Transition of Independent Verification and Validation Activity and Refined Concept at the Mature Age

By Naoko OKUBO, Hiroki UMEDA, Shinji KAWAGUCHI, Taisuke KANBE, and Yasushi UEDA

1) Research Unit III, Research and Development Directorate, JAXA, Tsukuba, Japan

(Received June 23rd, 2017)

This paper describes how Independent Verification and Validation (IV&V) has grown at the Japan Aerospace Exploration Agency (JAXA) and how the activity was devised over two decades. However, as the development process for aerospace products matured over the decades, the value which IV&V needs to provide has changed currently. Hence, JAXA IV&V refined the concept of IV&V to accommodate mature software products. Definition of IV&V and also the narrow definition of independent, verification and validation are introduced in the paper. The paper also introduces the challenges and aspiration to support the refined concept.

Key Words: IV&V, Verification, Validation, Software, Assurance

1. Introduction

Independent Verification and Validation (IV&V) is the activity of software verification and validation which is conducted by an organization that is technically, managerially, and financially independent from the development organization. For two decades, the Japan Aerospace Exploration Agency (JAXA) has been conducting an IV&V program which has contributed to the success of spacecraft projects. JAXA initiated IV&V activity in 1995, as a part of the International Space Station (ISS) program. The IV&V was a requirement for the manned mission software in the program. During the 1990s and early 2000s, development processes toward large-scale and complex aerospace software systems were not mature compared to current processes. One of the original objectives of IV&V was not only to reduce risks regarding software products, but also to spread new software engineering technologies based on the IV&V techniques, so as to help development organizations to increase their capabilities. Therefore, IV&V activity was somewhat more closely related to development activity than assurance.

During the late 2000s and early 2010s, the development process was significantly improved through the experience gained in various activities. Also, the number of projects and software which required IV&V had been increased. As a result, IV&V activities at JAXA needed to refine the concept in order to handle the increased number of products developed by a mature process.

In this paper, we first describe how IV&V has grown at JAXA and how the activity was devised over two decades. Secondly, we propose the refined concept of JAXA IV&V toward software products developed by a mature process. At the end of the paper, we introduce the challenges and aspirations in supporting the refined concept.

2. Related Activity

It is said that a first significant IV&V program was for the Safeguard Anti-Ballistic Missile System sponsored by the U.S. Army during the 1970s. Through this program, IV&V turned into a mature system and software engineering discipline from a fledgling stage.

In the aerospace domain, the National Aeronautics and Space Administration (NASA) established their IV&V program in 1993. NASA's IV&V program was founded under NASA's Office of Safety and Mission Assurance (OSMA) as a direct result of recommendations made by the National Research Council (NRC) and the Report of the Presidential Commission on the Space Shuttle Challenger Accident. The aim of NASA IV&V program is to reduce the risks and improve the safety and quality of software systems. Agency requirements for IV&V are defined in NPD 7120.4D NASA Engineering and Program/Project Management, and NPR 7150.2B NASA Software Engineering Requirement. Also, specific requirements for IV&V are defined in NASA-STD-8739.8 Software Assurance Standard. At NASA, OSAM selects the software that should undergo IV&V. The safety, criticality, and capability of software or systems are mainly considered for the selection.

As another example in aerospace domain, the European Space Agency (ESA) also conducts an IV&V program. In ESA, IV&V is called ISVV (Independent Software Verification and Validation), which began as a result of the Ariane-5 accident. ISVV is an engineering practice at ESA, intended to improve quality and confidence, as well as to reduce costs for mission and safety critical software. Agency requirements for ISVV are defined in ECSS-E-ST-40C Space Engineering -Software, and ECSS-Q-ST-80C Space product assurance -Software product assurance. Also, specific requirements for ISVV are defined in the technical note, ESA guide for independent software verification & validation. At ESA, software which should undergo IV&V is selected by each development project. Both the development project team and the prime system supplier determine the software on which IV&V should be performed by considering the criticality and the potential of error which can be predicted from the software development process.

