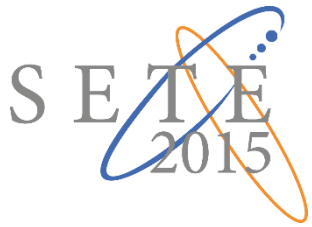


# Evaluation of a Model-based Technical Risk Assessment Methodology

Stephen Cook
Shoal Group Pty Ltd
Stephen.Cook@shoalgroup.com

Axel Bender
Defence Science and Technology Organisation
Axel.Bender@dsto.defence.gov.au

Daniel Spencer
Shoal Group Pty Ltd
Daniel.Spencer@shoalgroup.com

Michael Waite
Shoal Group Pty Ltd
Michael.Waite@shoalgroup.com

***Abstract***

Technical Risk Assessment (TRA) of Australian Defence Major Capital Equipment (MCE) projects is a core activity of the Defence Science and Technology Organisation (DSTO). In order to achieve improvement in the established TRA process, this paper explores the potential of a model-based technique to support TRA. The chosen approach is an extension of the Whole-of-Systems Analytical Framework (WSAF) that has been used successfully to capture the capability definition of a number of substantial Defence projects. Following Lukka's constructive research methodology, a TRA decision support tool demonstrator is constructed that maps candidate MCE solutions onto the WSAF model, guides technical risk evaluators systematically through the major TRA activities, and stores TRA outputs in a common relational database for traceability and future reuse. The construct is evaluated against a formal value model. It is found that model-based TRA has the potential to enhance DSTO's current TRA process and practices because it is able to achieve better justifiability of TRA assertions, improved information accessibility, and higher degrees of consistency of TRA products within and across MCE projects.

## INTRODUCTION

In accordance with the findings of the Kinnaird review of Australian Defence procurement (Kinnaird, 2003), the Defence Science and Technology Organisation (DSTO) took on the role of providing technology readiness analyses of Major Capital Equipment (MCE) projects. In 2005, DSTO implemented an approach to Technical Risk Assessment (TRA) and certification (Moon et al, 2004; Moon et al., 2005) that has since been progressively refined (DSTO, 2010), along with the Defence capability development process it supports (Defence, 2014). In 2013, the Australian National Audit Office (ANAO) recognised, firstly, that the TRA process and the assessments it delivers have improved over time in response to previous audits and internal process improvement efforts (ANAO, 2013). Secondly, it found that there was good compliance with the prescribed process. Nonetheless, drawing on the Pappas Review (Pappas, 2009), it stated that technical risk was the largest source of project slippage for post-Kinnaird projects. Accordingly, it recommended that a study be conducted to assess the accuracy of the risk assessment advice. It also mentioned that TRAs had sometimes, particularly in the past, restricted their focus to technology risk, i.e. the risk that technology immaturity

would negatively impact on project success, rather than the full range of technical risk, i.e. the risk that "a system will not reach its capability, cost or schedule goals as a result of the maturity of the underlying systems or the design, configuration, integration and implementation aspects of the system" (ANAO, 2013). Indeed, the audit cited the Chief Defence Scientist who asserted that "the major value added to the project and the senior Defence committees by the DSTO technical risk assessment process is the identification of integration risks and dependencies, particularly across projects." Thus while there is growing satisfaction with the TRA process and its deliverables, the ANAO, and anecdotally other stakeholders in the TRA process, have identified areas that could benefit from ongoing improvement as advocated by contemporary process improvement practices (e.g. CMMI, 2010).

A potential area of improvement derives from the 2013 ANAO report's realisation that a TRA needs to be specific to a particular technical solution that purportedly satisfies a capability need. Therefore it can be argued that a meaningful TRA cannot be produced without a comprehensive description of the candidate solutions in a form that directly supports reasoning about the sources of system-level technical risk and the risk sensitivity of the architectural decisions relating to the candidate solutions' system designs. It is recognised that Model-Based Systems Engineering (MBSE) approaches offer the potential to address system-level risk assessments (e.g., Estefan, 2008; Ramos et al., 2012). More generally, Friedenthal et al. established MBSE's capacity to promote the discovery of non-obvious issues and problems; to surface design and contractual problems that might otherwise be ignored; to provide traceability and transparency to all parties in a way that ensures requirements and other key design artefacts are consistently documented; and to highlight the impact of design evolution across the whole project space (Friedenthal et al, 2008). Subsequent reported benefits of MBSE include: enhanced team communications, explicit processes for reasoning about system issues, early detection of errors and omissions, improved systems architecture and detailed design integrity, and effective design traceability (NDIA, 2011; Kalawsky et al., 2013). Thus the investigation of model-based risk assessment that utilises the systems engineering models that are central to an MBSE-based project is a compelling research topic.

This paper describes ongoing research that has extended the model-based Whole-of-Systems Analytical Framework (WSAF) to provide a decision-support tool for a Model-Based TRA (MB-TRA) process and the evaluation of the potential of the resulting tool and associated process against a value model derived to assess the relative merits of different TRA methodologies. The paper opens with some background on the WSAF approach and its utility and research trajectory. This is followed by an appraisal of DSTO's current TRA process and methodology. A key aspect of the research project was to make a rigorous assessment of the potential value of any model-based methodology with its inherent tools, processes and artefacts compared with contemporary practice. To this end, significant thought was given to the selection and design of the constructive research methodology employed in the project and this is described next along with the evaluation instruments and technique used to derive the findings of the research project. The design and implementation of the MB-TRA methodology and, in particular, the TRA decision support tool follows. The paper concludes with the application of the value model to the MB-TRA decision support tool demonstrator, a discussion of the findings and a discussion of the research project.

