IV&V Challenges for COTS-based Safety Critical Systems

Haruka Nakao	Masafumi Katahira	Dan Port
Japan Manned Space Systems Corporation	*Japan Exploration Agency*	*Univ. of Hawaii*
{haruka,nomo, mamiya}@jamss.co.jp	*Katahira@*	*dport@hawaii.edu*

Abstract

COTS has complicated the IV&V process for our safety critical satellite and ground control systems. IV&V on the COTS products used must be done far in advance of a fully developed system to avoid COTS "black-box" complications. This cannot be done outside the context of system development due to the risk of committing to COTS products that are inappropriate or mismatched for the system. By integrating IV&V assessment with well established, developer-oriented COTS assessment techniques, we may be able to effectively address the challenges of COTS V&V for safety critical systems.

1. Introduction

Exploding costs and shrinking budgets have necessitated the use of COTS (Commercial off the shelf) in the development of new safety critical systems such as satellites and spacecraft ground control [1]. Enthusiasm for this faded after the recent high-profile space-mission failures underscored the need for highly reliable software [1]. Indeed COTS and safety is a critical issue [2, 3], and independent verification and validation (IV&V) on COTS is clearly absolutely necessary [4], yet remarkably is not well established for safety critical systems [1].

In the development of our satellite and ground control systems we have observed that the traditional IV&V approach for safety critical systems has not been effective when these systems critically rely on COTS. COTS "black box" effects tend to run IV&V aground. One problem is a classic "chicken and egg" dilemma. On one side, it is too late to perform COTS IV&V after a system has been developed where critical COTS risks cannot be addressed or are too costly to mitigate. On the other side, before the system is built, assessment and selection of COTS is done without the critical safety assurance of IV&V with respect to the target system.

The purpose of this work is to elaborate on these and other related COTS IV&V concerns and describe some efforts in developing an alternative approach that integrates COTS assessment with IV&V COTS Verification and Validation early within the development cycle.

2. Safety Critical V&V and COTS

Traditional IV&V is usually predicated on having a fully developed system. The IV&V team performs an assessment to assure the system meets requirements and quality standards (e.g. safety critical). However, waiting until after a system has been implemented is generally too late to take action on IV&V COTS assessment results. Some of the reasons for this include:

- A fully developed system may obscure potentially fatal COTS risks such as "dormant code" by making it difficult to access or uncover [5].
- It is difficult to determine potential risks " fter the fact" with limited access to source code.
- If problems within the COTS are found after they are integrated into the system, there is limited means of addressing them within the COTS without introducing new " ollateral" risks that require additional IV&V effort.
- COTS that are intimately integrated within a system or have a high dependency with (e.g. proprietary API's, protocols, etc.) are generally not "exchangeable" with other COTS. One can't just find alternative COTS to replace problematic or difficult to validate COTS components.
- Developers "optimistically" assess COTS often assuming they are safe until shown otherwise, whereas IV&V "pessimistically" assess COTS assuming they are unsafe until shown otherwise. If the IV&V and developer's assessments of the COTS already chosen for the system are incompatible, it is risky to choose one assessment over the other.

This presents a dilemma – either have the developers re-work the system until assurance can be achieved or "gamble" and ignore the IV&V assessment results. The former may incur unreasonable and unanticipated development costs and unexpected risks in addition to additional IV&V effort to assure the re-worked system. In the latter, the "gamble" may prove to have unacceptable risk levels leading to operational disasters. We have experienced both scenarios and Table 1 summarizes our ongoing challenges with IV&V within some of our COTS based space systems.

Table 1. COTS IV&V Challenges at JAXA

System	Phase	COTS IV&V Problem
G (A)	RDM	Inability to balance COTS, legacy, and development items
G (B)	TI	Over 1,000 bug reports
OBS (A)	TI	Integration test OBS and sensor S/W failed
OBS (B)	A	Incoherent documentation quality
OBS (C)	A	Inability to integrate COTS and legacy

RDM = Requirements Definition and Management
TI = Test and Integration
A = Architecting
G = Ground Control Syst.
OBS = On Board Software

The above indicates that a traditional IV&V approach to COTS system assessment may result in unacceptably high uncertainty and difficult to mitigate risks. Some have attempted to address the above problems by "pre-assessing" individual COTS products well in advance of system development and then require developers to use only these COTS products. Aside from severely limiting the COTS choices (perhaps to the extent that none are actually deemed suitable for the system under consideration), this approach has also proven risky as it fails to adequately assess the COTS products for the particular system [6, 7]. This may include particular system safety requirements that a general purpose individual COTS product IV&V assessment may not have considered. As noted by Ronald Stroup, FAA Safety & Certification Lead, "An unwise [advance] purchase of a COTS product could doom your program to cost and schedule overruns and more importantly induce safety instability that in all likelihood will never be adequately mitigated."

The only remaining viable option is to have both developers and IV&V perform assessments of the COTS system (i.e. not just the individual COTS products within the system) *prior* to committing to a particular architecture. Given the significantly different developer and IV&V perspectives, a-priori we have no basis to assume that the two assessments will be consistent. In our own experience and through anecdotal interviews with other organizations we have observed that the two assessments frequently are at odds with each other even when both are done before architecture commitments are made.