We can see that both NASA and ESA perform IV&V to reduce risks and improve confidence regarding safety-critical software. However, it can be said that NASA tends to capture risk from the usage of the software, while ESA from the development process of the software.
Table 1. Transition of IV&V activity at JAXA.

<table>
<thead>
<tr>
<th>Time frame</th>
<th>Phase one</th>
<th>Phase two</th>
<th>Phase three</th>
</tr>
</thead>
<tbody>
<tr>
<td>Character of the IV&amp;V project</td>
<td>Around 1990s-2007</td>
<td>Around 2008-2013</td>
<td>After 2014-</td>
</tr>
<tr>
<td>Variety of system characteristics</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Technical readiness level for the software</td>
<td>Low</td>
<td>Low/Medium</td>
<td>Medium/High</td>
</tr>
</tbody>
</table>

3. Transition of IV&V Activity at JAXA

At JAXA, agency requirements for IV&V are defined in JERG-0-049A Software development standard. The IV&V activity is currently conducted by the R&D Directorate, Research Unit III, and based on requests from the project team. Figure 1 shows the organizational related to IV&V activity.

Table 1 represents the transition of IV&V activity at JAXA. Note that this discussion excludes manned mission software, as this paper focuses on the growth of IV&V at JAXA as fostered in the ISS program. In Table 1, phases are divided into three phases by mainly considering a variety of the system characteristics. We can see the variety of the system for IV&V, and also the maturity, are getting higher during the past two decades.

In next sections, a detail of each phase will be described.

3.1. Phase one

Phase one can be described as a period of rising. From the 1990s to 2007, IV&V was basically performed on the single most critical software for each system. On average, three IV&V activities, which means three software products, were driven each year by a small team.

Table 2 shows an example of IV&V activity during phase one. The activity toward attitude control on-board software in geosynchronous satellite was performed in 2003. For instance, insufficient or incorrect traceability such as lack of functionality which should be designed were found during the activity. Also, a lack of the expected function according to checklists was found as well.

In this time frame, since the development process for large and complex software was crude, IV&V worked closely with the development group. The aim of IV&V work was to improve the development process.

3.2. Phase two

Phase two can be described as a period of widening. Although only single software for each project was chosen for IV&V during phase one, IV&V was applied to several software systems in phase two. For example, IV&V activities for the attitude control, data management and memory recorder software from a single system were performed in 2008. Also, the variation of the system which applies the IV&V expanded to launch vehicles in addition to satellite projects. On average, IV&V was performed on seven software systems per year. Given the increasing IV&V performed on software, the IV&V team became a medium scale team.

Table 3 shows an example of IV&V activity during phase two. To satisfy the growing demand, strategies for IV&V tend to be simple, such as traceability review of artifacts, etc. And to support the activity, an efficient technique for assessment, such as a traceability checking support tool has been applied.

However, the following issues emerged for IV&V activity.

- Insufficient planning and scope of IV&V activity, including why, where and how to apply IV&V techniques. This issue leads to ambiguous IV&V results and a lack of ac-
4. Refined Concept of the IV&V at JAXA

4.1. Current status

Compared to past IV&V activity, the requirements for IV&V have recently been changed. As mentioned in the previous section, the software development process is obviously getting mature as compared to the 1990s and early 2000s. Therefore, the role to improve the development process, as was targeted during phase one, is getting smaller these days.

As shown in Figure 1, IV&V was an activity based on requests made by the development project teams at JAXA. Consequently, a development project team familiar with IV&V would make an appropriate request, while another team not knowledgeable about IV&V would not even request it, even if their product had safety and other critical issues. Currently, a determination of IV&V became a necessity as a rule, so almost all development project teams now request IV&V.

A unified definition of IV&V to match this situation is thus needed. It will also prevent IV&V from becoming an excess activity from total needs for assurance. The next section describes a narrow definition of IV&V.