## BACKGROUND

With WSAF, DSTO pioneered a novel application of MBSE to support Australia's Defence capability development process that uses Vitech's CORE® to capture the problem definition of a defence MCE project in the earliest phases of the project lifecycle. WSAF does not only add rigour to the Australian capability development process but also demonstrates an important new MBSE feature: the ability to hold key technical documents within the model of the system of interest, hereafter termed the *system model* (Logan & Harvey, 2011). WSAF is being used with success to define several substantial new MCE projects, such as the new submarine, the new mounted close reconnaissance capability, and a variety of command and control systems. It continues to be developed and the potential and practicality of MB-TRA approaches are actively being investigated (Tramoundanis et al, 2013). In addition, Cook et al (2014) showed how a WSAF-based model can be used to support system design

activities, system evaluation, and system trade studies.

The WSAF capability comprises six principal components (Figure 1): CORE®, the WSAF schema (metamodel) (Power and Robinson, 2010, Robinson and Graham, 2010), the libraries of functions and system implementation components, the document templates and the maps that associate document contents with model components, the scripts that generate the documents from the model, and the process used by the systems engineers to populate the model of the system of interest (Logan, 2011). The schema is an extension of the CORE® DODAF 2.02 schema (Long, 2010) that was designed to support architecture framework descriptions for complex communications, command, control, computing, intelligence, surveillance and reconnaissance system developments. The model of the system of interest is created according to a capability definition process (Logan, 2011) that follows systems engineering principles and is particularly strong on stakeholder needs analysis, mission definition, and requirements elicitation. The completed capability definition is represented as a set of entities and relationships whose semantics are defined in the WSAF schema. Textual descriptions of the system of interest are structured using the document templates with textual information distributed across the WSAF objects such that complete Operational Concept Documents, Function and Performance Specifications, and Test Concept Documents can be produced in the mandated Australian Defence formats by simply executing the WSAF CORE® scripts. For WSAF to support the TRA process, extensions needed to be made to the five WSAF components shown in green in Figure 1.

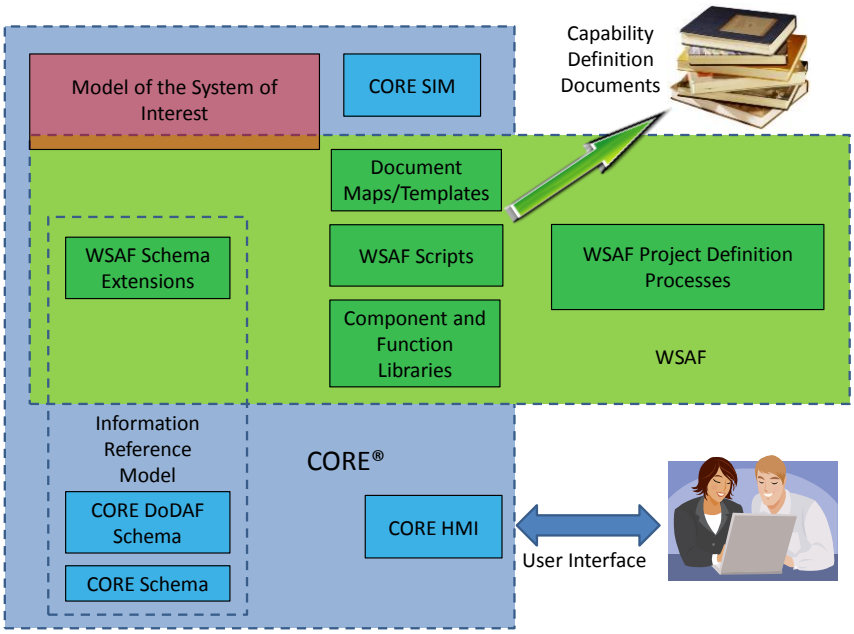


**Figure 1. WSAF foundational elements.**

In order to understand the additional functionality required to support a WSAF-based MB-TRA it is useful to examine the scope and process of TRA. TRA is risk assessment that largely conforms to the ISO risk management standard (ISO 31000, 2009); i.e. it is concerned with identifying, analysing and evaluating the effect of uncertainty on objectives. According to DSTO's TRA Handbook (DSTO, 2010), and current TRA template (DSTO, 2013), a TRA is produced by the Project Science and Technology Advisor (PSTA) and has two main concerns: (1) technology risks arising from immaturity of individual technologies, and (2) technical systems integration risks arising from technology immaturity of the interfaces between interoperating components and of the interfaces that integrate the MCE into the wider Defence capability. Technology risk assessment is supported by evaluation of the Technology Readiness Level (TRL) of the individual technologies that contribute to a capability. The System Readiness Level (SRL) scale assists in the assessment of technical systems integration risks.

The process that governs the production of a TRA, borrows key concepts from ISO 31000:2009 (ISO, 2009a) and ontology from ISO Guide 73:2009 (ISO, 2009b). DSTO's TRA commences with MCE project identification and option definition to support the establishment of the risk context (Figure 2).

Both MCE project and option definitions are external inputs into the process and are to reflect accurately the MCE capability owner's and developer's intents. The risk identification, risk analysis and risk evaluation steps mirror ISO 31000:2009's risk assessment activities (ISO, 2009a) and are followed by analysis of risk drivers, capability issues and risks other than technology or technical systems integration risks. Indicative technical risk treatment strategies are developed, before risk evaluations are aggregated to determine an overall technical risk value for each of the capability options put forward by the MCE capability developer. TRA accompanies an MCE project during capability option development, selection and introduction into service. It is, therefore, a continuous activity with various feedback loops and a requirement for good knowledge management practices.

