Resolving COTS System Assessment Clashes

Daniel Port[1], Haruka Nakao[2], Hideki Nomoto[2], Hitoshi Mamiya[2], and Masafumi Katahira[3]

[1] University of Hawaii at Manoa, College of Business Administration, Department of Information Technology Management, Honolulu, Hawaii, USA
dport@hwaii.edu
[2] Japan Manned Space Systems Corporation, Tsukuba, Japan
{haruka, nomo, mamuya}@jamss.co.jp
[3] Japan Aerospace Exploration Agency, Tsukuba, Japan
katahira@computer.org

Abstract. COTS significantly complicates the IV&V process. The necessarily pessimistic culture of IV&V has a perspective on which COTS assessment attributes and techniques are relevant that differs greatly from developer's typically optimistic, success-oriented perspective. There is no basis to assume that the COTS assessments made by developers will ultimately be consistent with IV&V COTS assessments. The result frequently results in a "lose-lose" situation where either large re-work costs are incurred to replace existing COTS with IV&V approved COTS, or higher risk and uncertainty must be tolerated (from the IV&V perspective) to continue with the COTS the developers chose. This work seeks to remedy this "culture clash" of COTS assessment perspectives by integrating IV&V and developers system level COTS assessments that provides a result that is both consistent and cost-effective.

1 Introduction

Exploding costs and shrinking budgets have necessitated the use of COTS (Commercial Off The Shelf products) in the development of new safety critical systems such as satellites and spacecraft ground system [1]. Enthusiasm for COTS use has faded after recent high-profile space-mission failures underscored the need for highly reliable software in safety critical systems [1]. COTS and safety has become a critical issue [2, 3] and along with it the challenges of performing Independent Verification and validation (IV&V) on COTS based systems [4]. Remarkably, many of these challenges have yet to be addressed [1].

In the development of satellite and ground control systems at the Japan Aerospace Exploration Association (JAXA) we have observed that the traditional IV&V approach for safety critical systems has not been effective when these systems critically rely on COTS. In particular, we have had trouble selecting a mutually acceptable (from the developers and IV&V risk perspectives) COTS system architecture among numerous architecture options. Our selections have been beset with late-term COTS "black box" effects that have run IV&V efforts aground. Efforts to increase or make our COTS assessment more rigorous have had little impact.

X. Franch and D. Port (Eds.): ICCBSS 2005, LNCS 3412, pp. 65–76, 2005.

Restricting developers to "pre-approved" COTS has not proven an effective remedy. As a result, the cost-effective IV&V of COTS based systems has become a major problem.

A contributor to this problem has been traced to *contradictory developer and IV&V COTS system assessment results*. When such a misalignment is present, it is difficult to judge which assessment results should be used, the developers or IV&V? In our experience, choosing one over the other has resulted in long-term problems. In this paper we will elaborate on the problem of developer and IV&V COTS system assessment conflicts with an actual case study from a COTS based space system currently under development at JAXA. This case study will also present a new approach to resolving this conflict to aid in making strategic risk reducing choices of COTS systems architecture options.

2 COTS System Assessments: Different Perspectives, Different Results

Of the many challenges of COTS and IV&V, this paper considers the particularly frustrating challenge of conflicting developer and IV&V COTS system assessment results. Here we differentiate "COTS system assessment" from "COTS assessment" in that the assessment is of the system that uses the COTS rather than for individual COTS products. A phenomenon we have observed in this is an unintentional "one hand doesn't know what the other hand is doing" problem. On one hand, a developer's assessment perspective is necessarily *optimistic* and success-oriented. The attributes developers are concerned with and the techniques they might use to assess such attributes are chosen to reduce overall *risk with respect to project development* cost, schedule, and the satisfaction of quality requirements. That is, potential losses that may occur in the *development* of the system. On the other hand, the IV&V perspective is necessarily *pessimistic*. A system is assumed to have risky defects until there is evidence that it does not. The attributes and techniques chosen by IV&V are to mitigate a systems' overall *deployment risk* (i.e. potential losses incurred during the operation of the system).

Both the IV&V and the systems developers COTS assessments must be done well in advance of system implementation in order to identify and avoid potentially critical deployment risks before committing to a particular COTS-based architecture. Failure to do so may result in costly re-work or unacceptable system quality or risk. In this regard, it is ideal if IV&V assessments are performed simultaneously with the developers assessments. However, an IV&V assessment cannot be done outside the context of the system development due to the risk of developers committing too early to COTS products that may be inappropriate, mismatched, or too risky for use within a system.

One suggested approach to this problem is to simply restrict developers to utilize only "IV&V pre-approved" COTS products. Unfortunately, this approach cannot provide the system-specific risk assurance required by rigorous IV&V (e.g. safety critical). Even without this consideration, this approach is generally infeasible as IV&V teams cannot provide a sufficiently large and diverse collection of "approved" COTS products for developers to utilize in the face of rapidly evolving COTS