D7

N85-16896

DEVELOPMENT AND IMPLEMENTATION OF THE VERIFICATION PROCESS FOR THE SHUTTLE AVIONICS SYSTEM

H. E. Smith
NASA Lyndon B. Johnson Space Center
Houston, Texas 77058

W. B. Fouts and J. Mesmer
Rockwell International
Downey, California 90241

ABSTRACT

The paper examines the background of the Shuttle avionics system design and the unique drivers associated with the redundant digital multiplexed data processing system. With flight software pervading to the lowest elements of the flight-critical subsystems, it was necessary to identify a unique and orderly approach of verifying the system as flight-ready for STS-1. The approach and implementation plan is discussed, and both technical problems and management issues are dealt with. A summary of "lessons learned" completes the presentation.

BACKGROUND

Before addressing the subject of this paper, it would be worthwhile to summarize the salient features of the Shuttle avionics system in preparation for the subsequent discussion (fig. 1).

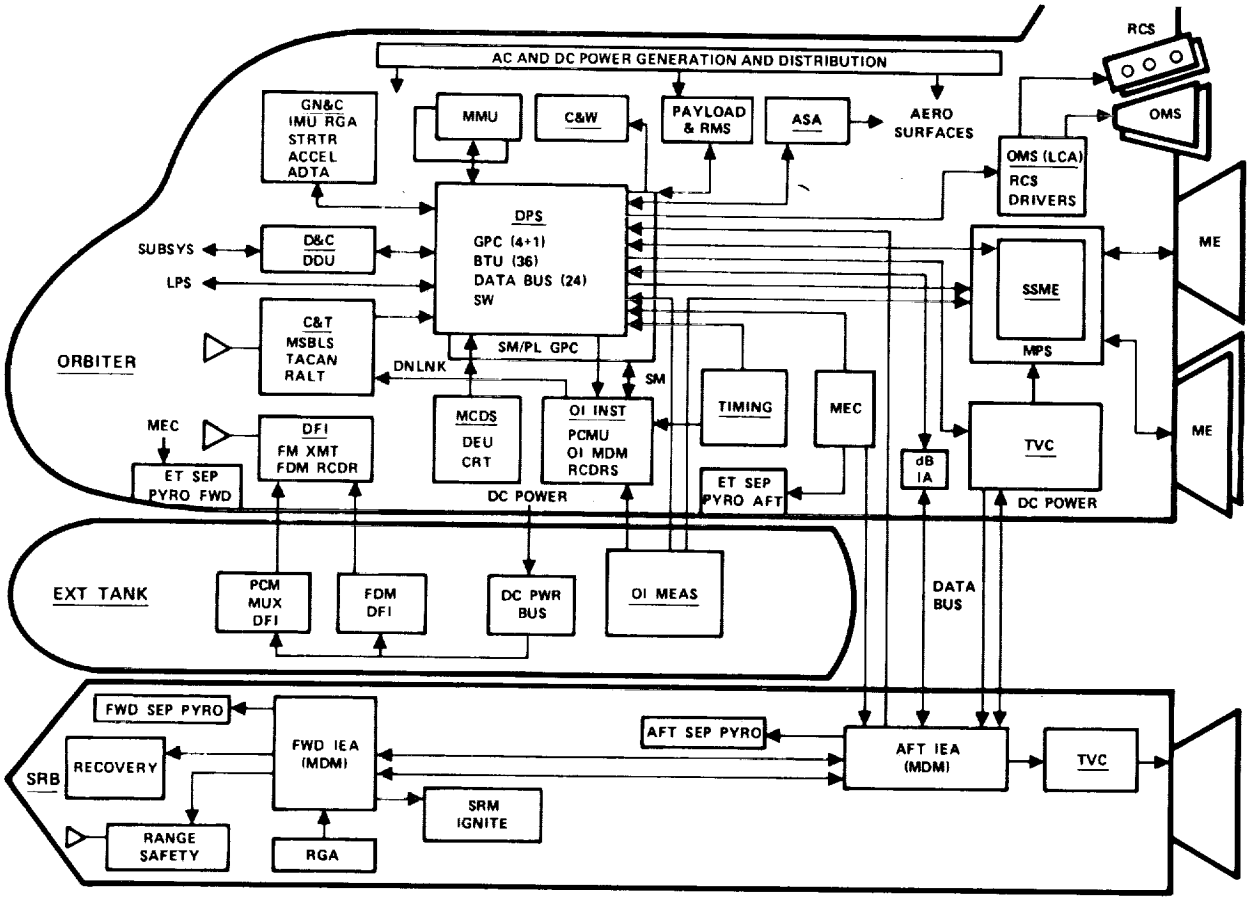

FIGURE 1.- AVIONICS SYSTEM FUNCTIONAL DIAGRAM.

1. The primary flight system (PFS) design is based on a centralized set of quad-redundant general-purpose computers (GPC's) within the data processing system (DPS) which provides the primary mode of acquiring flight-critical sensor data, processing the data, and, finally, generating and delivering guidance, navigation, and control (GN&C) commands to the various vehicle control elements (fig. 2).

2. Additionally, a single GPC with independently designed and coded flight software, called the backup flight system (BFS), is available to take over vehicle control through the primary bus structure from the PFS, if necessary.

3. The DPS bus structure contains 24 separate serial digital input/output (I/O) buses including 8 flight-critical (GN&C) and 5 intercomputer (ICC) buses, which provide for sensitive data communications and control through the GPC redundant set.

4. The various multiply redundant inertial navigation and flight control sensors and effectors must be in a constant state of readiness to perform the fault detection, isolation, and reconfiguration (FDIR) functions.

5. The avionics and nonavionics system management (SM) function is performed in conjunction with the operational instrumentation (OI).

6. A three-string electrical power distribution and control system provides single fault-tolerant power to non-flight-critical systems and dual fault-tolerant power to flight-critical systems (fig. 3).

