Independent Verification and Validation for Space Shuttle Flight Software

Committee for Review of Oversight Mechanisms for Space Shuttle Flight Software Processes
Aeronautics and Space Engineering Board
Commission on Engineering and Technical Systems
National Research Council

July 1992

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the panel responsible for the report were chosen for their special competencies and with regard for appropriate balance.

This report has been reviewed by a group other than the authors according to procedures approved by a Report Review Committee consisting of members of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine.

The National Academy of Sciences is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Frank Press is president of the National Academy of Sciences.

The National Academy of Engineering was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Robert M. White is president of the National Academy of Engineering.

The Institute of Medicine was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Kenneth I. Shine is president of the Institute of Medicine.

The National Research Council was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Frank Press and Dr. Robert M. White are chairman and vice-chairman, respectively, of the National Research Council.

This study was supported by Contract NASW-4003 between the National Academy of Sciences and the National Aeronautics and Space Administration.

Available in limited supply from
The Aeronautics and Space Engineering Board
2101 Constitution Avenue, N.W.
Washington, D.C. 20418

Printed in the United States of America

COMMITTEE FOR REVIEW OF OVERSIGHT MECHANISMS FOR SPACE SHUTTLE FLIGHT SOFTWARE PROCESSES

Nancy G. Leveson, *Chairperson*, Professor of Computer Science, The University of California, Irvine
Robert N. Charette, Chairman, ITABHI Corporation, Arlington, Virginia
B. A. Clausses, Executive Vice President, CTA INCORPORATED, Denver, Colorado
Carl S. Droste, Engineering Manager, Flight Control Systems Section, General Dynamics, Fort Worth, Texas
Roger U. Fujii, Operations Manager, Systems Technology Operation, Logicon, San Pedro, California
John D. Gannon, Professor of Computer Science, The University of Maryland, College Park Maryland
Richard A. Kemmerer, Professor of Computer Science, The University of California, Santa Barbara
Robert O. Polvado, Senior Scientist, Office of Research and Development, Central Intelligence Agency, Arlington, Virginia
Willis H. Ware, Senior Member, Corporate Research Staff, The RAND Corporation, Santa Monica, California
Wallace H. Whittier, Program Engineering Manager, Lockheed Missiles and Space Company, Sunnyvale, California

Staff

Martin J. Kaszubowski, Study Director
JoAnn C. Clayton, Director, Aeronautics and Space Engineering Board
Christina A. Weinland, Senior Project Assistant

AERONAUTICS AND SPACE ENGINEERING BOARD

Aeronautics and Space Engineering Board Staff

JoAnn C. Clayton, Director
Martin J. Kaszubowski, Senior Program Officer
Allison C. Sandlin, Senior Program Officer
Noel E. Eldridge, Program Officer
Anna L. Farrar, Administrative Associate
Christina A. Weinland, Administrative Assistant
Susan K. Coppinger, Senior Secretary
Maryann Shanesy, Senior Secretary

Independent Verification and Validation for Space Shuttle Flight Software

EXECUTIVE SUMMARY

The Committee for Review of Oversight Mechanisms for Space Shuttle Flight Software was asked by the National Aeronautics and Space Administration's (NASA) Office of Space Flight to determine the need to continue independent verification and validation (IV&V) for Space Shuttle flight software.[1] The Committee found that the current IV&V process is necessary to maintain NASA's stringent safety and quality requirements for man-rated vehicles. Therefore, the Committee does not support NASA's plan to eliminate funding for the IV&V effort in fiscal year 1993. The Committee believes that the Space Shuttle software development process is not adequate without IV&V and that elimination of IV&V as currently practiced will adversely affect the overall quality and safety of the software, both now and in the future. Furthermore, the Committee was told that no organization within NASA has the expertise or the manpower to replace the current IV&V function in a timely fashion, nor will building this expertise elsewhere necessarily reduce cost. Thus, the Committee does not recommend moving IV&V functions to other organizations within NASA unless the current IV&V is maintained for as long as it takes to build comparable expertise in the replacing organization.

INTRODUCTION

In early 1991, NASA's Office of Space Flight commissioned the Aeronautics and Space Engineering Board of the National Research Council (NRC) to investigate the adequacy of the current process by which NASA develops and verifies Space Shuttle flight software. In January 1992, the Board convened the Committee for Review of Oversight Mechanisms for Space Shuttle Flight Software Processes to evaluate the adequacy of the process from initial requirements definition to final machine loading. The Committee was given until the end of 1992 to complete its investigation and prepare a final report.

