Research and Development
Of
Space Systems Distributed-Verification Approach
With Modular Management Process

Satoshi Nagano

31 January, 2008

Abstract

Having a solid verification program that ensures a “system is built right” plays a crucial role in both government and commercial space programs, since even the smallest error in a requirement, design/analysis, test, or inspection at every level of a system development, could cause a major system post-launch failure or costly finding of latent problems late in system’s development phase.

Since the dawn of space age that started with Soviet Union Sputnik in 1957 and U.S. Explorer in 1958, space systems development activities have experienced a series of maturing processes; however, it became evident that a system engineering-centric centralized-verification approach was mainly used by the U.S. industry throughout its history. Unfortunately, this traditional centralized-verification approach was found to be rather ineffective for minimizing/preventing such costly problems as finding a unit deficiency during a higher level system integration & test phase or in worst case the loss of space or launch vehicles after launch. The main reason for this was that thorough and detailed verification at each phase and at every level of system development was missing under the traditional centralized-verification approach because of the magnitude and complexity of general space systems that were acquired under perennial budget constraints.

This paper examined the space and launch vehicles post-launch failures data that have been collected by The Aerospace Corporation since 1960ies and found that almost all of the post-launch failures could have been prevented, if their problems had been discovered prior to the shipment of these vehicles to

their launch sites In particular, it was found that the majority of these vehicles could have been successful, if deficiencies were corrected during early phase (requirement and design phases), or lower system level (unit and subsystems) of their systems developments; Hence, the study further points out the weakness associated with the traditional centralized-verification approach and the need for improvement.

This paper presents a systematic approach for planning and executing verification of space systems based on a newly developed distributed-verification approach that corrects fundamental deficiencies associated with the traditional centralized-verification approach. This newly developed distributed-verification approach enforces a standardized modular-management process, which contains a set of six specific verification management processes, to be adopted at every level and phase of space system development activities.

The newly developed distributed-verification approach also tries to prevent infamous “Faster, Better, Cheaper” or “Total System Program Responsibility (TSPR)” philosophy, from being unintentionally adopted at each level of a space system development due to schedule and cost pressures.

This newly developed distributed-verification approach is now explained in a U.S. DoD best practice document and also included in a core standard of The Aerospace Corporation. It has also been adopted as a compliance document in some major U.S. space programs such as the next generation GPS Block III, and some national security space programs. It is also currently studied by U.S

government-industry working group under the direction of its senior executive committee for the purpose of upgrading it to a government standard.

Table of Contents

- List of Acronyms ----------7
- List of Tables ----------11
- List of Figures ----------12

1 Introduction ----------14

1.1 U.S. Space Systems Acquisition Activities Historical Background-------14

1.2 Objective and Organization of the Thesis ----------20

(1) Objective of the Thesis ----------20

(2) Organization of the Thesis----------21

2 Assessment of Current Space Systems Verification Approach ----------23

2.1 Current Space Systems Verification Approach ----------23

2.2 "Faster, Better, Cheaper" vs. the Traditional ----------30
Centralized-Verification Approach

2.3 Fundamental Deficiencies of the Traditional Systems ----------38
Centralized - Verification Approach

(1) The Traditional Centralized-Verification Approach Deficiency 1:-----39
Lack of Well Orchestrated End-to-End Systems Verification
Program and Plan

(2) The Traditional Centralized-Verification Approach Deficiency 2: ----40
Lack of Documented and Traceable Proof of End-to-End Systems
Verification

(3) The Traditional Centralized-Verification Approach Deficiency 3: ----42
Lack of Oversight for Low-level Systems Verification

(4) The Traditional Centralized-Verification Approach Deficiency 4:-----44
Lack of End-to-End Systems Verification Risk Management

3 Examination of Past Space and Launch Vehicles Post-launch Failures-------46

3.1 Causes of Post-Launch Failures ----------48

(1) Development Phases ----------48

Table of Contents (Continued)

(2) Systems Development Level ----------51

(3) Technical Disciplines ----------53

3.2 Past Space and Launch Vehicles Post-Launch Failures ----------55
Assessment Summary

4 Newly Developed Verification Approach ----------57

4.1 Distributed-verification approach with Modular Management Process ---57

4.2 Synthesis of the Newly Developed Distributed-Verification Approach ----58

(1) Standardized Modular Verification Management Process----------58

(2) General Methods for Correcting Fundamental Deficiencies ----------59
Associated with the Traditional Centralized-Verification Approach
Using Newly Developed Distributed-Verification Approach

(3) Application of Distributed-Verification Approach with Modular -------62
Management Process to Each Level and Phase of System
Development

4.3 Establishment of A Distributed-Verification Program Management --------65
Organization

(1) Work Breakdown Structure Based Working Group (WBS-WG) -------67

(2) Verification Management Board (VMB) ----------70

(3) Independent Readiness Review Team (IRRT) ----------70

(4) Failure Review Board (FRB, Parts, Materials, and Processes --------72
Control Board (PMPCB), and Quality Assurance (QA) and Other
review boards such as Engineering Change Review Board (ECRB)

(5) Cost Impacts of Establishing the Newly Developed ----------73
Distributed-Verification Approach

4.4 The Newly Developed Distributed-Verification Program Plan ----------75
Using Standardized Modular Verification Management Process

(1) VM-Process 1: Requirement Flow-Down and Verification ----------75
Cross-Reference Matrix (VCRM) Process

Table of Contents (Continued)

(2) VM-Process 2: Verification by analysis, test, demonstration ----------77
and inspection process

(3) VM-Process 3: Integration and Test (I&T) Process ----------79

(4) VM-Process 4: Individual Specification Dedicated ----------80
Verification Ledger (ISDVL) Process

(5) VM-Process 5: Sell-Off/Consent-to-ship process ----------83

(6) VM-Process 6: Verification-Related Risk Management Process -----84

4.5 Documentation Requirements ----------85

4.6 Test Case Results ----------88

4.7 Verification Management Approach Comparisons between Space and---92
Aircraft or Automotive Systems (Suggested Future Research Project)

5 Conclusion ----------95

6 Acknowledgements ----------98

7 References ----------99

List of Acronyms

A, T, I, D	Analysis, Test, Inspection, Demonstration
AEHF	Advanced Extremely High Frequency
AFSAB	Air Force Scientific Advisory Board
ATP	Authority to Proceed
ACDS	Attitude Control and Determination Subsystem
CDR	Critical Design Review
DHS	Data Handling Subsystem
DID	Data Item Description
DoD	Department of Defense
DRC	Design Reference Case
DSB	Defense Science Board
EIA	Electronic Industries Alliance
EM	Engineering Module
EMC	Electromagnetic Compatibility
EPS	Electrical Power Subsystem
ESA	European Space Agency
EXT-IF	External Interface
FMEA	Failure Mode Effect Analysis
FRB	Failure Review Board
FRR	Flight Readiness Review
GAO	General Accounting Office
GPS	Global Positioning System

GS	Ground System
I&T	Integration and Test
IF	Interface
INCOSE	International Council on Systems Engineering
IRR	Independent Readiness Review
IRRT	Independent Readiness Review Team
ISDVL	Individual Specification Dedicated-Verification Ledger
LRR	Launch Readiness Review
LV	Launch Vehicle
MCR	Mission Concept Review
MDR	Mission Definition Review
MIL-Std	Military Standard
MRR	Manufacturing Readiness Review
MSFC	Marshall Space Flight Center
NASA	National Aeronautics and Space Administration
NPR	NASA Procedural Requirements
NRO	National reconnaissance Office
ORR	Operations Readiness Review
PCU	Power Conditioning Unit
PDR	Preliminary Design Review
PL	Payload
PMPCB	Parts, Materials, and Processes Control Board
PRR	Production Readiness Review

QA	Quality Assurance
RFP	Request for Proposal
S/A	Solar Array
SAR	System Acceptance Review
SBIRS	Space-Based Infrared Systems
S/C	Spacecraft
SE	Systems Engineering
SDR	System Definition Review
SIR	System Integration Review
SMC	Space and Missile Systems Center
SMSR	Safety and Mission Success Review
SRR	System Requirement Review
SS	Space System
SV	Space Vehicle
SV/LV	Space Vehicle/Launch Vehicle
T&C	Telemetry and Command
TLYF	Test Like You Fly
TOR	Technical Operating Report
TRD	Test Requirement Document
TRR	Test Readiness Review
TSPR	Total System Program Responsibility
U.S.	United State
V&V	Verification and Validation

VCRM	Verification Cross-Reference Matrix
VM	Verification Management
VMB	Verification Management Board
WBS	Work Breakdown Structure
WBS-WG	Work Breakdown Structure based Working Group
WG	Working Group

List of Tables

Table 1 Space Flight Program/Project Reviews ----------37
(Table from Reference 15)

Table2. An Example of SV Unit-Level ISDVL----------83

Table 3 Documentation Requirement ----------87

Table 3(a) Higher System Level Verification Program-Related Documents and Review Cycles

Table 3(b) Lower System Level Verification Program-Related Documents Review Cycles

List of Figures

Figure 1 Comparison of 450 U.S. Space Vehicles Success Rate: ----------16
Traditional vs. Higher Risk Acquisition Practices: “Faster, Better, Cheaper, or TSPR” (Graph from Reference 3)

Figure 2 U.S. Space Assets Lost During the 1990s in Dollars (Graph from------17
Reference 3)

Figure 3 A Typical Space System (Example)----------30

Figure 3(a) A Typical Space System That Consists of Several Elements

Figure 3(b) A typical Space Vehicle Element That Consists of Several Subelements

Figure 3(c) A Typical SV Subsystem That Consists of Several Units and Assemblies

Figure 4 Verification Management Approach Comparison: ----------34
The Traditional Centralized vs. “Faster, Better, Cheaper” or “TSPR”

Figure 4(a) Verification Management Approach During “Faster, Better, Cheaper/TSPR” Era

Figure 4(b) The Traditional Centralized-Verification Management Approach

Figure 5 Space Program Agencies vs. Post Launch SVs/LVs ----------47
Losses (1964-2003)

Figure 5(a) SV Failure Causes vs. Development Phase

Figure 5(b) LV Failure Causes vs. Development Phase

Figure 6 Deficiencies at Different Development Phase That ----------50
Caused the Loss of 102 SVs and 29LVs from1964 to 2003

Figure 6(a) SV Failure Causes vs. System Level

Figure 6(b) LV Failure Causes vs. System Level

Figure 7 Deficiencies at Different Level of System Development ----------53
That Caused the Loss of 102 SVs and 29LVs from1964 to 2003

Figure 7(a) SV Failure Causes vs. Technical Disciplines

Figure 7(b) LV Failure Causes vs. Technical Disciplines

Figure 8 Deficiencies at Different Technical Disciplines That ----------54
Caused the Loss of 102 SVs and 29LVs from1964 to 2003

Figure 9 Application of the Newly Developed Distributed-Verification ---------- 65
Program with Modular Management Process to Each Level
and Phase of System Development

Figure 9 (a) Modular Verification Management Process and Function

Figure 9 (b) Application of the Newly Developed Distributed-Verification
Approach to Each System Level

Figure 9 (c) Application of the Newly Developed Distributed-Verification
Approach to Each Development Phase

Figure 10 Example of the Newly Developed Distributed-Verification ---------- 67
Approach Managed by VMB and WBS-WGs

Figure 11 Example Product-Based WBS for an Aircraft System ---------- 94
Subsystems: Navigation Subsystem

I Introduction

1.1 U.S. Space Systems Acquisition Activities Historical Background

A brief summary of the history associated with general U.S. space systems acquisition activities is explained here as background information for delineating the thesis entitled “Research and development of space systems distributed-verification approach with modular management process”.

Since the first launch of Soviet Union’s Sputnik in 1957, space systems reliability in general has been steadily increasing in large part due to improvements in rocket and spacecraft technologies, components, and designs, modeling and simulations, and test capabilities as well as due to the fact that the space and launch environments have been characterized with greater accuracy. According to a space launch vehicle reliability study (Reference 1), the U.S., for example, has been steadily improving their launch success rates on every decade since the successful launch of Explorer in 1958 as follows:

(a) Launch success rate, 1957 -1966: 76.5% (328 out of 429 launch success)

(b) Launch success rate, 1967 -1976: 91.8% (326 out of 355 launch success)

(c) Launch success rate, 1977 -1986: 93.4% (185 out of 198 launch success)

(d) Launch success rate, 1987 -1996: 93.9% (215 out of 229 launch success)

(e) Launch success rate, 1997 - 2004: 95.7% (202 out of 211 launch)

Regardless of this overall success exemplified by these steadily increasing launch successful rates, the U.S. space industry in general is still currently experiencing problems of cost overrun, schedule delays or losing expensive space or launch vehicles in the worst case.

One of the main reasons for these current problems is that the U.S. government acquisition agencies, both DoD and NASA, are still suffering from the infamous “Faster, Better, Cheaper” or “Total System Program Responsibility (TSPR)” policy that was established by NASA in 1992 and by Air Force in 1995, respectively.

Although the NASA’s “Faster, Better, Cheaper” policy was never been officially defined, the intent of the policy was to promote all the NASA space systems to be acquired in shorter development time with less cost while achieving higher capabilities and reliability. On the other hand, the Air Force’s TSPR was more specific in that they effectively ended the use of military specifications and standards despite arguments that these standards represented best practices compiled through decades of costly and arduous trial and error. In effect, after the 1995 Air Force edict, commercial best practices were deemed suitable alternatives, although the effectiveness of these practices had not been clearly understood because each contractor had different set of standards and practices that were not necessarily proven by wide use in the space industry.

Unfortunately, these policies significantly impacted the reliability of the U.S. government‘s space systems because of their strong dependency on their contractors to develop their systems without government oversight. These policies, in turn, created an undesirable culture that encouraged space industry to set priority on the cost saving ahead of ensuring mission success.

Figure 1 shows the results of a study performed by The Aerospace Corporation that indicates that those developed using traditional acquisition practices showed a

consistently higher success rate in the first year of operations than the vehicles developed using higher-risk acquisition approaches, “Faster, Better, Cheaper” or TSPR. This conclusion was made based on the examination of a sample of more than 450 vehicles manufactured in the United States (Reference 3).

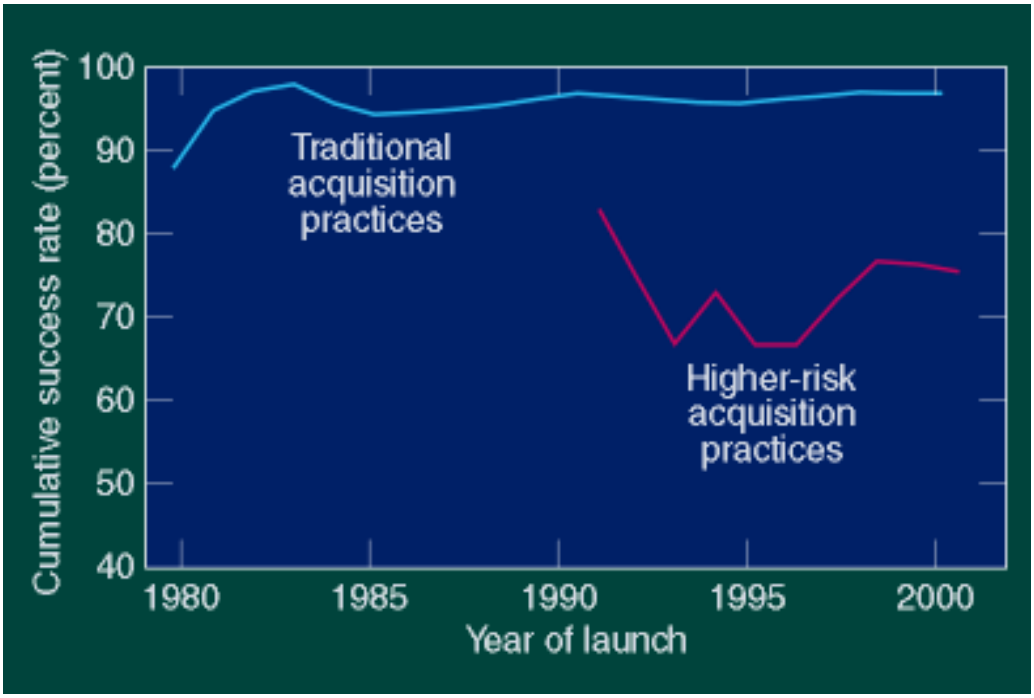


Figure 1 Comparison of 450 U.S. Space Vehicles Success Rate: Traditional vs. Higher Risk Acquisition Practices: “Faster, Better, Cheaper, or TSPR” (Graph from Reference 3)

The same study further expressed that “Data analyzed pointed to a number of systems engineering deficiencies that resulted in numerous late-build-cycle problems, highlighted by the large increase in design flaws (detected in system-level testing) since 1995. During this period, NASA experienced such catastrophic failures as Space Shuttle Colombia Mishaps (2003) while DoD experienced two successive failures of heavy-lifting launch vehicles, TITAN IV (1998 and 1999)”.

Figure 2 shows the value in dollars of U.S. space assets lost during the 1990s due to adopting these high risk acquisition approaches (Reference 3).