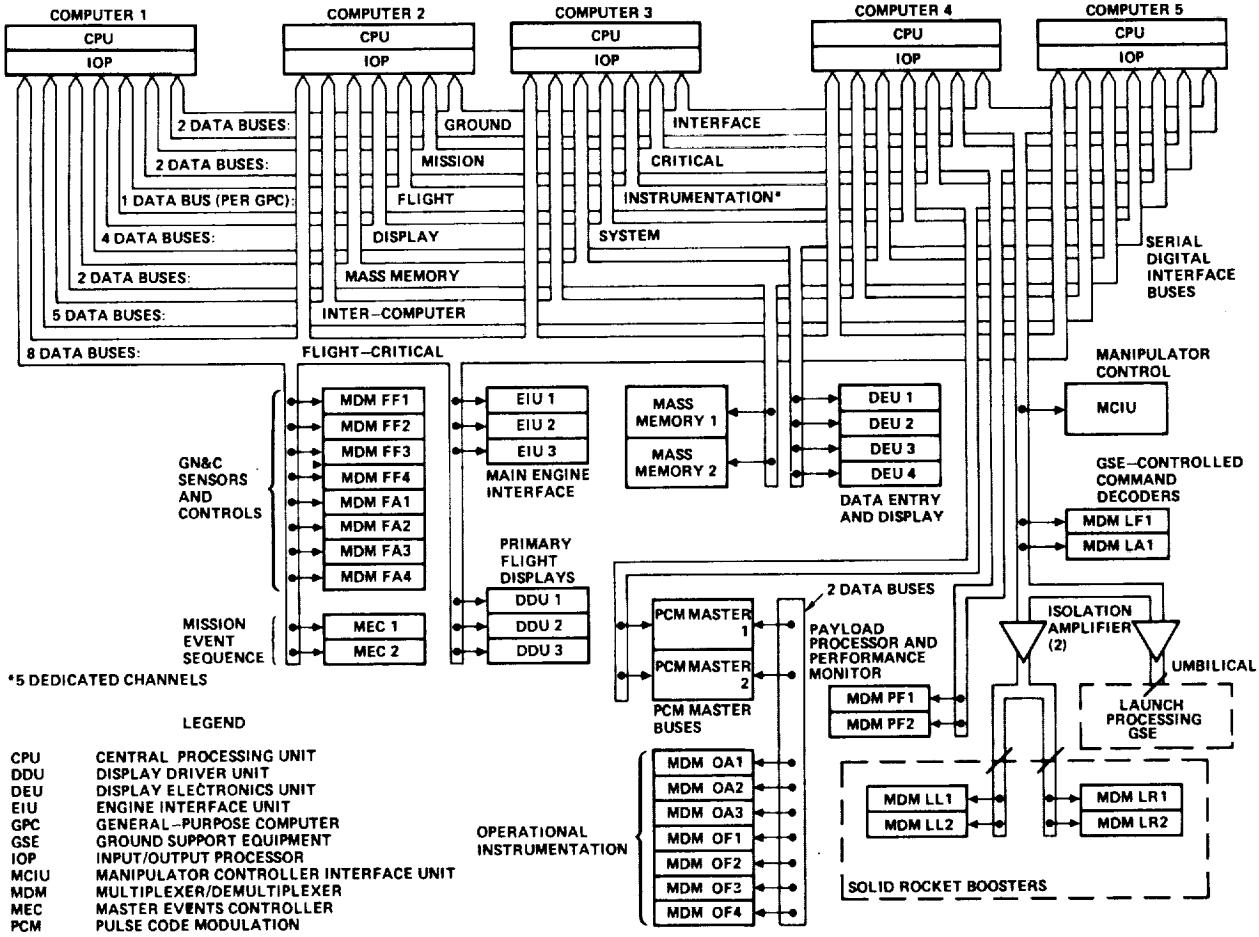

FIGURE 2.- ORBITER DATA PROCESSING SYSTEM.

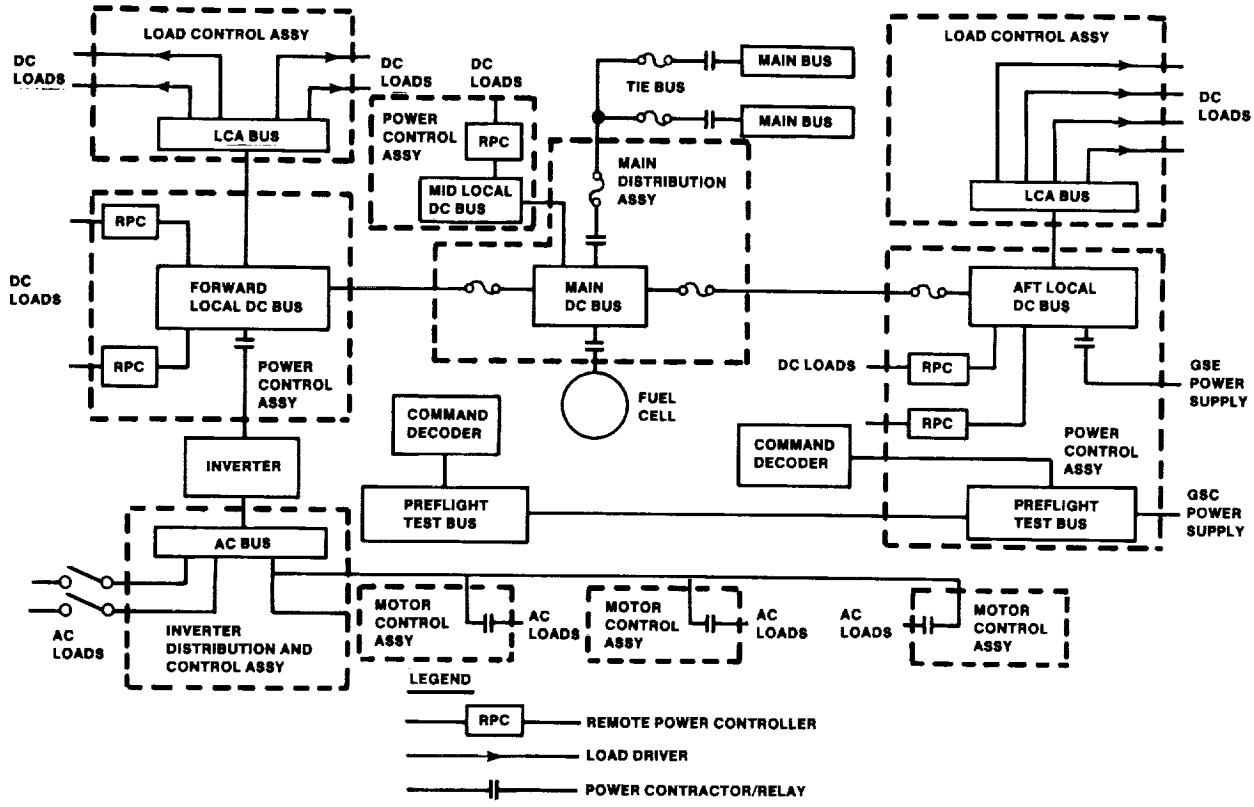

FIGURE 3.- ORBITER POWER DISTRIBUTION, SINGLE STRING.

During the early years of the Space Shuttle Program, the avionics system was defined and understood with regard to design requirements from the top downward, and it was assumed that the methods used for system certification during the Apollo Program would suffice for the Shuttle. However, it became apparent, as the various subsystem designs matured, that software would be increasingly dominant in the system functions. In fact, the flight software would pervade throughout multiple levels of the various elements as evidenced in the GN&C system (fig. 4).