One of the issues the Space Shuttle program office requested that the Committee specifically consider was the office's pending decision to eliminate the IV&V function currently

---

[1] It should be noted that the Committee was specifically asked not to evaluate the performance of the current IV&V contractor, Intermetrics, or its subcontractor at the Marshall Space Flight Center, Smith Advanced Technologies, but rather to concentrate on the need to continue the function they serve.

performed on the Shuttle flight software at an annual cost of $3.2 million. The IV&V function was instituted, in part, as a result of a recommendation of a previous NRC committee evaluating post-Challenger Space Shuttle risk assessment and management. The Shuttle program office now believes that the flight software and the processes that are used to develop and verify updates are sufficiently mature to permit a phase-out of the contractors that perform IV&V. Eliminating this function is primarily a cost-saving move, but one that the Shuttle program office believes is justified by the overall quality of the processes and personnel that are in place to maintain the software. In short, the Shuttle program office believes that the process is adequate without IV&V and the money may be better spent in other ways.

Because the IV&V function is currently scheduled to be eliminated by October 1992, the Office of Space Flight requested that the Committee first address whether there is a need to continue this function and later address other aspects of the flight software development process. Thus, the Committee focused on this issue in its first four meetings, and this report addresses the Committee's findings and conclusions on this one issue. The final report, which will examine other aspects of the flight software development process, will be available near the end of 1992.

BACKGROUND

Flight software is defined as the software that is loaded into the on-board computers for control of the Shuttle during launch, on-orbit operations, entry, and landing. The primary flight software consists of approximately 500,000 lines of source code in almost 400 compilable units, while the backup software is approximately 90,000 lines of code. The software has evolved over many years of operation to require a complex maintenance and upgrade process involving numerous contractor and NASA organizations at a cost of well over $100 million per year.[2] Upgrades are performed on a continuing basis (approximately one per year) to provide new functions and to fix the errors that are still being identified. Because it controls so many aspects of the Shuttle's operations, flight software is deemed by the Shuttle program to be a critical item for safety and reliability.

Following the Challenger accident in 1986, a number of assessments were made of the overall safety of the Shuttle program, many of which addressed software verification and validation as part of their investigations. These included evaluations by the Rogers Commission; an NRC committee; the House of Representatives' Committee on Science, Space, and Technology; and the General Accounting Office (GAO).

---

[2] The Committee was told that the yearly cost for the flight software development contractors (new development, maintenance, software configuration control, etc.) was approximately $60 million. Operation of the Shuttle Avionics Integration Laboratory, which is used to test the flight software, requires approximately $24 million per year. This total does not include costs for software reconfiguration, development and maintenance of Space Shuttle Main Engine software, and other support contractors.

The Rogers Commission[3] concentrated on the direct causes of the Challenger accident, but Appendix F of their report included a statement by Richard Feynman, one of the members of the commission, that pertained specifically to the flight software, ". . . there have been recent suggestions by [NASA] management to curtail . . . elaborate and expensive tests as being unnecessary at this late date in Shuttle history. This must be resisted, for it does not appreciate the mutual subtle influences and sources of error generated by even small changes to one part of a program on another."[4]

Among the recommendations of the Rogers Commission was that NASA review certain aspects of its Shuttle risk assessment effort and ". . . identify those items that must be improved prior to flight to ensure mission success and flight safety." It further recommended that an audit panel be appointed by the NRC to verify the adequacy of the effort and report directly to the Administrator of NASA.

This audit panel was convened by the Aeronautics and Space Engineering Board of the NRC in 1986, and its final report, dated January 1988, concluded that "In general, hardware certification and verification, and software validation and verification in STS [Space Transportation System] are managed and conducted primarily by the same organizational elements responsible for the design and fabrication of the units. Thus, the independence of the certification, validation, and verification processes is questionable. For example, . . . 'Independent' validation and verification (IV&V) of software is carried out by the same contractor (IBM) that produces the STS software, with some checks being made by the Johnson Space Center."[5]

The NRC committee recommended that "Responsibility for approval of hardware certification and software IV&V should be vested in entities separate from the NSTS [National Space Transportation System] Program structure and the centers directly involved in STS development and operation."