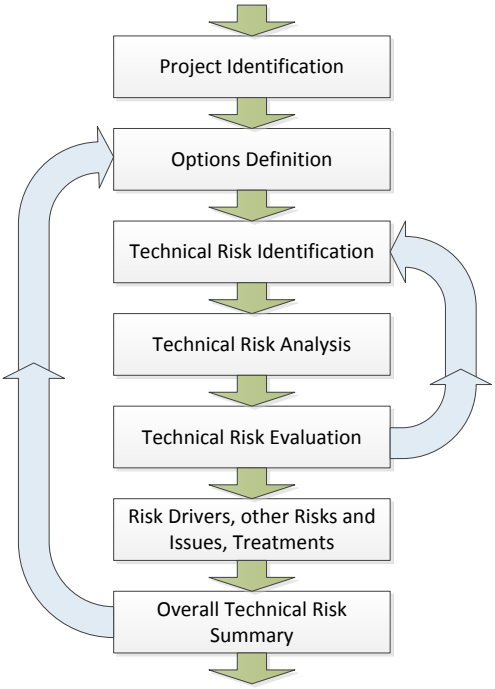


**Figure 2. The DSTO Technical Risk Assessment process.**

Discrepancies between DSTO's TRA process and ISO 31000:2009 are mainly due to DSTO's responsibility for the certification of MCE technical risk. Technical Risk Certification (TRC) is a quality assurance process that the Australian government expects to be external and independent of MCE project governance. As a consequence of its TRC responsibilities, DSTO's ability to fully integrate with an MCE project's risk management process is somewhat limited. For instance, while the internal and external risk contexts are to be identical to those of the MCE project, the TRA's risk management context (including risk criteria, thresholds for risk mitigation, etc.) is determined independently of the MCE project's risk context.

An additional complication arises because the technical risk consequence is to be derived from the effect that technology immaturity will have on the MCE project's capability, schedule and cost objectives. This is a testing demand on the PSTA, as he or she has to elicit consequence assessments "from within" the MCE project, while at the same time maintaining independence. Furthermore, in order to address the two main TRA concerns, technology risks and technical systems integration risks, the PSTA has to tackle a number of intellectual challenges associated with system needs interpretation, system conceptual design, and identifying and assessing risk. Explicitly, he or she has to: conceptualise how requirements may be realised; produce one or more high-level system models of candidate system solutions, especially in the early phases of the MCE capability development process; develop an as complete as possible list of risk events for each candidate solution from technological, performance, and integration perspectives; assign likelihood and elicit consequence of each risk event from subject matter experts including military experts, design engineers, technology experts and sustainment specialists; and synthesise an evaluation that includes all of the above and addresses the candidate solutions' fit for purpose.

From a systems engineering perspective, the PSTA must make models of the conceptual designs of the candidate solutions. These models of the system (hereafter termed the *science and technology system models*) are typically based on the PSTA's knowledge of relevant technologies and interfaces, his or her interpretation of the MCE capability needs, and his or her experience of capability implementation in real-world technologies and product designs to achieve performance specifications and fitness for purpose. Ideally, the science and technology models are congruent with the designs offered by MCE suppliers. However, *supplier models* are often not available to the PSTA, especially in the early stages of the capability development process. Thus, there are liable to be three classes of models (Figure 3): the supplier model, the science and technology model and the *system definition model* that encodes the capability owner's needs and requirements. TRA are based on the PSTA's science and technology models, which are bound by the system definition model and informed by real-world solutions. System definition dominates the science and technology models and thus the risk assessments in the early phases of the MCE project whereas the science and technology model converges to the supplier model close to and after procurement of the MCE from a prime contractor. Overall, it is expected that the science and technology models increase in fidelity as the project progresses.

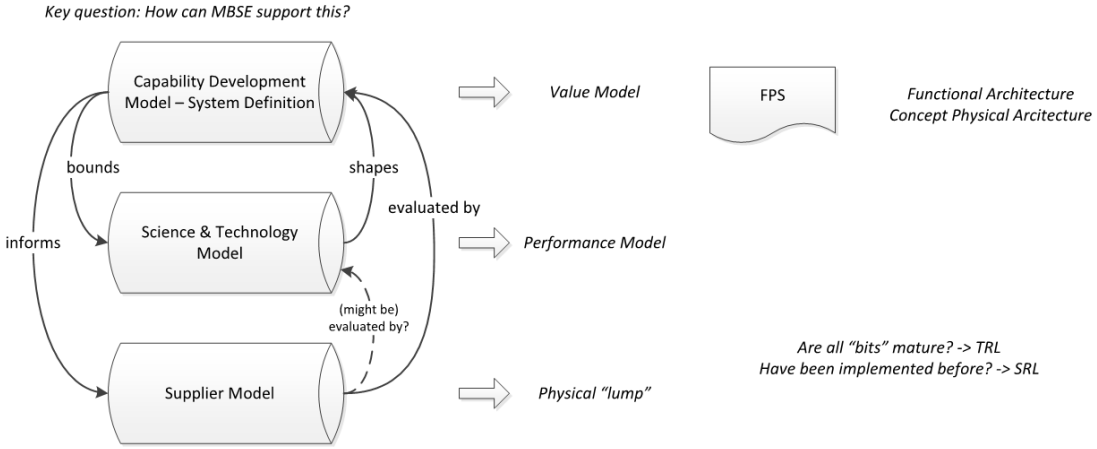


**Figure 3. The co-existing system models that may exist during the TRA activities.**

The US DoD has expressed an aspiration that one model be produced that can contain all three models (Baldwin, 2014). Cook et al 2014 found that this ideal will be challenging across the contractual boundary because the system definition and supplier models are created for somewhat different purposes and because, particularly during the tender process, commercial sensitivities and intellectual property issues will inhibit full model integration. Similarly, the science and technology models are not available to all parties. Thus for a WSAF-based TRA methodology to be successful, WSAF which to date has primarily embraced the system definition model, will need to be enhanced to provide a level of functionality of the other two models.

## RESEARCH DESIGN

The research reported here addresses the following question: "What is the potential value of a WSAF-based TRA Decision Support Tool system, in particular to the PSTA undertaking TRAs?" A constructive research methodology was found to be particularly suited because of the real-world nature of the problem in hand; the inclusion of the innovative construction of a software tool that can support design and risk analysis activities, represent knowledge in structured ways, and produce documentation artefacts through the conduct of associated processes; and the desire to link the empirical findings back to theory (Lukka 2000; Crnkovic, 2010). Table 1 illustrates the alignment of this research task with the core features of constructive research as of Lukka (2000).