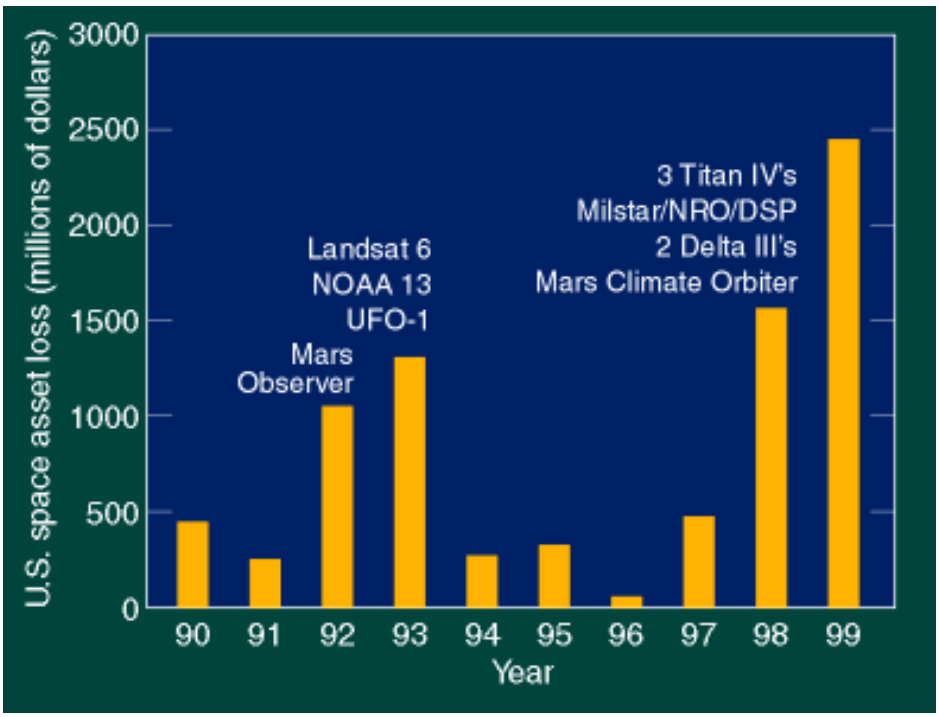


Figure 2 U.S. Space Assets Lost During the 1990s in Dollars (Graph from Reference 3)

Because of these costly problems, the U.S. space community, starting around year 2005, began to implement the old way of doing business in an attempt to correct the infamous “Faster, Better, Cheaper” or TSPR policy. In fact, these changes were directed based on the finding of the 2003 Defense Science Board (DSB)/ Air Force Scientific Advisory Board (AFSAB) task force and the General Accounting Office (GAO) that reported critical of the then on-going “Faster, Better, Cheaper” space-acquisition approach (Reference 4).

These reports expressed concerns about system-cost overruns and schedule slippages, especially in two vital space systems: the advanced extremely high frequency (AEHF) military-communication program and the space-based infrared systems (SBIRS) early-warning satellite program. Combined, both programs are more than $8 billion over budget. Both reports cited several underlying factors for these programmatic issues and provided viable solutions; however, neither confronts the fundamental issue, which mandates a revamped space-acquisition process. A list of key findings identified in these report were:

a. Cost has replaced mission success as the primary driver in managing space development programs, from initial formulation through execution.
b. Unrealistic estimates lead to unrealistic budgets and un-executable programs. The TSPR space acquisition system is strongly biased to produce unrealistically low cost estimates throughout the process.
c. Undisciplined definition and uncontrolled growth in system requirements increase cost and schedule delays.
d. Government capabilities to lead and manage the space acquisition process have seriously eroded.
e. Industry has failed to implement proven practices on some programs. Successful development of space programs requires strong leadership and rigorous management processes both in industry and in government.

Because of these findings, DoD space community immediately tried to implement the old way of doing business by bringing back to enforce a set of government

standards such as test requirements, MIL-Std-1540 (Reference 5) and software related requirements, MIL-Std-1833 (Reference 6).

On the other hand, NASA has embarked on new programs such as Ultra-Reliability Project (Reference 7) and Technical Excellence Program (Reference 24) that are designed to improve the reliability of NASA systems and help to achieve sound engineering in all aspects of NASA projects. The goal for the ultra-reliability program, for example, is to ultimately improve the systems by an order of magnitude. The approach outlined in this presentation involves five steps:

(i) Divide NASA systems into seven sectors.

(ii) Establish sector champions and representatives from each NASA center.

(iii) Develop a challenge list for each sector using a team of NASA experts in each area with the sector champion facilitating the effort.

(iv) Develop mitigation strategies for each of the sectors' challenge lists and rank their importance by holding a workshop with area experts from government (NASA and non-NASA), universities and industry.

(v) Develop a set of tasks for each sector in order of importance for improving the reliability of NASA systems. Several NASA-wide workshops have been held, identifying issues for reliability improvement and providing mitigation strategies for these issues.

In any regard, the U.S. space industry is currently still experiencing costly problems and schedule delays even after implementing the old traditional acquisition approach and other measures to improve the quality and reliability of space systems by both DoD and NASA.

1.2. Objective and Organization of the Thesis

(1) Objectives of the Thesis

(a) The first objective of this thesis is to examine the past and present U.S. space systems verification management approaches in an attempt to identify if any fundamental deficiencies exist such that they may be the sources for the perennial cost overruns, schedule delays, and post-launch mishaps. The reason for focusing on verification is because it plays a crucial role in ensuring “system is built right” in developing space systems. As a part of this objective, the verification approach differences between those used during the “Faster, Better, Cheaper” or TSPR and the traditional space systems acquisition policies are examined.

(b) The second objective of this thesis is to examine the past space vehicles and launch vehicles post-launch failures to understand exactly what went wrong in “system is built right” activities in an attempt to further enforce the argument that there exist some fundamental deficiencies in the traditional space systems verification approach even before the “Faster, Better, Cheaper” or TSPR era.

(c) The third objective of this thesis is to develop a new verification management concept that corrects the traditional approaches’ deficiencies identified by this research

(d) The fourth objective is to explain the results of a test case that used the new verification management concept.

(2) Organization of the Thesis

The thesis is organized as follows:

(a) Explain that the U.S. space industry is presently trying to recover from the infamous “Faster, Better, Cheaper” or “Total System Program Responsibility (TSPR)” policy that were created by NASA and DoD, respectively around 1992 and halted in 2003.

(b) Explain that the U.S. space industry in general is trying to go back to utilize a traditional acquisition approach including that relating to verification management that was utilized prior to the “Faster, Better, Cheaper” or TSPR era; however, the traditional approach is a centralized-approach in which verification management is focused on mission requirements and associated top-level systems and is conducted primarily by system engineering organizations.

(c) Explain that there are four fundamental deficiencies associated with the traditional centralized-verification approach.

(d) Enforce the arguments that the traditional centralized-verification approach had these deficiencies based on the detailed examination of over 140 space and launch vehicles post launch failures that happened between1963 and 2003.

(e) Present a new concept, distributed-verification approach with modular management process, which utilizes standardized modular process for managing verification of every system level throughout the system development activities. Also explain why/how the new concept corrects

the fundamental deficiencies associated with the traditional centralized-verification approach.

(f) Explain this new concept, distributed-verification approach with modular management process, with regard to its organizational structure, details of modular management process and documentation requirements.

(g) Explain the results of a test case in which this new concept was implemented in a major U.S. national space program on a voluntary basis.

(h) Briefly suggest future research projects that explore the differences in verification management among space, aircraft, and automotive systems since they are vastly different systems in terms of complexity, development & production approaches, operations, and maintenance.

(i) Explain conclusions of this research and development work.

2 Assessment of Current Space Systems Verification Approach

2.1 The Traditional Centralized-Verification Approach

As explained in section 1, Introduction, both DoD and NASA started to implement numerous measures in their attempts to correct the problems associated with the “Faster, Better, Cheaper” or “TSPR” policy. These corrective measures included establishments of new government policies that tried to change the government approach to manage their contractors in order to improve mission assurance of their acquiring systems.

In fact, the government started to take more responsibility for managing their space systems contractors; however, they could only afford to monitor the progress of top-level space systems but not the low-level systems. The major reasons for them to take this approach was due to (a) they were operating under perennial budget shortfalls, (b) space systems were increasingly becoming larger and more complex, and (c) they believed that the lower-levels systems were mostly heritage systems that used well proven designs and mature technologies that did not require extensive government oversight.

In any regard, under these top-level systems focused approach, management of the contractors including those relating to verification was primarily conducted by systems engineering organization.

One can, therefore, describe this particular verification approach as the traditional centralized-verification approach.

In any case, systems engineering organization managed their system verification activities utilizing several space systems engineering standards or

handbooks as their guide. Examples of these systems engineering standards and handbooks were MIL-Std-499A (Reference 8), NASA System Engineering Handbook (Reference 9), INCOSE Systems Engineering Handbook, Version 2.0 (Reference 10), or EIA-632 (Reference11). These documents were selected as government compliance documents either by itself or in combination with other standards such as aforementioned software military standard.

Unfortunately, both DoD and NASA, by this time, were used to focus on the utilizations and explorations of space using large scale systems instead of engaging in simply developing rocket and spacecraft technologies that had been considered as fully matured and ready to be procured on demand. Namely, the U.S. space utilizations and explorations efforts produced major space systems such as Apollo (1969), Voyager (1977), GPS (1978), Space Shuttle (1982) and International Space Station (1995) since the successful launch of the Explorer spacecraft in 1958. In addition, both DoD and NASA developed other large scale space systems such as weather satellite systems, surveillance, and communication satellite systems. These large scale space systems were accomplished by space system architectures with multiple space vehicles deployed on one or multiple orbits and with several ground stations. Again, these large scale space systems became possible as the industry gained sufficient experience and knowledge to build space vehicles or launch vehicles on their own. They possessed ready to use designs for many parts of these vehicles.

Consequently, most of the current major government space programs do not specify what types of spacecraft bus/payload or launch vehicle to be used in their

Request for Proposal (RFP) for acquiring their space systems. They rather rely on the industry to propose and develop space and launch vehicles based on their own experience and knowledge. These are the reasons for most government space systems acquisition agencies still focus their verification related oversight functions on top-level systems developments and associated mission requirements while relying on their contractors to ensure the successful development and delivery of low-level systems.

Placing mission requirements satisfaction on a list of their top priorities is imperative for the government space systems acquisition agencies, since these requirements are the very reason for them to be able to receive DoD or NASA fund to procure space systems.

These mission requirements are normally established by government users' community and space systems planning agencies, both considered as their missions stakeholders. These mission requirements are normally finalized after a series of government internal requirement development processes that generally take several years of development cycles to complete. These mission requirements are normally recaptured in a contractor's overall space system specification.

Incidentally, mission requirements usually specify such items as space systems constellation size (i.e., selected orbits and number of satellites per a given orbit), ground systems locations, sensor's detection capabilities (such as optical sensor's sensitivity to different light wavelengths), pointing accuracy, frequency band/band

width for communication satellites, mean mission duration/design life, and health/fault management, systems operations, etc.

As explained above, once the government selects a contractor to develop their systems, they manage their contractors develop and deliver their systems mainly based on a set of systems engineering processes specified in the aforementioned space systems standards or handbooks.

These systems engineering processes address those items such as schedule & cost management, risk management, configuration management, design review planning, verification and validation, quality assurance, etc. These systems engineering processes are normally managed by government's and their contractor's systems engineering groups, i.e., these systems engineering processes are owned and managed by these systems engineering groups and not by the product groups who actually design and develop hardware and software systems.

It, therefore, is not uncommon that contractually required deliverable documentations and reviews associated with these systems engineering processes are mostly relating to the top-level systems such as the overall space system, space vehicle, launch vehicle, and ground system, but not relating to the low-level systems.

As such, these space programs in general depend on contractors to manage and ensure that lower level systems (such as subelements, subsystems, units, and interfaces) are properly developed and delivered, i.e., government reviews of documentations for these low-level systems, in this case, are in general arranged

with the courtesy of their contractors. Another reason for the government tries to depend on their contractors to manage low-level systems development is budget constraints. All national security and science exploration space programs are constantly facing budget constraints exacerbated by competition from pressing operational needs such as programs for combating terrorism, and national social programs. Therefore, each space program, even if it is imperative to national security or science exploration purposes, must be managed in a very cost effective fashion to ensure its mission success.

Incidentally, top-level systems here generally are referred to “system” and “element” level and low-level systems indicate “sub-element”, “subsystem” and unit” level as illustrated in Figure 3 (a). In addition, Figure 3 (a), (b), and (c) show an example of a typical space system to illustrate that it requires multi-levels of system development efforts to develop a large scale space system. In refereeing to Figure 3, the following definitions are provided:

(a) Definition of space system levels

(i) Unit level: A unit is a electronic box that contains hardware/software to perform specific functions such as power conditioning, battery charge/discharge control, power distribution, etc.

(ii) Subsystem level: A subsystem contains several units to perform specific subsystem level functions such as those relating to electrical power, communication, attitude control and determination.

(iii) Sub-element level: A sub-element consists of several subsystems. It normally is a spacecraft bus, or payload that performs specific space mission such as communication, earth observation, etc

(iv) Element level: An element is normally a space vehicle, launch vehicle or ground system

(v) System level: A system level consists of several elements that perform the overall space missions such as sensing/collecting data, managing these data, and disseminating these data to users. Also space system level involves the command and control of deployed space systems.

(b) Definition of space system development phase

Once customer issues a Request for Proposal (RFP) after concluding space system architecture studies and having developed associated mission requirements, the project awarded contractor must in general go through the following phases at every level of their systems development:

