TECHNICAL RISK ASSESSMENT: INCREASING THE VALUE OF TECHNOLOGY READINESS ASSESSMENT (TRA)

Rebecca Addis
Systems Engineering
Tank Automotive Research, Development, and Engineering Center (TARDEC)
Warren, MI

ABSTRACT

As the Army focuses to modernize existing ground vehicle fleets and develop new ground vehicle platforms, Program Managers are faced with the challenge of how to best choose a set of technologies for the vehicle that will be mature, be able to be integrated onto the platform, and have the capability to meet defined requirements. To accomplish this, the Tank Automotive Research, Development and Engineering Center (TARDEC) Systems Engineering Group (SEG) has championed the development of a methodology for executing Technical Risk Assessments, one of the components of the overall Risk Assessment. The Technical Risk Assessment activity determines critical technologies, assesses technology maturity, integration and manufacturing readiness, and identifies the associated technical risks of those critical technologies and other technologies of interest. A standardized set of criteria is being utilized by technology subject matter experts to perform the assessments, and has been used consistently across programs to achieve uniformity in results.

INTRODUCTION

The Tank Automotive Research, Development and Engineering Center (TARDEC) has served as an active participant in the Army's Risk Integrated Product Team (IPT) with the objective to develop a methodology for executing Risk Assessments. While the IPT, led by the Army Materiel Systems Analysis Activity (AMSAA), has worked to develop execution methods for three main facets of risk assessment, including technical, cost, and schedule risk assessments, this paper will address only the technical risk assessment portion and how it not only relates to, but also compliments the Technology Readiness Assessment (TRA) process, and is necessary to understanding the true readiness of a technology by providing awareness of the risks of integrating a particular technology onto a known vehicle platform. The process that will be described in the upcoming sections of this paper is a seven step process utilized by the TARDEC Systems Engineering Group (SEG) for executing a technical risk assessment.

WHAT IS A TECHNICAL RISK ASSESSMENT?

A technical risk assessment is a process by which a program establishes and documents the maturity or technical readiness of identified Critical Technology Elements (CTEs) or other technologies of interest. In addition to assessing technical readiness, technical risks associated with each technology that are part of the assessment are identified and documented, to include a risk rating and identification of potential mitigation strategies.

Technical Risk Assessment methodology can be applied to both Acquisition programs and Science & Technology (S&T) programs alike. For Acquisition programs, Department of Defense (DoD) TRA Guidance requires each critical technology to achieve Technology Readiness Level (TRL) 6 by Milestone B and TRL 7 by Milestone C. The assessment is performed by independent Subject Matter Experts (SMEs) selected for each critical technology. For S&T programs, Program Management requires an informal assessment to determine if and when the

technology is ready to be implemented or transitioned based on test results and level of risks identified.

The role of the TARDEC SEG, specifically the Risk Management Team, in the development and utilization of the technical risk assessment methodology began as a research effort for how technical risk assessments have been executed on other defense projects, looking at other areas of the military such as the U.S. Air Force and the U.S. Navy for guidance and to understand how to integrate this process with the technology readiness process. With the consensus of the Army's Risk IPT, TARDEC established a set of structured guidance for a unified approach to executing a technical risk assessment, with the Research Development and Engineering Command (RDECOM) SMEs responsible for actually performing the technical risk assessments, and the TARDEC SEG serving as the responsible entity for the process development, tailoring (if necessary), preparation, and facilitation of the assessment for a given program, along with responsibility for meeting the established timeline.

TECHNICAL RISK ASSESSMENT AND TECHNOLOGY READINESS ASSESSMENT (TRA)

The latest DoD TRA Guidance dated April 2011, prepared by the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)) places emphasis not only on the technology maturity, but also at taking into consideration identification of technological risks for critical technologies and potential mitigation strategies, and how taking the appropriate actions can lower the risk to levels that are acceptable to a program.