**Table 1. Alignment of Research Activity to Lukka's constructive research features.**

| Constructive Research Feature | Nature of the Model-Based TRA Research Problem |
|---|---|
| Focuses on real-world problems felt relevant to be solved in practice | Defence considers TRAs to be an important task that it seeks to improve continuously. DSTO has aspiration to enhance rigour and consistency of TRAs and it is felt that it would be useful to strengthen TRA methodology through making it more systematic and through the use of an appropriate MBSE-based tool that holds the system solution definition, analysis decisions and assumptions, and simplifies the management, traceability and justification of knowledge generated throughout a TRA. |
| Produces an innovative construction meant to solve the initial real-world problem | TRA Decision Support Tool in the form of an extended version of the WSAF system concept definition capability that can support model-based TRA activities. |
| Includes an attempt for implementing the developed construction and thereby a test for its practical applicability | Production and demonstration of a prototype TRA Decision Support Tool. The potential of the tool is to be evaluated by a stakeholder group against an agreed set of criteria. |
| Implies a very close involvement and co-operation between the researcher and practitioners in a team-like manner, in which experiential learning is expected to take place | The project, in common with all WSAF implementations, is a co-operative activity between the model developers, the clients, subject matter experts and users. |
| Is explicitly linked to prior theoretical knowledge | The construction, the TRA Decision Support Tool capability, is linked to prior knowledge: WSAF background, in particular the reference model (ontology) and process. The construction draws on a large body of work on systematic design, design evaluation and MBSE. |
| Pays particular attention to reflecting the empirical findings back to theory | The Model-based TRA research uses an evaluation approach that supports publication and draws on pre-existing theory and practice. |

Given the decision to employ a constructive research methodology, the following research sub-questions were produced:

1. How is "value" best defined in the Model-based TRA research context?
2. How can the value be established?
3. What capabilities should the tool possess and how well could it perform?
4. How should the tool be developed further?

The research process is depicted in Figure 4. In the project initiation phase the project structure was established, reference materials were gathered, success-critical stakeholders were identified and the value model was developed. This was followed by the two design phases that derived the design solution for a WSAF-based TRA methodology decision tool and evaluated the evolving design against the value model. In the first implementation phase we performed the initial implementation of the TRA Decision Support Tool, investigated how the risk evaluation outcomes could be derived through the mapping of physical candidate solutions onto the WSAF model, and produced a demonstration to Stakeholder Group 1 for feedback. In the second implementation phase, we refined the TRA Decision Support Tool in line with the comments received, loaded an existing knowledge model for a distributed command and control system project, and ran an evaluation workshop that demonstrated the final version to Stakeholder Group 2 and elicited their response. The process placed strong

emphasis on engagement with TRA methodology stakeholders and employed critical reflective practice: both design and implementation phases had feedback loops back to the project initiation phase. A critical reflective approach was employed to encourage refinement of the intent of the project, the value model, and the constructive research methods on the basis of what was learned in assessing the value model and the tool and methodology under development.

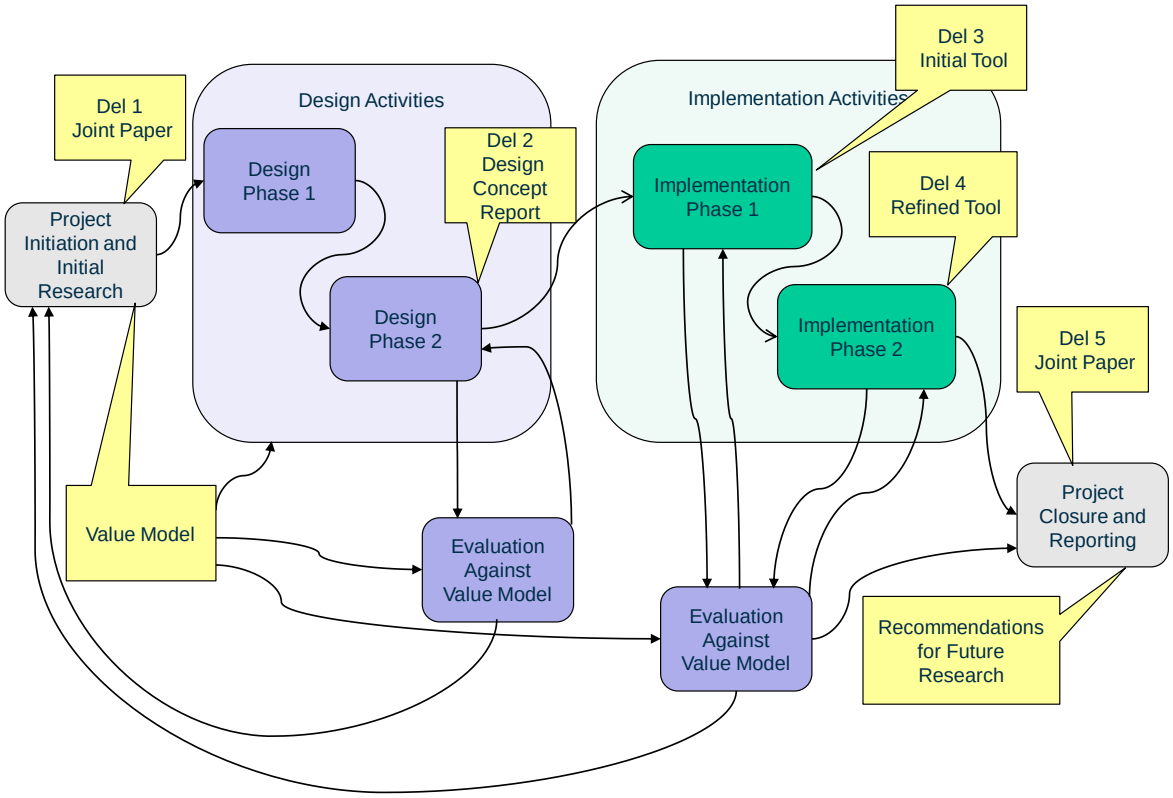


**Figure 4. Project research process showing key deliverables.**

The stakeholder community was divided into two groups. Stakeholder Group 1 comprised subject matter experts in WSAF-based MBSE approaches and in DSTO's TRA process and guidance. This group, firstly, supported the research team in determining what activities PSTAs need to perform when conducting a TRA and, secondly, produced the value model during the project initiation phase capturing the quality attributes that are desirable in a "good" TRA methodology. The second stakeholder group comprised experienced PSTAs who were not necessarily familiar with WSAF or MBSE techniques in the earlier stages of a project lifecycle. This group was engaged in the assessment of the research activity's construction (i.e. the MB-TRA support tool) during the project's implementation phases.