4.2. Definition of IV&V at JAXA

Before defining IV&V, we will look back to the characteristics of the software and its quality for aerospace product. Here, the meaning of product quality is close to the definition in the ISO/IEC 25010 system/software product quality model. Figure 2 represents the differences between aerospace and automotive software in general. Aerospace software is characterized by having a smaller volume of released products. From this aspect, we can say that the aerospace product tends to have fewer chances to check quality. Therefore, it can be said that the statistic quality metrics, such as defect removal effectiveness which is used in mass produced products, are relatively ineffective to show the quality of an aerospace product. One solution for trusting this kind of product is to make various opportunities to ensure the quality. Thus, IV&V activity will be one opportunity to ensure quality double that assured by V&V.

Based on this reason, we defined IV&V activity as follows.

- IV&V is one of the software assurance activity which ensures the software product quality and provides confidence about the quality.
- IV&V is a risk focused assessment in addition to exhaustive software testing conducted by the development organization.

Here, ensure means software assurance practitioners themselves perform the specified software activities. On the other hand, assure means software assurance practitioners make certain that the specified software assurance, management, and engineering activities have been performed by others.

At JAXA, software developers or prime system developers are responsible for ensuring a certain level of product quality. In cases where the V&V result is the first opinion to ensure product quality, IV&V plays a second opinion role to ensure that a product is developed to offer a certain level of quality. As the development organization conducts exhaustive software testing, IV&V focuses on critical and complex parts of a product. Therefore, the nature of the IV&V is a risk based software testing, which focus on a possibility which leads to an undesired outcome.

4.3. Narrow definition of independent, verification and validation

First, to provide an applicable second opinion service, the requirements for the independence at JAXA are defined as fol-
Fig. 3. Narrow definition of verification and validation in IV&V.

- Managerially independent: Person who engage in IV&V needs to not engage to the corresponding development work. Also, direct supervisor for the person who engage in IV&V should not be the same as the low level supervisor in the development team.
- Technically independent: The scope and aim of the evaluation need to be revealed in the scoping and planning. In addition, the IV&V result must clearly state the evidence if there is an issue or not.
- Financially independent: Do not mix the cost for IV&V with the development cost which is paid for by the software firm.

The IV&V activity should at least fulfill the upper requirements. Especially, the managerial independence is important to remove the bias of the product risk which may happen in the future.

Next, since the IV&V members tend to have insufficient knowledge about a product as compared to the development side, the way of thinking about verification and validation should be modified to become more effective. The most popular and simple definition is "Are we building the product right?" for verification and "Are we building the right product?" for validation. Especially for validation, IV&V often encounters a difficult situation where all information, such as user expectations, cannot be collected for evaluation. Hence, the IV&V at JAXA interprets the verification and validation as follows.

- Verification: Are the software products built in the right way based on the product risk?
- Validation: Will the built software product not lead to undesired condition for the user in the future?

Figure 3 represents the narrow upper definition. Each box expresses the artifacts of the software. The boundary shows the area in which IV&V ensures the product, and the upper part of the boundary is a baseline, expectation for the product. For verification, the overall evaluation is based not only on the system architectural requirements as typically defined but also on risks extracted by the IV&V team that may lead to an undesired outcome. For validation, as mentioned before, it is difficult to obtain user expectations, customer satisfaction etc. However, IV&V can confirm information about the software, such as how it is designed and its degree of fault tolerance. Therefore, the validation is the bottom-up point of view from concrete software information, and finds the possibility whether software may cause an undesired outcome. Since typical definition is top down approach from such as user expectation to software artifacts, the definition for IV&V is intended to reverse that approach.

4.4. Challenges and aspiration

This section introduces the challenges and aspirations in supporting the refined concept of IV&V.

Challenge 1: A method of revealing the scope, planning and result

Generally speaking, an evaluation by a third party adds confidence to the product. To be effective, the activity by the third party must be objective and clearly stated with supporting evidence, not to be subjective. Especially, careful share of the aim of the evaluation will strongly support the objectivity.

It is also true that IV&V activity and a peer review by experts are quite similar. However, since IV&V is an activity performed by a third party organization, reproducibility is needed even when the IV&V engineer is replaced. Lower reproducibility will also lower the objectivity regarding the result, as well
as its value.