With the significant improvements in capability of digital flight computers, the increasing importance of software within a hardware design was not unexpected. The unexpected factor was the time phasing of the software code design and development, which, because of the need to understand first the hardware design and operating characteristics, lagged behind the hardware in subsystem test readiness. A significant dilemma that emerged was a means of testing and certifying the lower level subsystem elements in a reasonable time phase in the program with already developed hardware and immature flight software.

The complexity of the problem became apparent during laboratory testing of the various avionics subsystems which were to be employed in the Orbiter 101 (Enterprise) Approach and Landing Test (ALT) Program at Edwards Air Force Base in 1977. During the laboratory test period, which preceded the flights by a year, concern was generated because of confusion arising in the following areas.

1. The scope of hardware certification, which generally was thought to be stand-alone line replaceable unit (LRU) (i.e., black box) testing, and its relationship with subsystem- and system-level function and performance testing, usually requiring some of the flight software elements in combination with hardware LRU's

2. The scope of testing necessary to declare the system ready to fly as compared to the test and analysis necessary to provide specification compliance

3. Visibility of the requirements to meet both flight-readiness and specification compliance

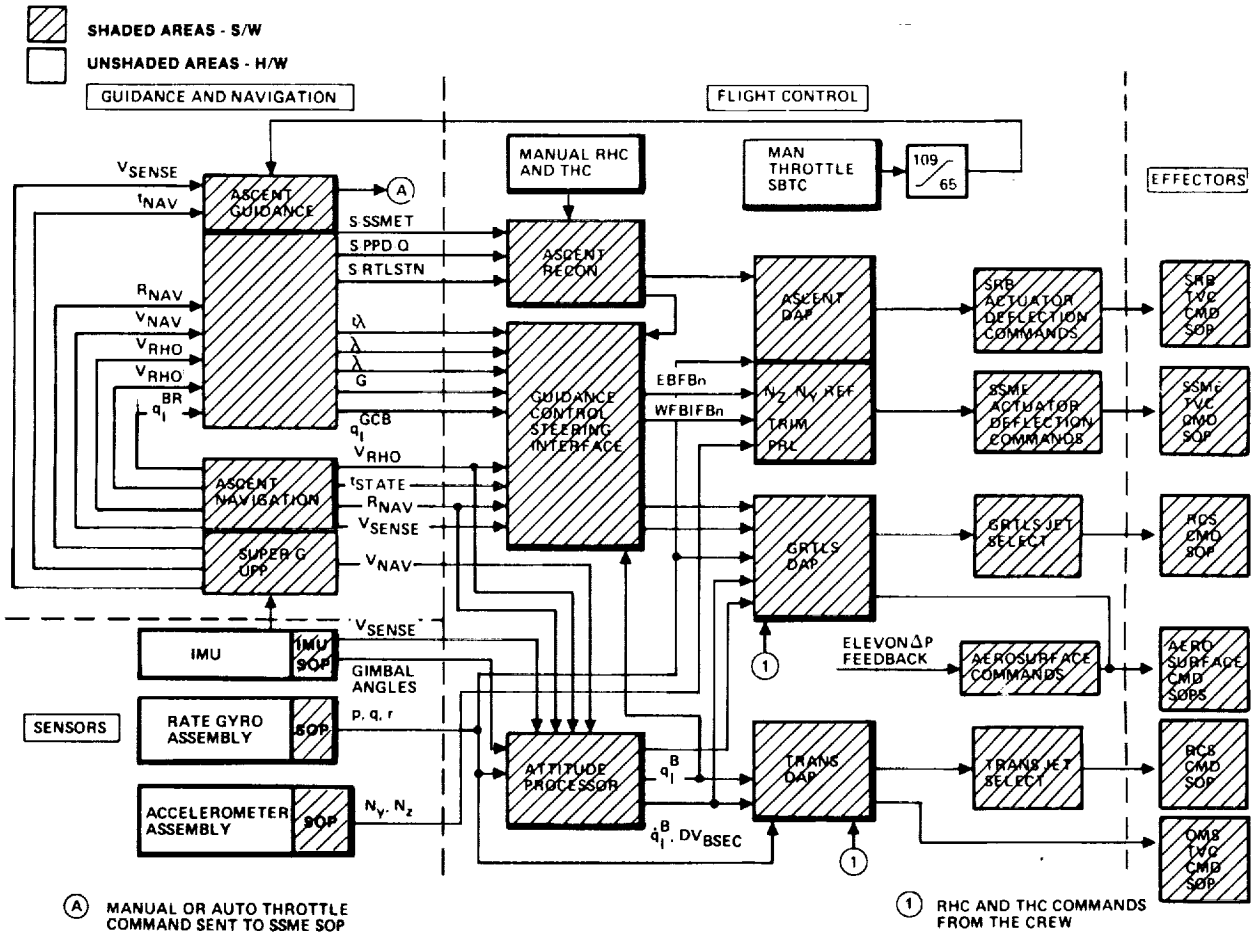

FIGURE 4.- ORBITER GUIDANCE AND CONTROL ELEMENTS.

In 1978, following the ALT Program, several members of Rockwell and NASA engineering management met for the purpose of addressing the previously mentioned problems before the onset of Orbital Flight Test (OFT) preparations. At the meeting, it was decided (1) to modify the scope and relationship of the Orbiter LRU certification and necessary subsystem- and system-level avionics tests and analyses, hereinafter called verification, (2) to differentiate between mission-to-mission flight readiness during OFT and operational readiness indicated by specification compliance, and (3) to develop a mission-to-mission verification process with adequate rigor and visibility necessary to identify the specific requirements to meet flight readiness during OFT.

GENERAL APPROACH

To establish a verification process, it was first necessary to establish the relationship between hardware and software. In the case of the Orbiter DPS, flight software elements which were commonly resident in the GPC's supported the lowest level hardware LRU's. To treat these software elements, which effectively stand alone in function, and their hardware LRU counterparts as functioning subsystems, the software elements were also called LRU's. Simply stated, verification may be defined as higher level tests and analyses above the LRU certification level necessary for compliance with predefined requirements. For purposes of Shuttle avionics verification, the various levels range from the lowest stand-alone functional element (actuation subsystem) to the highest level of integrated vehicle elements (mated Shuttle vehicle), as shown in figure 5. This definition also infers that the avionics verification process would transcend project-level boundaries between the various vehicle elements and would, indeed, be an integrated avionics verification process.

As a result of the 1978 discussions, it became apparent that it was neither necessary nor possible to complete all verification tests and analyses required to achieve specification compliance before the first OFT flight (STS-1). Instead, it was decided to address flight-readiness verification on a mission-by-mission basis. The cumulative mission verification effort coupled with a defined analytical effort became the building blocks to complete specification compliance verification (fig. 6). Finally, it was evident, because of the system complexity, that a highly visible and rigorous process must be in place to assure that the necessary tests and analyses had been completed to provide confidence in declaring system flight readiness.