## VALUE MODEL AND MB-TRA METHODOLOGY EVALUATION APPROACH

The notion of the value of an engineering solution has received considerable attention and a review paper by Finkelstein and Finkelstein (1983) describes the value model used to assess constructed solutions as "the criteria which arise from the requirements and by which candidate designs may be evaluated". They go on to say that "there is generally a multiplicity of separate criteria … by which the design has to be evaluated" and then proceed to discuss multi-attribute value analysis and utility analysis as one possible mechanism for doing this. We are concerned with the relative value of a methodology and its enabling tools (namely model-based TRA) compared with the conventional TRA methodology, rather than the value of a product design but Finkelstein and Finkelstein's concepts still remain valid.

It is useful at this juncture to be clear about what we mean by a methodology. Jackson (2000; p14) and Midgley (2000) state that methodology is a kind of transferable problem solving capability. They argue that methodology facilitates, organises and reflects on the use of methods, procedures, models, tools, and techniques. Methodology establishes the principles behind the use of system models such as WSAF models and of mathematical models. A methodology draws on an agreed framework of ideas and operates on an agreed area of concern (class of problems). For the purposes of this project, the term methodology includes processes, tools, methods, and techniques as well as the world-view and philosophical position that are put together in a systematic manner to generate value (as of a value model) and to establish confidence that the value is present in the methodology's output(s).

It is also useful to define the term process as used in this paper. A process is a set of activities that are interrelated or that interact with one another (ISO 9000:2005). Processes have defined inputs and outputs and describe *what* needs to be done while leaving the selection of resources, methods, tools and techniques to the process user. Executing processes can be a routine matter or can be a highly intellectual activity such as undertaking a research process or a design process. An effective process is one that produces the defined set of outputs to the quality level expected. Processes are one of the key elements of a mature methodology, for example, the systematic design process (Pahl et al., 2007).

The instrument for determining the value of a TRA methodology is shown in Table 2 which is the fourth iteration of this research project's value model. Kroeger et al.'s approach (Kroeger et al., 2014) was adapted to suit TRA methodologies and then iterated in consultation with representatives from Stakeholder Group 1. The weighting of the importance of the attributes was determined by consolidating and normalising the ranking preferences provided by Stakeholder Group 1. Members of Stakeholder Group 1 allocated preferences based on a five point scale running from unimportant (1) to important (5).

**Table 2. Quality Attributes for a TRA Methodology.**

| Rank | Value Attribute | Description | Weighting |
|---|---|---|---|
| 1 | **Insightfulness and Comprehensiveness** | The capability of a TRA Methodology to aid an MB-TRA practitioner to uncover a comprehensive set of risks and risk drivers (some of which would not be apparent to a PSTA without the methodology) and to assess the risks appropriately. | 0.14 |
| 2 | **Justifiability** | The degree and ease with which one can demonstrate that assertions made in the TRA can be substantiated. | 0.13 |
| 3 | **Effectiveness** | The capability of a TRA methodology to produce an insightful TRA that meets consumers' needs and addresses the basic TRA problem situation as stipulated in guidelines and instructions. (The methodology will be likely judged to be effective if it enables a suitably-qualified practitioner to be able to produce the desired set of outputs.) | 0.13 |
| 4 | **Adaptability and Scalability** | The ease with which a TRA methodology can be adapted for use in different situations including by teams of analysts, potentially at distributed sites. This includes supporting distributed work practices. | 0.11 |
| 5 | **Supportability** | The ease with which a TRA methodology is able to be supported once deployed. This includes the practicality of maintaining it in use, the resource cost of doing so and the ease with which the TRA methodology can deal with changes in guidance. | 0.10 |
| 6 | **Information accessibility** | The ease of searching for and retrieving TRA-related information, intermediate artefacts, and assessment rationale over time. | 0.08 |
| 7 | **Efficiency** | The capability of a TRA methodology to achieve results with minimum expenditure of time and effort. This attribute includes the degree to which the methodology focuses on those activities necessary to achieve a high-quality TRA. | 0.07 |
| 8 | **Learnability** | The ease with which a process user is able to learn how to perform the activities of a TRA methodology. | 0.07 |
| 9 | **Consistency** | The degree of consistency of the presentation of information and the application of techniques across projects; and the consistency of information with other artefacts within the same project. | 0.07 |
| 10 | **Acceptability** | The degree to which the methodology is likely to be taken on by the users and accepted by the key stakeholders. | 0.05 |
| 11 | **Manageability** | The ease with which a process manager is able to estimate the time and resources needed to complete a TRA, determine the status of a TRA task, and apply corrective actions to maintain a specified level of effort and task performance. | 0.04 |

Given that we wish to compare the value of a new methodology to an existing methodology that is assumed to provide a good proportion of the value required of the process, it is appropriate to use an additive value function to calculate the value of the proposed methodology. This general value

function over the vector **x** of bottom-level objectives can be written as a weighted additive function of value functions on the individual objectives (Buede, 2000):

$$v(\mathbf{x}_j) = \sum_{i=1}^{n} w_i v_i(x_j)$$

where $n$ is the number of attributes ($n$=11 in our case), $w_i$ is the weighting of the $i^{th}$ attribute (see Table 2) and $j$ denotes the option being valued, and $v_i(x_j)$ is the value attributed to the $i^{th}$ attribute of the $j^{th}$ option. Given that we are concerned with the perceived relative value of the model-based TRA methodology versus the current TRA methodology, we need to evaluate $v(\mathbf{x}_{MBTRA}) - v(\mathbf{x}_{Current})$ which can be done most conveniently by asking stakeholders to assess each value attribute in Table 2 compared to the baseline of the present methodology.

