International Workshop on Strategic and Economic Methods for Assessment of IV&V Activity
JAMSS Position Paper

Success criteria and key points for successive IV&V outcome

Haruka Nakao, Hitoshi Mamiya, Japan Manned Space Systems Corporation

Abstract

Software IV&V plays an important role in Safety and Product Assurance activities. The IV&V mission is not fancy term of SQA. Successive and Efficient IV&V can be achieved certain conditions. JAMSS has several functional tools, methodologies and functions for each system and system phase based on experience. JAMSS has also successive experienced to achieve maximum outcome with limited human resource and limited target system data. If it is able to define IV&V success criteria, we define it 4 levels. We have to narrow the target part and IV&V criteria if we want to do successive IV&V. We show narrow the target is important for successive IV&V based on 6 project.

1. Introduction

JAMSS is a support engineering company for integrating Japanese Experimental Module called "KIBO" since 1990. 160 people work in the company.

IV&V team in JAMSS are doing software IV&V for space related software.
On-board software of International space station is required to do software IV&V. Therefore our team initiated IV&V activity for JEM, after that we starts IV&V for HII-A transfer vehicle, Centrifuge Roter, JEM payload software among International space station program. We start IV&V for un-manned vehicle such as satellite and ground system since 2000. Currently 6 people are doing IV&V 3 of manned system, and 5 of un-manned system in our IV&V team.

2. IV&V on software product assurance and safety

In order to enhance software safety, reliability, maintainability and quality, Software S&PA activity for manned system is required to evaluate by third party independently. Table.1 shows the S&PA required activities. Each description shows SPA activities and the characteristics.

Actually, it is hard to achieve the required activities entirely because they are required "to be Independent". The reason why it is hard for them is written in below.

- Evaluation criteria are not specified.
- SPA personnel less knows about target system than designer.
- SPA personnel do not have enough time and opportunity to evaluate.
- Flood of requirement specification documents contents
- Evaluation priority is unknown.

S&PA requirement on International Space Station requires IV&V activity in addition to original SPA activity. If software S&PA activity is an authorized activity by which project manager approve the development based from safety, Reliability, Maintainability and Quality point of view, IV&V activities are expected to carry out required SPA activity with priority definition even though it is like process sampling.

2. Success criteria of IV&V

If it is able to define success criteria of IV&V, we define it into 4 levels. The lowest level is no outcome or just finding editorial miss. The second level is finding defect of system. The third level is finding defect and ensuring certain evaluation criteria. The highest level is finding defect, ensuring certain evaluation criteria, and contribution to S/W development process improvement or system architecture improvement. It needs maximum effort with limited human resource and each system restraint. We have to discuss what is the key point to achieve successive IV&V

outcome. Fig. A shows image of IV&V success criteria. The first axis is IV&V coverage, the second axis is quality of RID, and the third axis cost effectiveness. However we have not amounted cost effectiveness of each IV&V experience.