Technical Risk Assessment and TRA work hand-in-hand. One should really not be conducted without the other. Even though the technology readiness or technology maturity of a particular technology may be rated as being high, quite the opposite may be the case when it comes to assessing technical risk. The same technology may not have low technical risk. By assessing the technical risk, the risk that a technology may be unable to meet performance goals, within a specified schedule and budget can be captured. It is important that the required system capabilities or specifications of the vehicle platform onto which the technology will be integrated are available to the SMEs who will perform the technical risk assessment. This will allow the SMEs to provide a more accurate assessment of the technical risk of the technology to meet required conditions within a required timeframe. Stated another way, it will provide a baseline to identify technical risks for the technology and give the SMEs an opportunity to identify detailed mitigation steps, or at the very least, summarize a mitigation plan. In addition, technical risk assessment provides the necessary input to the readiness assessment by identifying technology integration risks on the vehicle platform being considered. It is very possible, and almost certain, that for a given technology, different integration risks will be identified based on differences in the vehicle platforms. The interfaces of the technology onto the platform must be known to adequately identify integration risks. The use of interface boundary diagrams for identifying integration risk is helpful, as it allows the technology SMEs to consider how the technology will interface with other components of the vehicle and identify risks where areas of integration uncertainty exist. In cases where integration issues or certainties in integration problems exist, there no longer is risk, but an issue that should be tracked and a corrective action applied or an alternative solution considered.

THE TECHNICAL RISK ASSESSMENT PROCESS

STEP 1: GENERATE A LIST OF TECHNOLOGY ALTERNATIVES TO BE ASSESSED

The first step in the technical risk assessment process is to establish a list of technologies and

the associated technology alternatives to be assessed. The applicable Program Systems Book may be used to generate this technology list. The list may include any number of vehicle technologies, technology alternatives being considered for assessment, and vehicle platforms being considered for integration of the technology alternatives. In this step, identifying variations in the technology alternatives from the base case vehicle or identifying technology alternatives that meet system required capabilities may be the method used for assessment selection. The list should ultimately be agreed upon by all stakeholders before moving forward in the process.

STEP 2: GATHER RELEVANT AND SPECIFIC TECHNOLOGY AND VEHICLE PLATFORM INFORMATION

Once the technology list is solidified, it is crucial to the quality of the assessment to gather as much data about the technology to provide to the SMEs as possible. The more information that the SME obtains to provide their evaluation of the technology, the more accurate the assessment will be. Specific examples of data types are:

- Purchase description
- Test data
- Prototypes
- Modeling & Simulation analysis
- Risk data
- Issues data
- Trade studies
- Engineering presentations
- System interface analyses/diagrams
- Manufacturing data
- Contractor provided data
- Requirements documents

With regard to data, if the technology being assessed is being considered for more than one vehicle platform, it is pertinent that information on each specific vehicle platform(s) being considered and the interfaces with the technology is also provided. Since the assessment involves the identification of risks related to the integration of the technology on a specific platform, the SME is dependent upon knowing as much information as possible about not only the technology, but how it will integrate with the vehicle.

STEP 3: ALLOCATE THE TECHNOLOGIES TO THE APPROPRIATE SMES AND PROVIDE GUIDANCE

Following the identification of the technologies and the gathering of the required data, the name and organization of the appropriate SME who will perform the assessment for each technology needs to be identified. Identification of the correct SME can be challenging and time consuming, but once established, the list should be documented and filed for use in follow-on assessments.

As the facilitator for the technical risk assessment, the TARDEC SEG lead will facilitate a kick-off meeting with all SMEs identified to complete the assessment. During this meeting, guidance packages will be handed out to each of the SMEs with step-by-step instructions on what is expected of them to complete as they execute the technical risk assessment, the criteria that should be used to complete the assessment, the timeline for completion of the assessment, and any points of contact they can utilize for more information or to answer questions.

STEP 4: IDENTIFY CRITICAL TECHNOLOGY ELEMENTS (CTES)

Using the DoD TRA Guidance dated April 2011 and TRA expertise, the TARDEC SEG will provide guidance to the SMEs on how to classify a critical technology. The following criteria is used to determine if a technology element is critical:

1) The technology needs to be delivered for the system to work (i.e. The technology is

needed to meet the CDD KPP requirements to a minimum threshold level)
2) The technology is a new or novel application or modified technology beyond design intent
3) The technology poses a major technological or integration risk during detailed design or demonstration

If both 1) and 2) above are true for a given technology, then it is classified as being a critical technology. If 3) above is true, the technology is also classified as being critical. The SMEs will be asked to review these statements, determine whether or not each statement applies to the technology, and provide a rationale for classifying the technology as either critical or not critical.