$$\Delta v(\mathbf{x}_{MBTRA}) = \sum_{i=1}^{n} w_i (v_i(x_{MBTRA}) - v_i(x_{Current})) = \sum_{i=1}^{n} w_i \Delta v_i(x_{MBTRA})$$

Pahl (2007) suggests that for situations where the options are not comprehensively described it is appropriate to evaluate the difference of value attributes using low-resolution scales. Thus we asked the evaluators of Stakeholder Group 2 to assess the comparative value, $\Delta v_i(x_{MBTRA})$, using the five value levels shown in Table 3.

**Table 3. Evaluation scale.**

| Evaluation | Score | $\Delta v_i(x_{MBTRA})$ |
|---|---|---|
| Much improved | ++ | 2 |
| Improved | + | 1 |
| Not substantially changed (neutral) | = | 0 |
| Degraded | - | -1 |
| Much Degraded | -- | -2 |

As the weights in Table 2 are normalised, the overall assessment of the difference in value that MB-TRA can provide is found by matching the numeric result from evaluating $\Delta v(\mathbf{x}_{MBTRA})$ to the closest integer shown in Table 3 above. For example, if say $\Delta v(\mathbf{x}_{MBTRA})$ is -1.1 then we are able to say that the stakeholders believe that the application of MB-TRA methodology would degrade the TRA process.

## MODEL-BASED TECHNICAL RISK ASSESSMENT

The purpose of this research project is to investigate the potential of extending the WSAF MBSE methodology to provide a decision support tool and associated methodology for TRA. Using a WSAF model has the advantages of linking TRA information to common project information and enables the reuse of existing project model data to support risk assessment. It also allows the assessment outputs to be stored in a common relational database and to record TRA releases and rationale for future use.

In order to investigate the potential of this approach, a set of prototype tools were developed alongside the existing WSAF methodology. The approach taken to develop these supporting tools was:

1. Identify the high-level processes that need to take place to complete the TRA activity (whether it be using traditional or model-supported approaches).
2. Identify the existing information contained in the WSAF models that may help support these processes. This includes:
    a. Project-level information living in the models that can be consistently reused and directly placed into the TRA document output.

b. Capability and system information that can be used to inform the TRA analysis.

3. Investigate how these data could be presented appropriately to the analyst performing TRA.
4. Develop a prototype of these representations as the initial scripted support tools.
5. Identify the information gathered as part of the TRA process and the applicability of the data to the MBSE models to determine what should be stored in the model. Define the structure and interrelationships between data to update the WSAF metamodel.
6. Extend the support tools to provide support for creating this model information.

Figure 5 reiterates Figure 2 above and shows a high-level overview of the processes taking place as part of a single iteration of producing a TRA report for an MCE project. Also shown are names of the scripts (programs written in CORE®) that support the process. The scripts read the data within the model and provide automated functionality that helps the PSTA produce the set of outputs. The outputs can take the form of either additional model data or artefacts.