(i) Specification and requirement development phase

(ii) Design and analysis phase

(iii) Manufacturing phase

(iv) Integration and test & evaluation phase

(v) Sell-Off/Consent-to-Ship phase

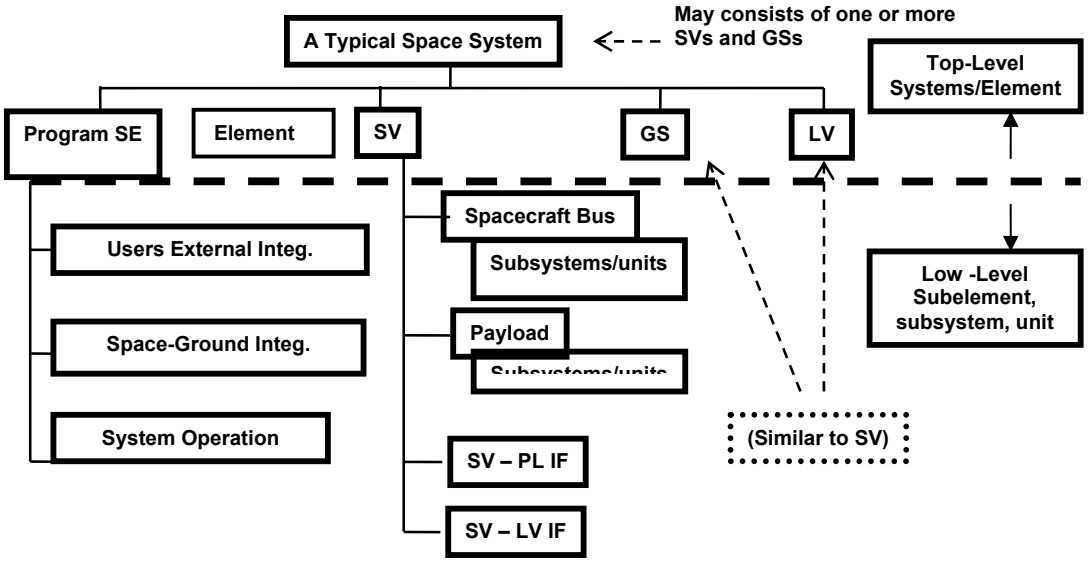


Figure 3(a) A Typical Space System That Consists of Several Elements

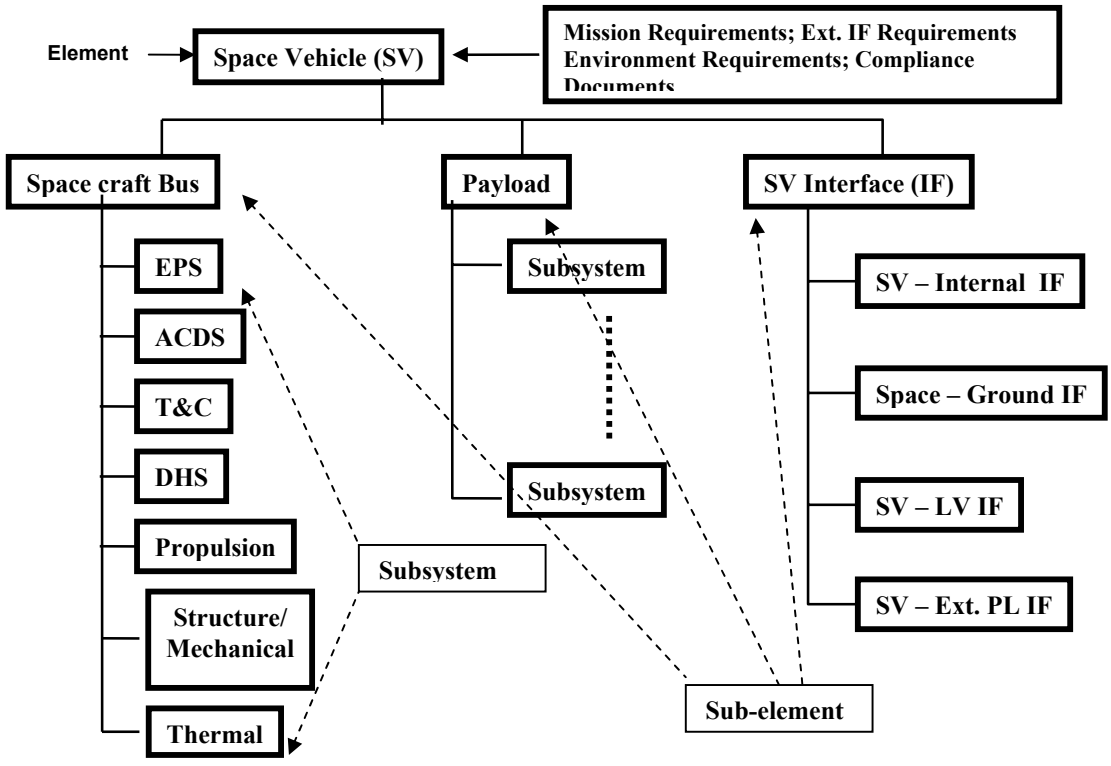


Figure 3(b) A typical Space Vehicle Element That Consists of Several Subelements

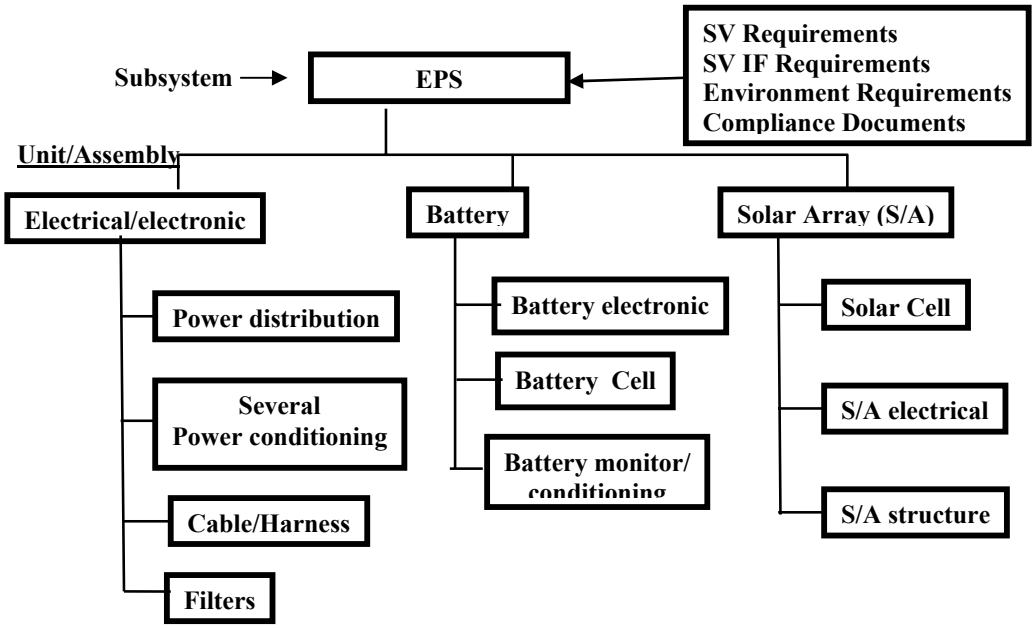


Figure 3(c) A Typical SV Subsystem That Consists of Several Units and Assemblies

Figure 3 A Typical Space System (Example)

2.2 "Faster, Better, Cheaper" vs. the Traditional Centralized-Verification Approach

As explained in Section 1, Introduction, both DoD and NASA immediately tried to implement the old way of doing business in order to correct problems that were found during the "Faster, Better, Cheaper " (NASA) or TSPR(DoD) era.

Incidentally, there is no document that delineates differences between "Faster, Better, and Cheaper" or "TSPR" and traditional way of doing business, since exact definition of the former approach terms are not clear. In fact, U.S. Inspector General's audit report that was sent to NASA in March, 2001 after several NASA space mission failures including the $125 million Mars Climate Orbiter in 1999, recommended NASA to develop written policies and guidelines to define the

“Faster, Better, Cheaper” policy so that they could improve their management of their programs (Reference 12).

Regardless, it appears that the goal of this infamous NASA policy was to increase the number of missions and their scientific results while reducing the development cost. Under this approach, NASA moved their works to private industry and minimized government oversight. NASA also reduced NASA's infrastructure to the point that the agency's role shifted from mainly technical support to contract administration.

This “Faster, Better, Cheaper” policy that had started in 1992 was effectively terminated by U.S. congress after the 2003 Space Shuttle Colombia’s disaster. (Reference 13)

One of the main reasons that NASA established the “Faster, Better, Cheaper” policy was to reduce the cost. For example, one of the successful projects under this policy was MARS Pathfinder that cost $270 million, a fraction of the budgets for NASA's more typical missions in years past, such as the Galileo spacecraft at Jupiter and the Cassini spacecraft which frequently climbed higher than $1 billion per mission (Reference 14).

As explained earlier, one of the corrective measures for going back to the old ways of doing business was to focus on managing the acquisition of space systems using a set of government standards and guidelines. The other approach was to revive the government technical oversight of the contractors’ work; however, this oversight function is still limited to the top-level systems only as explained earlier.

Figure 4(a) and (b) attempt to illustrate what it means by “Faster, Better, Cheaper” or TSPR” vs. the traditional centralized-approach in terms of managing space systems verification, respectively.

It can be safely explained that the generally adopted verification management by the space industry during the “Faster, Better, Cheaper” or “TSPR” era employed almost no government oversight for the verification of the entire system, as shown in Figure 4(a). On the other hand, the traditional centralized-verification approach could afford the government oversight only for the top-level systems verification as shown in Figure 4(b).

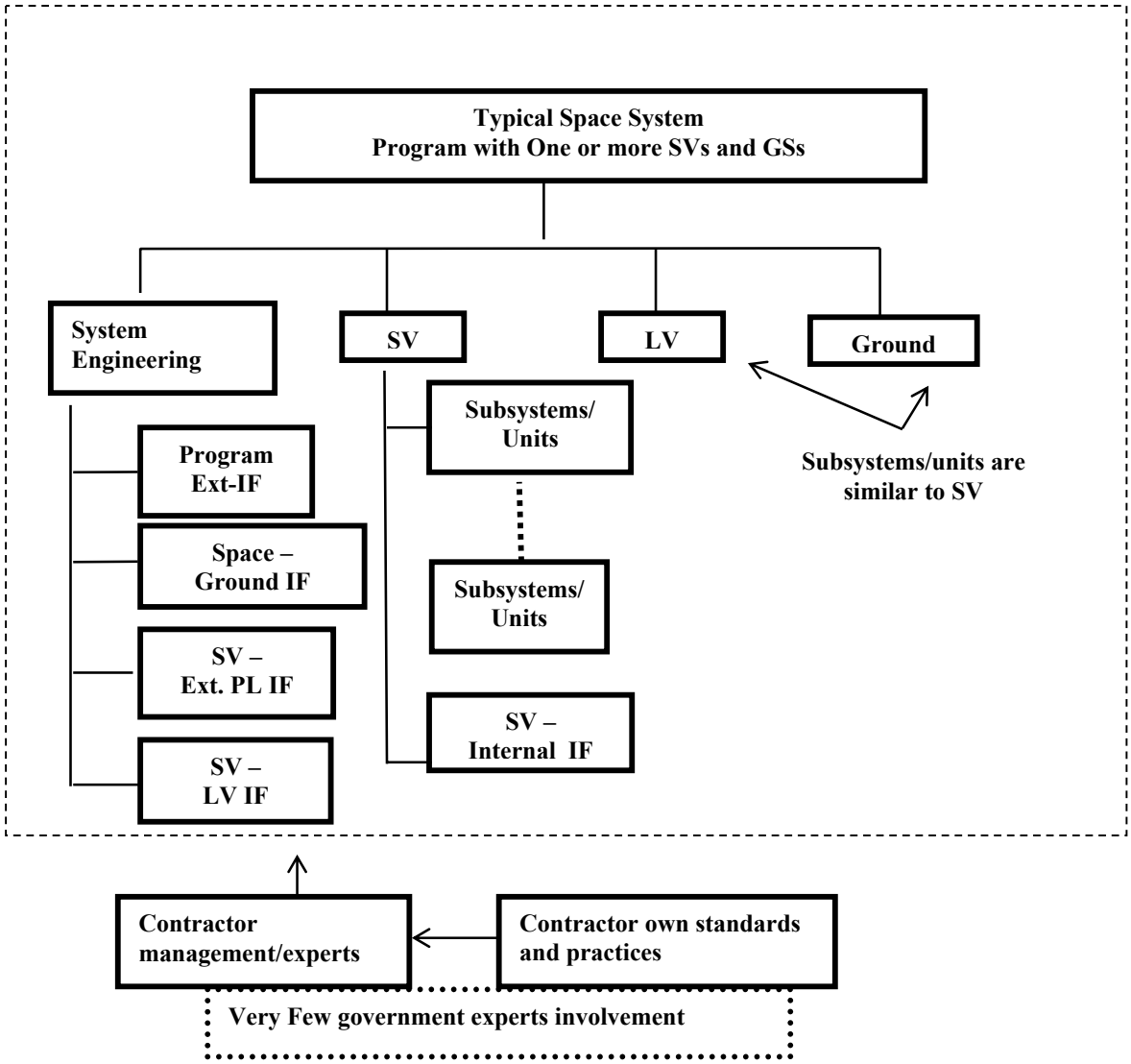


Figure 4(a) Verification Management Approach During "Faster, Better, Cheaper/TSPR" Era

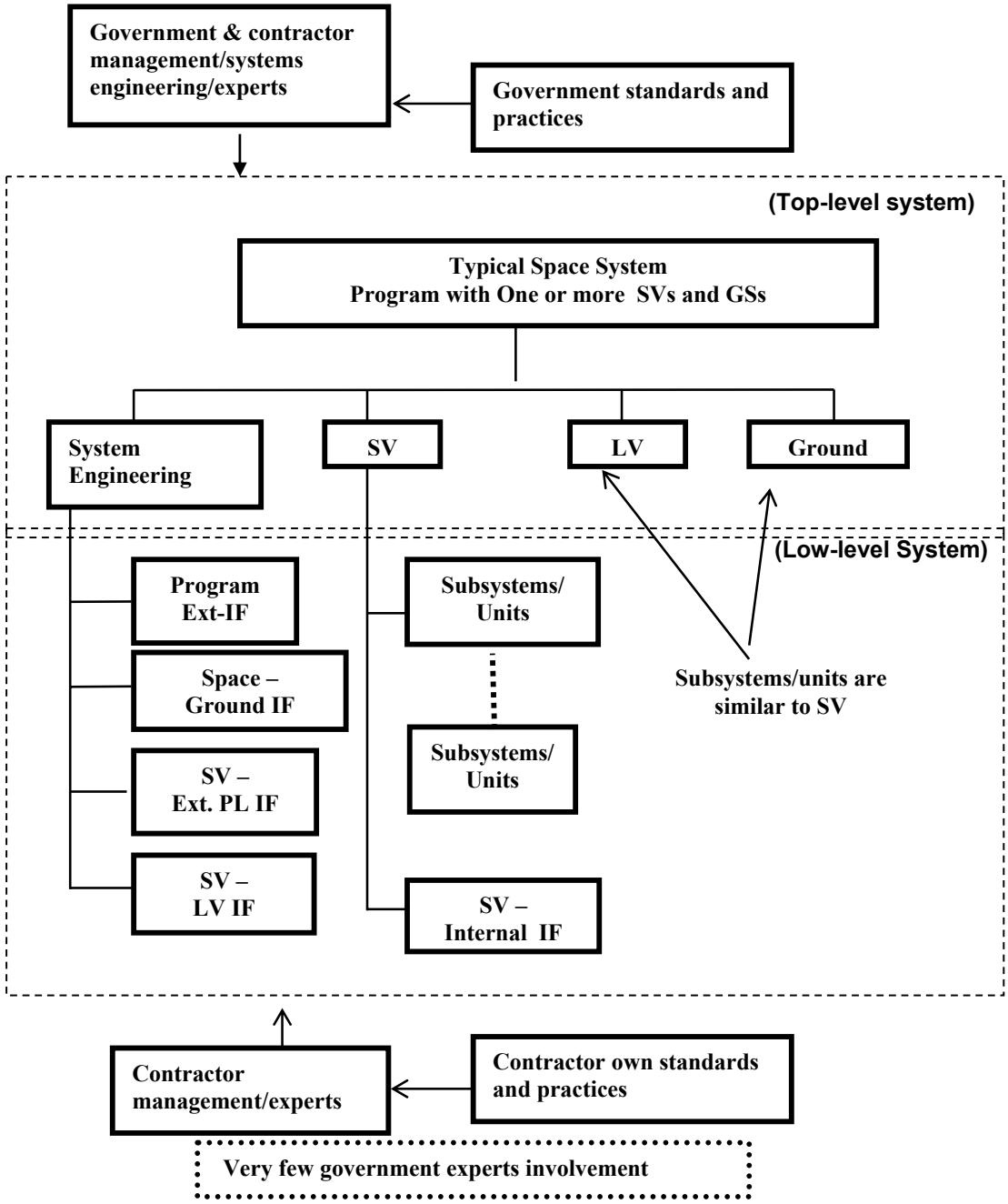


Figure 4(b) The Traditional Centralized-Verification Management Approach

Figure 4 Verification Management Approach Comparison: The Traditional Centralized vs. “Faster, Better, Cheaper” or “TSPR”

In space system acquisitions for government or commercial applications, verification, “system is built right” plays a very significant role, since it is almost impossible to repair and recover failed space systems once they are launched into space, as explained in Section 1.2. (1), Objectives of the Thesis. Even if a problem is found before launch, any repairs or replacements of hardware in the late development phase will seriously impact the cost and schedule of a program because of the complexity and intricacy associated with building a space system. Hence, it is very critical to ensure that thorough verification activities are planned and executed at every level and phase of a system development. Regardless, both DoD and NASA still utilize systems engineering-centric and top-level systems focused centralized-verification approach to ensure that their “systems are built right” as explained in section 2.1. In fact, most of the major programs do not require development of verification plan for low-level systems but only for verification plans for the overall top-level systems.

As explained above, developing a space system requires several layers of system level development activities and each one of them needs to go through a series of development phases. In this process, verification activities must ensure that the developed systems satisfy, for example, several hundred missions’ related requirements (i.e., customer requirements) and several thousands of contractor derived/functional requirements with proper designs/analyses, tests, and inspections from low-level to top level systems.

NASA recently published NASA Procedural Requirements (NPR) that are compliance document for managing all of their current and future flight programs

and projects that include spacecrafts, launch vehicles, and instruments developed for space flight programs and projects, etc. (Reference 15). Table 1 summarizes a list of reviews and the nature of each review that must be officially conducted for all NASA flight programs/projects according to this compliance document.

According to Table 1, system requirements (that are equivalent to mission requirements) and verification & validation (V&V) plan reviews, for example, will be reviewed as a part of the System Requirements Review (SRR) and System Integration Review ((SIR), respectively. In addition, all of these reviews in Table 1 are accomplished in accordance with systems engineering processes defined in the latest NASA systems engineering related compliance document (Reference 16). Once again, these requirements, design, or verification related reviews are focused on top-level systems and systems engineering processes conducted by systems engineering groups; as such, one can conclude space systems verification approach even with these latest NASA compliance documents can be still classified as the traditional centralized-verification approach.

Incidentally, a new INCOSE Systems Engineering Handbook has been published (Reference 17); however, the guidelines for system verification are still described based on a systems engineering-centric and centralized approach.

