, the Boeing request includes only the proposed Space Shuttle de-orbit, reentry, and landing phase of the flight test program. Boeing's request may be amended in the future to include a precursor series of unpowered B-52 drop tests.

Findings: X-37 Assurance Process Management

In general, the OSMA Independent Assessment Team (IAT) found that key Boeing life-cycle assurance processes have been established.

Findings: Reliability Estimates

The team has significant concerns regarding the development of X-37 reliability estimates and the application of those estimates in satisfactorily demonstrating compliance with range safety requirements.

Findings: NASA Assurance Management

The MSFC X-37 program office and SMA organization must coordinate their mission assurance efforts to ensure appropriate follow-through regarding the industry partner Boeing's implementation of the required SMA processes. In the case of NASA safety and mission assurance activities, additional personnel resources are required to provide the necessary surveillance, insight, and independent assessment capability for the X-37 program.

Conclusion

While the X-37 program has many excellent safety, risk management, and assurance processes in place, the IAT cannot presently support a preliminary letter of endorsement for the X-37 program. Specific reservations include:

- the level of maturity and fidelity of the X-37 reliability analysis and methodology is inadequate and does not provide confidence that the program will satisfactorily meet the Ec range safety criteria.

- the NASA MSFC/SMA staffing is inadequate to provide ongoing verification and objective evidence that assurance processes are being effectively implemented.

Addressing the recommendations contained in section 5.0 represents a necessary first step in acquiring the NASA AA/SMA endorsement for either a third-party indemnification request or a certificate of flight readiness.

Table of Contents

1.0 Introduction

1.1 Purpose

The X-37 industry partner, Boeing-Seal Beach, has requested NASA to grant indemnification against third party lawsuits stemming from the operation of the X-37 vehicle. To qualify for indemnification, the developer (contractor/industry partner) must establish, to NASA's satisfaction, compliance with NASA-prescribed safety procedures and practices as outlined in the following section. At present, the Boeing request includes only the Space Shuttle de-orbit, reentry, and landing tests. Boeing's request may be amended in the future to include the B-52 drop tests, as well.

1.2 The Law

Section 435, "Insurance; Indemnification; Liability. (a) Amendment: The National Aeronautics and Space Act of 1958 (42 U.S.C. 2451 et seq.)" of Public Law 106-74 authorizes NASA to indemnify the developers of "experimental aerospace vehicles" against death, injury, and property damage claims by third parties. The statute establishes three prerequisites before NASA can make indemnification available:

- The developer must establish, to NASA's satisfaction, compliance with NASA-prescribed safety procedures and practices.
- The developer must obtain insurance in the amount NASA determines (but not exceeding the "maximum probable loss") against third party losses associated with vehicle operations.
- Government and each developer must execute appropriate cross-waivers of claims

Specifically, Section 435 has been amended to state:

> "EXPERIMENTAL AEROSPACE VEHICLE
>
> (b) Terms and Conditions:
>
> Safety review required before administrator provides insurance: The Administrator may not provide liability insurance or indemnification under subsection (a) unless the developer establishes to the satisfaction of the Administrator that appropriate safety procedures and practices are being followed in the development of the experimental aerospace vehicle."

The above information was excerpted from the Conference Report on H.R. 2684, Departments of Veterans Affairs and Housing and Urban Development, and Independent Agencies Appropriations Act, 2000 (House of Representatives - October 13, 1999).

1.3 Independent Assessment Background and Methodology

The Office of Safety and Mission Assurance (OSMA) conducts independent assessments to identify and evaluate processes employed by prime contractors, NASA program management, and the NASA Center safety and mission assurance (SMA) organizations as an Agency due diligence management function. The independent assessment methodology and approach is based on the OSMA Process Based Mission Assurance Knowledge Management System (PBMA-KMS) model (see paragraph 1.5).

In general, the independent assessments conducted by the OSMA proceed in the following phases:

- Discovery
- Data Synthesis and Evaluation
- Factual Review Draft and Final Report Preparation

1.3.1 Discovery

The Discovery phase begins with the identification, collection, and review of all pertinent documentation. This typically includes all relevant NASA policy documents and standards including Lead Center policy documents, SMA Annual Operating Agreements (AOA), Lead Center documented procedures, Memorandums of Understanding (MOU's), the Program Committment Agreement, the Program Plan, the Project Plan and the Cooperative Agreement. In addition, all pertinent program management, systems engineering, and assurance planning documents are reviewed.

The next step in the Discovery phase involves the conduct of individual interviews with the principal assurance process owners. This is usually accomplished by holding an initial series of telecons that may be supplemented by additional telecons were further information or clarification is required.

The final step in the Discovery phase involves an onsite visit usually conducted at the facilities of the primary contractor or industry partner. The purpose and scope of the initial onsite assessment is described in further detail in paragraph 1.4.

Thus, the documentation review, process owner interviews, and the onsite visits represent the principal mechanisms by which objective evidence is obtained to verify assurance process fidelity and implementation.

1.3.2 Data Synthesis and Evaluation

Based on the information obtained during the Discovery phase of this assessment, the review team typically develops an assurance process map. The purpose of this map is to capture in a single organizational/functional flow diagram the totality of the mission assurance activities, key participants, and principal interfaces which are in place to assure

safety, manage risk, and maximize the likelihood of mission success. A detailed description of the X-37 process map is provided in paragraph 3.7 of this report.

1.3.3 Factual Review Draft and Final Report Preparation

The assessment team prepares a factual review draft, comprised of factual or objective evidence compiled by the review team. This draft is submitted to the organization(s) under review and to those individuals who were interviewed during the telecons and onsite visits for review and comment. The revised/corrected factual review draft is subsequently combined with the review team's findings, observations, conclusions, and recommendations. This is submitted for an internal review and evaluation. Final report preparation follows.

1.4 Process Based Mission Assurance (PBMA) Philosophy

OSMA's evaluation of third-party indemnification requests and support of certification of flight readiness (CoFR) activities follows a simple "define-verify-certify" approach. The process begins with an independent assessment of the program through a Process Readiness Review (PRR). The PRR is a life-cycle systems engineering assessment of the safety and mission assurance processes employed by a program to Make it Safe, Make it Work and Manage Risk. The PRR requires prime contractors and program managers to identify and define specific assurance plans and processes to be developed and implemented on the program/project. Subsequent to the PRR, ongoing implementation of the SMA plans and processes will be verified by the NASA Lead Center SMA organization. Finally, certification of flight readiness and a final decision concerning third-party indemnification requests is established and certified through future assessments which include the OSMA-required Operational Readiness Review (ORR) and the programmatic Flight Readiness Review (FRR).

This philosophy is described in further detail in the following table:

	Mission Success Management Approach: Developing the Knowledge and Understanding Necessary to: Protect the Public, Astronauts and Pilots, the NASA Workforce, and High-Value Equipment and Property	
	Objectives	Means
1	**Define:** Assurance Processes and Design Features	- Process Readiness Review (PRR) - Development of Assurance Process and Design Feature Baseline Document
2	**Verify:** Implementation of stable, capable, and controlled processes	- Lead Center SMA and Program/Project Management surveillance/insight - Contractor/Subcontractor Activities
3	**Certify:** Operational Readiness	- Operational Readiness Review (ORR) - Lead Center formal Flight Readiness Review (FRR) process

This report documents the X-37 PRR which, as described above, constitutes the initial assessment and evaluation of the X-37 program's assurance processes and activities as established and implemented by the Marshall Space Flight Center (MSFC) program office, the MSFC/SMA organization, and the industry partner Boeing.

The X-37 PRR was conducted at Boeing, Seal Beach on January 31-February 1, 2001. The PRR included presentations by NASA X-37 program management, Boeing program management and process owners, and the US Air Force Flight Test Center. Attendees included representatives from:

- NASA Headquarters, Office of Safety and Mission Assurance
- NASA Headquarters, Office of Aerospace Technology (OAST)
- NASA MSFC
- NASA Dryden Flight Research Center (DFRC)
- Federal Aviation Administration (FAA)
- United States Air Force (USAF) Air Force Flight Test Center (AFFTC)

1.5 PBMA-KMS Model

OSMA has developed and employs the PBMA-KMS model as the basic framework against which to assess the capability and fidelity of NASA programs. The model, described below and depicted in figure A.1, represents the best of current industry and government practices for assuring safety, managing risks, and maximizing the likelihood of mission success. The model provided the basis for assessing previous NASA X-vehicle (X-33 and X-34) program eligibility for third-party indemnification as required. It has also been used to evaluate the capability and stability of Space Shuttle Ground Operation processes employed by United Space Alliance (USA) at KSC, and to conduct an independent assessment of the NASA ELV launch services program. The PBMA-KMS model is available on the web at http://pbma.hq.nasa.gov.

1.5.1 Model Description

The PBMA-KMS model provides a consistent yardstick for mission success planning and evaluation. Irrespective of contract type, acquisition instrument, or management approach, a core set of assurance activities must be implemented over the life of any successful program. PBMA-KMS provides a framework for developing program-specific assurance profiles and assurance process maps.

The model structure consists of eight basic assurance process elements:

- Management
- Concept development
- Acquisition
- Hardware design and verification
- Software design and verification
- Manufacturing
- Pre-operations integration and test,
- Operations

For each of these eight elements the model contains the following five subelements:

- Policies
- Plans
- Processes
- Program Control
- Verification and Test

The model's elements parallel a typical project design and development cycle reflecting and reinforcing the importance of a systems engineering or life cycle assurance approach.

1.5.2 Risk Management Philosophy

The backbone of the PBMA concept is a risk management philosophy and the recurrent use of the risk management discipline across and throughout the program/project life cycle. Thus, risk management serves as a framework and a mental discipline as well as a formal tool within the model. Risk management typically includes: 1) identification and analysis of risk, i.e., likely failure modes, hazards, sources of variation, etc.; 2) planning for control and mitigation of potential failure mechanisms; and 3) documentation, review, and tracking of identified risks. Program management consensus and informed acceptance of residual risks are crucial elements of informed management decision making.

1.6 OSMA Independent Assessment Team (IAT)

The review team was comprised of the following members:

- J. Steven Newman, OSMA (Team Lead)
- Stephen M. Wander, OSMA
- John Castellano, Office of Space Flight

The team appreciates the support of the Boeing X-37 Program Manager, Richard Cervisi and his deputy, Ray Bartlett, and the MSFC X-37 Project Manager, Susan Turner and the many members of their staffs that supported the review. Special thanks and appreciation go to Kip Mikula, Marianne Redgate, and Todd Jensen who provided excellent management and logistics assistance to the team.

1.7 Report Structure and Format

Section 2.0, "X-37 Program Background," of this report serves to establish the basic level of programmatic insight, knowledge, and understanding that the IAT has acquired, through document review, individual interviews, and the onsite meeting, necessary and sufficient to lend appropriate weight and credibility to the team's observations and recommendations (section 5.0) and conclusions (section 6.0).

The intent of section 3.0, "Assurance Process Participants- Roles, Responsibilities, and Interactions," is to accurately define and document the specific safety and mission assurance roles and responsibilities for all of the organizational elements, both government and contractor, participating in the X-37 program. In particular, the Assurance Process Map of section 3.7 attempts to concisely describe the principle relationships and key interactions among these various organizations established expressly for the purpose of accomplishing the required SMA functions of the program.

Finally, section 4.0, "Assurance Process Profiles," defines and describes the baseline of assurance processes currently established for the X-37 program to support overall mission safety and success. The delineation and specification of this assurance process benchmark is the first important step in the "define - verify - certify" approach described in section 1.4. It is principally through the successful completion of this process that the OSMA can effectively support the program/project CoFR/FRR processes and provide informed decisions regarding third-party indemnification requests.

2.0 X-37 Program Background

Consistent with national policy and overall NASA strategic interests, the Office of Aerospace Technology (OAST) is identifying and developing launch vehicle technologies that have the potential for significantly increasing safety and reliability of future space transportation systems while dramatically reducing their costs. In order to validate and bring these key launch vehicle technologies to an acceptable level of developmental maturity, demonstration in a relevant flight environment is required. Thus, the X-37 technology demonstration test bed project has been initiated and represents a vital component of the Agency's advanced space transportation activities. This section describes the goals, requirements, and objectives of the X-37 program.

2.1 X-37 Program Objectives – Success Criteria

The X-37 project is managed by the MSFC and directly supports the Aerospace Technology Enterprise "Access to Space" pillar or strategic goal. The principle focus of this strategic objective includes the achievement of a ten-fold reduction in the cost of placing payloads into low-Earth orbit within the next decade and an additional ten-fold reduction in cost in the decade beyond.

A primary X-37 objective is to provide an economical test bed capability for fully automated and unmanned orbital/reentry/landing technologies and flight operations. Since low cost operation is the key element of an eventual low cost, reusable space transportation system, a primary emphasis of the X-37 flight project is the demonstration of operability technologies and concepts, in addition to functional validation of selected design technologies. The mission success criteria for the X-37 project are to successfully achieve orbit and return safely to Earth and to demonstrate key reusable launch vehicle (RLV) technologies.

2.2 Project Technical Requirements

The top-level project requirements that flow from the stated objectives and mission success criteria are as follows:

- Complete low-speed, atmospheric flight tests of the X-40A vehicle, an X-37 proto-type vehicle developed by the USAF (see figure 2.1)
- Develop and build the X-37 flight vehicle hardware and software and the associated necessary ground segment hardware and software to support the planned flight tests
- Perform flight tests of the X-37 vehicle
    - B-52 captive carry and drop tests
    - Low Earth Orbit (LEO) and reentry flight tests
- Develop both embedded and test bed experimental technologies to be demonstrated on the X-37 flight vehicle
- Acquire technology and flight data that will reduce the risk of development of trailblazer and/or operational reusable launch and space vehicles
- Execute the X-37 project within the cost and schedule commitments specified in the appropriate Program Commitment Agreement (PCA)

- Prior USAF Contract: Successful automated approach and landing flight in October 1998

- Modified for early atmospheric flights to support X-37 design

X-37 Design Risks Reduced Through X-40A Testing

- Advanced Technology Flight Demonstration Vehicle
- Linked to Space Maneuver Vehicle design

Figure 2.1 X-40A and X-37 Vehicles

2.3 Cooperative Agreement Team Members

The X-37 project is being executed under a cooperative agreement (NCC8-190) between MSFC and its industry partner, The Boeing Company. The project team (shown in figure 2.2) consists of a number of supporting organizations from NASA, Department of Defense, and industry.

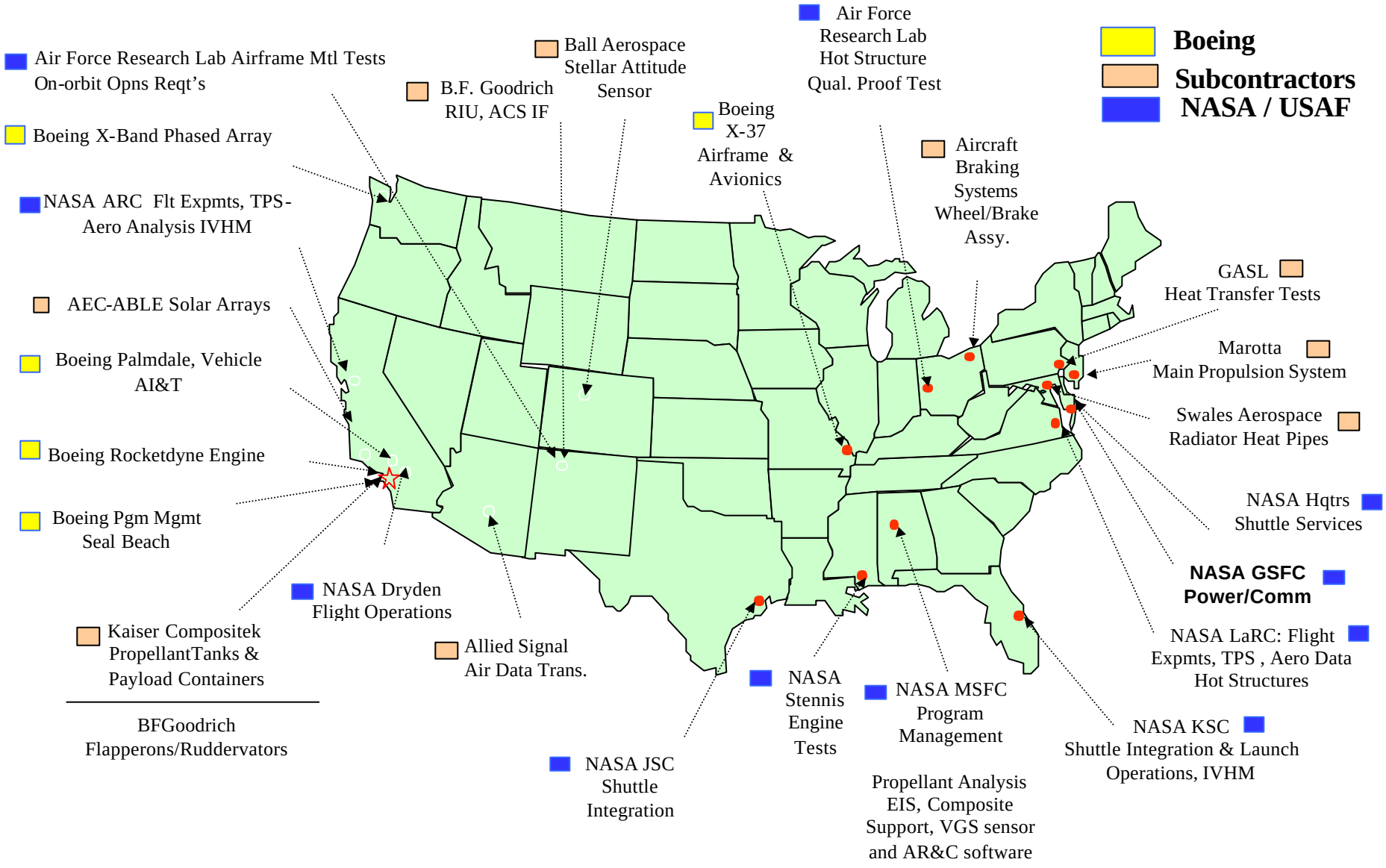


Figure 2.2 X-37 Program Participants

2.4 System Definition Overview

2.4.1 X-37 Vehicle

The X-37 vehicle is a wing-body-tail configuration designed to exhibit robust flying qualities over a wide range of Mach numbers. The vehicle is designed to perform the Design Reference Missions (DRMs) which are shown in table 2.1 below.

Mission Designation	DRM-1	DRM-2	DRM-3	DRM-4	DRM-5	DRM-6
Objective	Functional Checkout Demo Tech & Experiments, Turnaround metrics	Demo Tech & Experiments - Rendezvous & Station Keeping	Taxi Tests (5/day)	Atmospheric	ELV Boost	Aero/TPS/ GN&C Design Traj
Duration	2 days	21 days	30 mins	2 hrs	2 days	60 mins
Launch Vehicle	STS	STS	Truck	B-52	Delta IV	na
Landing Site	EAFB/VAFB	EAFB/VAFB	EAFB/VAFB	EAFB/VAFB	EAFB/VAFB	EAFB/VAFB
Orbit Altitude	160 nm	160 nm	2300 ft	40000 ft to 2300 ft	160 nm	160 nm
Inclination	39 degrees	39 degrees	na	na	TBD	57

Table 2.1 X-37 Design Reference Missions

A typical X-37 flight reentry profile (figure 2.3) is compared to those of other fully or partially reusable systems. As indicated, the altitude and reentry speed of the X-37 is comparable to that of the Space Shuttle.

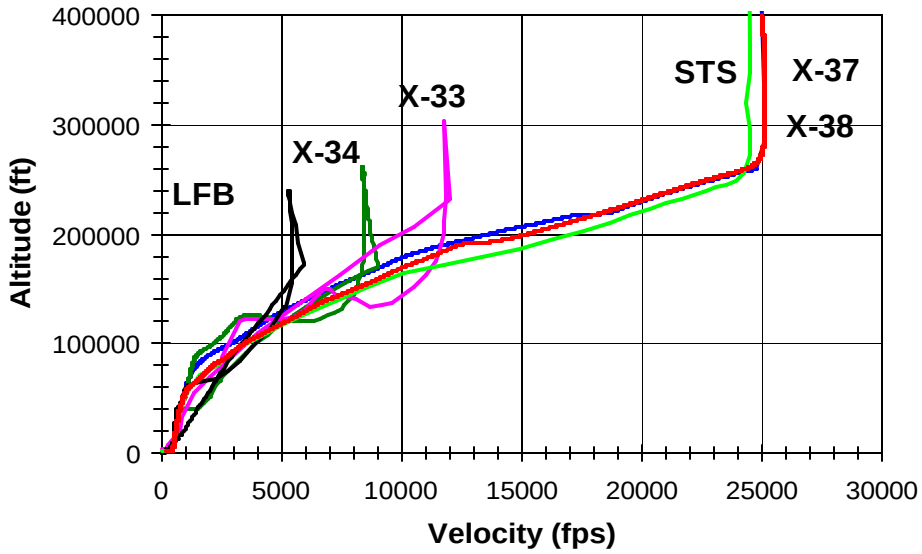


Figure 2.3 Reentry Profile Comparison

A cutaway view of the X-37 vehicle is shown in figure 2.4, acquired from the Dassault CATIA CAD/CAM software used in the X-37 development (discussed later in this report). Weekly "fly-throughs" of the fore, mid, and aft zones provide for detailed coordination among design teams.