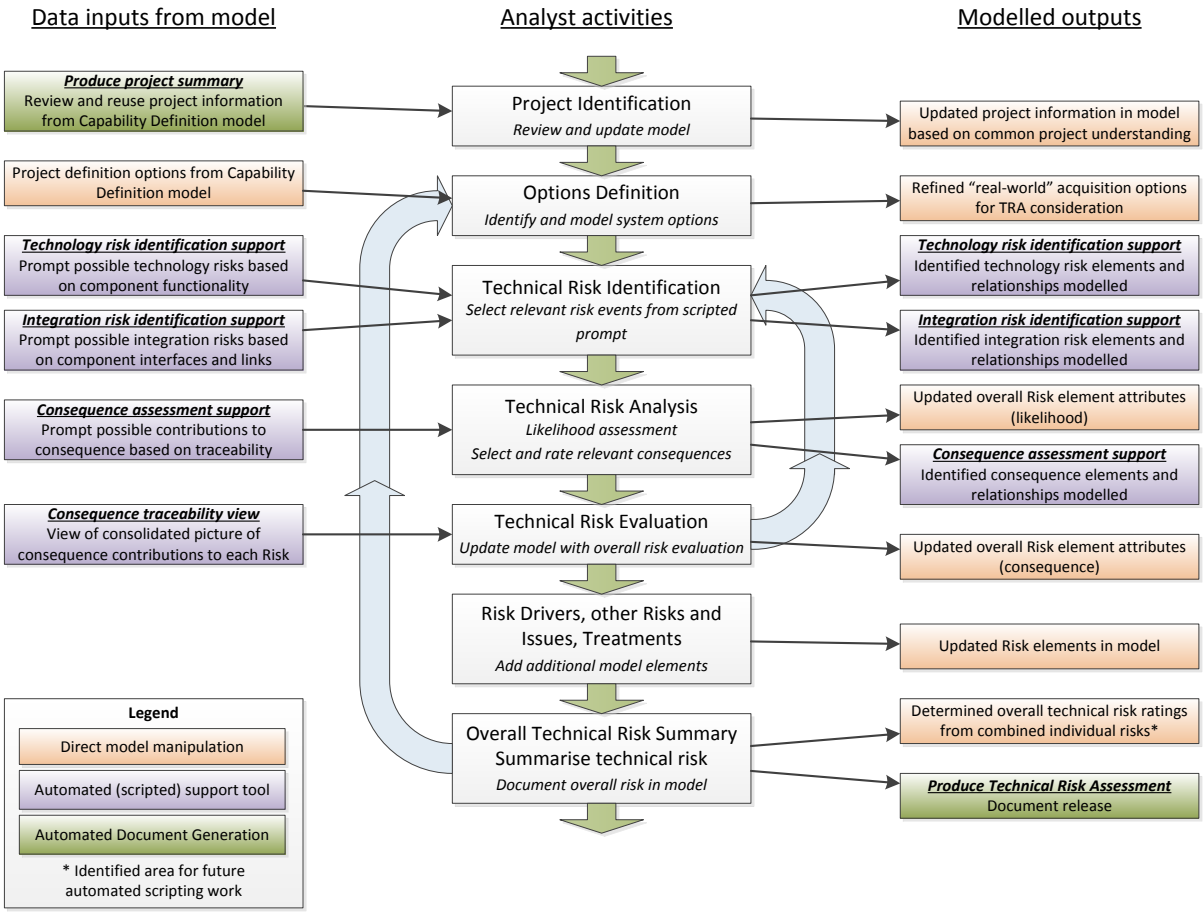


**Figure 5. Overview of model-based TRA process and supporting elements.**

The colour coding on Figure 5 indicates the level of automation provided to the PSTA through the tool suite. At the lowest level (red), the process is achieved through the PSTA directly manipulating the model through the normal CORE® interface. Even at this level, the PSTA has the advantage of a comprehensive description of the problem definition and the proposed system held in a coherent knowledge repository. The next level of automation (purple) uses data-driven user interface windows to elicit context-sensitive information and store it in appropriate places in the model. At the highest level (green), the TRA document is automatically produced from the information held within the model.

In the TRA process, the project identification step involves gathering information from the project to be used to set the context of the risk processes. This information includes the project aims, operational

concept, system context and boundaries, and key requirements. It was identified that this information was held in pre-existing WSAF models, and thus these models would be a good candidate for reuse of data from capability definition. It was also noted, however, that one purpose of explicitly defining this information as part of the TRA process is to set the project context clearly in the mind of the analyst, so a fully automated approach to producing this information would not be fit-for-purpose. To cover this, the model-based support tool produced for the project identification phase is a report generator that elucidates existing information, which requires review and agreement from analysts performing TRA. This aims to generate consistency in the understanding of the MCE project between PSTA and MCE capability developer.

The option definition process needs to create and develop solution options to the level of detail appropriate to conduct the TRA for the current project phase. Existing system models used for capability definition may include some information of relevance, however, it may not be at the desired level of detail for TRA. This is particularly true in early stages of projects, where the system definition model may be looking at a "black-box" system, possibly with some solution concept options, whereas the TRA needs to identify real-world solution options, see discussion around Figure 3 above. The model-based tool supporting this stage was designed to utilise existing information where useful, and also record in the model any additional details used for the analysis (as of the science and technology system model discussed around Figure 3 above). To achieve this, schema extensions were required in the WSAF to clearly demarcate the additional information from options in the system definition model. The extensions are based on those developed by Cook et al (2014).

Once the solutions options are defined, technical risk identification commences. This activity inherently relies on analyst expertise. However, it was identified that existing WSAF models contain information of use to an analyst identifying technical risks. A model-based tool was built to prompt the PSTA to consider the possibility of a technology risk arising from each system component performing its functions inadequately owing to immature technology. A script was also built to prompt the PSTA about the possibility of technical system integration risks arising during the integration of system components either from the integration itself or because of the components' connections to networks, links and other interfaces (both internal and external to the system of interest).

Additionally, recording the identified risks is key to being able to appropriately link all technical risk information in the model. The risk identification scripts were extended to automatically create model elements and the necessary relationships between them based on user selections. These scripts can be re-run as necessary to create more risk elements. The analyst may also manually edit the risk elements using the standard WSAF tools.

Analysis of the technical risks focuses on risk likelihood and consequence ratings for the identified risk events. This process relies significantly on professional judgement from the PSTA and from subject matter experts. A key feature of the WSAF models is the traceability of the system models to other elements that are used to define the capability. This traceability can be queried to provide supporting information to the analyst on risk consequence assessment. Figure 6 shows the possible traceability relations between element classes in the WSAF schema from a component, through a function, to the rest of the model.

The model-supported TRA includes a script that traverses all the relevant traceability relationships existing in the model, and presents these to the analyst as possible consequences of identified technical risks. For example, the decision support tool can show operational needs that will not be met due to a component being unable to fulfil its functionality. This script presents one layer of traceability at a time to avoid the proliferation of affected elements in the display presented to the PSTA.

The WSAF schema was extended to support appropriate recording of risk likelihood and consequences as part of the model-based support to risk analysis. An attribute for recording likelihood rationale was added to existing risk likelihood ratings. A new element class for recording consequences was added to provide the appropriate recording and linking of risk consequence details used in the analysis. The scripts used in the support of consequence analysis were extended to populate these elements and attributes, and relate them appropriately to the risk elements and other model elements impacted by the risk event.