Review	Description
Mission Concept Review (MCR)	The MCR affirms the mission need and examines the proposed mission's objectives and the concept for meeting those objectives. Key technologies are identified and assessed. It is an internal review that usually occurs at the cognizant system development organization. (The SRB may not have been formed.) ROM budget and schedules are presented.
System Requirements Review (SRR)	The SRR examines the functional and performance requirements defined for the system and the preliminary Program or Project Plan and ensures that the requirements and the selected concept will satisfy the mission.
Mission Definition Review (MDR) or System Definition Review (SDR)/ Preliminary Non-Advocate Review (PNAR)	The MDR (or SDR) examines the proposed requirements, the mission/system architecture, and the flow down to all functional elements of the system. The PNAR is conducted as part of this review to provide Agency management with an independent assessment of the readiness of the project to proceed to Phase B.
Preliminary Design Review (PDR)/ Non-Advocate Review (NAR)	The PDR demonstrates that the preliminary design meets all system requirements with acceptable risk and within the cost and schedule constraints and establishes the basis for proceeding with detailed design. It shows that the correct design option has been selected, interfaces have been identified, and verification methods have been described. Full baseline cost and schedules, as well as risk assessments, management systems, and metrics are presented. The NAR is conducted as part of this review to provide Agency management with an independent assessment of the readiness of the project to proceed to implementation.
Critical Design Review (CDR)	The CDR demonstrates that the maturity of the design is appropriate to support proceeding with full scale fabrication, assembly, integration, and test, and that the technical effort is on track to complete the flight and ground system development and mission operations in order to meet mission performance requirements within the identified cost and schedule constraints. Progress against management plans, budget, and schedule, as well as risk assessments are presented.
Production Readiness Review (PRR)	The PRR is held for projects developing or acquiring multiple similar or identical flight and/or ground support systems. The purpose of the PRR is to determine the readiness of the system developer(s) to efficiently produce (build, integrate, test, and launch) the required number of systems. The PRR also evaluates how well the production plans address the system's operational support requirements.
System Integration Review (SIR)	The SIR evaluates the readiness of the project to start flight system assembly, test, and launch operations. V&V plans, integration plans, and test plans are reviewed. Test articles (hardware/software), test facilities, support personnel, and test procedures are ready for testing and data acquisition, reduction, and control.
System Acceptance Review (SAR)	The SAR verifies the completeness of the specific end item with respect to the expected maturity level and to assess compliance to stakeholder expectations. The SAR examines the system, its end items and documentation, and test data and analyses that support verification. It also ensures that the system has sufficient technical maturity to authorize its shipment to the designated operational facility or launch site.
Operations Readiness Review (ORR)	The ORR examines the actual system characteristics and the procedures used in the system or product's operation and ensures that all system and support (flight and ground) hardware, software, personnel, and procedures are ready for operations and that user documentation accurately reflects the deployed state of the system.
Safety and Mission Success Review (SMSR)	SMSRs are conducted prior to launch or other mission-critical events/activities by the Chief SMA Officer and Chief Engineer (or senior Center-based SMA and engineering officials) to prepare for SMA and engineering participation in critical program/project reviews/decision forums. The SMA lead and lead PCE are the focal points for planning, coordinating, and providing the program/project elements of these reviews.
Flight Readiness Review (FRR)	The FRR examines tests, demonstrations, analyses, and audits that determine the system's readiness for a safe and successful flight/launch and for subsequent flight operations. It also ensures that all flight and ground hardware, software, personnel, and procedures are operationally ready.
Launch Readiness Review (LRR) (Launch Vehicle)	Final review prior to actual launch in order to verify that Launch System and Spacecraft/Payloads are ready for launch.

Table 1 Space Flight Program/Project Reviews (Table from Reference 15)

2.3 Fundamental Deficiencies of the Traditional Centralized-Verification Approach

It is understandable that main reasons for government agencies to adopt the aforementioned traditional centralized-verification approach are (a) they, under constant budget constraints, forced to focus on managing the acquisition of only top-level systems of space systems that are increasingly becoming more complex. A major space system, for example, consists of one or more space vehicles each of which has a spacecraft and payload(s) that by itself is as complex as a launch vehicle or an airplane, and (b) they believe that space industry, in general, has established sufficient know-how and experience to confidently develop low-level systems, most of which are heritage designs, using their own internal standards and best practices. These contractors' own internal standards and best practices generally cover numerous subjects such as those relating to design audits, test planning and reviews, manufacturing reviews, and quality assurance programs; as such, the government has confident that their contractors, in general, can develop low-level systems on their own without the government's oversight.

Regardless, the traditional centralized-verification approach has some fundamental deficiencies in accomplishing thorough verification, "System is built right", because of the very nature of its systems engineering centric and top heavy focused centralized-verification approach as explained above.

There are four principle deficiencies in the traditional centralized-verification approach. These deficiencies are lack of oversight, plan, ownership, and risk

management in conducting verification at every level of system development as follows:

(1) The Traditional Centralized-Verification Approach Deficiency 1: Lack of Well Orchestrated End-to-End Systems Verification Program and Plan

The traditional centralized-verification approach will not likely to accomplish thorough verification of end-to-end space systems verification because both DoD and NASA focus on mostly on the verification of mission requirements and top-level systems developments mainly due to budget constraints for managing very complex large scale space systems coupled with their reliance on their contractors to develop technically mature low-level systems as explained in Section 2.2.

Furthermore, verification management processes are generally described as one of many systems engineering topics in systems engineering standards or handbooks that are primarily focused on the development of overall and top-level systems; hence, many space verification programs under these environments require their contractors to develop verification plans focusing only on overall or top-level systems. In fact, these guidelines or standards contain such statements as, “verification activities are an integral part of the systems engineering process. At each stage of the process, the system engineer's job is to understand and assess verification results and to lead in the resolution of any anomalies” (Reference 9).

Although, some agencies have developed stand-alone verification handbooks or guidelines such as an ESA verification standard (Reference 18) and NASA MSFC standard (Reference 19), these documents, however, are written such that systems engineering organizations are still responsible for the end-to-end system

verification, i.e., lower-level product teams' roles and responsibilities for managing the verification of their subsystems and unit levels are not clearly defined in these documents except for demanding a set of a large numbers of deliverable documents to the government. Namely, these ESA and NASA documents lack requirements that enforce a set of specific management processes to accomplish proactive and continuous verification activities at every level and phase of their developing systems. As such, it is normal that each developer plans and executes verification of lower level systems based on their responsible engineer's or manager's understanding of what needs be done to accomplish thorough verification of their products. Unfortunately, this approach will create problems since these lower level engineers and managers are in general demanded to develop their systems within the mandated cost and schedule; as such, they more often than not tend to overlook some important verification activities even if they are intended to do so. In order to accomplish thorough end-to-end system verification, the government should develop a stand-alone guideline document that enforces a set of standardized management processes to accomplish each level of system verification. This stand alone government guideline in particular demands each contractor to establish a verification program and associated verification plan, for each level of their developing systems, that will be reviewed and approved by the government.

(2) The traditional Centralized-Verification Approach Deficiency 2: Lack of Documented and Traceable Proof of End-to-End Systems Verification

As explained earlier, contractors are generally responsible for conducting low-level systems verification, and they assign their systems engineering organization

to accomplish this; however, it should be noted that even low-level systems of a major space program is very complex as they involve numerous units, subsystems, interfaces as shown in Figure 3.

In fact, a typical spacecraft bus of a space vehicle, for example, normally consists of at least six subsystems, each of which generally includes approximately 6-12 units depending on a subsystem. Furthermore, each of these units and subsystems typically contains approximately 100-400 requirements in each of their specifications; as such, one must deal with over 10,000 requirements in their efforts to properly accomplish requirement verification alone. For the same token, one mission payload can add similar numbers of requirements that need to be verified. Furthermore, most major space vehicles carry multiple payloads; as such, one must address tens of thousands of requirements to complete an end-to-end space vehicle verification. In addition, space systems verification must also address other verification activities such as those relating to design, manufacturing, test, and Sell-Off/Consent-to-Ship.

As such, under the traditional centralized- verification approach, the system engineering organizations that are responsible for the end-to-end system verification must address enormous amount of verification related activities just for low-level systems alone, if they try to do these activities by themselves. Hence, these contractors' systems organizations generally try to depend on each low-level system product organizations to complete verification of each of their developing systems without proper guidelines and without properly delegating them the responsibility for completing necessary verification; however, because of the large

numbers of units and subsystems and associated requirements, these contractors' systems engineering organizations most likely cannot collect sufficient documentations to prove that each low-level system organization conducted thorough verification

In fact, documented and traceable proof of verification of every requirement of each low-level system specification is rarely required under the traditional centralized-verification approach. In numerous occasions, analyses or test results that were supposed to have verified requirements, for example, were found to have been captured in engineers' personal notebooks that could not be traceable later-on after these engineers left their organizations or retired.

In order to effectively conduct low-level systems verification, each of the low-level systems developer must take ownership of the verification of their system so that they, instead of systems engineering organization, become responsible for completing their required verification with documented and traceable proof of verification. This verification ownership philosophy must be adopted by all prime contractor, subcontractors, and vendors.

(3) The Traditional Centralized-Verification Approach Deficiency 3: Lack of Government Oversight for End-to-End Systems Verification

The traditional centralized-verification approach most likely cannot accomplish thorough verification of an end-to-end space system, due to the absence of peer reviews and oversights by internal and external experts, at every level of system verification.

As explained earlier, most of the government acquisition agencies traditionally perform their oversight management functions focusing on top-level systems

development. In fact, official design reviews are conducted mostly on top-level systems based on their contract agreements. As such, the low-level systems design reviews milestones, for example, do not include the reviews of verification plans and their progresses by government experts or other organizations; hence, verification of these low-level systems might not be thoroughly planned and executed. This condition effectively opening up opportunities for each of the low-level systems developers to perform verification based on their understanding of verification. Unfortunately, each low-level system developer normally operates under constant schedule and cost constraints so that they will not necessarily be able to conduct solid verification of their systems even if they wish to do so. This phenomenon creates unintended TSPR approach as they are practically given full responsibility to develop these low-level systems without any customer oversights or peers reviews. Consequently, the responsible managers or engineers conduct their own way of verifications without proper guidelines or supervisions. This is one of the reasons that many space programs keep experiencing very costly latent problems discoveries late in systems development phases or in the worst case losing their launch or space vehicles after launch throughout the history of space systems acquisition activities including present time. In order to correct these problems, each level of system verification must be monitored by both government and contractor experts under a working group (WG) process so that peer reviews can be performed on almost continuous basis. This WG based oversight activities must be utilized by all prime contractor, subcontractors and vendors.

(4) The Traditional Centralized-Verification Approach Deficiency 4: Lack of End-to-End Systems Verification Risk Management

The traditional centralized-verification approach will not likely to accomplish thorough verification of an end-to-end space system verification since its verification processes are not properly integrated with risk management process at every level of system verification activities.

As explained earlier, systems engineering organizations conduct their verification mostly focusing on the top-level systems. For the same reason, risk management process is also mostly applied to top-level systems; as such, verification activities are not properly integrated with risk management processes particularly at the low-level systems development. With the lack of appropriate risk management integrated with verification process at every level of systems development, it is likely that a few of the large numbers of verification items could easily be overlooked or poorly performed. In addition, some important verification risks at low-level systems, that could impacts overall program's schedule and cost, might not be properly reported up to the top level management in timely manner.

The same can be said for other systems engineering processes such as quality assurance, PMPCB, FRB, configuration management and validation processes. These systems engineering processes must also be properly integrated with verification processes at every level of verification activities.

Again, a stand-alone government verification guideline document is required in order to effectively integrate verification process with risk management process and other appropriate systems engineering processes. This verification risk

management activities must be conducted by all prime contractor, subcontractors and vendors.

3 Examination of Past Space and Launch Vehicles Post-launch Failures

As a part of this research, it was investigated if the fundamental deficiencies of the traditional centralized-verification approach identified in section 2.3 above had existed even prior to the “Faster, Better, Cheaper” or TSPR era. This examination was accomplished based on the analysis and assessment of the past space vehicles and launch vehicles post-launch failures in terms of exactly what went wrong in their “system is built right” efforts during the development of these failed systems.

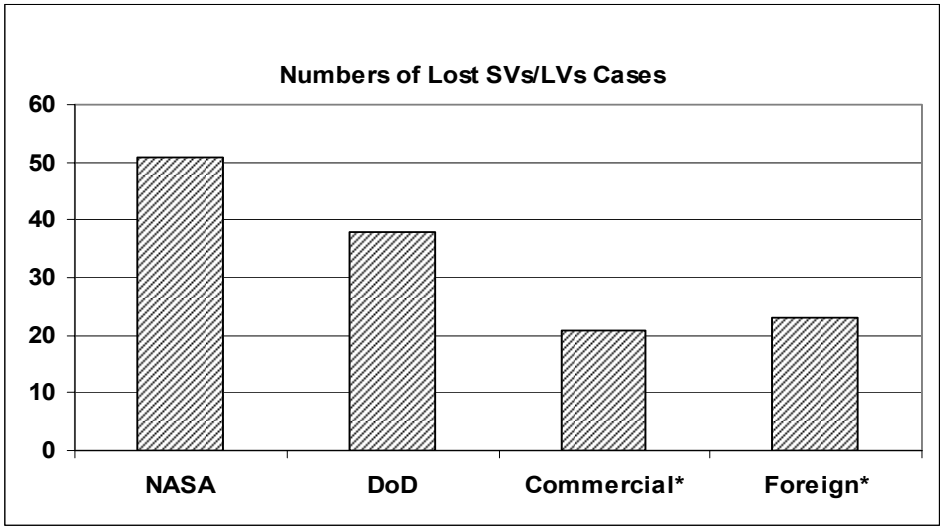
The Aerospace Corporation has collected data and lessons learned on nearly all U.S. national and NASA programs and a number of commercial, and foreign space/launch vehicle (SV/LV)-related failures that have occurred since 1960s. It reports, for example, a sample of 133 cases of lost- SVs/LVs for the period between 1964 and 2003 (Reference 20).

Figure 5 shows these SV/LV mishaps were sampled from those vehicles developed by NASA (51 cases), DoD (38 cases), commercial (21 cases) and foreign space programs (23 cases).

Subsequently, this paper examined each of their failure causes to understand what went wrong at (a) each system development phase (i.e., requirement, design/analysis, part and material process, manufacturing, and test disciplines), (b) each level of system development (i.e., unit, subsystem, system and launch integration), and (c) each technical discipline.

It was found that two cases (both foreign built SVs) out of 104 SV losses would have been very difficult to prevent, regardless what activities/processes were employed in their system development stages since these failures were determined to be caused by space debris. These two on-orbit failure cases were omitted from further examination.

It should be noted that SVs that were collaterally lost due to the LV launch failures were not included in this data analysis. In fact, the numbers of SVs that were also lost due to these 29 cases of LV failures exceeded over 40, since several LVs carried multiple SVs as their payloads.



(* Reported failure cases only)

Figure 5 Space Program Agencies vs. Post Launch SVs/LVs Losses (1964-2003)

3.1 Causes of Post-Launch Failures

(1) Development Phases

Figure 6 explains “in which phase of system development” they should have done better to minimize these SVs and LVs from failing during launch, separation and/or during on-orbit operations.

- Figure 6(a) shows that the majority (54%) of the SV failures were caused by deficiencies in design and analysis phase, followed by those caused by faulty tests (12%), ill-defined or lack of solid requirements (9%), errors in manufacturing and inspection (9%) and ill handled parts, materials and processes (PMP) (16 %).
- Figure 6(b) shows the similar trend for LV failure causes; failure causes were similar to those for SVs relating to deficiencies in design/analysis (64%), test (7%), and PMP(4%); however, faulty manufacturing/inspection (25%) and insufficient requirements (0%) appeared to be different from those of SVs.
- It should be noted that these statistical data apply only to primary sources of failures, and that other interrelated disciplines also failed to identify and correct problems were not included in this statistical analysis. For example, a deficient design could have been identified and corrected by thorough tests, if performed properly; however, only designs (not tests) are included as the sources of the problems in the calculations in this case. In another example, reasons for design deficiencies could have been due to ill-defined requirements. Even if it was identified in Figure 6 (a) or (b) that no

requirement related LV failures, this does not imply that the requirements were properly established or perfect for all LVs.

- Examples of deficiencies that occurred during different development phases are listed as follows:
  - Deficiency in requirement phase

    A main mission payload of a space vehicle was completely destroyed due to an application of reverse power because of a badly verified interface (IF) specification between domestic and off-shore-built hardware. This IF specification was later found to be ill-defined and not properly tested due to miscommunication between the foreign instrument provider and the SV developer/integrator.
  - Deficiency in design/analysis phase

    Several SVs' structures were damaged due to perturbation caused by flexible solar arrays (S/As) upon entering and leaving Earth shadows. Their designs/analyses did not consider that large temperature gradients could develop within an S/A under theses conditions such that it could torque an entire SV and damage weak points of SV's structure.
  - Deficiency in manufacturing/inspection phase

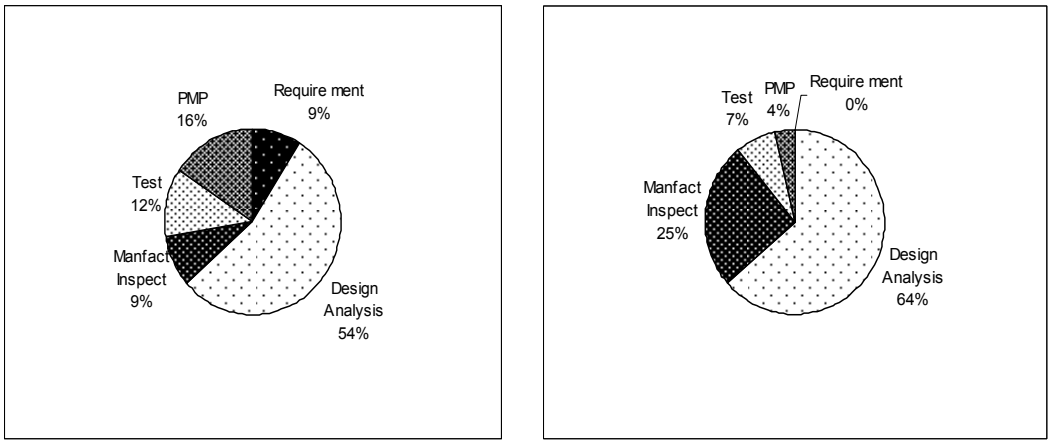
    An improperly installed/inspected thermal blanket prevented an antenna that was required to transmit mission data from being deployed.
  - Deficiency in test

    Spacecraft and main mission Payload (PL) computer IF was not properly tested, resulting in the loss of the main mission.