Figure 1 presents an example of two such incompatible COTS system assessments. Analysis of the developers assessments in figure 1a indicate that if arbitrarily large effort is expended then the risk for systems B or C would be about tied for lowest. However, the rate of risk reduction is clearly greater for system A and the ultimate risk level is not significantly higher than for systems B and C. The developers believe that it is risky to assume that the full assessment will be performed for all the systems and that the outcomes of these assessments will turn out exactly as hoped. Based on this perspective, system A presents the overall lowest risk from their perspectives. The IV&V assessment expectations in Figure 1b tell a different story. System B has a considerably better risk reduction profile. The ultimate expected risk level is significantly lower and even if only half the assessment effort is made, clearly system B has lower risk than system A. The result concluded by the IV&V team is that system B provides the lowest overall risk.

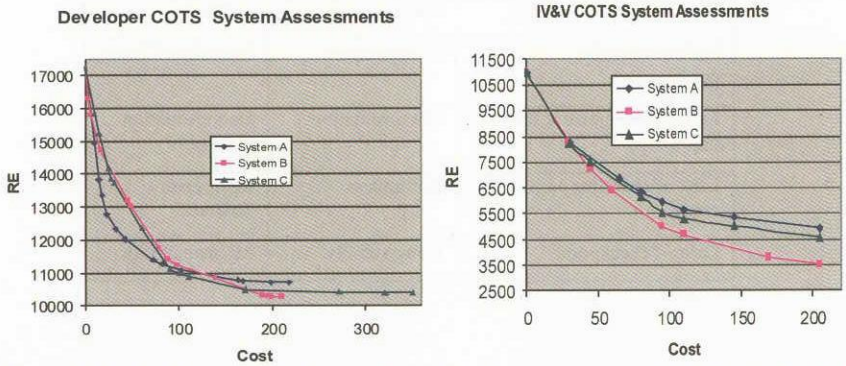

Fig. 1. (a) Developer Assessment Risk Reduction (b) IV&V Assessment Risk Reduction

3. Integrating COTS assessment and V&V

Based on our observations, it is clear that some IV&V of COTS must begin before the system is fully developed but not so early that the system dependent safety critical requirements cannot be validated leading to risky COTS components. COTS products must initially be thoroughly assessed for their suitability in the target system and filter those that fail basic IV&V criteria. Surviving COTS candidates must then pass on to a more rigorous IV&V and COTS assessment process. However this brings to light several challenging questions such as:

- What are the safety parameters and risk tolerance?
- What are the specific nominal and off-nominal safety scenarios the COTS must support?
- What COTS attributes are relevant to safety and to what extent?
- How much is enough assessment to validate the COTS?

To begin tackling some of these questions, we must somehow integrate the COTS assessment and IV&V perspectives, The COTS assessors' perspective is to evaluate COTS candidates with respect to the project relevant COTS attributes such as those listed in the second column in Table 2. One the other hand, the IV&V perspective is evaluate system risks with respect to IV&V attributes such as those shown in columns 1 and 3 in Table 2 respectively. The evaluation process is used for both COTS and IV&V should be done concurrently and output a combination of the two evaluations based on risk exposures such as the Max-Min method described in [ ].

Table 2 COTS and V&V Attributes for OS

System Issue	COTS Attribute	V&V Attribute
Lack of Memory	Performance	Memory Utilization
Memory deployment lack	Robustness	Fail Safe
Deference test and operation configuration	Compatibility	With other component
Lack of COM test capability	Understandability	Testability
Lack of Error handling	Robustness	Error handling
Message queue overflow	Robustness	Fail Safe
Lack of real time performance	Performance	Execution Timing
Lack of requirement flow down	Documentation	Documentation Quality
Lack of checking parameter range	Robustness	Input Error Tolerance
Lack of checkpoint	Compatibility	Maintainability

4. Conclusions

We have identified a serious incompatibility between traditional IV&V systems assessment and developer based COTS assessment within safety critical systems. This frequently results in higher project risk and uncertainty. In particular, the incompatibility raises serious unanswered questions such as:

- What is an acceptable IV&V standard and measures for safety critical COTS?
- How can IV&V mitigate the risk of COTS "dormant" code?
- How can incompatible developer and IV&V COTS assessments be reconciled?
- What is an effective tactical IV&V response to COTS problems?
- What is an effective strategic planning of IV&V COTS activities?
- How can the cost and benefits of COTS IV&V be rationalized?
- How much is enough COTS IV&V?

It is clear that some form of early IV&V on COTS integrated with developer COTS assessment is needed to address this problem. We are currently investigating a "side by side" COTS IV&V and COTS assessment approach that integrates related COTS and IV&V evaluations weighted by project risk exposures. We hope to validate and refine this approach in the near future.

References

[1] M. Rahmatipour, V&V of COTS RTOS for Space Flight Project, The 1st NASA OSMA SAS, 2000
[2] RTCA Inc., "Final Report for Clarification of DO-178B 'Software Considerations in Airborne Systems and Equipment Certification'," Washington, D.C. RTCA/DO-248B, October 12, 2001.
[3] G. Brower, Validation of Commercial Off the Shelf Software, Journal of Validation Technology, 1999
[4] R. Kohl, V&V of COTS Dormant Cord: Challenge and Issues, GSAW, 1999
[5] C. Abts, B. Boehm, and E. Bailey Clark, COCOTS: A Software COTS-Based System (CBS) Cost Model, Proceedings, ESCOM, 2001
[6] D. Port, S. Chen, Assessing COTS Assessment: How much is enough?, Proceedings, ICCBSS, 2004
[7] B. Boehm, Software Risk Management: Principles and Practices, IEEE Software, 1991
[8] D. Port, H. Nakao, H. Nomoto, H. Mamiya, M. Katahira, Resolving COTS System Assessment Clashes, Proceedings, ICCBSS, 2005 (to appear)