STEP 5: ASSESS TECHNOLOGY READINESS LEVEL (TRL), MANUFACTURING READINESS LEVEL (MRL), AND INTEGRATION READINESS LEVEL (IRL)

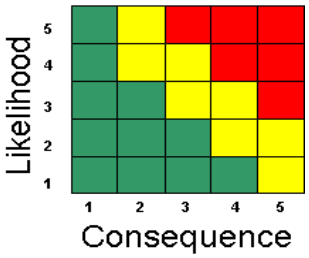
Following the evaluation of CTEs, the SMEs will be asked to provide a rating of the TRL, MRL, and IRL for all critical technologies as well as the other technologies of interest. In the case where the timeframe given for a program does not allow for this type of evaluation for all the technologies being considered, the assessment should be conducted for the identified critical technologies at a minimum. The guidance provided to the SMEs to perform the TRL, MRL, and IRL assessment consists of definitions, descriptions, and questions to consider for evaluating a particular technology. The TRL criteria to be used consists of a 1 to 9 rating scale, and is taken from the DoD Deskbook, 5000.2-R, Appendix 6, TRL and Their Definitions. The MRL criteria, rating scale of 1 to 10, is taken from the DoD MRL Deskbook (July 2011). Since no DoD standard currently exists for definitions of IRL, the development of the 1 to 9 rating scale for the IRL definitions was championed by the TARDEC Systems Engineering Group using various sources, with consensus on the definitions received from AMSAA and the rest of the Army's Risk IPT. The primary source for the IRL definitions is the Stevens Institute of Technology software integration readiness level criteria, tailored using inputs from various other areas of integration expertise. Sources of reference for the IRL criteria include: A Systems Approach to Expanding the Technology Readiness Level within Defense Acquisition, Stevens Institute of Technology, 2008; US Air Force Risk Identification: Integration & Ilities (RI3) Guidebook; Integration Readiness Levels, Naval Air Systems Command, Jennifer M. Long; Technical Risk Assessment of Australian Defence Projects, 2004, Appendix B: System Readiness Levels; DoD MRL Criteria, MRL Deskbook, July 2011; and expertise leveraged from the TARDEC Center for Ground Vehicle Domain Integration (CGVDI) group. Similar to the critical technology assessment, the TRL, MRL, and IRL assessment by the SMEs requires that a rationale for the assigned rating be provided.

STEP 6: IDENTIFY TECHNICAL RISKS, RATE RISKS, AND IDENTIFY POTENTIAL MITIGATION STRATEGIES

In addition to the assignment of the TRL, MRL, and IRL ratings, as part of the assessment, the SMEs will be asked to identify any known technical risks of the technologies. These risks should serve as input to and influence the TRL, MRL, and IRL ratings. For any technical risks identified, the SMEs will be asked to independently rate the likelihood and consequence of each risk using the standard DoD 5x5 risk matrix and the criteria as stated on the Risk Recon Risk Management Tip Sheet for high, medium, and low risks. In addition, they will be asked to identify any potential mitigation actions or strategies that they can recommend for

each risk and to capture these actions as part of their risk assessment.

Figure1. DoD Risk Matrix



To assist in the risk identification process, there are some reference tools that have been used and integrated in the "Questions to Consider" that are part of the criteria that is provided to the SMEs for conducting their technical risk assessment. These questions have been developed with the help of the U.S. Air Force Risk Identification: Integration & Ilities (RI3) Guidebook. The RI3 contains lists of questions in nine specific areas that can be used as a tool to identify risks. The questions reside in the following areas:

1) Design maturity and stability
2) Integrability
3) Software development
4) Reliability
5) Testability
6) Human factors
7) Scalability and Complexity
8) Maintainability
9) People, organizations, & skills

It should be noted that the questions in the areas above will most likely only be able to be answered at later stages in the programs lifecycle when technology development becomes more mature and there is adequate data and supporting technology information. For the earlier stages of technology development, such as the concept phase, risks can be identified by using a work breakdown structure (WBS) and system boundary diagrams.