– Deficiency in PMP phase

The use of prohibited materials (such as pure tin plating that grows conductive filaments after installation) caused short circuiting of connectors in a number of space vehicles resulting in the loss of their missions.

The data shown in Figure 6 clearly indicates that rigorous verification processes, if implemented in each system development phase, would have reduced the numbers of these mishaps by verifying that (a) all the requirements had been properly established, (b) design and analysis had been thorough and complete, (c) manufacturing had followed drawing instructions/inspection requirements, (d) integration and test had been thoroughly conducted with successful results, and (e) all parts and materials processes (PMP) had been approved for their uses.



(a) SV Failure Causes vs. Development Phase (b) LV Failure Causes vs. Development Phase

Figure 6 Deficiencies at Different Development Phase That Caused the Loss of 102 SVs and 29LVs from1964 to 2003

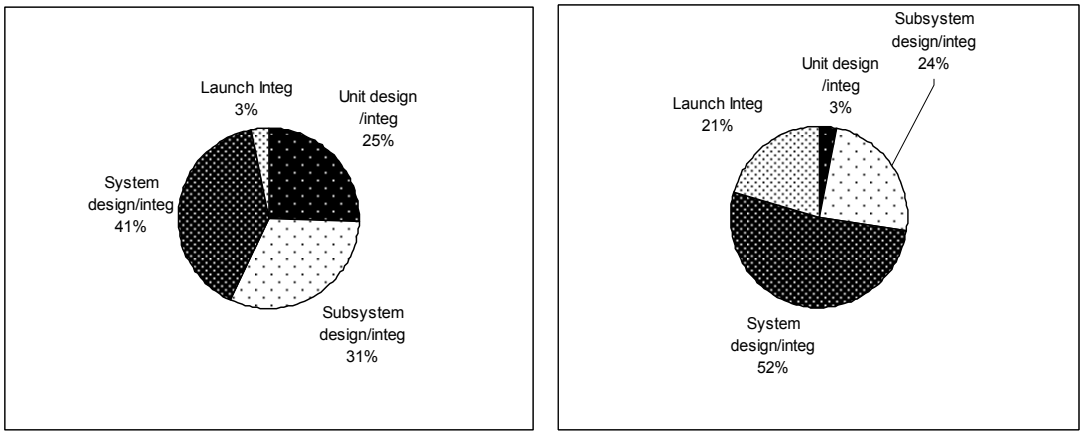
(2) Systems Development Level

Figure 6 explains "what level of system development (i.e., unit, subsystem, system and launch integration)" they could have done better jobs to mitigate them from becoming the culprits of these failures. It should be noted that Sub-element and element levels failures are included as a part of system failures in this analysis.

- Figure 7(a) shows that the majority (56%) of the SV failures were caused by deficiencies in lower levels of system development, i.e., 25% at unit and 31% at subsystem development phases.
- Figure 7(a) also shows that the almost all of the failures could have been avoided if solid work was done prior to the shipment of SVs to the launch integration and test; i.e., 97% of the 102 SV failures were caused by poor efforts in the SVs development prior to their shipment to their launch sites.
- Figure 7(b) shows a slightly different trend for LVs; i.e., the majority of the deficiencies occurred at higher level of LV development (52% system design and integration, and 21% launch integration).
- Figure 7(b) also shows that deficient work at each level of system development contributed to the loss of 29 LVs.
- Examples of deficiencies that occurred during unit to system level development are listed as follows:
  - Unit level problem: An oxygen tank on Apollo 13 blew up because two bimetallic thermostats contacts that were supposed to control a main tank heater circuit to prevent the tank from over temperature, welded shut due to a high voltage arcing because the 28V rated- thermostats

was used at 65V. This problem could have been avoided if the circuit with more robust thermostat were designed at unit level.

- Subsystem level problem: A spacecraft broke up near Mars S/C because the navigation control subsystem was made in wrong measurement unit causing the probe to be 100 kilometers off course. Standardized measurement unit (English or Metric units) not utilized causing confusion in specification, design and SW coding.
- Subsystem/Bus level problem: A solar array drive failed soon after deployment, because solar array boom drive motor fuses (both primary and redundant) was blown-out due to a sneak circuit path created through a EMI filter in the Sun sensor circuit and motor drive. The EMC current through a sneak circuit momentarily activated 4 transistors of a bridge motor drive blowing up the fuse. A solid FMEA and a sneak analysis (with teat) should have been conducted at EPS subsystem and/or Bus level development.



(a) SV Failure Causes vs. System Level (b) LV Failure Causes vs. System Level

Figure 7 Deficiencies at Different Level of System Development That Caused the Loss of 102 SVs and 29LVs from1964 to 2003

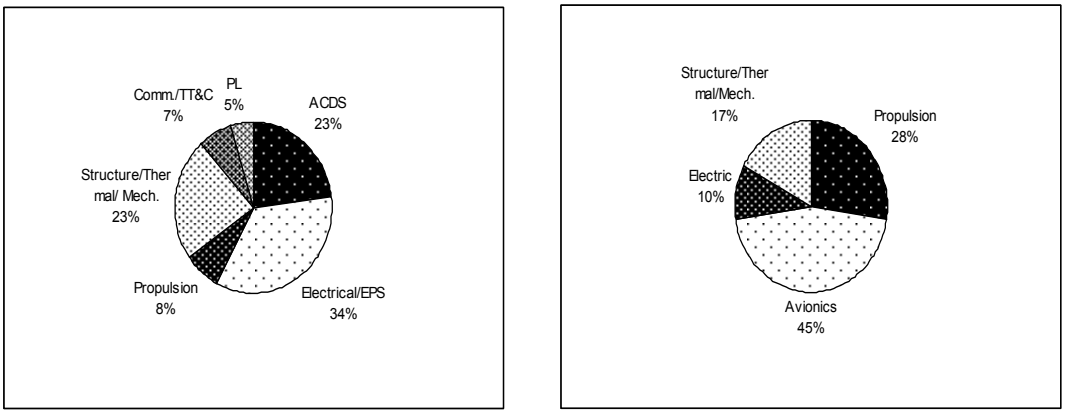
The statistics shown in Figure 7 clearly indicates that they could have mitigated the occurrence of these mishaps with rigorous verification processes, if implemented in each level of system development.

(3) Technical Disciplines

Figure 8 explains in which technical disciplines (such as electrical, mechanical, thermal, etc) they could have done a better job in order to mitigate the loss of these SVs/LVs.

- Figure 8(a) shows that the majority (57%) of the SV failures were caused by deficiencies in two subsystems: 34 % in electrical power subsystem (EPS), 23% in attitude control and determination subsystem(ACDS). The reasons for this were that both subsystems involve complex hardware and software related designs/analysis/simulation, coding, and tests.

- Regardless, the combinations of structure/thermal/mechanical (23%) and propulsion subsystems (8%) also caused substantial numbers of SV failures.
- Figure 8(b) shows the similar trend for LVs; i.e., the majority of deficiencies that caused the losses of LVs are relating to the combination of avionics (45%) and electrical (10%).
- However, propulsion (28%) and structure/thermal/mechanical (17%) caused substantial numbers of LV losses, because of the fundamental characteristics of the LV that involves hi-force to place the payload into the required orbit.



(a) SV Failure Causes vs. Technical Disciplines (b) LV Failure Causes vs. Technical Disciplines

Figure 8 Deficiencies at Different Technical Disciplines That Caused the Loss of 102 SVs and 29LVs from1964 to 2003

Again, the statistics shown in Figure 8 clearly indicates that they could have mitigated the causes of these mishaps with rigorous verification processes, if implemented in the development of each technical discipline.

3.2 Past Space and Launch Vehicles Post-Launch Failures Assessment Summary

The analysis and evaluation of the past space and launch vehicles post-launch failures described in Section 3.1 indicate that the majority of the principle causes of these failures might have been discovered and corrected, if rigorous verification processes had been implemented in the development of each phase, level and technical discipline associated with the development of these space systems.

For example, the overwhelming majority of these space vehicle failures could have been minimized and/or avoided if solid verification had been conducted starting earlier phases of systems development instead of just relying on test phase, i.e., 72 % for earlier phases (requirement, design and manufacturing) vs. 12 % for test phase test phase (See Figure 6).

In addition, the majority of these space vehicle failures could have been minimized and/or avoided if thorough verification had been conducted during the low-level systems, i.e., 56% for low-level systems (unit, and subsystem) vs. 41% for top-level (sub-element and element level) (See Figure 7).

Furthermore, these space vehicle failures could have been minimized and/or avoided if thorough verification had been applied to each technical discipline, such as electrical power subsystem (EPS), attitude control and determination subsystems (ACDS), and other subsystems during these space vehicles developments.

In summary, the results of analysis and evaluation of the past space and launch vehicles post-launch failures enforce the argument that the traditional centralized-

verification that focuses on top level- systems has fundamental problems for conducting thorough end-to-end system verification as explained in Section 2.

4 Newly Developed Verification Approach
(Distributed-Verification Approach with Modular Management Process)

It became evident in the course of this study that the traditional centralized-verification approach has fundamental deficiencies as explained in Section 2.3 and Section 3.0. In fact, these deficiencies, if not corrected, will continue to cause perennial cost overrun, schedule delay, and post-launch failures in worst case, as both DoD and NASA space programs are presently experiencing.

These findings, therefore, strongly suggest the needs for the development of more improved systematic verification management processes that can be forced to all level, phases, and technical disciplines associated with space systems development. In effect, the improved verification approach must be adopted by a prime contractor, subcontractors, and vendors. The improved verification approach must be designed such that it minimizes a simplest mistake in conducting verification at all aspects of systems developments.

This paper, therefore, proposed a new way of managing space systems verification program that implements a distributed-verification approach instead of the traditional centralized-verification approach.

4.1 The Newly Developed Distributed-Verification Approach with Modular Management Process

In an attempt to correct the deficiencies associated with the traditional centralized-verification approach and to provide more effective verification of space systems, a distributed-verification approach that utilizes a standardized modular management process was proposed (Reference 21).

The basic principle of this newly developed distributed-verification approach is to conduct end-to-end system verification by distributing (or delegating) the verification management responsibility to each level of system developer (be it a specific unit, subsystem, payload, ground system, space vehicle, or launch vehicle, i.e., be it a prime contractor, subcontractor or vendors). Then, each level of system developer conducts their verification activities using a standardized modular management process. Hence, this proposed approach is named as distributed-verification approach with modular management process.

Under this newly developed distributed-verification approach with modular management, each responsible system developer must ensure that their verification program is properly planned and executed at every phase and level of their systems development activities.

4.2 Synthesis of the Newly Developed Distributed-Verification Approach

(1) Standardized Modular Verification Management Process

This newly developed distributed-verification approach is designed such that each contractor, subcontractor, and vendor can easily establish and manage their verification programs by implementing a standardized modular verification management process that contains a set of six specific verification management processes, VM-Processes. These VM-processes are listed below while the details functions of these processes are explained in Section 4.4.

- VM-Process 1: Requirement flow-down and verification cross-reference matrix verification correlation matrix (VCRM) development process
- VM-Process 2: Verification by analysis, test, demonstration and inspection process

- VM-Process 3: Integration and test (I&T) process
- VM-Process 4: Individual specification dedicated verification ledger (ISDVL)process
- VM-Process 5: Sell-Off/Consent-to-Ship process
- VM-Process 6: Verification-related risk management process

(2) General Methods for Correcting Fundamental Deficiencies Associated with the Traditional Centralized-Verification Approach Using the Newly Developed Distributed-Verification Approach

The newly developed distributed-verification approach tries to correct the four fundamental deficiencies associated with the traditional centralized-verification approach, that are explained in Section 2.3, by establishing verification program with modular management process at each level of a developing system as follows:

(a) Under the newly developed distributed-verification approach, each level of system developer must develop a verification program and its plan that implement a set of six specific verification management processes, VM-Process 1 through 6, in order to conduct thorough verification at their level. By doing so, it corrects “The Traditional Centralized-Verification Approach Deficiency 1: Lack of Well Orchestrated End-to-End Systems Verification Program and Plan” explained in Section 2.3.

- This newly developed distributed-verification approach and associated verification plan for each level of system development will be developed using a stand alone verification management guideline document such

as a DoD best practice document entitled “Space System Verification Program and Management Process” (Reference 21) instead of exclusively relying on systems engineering standards or handbooks that generally lack detail guidelines for establishing a solid verification program.

(b) With the use of VM-Process 1 through 5, the proposed distributed-verification approach corrects “The Traditional Centralized-Verification Approach Deficiency 2: Lack of Documented and Traceable Proof of End-to-End Systems Verification”.

- Each level of system developer using these VM-Processes must ensure that (i) their specifications are properly established by verifying that upper level requirements are properly flow-down to their systems and derived/functional requirements are properly established for developing their systems, (ii) verification methods (analysis, test, inspection, and demonstration) and actual plan to complete these methods for verifying each requirement of a specification are properly developed and executed, (iii) end-to-end I&T plan for both top and low-level systems are properly developed and executed, (iv) plan to document proof of verification of every requirement of a specification is developed and executed with the use of ISDVL process, and (v) each of the delivered system has the proof of completion of verification relating to requirement, design/analysis, test, inspection and demonstration that is traceable to sufficient documentation. These documented proof of verification must

be able to show that appropriate disposition are complete for all the changes associated with requirements and designs, all the test anomalies, parts and materials problems, and manufacturing problems. As such, each of the documentation must have a proof of approval by appropriate authorities such as by those relating to quality assurance (QA), failure review board (FRB), configuration control board (CCB), parts, materials and process control board (PMPCB), etc.

(c) With the use of working group (WG) based verification activities, the newly developed distributed-verification approach corrects “The Traditional Centralized-Verification Approach Deficiency 3: Lack of Government Oversight for End-to-End Systems Verification”.

- A verification WG that consists of experts from government and contractors will be established at each level of system development. These WGs will help develop verification plan, and monitor the verification progress on continuous and proactive manner. Under this WG based management, contractor’s end-to-end system verification progress will be monitored by experts internal and external to the contractor, i.e., the inadvertent use of “Faster, Better, Cheaper” or “TSPR” approach in low-level systems development that tends to flourish in the traditional centralized-verification approach will be eliminated.

(d) With the use of VM-Process 6 (verification-related risk management) at each level of system verification, the newly developed distributed-verification program corrects “The Traditional Centralized -Verification

Approach Deficiency 4: Lack of End-to-End Systems Verification Risk Management".

- Each WG, dedicated to each level of system development, will be proactively and continuously identifying and resolving verification-related risks, small or large, throughout the program phases in order to minimize/prevent latent problems that could impact technical integrity of their developing systems. These risks, if not corrected in timely manner, could cause such costly problems of finding problems and repairing units late in a program phase and in worst case could cause the types of space and launch vehicles post-launch failures, described in section 3.

(3) Application of the Newly Developed Distributed-Verification Approach with Modular Management Process to Each Level and Phase of System Development

As explained earlier, each space system contractor including prime contractor, subcontractors, and vendors must apply the newly developed distributed-verification approach with modular management process in order to accomplish solid verification at each level and phase of their system development. In order to accomplish this, modular verification management process shown in Figure 9 (a) must be utilized at each level and phase of system development as shown in Figure 9(b) and (c), respectively.

Each space system contractor including prime contractor, subcontractors, and vendors accomplishes thorough verification by applying the newly developed distributed-verification approach with modular management process at each level and phase of their developing systems as follows:

(a) First, each contractor will be forced to recognize the importance of performing verification for their contracted systems by establishing the newly developed distributed-verification approach under the supervision of a verification management board.

(b) Each team, including systems engineering (SE), SV, LV, GS, and subsystem or unit development group, takes ownership of the newly developed distributed-verification approach for their responsible areas.

(c) Thorough documented proof of verification and traceability are established for every requirement of a product/system specification

(d) Each level verification program is planned, executed, and monitored under a customer-contractor cooperative working group (WG)

(e) Risk and problem items are proactively and continuously identified and resolved by each WG throughout the program phase in order to prevent/mitigate risk items at the earliest phase and in the lowest level of system development activities. This newly developed distributed-verification approach, thus, corrects the traditional centralized-verification approach's fundamental deficiencies that are listed in Section 2.3 as explained earlier.

