Independent Verification and Validation of Software for Weapon Management System of a High Performance Aircraft

Sudha Srinivasan, Rekha.R, Dr.K.Karunakar
IV&V, Aeronautical Development Agency, Bangalore, Karnataka, India

Abstract - The failure of safety critical embedded software is unacceptable be it for safety, security or economic reasons. The risk of software failure in complex embedded systems is overcome by using the Independent Verification and Validation (IV&V) technique. The process of IV&V and its planning needs to be initiated early in the development life cycle of the weapon management system for a high performance aircraft. In the present context, the aircraft has so far achieved successful integration and release of Air-to-Ground weapons and Air-to-Air close combat missiles. The above functionalities are achieved by complex embedded software systems which constitute the weapon management system for which advanced IV&V techniques have been used to remove errors during development phase. The methodology used for performing IV&V of software for weapon management system has been discussed in this paper.

Keywords: Independent Verification and Validation, Safety Critical Embedded System

1 Introduction

Software IV&V is a systems engineering process employing rigorous methodologies for evaluating the correctness, quality and safety of the airborne embedded systems throughout the software development life cycle. It provides for the early detection and identification of risk elements. The program is then able to take actions to mitigate these risks early in the life cycle.

The IV&V Program plays a key role to identify, understand and mitigate risks associated with the safety critical systems, increase the probability of success of the mission as a whole while reducing software errors, development cost and development time.

The weapon management system is a high integrity software system which manages the integration, preparation, selection and firing of Air-to-Ground Weapons and Air-to-Air Close Combat Missiles.

In this paper, the method used for performing the IV&V of the weapon management system of a high performance aircraft which is categorized as an airborne safety critical embedded system is discussed. The importance of carrying out the compiler validation, evolving the coding standards and performing the independent verification and validation of the Programmable Logic devices, INSITU software, device driver software and acceptance test software for hardware is discussed apart from the method used for performing the IV&V of the application software of the embedded system. The architecture and system details of the weapon management system is however not discussed in this paper since this paper emphasizes on the work carried out for the IV&V of weapon management system , which can be followed as a generic approach for performing the IV&V of any safety critical airborne embedded system.

Outline of this paper is as follows: section 2 describes the Independent Verification and Validation, Section 3 describes IV&V of application software, Section 4 describes the IV&V of hardware related software, Section 5 describes the coding standards and compiler validation and Section 6 summarizes this paper.

2 Independent Verification & Validation

In the modern high performance aircraft, when the initial design was perceived, many safety and mission critical functions were planned to be implemented in software which amounted to many embedded software systems.

In order to ensure safe flight and error free performance, the technique of IV&V was adopted and has pioneered in the country from the year 1990 in order to bring out new techniques and new methods to evaluate complex systems.

The three types of independence required for an effective verification and validation process identified for the IV&V of weapon management system software are:

Firstly , Technical independence where the members of the IV&V team are not involved in the development of the software and this team works with an unbiased approach in learning about the system requirements, proposed solutions for building the system, and problems encountered. Technical independence of the IV&V team is crucial in the team's ability to detect the subtle software requirements, software design, and coding errors that frequently escape detection during development testing and Software Quality Assurance reviews.
Secondly, Managerial independence where the IV&V team independently decides the areas of the software or system to be analyzed and tested, the IV&V techniques to be conducted, schedule of tasks (within the framework of the system schedules) and technical issues to act upon. The IV&V team provides its findings in a timely fashion to the development team who act upon the reported discrepancy and findings.

Thirdly, financial independence is achieved with the budget being allocated by programme management and controlled at high level such that IV&V effectiveness is not compromised. This independence helps in usage of appropriate tools and preventing the delays of IV&V analysis and timely reporting of the results.

The focus of the IV&V objective is accomplished by providing value-added, high quality, technical assurance that the safety critical system being used is meeting its requirements in terms of the technical, safety, security, and reliability objectives of that mission.