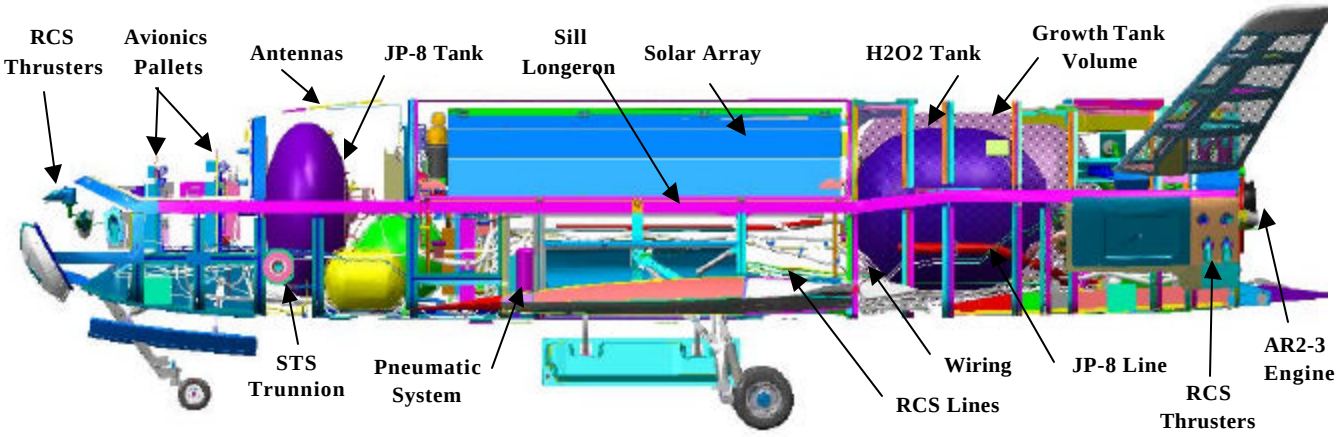


Figure 2.4 X-37 Cutaway View from Digital Mockup Unit (DMU) CAD/CAM

The main propulsion system (AR2-3 engine/JP-8/H2O2) provides maneuvering capability for orbit insertion (DRM-5), on-orbit maneuvers, and de-orbit. On-orbit attitude control is provided by a monopropellant reaction control system (RCS). The X-37 provides a modular payload experiment container for space experiments to demonstrate rapid payload processing. Other features include replaceable test panels, solar arrays, ruddervators and flaperons, landing gear, and adaptable thrust structure. The vehicle is designed to land autonomously. Guidance and navigation functions are performed using a Honeywell Space Integrated Global Positioning System and Inertial Navigation System (SIGI). The current baseline flight test schedule calls for two Space Shuttle-launched flight tests.

2.4.2 Precursor Programs

The USAF Space Maneuver Vehicle (SMV) and earlier programs formed the basis for the X-37 project. The Boeing core team has a heritage to the original REusable FLYback (REFLY) satellite concept. This was followed by the X-40 and X-40A programs and the incorporation of these programs into the current X-37 project. At the time of this report the X-40A has completed taxi tow tests, CH-47 helicopter captive carry tests, and a series of seven free-flight tests at DFRC and Edwards Air Force Base. With the successful completion of these tests, the X-40A flight program provides additional risk reduction for the X-37 vehicle through the following:

- Evaluation of the performance characteristics of the Computed Air Data System (CADS) under dynamic flight test conditions

- Evaluation of the Honeywell Space Integrated GPS/INS (SIGI) under flight conditions
- Site integration and flight test operation of the Flight Operation Control Center (FOCC)
- Flight testing and tuning of the GN&C algorithms
- Improvement of the X-37 aerodynamic database via wind tunnel (X-37) to flight (X-40A) correlations

In addition, the X-40A-derived flight operations support equipment and procedures will be upgraded and infused into the X-37 project by the experienced X-40A flight operations team.

2.4.3 Development and Operational Phase

Flight Test Team

The flight operations approach is patterned after prior successful X-vehicle flight test programs, e.g., X-40A and DC-X, and the established operations for flying on Shuttle and B-52 and at the launch sites, test ranges, and landing sites. The Combined Test Team (CTT), comprised of Boeing, USAF Space and Missile Command, USAF AFFTC, MSFC, and DFRC, will conduct the atmospheric flight test program at DFRC, Edwards AFB, California. The specific flight test responsibilities and relationships assigned to Boeing, USAF, and NASA will be established by the Flight Test Planning Group (FTPG). The FTPG consists of the CTT with the addition of NASA Kennedy Space Center (KSC) and Johnson Space Center (JSC). The FTPG establishes the various flight test plans and requirements, and the CTT executes the plans to those requirements. NASA MSFC chairs the FTPG.

Initial Flight Test Phase

In this phase, the X-37 undergoes a series of towed taxi tests to demonstrate its ability to navigate and control rollout and verify instrumentation and data collection. These tests are followed by a series of captive-carry flights with the B-52 to verify the flight qualities while attached to the B-52 and vehicle data links (i.e., command, control, telemetry, tracking, and flight termination). The final series of tests from the B-52 are up to five free-flight approach and landing tests (ALT) to demonstrate unpowered flight and landing characteristics of the X-37 vehicle. Subsequent to completing the ALT flights, a flight readiness firing (FRF) test of the X-37/AR2-3 engine is planned at facilities adjacent to DFRC. Completion of this event will conclude the project's initial flight test phase at Dryden.

Orbital Deployment/Reentry Phase

Following the FRF, the X-37 is transported to the Boeing Huntington Beach facility to undergo thermal vacuum and vibro-acoustic testing. At the conclusion of these tests, the vehicle is declared ready for orbital flight and transported to the selected launch site at KSC for a Space Shuttle launch. The self-contained payload container with its experiments and launch vehicle interface hardware is delivered to the launch site, separately. The current project plan specifies two Space Shuttle orbital flight tests. The first flight is tentatively scheduled for early CY 2003. (Note: At the time of this report neither flight test has been manifested on the Space Shuttle.)

Subsequent to the delivery of all flight hardware to KSC, the payload container installation and all pre-Shuttle mating operations are performed in the vertical processing facility. The final step is X-37 fueling and final checkout prior to transporting the X-37 to the vehicle assembly building (VAB) for installation into the Space Shuttle orbiter payload bay. The Space Shuttle will monitor safety-critical X-37 systems during the time that the X-37 remains in the payload bay.

Following system status verification from X-37 ground control, the X-37 is deployed from the Space Shuttle cargo bay with the RMS, and the Shuttle then maneuvers to a safe stand-by distance. After a timed interval, the X-37 will automatically initiate activation of the vehicle subsystems required for orbital operations. Prior to initiating X-37 maneuvering, the link to the tracking and data relay satellite system (TDRSS) will be established.

While on orbit, the X-37 may perform technology demonstrations and experiments. For flights where the X-37 carries a payload in its payload bay, experiments will be performed while on orbit. At the end of the on-orbit phase of the mission, the X-37 will perform a de-orbit maneuver to return for autonomous landing at either EAFB or VAFB. (If the X-37 is unable to de-orbit, there is no current provision for the Space Shuttle to retrieve it and return it to Earth.) Turnaround operations and payload experiment container change-out will also be demonstrated between the two Space Shuttle flight tests.

3.0 X-37 Assurance Process Participant - Roles, Responsibilities, and Interactions

This section identifies the major assurance providers participating in the X-37 program along with a high level description of their assurance functions and resource levels. A more detailed description of Boeing and NASA X-37 management assurance processes and functions is provided in Section 4.0.

3.1 NASA MSFC X-37 Project

3.1.1 Organization

The X-37 project represents one of several projects managed by MSFC within the Space Transportation Directorate.

3.1.2 X-37 Project Insight

The overall management of the X-37 project is consistent with a general approach which specifies adequate, but not "burdensome, government insight" and a streamlined program management structure. (This is consistent with the direction issued by the MSFC Director as a result of the Mars Climate Observer checklist developed by the failure investigation team (reference section 3.2)). The intent is that this insight into the execution of the cooperative agreement with the industry partner Boeing will be sufficient to ensure that the project is being conducted within the established cost and schedule constraints and that all significant technical and programmatic risks are adequately identified, tracked, and mitigated. Additionally, the reporting requirements are to be limited to those that are essential to support key decisions and to assure that the agreed to research and technology return is commensurate with the committed cost, schedule, and performance requirements.

Within the context of insight, key X-37 project assurance roles are assigned to the project manager and deputy project manager as well as the risk manager, lead system engineer, and the resident manager.

3.1.3 X-37 Project Office Responsibilities

General duties and specific assurance responsibilities of the X-37 project manager include:

- Executing NASA's roles set forth in the cooperative agreement
- Preparing and maintaining the project plan, specification, schedules, and budgets
- Acquiring and utilizing participating contractors/industry partners
- Executing the Project Plan
- Supporting project management and integration
- Reporting project status and contractor/industry partner performance

- Interfacing with NASA Centers, Headquarters, and other government agencies, and contractor personnel as required to ensure mission objectives are being met
- Complying with applicable Federal law, regulations, Executive Orders, and Agency directives
- Serving as overall risk manager

Lead System Engineer's Role

The lead system engineer is accountable to the project manager to ensure that the project system requirements are met in the following areas:

- Hardware and software requirements and verification development
- Flow down of requirements to subsystem and component level
- Allocation of technical resources and error budgets to lower levels
- Monitoring technical progress through Technical Performance Measurement parameter reporting
- System modeling and analysis for the purpose of validating system requirements
- Performance of system level trade studies leading to the best approach to meet the requirements
- Engineering discipline interface and design review coordination
- Hardware/software integration, testing, and operation

Risk Manager's Role

- Identify new risks
- Integrate risk information from all task managers (includes NASA identified risks and Boeing identified risks)
- Assist project manager in reprioritizing all risks to determine the top project risks
- Assist task managers in risk prioritization to determine top risks in each area
- Assist risk owners in development of research and mitigation plans
- Ensure that the appropriate engineering personnel have focused insight into the high-risk areas
- Ensure risk information sheets and risk database are prepared and updated as necessary
- Prepare and update X-37 project risk status report
- Review risk attributes, status, and trends with project manager each quarter to evaluate effectiveness of the risk management effort
- Forward all identified risks to Boeing's risk manager for review

3.1.4 MSFC X-37 Resident Manager at Boeing-Seal Beach Facility

The MSFC Resident Manager for the X-37 program has a broad set of responsibilities involving management and technical monitoring of the Boeing X-37 project activity. Key assurance functions include:

- Assuring that systems engineering/design requirements are addressed
- Providing independent assessments of contractor performance
- Serving in a technical review role
- Participating in design and management reviews
- Serving as chair or member of various technical evaluation panels, working groups and technical committees

3.2 MSFC Engineering Support

The MSFC Center Director has tasked the MSFC Engineering and Space Transportation Directorates to become more involved in supporting program and project activity. This increased involvement is demonstrated through a recurring support role to the X-37 in managing technical and engineering risks. The objective is a shared partnership for mission success, assuring the right level of government involvement to mitigate program risks. The strategy is to deploy the workforce with emphasis on the highest risk areas, utilizing a risk management approach and applying penetration levels as described below:

Technical Penetration Level 0 - No Penetration

- Accept performing organization's tasks at face value (based on assessment that no penetration is required)
- Contractor develops and implements verification plan

Technical Penetration Level 1 - Low Penetration

- Participate in reviews and technical interchange meetings and assess only the data presented
- Perform periodic audits on predefined processes
- Chair board or serve as board member, or RID writer, at a formal review
- Participate in resolution and closure of issues
- Review verification plan and its implementation

Technical Penetration Level 2 - Intermediate Penetration

- Perform low penetration tasks with addition of daily or weekly involvement to identify and resolve issues
- Review verification plan, its implementation, and selected verification closure data

Technical Penetration Level 3 - In Depth Penetration

- Perform all tasks at the intermediate penetration level
- Perform methodical review of details
- Develop independent models to check and compare vendor data, as required
- Review verification plans and their implementation and concur in all verification closure data

Technical Penetration Level 4 - Total Penetration

- Perform a complete and independent evaluation of each task
- Perform independent review of all verification documentation (including closure data) and witness verification testing

The MSFC Engineering and Space Transportation Directorates have prepared initial assessments of X-37 technical and engineering areas and assigned penetration levels. In at least 25 areas they have assigned a penetration level of 2 (intermediate penetration) or 3 (in depth penetration) as shown in figures 3.1a and 3.1b.

AREA OF PENETRATION	Liquid Engine Systems	Solid Motor Systems	Vehicle Systems Integration	Main Propulsion System	Storable Propulsion	Propellant Management	Solid Motor Performance	Cost/Ops/Reliability Analysis	Liquid Engine Performance	Fluid Systems Design Analysis	Engineering Photographic Ana	Flow Path Analysis	Control Mechanisms/TVC	Control Systems	Rotordynamics/Pogo	Turbomachinery	Combustion Devices	Energy Conv. Des.	Fluid Systems Design	Mechanical Design and Draftin	Dynamic Data Analysis	Acoustics	Unsteady Fluid Dynamics	Experimental Fluid Dynamics	Aerodynamics	Aerothermodynamics
Structural Test Rqmts (Proof Loads)																										
Peroxide Issues (Comp,Clean,Venting)						2													1							
MPS/RCS Propellant Transfer				3						1							1		1							
C/SiC Performance																										
SIGI																										
Retractable Solar Array																										
WLE Surface Temperatures																										1
Li Ion Batteries																										
CADS																									2	
Software V & V																										
Communication System																										
High Temperature Bearings																										
Laser Initiated Pyrotechnic FTS																										
Composite Materials																										
Systems Engineering/Integration Issues			3																							
AL 5254 Tank																										
Component Qualification Rqmts	1								1								1		1							
Structural Verificaton & Testing																										
Environmental Assessment/Effects																										

Level 1 - Low Level Penetration - Participate in reviews and TIMs, assess only the data presented, perform periodic audits
Level 2 - Intermediate Level of Penetration - Level 1 plus daily or weekly involvement to identify and resolve issues
Level 3 - In-depth Level of Penetration - perform independent assess. and run independent models to check and compare vendor data
Level 4 - Total Penetration - perform a complete and independent evaluation of each task

Figure 3.1a X-37 Space Transportation Directorate Engineering Support

AREA OF PENETRATION	ENGINEEERING SERVICE	Electrical Power	Instrumentation and Control	Computers and Data Systems	Flight Software	Avionic Systems	EEE Parts and Packaging	Control Electronics	Radio Frequency	Avionics Simulation	Structural and Dynamic Loads	Strength Analysis	Structural Design	GSE and Mechanisms Design	Thermodynamics and Heat Transfe	Thermal and Fluid Systems	Structural and Dynamics Testing	Environmental Effects	Non-Destructive Eval & Tribology	Metallic Materials and Processes	Non-Metallic Mtls & Processes	Project Engineering	Chemistry	Manufacturing Services	Special Test Equipment Design)	Sys Engr Support	Configuration and Data Mgmt
Structural Test Rqmts (Proof Loads)											1	1	1				2			1							
Peroxide Issues (Comp,Clean,Venting)																		2					2				
MPS/RCS Propellant Transfer																											
C/SiC Performance											2	2					2				1						
SIGI			2						2																		
Retractable Solar Array		2						2						2													
WLE Surface Temperatures															2												
Li Ion Batteries		3																									
CADS			2																								
Software V & V					3																						
Communication System									2																		
High Temperature Bearings															2				1								
Laser Initiated Pyrotechnic FTS													1														
Composite Materials																					2						
Systems Engineering/Integration Issues																				1		1				1	
AL 5254 Tank																			2	2							
Component Qualification Rqmts											2					1						1				1	
Structural Verificaton & Testing											1	1	1	1	1	1	1	1	1	1	1	1				1	1
Environmental Assessment/Effects													1					1									

Level 0 - No Penetration

Level 1 - Low Level Penetration - Participate in reviews and TIMs, assess only the data presented, perform periodic audits

Level 2 - Intermediate Level of Penetration - Level 1 plus daily or weekly involvement to identify and resolve issues

Level 3 - In-depth Level of Penetration - perform independent assess. and run independent models to check and compare vendor data

Level 4 - Total Penetration - perform a complete and independent evaluation of each task

Figure 3.1b X-37 Engineering Directorate Engineering Support

3.3 MSFC Safety and Mission Assurance

The MSFC SMA organization (as of February 2001) has a single individual assigned one-half time to support the X-37 program. This activity involves attending reviews and co-chairing the System Safety Working Group along with the Boeing System Safety manager.

SMA management has indicated the intention to implement the following measures to increase its insight verification and surveillance capability:

- Develop an X-37 Safety and Mission Assurance Plan

- Establish a full-time SMA manager, resident at the Boeing Seal Beach facility. It is anticipated that the current X-37 manager (based in Huntsville) would continue to support the program.

- Engage MSFC SMA support contractor, Hernandez Engineering to support verification and surveillance activity as required.

3.4 Boeing X-37 Program Management

The Boeing X-37 program management team, based in Seal Beach, plays the central role in overall X-37 assurance management. Key assurance participants include the program manager, deputy program manager for systems engineering, system safety manager, quality assurance manager, and as design and verification Integrated Product Team (IPT) members.

Boeing is implementing a rapid-prototyping approach, consistent with the NASA cooperative agreement performance based management approach. Accordingly, the Boeing assurance approach is described as "streamlined" and incorporates the following features:

- No prescriptive flowdown of contractor stipulated quality requirements
- (MIL-STD's, MIL-Q, ISO, etc.).
- Statement of Work requires a Quality Assurance Plan.
- Quality Assurance Plan is supplemental to PRO-570, the Boeing Quality Management System (BQMS).
- BQMS is ISO-9001 and AS-9100 compliant.
- Quality Assurance Plan has a main message, "utilize your site specific BQMS procedures" unless the contents of the plan dictate something that is program unique.
- Intercompany Work Assignment (IWA) sites create additional quality plans for more specificity.
- Cooperative agreement reflects an "insight" role by NASA rather than the traditional "oversight" role.

The X-37 Combined Quality Assurance Team directs quality assurance requirements flow, oversight and guidance, process controls, validation and acceptance, and provides data package management. The team is comprised of the following participants:

- Program Quality Office - Seal Beach
- Procurement Quality Assurance - Huntington Beach (HSF&E Core)
- Software Quality Assurance - Huntington Beach (HSF&E Core)
- Manufacturing Quality Assurance - Multiple IWA Sites: Rocketdyne, Palmdale, Seattle, St. Louis, Assembly, Integration and Test Quality Assurance - Palmdale

3.5 USAF AFFTC and DFRC - Integrated Responsibilities

Under the X-37 Cooperative Agreement the AFFTC and DFRC work in close partnership to implement many of the key assurance functions necessary to protect the public. This section describes their respective roles and responsibilities in implementing safety critical flight test and operational assurance processes. Pertinent text has been abstracted from the X-37 Cooperative Agreement.

3.5.1 Range Safety Management Responsibilities (Drop Test and De-orbit Operations)

Safety Review and Approval

The AFFTC will lead the range safety and flight approval process with Boeing assistance for the Edwards AFB Range and other government agencies as required for reentry. AFFTC is responsible for Edwards AFB Range Safety approval. This task includes B-52 drop tests and reentry portion of orbital flights launched from KSC or CCAFS and returning to the Edwards range for landing.

Hazard Analysis Review and Approval

Review and approval is a shared USAF/NASA responsibility. Boeing is responsible for developing the documentation necessary to meet the requirements of EWR 127-1 and NSTS 22254. Preliminary hazard analyses were prepared by Boeing and reviewed by AFFTC in time to support the X-37 IDR.

Dispersion and Breakup Analysis Review and Approval

The AFFTC is responsible for dispersion analysis approval.

Safety Review Board

The USAF and NASA share Safety Review Board (SRB) responsibilities. AFFTC and DFRC provide members for the independent FRR Committee. AFFTC and DFRC conduct the Safety Review Board. Separate FRR and SRB's will be required for drop flights and reentry flights.

3.5.2 Flight Termination System (FTS)

FTS Certification Oversight and Approval

The AFFTC FTS Office and DFRC FTS Office participate in the IPT responsible for design of the FTS. AFFTC and DFRC provide configuration control for onboard FTS hardware. The joint team is also responsible for:

- Verifying end-to-end operation of the FTS system.

- Qualification test review, approval, and witnessing
- Acceptance test review, approval, and witnessing

3.5.3 Range Safety Operations Responsibilities

Range Safety Officer

AFFTC and DFRC will supply Range Safety Officers (RSO) during all flight-testing for which AFFTC is the lead range. The RSO's will develop range safety Go/NoGo criteria for drop and the flight termination criteria after the vehicle is released during flight. The RSO's will be included as a member of the Go/NoGo polling for drop.