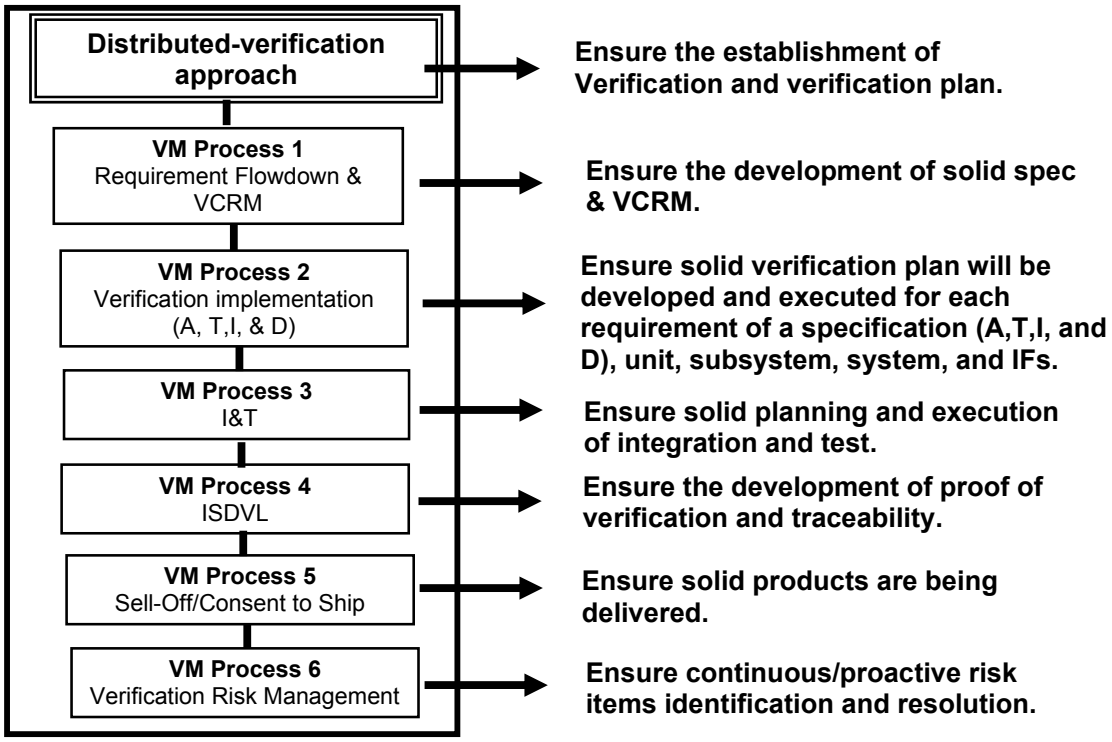


Figure 9 (a) Modular Verification Management Process and Function

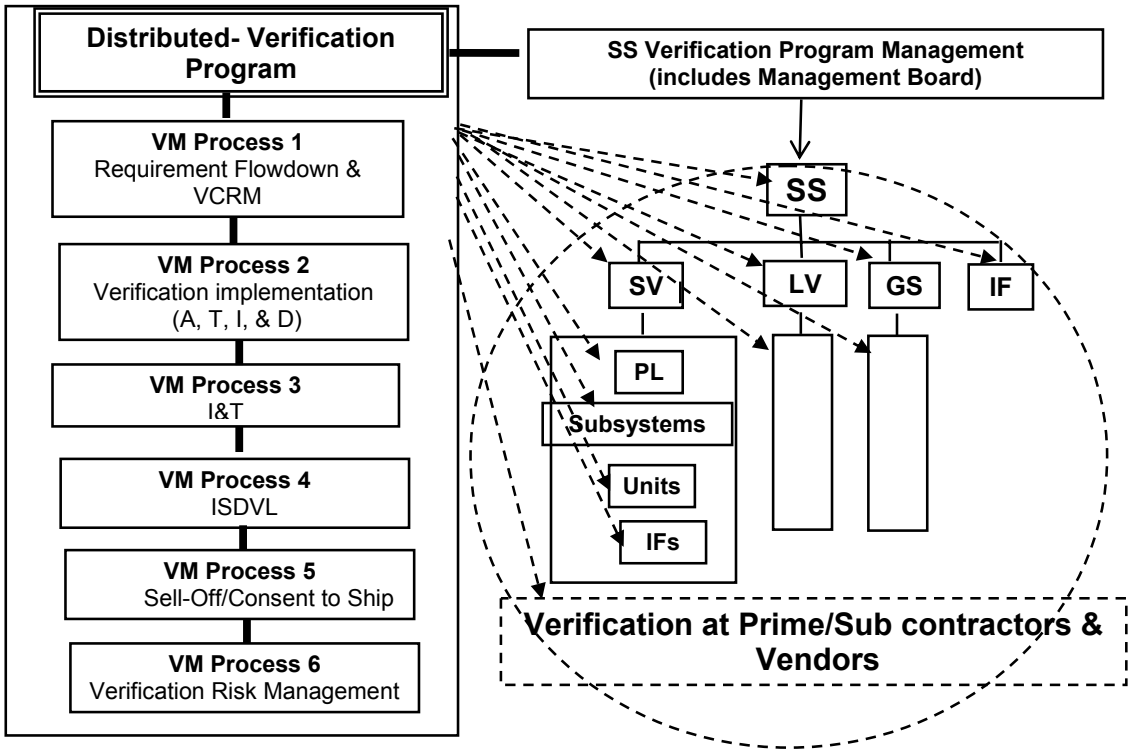


Figure 9 (b) Application of the Newly Developed Distributed-Verification Approach to Each System Level

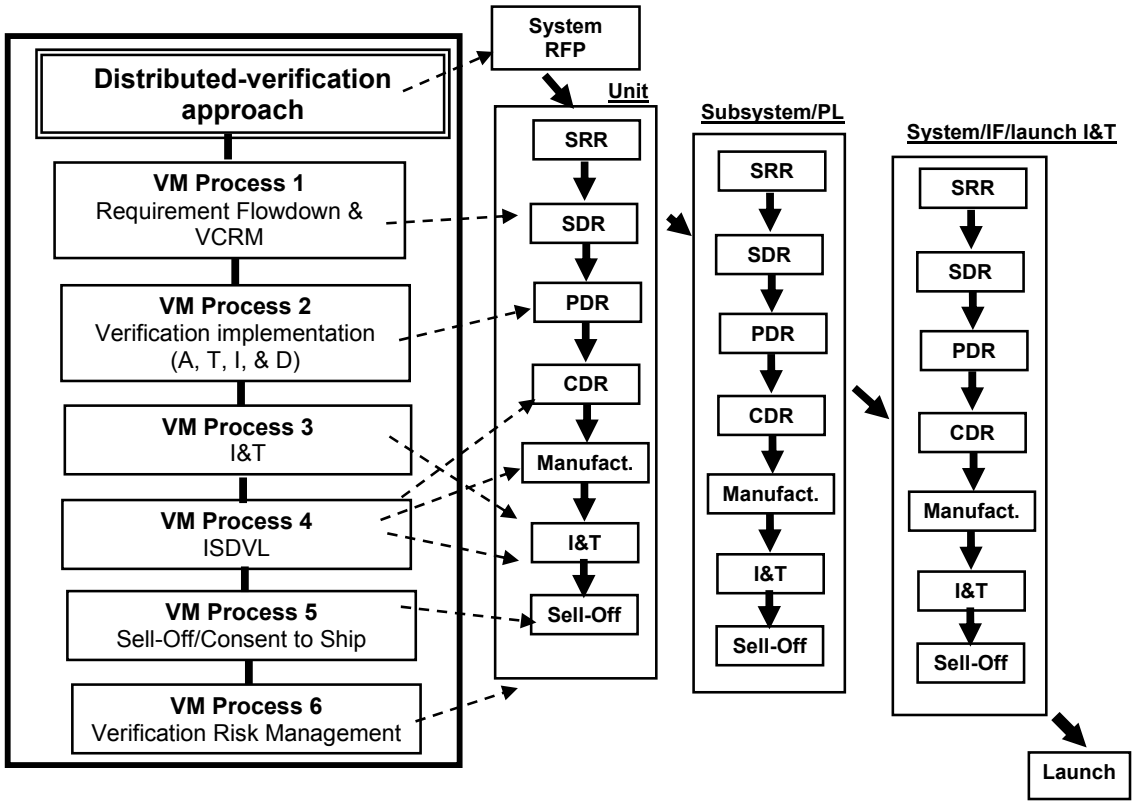


Figure 9 (c) Application of the Newly Developed Distributed-Verification Approach to Each Development Phase

Figure 9 Application of the Newly Developed Distributed-Verification Approach with Modular Management Process to Each Level and Phase of System Development

4.3 Establishment of the Newly Developed Distributed-Verification Approach Management Organization

It is essential for each space system (SS) contractor, subcontractor, and vendor establish a proper verification management organization in order for them to conduct thorough verification at each level and phase of their developing systems using a set of modular verification process, as explained in Section 4.2.

One of the most effective approaches for establishing an organization to implement the newly developed distributed-verification approach is to take

advantage of a Work Breakdown Structure based working group (WBS-WG), as WBS based management approach is broadly used in general space and other industries. Each WBS-WG will manage the verification of their developing systems and also coordinate their activities with external mission assurance related organizations such as failure review board (FRB), quality assurance (QA), independent readiness review team (IRRT), and parts materials, and processes control board (PMPCB).

In addition, it is essential to establish a verification management board (VMB) that provides continuous insight and oversight of these WBS-WG based verification activities in order to ensure that the thorough verification of the overall end-to-end system will be accomplished.

Figure 10 shows an example of the newly developed distributed-verification approach managed by VMB and WBS-WGs.

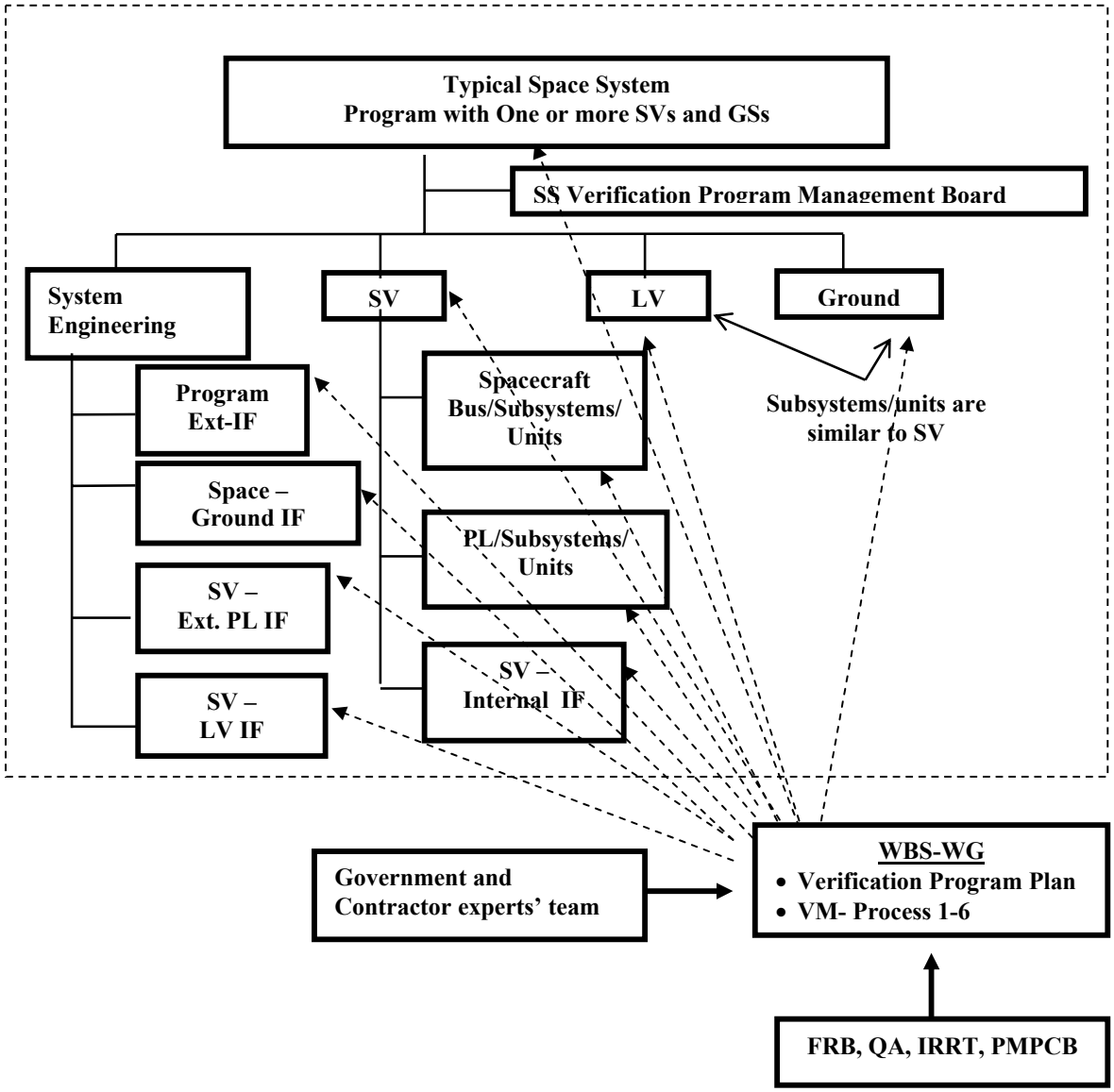


Figure 10 Example of the Newly Developed Distributed-Verification Approach Managed by VMB and WBS-WGs

(1) Work Breakdown Structure Based Working Group (WBS-WG)

With the use of working group (WG) based verification activities, the newly developed distributed-verification approach corrects the traditional centralized-

verification approach Deficiency 3: Lack of Government Oversight for Low-level Systems Verification".

As suggested earlier, most effective way to manage verification of each level of system development using the newly developed distributed-verification approach is to utilize WBS-WG organizational structure. In fact, NASA requires their space programs to utilize WBS-WG organizational structure to manage the development of their systems (Reference 15). The WBS-WG based management concept is not new; however, verification or risk management that is traditionally a system engineering related process is normally managed by systems engineering organization regardless of how they manage space systems; As such, these systems engineering functions are not generally delegated to product organizations that actually design, manufacture and test their developing systems.

One can conclude, therefore, that systems engineering related activities are still managed by systems engineering-centric centralized management approach even if WBS-WG structure is adopted for developing space systems. In the newly developed distributed-verification management approach, these systems engineering processes, both verification and associated risk management, will be conducted by each of the WBS-WG teams for each level of systems. This WBS-WG based verification program will be continuously active throughout each program's existence. These WBS-WG activities must be conducted under a government-contractor experts cooperative team work environments to encourage free discussions and evaluations with regard to the progress of their verification activities. Any WBS-WG disputes must be raised up to the verification

management board (VMB) so that they can resolved the issues based on overall technical or programmatic decisions and/or based on contractual requirements.

The philosophy of depending on each WBS-WG to conduct its own verification is due to the fact that the WBS-WG members are best-qualified to understand what needs to be verified in their respective systems. They are the ones who can successfully plan and execute the verification of that particular area on a continuous basis while managing their cost and schedule associated with their works. In addition, this WBS-WG approach enables customer experts to work with their contractors' counterparts on almost continuous basis. The participation of customer experts in the WBS-WG based verification management brings in advantages to the teams as follows:

(a) Government experts usually bring experience and knowledge that may not be necessarily available from the contractor's engineers. These government experts usually work on multiple space programs accumulating broader knowledge and experiences, whereas contractor engineers/technicians normally work on specific programs.

(b) They can also find and assess issues or concerns from an independent point of view on a near real time and continuous basis as WBS-WG members, without waiting for findings by an Independent Readiness Review Team (IRRT) that typically meets at periodic review milestones or later in the program phase such as at the time of periodic program reviews, at the time of SV/LV shipment, or prior to launch. Government WBS-WG members can also perform independent analyses/tests to continually evaluates the

contractor's work, thereby performing independent review on a near real time basis while participating in verification activities.

It is essential that the newly developed distributed-verification approach is properly flowed down from the prime contractor to the subcontractors and vendors so that each individual verification program is consistent with the prime contractor's verification program approach.

(2) Verification Management Board (VMB)

In addition, it is essential to establish a verification management board (VMB) that provides continuous insight and oversight into each individual system level and overall SS verification activities to ensure that they are properly planned and executed in well integrated manner. This VMB will report directly to the program manager. The VMB membership consists of both government and contractors representatives from program management, systems engineering and the rest of the working groups as well as those from other disciplines such as quality assurance, and manufacturing groups as needed basis.

This VMB should meet on a periodic basis throughout the program phases to ensure the development of hi-quality and reliable systems. In effect, verification progress status will not only be reviewed by each WBS-WG on almost continuous basis, but also evaluated by VMB team on a periodic basis.

(3) Independent Readiness Review Team (IRRT)

Independent readiness review team (IRRT) will be normally formed upon request from NASA or DoD to review both programmatic and technical progress of selected space programs at their major program milestones such as critical design

review (CDR), Sell-Off/Consent-to-Ship or prior to launch time frame. An IRRT will be formed with very experienced experts from internal government organizations and external technical consultant organizations. An Independent readiness review (IRR) will be conducted in addition to the verification activities of space programs. Each expert of an IRRT reviews and assesses contractor's works that relate to the areas of their expertise and provide action items to the programs being reviewed, if they do not understand or disagree with the contractor's works such as relating to design analyses, test anomalies resolutions or use of questionable piece parts. The complete disposition of all the action items provided by IRRT is mandatory, i.e., a program that is being reviewed by an IRRT cannot proceed with next phase of the program activities without resolving all these action items.

Most frequently conducted IRRs are launch readiness reviews that will be conducted to review and assess the flight readiness of space and launch vehicles. Theses launch readiness reviews will be usually initiated when the space and launch vehicles are started to get integrated at their launch sites. The space and launch vehicles will be launched when the launch readiness IRRT certifies the flight readiness of these vehicles.