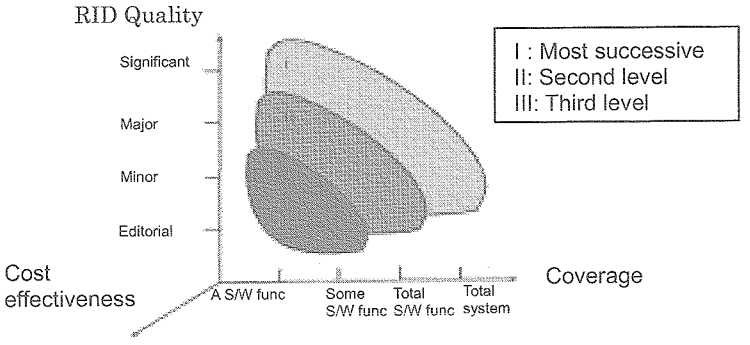

Fig. A IV&V success criteria

Table. 1 Required S&PA Activity

S&PA required activity	Actual detailed activity
(1) Documentation review Review the submission of S&PA documents takes appropriate process and phase.	Evaluation criteria (submission document and phase) is defined specifically.
(2) Requirement Specification Review Review and assure that the description of requirement specification is complete, consistent, not ambiguous and verifiable and traceable.	Flood of document contents volume. Reviewer less knows about target system than designer. There are no specific evaluation criteria. Evaluation priority is unknown.
(3) Applicable document is specified	Evaluation criteria are defined specifically. Reviewer does not need to know about amount of design information.
(4) Interface document review	In order to review the interface document, reviewer needs to know about big picture of target system.
(5) Code Inspection	Plenty of source code documentation. SPA personnel less knows about target system than designer. Constraint on disclosure of information on source code.
(6) Software testing	Evaluation criteria for test program are not specified. It takes long time to review each test case and test result in step by step.
(7) Configuration management	Confirmation of Configuration Change can be reviewed but detail of change is not reviewed because of constraint on disclosure.
(8) Assure tradeoff study	SPA personnel review tradeoff study after decision making (because SPA personnel does not have enough time to attend most design activity).
(9) Interface review after integration	Evaluation criteria for test program are not specified. SPA personnel do not have enough time to see H/W design or system operator.
(10) Review a conformance to software standard	Designer do not follow software standard in a positive manner.
(11) Software Safety	Evaluation criteria for computer based control system are not specified. Responsibility for incidents or accidents is clear.

3. The critical condition for effective IV&V activity

In order to overcome 5 barriers for S&PA activities shown in section 1, IV&V activity should be

efficient. In this position paper we define essential prerequisite and baseline approach to carry out IV&V activity in an efficient manner.

(a) Specified evaluation criteria
Evaluation criteria should be specified through software lifecycle (Requirements analysis, design, Implement, Test, Operation and Maintenance). IV&V should evaluate if target system fulfill the defined criteria or not. Evaluation results should be reported to project manager (or decision maker) for judgment. IV&V personnel also feel a sense of achievement through evaluation activity based on specified criteria.

(b) Knowledge of target system property
Comparing to developer, IV&V personnel do not have enough knowledge of target system. However if target system can be defined as a part of domain technology, storing up knowledge of domain technology makes IV&V personnel sense improve. IV&V personnel use knowledge of domain technology as evaluation criteria by making its checklist.

(c) Ease of access to target system development activity
If IV&V personnel can easily access to information of target system, Evaluation result will be more precise. It's also necessary to keep good relationship between project management personnel and IV&V personnel.

(d) Rules and tools to make review efficiency
Because flood of software documentation, It takes a long time to evaluate all documentation based on a defined criteria and the IV&V activity will be too expensive for target system development. Making a rule and developing a tool based on the rule takes it easier to evaluate. Cost performance becomes far better.

(e) Risk identification for target system
It is necessary to investigate what does project management concern about during identification risk of target system. It is also necessary to identify the most important factor.

4. IV&V activities on 6 projects
We choose 6 projects from former IV&V experience. Each projects has characteristics on system, phase, and constraint for IV&V activities. We show human resource, system characteristic, target identification, methodology and process. In addition to them, we show outcomes of IV&V activities, advisary for S/W development process improvements from the IV&V activities (Table. b).
Each methodology on The methodologies and process (Table. b) is shown in Table. c. We developed them in former IV&V activities. These are categorized by development phase.

5. Conclusion
Even if there is limitation of human resource or data access constraint we experienced to achieve successive IV&V outcome. Because we have developed methodologies and we can newly develop methodologies applied to each system character, development phase. However,
An important process to achieve IV&V successively is to narrow the range and evaluation criteria to carry on, because IV&V personnel should get over the circumstance of in which limited human resource and restrict some restraint.
We take Hazard Reports, Fault Tree Analysis, Accident (Incident) report, and interview to project personnel as narrowing down the target. Some IV&V activities for projects didn't success like projects on the Table. 2 because we didn't sufficient narrow down. In fact successive narrowing down leads to successive IV&V outcome. How much is narrowing down enough to achieve successive IV&V outcome? The average of percentage is 40% based on JAMSS's past experiences.

