This article is part of the IEEE Reliability Society 2008 Annual Technology Report.

Risk Assessment and Mitigation of COTS Integration in High Reliability Systems

Kenneth P Rispoli
Email: Kenneth_P_Rispoli@raytheon.com

Aaron DerMarderosian Jr.
Email:Aaron_Dermarderosian_Jr@raytheon.com

Application of Commercial Off The Shelf (COTS) products in DOD applications became possible with Secretary Perry's initiative of the 1990's and was further driven by the diminishing acquisition demands of the defense industrial sector. In parallel with this the commercial sector had an explosion of advance technology driven by the internet, auto electronics, telecommunication, home entertainment and computing to name a few. This provided the developers of high reliability systems the opportunity to tap advanced COTS technology for integration into their designs without incurring the cost of design and development. However application of COTS is not without potential problems and risk to system reliability and maintainability [1]. Commercial products are designed to less stringent application needs and rapid introduction of new technology leads to shorter product life cycles. These aspects have to be addressed, weighted and if gaps exist mitigated to insure system life and reliability are not compromised. There are many definitions of COTS from components to single board to modules to system level boxes however this paper will define COTS as any electronic, electrical & mechanical item including firmware and software developed by a supplier for an open market place using industry "best practices".

Risk can be defined as an uncertain event or condition that if it occurs has a positive or negative effect on a project's objectives, in other words risk is simply the deviation from the expected. A risk assessment flow diagram as shown outlines a top down process to identify and prioritize key risks and then reduce or if possible eliminate system risk altogether [2].

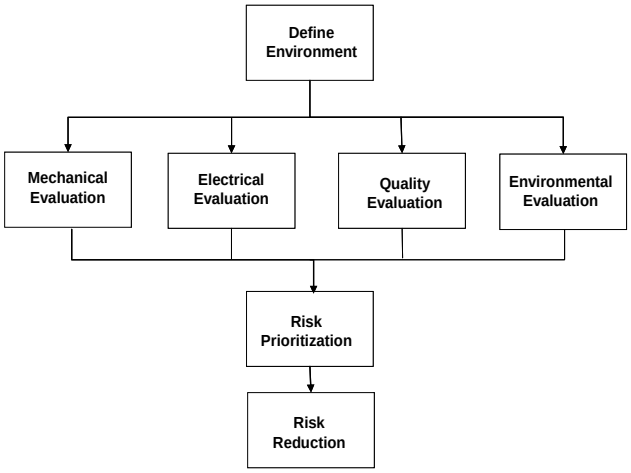

Figure 1 Risk Assessment Flow Diagram

The first step to identify COTS integration risk is to perform a full requirements review to determine critical, non-critical and requirements that can be mitigated or modified. From here a full review of the COTS supplier documentation needs to be performed to determine any gaps between

product capabilities and application requirements. Due to the often short life cycle of commercial products, obsolescence needs to be assessed. This review could include the possible insertion of future technology that would provide system enhancements.

Either following or in parallel with the specification to requirements review, a review of past application of similar products and any experience with the potential supplies should be conducted. This should include however not limited to the following:

- Comparison to similar designs to access what worked and hopefully avoid past failures.
- Lessons learned & team experiences to bring together cross discipline experiences [3].
- Knowledge base to expand beyond the immediate application.
- Trade studies to determine capabilities of the technology available
- Supplier review / assessment to choose the "best in class".

At this point in the process obvious gaps between the proposed product and the design requirement may be detected. The impact of these gaps on critical system performance will need to be assessed with one or more of the following tools.

- COTS integration program plan to control selection, evaluation, acceptance and life cycle support of COTS
- COTS supplier assessment scorecard to provide qualitative performance across all disciplines and functions.
- COTS Assessment Flow Diagram as shown above to provide a top down risk identification process.
- Failure Mode & Effects Analysis (FMEA) provides a systematic approach to identify potential failure and prioritize failures according to risk.