3 IV&V of Application Software

Incremental approach is followed for the IV&V of the application software of the weapon management system. The IV&V of the software life cycle artifacts for the application software are carried out incrementally for each weapon integrated to the aircraft. Regression analysis and testing is carried out when there is a change in requirements. Finally the IV&V with the integration of all the weapons is carried out.

Figure 1 represents the independent verification and validation process which is followed for the application software of the weapon management system.

![Figure 1: IV and V Process](image)

The IV&V of application software begins early in the life cycle, when the user requirements are captured and continues till the system testing is completed successfully without errors. As a part of the IV&V activity in the software requirements phase, the correctness of the allocation of system requirements to software is checked along with the correctness, completeness, non-ambiguity and testability of the software requirements.

Concurrently with software requirements IV&V, software system test planning is initiated. All the proposed testing for the system to ensure comprehensive testing and planning of appropriate resources are carried out. The Software Requirement Specification (SRS) and Interface Requirement Specification (IRS) documents supplied by the development team are analyzed and traceability to the system requirements documents are checked in order to ensure completeness.

The software design IV&V activities occur after the software requirements have undergone the software IV&V process and the software design or an increment of the software design is completed.

The software IV&V tasks of traceability, evaluation and interface analysis provide assurance that software requirements are not misrepresented, incompletely implemented or incorrectly implemented. By verifying that the software design meets its software requirements, the software design IV&V activity also supports validation that the software design meets system requirements. Code walkthrough is another opportunity to find and remove errors that can cause unnecessary costs and delays from advancing poor code into any of the test activities. Code validation is accomplished through unit test described below:

![Figure 2: Test setup for Unit Testing](image)

Unit testing is the test of the software elements at the lowest level of development. Since the weapon management software is a safety critical software, unit testing is performed on the target as shown in figure 2.

In order to ensure coverage, test tools are used for unit testing and the output of the tool such as the coverage chart shown in Figure 3 is released as evidence to the designers.
Appropriate regression testing with identified parameter setting is performed whenever changes are made in software.

System testing, in the context of software IV&V, involves the conduct of tests to execute the completely integrated system.

Figure 4 shows the plot of the number of errors detected by IV&V at each stage of the software development life cycle (SDLC) for one of the subsystems having about 20000 lines of code of the weapon management system.

The IV&V activities carried out for each of the hardware artifact of the weapon management system listed in the table is discussed below:

### 4.1 INSITU Software

INSITU programming is a special ground based software through which loading of software is carried out for safety critical embedded systems. This is a very effective method of downloading the application software onto the embedded system. The mode of operation of the subsystem can be either the INSITU mode in order to download/verify the application software or application mode for the execution of the application software itself.

All the IV&V activities carried out for the application software described in this paper is carried out for INSITU Software.

The INSITU software certified by IV&V is being used for downloading of application software and also for the checksum verification of the weapon management system. This is proved to be an efficient and time saving method.
4.2 Software for Acceptance Test of Hardware

The IV&V of software for the acceptance test of hardware is a very important activity since the application software is ported onto this validated hardware. Carrying out the acceptance test of hardware before testing the application software on target, enables clear bifurcation of errors encountered during development and testing of the embedded system.

The verification and validation of the software used for the acceptance test of all the hardware components present in the unit under test are performed. The activities carried out include, study of the data sheets of each of the hardware components and memory mapping, verification of software requirement specification, software design, code analysis of the acceptance test software and analysis of the coverage of each test. For example: Testing of the Flash memory involves the loading, verification and checksum calculation of the entire Flash contents.

The tests conducted are specific to the hardware design of the particular unit under test and the IV&V team participates in the final acceptance test of the hardware.

4.3 Device Driver Software

Device drivers act as translators between the device and programs that use the device. IV&V of device drivers of each device is carried out. Each device has its own set of specialized commands that its device driver software contains. The device driver accepts the generic commands from a program and translates them into specialized commands for the device.