Range Safety Trajectory Analysis

AFFTC and DFRC will host a real-time pilot-in-the-loop simulation (RTPILS) using an existing DFRC simulation skeleton, hardware, and cockpit. The RTPILS will be used to independently generate trajectory data to ensure range/flight safety goals. The analysis will also address control uncertainties and margin.

Flight Systems Failure Modes and Effects Analysis (FMEA)

DFRC is responsible for reviewing FMEA's provided by Boeing to the subsystem level by IDR and as they are updated. Boeing provides FMEA's in accordance with NASA NSTS 22206.

Vehicle Reliability and Capability Analyses

Both AFFTC and DFRC share responsibility for reviewing vehicle reliability and capability analyses as they pertain to range safety.

Performance, Stability, and Control

DFRC is responsible for reviewing Boeing provided aerodynamics models and for providing aerodynamic support for preflight planning.

Guidance, Navigation, and Control

DFRC is responsible for assessing Boeing's guidance, navigation, and control (GN&C) design and analytic results.

System Reliability, Failure Detection/Handling

DFRC is responsible for reviewing the X-37 vehicle design, reliability, and failure detection/handling systems to insure that they meet the requirements for range safety. DFRC is responsible for defining required strain gages, thermocouples, and accelerometers to evaluate structural integrity during reentry.

Verification and Validation

NASA/DFRC is responsible for reviewing Boeing verification and validation test plans, procedures, results, and analysis. DFRC shall review the vehicle systems and GN&C design.

Structural Design

AFFTC and DFRC share responsibility for reviewing flutter analysis and static structural design loads and analysis for support of the FRR and SRB process.

3.5.4 B-52 Safety (Drop Test Activity)

The AFFTC and DFRC share ownership of the lead safety approval process.

Separation and Recontact

AFFTC and DFRC are responsible for providing all test data and recontact analysis required to simulate the release of X-37 from the B-52 and meet review board requirements. AFFTC and DFRC are responsible for providing aerodynamic support for the design and analysis of the support system, as required. AFFTC and DFRC are responsible for supporting all B-52 flight safety reviews.

3.5.5 Ground Safety (Drop Tests)

DFRC serves as the leader of the ground safety approval process.

Review and Approve Ground Procedures

DFRC is responsible for providing all of the safety support required for developing, documenting, and approving all ground procedures with respect to utilization of DFRC assets, equipment, and personnel. DFRC with Boeing support is responsible for developing X-37 procedures for X-40/B-52 mate/demate. DFRC is responsible for providing safety support for Boeing development of other ground procedures used at EAFB.

Review and Approve Ground Tests

DFRC is responsible for providing all of the safety support required for developing, documenting and approving all ground test procedures with respect to utilization of DFRC assets, equipment, and personnel. DFRC, with Boeing support, is responsible for developing X-37 test procedures for the following: Combined Systems Test, Integrated X-37/B-52 GVT, and Hangar Radiation Test. DFRC is responsible for providing safety support for Boeing development of other ground test procedures used at EAFB.

Quality assurance oversight

DFRC is responsible for providing quality assurance to insure that all ground safety procedures are being followed.

3.5.6 Flight Operations (Drop Test and Reentry Operations)

Safety Chase Support

AFFTC and DFRC are responsible for providing chase aircraft with in-flight video for each B-52 flight (five flights total for X-37).

Mission Planning

AFFTC and DFRC are responsible for providing for mission planning including trajectory analysis, instantaneous impact point (IIP) analysis, scheduling, arranging for range assets, etc., using the Boeing provided test objectives and data requirements. This task applies only to on-range and reentry operations.

Test Planning

This task is only for on-range and reentry operations. AFFTC is responsible for detailed flight test planning and publishing flight cards using the Boeing provided detailed test objectives and data requirements for the X-37 from release though landing and rollout. AFFTC is responsible for coordination and publication of the flight rules.

Configuration Management

AFFTC and NASA/DFRC are responsible for providing configuration control/management of the range assets, including the B-52 and pylons. This includes developing and maintaining ICD for the range interface to the FOCC.

Range Control Officer

AFFTC is responsible for providing a Range Control Officer (RCO) for all ground and flight missions using range assets. The RCO shall insure that all range assets necessary to successfully complete the mission are available and operational during the mission. The RCO is the person responsible for coordination with all range asset groups during the missions. This task includes the range safety, FTS, tracking, telemetry (RCC IRIG Standard 106-96), uplinks, and downlinks.

3.6 Other NASA Center and Government Participants

Several NASA Centers (ARC, GSFC, LaRC) and two USAF Laboratories are providing technology and subsystem support to the Boeing X-37 team under task agreements. These support activities are equivalent to a Boeing subcontractor role. Therefore, Boeing engineering and quality assurance processes will govern those activities. MSFC SMA will not exercise formal insight or oversight roles. NASA Center SMA organizations exercise their normal institutional safety surveillance and insight for X-37 activities in work at their respective Centers.

3.6.1 Engine Test Support

Stennis Space Center (SSC) is providing test support for the AR2-3 engine. MSFC SMA will play an assurance role during engine testing.

3.6.2 Johnson Space Center (JSC) Payload Safety Review Process

JSC is responsible for assuring the safety of all Space Shuttle payloads, including the X-37. The JSC Payload Safety Review Process (PSRP) provides the structure and forum to assure that all safety hazards are identified, tracked, and mitigated to the extent required by NSTS 1700.7B, "Safety Policy and Requirements for Payloads Using the Space Transportation System." The X-37 has successfully completed the Phase 0/1 step of the PSRP process.

3.6.3 NASA Software Independent Verification & Validation (IV&V) Facility

The IV&V Facility, located in Fairmont, West Virginia is providing software assurance support to the X-37 program. The X-37 project performed an assessment per the criteria defined in NPG 2820 to determine the need for software IV&V. The results of the assessment indicated the need for IV&V on X-37 software.

<u>IV&V Scope</u>

The NASA IV&V team (including support contractor AVERSTAR) will perform lifecycle IV&V analyses on critical Guidance, Navigation, and Control (GN&C) software functions. The NASA IV&V team will perform a Criticality Analysis and Risk Assessment (CARA) on the GN&C to evaluate and identify the risk exposure for each GN&C function. The results of the CARA will help determine the most effective allocation of IV&V resources and tasks to be performed on each function. CARA's will be performed on a periodic basis to identify risk exposure changes and to reprioritize the IV&V effort. X-37 GN&C lifecycle IV&V shall cover requirements, design, code, and test analysis as outlined in the following paragraphs:

Requirements analysis is applicable throughout all life cycle phases of the project. This analysis will focus on the following requirement attributes:

- Clarity
- Consistency
- Completeness
- Correctness
- Testability

Design analysis is applicable during the design phase of the project. Analysis may include executing X-37 GN&C algorithms in Simulink block diagram form with Boeing's Shuttle Descent Analysis Program (SDAP) X-37 six-degree of freedom simulation. (This item is still under discussion with Boeing.) This analysis will focus on the following design attributes:

- Meets requirements
- Review for unanticipated consequences
- Independent algorithm derivation
- Interface verification

Code analysis shall be performed to verify that the software meets all GN&C requirements and conforms to the documented GN&C design. This analysis will focus on the following coding attributes:

- Traceable to design
- Visual inspection for obvious errors

Test analysis shall verify that test definitions, objectives, plans, and acceptance criteria are sufficient to validate GN&C requirements. The option exists for the NASA IV&V team to perform independent testing at the developer's hardware-in-the-loop facility. This analysis will focus on the following test attributes:

- Review of Program test plans, procedures and reports
- Refine additional testing needed if warranted by review

The NASA IV&V team will support periodic project, GN&C, and flight software reviews.

Products of IV&V Activity

- IV&V CARA Reports
- IV&V Problem Reports – submitted and tracked within the Boeing Problem Report/Change Request system
- IV&V Findings and Recommendations
- IV&V Test Plans, Procedures, and Reports (if necessary)
- IV&V Monthly Progress Reports

3.6.4 KSC (Shuttle Ground Processing and Launch Operations)

KSC has formed the X-37 Orbiter Flight/Ground Operations Team to conduct the planning and implement the processes necessary to support X-37 processing at KSC. The initial focus of the team includes operational safety, physical logistics, propellant loading and venting, integration, monitoring, and contingency planning consistent with abort scenarios. At the recent X-37 Final Design Review (FDR) it was noted that the FDR data package was immature in the area of flight/ground operations but that the lack of maturity was typical for a program at this point.

3.7 X-37 Integrated Safety, Risk Management, and Assurance Perspective

The Assurance Process Map (figure 3.2) presents a consolidated perspective describing specific responsibilities for making the X-37 program safe and successful. This integrated view represents a powerful tool for envisioning how overall program risk management and assurance activities are established and implemented in programs structured with many participants and complex relationships (cooperative agreements, task agreements, subcontractors, multiple locations, etc.).

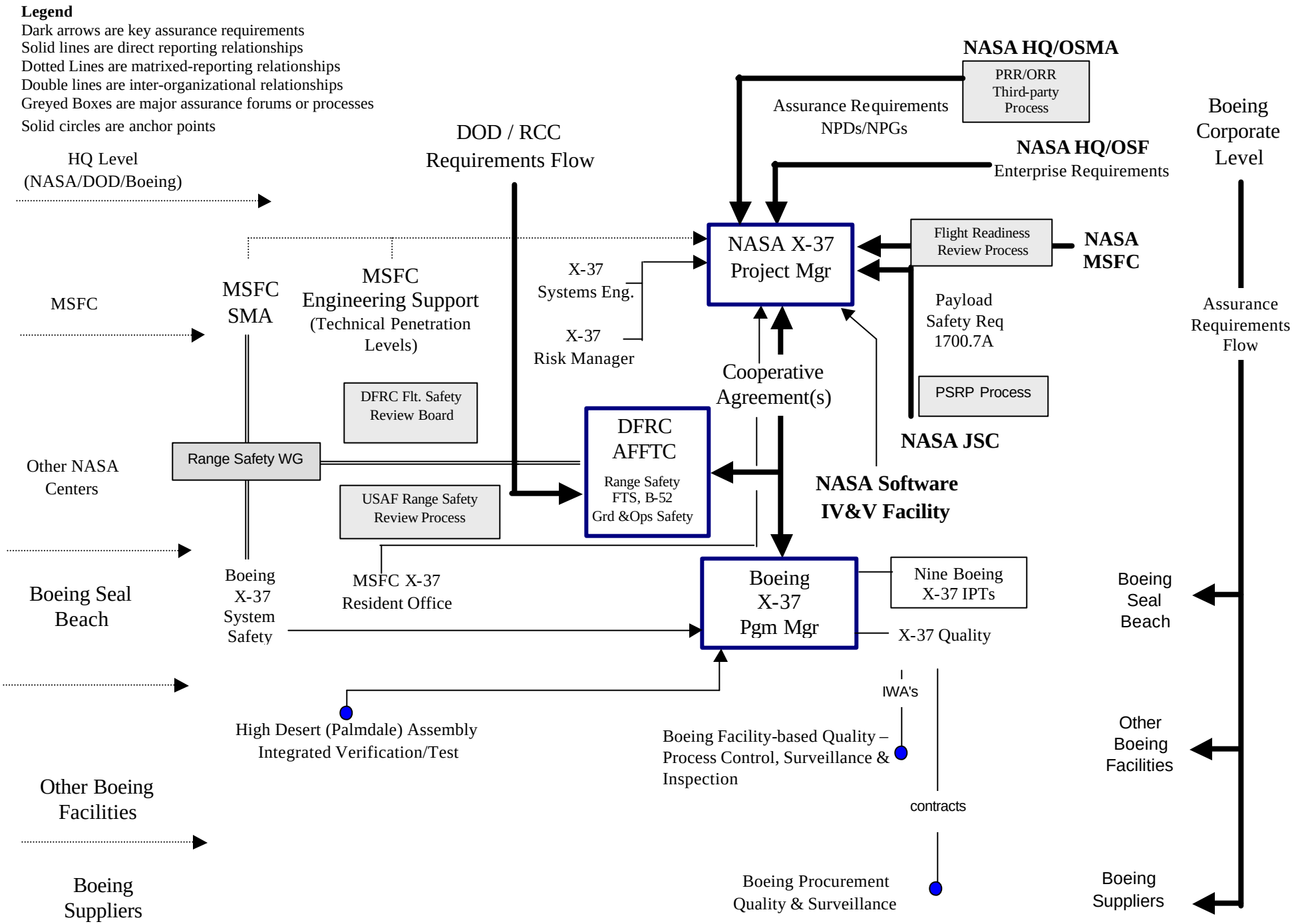


Figure 3.2 X-37 Integrated Safety, Risk Management, and Assurance Process Map

4.0 X-37 Assurance Process Profiles

This section defines and describes the baseline of assurance processes currently established for the X-37 program to support mission safety and success. The delineation and specification of this assurance process benchmark is the first important step in the "define - verify - certify" approach described in section 1.4. It is principally through the successful completion of this process that OSMA can effectively support the program/project CoFR/FRR processes and provide informed decisions regarding third-party indemnification requests.

The assurance process benchmark, described in this section is based on the PBMA model described in section 1.6 of the report. It has been tailored to reflect the unique aspects and organization of the X-37 project. These tailored mission assurance processes are listed below:

4.1 Management Assurance Processes
- 4.1.1 NASA Program Management
- 4.1.2 Boeing Program Management

4.2 Systems Engineering Processes
- 4.2.1 Risk Management
- 4.2.2 Configuration Management
- 4.2.3 Technical Reviews
- 4.2.4 System Safety

4.3 Quality Assurance Processes

4.4 Hardware Design and Verification Assurance Processes

4.5 Software Design and Verification Assurance Processes

4.6 Manufacturing Verification and Test Assurance Processes

4.7 Pre-Flight Integrated Verification and Test Assurance Processes

4.8 Operations Assurance Processes

4.1 Management Assurance Processes

4.1.1 NASA Program Management

The principle program/project management assurance functions specified in NPD 7120.4B, "Program/Project Management," and NPG 7120.5A, "NASA Program and Project Management Processes and Requirements," apply to the management of the X-37 project, the X-37 project plan, and Cooperative Agreement NCC8-190. The major

tailoring relates to establishing Boeing as an industry partner as opposed to the traditional government - contractor relationship. With Boeing as the lead partner, NASA has less direct control over the implementation of the agreement than with a traditional contract. However, strong control can be exercised by withholding payments until the NASA project office is satisfied with the Boeing products and progress.

The MSFC X-37 Project Office is relatively small which is consistent with the cooperative agreement procurement approach. In this approach NASA provides support to the industry partner while maintaining independent insight into the project. As an example of NASA insight, NASA must approve all top-level (Level 1A) changes to the cooperative agreement. Level definitions and corresponding NASA approval criteria are summarized in table 4.2. NASA and Boeing jointly conduct periodic change control boards with NASA as the co-chair of the board. In addition, NASA participates in material review boards (MRB's).

MSFC X-37 Project Office insight into the performance and programmatic issues occurs through several functions and insight mechanisms. These functions and mechanisms, listed in Table 4.1, provide timely decision data to help assure mission success.

Table 4.1 X-37 Project Office Insight System (Part-1)

Function	Insight Mechanism	Management Location	Product
MRB	Post review of all closed MRB actions	Resident Office at Boeing	Review Log/Project Office Notification of Problems
Problem Reporting & IFA's	PRACA	Resident Offices at Boeing & MSFC	Problem Report Log/Board Disposition
Alerts	GIDEP & MSFC	MSFC	QS20 File for Review
FRR - DFRC - X-37 Atmospheric - X-37 Orbital	 - Per DFRC Handbook - Per RAM - Per RAM	 - DFRC - MSFC - MSFC	FRR Package Sign-Off

Table 4.1 (cont.)	X-37 Project Office Insight System (Part-2)		
Function	**Insight System**	**Management Location**	**Product**
Indemnification	Under Investigation	NA	NA
Surveillance	Onsite Presence	Resident Office at Boeing	Weekly Notes/Project Office Notification of Problems
NEQA	As Required	Resident Office at Boeing	By-Product of Working Group Actions
NSRS	Current System	MSFC	NSRS Finding (report)
FMEA-CIL	Reliability Analysis	MSFC	FMEA-CIL Report
Hazards	System Safety Report	Resident Office at Boeing & MSFC	Date Package
Certification/ Verification	System Specification	Resident Office at Boeing & MSFC	Certificate of Conformance
Waivers	MSFC Approves All Waivers Prior to Flight	MSFC	Approval by FRR

X-37 Project Risk Management

A principal mission assurance function is that of overall risk management of the project. The X-37 project manager is assisted in performing the risk management function and duties by a support team drawn from within the Space Transportation and Engineering Directorates and the SMA Office at MSFC. The principal objective and focus of this team is to ensure mission success for all X-37 activities throughout all phases of the project via the following penetration level risk management strategy:

- Utilize a standard risk management approach (identify, analyze, track, mitigate, control) and assign penetration levels based on the level of risk in each critical project area
- Deploy workforce consistent with assigned risk
- Adjust penetration levels as risk areas/severity change over the project life cycle
- Penetrate to a level to assure that the industry partner, Boeing, is doing "the right things the right way"

Refer to Section 3.2 for a description of the penetration levels and specific examples of how MSFC Engineering and Space Transportation Directorate resources are currently assigned to address the most critical or highest risk areas identified for the X-37 project.

The MSFC X-37 team also supports the project manager in the development of the X-37 Risk Management Plan which identifies and focuses on the NASA "unique" risks. This plan provides the methodology and approach for the project manager/risk manager to determine if the particular risk is unique to NASA or should be passed on to Boeing for inclusion in their risk management plan. If a risk is designated as unique to NASA, it is assigned to an appropriate task manager, documented on a risk form, and added to the risk database. These risks and associated mitigation strategies are tracked and updated monthly. A risk is designated as unique to NASA if it can be assigned to or is related to one of the following categories:

- Top-level technical performance/safety issue
- Project schedule
- Funding availability
- Contractor/industry partner performance

The following figures represent examples of the risk information sheet that the X-37 project office uses to track the high-level risks that are unique to NASA.

X-37 Project Risk Information Sheet		
Originator: E. Semmes	**Date: 1-18-01**	**Risk #: S1**

Likelihood: 5 **Consequence: 3** **Timeframe: Current**	**Risk Statement: (condition; consequence)** Airframe Manufacturing Proceeding w/inadequate design maturity.

Context:
The X-37 has proceeded with airframe manufacturing absent of a rigorous requirements review and a traditional critical milestone review. Fundamental requirements documents remain at large and requirements flowdown has not been shown. Additionally, drawings and datasets are incomplete with ongoing impacts (e.g., load changes, fastener details) resulting in revisions and cancellations.

Approach: Research / Accept / Watch / Mitigate
A combination of approaches is being used including our acceptance of the programmatic consequences (cost, schedule) of proceeding with manufacturing without a mature design which has been thoroughly reviewed and subjected to traditional critical milestone reviews. We are monitoring the effects to manufacturing through weekly Airframe/Structures IPT telecons and will mitigate future manufacturing plans by conducting a CDR.

Contingency Plan and Trigger:
Contingency plans are based on severity of consequences and include repair, augmentation, redesign, and/or remanufacture.

Status: **Status Date:** **Lower Fuselage Repair – Including spring-in, core crush, ramp repair, and hole repair: Lower Fuselage repair is in its final stages w/core crush cure expected to begin on 2/13/01. Spring-in and ramp repair reportedly have produced good results. Upon completion of core crush autoclave curing, the fuselage will undergo NDT. We expect laser tracking and/or other methods to provide better insight into manufacturing tolerance results in early March.**		
Lessons Learned: **Ensure formulation rigor and implementation discipline through conduct of adequate reviews and gates at critical milestones.**		
Approval	**Closing Date**	**Closing Rationale**

X-37 Project Risk Information Sheet			
Originator: Stewart		**Date: 11/29/00**	**Risk #: Ops-4**
Likelihood: 1 **Consequence: 5** **Timeframe:** **Mid**	**Risk Statement: (condition; consequence)** **Shuttle flight for X-37 is not approved; possible delay in working Shuttle integration activities such as timeline development**		
Context: **Current plan is to have 2 Shuttle flights with the X-37 vehicle. Currently we are not on an approved manifested flight. Depending on the timeframe of this flight, integration activities might be impacted**			
Approach: Research / Accept / Watch / Mitigate **Watch**			
Contingency Plan and Trigger: **ELV launch**			
Status: **Status Date: 11/29/00** **- Preliminary manifested on STS-120 in May of 2003**			
Lessons Learned:			
Approval	**Closing Date**	**Closing Rationale**	

Certification of Flight Readiness (CoFR) and Flight Readiness Review (FRR)

An additional responsibility and function of the NASA X-37 project office/project manager is to develop a comprehensive CoFR/FRR process which addresses the specific and unique needs of the project. This process is currently under development and is being tailored from a generic CoFR/FRR process.