These major IRRs are well proven techniques to assess the development history of their reviewing systems from independent point of view. These IRRTs, on numerous occasions, successfully identified problems prior to launch; however, problems found by IRRTs are normally very costly to fix and can cause significant schedule delay, because these space or launch vehicles are usually already being integrated together when problems are found. Any late changes such as removal

and repairs or replacement of a unit or piece parts during these major SV/LV integration phase could significantly jeopardize the integrity of these systems that have already been verified. The resolutions of these problems, therefore, require a series of serious re-verification activities including re-analysis and re-test, etc.

On the other hand, government and contractor experts participating WBS-WG based verification activities explained earlier play key roles for minimizing or avoiding IRRT discoveries of problems late in the program phase. WBS-WG based verification activities provide much more cost-effective ways of finding problems than an IRR as the former find problems at the earliest possible phase and at the lowest possible level of their systems development.

(4) Failure Review Board (FRB), Parts, Materials, and Processes Control Board (PMPCB), and Quality Assurance (QA)

FRB, PMPCB, and QA are generally independent organizations that are normally operated outside of specific space system programs; however, these organizations play important roles for ensuring thorough verification of each individual space system. These organizations are usually formed by contractor's experts and managers that oversee several programs within a contractor. FRB will be activated when a particular space system experienced some test anomalies. FRB will, for example, examine if the root cause of a test anomaly is properly identified and corrected, and a required re-test is completed. Then, they will certify that the problem is properly corrected and approve that the program can proceed with a next step of their planned activities. PMPCB ensures that each space program uses flight approved piece parts and materials control processes. Also they ensure that all the piece parts are properly used in the systems within their

accepted specifications' limits. QA performs variety of activities to ensure the quality of products. They, for examples, will examine if manufacturing of assemblies/units followed the proper manufacturing processes including inspection, and they will also examine if each step of test procedures was successfully tested or not. If so, they will provide so called QA stamp to certify the test is passed, if not, they write up a test anomaly report and request further investigation. Incidentally, each verification WBS-WG will closely work with each of these FRB, PMPCB and QA teams to ensure that each program properly addresses action items given by these organizations.

(5) Cost Impacts of Establishing the Newly Developed Distributed-Verification Approach

A concern might be raised with regard to the cost impacts of implementing the newly developed distributed-verification approach to an overall program cost, as establishing WBS-WG and VMB for conducting each system level and overall verification appears rather costly; however, it should be noted that almost all of the contractor members participating in a WBS-WG are those who actually perform requirement flow-down, design &analysis, manufacturing or tests for their developing systems. Their tasks are to follow up the proposed standardized modular verification management process while they are engaging in their regular work such as actually designing, analyzing, manufacturing or testing their developing systems. One of the main benefits of using the standardized modular verification management process is that it will force each engineer, manager or technician to be more thorough, precise and watchful while performing their daily works. Namely, the modular verification management process simply forces each

engineer, manager or technician to (1) document their works such as relating to their designs, analyses or tests and (2) help them to be proactive in identifying problematic items as a part of their risk management. Their responsibilities as representatives to a WBS-WG are to simply explain their verification progress status and the results of their analysis or tests for review by other members of WBS-WG at their periodic meetings. Most of these meetings can be informal face-to-face meetings between government and contractor experts or simple e-mail exchanges, as long as they conduct some regularly scheduled weekly, bi-weekly, monthly or quarterly WBS-WG meetings depending on the development phases of their program. In essence, a WBS-WG based verification approach will have minimal cost impact to their program since it simply forces each engineer, manager or technician to conduct their normal course of works in more rigorous manner using the modular verification management process as their guide.

Furthermore, the implementation of VMB should not add significant cost to the overall program cost. VMB will be normally led by a representative from their systems engineering organization and the members will consist of representatives from each WBS-WG. VMB meetings can be held informally between VMB lead and WBS-WG representatives in the form of e-mails or face-to-face meetings as long as they have arranged regularly scheduled periodic meetings. The VMB meetings are normally held in much less frequency than those of WBS-WG.

In summary, implementation of WBS-WG and VMB should have minimum impacts to the overall program cost.

4.4 Development of Verification Plan Using Standardized Modular Verification Management Process

The utilization of the newly developed distributed-verification approach and its plan should be included in the government RFP and in the contract agreement of a winning contractor. Under the newly developed distributed-verification approach, the verification plan should describe the verification requirements for each of the SS system elements, higher-level interfaces (IFs), segment (e.g., SV, LV, GS, system IFs) and subelement (e.g., bus, payload, and upper stage) level that will be undertaken by the prime contractor, subcontractors, and vendors. In particular, each verification plan should, at a minimum, explain what/how each of the six modularized verification management processes will be implemented at each SS level. Each of these plans should be further updated by an appropriate WG as the program proceeds. It also should be officially reviewed at each associated System Requirement Review (SRR), System Design Review (SDR), Preliminary Design Review (PDR), and Critical Design Review (CDR).

A standardized modular verification management process is intended to be adopted and tailored to fit the planning and execution of verification at each level of space system development; this includes the top-level space system, as well as the SV, LV and GS segments, including their lower-level subsystems, units, and interfaces. Each of the VM-Processes is delineated below:

(1) VM-Process 1: Requirement Flow-Down and Verification Cross-Reference Matrix (VCRM) Process

In this requirement flow-down process, not only the top system levels requirements but also low system levels hardware/software design specific

requirements that are usually not covered under the traditional centralized-verification approach must be addressed. In fact, the latter requirements normally far more exceeds than the former in numbers as explained earlier. In this VM-Process 1, requirement flow-down from the top to lower-level systems specifications (including unit and interface specifications) must be properly performed with documented traceability and appropriate assignment of verification method(s) for each requirement of a specification. The rationales for the selected choices for the flow-down and verification method assignment must be specified for each requirement. These assigned verification methods must be summarized as a VCRM in each of the top and lower-level system specifications as has been traditionally done, while the documented rationales for the requirement flow-down and verification method must be also captured using commercially available requirement allocation documentation software database tools. Any requirements in each of the space system specifications must be written such that it is objectively verifiable. As an example, one must strictly avoid such subjective requirement as “Single point design shall be avoided, as much as possible”. Instead, it should state “Single point design shall be avoided unless it is listed in critical design items that identify allowed single point failure designs due to impracticality of designing redundant systems”. The requirement flow-down and the associated VCRM development process for each SS level must involve periodic reviews by appropriate WBS-WGs. In addition, the results must be reviewed at each of the major program review milestones, SRR, SDR, PDR, and CDR. Again, contractor must deliver requirement allocation database that shows

the requirement flow-down from top to low level specification including internal and external IF specifications.

(2) VM-Process 2: Verification by analysis, test, demonstration and inspection process

Requirement verification generally involves verification by analysis, test, inspection, or demonstration. Each WBS-WG must develop its own requirement verification plan for accomplishing the verification of each requirement of their associated specification. In this planning process, the verification of internal and external IF specifications should not be overlooked, since deficiencies in these areas are often found to be the causes of system failures later on in program development. A WBS-WG management approach must be also utilized in the IF verification planning process, as is the case for the SS and lower-level systems.

In accomplishing verification by analysis, a list of analyses along with recommended approaches/methods, and a set of design reference cases (DRCs) for each analysis type must be defined and documented for each of the SS and lower-level specifications. The DRC is a set of worst-case conditions under which a requirement must be satisfied. Determining appropriate worst-case conditions can be a very contentious process, or can even become a contractual issue, if not properly agreed-on between the customers and their contractors; hence, the development of DRCs using customer-contractor WG philosophy becomes even more important.

In accomplishing verification by test, a test requirement document (TRD) must be developed for each specification to ensure that the requirements will be verified by appropriate tests and testing conditions. A TRD must include a list of tests along

with recommended approaches/methods (such as the use of flight units, engineering units, breadboard, solar array life-test coupon, and hardware/software-in-the-loop test) and the test levels (acceptance, qualification, or proto-qual level defined in such document as Reference 5) for each test article. In addition, rationales for selecting a given test level must be documented in an appropriate TRD for each of the top and lower-level systems. Again, each TRD must be developed by an appropriate WBS-WG to minimize shortfalls and disputes later on in the program phase. It is also imperative that a list of approaches/methods used for verification by inspection and demonstration be identified and documented for the SS and each lower-level system specification. Verification by similarity must be strictly avoided unless documented analyses/assessments demonstrate that application of a heritage system is completely the same as the earlier use. These include operating environments, electrical/mechanical/physical interfaces, design life, and piece parts, manufacturing, and I&T processes, and other relevant technical constraints. Verification by similarity, its rationale, and associated analyses/assessment that demonstrates its acceptability must be reviewed at SRR, SDR, PDR and CDR. Finally, each of the WBS requirement verification plans that include verification by analysis, test, inspection, and demonstration must be reviewed, as appropriate, at SRR, SDR, PDR and CDR. Each TRD must also be reviewed at appropriate test readiness review (TRR). Reviews of the verification by inspection and demonstration plan must be conducted at each related manufacturing readiness review (MRR).

(3) VM-Process 3: Integration and Test (I&T) Process

An Integration and Test (I&T) plan must be developed for the SS and each lower-level system to (a) test all the items listed in TRD for each associated specification, and (b) verify the integrity of the designed/manufactured system under the appropriate environments or test configurations specified in appropriate compliance documents such as MIL-Std-1540, Test Requirements for Launch, Upper-Stage, and Space Vehicles (Reference 5) and MIL-Std-1833 , Test Requirements for Ground Equipment and Associated Computer Software Supporting Space Vehicles (Reference 6).

The sequence, environment, types/levels, and duration of tests for the SS and each of the lower-level systems, including units and IFs, must be summarized in the top-level SS I&T plan, as well as in the lower-level segment verification plan.

A test-like-you-fly (TLYF) approach must be incorporated in each of the SS, segment, and module I&T plans in order to verify that the planned flight sequences and timelines, command operations, and data/telemetry uplinks and downlinks, etc., function under worst-case anticipated flight conditions

Developing an I&T plan for each SS system, element, subelement, subsystem, and unit as well as for each of the subcontractors and vendors, must be included in the contractor's proposal. Top level systems I&T plans must be delivered as Data Item Description (DID) items for review at SRR, SDR, PDR, CDR and TRR. Each of the verification plans for lower-system level should be reviewed at each system's major review milestones, SRR, SDR, PDR, CDR, and TRR.

TRR presents an important opportunity to accomplish thorough integration and test and must be conducted prior to each of the SS and lower-level system's I&T based on the entry and exit criteria that are reviewed and approved at SRR, SDR, PDR, and CDR.

Test discrepancies, resolutions, and scope of retests at each of the SS and lower-level system's I&Ts must be reported to the Failure Review Board (FRB), Parts, Materials, and Processes Control Board (PMPCB), Quality Assurance (QA), appropriate WBS leads, and the SS verification management board for their reviews and approvals.

Finally, each of the top and lower level systems' I&T summaries, including a list of discrepancies and their disposition, retests, and burn-in time, along with the summary results of the "as tested" data, must be documented and reviewed by QA, FRB, PMPCB, the appropriate WBS lead, and SS verification management board at the conclusion of the test and before the tested system is integrated into the next level.

(4) VM-Process 4: Individual Specification Dedicated Verification Ledger (ISDVL) Process

The ISDVL process, named by the author, will be used to ensure that every requirement in a specification has documented proof of verification and traceability to the responsible party and appropriate documents/data set. The ISDVL process must be implemented for each of the top and lower-level systems, including associated IFs, using a form that clearly summarizes a set of key information that demonstrates proof of verification and establishes traceability. An ISDVL generally consists of a traditional verification cross-reference matrix (VCRM) that specifies

the verification method for each requirement of a specification, and other columns that provide a synopsis of the verification method/approach identify where/who performed the verification, and list the report ID/ number that capture the verification results, such as an analysis, test, or inspection report. An example of an ISDVL form is shown in Table 2; its contents are as follows:

- The first column, “Paragraph or Requirement Number,” identifies the requirement or paragraph numbers designated in a specification.
- The second column, “Requirement Description,” provides a synopsis of each requirement.
- The third column, “Verification Method,” indicates the assigned verification method (or methods) for each requirement.
- The fourth column, “Verification Level,” identifies at what level of SV assembly the requirement was actually verified. It should be noted that some system-level SS specification requirements might not be verified at that level. Some of these requirements can be directly flowed down to lower-level specifications where the actual verification takes place. This column is particularly useful for the verification planning and Sell-Off of a higher-level SS component, since it identifies a particular unit(s) where the requirement has been or will be verified.
- The fifth column, “Responsible Person or Department,” lists the designated parties responsible for performing the verification and thus identifies appropriate individuals for further discussions/inquiries with regard to planning or results.

- The sixth column, “Documentation,” which consists of two subcolumns (“Verification Approach Summary” and “Verification Products”), is a summary of the verification and the data package/reports. This column is important because it forces official publication of the data. These columns also help to expedite the Sell-Off, latent troubleshooting, or Independent Readiness Review (IRR) process, since the data can be easily tracked down and obtained when required.

The ISDVL process and implementation status should be reviewed for the SS and each lower-level system at appropriate SRR, SDR, PDR, CDR, MRR, TRR, and Sell-Off/Consent-toShip reviews. The entire set of ISDVLs for the SS and all lower-level systems must be stored in a computer data base file for easy access and future traceability.

	Power Conditioning Unit (PCU) ISDVL (Example)**								
Paragraph or Requirement No. Designated in PCU Specification	Requirement Description	Verification Method*				Verification Level	Responsible Person or Department	Documentation	
		A	I	D	T			Verification Approach Summary	Verification Products
3.2.1	The output voltage regulation must be ≤100mV.	X			X	PCU Unit level	Unit design engineer or dept. name	W.C end of life analysis and EM Test	Power quality W.C analysis doc. No # xxx; EM Test Doc. # yyyy
3.2.2	The Phase margin of the unit must be greater than 30 deg.	X			X	PCU Unit level	Unit design engineer or dept. name	W.C stability analysis and EM Test	W.C stability analysis doc. No # xxx; EM Test Doc. # yyyy
3.2.3	Unit weight			X		PCU Unit level	Unit Test Dept.	By actually weighing unit	S/V mass property doc zzzz

* A: Analysis, I: Inspection: D: Demonstration, T: Test

** It may be desirable to indicate the verification completion date by adding an additional column

Table2. An Example of SV Unit-Level ISDVL

(5) VM-Process 5: Sell-Off/Consent-to-Ship Process

A set of entry and exit criteria must be developed for each of the top and lower-level systems' "Sell-Off/Consent-to-Ship" and be reviewed at each appropriate SRR, SDR, PDR, CDR, MRR, TRR, and prior to each system's Sell-Off/Consent-to-Ship review.

It should be noted that the entry/exit criteria for the Sell-Off and Consent-to-Ship reviews are not necessarily the same, since the completion of a SV/LV component Sell-Off sometimes requires the results of higher-level I&T results.

A set of data packages for each of the top and lower-level systems' Sell-Off and Consent-to-Ship must include, at minimum, the following items together with approval signatures of the appropriate WBS-WG lead, VMB, and representatives from QA, PMPCB, and FRB:

- ISDVL.
- As-tested test report approved by responsible engineers/QA department.
- Test summary, including environmental test history, summary of test anomalies and their resolution, and retest process/results.
- FRB/PMPCB summary, including approved/waived part lists.
- Deviations/waivers summary.
- Disposition status of action items generated at major SV unit-level CDR, TRR, and MRR.
- Disposition status of all the issue/concern items associated with each Sell-Off and Consent-to-Ship.

Each of these Sell-Off packages should be filed in an easy-to-track-and-retrieve computer database.

(6) VM-Process 6: Verification-Related Risk Management Process

Verification-related issues and concerns must be proactively and continuously identified, resolved, and documented for each of the top and lower-level systems throughout the requirement flow-down, design, manufacturing, test, and Sell-Off phases of the program. Each of the verification-related issues and concerns should be documented in a list that includes the problem description, responsible

department/engineers, problem identification and required resolution date, and its resolution.

Each of these verification-related issues and concerns and their disposition status must be reviewed on a periodic basis, such as at a weekly WBS-WG, monthly verification management program review, and/or at SRR, SDR, PDR, CDR, MRR, TRR, and Sell-Off/Consent-to-Ship. Finally, any verification-related issues that are deemed to seriously impact the schedule and cost of the program must be reported out to the overall program level risk management board in timely manner.

4.5 Documentation Requirements

It is important that each contractor representing member to a WBS-WG continually presents progress status of their related SS verification program to the WBS-WG members for their reviews and consultation. In addition, it is important to explain the detailed progress of each of the documents that are required by their verification plans for review by the rest of the WBS-WG members prior to their official presentation at program review milestones as shown in Table 3. Table 3(a) shows a list of these verification related documents for higher level systems. In general, these higher level documents are required to be officially delivered to the customer for their reviews as DID items at each major program milestone. Table 3(b) shows a list of these documents for lower level systems.

In general, these lower level documents are required to be presented at lower level system review milestones such as PDR, CDR, or Sell-Off/Consent-to-Ship review and are not normally delivered to the customer. These documents still need

to be captured in their computer filing systems in order to ensure the documented proof of verification planning and execution associated these VM processes. Regardless, ISDVL that is required as a part of Sell-Off package/Consent-to-Ship as explained earlier.