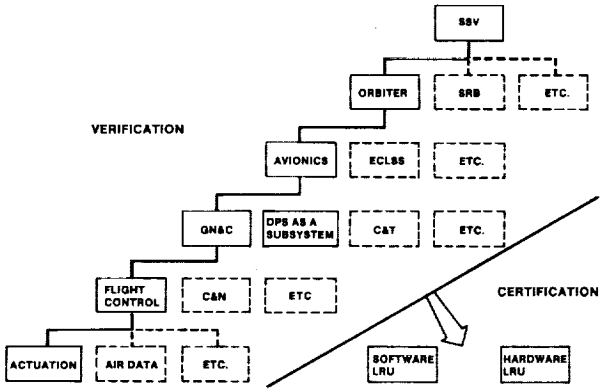

FIGURE 5.- SHUTTLE LRU CERTIFICATION AND SUBSYSTEM- AND SYSTEM-LEVEL VERIFICATION.

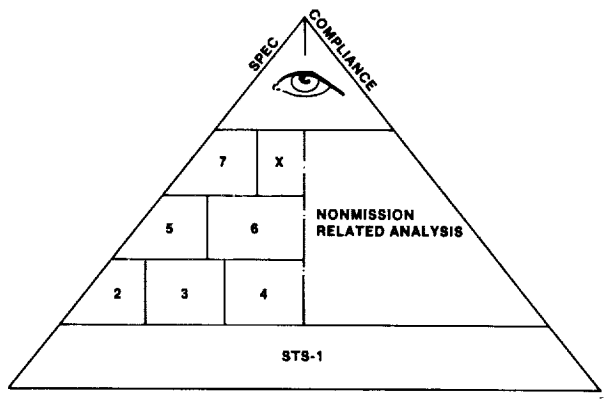

FIGURE 6.- RELATIONSHIP OF FLIGHT-READINESS VERIFICATION TO TOTAL VEHICLE SPECIFICATION COMPLIANCE VERIFICATION.

In the case of the DPS and the GN&C system, the design teams were in place and were sensitive to the relationship of their respective technical disciplines with the integrated avionics system. This was not necessarily the case for the nonavionics disciplines, for which sequencing, control, and system management functions for power generation, mechanical, and propulsion systems were provided as a service by the DPS. To provide verification requirements visibility within the nonavionics systems, three-man subsystem teams, consisting of one each software, hardware, and test specialist familiar with each of the subsystem designs, were formed. They were responsible for using the various subsystem specification and design documents to define a bottom-upward approach to the verification requirements.

In the case of all systems, as the requirements were identified, they were mapped, using as a reference hardware, drawings, software specifications, certification, qualification test, acceptance test plans, and designer insight. The resulting "roadmap" identified the type of analysis, laboratory, and/or flight vehicle test necessary to accomplish verification for that specific element, function, or subsystem. Each roadmap stood alone but provided the foundation for higher level elements in the verification tree (fig. 7). Each roadmap evolved into a verification plan which was jointly negotiated between the Rockwell sponsor responsible for design and acceptance in the respective technical discipline and the NASA counterpart. Tests and analyses were conducted and results jointly reviewed by the sponsors. The final conclusions were documented in a Verification Completion Notice (VCN), which was signed by the sponsor counterparts. The resulting documentation (verification plan, VCN, and associated test and data requirements documents) provided the desired rigor and traceability to the process.

In summary, the role of the technical sponsors was the keystone to the verification process. Each was charged with the responsibility of defining the verification requirements, determining the method of test or analysis to meet requirements, defining the criteria for test site acceptance, determining the data requirements for the tests, determining the pass-fail criteria for those data, resolving test anomalies, reporting the test results, and, finally, determining the flight readiness of his function or element. It is now appropriate to describe the technical and management tools necessary to make the verification process work.

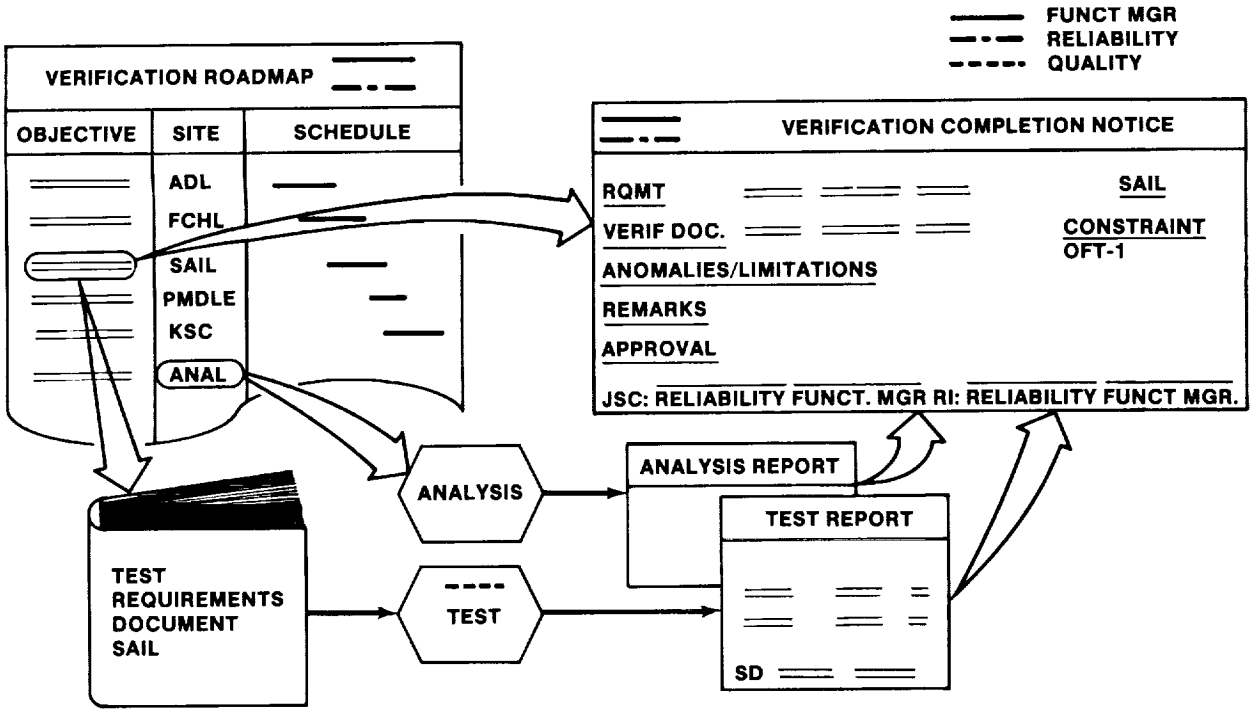

FIGURE 7.- OFT FLIGHT-READINESS VERIFICATION PROCESS.