In March 1988, the House Committee on Science, Space, and Technology, echoing the concerns expressed in the NRC report, recommended that NASA establish IV&V to evaluate the development and modification of Shuttle software. Based on these two recommendations, in May 1988 NASA expanded an existing contract with Intermetrics, Inc., and instituted the current IV&V function. The original IV&V contract with Intermetrics supported 40 people; recently, the support has been reduced to 24 people, at an approximate annual cost of $3.2 million. Table 1 shows the functions that were encompassed by the original 40-person effort and the corresponding functions addressed by the present, reduced level of effort. The current plan by NASA will completely eliminate IV&V for all the functions shown in Table 1.

In February 1990, the House Committee requested that the GAO determine NASA's

---

[3] Report of the Presidential Commission on the Space Shuttle Challenger Accident, by William P. Rogers, Chairman (Washington, D.C.: Government Printing Office, 1986).

[4] Feynman, R. P., "Personal Observations on Reliability of Shuttle," Appendix F of the Report of the Presidential Commission on the Space Shuttle Challenger Accident, by William P. Rogers, Chairman (Washington, D.C.: Government Printing Office, 1986).

[5] Post Challenger Evaluation of Space Shuttle Risk Assessment and Management, by Alton D. Slay, Chairman of the Committee on Shuttle Criticality Review and Hazard Analysis Audit (Washington, D.C.: National Academy Press, 1988).

TABLE 1 Functions Covered by the IV&V Contractors

IV&V Functions	IV&V Functions at Start of IV&V Contract (40 full-time workers)	Current IV&V Functions (24 full time workers)
Ascent guidance, navigation, and control	X	X
Entry guidance, navigation, and control	X	X
On-Orbit guidance, navigation, and control	X	X
Sequencing	X	X
Data processing system	X	X
Main engine controller	X	X
Systems management/payload	X	
Redundancy management	X	
Launch processing systems	X	
Documentation-only Change Requests	X	
Flight software tools	X	
Reconfiguration	X	
Downlist	X	
I-Load to K-load Change Requests	X	
"Living" Change Requests	X	

SOURCE: Intermetrics

progress in improving independent oversight of Shuttle software development. The GAO report,[6] dated February 1991, recommended that NASA "require independent V&V [Verification and Validation] for Shuttle software, bearing in mind the views of the NRC, the House Committee, the [NASA Space Shuttle] software steering group,[7] and NASA-wide guidance, and ensure that the independent V&V organization is outside the control of the Shuttle program office."

In requesting the current review of the IV&V process, the Shuttle program office has stated that if funding were not an issue they would continue with a robust IV&V program. However, if it can be shown that the current implementation of IV&V does not appreciably reduce risk, or that its cost cannot be justified by the risk it avoids, it can reasonably be eliminated. The Shuttle program office does not believe that these issues were adequately addressed by previous studies, which did not have the benefit of recent efforts to document the current V&V process.

To investigate the question of whether to continue IV&V, the Committee heard

---

[6] United States General Accounting Office, Space Shuttle: NASA Should Implement Independent Oversight of Software Development (Washington, D.C.: United States General Accounting Office, 1991).

[7] The software steering group consisted of officials from the Johnson Space Center, the Kennedy Space Center, the Marshall Space Flight Center, NASA Headquarters, the software development contractors, and the Space Transportation System Operations Contractor. The group met once to address the need to bring about changes in NASA's software development and assurance processes but did not produce formal recommendations.

presentations from the Shuttle program office, the software development contractors, the current IV&V contractors, and several outside organizations and experts, including the U. S. Air Force and Navy. The Committee also reviewed extensive documentation and data provided by NASA and the contractors describing both the independent and "embedded"[8] verification and validation processes. The following sections present the findings of the Committee along with a recommendation regarding the continuation of IV&V on the Shuttle software. It should be noted that the Committee was specifically asked not to evaluate the performance of the current IV&V contractor, Intermetrics, or its subcontractor at the Marshall Space Flight Center, Smith Advanced Technologies, but rather to concentrate on the need to continue the function the contractors serve. This proved to be a difficult restriction because the argument for continued IV&V hinges partly on the capabilities these two companies bring to the process.