STEP 7: EXECUTE THE RISK WORKSHOP

The first step in preparing for the risk workshop is to gather the independent SME risk ratings for any technical risks that are identified. Following identification and independent rating of all technical risks by the SMEs, a risk workshop will be hosted by TARDEC. The purpose of the risk workshop is to review each technical risk identified by the SMEs and obtain consensus amongst the technology and program stakeholders regarding the assigned risk rating. The risk ratings are assigned using the standard DoD 5x5 risk matrix and the agreed upon criteria for consequence and likelihood for high, medium, and low risks (currently using the guidance stated on the Risk Recon Risk Management Tip Sheet). Participants of the risk workshop include the technology SMEs, representatives from the Program Management Office (PM), AMSAA, the TRADOC Analysis Center (TRAC), the TARDEC program liaison to the PM (LNO), and the TARDEC Systems Engineering risk assessment team. The execution of the risk workshop will prepare the program for management of its identified technical risks. After the risks are identified, ranked, and mitigation strategies identified, they can be entered into the program's risk management tool. In this case, the Army developed and owned risk management tool called Risk Recon is used.

DELIVERABLES AND RESULTS

Upon completion of the technical risk assessment, TARDEC SEG will compile all information and results in a Technical Risk Assessment Report. The report is provided to the PM and includes a list of all technology alternatives and vehicle alternatives considered in the assessment; a list of all SMEs who conducted the assessment for each technology alternative, their organization and contact information; the guidance provided to the SMEs to conduct their

assessments including CTE identification criteria, TRL, MRL, and IRL descriptions, definitions, and questions to consider; a list of all technologies that were determined to be CTEs and the rationale provided by the SMEs; a list of all determined TRL, MRL, and IRL ratings for each technology alternative and vehicle alternative considered, based on available expertise/data and rationale provided by the SME; a list of all identified technical risks associated with each technology alternative and vehicle alternative considered; the agreed upon risk ratings (consequence and likelihood) for each technical risk identified; and any other data provided by the SMEs during the assessment.

PROGRAM BENEFITS OF PERFORMING TECHNICAL RISK ASSESSMENT

The results of the technical risk assessment, if utilized and managed appropriately, can provide many benefits to a program. The results provide an independent SME assessment of CTEs and their readiness levels using a consistent methodology across the program; they can be used to help the program to make informed decisions by providing technology readiness evaluations with regard to development, manufacturing, and integration; can identify technical risks associated with materiel solutions being considered to meet existing capability gaps; provide the associated consequence to performance, schedule, and cost if the technology is not achieved; offer valuable insight of where mitigation plans need to be developed for chosen technologies; identify up front which technical areas have the most potential to become issues; assist in determining where to focus use of limited resources (areas of highest risk); prepare risks to be transferred directly into the program's risk management tool (Risk Recon). Without conducting a technical risk assessment, it is likely that technical risks may not be identified up front, and therefore, it will most likely not be understood which technical areas have the most potential to become issues, with the most likelihood to impact program cost, performance, and schedule. It may also not be obvious as to which technology and vehicle choices offer better and less risky solutions amongst the alternatives, or which areas pose high risk, requiring the program to commit its resources to mitigation planning and execution before issues arise.

REFERENCES

[1]DoD Technology Readiness Assessment (TRA) Guidance, April 2011.

[2] DoD Deskbook, 5000.2-R, Appendix 6, TRL and Their Definitions.

[3]DoD MRL Deskbook (July 2011).

[4]A Systems Approach to Expanding the Technology Readiness Level within Defense Acquisition, Stevens Institute of Technology, 2008.

[5]U.S. Air Force Risk Identification: Integration & Ilities (RI3) Guidebook.

[6] Integration Readiness Levels, Naval Air Systems Command, Jennifer M. Long.

[7] Technical Risk Assessment of Australian Defence Projects, 2004, Appendix B: System Readiness Levels.