DESIGN VERIFICATION APPROACH

The avionics design verification approach employed the following methodology.

1. Divide the total avionics system into technical disciplines.

2. Utilize the best technical resources for verification; i.e., assign the best technical personnel as verification sponsors for each technical discipline and determine the best combination of test and analysis tools for the job.

3. Establish a framework for avionics integration.

Figure 5 shows the application of this logic tree process to the lowest levels. As a basis for the verification, the sponsors treated both the hardware and the software LRU's as flightworthy elements; i.e., the hardware LRU's were certified to withstand the flight environments, and software was independently tested to show requirements compliance.

The sponsor's challenge was to demonstrate the flightworthiness of his respective hardware or software element to accomplish the mission. The following tools were used as appropriate.

1. Hardware and software laboratories and test facilities

2. Analysis programs

3. Airborne test articles

4. Shuttle flight vehicle prelaunch testing

The use of the flight vehicle was very restricted. The strategy was to perform the bulk of verification through laboratory testing and analysis.

HARDWARE AND SOFTWARE LABORATORIES AND TEST FACILITIES

The Flight Systems Laboratory (FSL) at Downey, California (fig. 8), and the Shuttle Avionics Integration Laboratory (SAIL) at the NASA Lyndon B. Johnson Space Center (JSC), Houston, Texas (fig. 9), had been developed as the primary test facilities for avionics verification. Because of avionics system complexity and for schedule considerations, the SAIL was developed for the ascent flight phase and the FSL was developed for the descent flight phase. The FSL and the SAIL shared the on-orbit verification. Both facilities provided system-level open- and closed-loop capability, and SAIL possessed a complete set of flight-type avionics hardware and cable harnesses.

Other hardware test facilities included the Flight Control Hydraulic Laboratory (FCHL), the JSC Electronics Systems Test Laboratory (ESTL), Thiokol, the Main Propulsion Test Article (MPTA), and the NASA George C. Marshall Space Flight Center (MSFC) Main Engine Simulator. Using these facilities, the sponsor would typically develop and validate math models, establish open- and closed-loop function and performance, and confirm hardware-to-hardware and hardware-to-software compatibility. Before a facility was used for formal verification, the sponsors performed site acceptance testing using off-line analytical data as a reference. Site acceptance provided sponsor confidence in facility representation of the flight article.

ANALYSIS PROGRAMS

The sponsors used analysis programs to confirm stability and to verify dynamic performance considering nominal and off-nominal conditions. The sponsors developed the analysis programs in parallel with the system design, development, and verification testing. The fidelity of the analysis programs was updated by correlating their performance with test results. Eventually, the analysis programs became key off-line analysis tools that could repeat test results and expand operating conditions by parametric changes to establish envelopes about the design nominal. These analysis tools effectively supplemented the hardware test articles for complete system verification.

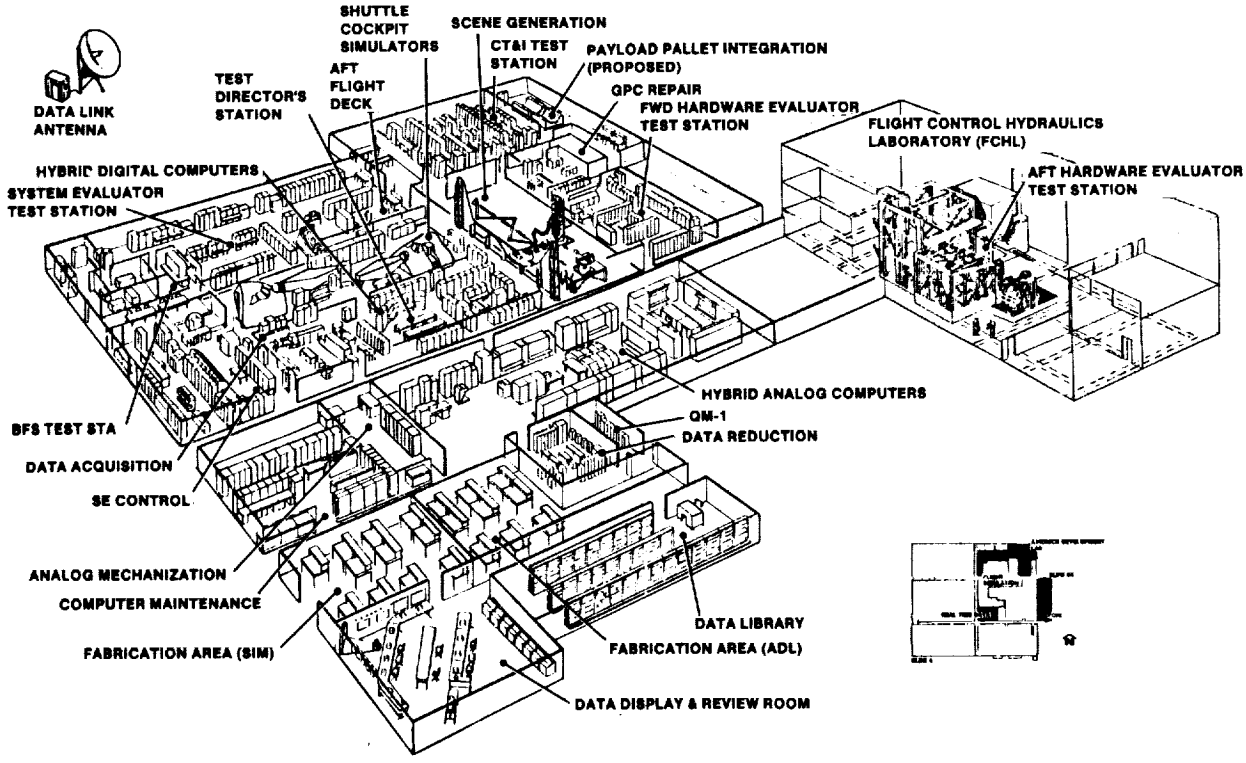

FIGURE 8.- FLIGHT SYSTEMS LABORATORIES.