Based on this investigation, the Committee concluded that the current IV&V process is necessary to maintain NASA's stringent safety and quality requirements for man-rated vehicles. Therefore, the Committee does not support NASA's plan to eliminate funding for the IV&V effort in fiscal year 1993. The Committee believes that the Space Shuttle software development process is not adequate without IV&V and that elimination of IV&V as currently practiced will adversely affect the overall quality and safety of the software, both now and in the future.

This report focuses solely on the need to continue IV&V. A complete discussion of the embedded process will appear in the Committee's final report. Regarding the issue of continuing IV&V, the Committee's evaluations are based on answers to the following questions:

1. Does the current approach to IV&V improve the quality of the software beyond what the embedded process alone provides?
2. Does the improvement justify the cost?
3. Will NASA's proposed alternatives to IV&V provide the same benefits for a lower cost?

The following sections present the Committee's findings and recommendations with respect to these questions.

THE BENEFITS OF IV&V

The flight software development process is described in detail in a document recently prepared by Intermetrics and approved by the Space Shuttle program office.[9] This document discusses what NASA calls its "embedded" process, which excludes the IV&V effort. It is the

---

[8] The term "embedded V&V" was coined recently by the Shuttle program office in their argument to eliminate IV&V. In the Committee's judgement, it is equivalent to what is commonly referred to by industry as simply "verification and validation."

[9] National Aeronautics and Space Administration, Space Shuttle Flight Software Verification and Validation Requirements, NSTS-08271 (Houston, Texas: Johnson Space Center, 1991).

understanding of the Committee that if the IV&V function were to continue, it would do so in addition to the embedded process described in the above document.

The embedded process provides a number of checks and rigorous configuration control mechanisms. Ultimately, however, the embedded process relies on the development contractors[10] to perform their internal verification and validation correctly, and on an extensive set of system integration test simulations to expose any potential problems. Once a change to the software[11] is agreed upon by all members of the flight software community,[12] the development contractors perform their work according to their own established procedures. Later, when the development contractors have completed their internal tests, the software is released to the flight software community for additional testing. The Committee believes that the organizations involved are truly concerned with producing the best software possible and has found them willing to discuss any and all aspects of the process (within bounds of proprietary information) at any time. The Committee was particularly struck by the degree of teamwork that is shown in addressing problems and believes this emphasis on openness and consensus is one of the strengths of the process. Furthermore, the process is relatively mature and each organization knows its role and has much experience performing it. The Committee's full report will include a complete discussion and evaluation of the embedded process.

In examining the need for continuing the IV&V function, the Committee identified four areas where the embedded process clearly benefits from the on-going independent technical assessment. The Committee believes that the current implementation of IV&V:

Provides a broad perspective: As mentioned above, the embedded process relies heavily on the development contractors (IBM, Rockwell, and Rocketdyne) to perform their internal verification and validation correctly. This is appropriate and reflects the approach used throughout the industry, as well as in the U. S. Air Force and Navy software development procedures. However, the development contractors have incentive to consider only those components with which they are specifically concerned. This lack of broad perspective makes it more likely that errors will slip through in areas that do not fit any particular organization's responsibility. The IV&V function is specifically chartered to provide this broad perspective. For example, the current flight software IV&V contractor has been particularly active in addressing issues that relate to the interface between the primary avionics software (developed by IBM) and the backup flight software (developed by Rockwell) and has identified several potentially serious errors

---

[10] IBM is the development contractor for the primary avionics software system, Rockwell develops the backup flight software, and Rocketdyne is responsible for the main engine controller software.

[11] Changes are implemented through Change Requests (CRs), which are requested to enhance the functionality of the software, and Discrepancy Reports (DRs), which describe errors in the software that require action.

[12] The flight software community includes all the organizations within the Shuttle program that have an interest in the development, verification, or performance of the software. This includes representatives from the Mission Operations, Flight Crew, and Engineering Directorates at the Johnson Space Center; NASA's Safety and Mission Quality Office; the software development contractors (IBM and Rockwell International); the operations contractors (also IBM and Rockwell); the Shuttle system design contractors (Lockheed and Charles Stark Draper Labs); and the IV&V contractor (Intermetrics). At the Marshall Space Flight Center, this includes the NASA personnel, the development contractor (Rocketdyne), and the IV&V contractor (Smith Advanced Technologies) that develop the Space Shuttle main engine controller software.