Design Function	Potential Failure Mode	Potential Effects of Failure Mode	C	S	Potential Cause of Failure	O	Current Controls	D	RPN	Recommended Action
12.5 db RF Gain	Maximum specified temperature of 50C will be exceeded at maximum system requirement of 70C	Mechanical mounting failure	Yes	3	Differences in package to board TCE	3	ESS	6	54	None
		Loss of mechanical integrity of internal components	Yes	5	Assembly workmanship	5	None	7	***175***	Perform DPA inspection
		Reduced Mean Time To Failure	Yes	5	Excessive junction temperature	5	Life Prediction Calculated	2	50	None
		Reduced gain	Yes	7	Excessive junction temperature	5	Undetectable	5	***175***	Perform Thermal Test Analysis

C = Is the component or operation considered critical, key or significant?
S = Severity of effects of the failure — 1 = low, 10 = high
O = Probabilty of failure occuring — 1 = low, 10 = high
D = Likelihood failure is detected — 1 = high, 10 = low
RPN = Risk Priority Nunber — S x O x D

Figure 2 Example of Component Level Design FMEA

- Risk Trade Off (RTO) to balance program risk against potential performance gains
- Un-desirable effects (UDE) analysis provides risk ranking based on occurrence.

- Non- Destructive teardown analysis provides cursory product review for possible design risks based on lessons learned and physics of failure.
- Destructive Physical Analysis (DPA) based on Physics of Failure (PoF) provides additional product design information from subject matter expert review.

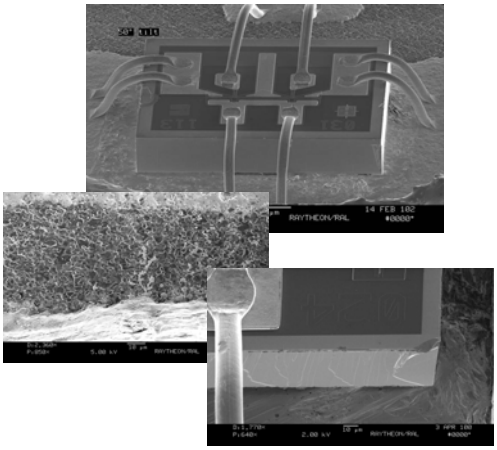

Figure 3 Example DPA Results

System requirements and product capabilities gaps can be closed or mitigated by either establishing compliance of the COTS item to the requirement or modification of the COTS item or system environments. If gaps between critical system requirements and product capabilities can not be closed the product should not be considered for the application. In some cases this might lead to a critical decision point in the process in that there does not exist any commercial product that meets the desired critical requirement. This would require possible system requirement relaxation or possible design change that would mitigate or isolate the commercial item to a level that is within the products capabilities.

To fully assess and analyze the risk associated with the application of COTS items into a design requires the involvement of all the stakeholders. This requires collaboration across electrical, mechanical, reliability, software, test, manufacturing, safety, compliance and systems engineering. These stakeholders need to work together with the supply chain, program office and contracts to insure the customer's objectives are met. The key to the successful design with COTS requires the flow of information, experience and lessons learned across all these groups. One approach is through Technical Interest Groups (TIG) that can act as a medium for focused technology interchange and connectivity to gather and disseminate technical knowledge. TIG's are structured across business unit collaboration. Since risk may not be limited to a single discipline, organized Communities of Practice (CoP) can provide a boundary less vehicle for peer-to-peer collaboration and knowledge sharing. CoP's are similar to TIG's but are aligned by product or core technologies.

In summary, COTS design integration approach should utilize existing processes with new tools to drive a successful implementation strategy through the application of a COTS management plan together with the robust risk defining tool set.

References

[1] K. Rispoli, A. DerMarderosian,"Risk Assessment and Mitigation of COTS Integration in High Reliability Systems" Minnowbrook Microelectronic Conference Oct 8-9, 2008
[2] K. Rispoli, A. DerMarderosian, "Failure Leads to COTS Integration Strategy" 2006 International Military & Aerospace / Avionics COTS Conference August 22 -24, 2006
[3] K. Rispoli, A. DerMarderosian "Power Supply Reliability- COTS Integration, Lessons Learned" October 15, 2008