4.1.2 Boeing Program Management

Integrated Management Structure

The integrated management structure for the X-37 project represents a tailored version of the overall integrated product/process development (IPPD) management approach Boeing has deployed on all programs in recent years.

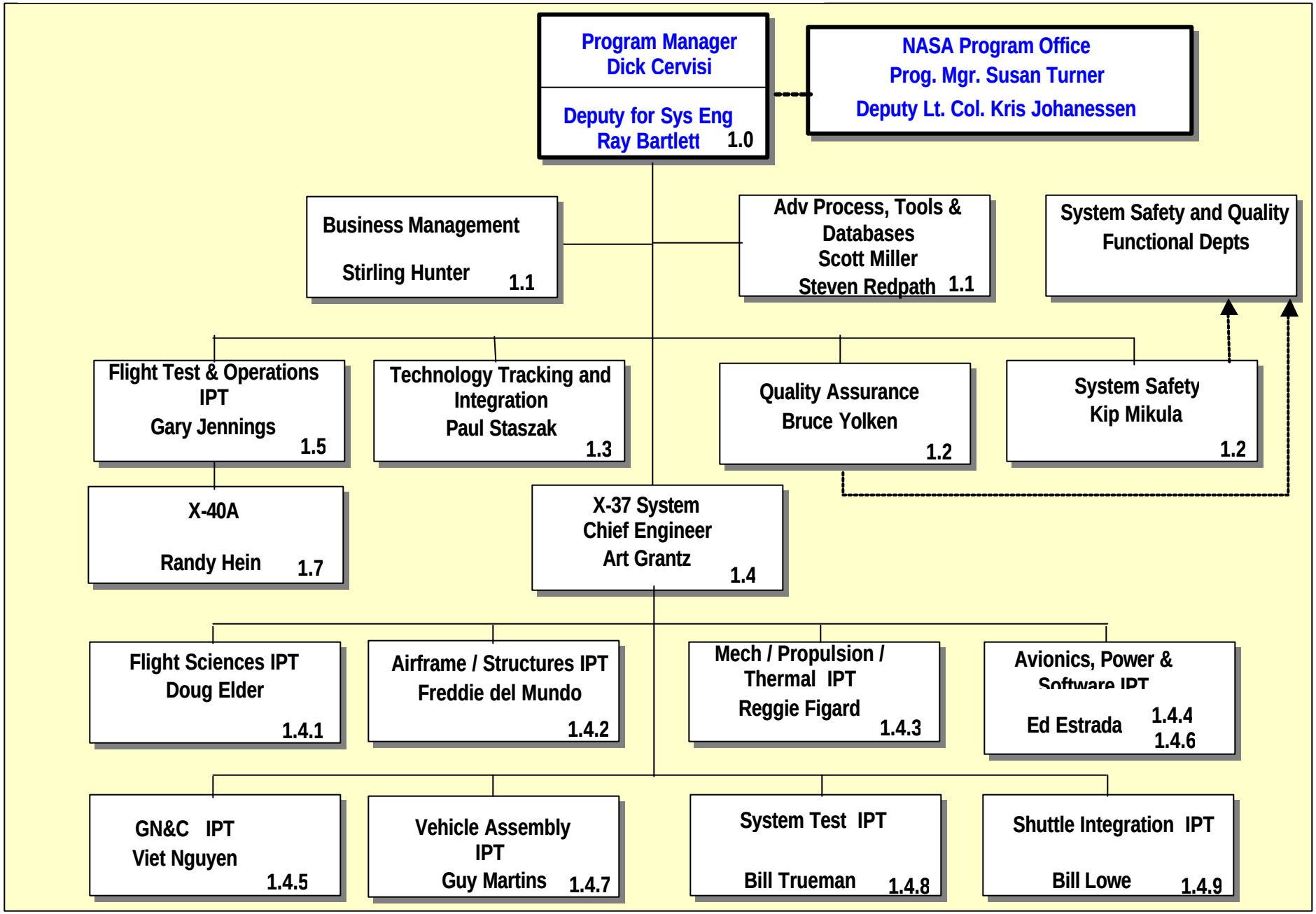
The principal features or attributes of the IPPD management approach include: 1) aligning the organizational structure with the work breakdown structure (WBS) to increase product-focused accountability and clearly define responsibility; 2) blending functions into a seamless organization to eliminate barriers and enhance producibility and supportability during the design process; 3) defining product ownership in a multidiscipline team to foster communication and coordination and facilitate exchange of ideas; 4) integrating lead and support contractors into full participation in the integrated product teams (IPT's); and, 5) assuring full customer participation and insight to improve quality of the final product.

Thus, the X-37 program team is product-focused and consists of a number of multidiscipline IPT's. These IPT's are centered on identifiable products with complete responsibility, accountability, authority, and the requisite resources (budgets, skills, knowledge, tools, and integrated information systems). Full partnership with the customer and suppliers is achieved, as they are working members of the IPT's.

Organization and Responsibilities

As mentioned above, the Boeing X-37 program organization (figure 4.1) is keyed to the program work breakdown structure (WBS). The program manager has selected support staff and integrated product team leaders empowered with the appropriate responsibility, accountability, and authority for execution of their assigned WBS elements. Government and major subcontractors are integrated into the IPT, as appropriate, to their functional involvement in the program.

Figure 4.1 Boeing X-37 Project Organization



X-37 Program Operation Guidelines Document

The overall management process for the X-37 program is defined by the program operations guideline (POG) document. The POG provides direction for the implementation and establishment of processes and procedures to permit the expeditious design, development, production, checkout, and test of the X-37 system. These guidelines also provide documentation that will satisfy both Boeing and NASA management that the design intent has been accomplished and verified.

Program Management for Rapid Prototyping

As noted above, the program management philosophy implemented in response to the POG is centered on the IPPD approach which facilitates timely decisions, promotes effective communication, and provides direct customer insight throughout all program phases. To accomplish their responsibilities and duties, the X-37 program manager and his or her staff will, as a minimum, employ the following best practices to ensure contract compliance, customer satisfaction, timely decision-making, and sound technical, financial, and schedule performance:

- Detail program planning/program execution and integrated schedules
- Earned-value/payment milestone system
- Closed-loop corrective action
- Management information system visibility
- Risk management
- Configuration management
- Technical performance measurement (TPM)
- Customer communication plan
- Supplier management system
- Use of independent review
- Help-needed system executive management support

A number of the above areas will be described in detail in later sections of this report.

Each of the above best practices will be oriented specifically to the rapid prototyping needs of the X-37 program, the customer, and Boeing management in order to enhance successful program execution. Additionally, the X-37 program will take maximum advantage of breakthrough processes used on other Boeing programs. To ensure the success of these improvements in cost, schedule, and quality, Boeing embraces the following program philosophies:

- One hundred percent electronic solid model design
- Use of digital pre-assembly, assembly simulations, and electronic work instructions
- Full configuration management of all electronic design/build data
- Digital model as sole authority
- IPT's will release electronic build-to packages that have part number controlled relationships

- Program provides a controlled single source of product data
- Computing tools follow open-standard architecture principles

Boeing program management will evaluate exceptions to the best practices indicated above on a case-by-case basis.

4.2 Systems Engineering Processes

Boeing, as the lead partner, has the overall responsibility for X-37 project systems engineering and integration. To this end, the following sections describe major system engineering and integration assurance functions.

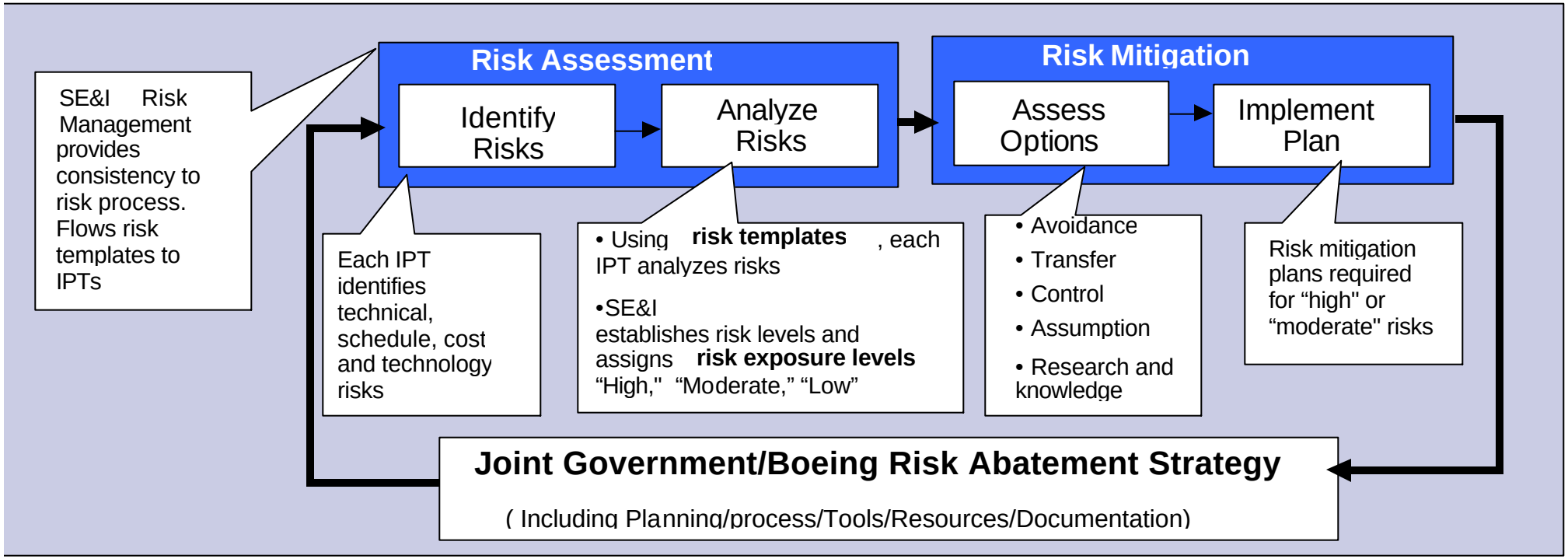
4.2.1 Risk Management

The X-37 risk mitigation management process derives from the Boeing best practices developed from past programs and employed in current programs. The process has been tailored to meet the requirements of the X-37 program while operating in the rapid prototyping mode.

The risk mitigation plans developed by each IPT and reviewed weekly by the program manager are key to the risk mitigation process.

Responsibility for implementation of the risk mitigation plans resides with the IPT's. Figure 4.2 depicts the elements of the program risk process. Each IPT and its team members have responsibility for identifying risks within their own IPT. Once a risk has been identified, a risk analysis is performed to assess: 1) the likelihood that the risk will occur, and 2) the severity of consequences to the program should the risk occur. The risk analysis is conducted by a team which includes the risk manager, the IPT leads, and other personnel as required.

Figure 4.2 Elements of the Program Risk Process



For each defined program risk, the assessed likelihood and severity values are plotted on a risk map to determine the overall program risk level. A color code is used to denote the risk level, (e.g., low-green, moderate-yellow, high-red). Figure 4.3 is an example of a program risk map.

The main goal of the risk mitigation process is to move all defined risks to the lowest (green) level. There are five basic risk mitigation options: 1) avoidance, 2) transfer, 3) control, 4) assumption, and 5) research and knowledge. The IPT assigned to a risk is responsible for preparing a mitigation plan. The plan must define the options for mitigation, the selected approach, and recovery options in the event the basic plan falls short of predictions. The Systems Engineering and Integration (SE&I) IPT updates the risk list and reviews the status of IPT risk mitigation planning on a weekly basis. Authority to adopt all resolution plans lies with program management.

4.2.2 Configuration Management (CM)

The Boeing CM approach is designed to provide support to all areas of the X-37 project. The X-37 CM lead, as a member of the SE&I IPT, is responsible for planning, establishing, and implementing the CM systems, procedures, and controls across all elements and levels of the program. These include:

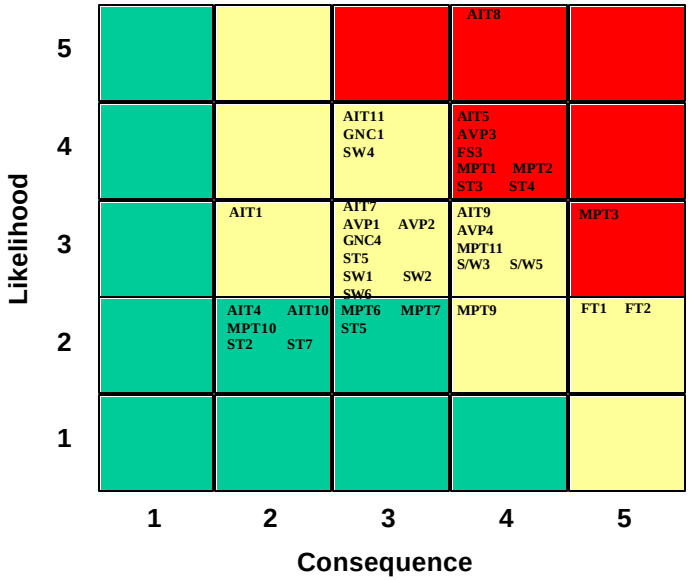
- Program Management
- Integrated Product Teams
- Subcontractors
- Airframe Manufacturing (St. Louis, Mo.)
- Assembly, Integration, and Test (AIT) (Palmdale, Ca.)

The principal CM operating documents employed by Boeing for the X-37 project are:

- Program Operating Guide (POG)
- CM Plan - PP877-0002A
- EIA-649 - National Consensus for Configuration Management
- MIL-STD-973
- ISO 9000 Series
- Boeing internal procedures
  - Specification requirements
- Deviation/waivers

-
-

Likelihood
5 Near Certainty
4 High Likelihood
3 Possible
2 Low Likelihood
1 Not Likely



Conseq	Technical	Schedule	Cost	Program
5	No alternatives	No alternatives	No alternatives	Cancellation
4	A few very difficult alternatives	Major program milestone delays	>40% Cost Growth	Unable to satisfy many program objectives
3	Alternatives very complex	Significant schedule delays	>20% Cost Growth	Requires program restructure
2	Alternatives more difficult	Some schedule slippage	<20% Cost Growth	May require program restructure
1	Alternatives equal to baseline	Alternatives within schedule	Alternatives within cost	No impact to program objectives

Figure 4.3 Program Risk Map

The overall CM change control process as applied to the X-37 project incorporates four levels of control and the associated NASA approval criteria (see table 4.2).

Level Definition	NASA Approval Criteria	
• Level 1A Definition - changes that affect the contract/agreements including any additions, deletions, or modifications to task agreements with government centers.	NASA agreement and signature required. (Boeing may proceed at their own risk pending NASA approval or disapproval)	Special Boards
• Level 1 Definition - changes that significantly impact total program cost, schedule, or objectives. • cost ³ $500 K • schedule ³ any schedule increase to critical program milestones • objectives ³ any change from SRR	NASA signature required; agree or disagree recorded. Boeing may proceed without NASA approval within the contract/agreement.	
• Level 2 Definition - changes that fall below the criteria for Level 1, but impact total vehicle performance, interfaces, or multiple IPTs.	Participation welcome, but approval not required.	Technical Interchange Meetings
• Level 3 Definition - changes that affect subsystem performance only, and do not affect vehicle performance or IPT interfaces	None	IPT Meetings

Table 4.2 Approval Criteria

A principle distinction between Level 1A and Level 1 is that Level 1A encompasses changes in scope of work whereas Level 1 represents within scope changes.

Accomplishing the traditional configuration management functions of authorizing, archiving, and distributing within the dynamic trade study environment of the one-of-a-kind X-37 project presents a significant challenge. This requires the application of CM in the traditional area of document control and the development and implementation of CM techniques for the control of electronic engineering databases.

As regards the change control of documents, the CM lead has the responsibility for formal release of hardware and software including:

- Specifications
- Statements of Work
- Test Plans, Procedures, Reports
- Program Milestone Documents

Specific assignments include the issuing of document numbers, master change record (MCR) numbers, reviewing all documents, maintaining hard copy files, and maintaining document and MCR status logs on the Enterprise Visibility System (EVS). The CM lead

also has responsibility for maintaining the status of deviations, waivers, and engineering change proposals (ECP's).

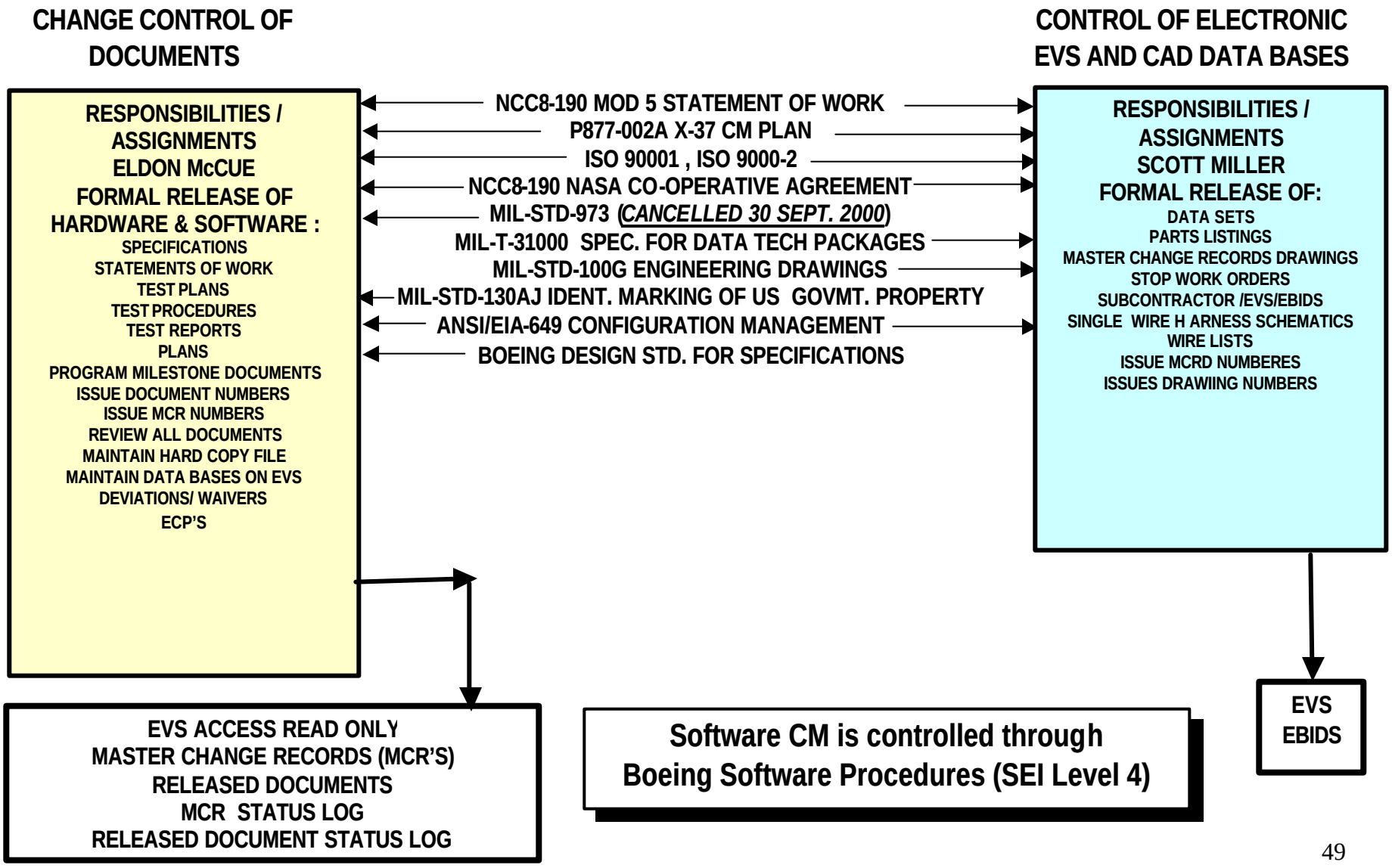
The CM lead is supported and assisted by an individual who has the responsibility for control of the electronic EVS and computer aided design (CAD) databases. These responsibilities include the formal release of:

- Data Sets
- Parts Listings
- Master Change Records Drawings (MCRD) drawing numbers
- Stop Work Orders
- Subcontractor/EVS
- Single Wire Harness Schematics and Wire Lists

Overall CM and change control process responsibilities are depicted in figure 4.4.

Figure 4.4 Configuration Management Responsibilities

Configuration Management Responsibilities



Change control management at the top levels (i.e. Levels 1A and 1) address the definition of top-level system requirements and the flow down of those requirements into lower level subsystem and parts level specifications.

4.2.3 System Safety Process

The top-level system safety process for the X-37 project is based upon a traditional approach of identification, assessment, and mitigation of all potential system safety hazards and risks. In particular, the mitigation approach follows a standard hazard reduction hierarchy where precedence is given to "designing out" hazards followed by providing safety devices, warning devices, or special procedures (see figure 4.5).