(discussed in the next section) that were not caught by the embedded process.

Maintains vigilance over the quality of the process: The Committee believes that the reliance on the development contractors to perform their internal process is appropriate. Also, except for the previous comment regarding a broad perspective, the embedded process includes numerous checks on the development contractor's products to ensure that safe, reliable software is produced. For these checks to work, however, they must continue to be performed with diligence, aggressiveness, skill, and integrity. Unfortunately, there is increasing risk that the quality of the software will degrade as it is changed. Over a long period of time, a mechanism that provides an independent technical review will significantly enhance the embedded process.

Offsets the erosion of expertise: Developing software, particularly software as complex and specialized as that for the Shuttle avionics, requires considerable specific expertise and correspondingly sophisticated tools. It is not enough to design a process that covers all aspects of the problem, the expertise and capabilities that are built up over a period of years need to be maintained.[13] Many of the original developers of the Shuttle flight software have already gone on to other projects, and the perception that the flight software is mature indicates that in the future it will be difficult to retain many of the highly competent software engineers and managers that are currently involved in the process. According to statements by several of the NASA and contractor managers interviewed during the Committee's investigation, programs that involve a greater degree of new development, such as the Space Station Freedom and the National Launch System, will likely continue to attract experienced personnel away from the Shuttle program. Continued steps must be taken to maintain skills and provide additional checks on the process. Independent oversight is a partial solution, but only if the group that performs the oversight also provides a significant level of experience and technical capability.

Avoids bias and peer pressure: The emphasis on consensus that is evident in the embedded process is admirable, but the Committee believes it brings with it the possibility that individual assessments of important issues can be stifled through peer pressure, through the desire to protect organizational interests, or through the simple desire to make the process run smoothly. Furthermore, when a problem is recognized and an initial solution is proposed, particularly when it is proposed by a customer, it often serves to bias further thinking on the subject towards that initial solution. While the Committee has found no instances where this type of contamination or stifling has occurred, it believes that the risk is significant without some degree of oversight that is explicitly designed to be independent.

---

[13] In discussions with the Committee, IBM has estimated that it takes at least two years for new employees to adequately understand the Shuttle flight software. Estimates obtained from the contractors regarding the experience of their current personnel specific to Shuttle software are as follows: IBM has 153 workers with an average experience of 13 years, Rockwell has 85 workers with an average of 7.8 years of experience, and Intermetrics has 24 people who average 6.7 years of experience with Shuttle systems and 14.9 years of avionics/software experience.

IV&V IN THE SPACE SHUTTLE PROGRAM

Independent verification and validation of software has been used by industry for over twenty years in many different forms—tailored by the user's need, the complexity of the system, the criticality of the system's application, and budget and schedule constraints. In NASA's current implementation of IV&V in the Space Shuttle program, the contractors responsible for IV&V are involved in the process from the beginning, provide a high level of technical expertise and knowledge of the software, and are specifically charged to consider the safety and quality of the product, as opposed to simply checking the performance of the process. Because of this, they are able to provide an in-depth evaluation of the components they inspect. Unfortunately, due to the limited funding available, the full potential benefits have not been realized. Still, despite the limited resources, the Committee has found that the current implementation of IV&V in the Shuttle program is valuable and effective. The NASA Shuttle program office acknowledges that the IV&V effort, as practiced on the Shuttle flight software, has been valuable and effective.

The IV&V contractors have identified errors, including several Severity 1 errors,[14] that were not found by the embedded process. Among the 37 Discrepancy Reports authored or prompted by the IV&V contractors since the beginning of their contract, there were 12 Severity 1 errors and 3 Severity 1N errors. Also, the development contractors and NASA personnel interviewed by the Committee agree that other errors have been found or avoided through the close interaction of the IV&V teams with the software developers throughout the development process. Although the IV&V contractors are, by definition, independent, they interact with the software developers and other members of the flight software community throughout the process through their evaluation of Change Requests and Discrepancy Reports, through routine discussions with the developers, and ultimately through participation in the Shuttle Avionics Software Control Board, which is the final arbiter of software changes.