The activities for IV&V of device driver software included the study of the devices used, analysis of software requirements for each of the devices, analysis of the device driver design document, code analysis, preparation of test plan for testing each of the device driver functions, preparation of test matrix table for all the functional test cases and preparation of test drivers for each unit level function for each of the devices.

4.4 IV&V Of Programmable Logic Devices

The application of Programmable Logic devices has become widespread, especially in mission/safety critical applications and hence the means to verify and validate their design and functionality is essential.

The IV&V of the requirements of Programmable Logic Devices involves analysis of requirements, traceability of requirements to hardware specifications, check for missing requirements, ambiguous requirements, duplication of requirements and correct functional partitioning.

Programmable hardware designs that are primarily designed at the behavioral and the structural level using Very high speed integrated circuit Hardware Description Language (VHDL) are good candidates for IV&V methods. IV&V involves understanding & analysis of design and verification of correct implementation of every requirement.

IV&V of VHDL source code includes checking the entity declarations, architecture declarations, structural and behavioral functionality, and verification of Pin numbers against the hardware schematics.

Figure 5 shows the device driver test setup with a Host PC having compiler and BDM tool which is used to download the software and to access the RAM to see the results. It is connected to the Background Debug Mode (BDM) port of the unit under test.

The test set up for testing of device driver software is established based on the devices used and the test approach involves the following steps:

STEP 1: Identification of inputs: The necessary input parameters are identified as per the functional requirements.

STEP 2: Test driver: The test driver is custom written for testing identified drivers.

STEP 3: Development of Test Matrix: After the code analysis, based on the functionalities, the test cases are generated manually.

STEP 4: Test Execution: The test cases are executed on the unit under test.

STEP 5: Result analysis and generation of report: The result obtained after the execution of the test cases is compared with the expected output and Pass / Fail criteria is recorded.

The IV&V report with the observations documented is released for all the activities carried out for the device driver software.
results, preparation of test report with simulation results captured as waveforms. Further, testing on target is carried out to ensure correctness.

Figure 6: Simulation Results

The report is then released to the designers and the regression testing is again carried out for the corrected version. Figure 6 shows the simulation results for a sample test case.

5 Coding Standards and Compiler Validation

The general-purpose languages like Ada and C, which were developed to meet a number of different needs makes the supporting compilation system and run-time environment too large to be used with confidence on safety-critical applications.

It is not considered safe to use these languages in its complete form for safety critical applications. The use of the programming language is restricted to a well-defined and analyzable subset which does not contain complex and non-deterministic features of the language. For the weapon management system software, the safe subset was defined by the IV&V team which was followed for the design and development of the software system.

The compiler has direct effect on the final code that is produced and the compilation process could introduce faults or unsafe features into the object code. Thus, it is necessary to take steps to ensure that the conversion to object code does not introduce errors or undesirable machine level features.

In order to find compiler code generated faults and to provide the level of confidence required for safety critical software, compiler validation is carried out before the compiler is used for the development of software of safety critical systems like the weapon management system.

6 Summary

IV&V is a valuable tool for increasing software quality and reliability. Verification, Validation, and Certification are essential in the life cycle of any safety critical embedded system.

Independent Verification and Validation (IV &V) is important, especially in software, as the complexity of software in systems has increased and planning for IV&V is necessary from the beginning of the development life cycle.

It is also very important to perform the Compiler Validation, IV&V of Programmable Logic devices, INSITU software, Device Driver software and software for acceptance test of hardware apart from the IV&V of application software as brought out in this paper. Many errors are detected during these phases and subsequently they are removed from the system.

IV&V stands tall in the software life cycle of an embedded application and is very closely linked with certification because it is a major component in support of certification.

Shouldering the responsibility of correcting the design/development mistakes on one hand and working hand in hand with the designer to produce every evidence to certification agencies on the other hand is a major challenge of an IV&V specialist.

7 References