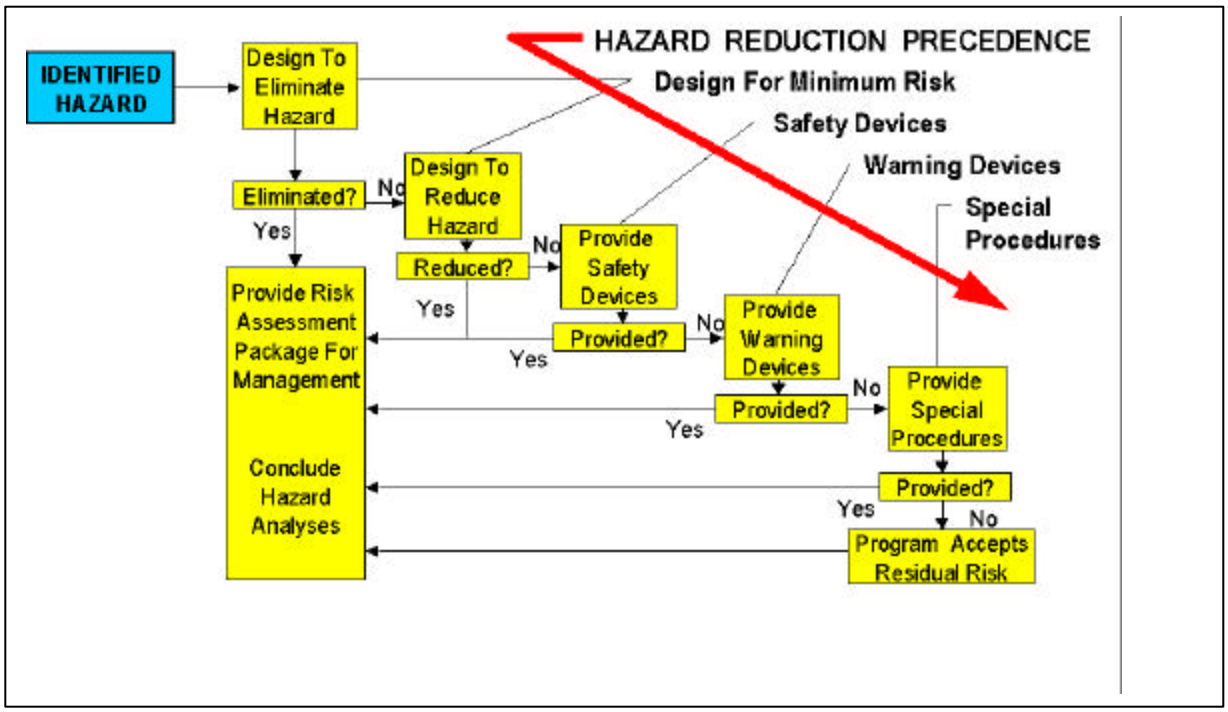


Figure 4.5 Hazard Reduction Procedure

The totality of the system safety process is documented to ensure appropriate participation and communication across all levels of the project. This is accomplished through a number of critical communications interfaces:

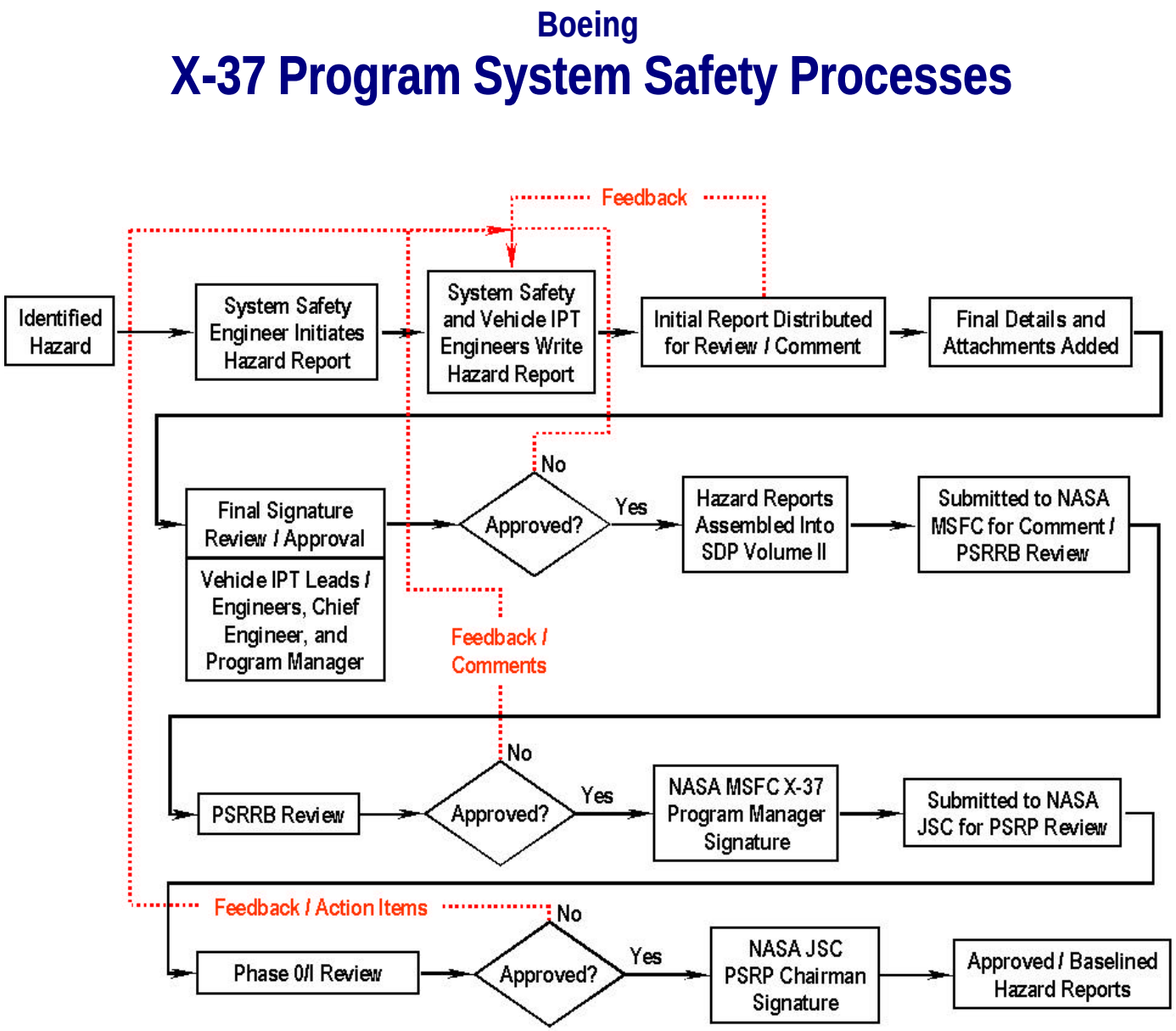
- Safety Watch List (Boeing internal)
- Direct personal interface/interaction with Boeing Seal Beach X-37 vehicle IPT design engineers
- Direct personal interface/interaction with MSFC SMA lead
- Interface/interaction through technical interchange meetings (TIM) with NASA
- KSC/JSC/DFRC/LaRC, USAF AFFTC/30th Space Wing/45th Space Wing, Boeing Huntsville System Safety

- PSRP Reviews
- GSRP Reviews
- SSWG Meetings

Hazard Report Process and Scope

As a potential Shuttle payload, the X-37 is subject to the Shuttle Payload Safety Review Panel (PSRP) process (see figure 4.6).

Figure 4.6 System Safety Process



Shuttle Payload Safety Hazard Report Documentation and Approval Process

Consequently, the project is also developing and implementing an internal hazard report documentation, review, and approval process patterned on the known and proven Shuttle process. This process is described in figure 4.7.

The intended scope of the hazard reporting process addresses all potential phases of X-37 vehicle operation from manufacturing through post-flight recovery as depicted in figure 4.8.

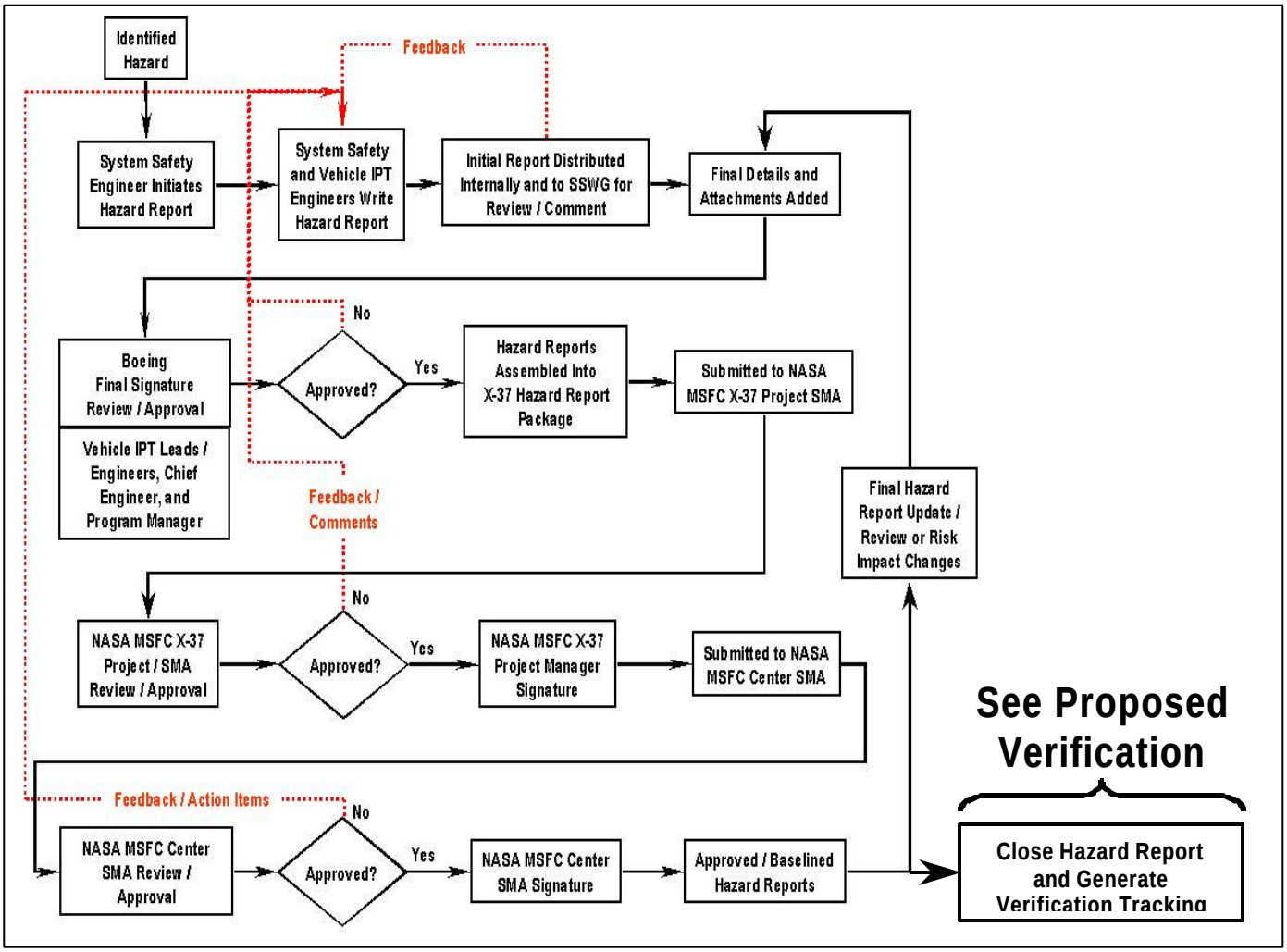


Figure 4.7 Hazard Reporting and Approval Process

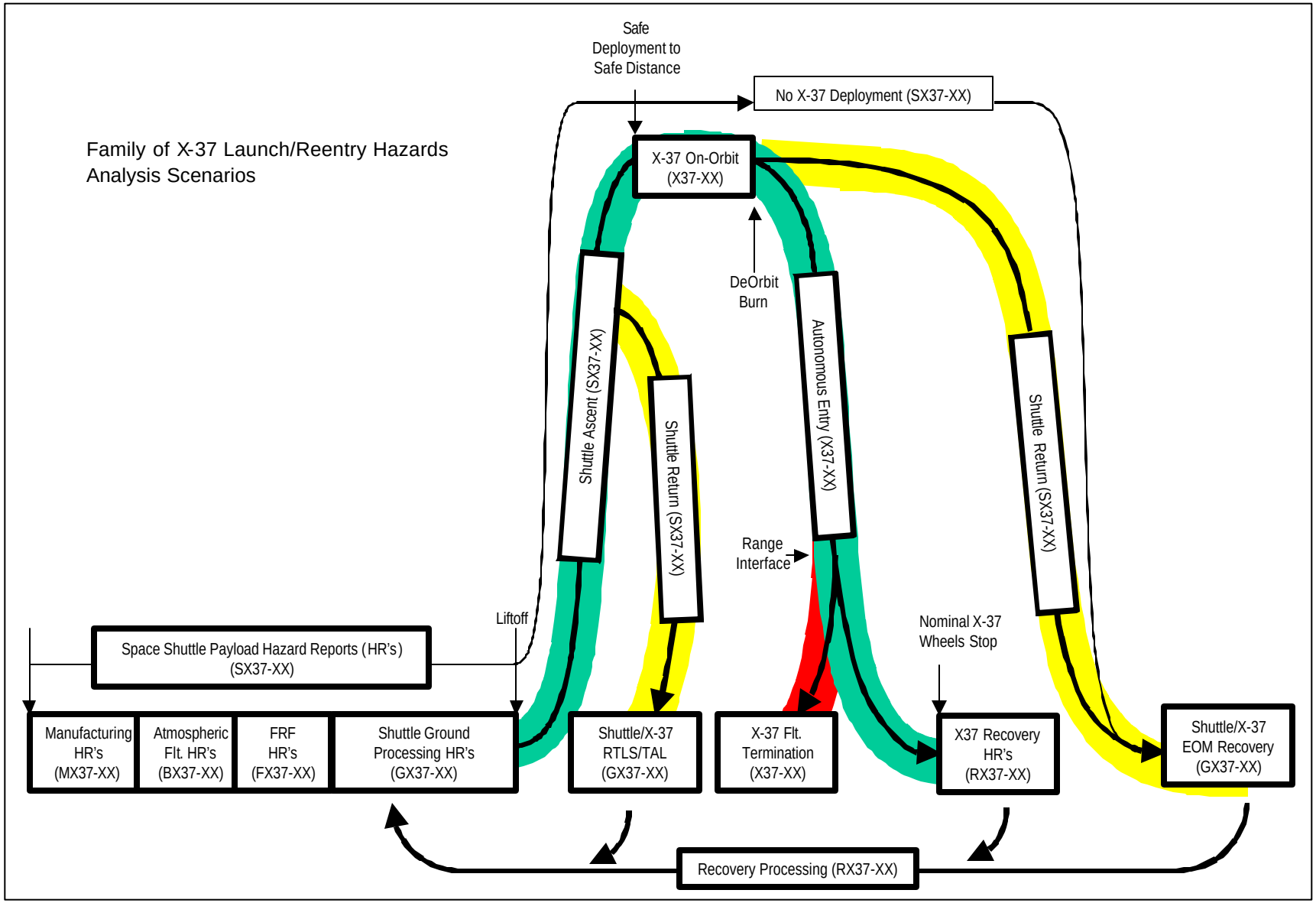


Figure 4.8 Program Hazard Report Scope

Concerning preflight/operations verification, Boeing has proposed a Verification Tracking Database (VTD) process that parallels the process used for payload and ground safety as defined in NSTS/ISS 13830. In this process the signed and baselined X-37 hazard reports are archived in the EVS database. All open items are logged into the VTD process where the test team and system safety team track the closure of these open items based on the appropriate milestone event. These critical milestones are currently defined as:

- X-37 Rollout
- Atmospheric Flight Tests
  - X-37 CoFR
  - Dryden Independent Review Team/Airworthiness Flight Safety Review Board (AFSRB)
  - Taxi Tests
  - Captive Flight
  - Free Flight
- X-37 Flight Readiness Firing (FRF)
- Shuttle Flight Tests
  - KSC Delivery
  - X-37 FRR
  - X-37 ORR
  - Shuttle FRR

VTD closing actions will be verified complete when signed by program management at both Boeing and NASA/MSFC.

Tools

The principal hazard reporting and database tool is the Hazard Entry and Maintenance Program (HEMP) which is a locally developed, Microsoft Access based program. It is proven, accepted, and baselined for usage on the Shuttle program (particularly orbiter and integration hazard reports) and has been modified for application on the X-37 project. Other tools include the Computer Aided Fault Tree Analysis (CAFTA) which is a SAIC developed, commercial off-the-shelf (COTS) product and the Boeing developed Fault Tree Analysis and Builder (FTAB). Standard COTS Microsoft Office 2000 software is also used.

Internal/External Reviews

Internal and external reviews provide control and verification of the system safety processes and the identification and tracking of hazards. The internal Boeing reviews involve the system safety team, vehicle IPT leads and design engineers, and program management. External reviews include:

- MSFC Payload Safety Readiness Review Board (PSRRB)
- JSC Payload Safety Review Panel (PSRP) Phase 0/l, II, III

- KSC Ground Safety Review Panel (GSRP) Phase II, III
- DFRC Flight Test Independent Review Team
- USAF/Range Flight Test AFSRB

An additional independent assessment is provided by the X-37 Program System Safety Working Group (SSWG). This working group has the initial responsibility of reviewing and providing comments to the preliminary hazard report prepared by the system safety lead and the vehicle IPT engineers as indicated in figure 4.9. The SSWG is co-chaired by NASA and Boeing and includes membership from:

- MSFC SMA and Project Office
- JSC SMA
- KSC SMA
- DFRC SMA
- AFFTC Range and Flight Safety
- Vandenberg Air Force Base (VAFB) Range and Flight Safety
- Boeing/Seal Beach System Safety
- Boeing/Huntsville System Safety
- NASA Headquarters SMA

Planned Products

Principal products in work include fault tree analyses addressing the following specific top-level events:

- Inability to deploy the X-37 from the Shuttle payload bay
- Inability of the X-37 vehicle to deorbit
- Inadvertent venting of hydrogen peroxide (oxidizer for the AR2-3 engine) from the X-37 vehicle while captive in the Shuttle payload bay
- X-37 vehicle flies or lands outside planned trajectory or landing site
- X-37 vehicle re-contact with the B-52 aircraft following release

4.2.4 Major Technical Reviews

Technical engineering reviews are scheduled during the life of the X-37 project. The type and frequency of reviews is established according to the unique needs and requirements of the program.

Systems Requirements Review (SRR)

The program had completed the SRR in the mid-1999 time frame. System functional and programmatic requirements were identified which provided the basis for release of the X-37 system specification.

Shuttle Payload Safety Review Panel (PSRP)

Shuttle payload safety reviews are held by the JSC payload safety organization. The purpose of these phased reviews is to assure that the X-37 vehicle satisfies the safety requirements of the Shuttle Safety (NSTS 1700.7B). The phase 0/1 review was completed in (12/00). The remaining reviews to be conducted are the phase 2 (verification) and phase 3 (certification).

Initial Design Review (IDR)

Boeing has completed an IDR in early 2000. The review was conducted for the vehicle and associated ground equipment initial design. The following plans were reviewed: program plan, configuration management plan, risk management plan, program safety plan, quality plan, technology tracking plan, and the flight test plan. An additional IDR (#2) is scheduled for early 2001.

Final Design Review (FDR)

Boeing will conduct a review of the X-37 vehicle and ground equipment final design and updates to the plans baselined at the IDR.

Design Certification Review (DCR)

A DCR will be conducted by MSFC upon execution of the verification plan and IV&V efforts, prior to flight test. The review and participants will provide certification documentation and supporting data that the design satisfies the requirements and that the system performance is satisfactory to achieve mission success. The DCR will be conducted after the FDR, but prior to the FRR. The review will include participation of cognizant management personnel from NASA, US AF, and Boeing, as appropriate.

Flight Readiness Review (FRR)/Certification of Flight Readiness (CoFR)

Prior to each flight test a FRR will be conducted to gain the commitment from all responsible parties, through a CoFR, that the system is ready for the flight test. Additional reviews will be conducted in support of flight readiness:

- Airworthiness Flight Safety Review Board
- Risk Assessment Review for Atmospheric Flights
- Orbital Flight Readiness Review

Other technical reviews may be scheduled as required and as agreed to by the parties.

4.2.5 Reliability

As the X-37 project is currently defined, Boeing has established a reliability program and approach that incorporates most of the elements typically found in a major flight hardware development program. This begins with a numerical reliability requirement as specified by NASA and which has been translated into design specifications which will in turn meet the probability of mission success (POMS) and fault tolerance requirements. This overall approach ensures the earliest participation in design reviews and critical trade studies and requires reliability analysis and modeling which accepts and can incorporate both estimates and test data.