Although the current IV&V personnel are an integral part of the team, and so may be subject in part to peer pressure and potentially faulty group solutions, they provide a broad-based viewpoint and are specifically chartered to question group solutions from an independent stance. For example, the IV&V function specifically maintains an effort to examine the ways in which various parts of the primary and backup software interact. Included in the 37 Discrepancy Reports mentioned above were 4 Severity 1 reports on problems occurring between the primary and backup software. One of these involved a scenario that could have caused shutdown of all the Shuttle's main engines. The other three involved errors that could have caused the loss of the orbiter and crew if the backup software was needed during an ascent abort maneuver.

Ultimately, the value of the IV&V function, as it relates to the embedded process, is

---

[14] Shuttle flight software errors are categorized by the severity of their potential consequences without regard to the likelihood of their occurrence. Severity 1 errors are defined as errors that could produce a loss of the Space Shuttle or its crew. Severity 2 errors can affect the Shuttle's ability to complete its mission objectives, while Severity 3 errors affect procedures for which alternatives, or workarounds, exist. Severity 4 and 5 errors consist of very minor coding or documentation errors. In addition, there is a class of Severity 1 errors, called Severity 1N, which, while potentially life-threatening, involves operations that are precluded by established procedures, are beyond the physical limitations of Shuttle systems, or are outside system failure protection levels.

dependent on the aggressiveness and skill (e.g., the expertise, tools, and corporate knowledge) with which the IV&V contractors perform their work and their ability to remain independent and unbiased. The Committee understands that NASA's current plan is to eliminate the IV&V function but to retain a small portion of the systems engineering capability currently performed by the IV&V contractors. It is clear, however, that much valuable and probably irreplaceable expertise will be lost in scaling down to a lower level of effort, and the ability of the process to identify errors and determine appropriate solutions will be reduced. The Committee questions whether there are enough people assigned to this task at the present time. If the personnel are reduced further, the result may be that the entire effort becomes ineffective.

COST/BENEFIT CONSIDERATIONS

Even if a process is effective, there may be justifiable cost/benefit reasons for eliminating it. If the cost of the service exceeds its value, it should be eliminated. Clearly, the cost of the Intermetrics contract (which encompasses the work done by Smith Advanced Technologies) is a factor in the pending decision to eliminate IV&V. In an era when NASA is experiencing little real growth in its overall budget, and given the internal pressure to reduce costs associated with the Shuttle program, it is understandable that the Shuttle program office would seek to unburden itself of the current $3.2 million annual cost for IV&V. However, a true definition of the cost of eliminating IV&V must include the consequences of a failure of the software that results in a loss of life, causes the loss of a Shuttle,[15] produces a stand-down of Shuttle operations, or causes the loss of expensive hardware. In proportion to the potential losses, the cost of IV&V is clearly justified. The question reduces to one of determining where risk reduction resources are best placed when competing uses are possible.

Accurately assessing the risk of software-related accidents, or judging the risks of such accidents in comparison with other possible sources of risk, is not possible. Because a single error is sufficient to cause a serious accident, a decrease in the number of software errors detected is not a valid measure for confidence in the safety of the software or the process. Nor is the fact that no Shuttle accidents have resulted from software errors a cause for complacency. A more valid measure of risk is the fact that the IV&V effort has detected potentially catastrophic errors not caught by the embedded process. The recent incident aboard Endeavor[16] should serve as a warning that software, even at this stage in its life, can contain critical errors and that new errors can be introduced whenever the software is altered. Accidents, including,

---

[15] NASA has estimated that the Shuttle Endeavor, which was a replacement for Challenger, cost approximately $2 billion.

[16] A loss of expensive hardware nearly occurred during the recent (5/12/92) maiden flight of Endeavor (STS-49) as the crew attempted to rendezvous with and repair the Intelsat satellite. The software routine used to calculate rendezvous firings failed to converge to a solution due to a mismatch between the precision of the state-vector variables, which describe the position and velocity of the Shuttle, and the limits used to bound the calculation. The state-vector variables were double precision while the limit variables were single precision. The rescue mission was nearly aborted, but a workaround was found that involved relaying an appropriate state-vector value from the ground.