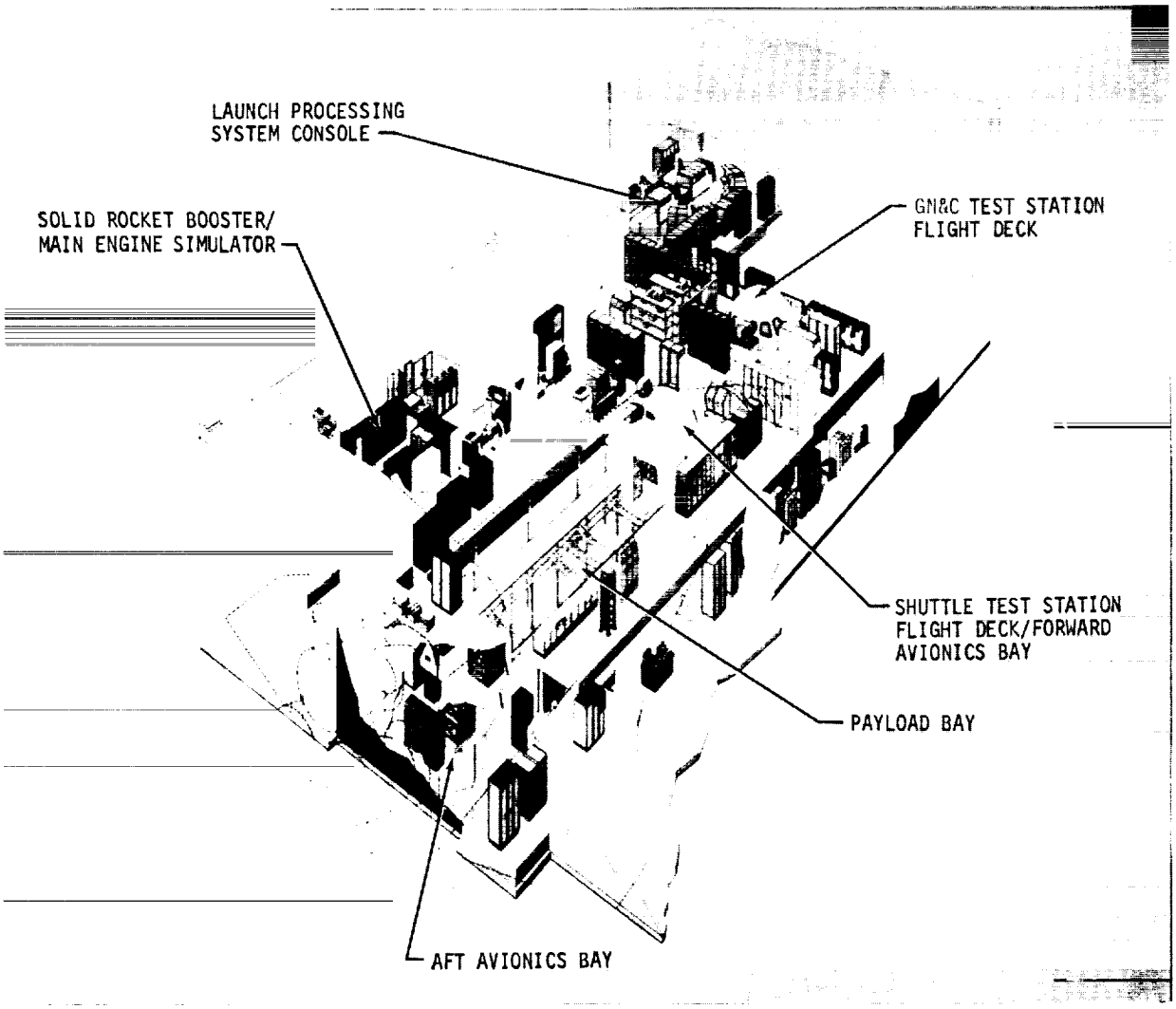

FIGURE 9.- SHUTTLE AVIONICS INTEGRATION LABORATORY.

AIRBORNE TEST ARTICLES

The Shuttle Training Aircraft (STA) and the SR71 flight test program supplemented avionics verification by providing in-flight characteristics to enhance sponsor understanding. Limited but valuable flight insights were derived through use of this technique.

SHUTTLE FLIGHT VEHICLE PRELAUNCH TESTING

Ground testing of the actual vehicle to be flown provided an extremely beneficial understanding of specific flight vehicle characteristics. In addition to the rigorous ground checkout process, which was an independent key element for committing to flight, specific verification ground tests were accomplished on the flight vehicle. These tests required a higher level of assembly and integration than could prudently be accomplished in a laboratory. End-to-end flight control tests, dynamic stability verification, and simulated integrated mission runs were typical types of tests. Because these tests used both flight hardware and flight software, extremely high preflight confidence in the integrity of the flight article was obtained.

To complete the framework for the avionics integration, a challenge emerged which required the NASA and contractor institutional managers to coordinate their various technical resources and meet a time-critical flight-readiness schedule.

MANAGEMENT CHALLENGE

Because the various elements of the integrated avionics system were being developed by three NASA field centers and numerous contractors, it was necessary to provide some means of unified control. The myriad of diverse program elements (fig. 10) had to be integrated by a process capable of developing the confidence necessary to ensure that the avionics hardware and software system was ready for flight within a defined time schedule. The control mechanism had to be capable of providing communication among the various program elements, system technical areas, and program management. It also had to be capable of controlling all aspects of the avionics verification process without restricting the feeling of personal accountability. In addition to providing for program biases, the management function also had to be responsible for assuring availability of the tools necessary for providing the test and the analysis data base required for proof of system flight readiness.

Taking into account these fragmented but critical activities, the complexity of the avionics system, and the magnitude of verification requirements, it was necessary that specific management controls be provided. These included the following.