Specifically, reliability data will be used to determine:

- POMS
- Probability of meeting expected casualty rate (Ec) and property loss due to over-flight and landing accidents
- If, and when, alternative landing sites need to be considered
- Scope of prelaunch checkout activities required to maximize the POMS
- Degree of fault tolerance compliance

The reliability process encompasses knowing what could fail, how it could fail, what the consequences are, how often failures will occur, and when failures are likely to occur. This process will also account for the likely condition of each line replacement unit (LRU) for each hour of the mission including reentry and landing. The principal tools to accomplish these "what's" are the development of key failure modes effects and critically analyses (FMECA) and the application of the MAtrix reliability and the SIMtrix simulation models.

Currently, a first draft FMECA is available for the following areas:

- Power distribution and control
- Flight termination system
- Flight management system
- GPS system
- Attitude control
- Ku band
- Radar altimeter
- Airframe structure
- Thermal control
- Brakes
- Pressurization
- Fuel system
- Main engine
- RCS
- Actuators
- Landing gear
- Power generation
- S-band
- Avionics

The Excel-based matrix model generates "standard" USAF reliability/maintainability/availability parameters (i.e., MTBM, MTBR, MTBF, etc.) and loss of vehicle (LOV) and loss of mission (LOM) calculations. It encompasses major operating environments (launch, on-orbit, and reentry) and aircraft type. Each component and LRU is modeled, each having a unique duty cycle and, where applicable,

quiescent time. Redundancy, fault tolerance, and mission criticality is applied where appropriate from embedded reliability block diagrams. The model is also designed for easy replacement of preliminary reliability and maintainability estimates with vendor-supplied data when available. The model provides POMS and vehicle loss rates over an entire mission, or by mission segment, e.g., during approach and landing.

The SIMtrix model, which provides a Monte Carlo simulation of the X-37's major subsystems and components, has been completed and is currently operational. The model steps through the X-37 mission in 1 hour time increments. At each time increment the failed or non-failed status of each component is determined based upon previously supplied component failure rates. The Monte Carlo nature of the simulation requires that each mission be repeated often enough so that valid output statistics can be obtained. Typically, each mission is "flown" a minimum of 25,000 times. Output tables depict for each component if and when failure occurred (in terms of how many of the 25,000 simulated missions had failures and at what time of the mission each failure occurred). The potential consequence of each failure is used, if necessary, to redirect the course of the mission.

4.3 Quality Assurance (QA) Processes

The mission of Boeing's Program Quality Office at Seal Beach is to ensure high quality standards are met while keeping within the X-37 project's rapid prototype structure. This is to be accomplished through the uniform application of QA requirements consistent with established Boeing Company policies, procedures, and standards. The overall objective is to ensure effective quality processes are in place and implemented, resulting in:

- Conforming parts and assemblies
- Conforming assembly, integration, and test
- Authorized disposition for nonconformance resolution
- Acceptance records and traceability data required for vehicle certification

The overall approach for implementing quality assurance on the X-37 project centers on the cooperative agreement philosophy that reflects an "insight" role by NASA rather than the traditional or conventional "oversight" role. Thus, there is no prescriptive flow down of NASA stipulated quality requirements. However, the cooperative agreement statement of work does require the development and implementation of a quality assurance plan. The development of the X-37 quality assurance plan conforms to the ISO compliant Boeing Quality Management System (BQMS) and stipulates that the various interdivisional work authority (IWA) sites are to use their site-specific BQMS procedures unless the content of the top-level plan dictates unique project specific procedures and processes. To this end, the IWA sites will create additional quality plans if additional site specificity is required.

Figure 4.9 depicts the quality requirements flow down from the cooperative agreement to the BQMS, the program quality office, the IWA sites, and external suppliers

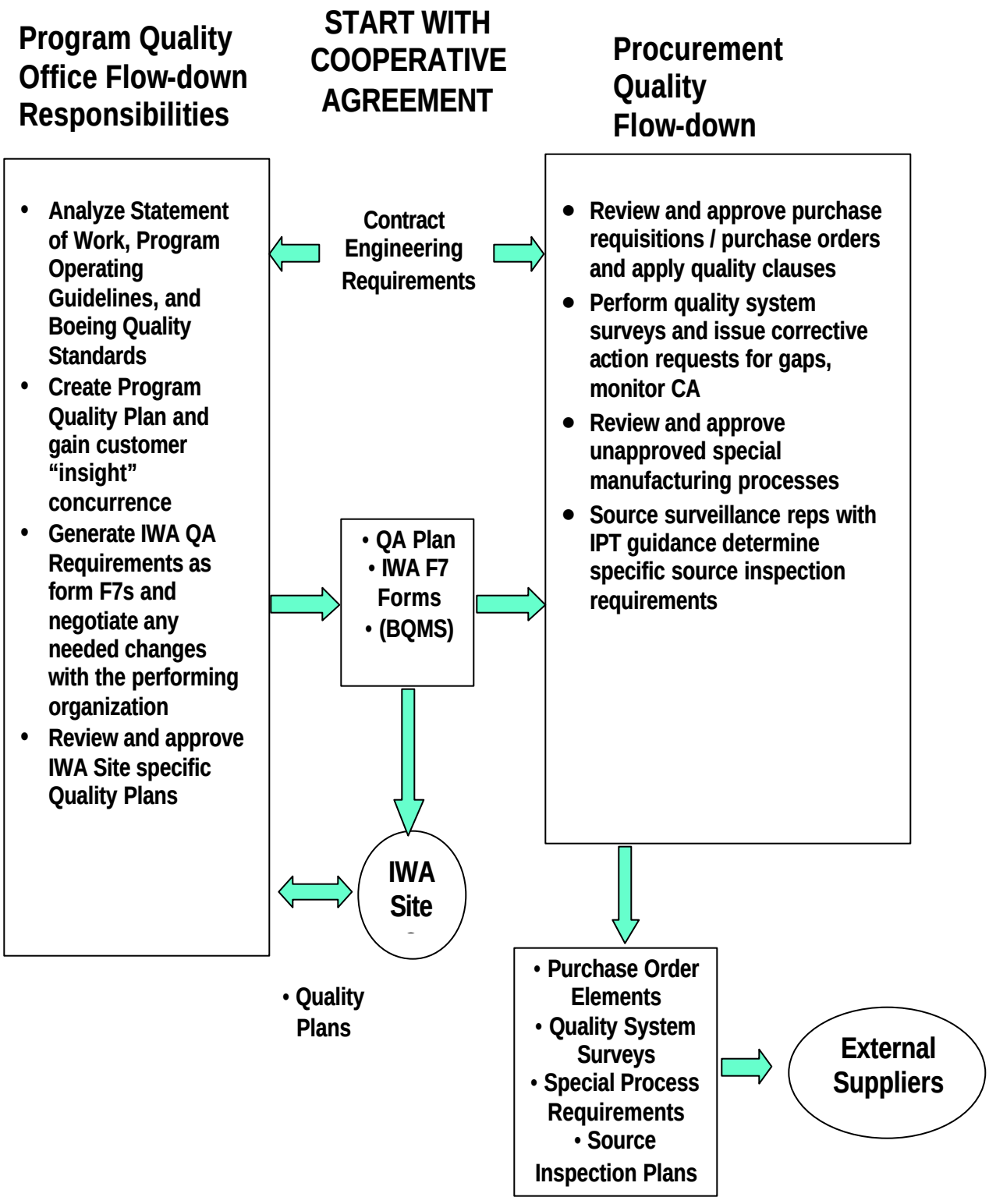


Figure 4.9 Flow of Quality Assurance Requirements

To assure the satisfactory completion of the above activities, a combined quality assurance team will be formed. The team will be composed of representatives from:

- Program Quality Office - Seal Beach
- Procurement QA - Huntington Beach
- Software QA - Huntington Beach
- Manufacturing QA - Multiple IWA sites
- Assembly, Integration, and Test QA - Palmdale

The primary function of this team is to provide for the appropriate QA requirement flow down both internally (to IWA sites) and to external suppliers by way of the purchase order system. The team will also provide QA oversight and guidance across Boeing X-37 participants and assure that basic process controls, validation and acceptance practices, and data packages meet required QA standards.

In general, the program quality office provides support in the following functional areas:

- Establish quality requirements
  - create quality assurance plan
  - review A and B level specifications
  - create IWA quality requirements
- Provide IWA support
  - assure flow down of quality requirements
  - review IWA site-specific quality plans
  - provide ISO audit support
- Provide program management support
  - attend biweekly program manager's meeting
  - address QA issues for IPT leads and PM
- Analyze digital mock-up (DMU)
  - assure supplier ability to maintain configuration management and produce conforming hardware and software
- Serve as customer QA interface
  - notify NASA of major QA issues
  - provide software QA support
  - monitor and support SQA problem reporting/resolution
- Conduct supplier quality surveys
  - establish quality system/ISO 9001 status
  - monitor supplier corrective action requests resulting from surveys
- Provide backup for Procurement QA
- Conduct supplier oversight
- Provide oversight of preparations for verification/certification of atmospheric and orbital testing

Project specific support in these functional areas will be provided to the X-37 project as appropriate.

4.4 Hardware Design and Verification Assurance Processes

4.4.1 Boeing Design Philosophy

The design approach employed on the X-37 program is based on the rapid prototype philosophy and processes developed within the Boeing Phantom Works organization. The key elements of this design and design verification process are described below.

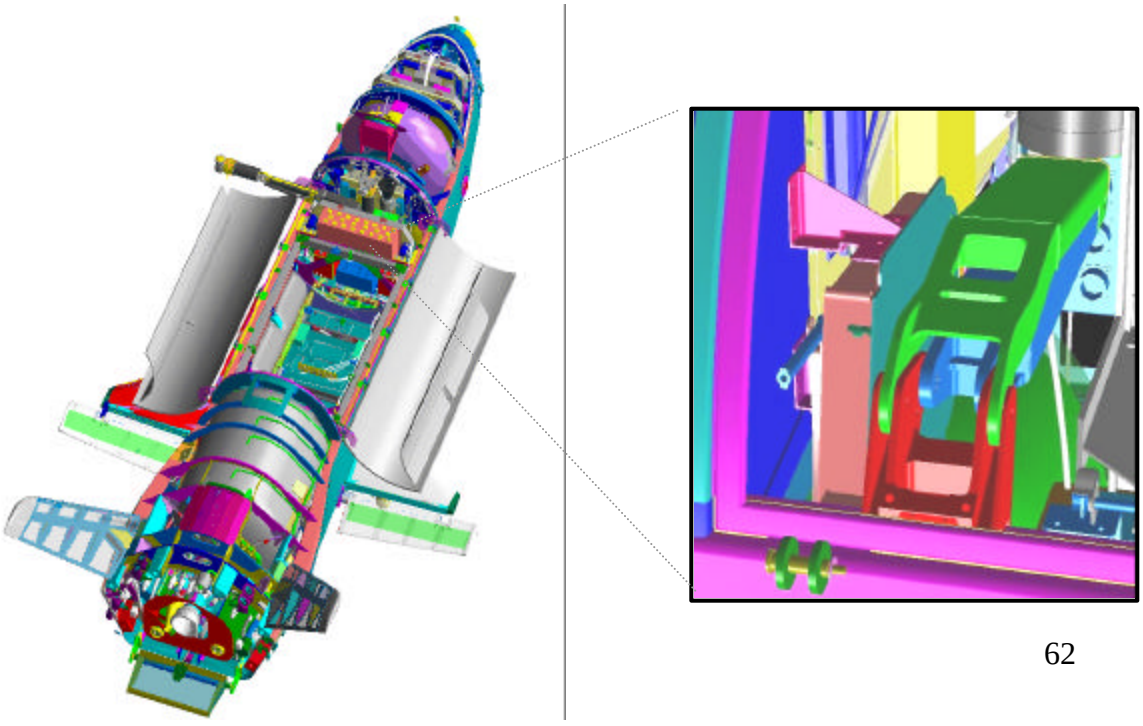
Co-Location of Personnel

Approximately 85 percent of the X-37 core project team (approximately 200 people) are collocated on one floor of the Seal Beach facility. This provides easy and convenient access among project team members and facilitates effective communication and problem resolution.

Digital MockUp (DMU)

The DMU is a computer-aided design tool that utilizes the CATIA software. The DMU, composed of the CATIA-generated solid model, parts list, and requirements, is an electronic digital mockup that facilitates the development, integration, and management of complex systems. The DMU facilitates real time, synchronized design integration across all disciplines and provides electronic configuration control and single source of design control. The DMU provides integration of over 2500 CATIA solid models with resolution down to the fastener level. Figure 4.10 is a typical representation of the utilization of the DMU.

Figure 4.10 Digital Mockup Unit (DMU): X-37 Vehicle Solid Model (with expanded view of mid-body battery pallet components)



Utilization of IPT's

IPT's corresponding to the eight major design elements of the X-37 project (listed below) have been formed.

- Flight Sciences
- Airframe/Structures
- Mechanical/Thermal/Propulsion
- Avionics, Power, and Software
- GN&C
- Vehicle Assembly
- System Test
- Shuttle Integration

Each team has a lead and the individual teams have primary responsibility for maintaining their own subsystem specifications, change control baselines, subcontractor requirements and statements-of-work (SOW's), material review boards, and risk mitigation activities. The SE&I IPT, as noted in the previous section of this report, has responsibility for assuring appropriate integration of the individual subsystem IPT activities. The X-37 Deputy for Systems Engineering leads the SE&I IPT with membership comprised of the various subsystem IPT leads, in addition to representation from Configuration Management, Risk Management, Requirements and Analysis, Systems Integration, and Reliability, Maintainability, and Supportability. Each individual IPT holds weekly technical interchange meetings (TIM). In addition, the IPT leads have their own weekly TIM.

Zone Managers

The X-37 vehicle has been divided into "zones" (i.e., fore, mid, aft) with each zone designated a zone captain. Their primary responsibility is to assure that all components within their zone are properly integrated within the Digital MockUp (DMU). The zone captains hold thrice weekly "fly-throughs" using the DMU.

Focused Tiger Teams

Tiger teams, smaller groups of engineers from across the IPT's, are formed to resolve specific multidisciplinary design problems when they arise.

4.5 Software Design and Verification Assurance Processes

4.5.1 Guidelines and Plans

Boeing software quality assurance (SQA) affects every aspect of the X-37 development effort. SQA covers activities conducted in-house at Seal Beach, at the IWA partners, and at external software suppliers. Software quality "how's" are documented in Boeing and X-37 project standards and guidelines. These include:

- General guideline documents (GV specifications) and Software Process Manual (SPM)
- X-37 planning documents
- Software Product Plan (SPP)
- Software Standard and Procedure Manual (SSPM)
    - coding standards
- Software Process Design Document (SPDD)
- Software Development Plan (SDP)
- Software Quality Plan
- Configuration Management Plan
- Risk Management Plan

As indicated above, the Software Development Plan is the key document that defines the overall software quality assurance role for the project. This includes a description of the technical interchange meetings (TIM), reviews, and audits to be conducted. In addition, to providing details of the configuration management, risk management, and software supplier oversight processes, it also addresses software corrective actions and IV&V process and liaison activities.

4.5.2 Design and Development

The general software development process is depicted in figure 4.11.

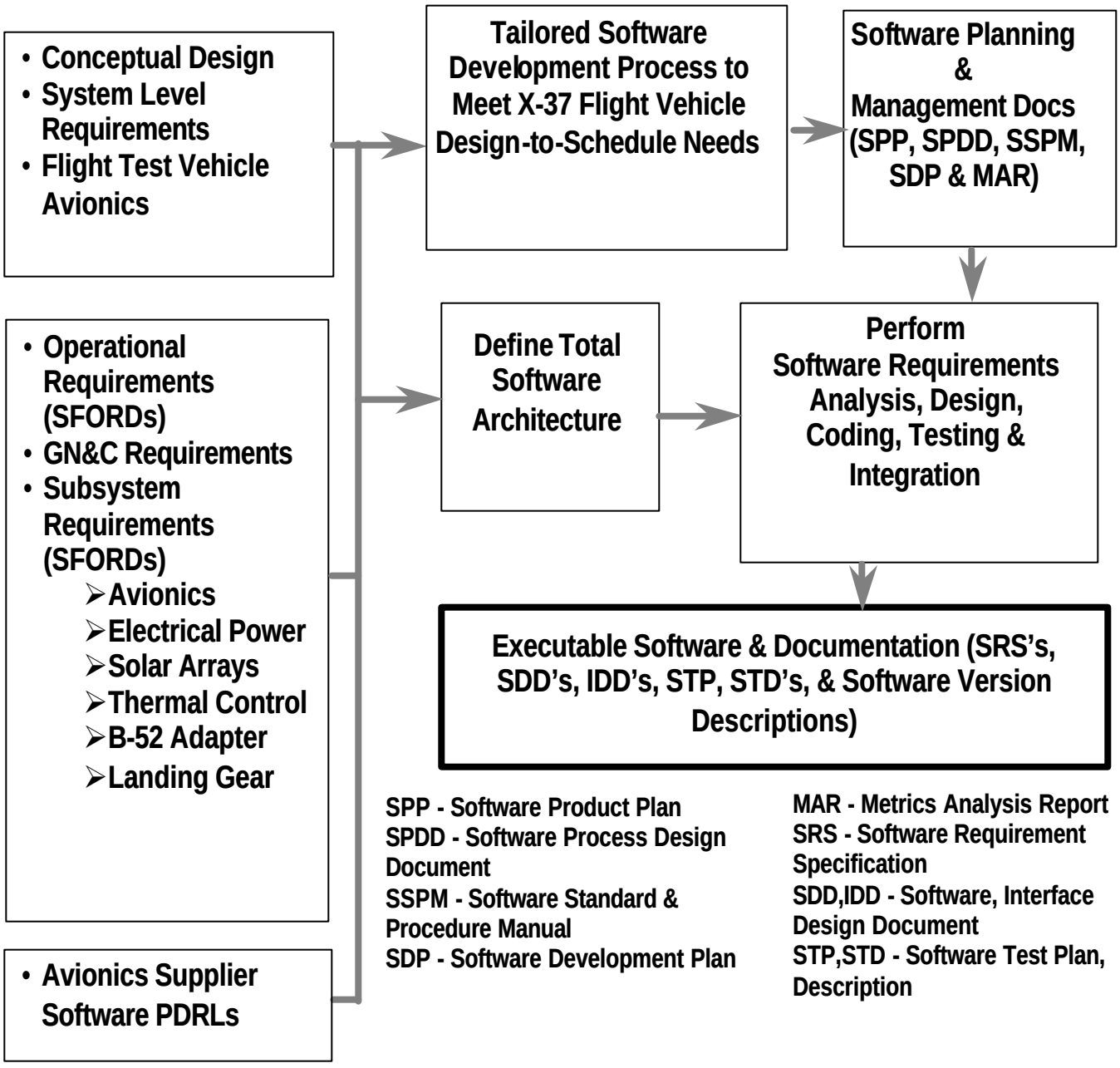


Figure 4.11 Software Design and Development Process

This process describes the top-level requirements analysis/flow down process and subsequent design activities which begin with system/subsystem level and operational requirements and result in executable software and documents. Figure 4.12 provides details concerning the flight software development steps including where static, real time, and hardware-in-the-loop integrated testing typically occur in the developmental process.