TABLE 2 Operational Increment Change History

Operational Increment	Description	Year of Incorporation	Lines of code (percent of total)[a]
OI-2	Rendezvous software, Spacelab software	1983	10,600 (1.8%)
OI-3	Redesign of main engine controller	1983	8,000 (1.4%)
OI-4	Payload re-manifest capabilities	1984	11,400 (1.9%)
OI-5	Crew enhancements	1984	5,900 (1.0%)
OI-6	Experimental orbit autopilot, Enhanced ground checkout	1985	12,200 (2.1%)
OI-7	Western test range, enhanced propellant dumps	1985	8,800 (1.5%)
OI-7C	Centaur	1985	6,600 (1.1%)
OI-8A	Post 51-L safety changes	1987	6,300 (1.1%)
OI-8B	Post 51-L safety changes, Bailout capability	1988	1,100 (0.2%)
OI-8C	System Improvements	1988	7,200 (1.2%)
OI-8D	Abort enhancements	1989	12,000 (2.0%)
OI-8F	Upgrade of general purpose computer (GPC)	1989	1,700 (0.3%)
OI-20	Extended landing sites, Trans-Atlantic abort code	1990	28,000 (4.7%)
OI-21	Redesign of abort sequencer, 1-engine auto-contingency aborts, hardware changes for new Orbiter	1991	32,000 (5.4%)

SOURCE: NASA Office of Space Flight

[a] Percentages based on the combined approximate sizes of the primary avionics software system (500,000 lines of code) and the backup flight software (90,000 lines of code).

in particular, Challenger, result at least in part from complacency arising from lack of problems in the past and the corresponding relaxation of protection mechanisms and procedures. Overconfidence in software is common and usually unwise.

The fact that the Shuttle software has yet to cause a serious loss is due primarily to the diligence of NASA and its contractors. Without this diligence, software could easily have caused serious, perhaps life-threatening and program-threatening problems. The Committee believes that elimination of IV&V at this stage in the program would serve to erode this

diligence.

The potential risk reduction functions of IV&V are particularly important in light of the proposed changes[17] to Shuttle hardware and operations and the likely effects on the software. Although it may seem that software reliability and safety should increase over time, this is not necessarily true; as software changes, its structure degrades and, over time, the people who were responsible for initial development of the software move on to other programs or retire. These two factors make it increasingly difficult to change the software without introducing errors.

Each new release of the Shuttle flight software includes significant additions to increase functionality or to fix errors that have been identified. Table 2 shows the number of lines of source code that were changed in each update (called "operational increments," or OIs) during the ten years of Shuttle operations. The two most recent updates (OI-20 and OI-21) included very significant changes to the code (4.7 percent and 5.4 percent of the total, respectively). The error experienced on the recent mission of Endeavor was introduced into the software as part of OI-21. In addition, both modified and aging hardware can create conditions not accounted for in the software. Experience has shown that it is in this environment that errors are most likely to be introduced and that off-nominal situations are most likely to arise. For example, when the software's original 16-bit addressing was changed to a new 20-bit format to take advantage of capabilities in the new general purpose computer (OI-8F), programmers incorrectly used address bits that were reserved for the processor's microcode. Executing these instructions would have caused branches to unknown locations. The IV&V contractors authored 5 Discrepancy Reports that identified illegal use of these address fields.[18] Thus, although it seems paradoxical, the risk of a software-related accident may very well increase as software evolves.

Considering the continued risk of a software failure, the consequences of a failure, and the benefits gained through IV&V, the cost of maintaining IV&V is small. Furthermore, the Committee has heard no specific proposals for alternative uses of the money that would be wiser than continuing IV&V as it is currently implemented. Proposals presented to the Committee, such as the implementation of the new HAL/S compiler and the Enhanced Software Product Assurance program proposed by the Safety, Reliability, and Quality Assurance office at the Johnson Space Center, were judged to be less important. Thus, it is the opinion of the Committee that the current implementation of IV&V provides important, low-cost insurance to the Shuttle program that materially reduces the risk of a software failure and, thus, of a software-related accident.

---

[17] In response to a written question from the Committee, NASA has stated that over the next five years several major changes to Shuttle hardware will be made. These include: the Advanced Solid Rocket Motor to replace the current solid rocket motor; the Multi-function Electronic Display System to replace the current displays and keyboards; implementation of the Global Positioning System (GPS) for on-orbit navigation; and numerous upgrades to implement Extended Man-Tended Capability to allow for much longer missions. Details regarding the changes to the software due to these hardware changes cannot be completely known until the hardware designs are completed. NASA has stated, however, that the upgrades will require changes to the ascent software, a new navigation program to process GPS data, and additions to the autoland program.