Table. 2 Experience from 6 projects

System A					
[1] Total effort man month j	3 Years 20MM				
[2] characteristic	System property	✣ Manned System	O Unmanned System		
		✣ Onboard Software	O Ground System		
		✣ Space Station Module	O Satellite	O vehicle	
	IV&V phase	O Requirement	✣ Design	O Test	O Operation
[3] Effort pattern [%]	0 <---------- >50< ---------- 100				
	Planning	Identification	Analysis	Summarizing	
[4] Identification	Hazard Report Catastrophic Hazard j				
[5] Condition	IV&V condition			YES	NO
	Sufficient human resource			✣	
	Easiness data accessing			✣	
	System and Operation knowledge			✣	
	Developer's help			✣	
	Code availability				✣
	Inspection of operation				✣
[6] Methodology / Process	Model Checking (2.) [Parallel e c execution analysis] Ensure not to conflict of valve open and close by mode transition model of FDIR procedure.				
[7] Outcome	It was ensured that there is no couple of procedure to conflict.				
[8] Contribution to S/W process improvement	We found that time critical 2 fault tolerant system is required automatic FDIR. Resemble FDIR procedures should be integrated in CDR phase.				

System B					
[1] IV&V time span /man month	1 Year 6MM				
[2] characteristic	System property	✣ Manned System	O Unmanned System		
		✣ Onboard Software	O Ground System		
		✣ Space Station Module	O Satellite	✣ vehicle	
	IV&V phase	O Requirement	✣ Design	O Test	O Operation
[3] Effort pattern [%]	0 <---------- >50< ---------- 100				
	Planning	Identification	Analysis	Summarizing	
[4] Identification	Hazard Report Catastrophic Hazard ,jOperation event density				
[5] Condition	IV&V condition			YES	NO
	Sufficient human resource			✣	
	Easiness data accessing			✣	
	System and Operation knowledge			✣	
	Developer's help			✣	
	Code availability				✣
	Inspection of operation				✣
[6] Methodology / Process	FDIR test coverage analysis (5.) In order to ensure the sufficiency of test cases in CSCI test, This analysis outputs sufficient test cased based on couple of hazard controls (couple of 2 failure isolation and recovery sequence).				
[7] Outcome	Sufficiency of test cases for hazard control in CSCI test.				
[8] Contribution to S/W process improvement	We developed rules to output sufficient test cases using Hazard Report.				

System C					
[1] IV&V time span /man month	6 month 2 MM				
[2] characteristic	System property	O Manned System		+ Unmanned System	
		O Onboard Software		+ Ground System	
		O Space Station Module	O Satellite	O vehicle	
	IV&V phase	O Requirement	O Design	O Test	+ Operation
[3] Effort pattern [%]	0 <---------- >50< ---------- 100 Planning | Identification | Analysis | Summarizing				
[4] Identification	Critical accident in an operation				
[5] Condition	IV&V condition			YES	NO
	Sufficient human resource			+	
	Easiness data accessing			+	
	System and Operation knowledge			+	
	Developer's help			+	
	Code availability			+	
	Inspection of operation			+	
[6] Methodology / Process	Code check (4.) [Common variable conflict analysis, Code differential check] Onsite check of compatibility of code modification for launch operation.				
[7] Outcome	We ensured there is no wrong code modification for about 10,000 LOC.				
[6] contribution to S/W process improvement	We found that It is necessary to check one by one on the version management since acceptance until operation.				