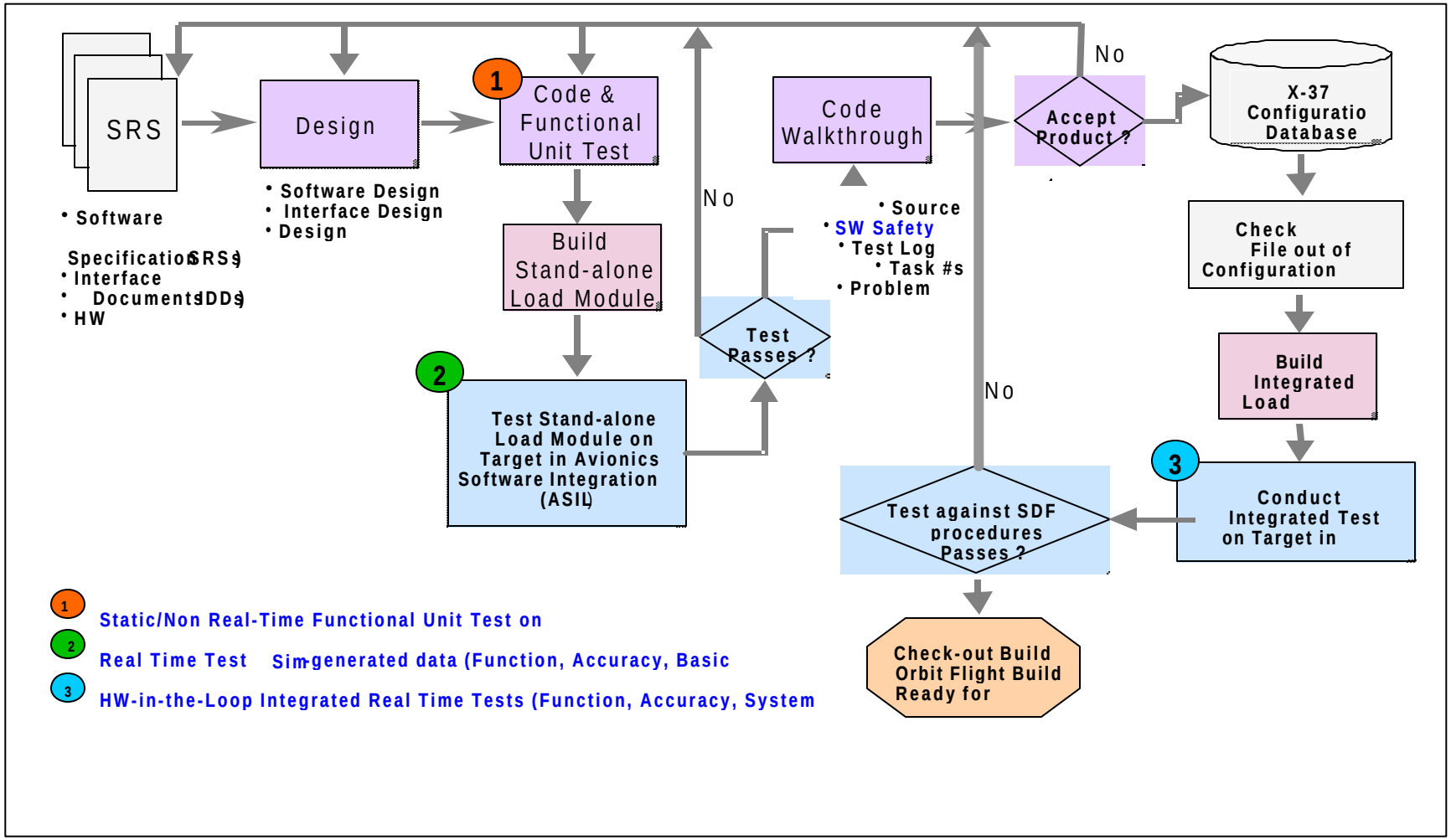


Figure 4.12 Flight Software Development Steps

4.5.3 X-37 Software Products

Figure 4.13 identifies the current mission critical and support software deliverables for the X-37 project. This chart also identifies software products with respect to in-house or subcontractor development responsibilities.

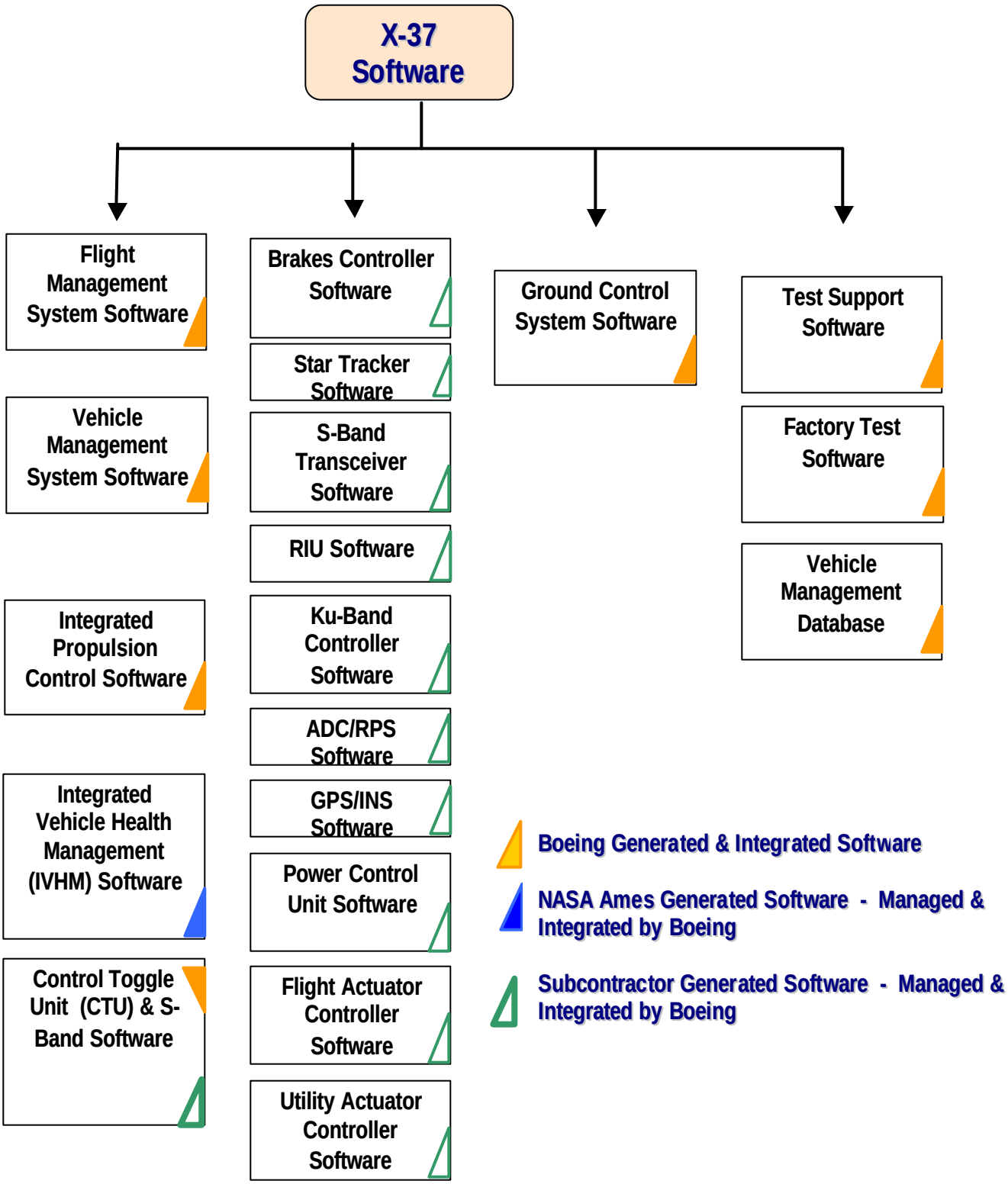


Figure 4.13 Software Deliverables

It should be noted that while Boeing is rated at Software Engineering Institute Capability Maturity Model (SEI/CMM) Level 5, the X-37 software development activity is following SEI/CMM Level 4.

4.5.4 Software Supplier Oversight

Oversight of software suppliers and subcontractors is governed by Boeing general guideline documents (referenced in paragraph 4.5.1) which specifically address selecting subcontractors, planning work packages, and monitoring software quality assurance and configuration management activities. Typically, a software engineer (subcontractor software oversight manager) is assigned to oversee suppliers and products. His tasks generally include:

- Interfacing with NASA (including IV&V), Boeing contract, management and leads, SQA, and configuration management
- Maintains software suppliers (internal and external), products, and contents lists
- Utilizes software suppliers tracker tool to monitor each product
- Identifies nonconformances and tracks to closure
- Communicates progress/issues/risks to supplier, Boeing management, and NASA

The software engineer or oversight manager also reviews and approves supplier documentation for technical content and attends supplier reviews as appropriate.

4.5.5 IV&V Liaison and Support

Boeing will maintain active liaison between the X-37 project software development activities and AVERSTAR/NASA IV&V teams. The principal objective of this liaison and support function will be to verify systems and operational requirements compliance, feasibility, testability, and traceability and to work with NASA on process recommendations and nonconformance issues. The planned scope of this effort will include all flight critical software as defined by the IV&V facility's criticality and risk assessment (CARA) process. Boeing will also be responsible for monitoring IWA and outside supplier software processes, products, and development efforts.

4.5.6 Software Test Strategy

Boeing has adopted a flight software test approach that involves parallel code and test development. Beginning with top-level requirements, the development path includes design, coding, and testing while the parallel verification path provides for test case description and test case implementation. These two paths then converge to produce the validated computer software configuration item (CSCI). Independent verification and validation provides an additional parallel check for this development and test approach. The system test bed build-up begins in the X-37 Avionics and Software Integration Laboratory (ASIL) and culminates in vehicle-in-the-loop testing. At this point formal qualification tested (FQT) software CSCI's are turned over to X-37 vehicle integration. FQT documentation and the software development folders (SDF) serve as the basis for

software vehicle integration test support. To assure continuity, the software engineers responsible for flight, ground control, and factory test software development support the hardware/software vehicle integration activities.

4.6 Manufacturing Verification and Test Assurance Processes

4.6.1 Assembly, Integration, and Test

The responsibility for assembly and integration lies with the Assembly, Integration, and Test (AIT) IPT. This team's overall responsibility includes assistance in:

- Collaborative design engineering for manufacturability as well as testability
- Development and execution of vehicle assembly planning and procedures
- Functional test and evaluation of the flight vehicle systems
- Configuration of the vehicle as an atmospheric test article and its modification into a space-flight configuration

The Boeing Aircraft and Missiles (A&M) and the Reusable Space Systems (RSS) business units are assisting in the fabrication of parts, flight test equipment, and support items required by the program. These business units provide the staffing levels, utilizing "best" personnel assets, to assure assembly, integration, and test success. Each business units' respective staff operate under one individual who oversees both units for onsite program management and reports directly to the AIT IPT lead. The "Best of Boeing" practices, separate from the mainstream facility environment, are being utilized.

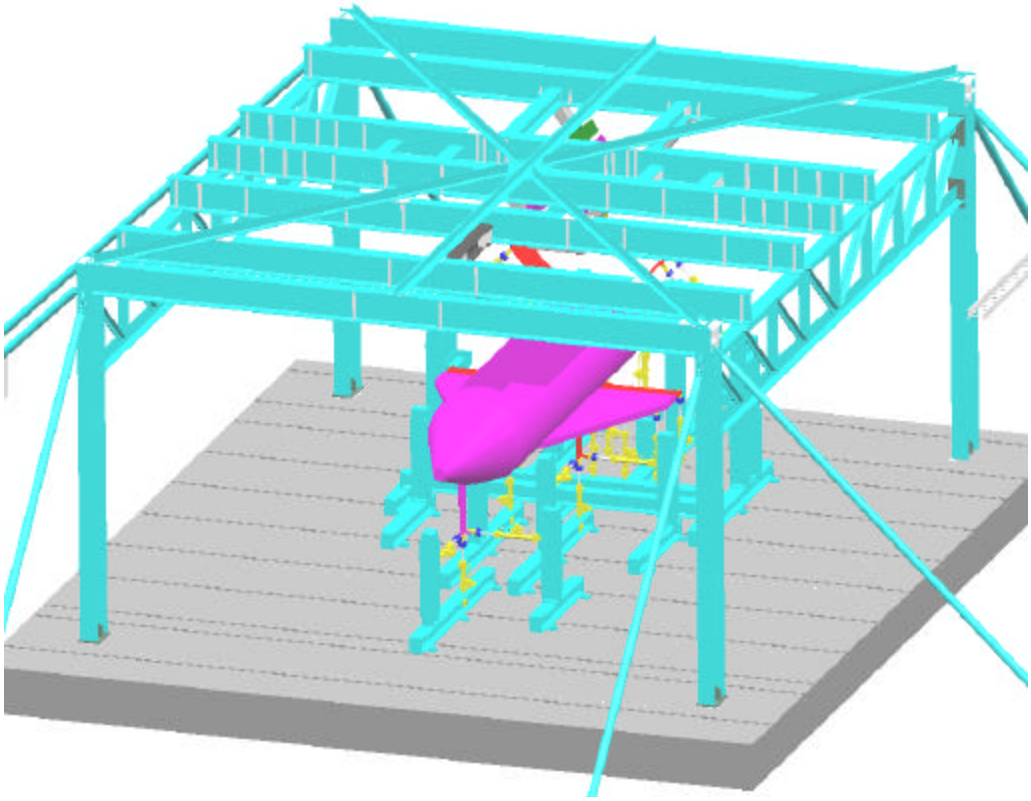
The AIT process controls employed on X-37 are either currently in use on the Space Shuttle or International Space Station or are unique adaptations of previously approved processes. AIT variability reduction activities, based on collaborative engineering and assembly simulations, are planned to reduce the variability issues between as-designed components. Digital capture of the as-built parts as they become available will be incorporated to further reduce variability risks.

In the manufacturing areas, quality engineers currently supporting both Space Shuttle hardware and International Space Station development will be utilized to review all build and test procedures. Dedicated quality inspectors are planned to be on the factory floors to support daily build and test operations.

4.6.2 Major Manufacturing, Assembly, and Integration Locations

The X-37 major airframe (fuselage) will be manufactured at the Boeing A&M facility located in St Louis, Missouri. Upon completion, the fuselage will be shipped to Palmdale, California. The fuselage and major structural components will be assembled at the High Desert Assembly and Integration Test Facility (HDAIT) Building 145. Following initial assembly, the vehicle will be subjected to static proof loading as depicted in figure 4.14.

Figure 4.14 X-37 Static Proof Loading



The X-37 final assembly and integration of subsystems will be done jointly utilizing the assets of the HDIAT and the Reusable Space Systems Assembly, Integration, and Test Facility. Both of these facilities are collocated at the Air Force Plant 42, Site 1, in Palmdale, California.

4.6.3 Program Plans

Specific program level plans have been drafted in support of the AIT effort. These include:

- Quality Assurance Plan
- Safety Plan
- Contamination Plan
- Integrated Vehicle Test Plan
- Manufacturing Test Plan
- Transportation Plan
- Configuration Control Plan
- GSE/STE
- Material Control Plan
- Facilities Utilization Plan

4.7 Pre-Flight Integrated Verification & Test Assurance Processes

4.7.1 Integrated System Test Process

Upon completion of assembly and integration, the X-37 will be subjected to a series of systems tests to verify implementation of system requirements. The systems test responsibility comes under the Systems Test IPT. The overall system test program identifies a three-phase test flow approach.

Phase 1

Phase 1 consists of three levels of pallet testing. The first is Pallet Level Functional Testing. The second level consists of Pallet Integrated Testing – standalone. The third level is the Pallet Functional Testing (soft-mate) with the X-37. This series of tests are to be performed at Huntington Beach. At successful conclusion of this phase, the X-37 is ready to support the B-52 Integrated System Test described in the next phase.

Phase 2

Pre-approach and landing tests (ALT) integrated testing will be performed making maximum use of flight vehicle functionality for those systems active during the ALT program:

- Entry GN&C verification (Software)
- Avionics Functionality (Guidance, Command and Control (RF Systems), Air Data Sensors and Power
- Mechanical Systems Functionality (Landing Gear and Brakes, Surrogate Aero Surfaces)
- Vehicle Characterization for GN&C (Guidance-Alignment Verification, Mass Properties-Weight and C.G., Aero Surfaces-Ground Vibration Testing

Upon successful completion of this phase of system testing, the X-37 is ready to support the B-52 flight operations testing at DFRC as described in section 4.8.

Upon completion of the ALT flight testing, the X-37/AR2-3 will undergo a Flight Readiness Firing (FRF) at a facility located near DFRC.

Following the X-37 FRF the vehicle will be shipped to Huntington Beach for the next phase of the test program.

Phase 3

Pre-orbital flight test functional and environmental testing is designed to encompass the full rigor of space flight environments and operational requirements. Environmental test series are based on flow down of requirements from the Space

Shuttle/Payload ICD-2 19001. A tailored proto-qualification/flight proof strategy based upon MIL-STD-1540C will include the following:

- Propulsion leak and proof load test
- SV Alignment verification
- Functional test
- Weight and center of gravity
- Ground vibration test and modal survey
- X-37 free body with minimum H2O2
- X-37 free body with maximum H2O2
- Thermal vacuum and balance test
- X-37 free body proto-qualification
- X-37 free body thermal balance
- EMI/EMC (per MIL-STD-1540C 6.2.2, qualification level tailored to MIL STD-1541)
- Acoustic test (levels per MIL-STD-1540C, acceptance level plus 3db)
- X-37 free body
- X-37 with launch ring
- Final alignment
- Final Factory Test

Upon the successful completion of these final series of system tests, the X-37 will be shipped to KSC in preparation for launch in the Space Shuttle and orbital flight operations.

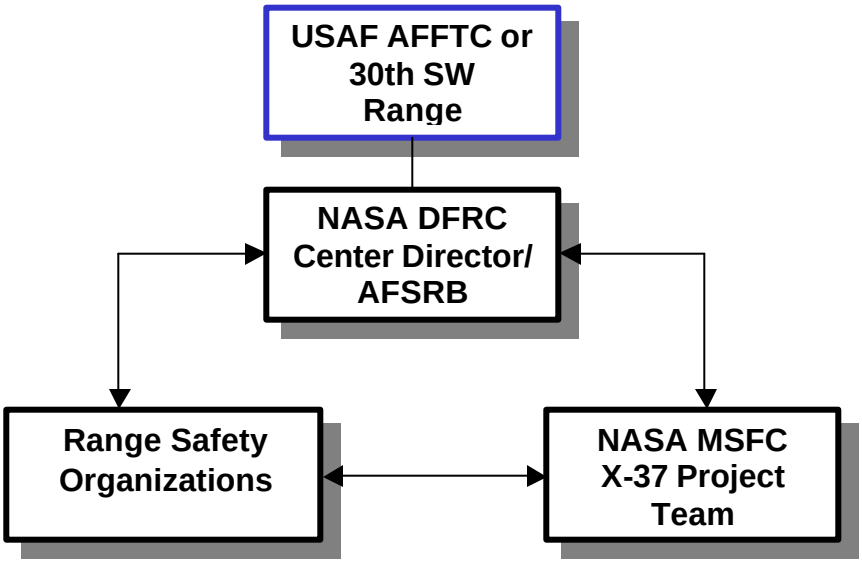
4.8 Operations Assurance Processes

4.8.1 USAF/30th Space Wing/AFFTC

Range Safety

The X-37 landing site(s) identified in Design Reference Missions 1 through 6 are either EAFB or VAFB. Range operations planning is moving forward on this basis and is governed by the AFFTC or 30th SW Range Commanders for landing and operations at VAFB and the DFRC Center Director/AFSRB for landing and operations at DFRC. Figure 4.15 depicts this functional organizational relationship for range safety.

Figure 4.15 Range Safety



Since activities are planned at both sites (altitude drop tests, de-orbit and reentry) operations range approvals are subject to several range safety policies. These are:

- DOD/USAF- DoDD 3200.11 (Major Range and Test Bases)
- NASA NPG 8715.3 (NASA Safety Manual)
- NASA NPG 2810.1 (Security of Information Technology)
- NASA DPD 8740.1 (Range Safety Policy)

Additionally, the X-37 is subject to several range safety processes. These are:

- DoD/USAF EWR/AFFTC 127-1 (Tailored for the X-37)
- DoD/USAF AFI 13-212 (Weapons Range Management)
- DoD/USAF AFFTCI 11-1 (Flight Operations)
- DoD/USAF AFFTCI 91-5 (Test Safety Review)
- NASA DCP-X-009 (Air Worthiness and Safety Review)

- NASA DCP-F XXX (Range Safety Systems Office Organization Process) Draft
- NASA DCP-F XXX (Range Safety Analysis Process) Draft
- NASA DCP-F XXX (Range Safety Officer Process) Draft
- NASA DCP-F XXX (Flight Termination System Process)
- NASA DCP-F-104 (FTS Configuration Control Process)

The overall range safety approval process and the interrelationships between the ranges and the X-37 program office is depicted in figure 4.16.

4.8.2 Flight Termination

One feature of vehicle design that is required due to potential atmospheric flight over populated areas is a flight termination system (FTS). This system consists of laser initiated ordnance used to separate the wings, resulting in loss of aerodynamic lift capability and loss of vehicle. The requirement and implementation of the FTS is governed by EWR 127-1. The Range Control Officer in concert with the X-37 project office will develop and execute agreed upon mission rules and area clearance and termination criteria. The system is single fault tolerant for safety. The system will only be activated should the vehicle stray from its intended flight path during reentry and atmospheric flight.

Since a final decision on a landing site has not yet been made, EWR 127-1 is being tailored to provide a consolidated set of range safety requirements regardless of landing site decision. This involves an ongoing coordination between DFRC/AFFTC/30 SW to support all potential mission scenarios and requirements. Initial de-orbit trajectories have been developed and reviewed (for 28.5, 39.0, 51.6 degrees of inclination) with respect to meeting the Expected Casualty, Ec requirement (see paragraph 4.2.5).