[18] These errors were classified as Severity 4 and Severity 5 errors since their resolution involved only changes to documentation and non-flight software (i.e., the HAL/S compiler). However, had the issue not been addressed, and the potential of causing branches to unknown locations remained, a more severe situation could have occurred.

ALTERNATIVES FOR IMPLEMENTATION OF IV&V WITHIN NASA

The primary reasons given by the Shuttle program office for wanting to eliminate the IV&V function, which they admit has been useful and effective, involve cost savings. The Committee has argued, in the previous section, that the cost versus benefit tradeoff justifies continued use of an appropriate form of IV&V. However, this does not address whether the same benefits could be achieved without using an IV&V contractor. This question of whether similar capability can be provided by organizations within NASA for lower cost prompted the Committee to investigate avenues other than the IV&V provided by Intermetrics and Smith Advanced Technologies.

Various members of the flight software community provide some degree of independence and technical capability. In particular, the Safety and Mission Quality Office at NASA Headquarters has the charter to oversee the safety and quality of Shuttle systems, including software. Accordingly, the Safety, Reliability, and Quality Assurance Office at Johnson Space Center has proposed a plan for taking over some, but not all, of the functions that are now performed as part of the IV&V effort. The Committee recognizes that the proposed plan is not meant to be a replacement for IV&V. The proposed plan emphasizes form over content and process over product. Under this plan, NASA personnel would check that the development contractor's processes were followed, but would not evaluate the software itself. Although such quality assurance activities can be valuable, they do not provide the same benefits as IV&V.

A possible option, although not one that the Committee recommends, would be for the Safety and Mission Quality Office to take over *all* the functions currently being performed by the IV&V contractors and, thereby, provide the same service. There are two reasons why, in the opinion of the Committee, this is not a viable approach.

First, the Committee was informed that neither the Safety and Mission Quality Office at Headquarters nor the Safety, Reliability and Quality Assurance Office at Johnson Space Center have the personnel, the expertise, or the tools to replace the capabilities of the current IV&V effort. Thus, if an attempt were made to fully duplicate the IV&V function, there would necessarily be a significant time lag between the phase-out of the current IV&V function and the development of a corresponding capability elsewhere in the agency. For example, the plan presented to the Committee, which includes replacing only part of the current IV&V functions, will not be in place until well after the time when the current IV&V is scheduled to be eliminated.

Second, if another organization within NASA were to attempt to duplicate the capabilities provided by the current IV&V effort, they would be required to increase their personnel accordingly, develop or acquire software verification and validation tools similar to those used by the IV&V teams,[19] and provide appropriate facilities for housing the personnel and equipment. While the Committee was not constituted to evaluate the relative expense of

---

[19] Intermetrics has acquired or developed numerous tools specifically for Shuttle software. These include tools tailored for the IV&V task that check cross-references and data dependencies, compare source code listings, and identifiy absolute addresses. Intermetrics also has several tools that apply to the specific programming languages (HAL/S and AP101 assembler) used in Shuttle software development.

developing and maintaining such capability within NASA, it fails to see how making such a change could result in a net savings.

The Committee was told that no organization within NASA has the expertise or the manpower to replace the current IV&V function in a timely fashion, and the Committee believes that building this expertise elsewhere will not necessarily reduce cost. **Thus, the Committee does not recommend moving IV&V functions to other organizations within NASA unless the current IV&V is maintained for as long as it takes to build comparable expertise in the replacing organization.**

RECOMMENDATIONS

Based on evaluation of the presentations and documents given to the Committee, and considering the Committee's own industrial and academic experience and knowledge, the Committee concludes that the current IV&V process, as defined and practiced for the Space Shuttle software, is effective and that cost/benefit and risk considerations do not justify its elimination from the fiscal year 1993 budget. Furthermore, the Committee concludes that the Space Shuttle software development process is not adequate without current IV&V practices and their elimination will adversely affect the overall quality and safety of the software, both now and in the future.

Accordingly, the Committee recommends that NASA:

1. **maintain the currently implemented independent verification and validation for Space Shuttle flight software; and**

2. **not transfer IV&V functions to other organizations within the agency unless the current IV&V effort is maintained for as long as it takes to build comparable expertise in the replacing organization.**

Further recommendations regarding the development process for Shuttle flight software, including an evaluation of the embedded V&V process and a comparison with other, similar processes, will be contained in the Committee's final report.