		Proposal	SRR	SDR	PDR	CDR	Manufacturing/Test	Sell-Off/Consent-to-Ship
SS, Higher level IFs, Segment and Module	Data Items	Proposed Verification approach	Requirement verification	VCRM/Detailed verification approaches	Preliminary Design analysis	Final Design Analysis	Inspection/ Demo/Test	Sell-off Package
SS Verification Program	SS Verification Program Plan	X	X	X	X	X	X	
•VM Process 1	Requirement Flow-Down & VCRM Plan		X	X	X	X		
•VM Process 2	Requirement Verification by Analysis, Test, Inspection and Demonstration Plan		X	X	X	X	X	
•VM Process 3	I&T Plan	X	X	X	X	X	X	
•VM Process 4	ISDVL Plan		X	X	X	X	Y	X
•VM Process 5	Sell-Off/Consent-to-Ship Plan		X	X	X	X		X
•VM Process 6	Verification-related Risk Management Plan		X	X	X	X	Y	X

(X: Denotes deliverable documents, Y: Review required by WG and at program milestones)

Table 3(a) Higher System Level Verification Program-Related Documents and Review Cycles

Subsystem, Unit, Lower level IFs	Review Data Package	Proposal	SRR	SDR	PDR	CDR	Manufacturing/Test	Sell-Off/Consent-to-Ship
Lower Level SS Verification Program	SS Verification Program Plan		Y	Y	Y	Y	Y	
•VM Process 1	Requirement Flow-Down & VCRM Plan		Y	Y	Y	Y		
•VM Process 2	Requirement Verification by Analysis, Test, Inspection and Demonstration Plan		Y	Y	Y	Y	Y	
•VM Process 3	I&T Plan		Y	Y	Y	Y	Y	
•VM Process 4	ISDVL Plan		Y	Y	Y	Y	Y	Y
•VM Process 5	Sell-Off/Consent-to-Ship Plan		Y	Y	Y	Y		Y
•VM Process 6	Verification-related Risk Management Plan		Y	Y	Y	Y	Y	Y

(Y: Review required by WG and at program milestones)

Table 3(b) Lower System Level Verification Program-Related Documents Review Cycles

Table 3 Documentation Requirement

4.6 Test Case Results

The newly developed distributed-verification approach that utilized modular-management process was implemented in a major U.S. national space program as a test case. This example space program accepted the customer's recommendations to implement this new verification approach for their SV development on a voluntary basis, since it was not a contractually agreed activity. Regardless, many of their system development groups accepted to implement this newly developed distributed -verification program with modular management process. It was found that the newly developed distributed-verification approach has been very effective for the development of their space vehicle, bus, payloads and associated subsystems and units. Most of their systems have been delivered within the contracted cost and schedule without adding any additional man-hour labor cost as they considered these verification activities anyway should have been conducted as a normal course of their contracted activities. For the space program community, these on-schedule deliveries would be considered a major accomplishment.

This particular space program, however, was not free of problems that were estimated to cost over $100 million loss because they lost one-half of the main mission. It was found that some spacecraft bus subsystems did not implement this distributed-verification program with modular management process as follows:

(a) It was discovered that the system did not have sufficient motor drive for operating normal mission after launch. In addition, it failed to deploy a

mechanism post launch because it was obstructed by spacecraft thermal blanket.

It was later found that these problems belonged to a subsystem that did not rigorously follow the modular verification management process that was required by the newly developed distributed-verification approach. If they had followed the standardized modular management process, they would have had realized that some requirements in a heritage unit needed to be changed in their designs along with their verification plan. It would have required not more than an additional 0.1 man-year for 8 years of labor cost for three engineers (i.e., 2.4 man-year that would be approximately $2-300,000 altogether), if any, for the contractor to implement the modular verification management process for this particular subsystem. Without implementing this process, they could not avoid these very costly mishaps that caused the loss of millions of dollars worth of the national space missions.

(b) Another costly example of this program was that a spacecraft structure adapter that support its payload had to be scrapped and redesigned after it was manufactured.

Again, if this structure subsystem had implemented the process the VM-Process 4, ISDVL process, they would have found that the analysis was not properly performed and not documented for the adapter design that should have been done as a normal course of their contracted activities. In effect, this newly developed distributed-verification approach, if it had been implemented, would have avoided

this problems that cost $ millions for no additional cost to implement this new verification approach.

Finally, another episode that demonstrated the effectiveness of this newly developed distributed-verification approach was as followed:

One another major space program (designated as Program B for convenience for this discussion) shut down a factory for repeated verification related problems, for several months. This factory was the same factory that had designed, manufactured, and tested the electrical/EPS subsystem for the program (designate as Program A for this discussion) that utilized the new verification approach around the same time frame. The key difference between the two programs was that Program B did not implement any of the "Six" verification management processes that Program A had implemented. The cost of implementing these processes for Program A was the cost for an approximately 0.5 man-year labor for 5 years (i.e., 2.5 man-year total that was equivalent to approximately $ 500,000 or so) that required for coordinating the activities between the factory and the Program A office. A coordinator was required to ensure the well orchestrated subsystem's WBS-WG activities between the Program A and the factory. In effect, the coordinator's function was to ensure that the factory engineers to become the members of the subsystem WBS-WG and their work progress were continually reviewed by the WBS-WG. In effect, Program B could have saved millions of dollars by just investing $0.5 million labor cost. Furthermore, this electrical/EPS subsystem developed under this new verification approach did not experienced any repairs or replacement of a

unit at a higher level of system integration and test or post launch failures as other subsystems had encountered.

In summary, it was found that the newly developed distributed-verification approach with standardized modular management process helped the contractor engineers and managers change their attitude toward engaging in their daily works. For example, they had to be able to show documented proof of their verifications and their traceability, as required by this standardized modular-process. The customer-contractor working groups had to agree with a set of the design reference cases (reasonable worst case conditions) in earlier design/analysis phase preventing any disputes later on in the program. They no longer recorded/documented analyses or tests that were needed for their requirement verification in their personal notebooks. Also, most of them became familiar with the proactive issue/concern items identification and resolution process. It helped them successfully avoid or minimize schedule and cost impacts to their system development by preventing or minimizing risk items in timely manner.

In effect, these aforementioned problems became testimonial cases to prove that the newly developed distributed-verification approach is a very cost effective verification management approach.

4.7 Verification Management Approach Comparisons between Space and Aircraft or Automotive Systems (Suggested Future Research Project)

It was suggested that the many of this newly developed space systems distributed-verification approach with standardized modular management process has already been implemented by general aircraft or automotive industries. However, it will require some extensive research and analysis in another research project to truly understand differences between space industry and these two industries with regard to the way verification of systems are managed. The principle reason for this is that these three industries are vastly different in complexity, development and production approaches, applications, operations, maintenance and safety considerations. This suggested research project needs to consider the following items in conducting the study:

(a) A major space system, that needs to operate several space vehicles and ground systems to satisfy their mission requirements, is much larger and more complex than an aircraft or automobile alone that can satisfy its mission by itself, See Figure 11 for an example of aircraft system (Reference 23).

It should be noted that one space vehicle of a major space systems such as GPS, communication satellite system, etc includes a spacecraft bus that by itself has a complexity equivalent to a launch vehicle or airplane. In addition, a normal payload itself has a comparable complexity as a spacecraft bus. Furthermore, one space vehicle normally carries several

payloads and a satellite constellation requires several space vehicles on one or multi orbits, and so on.

(b) The priority of the verification for these vastly different systems may not be the same. A space systems, for example, emphasizes overall mission requirements satisfaction for a long term (10-15 years) operations without ground repairs, whereas an aircraft system might focus on its performance and safety requirements.

(c) The verification management approaches for these vastly different systems may not be the same because of the differences in their production approaches, i.e., a single custom made vs. mass production.

In any regard, one cannot conclude that the verification management approach utilized by aircraft or automobile industries is applicable to space systems industry, or vice versa without an extensive research.

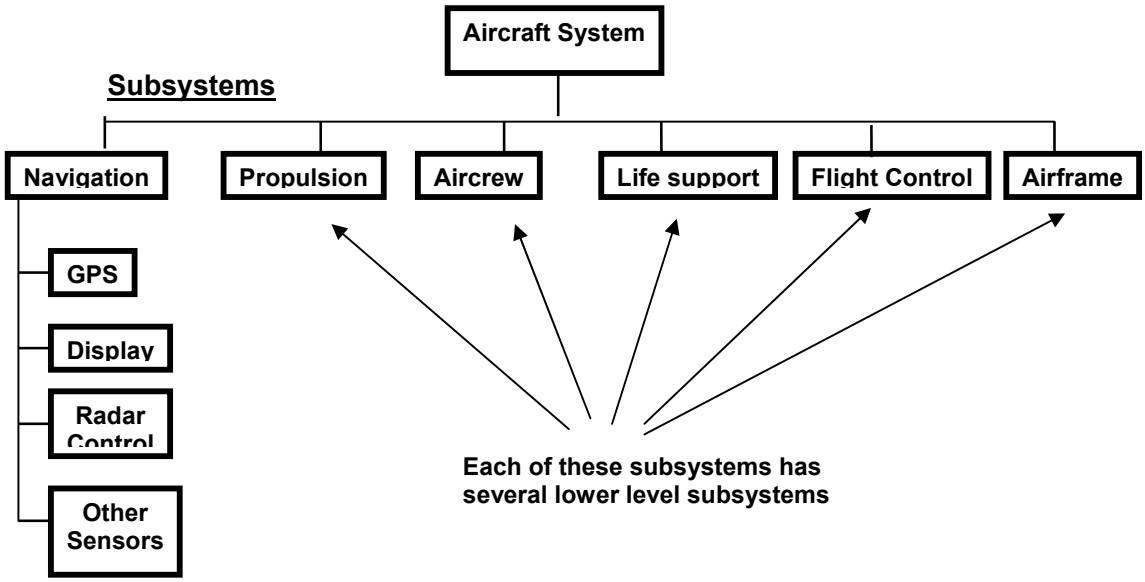


Figure 11 Example Product-Based WBS for an Aircraft System and one of its Subsystems: Navigation Subsystem. (Reference 22)

5 Conclusion

Since the dawn of space age that started with Sputnik in 1957 and Explorer in 1958, U.S. space systems acquisition activities have experienced a series of maturing processes; however, this research found that a systems engineering-centric centralized-verification approach was traditionally used throughout the space systems acquisition history. This study also found that this traditional centralized-verification approach has four fundamental deficiencies mainly because it failed to conduct thorough and detailed verification at each phase and at every level of system development due to the lack of appropriate government guidelines. These deficiencies are (a) lack of well orchestrated end-to-end system verification program and plan, (b) lack of documented and traceable proof of end-to-end system verification, (c) lack of government oversight for end-to-end system verification, and (d) lack of end-to-end verification risk management.

These findings were further confirmed by the examination of sampled102 space vehicles and 29 launch vehicles that had failed after launches between 1964 and 2003. In fact, this study points out that almost all of theses post launch vehicle failures could have been avoided, if the causes of the problems had been discovered prior to the shipment of these vehicles to their launch sites. Furthermore, it was found that the majority of theses space and launch vehicle failures could have been reduced in numbers, if contractors had conducted thorough verification of these failed vehicles during early phase (requirement and design phases), or at low-system levels (unit and subsystem levels) of development.

In an attempt to correct the fundamental deficiencies associated with the traditional centralized-verification approach, a distributed-verification approach was developed. It utilizes a standardized modular management process that contains a set of six verification management processes which, along with a verification plan, is required to be implemented at every level and phase of space systems development efforts.

This newly developed distributed verification-management program was found to be very effective in a test case using a U.S. major space program. It was estimated that a less than 10% of man-year per person for total of three engineers for 8 years, i.e., 2.4 man-year total (approximately $ 0.5 million) per each subsystem to implement this new distributed-verification approach; however, it will not be surprised to find that these cost will not be added to as an extra cost under competitive RFP. The reason for this is that the types of the activities required by this new verification approach are considered to be those tasks that each contractor should be doing as a normal course of conducting their business. In any case, the test program might have been able to avoid over $ 100 million worth mission loss, had they invested $ 0.5 million for implementing this new verification approach.

The details requirements for implementing this new distributed-verification approach are described in a Technical Operating Report (TOR) published by The Aerospace Cooperation (Reference 21).

The TOR has been reviewed by three separate U.S. Specification and Standard Advisory Committees from the National Reconnaissance Office (NRO),

Air Force, and The Aerospace Corporation, respectively. The NRO has decided to make the TOR as a Best Practice document whereas The Aerospace Corporation has selected it as a "core" standard that can be recommended to all the space community to implement. Air Force is currently planning to upgrade their system engineering standard that includes the TOR as a compliance document. Furthermore, the TOR has also been adopted as a compliance document in other major U.S. space programs, such as GPS Block III, and national security space programs.

This new way of managing space system verification has been explained in international conferences (Reference 23) and it is currently being reviewed by a U.S. Government-space industry working group, under the direction of its senior executive committee, for the purpose of making it as U.S. standard.

6 Acknowledgements

I would like to express my sincere appreciation to Professor Mengu Cho of Kyushu Institute of Technology (KIT), Japan for his very thoughtful guidance and advice that made the completion of this PhD thesis possible. I would also like to extend my appreciation to my thesis review committee members, KIT Professors: Prof. Koichi Yonemoto, Prof. Ysunori Mitani, and Prof. Masayuki Hikita for their very insightful, constructive comments and advice that helped me significantly improve the thesis.

7 References

1. Chang, I-Shih, Space Launch Vehicle Reliability, Crosslink Spring 2005, The Aerospace Corporation Publication, (www.aero.org/publications/crosslink/spring2005/03.html).

2. Explorer Missions, National Science Data Center (NSSDC)/NASA Goddard Space Flight Center, (http://nssdc.gsfc.nasa.gov/multi/explorer.html).

3. Tosney, W., and Pavlica, S., A Successful Strategy for Satellite Development and Testing, , Crosslink, Fall 2005, The Aerospace Corporation Publication. (www.aero.org/publications/crosslink/fall2005/01.html).

4. Lee, D., Space Reform, Air Force Institute of Technology, Air and Space Power Journal –Summer, 2004, pp103-112, (www.airpower.maxwell.af.mil/airchronicles/apj/apj04/sum04/sum04.pdf).

5. MIL-Std-1540 (Also, designated as SMC-TR-06-11 TR-2004(8583)-1 A), Test Requirements for Launch, Upper-Stage, and Space Vehicles, September, 2006.

6. MIL-Std-1833, Test Requirements for Ground equipment and associated computer Software Supporting Space Vehicles, November, 1989.

7. Shapiro, A., NASA Ultra-Reliability Project, IEEE Aerospace Conference, Aerospace Conference, 2005 IEEE Vlume , Issue , 5-12 March 2005, pp99 – 110, (www.ieeexplore.ieee.org/iel5/10432/33126/01559303.pdf).

8. MIL-Std-499A, Engineering Management, May, 1974.

9. NASA System Engineering Handbook, SP610S, Section 6.6 Verification, June,1995, pp103-111

10. INCOSE Systems Engineering Handbook, Version 2.0, July 2000.

11. EIA, Processes for Engineering a System, EIA Standard, EIA-632, 1999.

12. Audit Report IG-01-009; Faster, Better, Cheaper Policy, Strategic Planning, and Human Resource Alignment, March 13, 2001, Office of Inspector General), (www.hq.nasa.gov/office/oig/hq/audits/reports/FY01/ig-01-009).

13. NASA Responds to the Columbia Accident Report: Farewell to Faster - Better – Cheaper, Space Ref.Com report, Keith Cowing, September 15, 2003, (http://www.spaceref.com/news).

14. NASA Report: Too Many Failures with Faster, Better, Cheaper, By Leonard David , Senior Space Writer, 13 March, 2000,

(http://www.google.com/search?hl=en&q=Faster%2C+Better%2C+Cheaper&btnG=Google+Search).

15. NASA Procedural Requirements (NPR): NPR 7120.5D NASA Space Flight Program and Project Management Requirements, Office of the Chief Engineer, 06 March, 2007, pp18-22.

16. NPR 7123.1, NASA Systems Engineering Processes and Requirements, March 26, 2007.

17. INCOSE Systems Engineering Version 3.1, Verification, August, 2007. pp237-242.

18. ECSS Standard, Space Engineering/Verification, ECSS-E-10-02A, 17 November 1998.

19. NASA Verification Handbook, MSFC-HDBK-2221, February, 1994.

20. 100 Questions for Technical Review. Aerospace Report Number TOR-2005(8617)-4204, Cheng. P.G, 30 September, 2005.

21. Space System Verification Program and Management Process, Aerospace Report Number TOR-2006(8506)-4732, Nagano, S., 30 June, 2006.

22. NASA Systems Engineering Processes and Requirements Responsible Office: Office of the Chief Engineer, NPR 7123.1A, 26 March, 2007.

23. Nagano, S., Importance of Establishing a Solid Space System Verification Program, Proc. 6th International Symposium on Environmental Testing for Space Programmes, ESA SP-639, 12 June, 2007.

24. Scolese, S., NASA Interim Directive (NID), NASA Engineering Technical Excellence February 2, 2006, http://nodis3.gsfc.nasa.gov/npg_img/N_PR_7120_005C_/NM_7120-38_.doc.