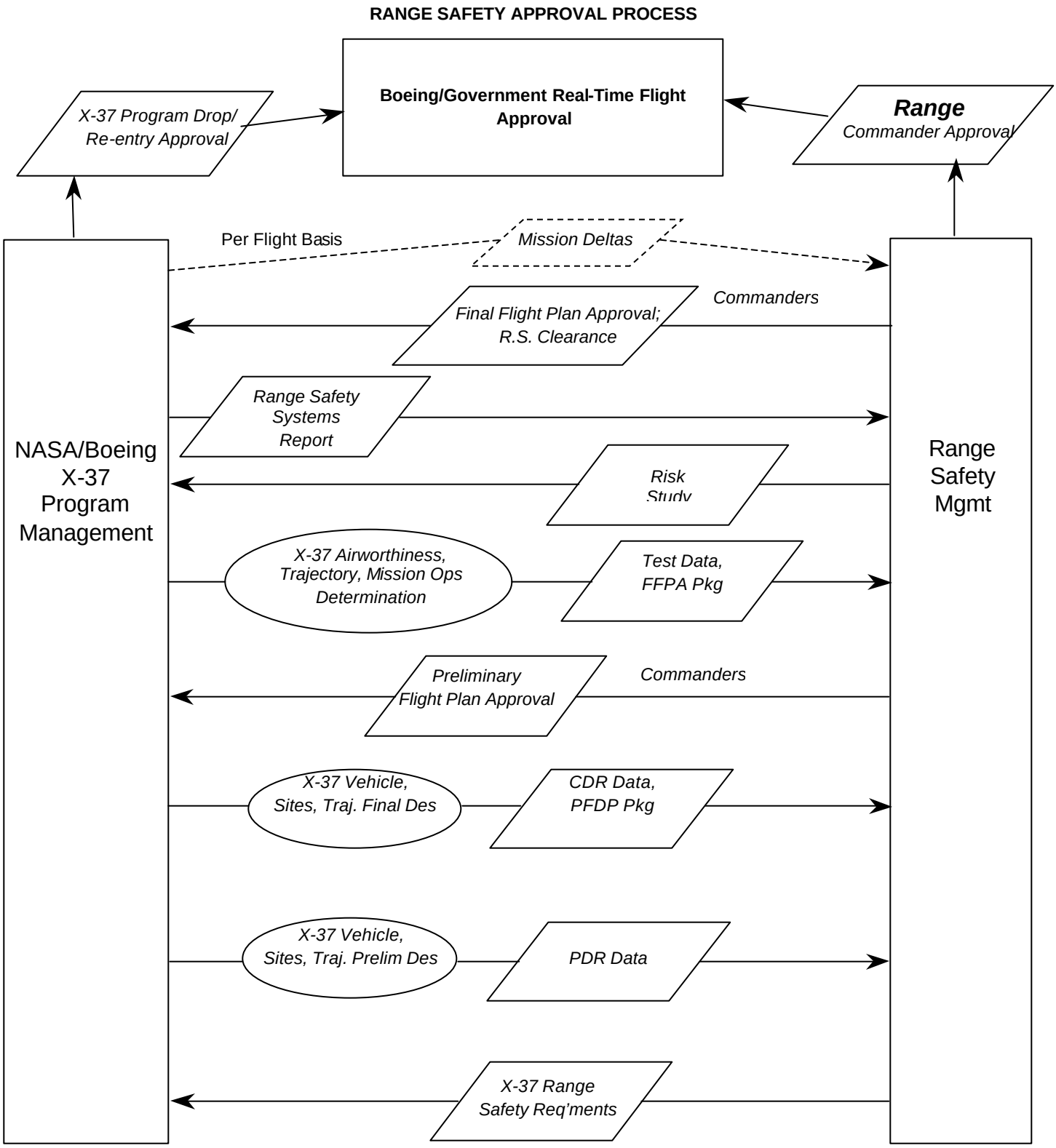


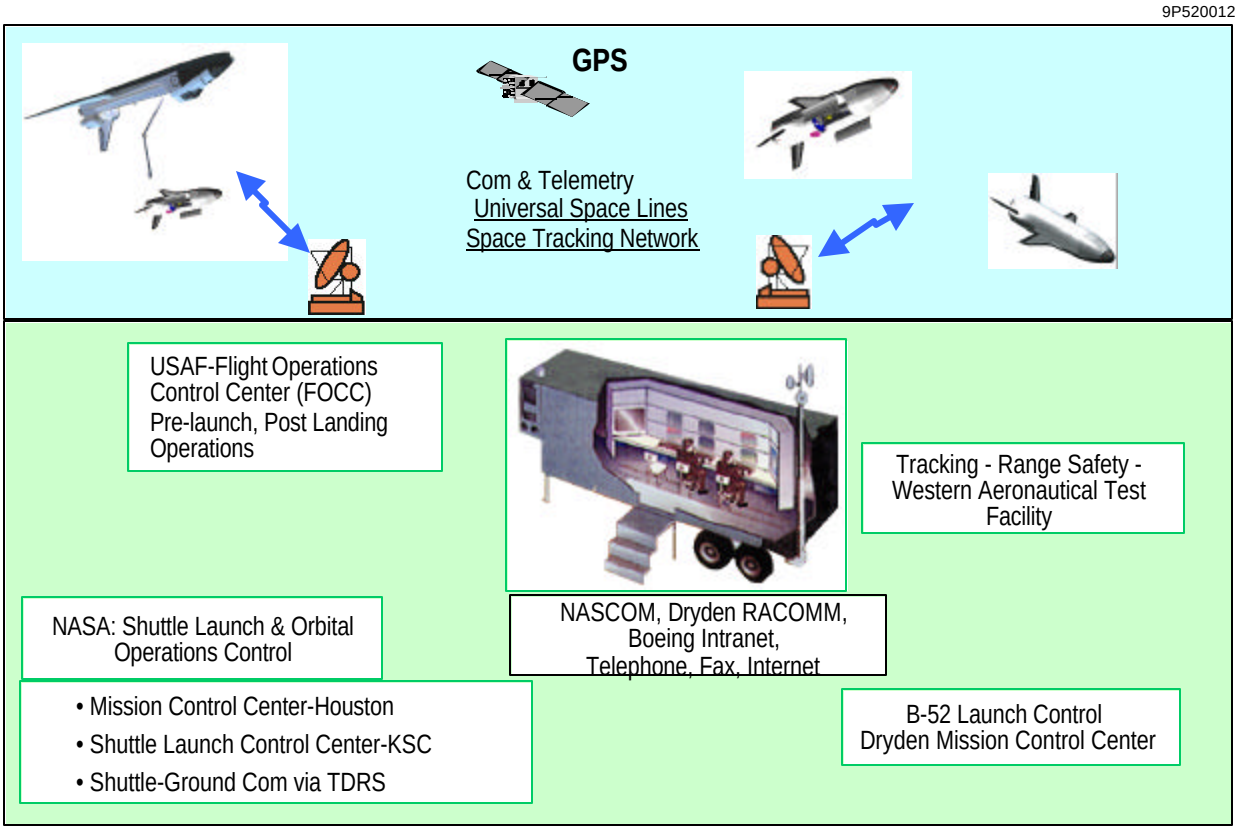
Figure 4.16 Range Safety Approval Process

4.8.3 Flight and Ground Operations

Ground/Flight Operations Control Center (FOCC)

The concept for the X-37 program ground operations is aircraft-like operability and rapid turnaround capability designed into the vehicle. The ground and flight operations equipment elements include the Flight Operations Control Center (FOCC) equipment and software which will be employed for command, control, and data handling of all phases of flight (ALT, On Orbit) and vehicle ground processing and testing. The FOCC is a mobile facility configured with workstations and communication interfaces for range, communication network, and Internet access. Test and ground control software will be used in the FOCC to support training and flight operations. Figure 4.17 depicts the ground segment and FOCC external interfaces.

Figure 4.17 Flight Operations Control Center



Atmospheric Test Phase

The atmospheric test phase is the Approach and Landing Test (ALT), designated DRM-4, to be performed at DFRC and Edwards AFB. The duration is approximately 2 hours. The ferry vehicle will be the Atmospheric Test Launch Vehicle (B-52). A series of drop tests are planned to verify the GN&C control parameters and sensors that control the vehicle from altitudes of 40,000 feet down through the approach, landing, and rollout phase. After release, the X-37 will glide in for an unpowered autonomous landing utilizing the INS/dGPS, calculated air data system (CADS), radar altimeter, and aerosurface controls.

The X–37 ALT program objectives will build upon and extend the testing to date on the X-40A program. X-40A helicopter-launched autocontrol flight demonstrations are complete and data has been incorporated into the GN&C and avionics design of the X-37. While additional drop tests are planned for the X-40A, ground and flight operations lessons learned are being transferred to the X-37 development and operations planning. The X-40A derived flight operations support equipment and procedures are to be upgraded and infused into the X-37 program by an experienced X-40A flight operations team.

The X-37 will undergo a series of towed taxi tests (DRM-3) to demonstrate its ability to navigate and control rollout and verify instrumentation and data collection. These tests are followed by a series of captive-carry flights with the B-52 to verify the flight qualities while attached to the B-52 and vehicle data links (command, control, telemetry, tracking, flight termination). The final series of X-37 tests from the B-52 are five free-flight approach and landing tests to demonstrate unpowered flight and landing characteristics of the X-37.

The X-40A flight tests are designed to help mitigate risks to the X-37 in several areas:

- CADS test and evaluation in an aerodynamic flight environment
- Evaluation of the Honeywell SIGI (GPS/INS) under flight conditions
- FOCC site integration and flight test operation
- Flight test and tune GN&C algorithms
- PID maneuvers to improve the X-37 aerodynamics database

Safety requirements concerning the approach and landing tests, flight demonstrations from the B-52 carrier aircraft, and the return from orbit can be found in both the DFRC DCP-S-002, "Hazard Management," and the Air Force EWR 127-1 documents, as referenced.

Shuttle On Orbit Operations

The X-37 will be delivered to orbit as a payload on board the Space Shuttle where it will accomplish the design requirements for orbital missions, as specified in DRM-2.

During ascent, the X-37 will be in the payload bay and will be supported by two modified Spacelab pallets (one forward and one aft). Also located aft is a launch ring where the X-37 attaches to the Space Shuttle aft fuselage frame via four pyrotechnic bolts and two trunnion mechanisms located on both sides of the X-37 forward fuselage.

Once the X-37 is carried to orbit, the payload bay doors are opened and a limited amount of X-37 vehicle activation and checkout (C/O) is conducted. The intent of the limited C/O is to verify the vehicle is ready for autonomous flight as well as to make sure X-37 vehicle critical systems such as the propulsion system and reaction control system are in a safe state to protect the Space Shuttle crew and vehicle. Upon completion of the C/O, a grapple fixture located on the X-37 upper fuselage is grappled by the Shuttle Remote Manipulator System (SRMS). The trunnion mechanisms are retracted, freeing the forward fuselage on the X-37 from the Spacelab cradle. Using the SRMS, the X-37 is rotated, while still attached to the aft ring, to approximately 30 degrees nose up.

The four pyrotechnic bolts are then fired releasing the vehicle from the aft ring. Once free from its aft ring, the SRMS maneuvers the X-37 to a release point outside the payload bay. At a predetermined point, the X-37 is released from the grapple fixture and the X-37 becomes free in orbit. With the X-37 in free flight the Space Shuttle fires its RCS for a separation burn maneuver so as to increase the distance between itself and the X-37.

When the X-37 is at the minimum safe distance from the Shuttle a command is sent to the X-37 from the ground based FOCC via the Tracking and Data Relay Satellite System (TDRSS). This command triggers the onboard flight management computers (FMC's) and vehicle management computers (VMC's) to load the operational flight software and bring the X-37 vehicle to full activation.

At this point the X-37 vehicle begins its autonomous flight. A flight will last anywhere from 2 to 21 days depending upon the mission objective. During this time the vehicle will perform a variety of flight activities focusing on the demonstration of the 39 embedded technologies. The elements of the On-Orbit Flight Control System (i.e., the INS/GPS and Stellar Attitude Sensors and the primary and vernier RCS thrusters) will be verified.

At the end of orbital operations and system verification, the X-37 will perform de-orbit maneuvers utilizing the AR2-3 engine performing a short burn for reentry and utilizing the primary RCS for de-orbit trim burns. The primary RCS provides a redundant means of de-orbiting the vehicle should the AR2-3 fail. Autonomous atmospheric flight and landing will occur at a selected West Coast landing site. The GN&C system utilizes the automated capability derived from man-in-the-loop Space Shuttle experience. The vehicle design is double fault tolerant for Space Shuttle flight safety and single fault tolerant for mission success.

5.0 Observations, and Recommendations

5.1 Reliability Analysis

Observations

The IA team has significant concerns related to the overall reliability analysis as presented. Specific issues include:

- The overall reliability analysis approach/process/methodology was inadequate.
- The absence of software being realistically considered and included in the overall system reliability analysis
- The need to specifically address the potential of common mode failures
- The lack of consideration for incorporating the human element as a potential failure mode
- The lack of meaningful discussions of the basis (e.g., specific component design knowledge, previous flight or test data, use of expert judgement) for the component failure probabilities used in the FMEA descriptions.

Recommendations

R1. Provide the team with further discussion and clarification with respect to the establishment of a probability of mission success (POMS) number.

R2. Expand the definition and derivation of the POMS. Specifically, is the POMS of .975 a top-level program requirement which subsequently drives the system and subsystem design or are the component level probability estimates aggregated to result in the POMS? In other words, is this a top-down or a bottom-up process?

R3. Define exactly what is meant by mission success in the context of the expression "probability of mission success (POMS)." Explain the specific phases of operation (launch, on-orbit, reentry) associated with the definition of "mission" and POMS.

R4. Define and defend how the POMS level of reliability will, in fact, be achieved.

R5. Demonstrate how the POMS estimate will meet the Eastern and Western Range Safety Requirements (EWR 127-1) expected casualty rate, Ec, of not more than 30 casualties in one million for the general public during the flight operations of the X-37. This requires showing how the aggregate X-37 component reliability estimate couples to the X-37 vehicle breakup and debris pattern (and assumptions) and the population density profile along the primary reentry corridor as well as contingency landing sites (separate analyses).

R6. The team recommends that the NASA X-37 project office work with Boeing to conduct a parametric assessment of Ec for various alternative assumptions (other

than the probability of success equals 1.0) concerning human reliability and software reliability.

Without checks and balances, human reliability in performing critical tasks is generally assumed to be no better than a probability of .997. Bounded values for each of these critical X-37 system elements (software and people) should be derived through consultation with appropriate literature, experts, and organizations. These would include the NASA IV&V Facility, Carnegie Mellon Software Engineering Institute (SEI), and human reliability data from the nuclear power industry and the Department of Energy. Key references include:

- Handbook of Human Reliability Analysis (NUREG/CR-1278, August 1983)
- THERP - Technique for Human Error Rate Prediction, (Swain and Guttmann, 1983)
- A Procedure for Conducting a Human Reliability Analysis (NUREG/CR-2254, May 1983)
- Accident Sequence Evaluation Program (ASEP) Human Reliability Analysis Procedure (NUREG/CR-4772, October 1986)
- A Manager's Guide to Reducing Human Errors (CMA, July 1990)

(Also see <http://www.nrc.gov/NRC/NUREGS/BR0184/part13.html.> and http://www.dne.bnl.gov/rmq/rmq0494/0494_13.HTML)

The sensitivity of Ec to these assumptions should be established and presented along with rationale for the ultimate reliability estimate presented to range officials.

5.2 Assurance Support Staffing and Coordination

Observation

The IAT noted the very positive aspects of addressing X-37 assurance needs through a combination of SMA and space transportation and engineering directorate support. While noteworthy, and fundamentally positive, it appears that working level coordination between participants in the overall X-37 verification and assurance activities is inadequate.

However, the IAT has concerns regarding the SMA staffing for the X-37 program. The scope of assurance activities outlined for the SMA function includes 16 distinct functional areas. The MSFC SMA allocation of 1.0 FTE is obviously inadequate (until very recently, support was only 0.5 FTE), even with limited contractor support.

Recent MSFC senior management decisions redirected 4.0 FTE from the MSFC SMA organization that could have addressed the shortage in SMA resources. This issue needs to be addressed at the highest management levels at MSFC and NASA Headquarters

Recommendation

R7. The team recommends that the NASA X-37 project manager establish (under the Chief Engineer or Risk Manager) a weekly coordination meeting between all individuals involved in safety, risk management, and/or assurance activities.

R8. The team recommends that SMA staffing be increased as soon as possible to adequately support both the in-line support activity (currently provided) and the independent assessment role.

5.3 Main Propulsion System Heritage

Observation

The IAT did not see any evidence of an established selection criteria for the AR2-3 engine, particularly as it related to previous use or heritage, i.e., specific descriptions of past applications in terms of flight duration/environments/failures, storage and perishable parts replacement history, previous ground testing, etc.

Recommendation

R9. The team recommends establishing a process to clearly define/document the pedigree, test history, verification and re-certification of the AR2-3 propulsion system. (Indeed, the same process should be applied to all software and hardware heritage components). In addition, this documentation will be necessary to support formal flight readiness review certification (i.e., CoFR) activities.

5.4 VAFB verses EAFB Landing Site Risk Tradeoffs

Observation

Tradeoff analyses to determine the final selection of a landing site must include consideration of the X-37 program's ability to meet the E_c requirement.

Recommendation

R10. The degree of confidence placed in the E_c estimate and the sensitivity of the E_c calculation to key assumptions must be described and defended.

5.5 Reentry Operations

Observation

The team has noted an absence of a detailed pre-deployment plan which would verify, prior to release and free flight of the X-37 vehicle, the functional operability of avionics, system redundancy, overall GN&C system, and the command and control links between the FOCC and TDRSS.

For potential Space Shuttle operations, it was indicated that insufficient avionics mounting cold plate cooling capability could preclude these verification checks from being accomplished. It was also noted that the Spacelab mounting pallets could be modified to achieve the appropriate cooling. In any event, the team considers system verification prior to deployment from the Space Shuttle payload bay a critical safety and mission success concern.

Recommendation

R11. The IAT recommends that the X-37 Program consider the following operational constraints:

- Monitor and verify the status of critical flight control systems and redundancy prior to launch, during flight, and prior to reentry
- Establish a formal protocol (documented procedure) for verification of reentry enabling ground command up-link and range control radar and communication lock.

5.6 Human Intervention/Command Uplink

Observation

Fully autonomous guidance navigation and control systems (the current approach) are potentially vulnerable to failure scenarios leading to commanded destruct. Override control authority (software and/or hardware reset commands in the event of off nominal flight conditions) could potentially obviate the need for unnecessary flight termination.

Recommendation

R12. In the interest of preserving mission success, and consistent with the concepts of Design for Safety (see <http://dfs.arc.nasa.gov>), the team recommends that the X-37 program consider the option of incorporating command up-link capability during approach and landing operations.

5.7 Orbital Debris

Observation

The IAT was not presented with an orbital debris assessment for the X-37.

Recommendation

R13. The IAT recommends that the X-37 program conduct a formal assessment as required by NPD 8710.3 “NASA Policy for Limiting Orbital Debris Generation.”

5.8 Guidance, Navigation, & Control: Verification Simulation/Testing

Observation

NASA Goddard Space Flight Center (GSFC) Guidance, Navigation and Controls GPS Laboratory represents a word class capability in GPS operational simulation.

Recommendation

R14. The team recommends that the X-37 project consult with GSFC to leverage this in-house NASA capability to support X-37 space integrated GPS/inertial navigation system (SIGI) design and verification.

5.9 Inclusion of Safety in Integrated Risk Management Tracking System

Observation

The risk management process (identifying, tracking, monitoring, mitigating) currently employed by the X-37 program focuses primarily on cost, schedule, and technical performance risks but does not actively include consideration of safety risks as related to the public, government and contractor workforce, and high value equipment and facilities.

Recommendation

R15. As cost and schedule tradeoffs (risk tradeoffs) and decisions invariably impact safety in some manner, the team recommends that safety issues be incorporated into an integrated risk management tracking system.

5.10 Request for Third-Party Indemnification

Observation

At the time of this report, the Boeing request for third party indemnification addresses only the third phase of the flight test program, e.g., the orbital test flights. The first phase, the X-40A free-flight test series at Edwards Air Force Base in California, has been completed. The second phase consists of unpowered flight tests of the X-37 vehicle. If the unpowered flight tests are to be considered for indemnification it would require a decision sufficiently in advance of the tests to assure the proper completion of appropriate reviews and compilation of supporting documentation.

Recommendation

R16. The IAT recommends that Boeing and the X-37 Program management clarify the scope of the third-party indemnification request as soon as possible.

6.0 Conclusion

Knowledge derived from reviews, examination of process documentation, obtaining objective evidence of process implementation, establishing confidence in reliability and Ec analysis, and participation in flight/operational readiness review process will provide the basis for NASA AA/SMA endorsement decisions:

- Signature on flight or operational readiness documents (e.g. CoFR)

- Third-party indemnification endorsement/non-concurrence

While the X-37 program has many excellent safety, risk management, and assurance processes in place, the IAT cannot presently support a preliminary letter of endorsement for the X-37 program. Specific reservations include:

- the level of maturity and fidelity of the X-37 reliability analysis and methodology is inadequate and does not provide confidence that the program will satisfactorily meet the Ec range safety criteria.

- the NASA MSFC/SMA staffing is inadequate to provide ongoing verification and objective evidence that assurance processes are being effectively implemented.

Addressing the recommendations contained in section 5.0 represents a necessary first step in acquiring the NASA AA/SMA endorsement for either a third-party indemnification request or a certificate of flight readiness.

Appendix A: Safety & Mission Success Management Process