1. Obtain and maintain the commitment from the technical sponsors to do the verification job.

2. Provide interface between the program elements.

3. Allocate test facility resources.

4. Resolve issues.

5. Secure flight-readiness commitment from the sponsors.

6. Provide program management with focused visibility of verification progress and bring forth unresolved issues.

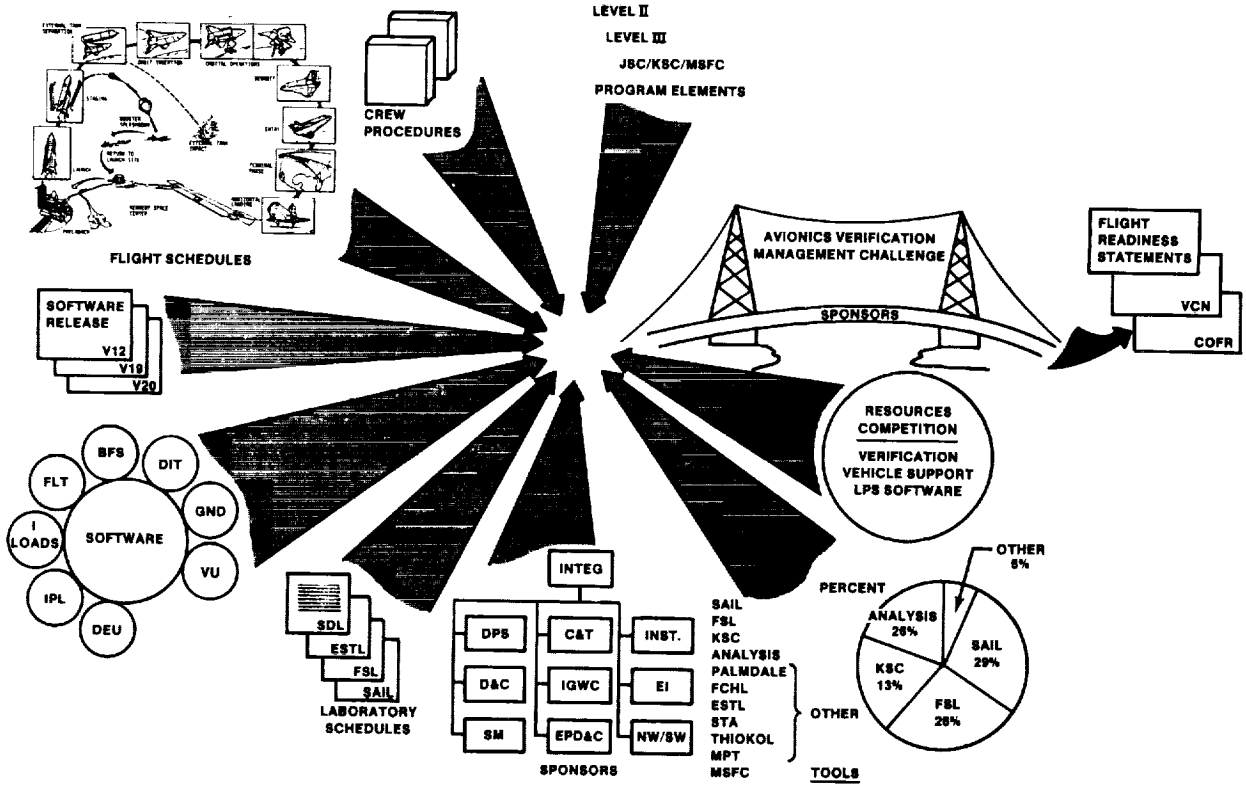

FIGURE 10.- MANAGEMENT CHALLENGES.

Early in 1978, the avionics verification management was established to provide these controls. It encompassed all aspects of avionics verification and was focused through a management review team, which presided over and administered the avionics verification activities. The team consisted of managers from each aspect of avionics verification, as follows.

Management Working Group (MWG) Membership

NASA	Rockwell
Systems Engineering	Systems Engineering
SAIL	FSL
NASA John F. Kennedy Space Center (KSC) Engineering	SAIL
GN&C Engineering	KSC Engineering
Flight Software Engineering	

The MWG was provided with tools to assure their ability to control the process. These tools consisted of the following.

VERIFICATION LOGIC TREE

The verification logic tree (fig. 11) defined the scope of avionics verification. It provided a single source to relate the individual subsystem function to other elements in the integrated avionics system. Each subsystem function is depicted in a block on the tree; relationships of subfunctions are listed below each block. The tree provides a "bottom-up" hierarchy of subsystem functions (such as flight control) to the higher functions (such as descent GN&C) and then to the top function (integrated avionics). The verification logic tree provided a reference tool with which to measure the verification progress, to establish priorities, and to determine areas requiring additional emphasis.

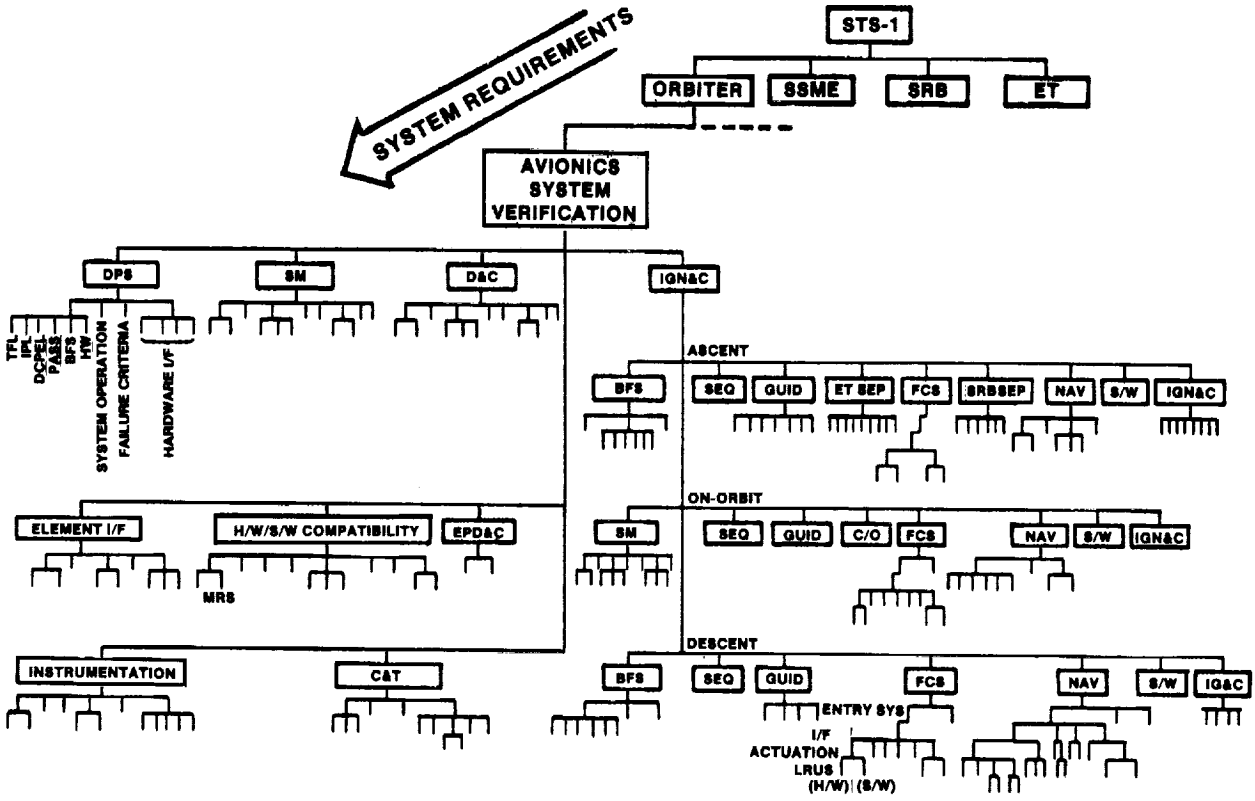

FIGURE 11.- AVIONICS VERIFICATION LOGIC NETWORK.

INDIVIDUAL ACCOUNTABILITY MATRIX

Related to the verification tree was the matrix of sponsor accountability. As previously mentioned, success of the verification process depended on the involvement of the avionics system design personnel. This involvement was assured by developing an accountability matrix based on the verification logic tree and assigning the appropriate NASA and Rockwell counterparts to each subsystem or function and by obtaining commitments from line management that avionics verification sponsorship was truly the individual's assigned task. In other words, the process was totally reliant on the design community for the technical effectiveness of avionics verification. Without the commitment of the proper personnel to the process and the backing of the process by program management, it would not have been possible to integrate and manage the effort required for commitment to flight readiness.