System D					
[1] IV&V time span /man month	6 month 1 MM				
[2] characteristic	System property	O Manned System		+ Unmanned System	
		+ Onboard Software		O Ground System	
		O Space Station Module	+ Satellite	O vehicle	
	IV&V phase	O Requirement	+ Design	O Test	O Operation
[3] Effort pattern [%]	0 <---------- >50< ----------> 100 Planning | Identification | Analysis | Summarizing				
[4] Identification	FTA (Not to lead mission fail)				
[5] Condition	IV&V condition			YES	NO
	Sufficient human resource			+	
	Easiness data accessing				+
	System and Operation knowledge				+
	Developer's help				+
	Code availability				+
	Inspection of operation				+
[6] Methodology and Process	Check list (1.) [Attitude Control Checklist] Check sheet technical advice memo for translation and attitude.				
[7] Outcome	*We found some critical RIDs (I.e. Deference of coordination between the requirement and design) from 300 pages documentation. *We found ambiguous expression of mode transition condition.				
[8] contribution to S/W process improvement	-				

System E					
[1] IV&V time span /man month	3 Years 10 MM				
[2] characteristic	System property	✣ Manned System		O Unmanned System	
		✣ Onboard Software		O Ground System	
		✣ Space Station Module	O Satellite	O vehicle	
	IV&V phase	✣ Requirement	✣ Design	O Test	O Operation
[3] Effort pattern [%]	0 <---------- >50< ----------→ 100 Plan | Analysis | Sum				
[4] Identification	Hazard Report ©atastrophic Hazard j				
[5] Condition	IV&V condition			YES	NO
	Sufficient human resource			✣	
	Easiness data accessing			✣	
	System and Operation knowledge			✣	
	Developer's help				✣
	Code availability				✣
	Inspection of operation				✣
[6] Methodology / Process	Model Checking (2.) [Completeness and Consistency analysis, Traceability analysis, Timing Analysis, and Interface analysis] Model checking using SpecTRM, SPIN, and in-house developed tools.				
[7] Outcome	We ensured that system didn't have incoherent description of mode transition. We ensured the compatibility between upper level system document and lower level document. We ensured the certified the execution of command sequence on a emergency.				
[8] contribution to S/W process improvement	We advice as to integrate the description of each CSCI documentation. We advice as to break down the upper level system documentation to lower documentation.				

System F					
[1] IV&V time span /man month	6 Month 20 MM				
[2] characteristic	System property	✣ Manned System		O Unmanned System	
		O Onboard Software		✣ Ground System	
		O Space Station Module	O Satellite	O vehicle	
	IV&V phase	O Requirement	O Design	✣ Test	O Operation
[3] Effort pattern [%]	0 <---------- >50< ----------→ 100 Plan | Identification | Analysis | Sum				
[4] Identification	2000 more over malfunctions analysis since CSCI test until sub-system test				
[5] Condition	IV&V condition			YES	NO
	Sufficient human resource			✣	
	Easiness data accessing			✣	
	System and Operation knowledge				✣
	Developer's help			✣	
	Code availability			✣	
	Inspection of operation				✣
[6] Methodology / Process	Documentation Review [Design coverage review, Test coverage review, I/F consistency review] Model Checking (2.) [Completeness analysis SpecTRM]j Code check (4.) [Source code analysis] PG-Relief ;j				
[7] contribution to S/W process improvement	*We ensure coverage of error detection and raise the system failure tolerance. *We ensure coverage of test cases at CSU test and integration test. *We found design defect by the analysis of critical function in critical design with source code.				

Table. 2 IV&V methodology and tool

Development phase / Methodology & Tool	Requirement	Design	Test (Coding)	Operation
1. Check list				
Attitude Control Checklist	+++	+++		
Voyger gallileo checklist	+++	+++	+++	
2. Model Checking				
Completeness analysis	+++	+++		
Inconsistency analysis	+++	+++		
Parallel FDIR execution analysis	+++	+++	+	+
Timing Analysis		+++	+	
Traceability Analysis		+++	+	
Reachability Analysis		+++	+	
Code crone analysis		+++	+	
3. Simulation				
Comparison check (RD-DD)		+	+	
Single failure point simulation	+			
Two failure simulation		+	+	
4. Code check				
Code crone analysis		+++	+	
Static analysis			+++	+++
Common variable conflict analysis				+++
Code differential check				+++
5. FDIR test coverage analysis		+++	+	
6.HAZOP analysis		+++		
7.Hierarcal Accident model analysis		+		+++

+++ FExperienced for real project, + FTrial