As one aspiration, there is a need for a method that can clearly and objectively represent how an engineer thinks about risk, the purpose of an evaluation, and its scope and planning.

**Challenge 2: Point out appropriate risk**

After clarifying how an engineer thinks, it is necessary to point out good quality risks to be verified. A good quality risk should be unique corresponding to the feature of the system/software which is meant to be optimized for each evaluation situation. As an aspiration, a method or framework of extracting unique product risk is needed. Such a method should also be one that can be used before the software artifacts are released when considering the structure of the IV&V business.

**Challenge 3: Continuous technical transition**

Related to reproducibility, continuous technical transition is an issue from phase one. In general, it is said that the software engineering education and training contains a numbers of challenges. For instance, following are the challenges for the technical transition.

- Need to identify the abilities, such as skills, which the engineers should possess; and
- Need to keep the training program up-to-date to follow rapid changes in techniques or technologies

Especially, it is also said that education or training related to software testing are limited compared to development techniques such as software architecture education, etc. To overcome this challenge, JAXA is now developing a training series to provide the knowledge, skills and attitude necessary to be an IV&V engineer.

5. Prediction of Future IV&V at JAXA

As a prediction, the next phase of IV&V will be described as a period of optimization. Here, we introduce a part of our on-going work in response to the previously mentioned challenges.

5.1. Method to visualize planning and scoping

To overcome challenge 1, a method to reveal the scoping, planning and result, JAXA introduces the GSN (The Goal Structuring Notation) to represent the logical representation of "How we think about risk” and "How to ensure there is risk or not". Figure 4 shows the basic structure of GSN. The GSN is a graphical technique which is well used to express the structure of the safety argument. It is basically consists of the goal, solution/evidence, strategy and context, and the connection of these elements.

At JAXA, we extend the usage of GSN and express the IV&V plan as shown in figure 5. Two structures, one for risk assessment and the other for test strategy, are used to express the planning and scope as a concept. The risk assessment GSN structure represents the product risk to be evaluated in the bottom element. Inside this structure, how the engineer thinks and captures the risk are represented. The bottom element of the test strategy is the criteria to determine if there is risk or not. Basically, the bottom element of risk assessment GSN and top element of the test strategy GSN are on one-to-one basis. At present, there are on-going works to define the process to apply this method and also the supportive tools.

5.2. Method to point out appropriate risk

After visualizing the way of thinking of the engineers including the aim of the evaluation by GSN, it is necessary to point out the good quality risk as mentioned in challenge 2. As a nature of GSN, it cannot represent a weight of impact and the probability of each sub-goal. It is thus necessary to point out the appropriate risk, which might high impact and more likely happens.

To overcome this issue, the use of reference data is one approach. In the context of IV&V activity, a previous defect or past anomaly data is a good reference to select the appropriate risk. Therefore, constructing references via defect data which collected by the special defect analysis is one of our on-going work.
6. Conclusion

This paper described how IV&V has grown at JAXA and how the activity was devised over two decades. JAXA IV&V was raised in the 1990s and then became popular and expanded by the 2010s. However, as the development process matured over the decades, the value which IV&V needs to provide has changed as well.

Therefore, IV&V at JAXA was challenged to refine the concept of IV&V to accommodate mature software products. The definition of IV&V and also the narrow definition of independent, verification and validation are introduced in the paper. It also introduced the challenges and aspirations in supporting the refined concept.

As a prediction, IV&V will become more optimized as part of assurance activities. The result of how we tackle the challenge will be reported in the future.

Acknowledgments

The authors wish to thank those colleagues who helped us understand the history behind how IV&V has grown at JAXA. Especially, thank to Masa Katahira, who contributed to JAXA IV&V from the beginning and even now leads the young IV&V engineers like us. Also, thanks to Pedro Barrios from the European Space Agency and Jennifer D. Neptune from the National Aeronautics and Space Administration who provided their way of IV&V in the frame work of IVV international working group. For Jennifer, special thanks to be our English coach as always.

References