MANAGEMENT WORKING GROUP

The MWG was the forum for administering the avionics verification process. It met weekly by teleconference to review progress of avionics hardware and software system verification and to resolve issues impacting the process as shown in figure 12. Specifically, the functions of the MWG were as follows.

1. Review and baseline the verification tests for each flight.

2. Review and approve changes to the baseline for new requirements (mission changes, software changes, or delivery schedules).

3. Establish test priorities.

4. Review laboratory schedules.

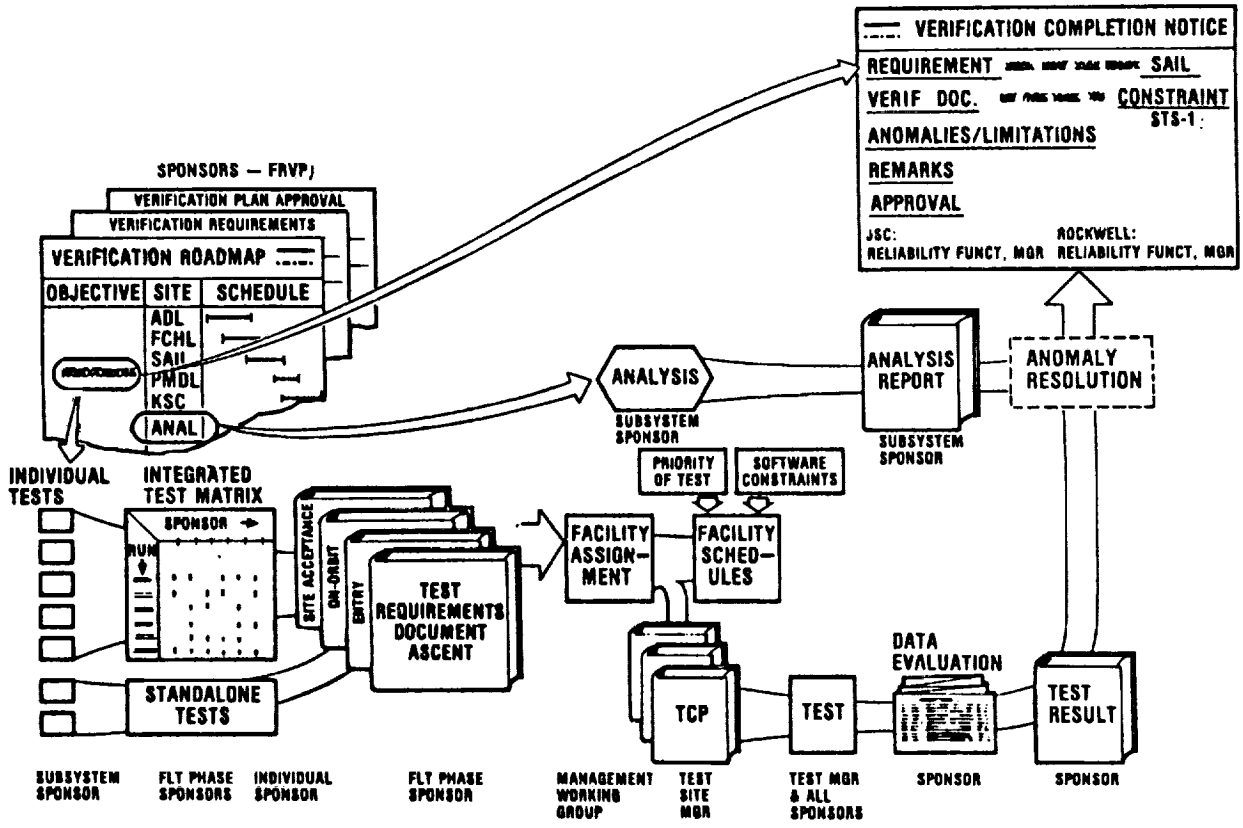

FIGURE 12.- VERIFICATION PROCESS FLOW AND DOCUMENTATION SUMMARY.

5. Identify laboratory problems, hardware availability issues, and manpower assignments that must be taken to program management for resolution.

6. Review verification issues.

The MWG provided the medium for sponsor interface with the laboratories, JSC, KSC, and MSFC. The MWG was co-chaired by Rockwell and NASA, and decisions of the MWG Board constituted direction to the verification community to proceed. Any issues which carried impacts beyond the verification community were taken forward to program management for disposition.

FLIGHT READINESS VERIFICATION PLANS

The Flight Readiness Verification Plans (FRVP's) provided traceability to the sponsor's verification requirements and consisted of three parts: (1) verification roadmaps, (2) verification requirements, and (3) an approval sheet. The verification roadmap identified the verification tasks, the test site, and the planned schedule for the tests. The verification requirements sheet defined each verification task in general terms and assigned a tracking number to each task. The tracking number was used to provide traceability from the VCN back to the FRVP. The approval sheet was signed by Rockwell and NASA counterparts after the plan and the details had been coordinated. The FRVP, in conjunction with the verification logic tree, defined the total task, which, when completed, would provide a data base sufficient to permit signoff at each level of the commit-to-flight process. These two documents provided the MWG with the necessary criteria for evaluation of the criticality of remaining effort.

SUMMARY - WITH REFLECTIONS

The resulting verification process culminated in an intense but orderly effort which provided the necessary confidence in the Space Shuttle avionics system to perform the STS-1 mission. The process remains in place today and is providing the necessary incremental verification to determine flight readiness for subsequent flights.

Throughout the effort leading to the first flight, the process provided the means for successfully resolving the conflicts which occurred during the integration of this complex system. Typical were the significant problems discovered within the Orbiter entry flight control system during initial verification testing. A resulting major redesign within the flight software required major replanning and schedule changes. During this period, the working relationships among the verification sponsors (designers), the laboratory test teams, and the flight software design and test personnel led to mutual respect for the common objective: "Get the avionics system ready to fly!" Their commitment to that objective minimized the conflicts that had to be resolved. Had management, early in the program, understood the impacts of software involvement throughout the avionics system, the logjam of concurrent subsystem- and system-level testing resulting from late release of flight software might have been minimized. As it was, the process lessened the logjam by integrating subsystem requirements into system-level test runs. The message, however, remains: "In future programs, the subsystem designs should acknowledge the need for an up-front verification strategy which minimizes the labor-intensive laboratory test effort."

Finally, the need to involve the designer personally in the flight-readiness verification process for future programs needs to be acknowledged. This involvement includes not only the planning phases of the verification but also the final decisions of system flight readiness. With the increased interaction of future flight systems, the individual designers must be accountable for the readiness of their respective elements for flight.