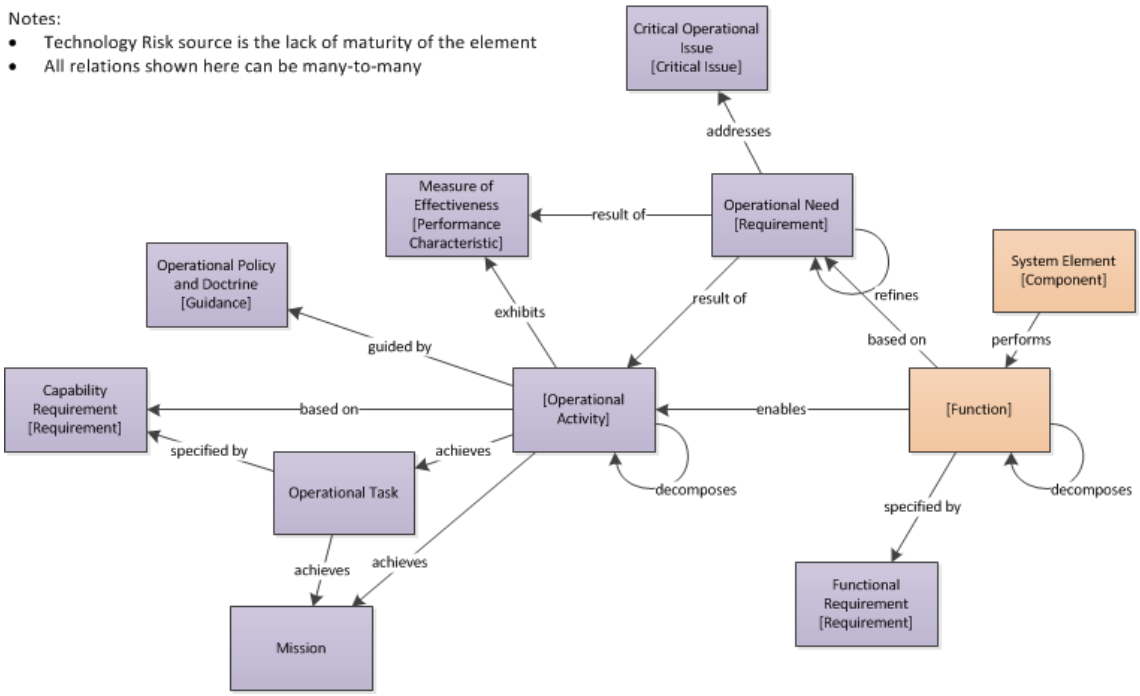


**Figure 6. Component-function traceability used to inform technology risk consequences.**

After collecting and recording the details related to risk, risk evaluation can take place. In the MB-TRA process, this involves gathering consequences of each risk together to determine an overall risk consequence rating. This is supported by specific model views, showing clearly the elements making up a particular risk. A simplified example is shown in Figure 7, looking at a fictional risk consequence for a Ground-Based Air and Missile Defence (GBAMD) system against the "technology risk that immaturity of RADAR technology results in the system being unable to meet its specification for detecting objects of interest in the assigned airspace".

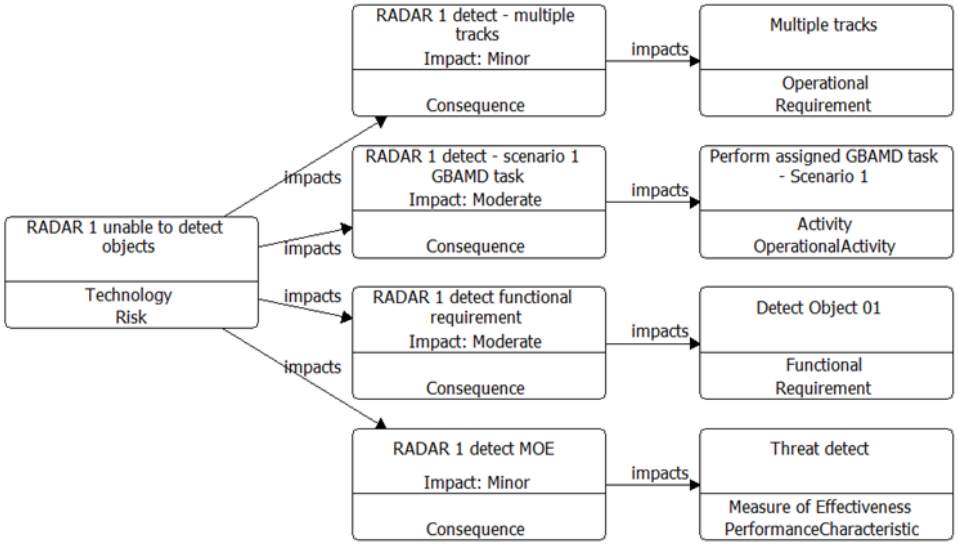


**Figure 7. Simplified example risk consequence view.**

All TRA information stored in the model can be accessed by the automated document generation capability inherent in the WSAF. This allows for TRA reports to be produced directly from the model, providing that all technical risk information has been included, and provides for baselining and re-visiting of previous TRA versions.

In summary, Implementation Phase 1 developed the following elements of the MB-TRA decision support tool:

- Modifications to the WSAF schema to incorporate the mapping of specific solution options to a conventional WSAF capability definition model;
- Production of a set of reports from a WSAF capability definition model to aid in risk consequence assessment;
- Incorporation of technical risk likelihood information into the WSAF schema; and
- Elements of an exemplar model to investigate and demonstrate risk modelling and analysis of the combination and interaction of multiple risks.

The subsequent development work in Implementation Phase 2 expanded this to include:

- An overarching process to direct how to undertake the TRA process using the prototype tools;
- Extension of the risk consequence assessment reports into a scripting tool to support and guide the user in the creation of elements and their relationships; and
- An additional scripting tool to support users in the identification of technology and technical systems integration risks.

## EVALUATION AND DISCUSSION OF THE MODEL-BASED TRA METHODOLOGY

The MB-TRA methodology with its associated process, methods, tools, techniques, and knowledge repository was evaluated by members of Stakeholder Group 2 as described at the end of the Research Design section. The quantitative results of this evaluation are shown in Table 4 and are ordered from most to least improvement over the current TRA methodology. MB-TRA was rated "Much Improved" for justifiability and information accessibility and "Improved" for consistency, insightfulness/comprehensiveness and effectiveness (see Table 2 for a definition of these value attributes). MB-TRA did not show any degradation, with MB-TRA supportability being close to "Degraded" compared with supportability of the current TRA methodology. Using the aggregation technique described in the Evaluation Approach section, the overall evaluation $\Delta v(\mathbf{x}_{MBTRA})$ was 0.7, i.e. MB-TRA constitutes an "Improvement" over DSTO's current TRA methodology.

**Table 4. Stakeholder evaluation of the model-based TRA methodology.**

| Value Attribute | Evaluation |
|---|---|
| Justifiability | 1.6 |
| Information accessibility | 1.6 |
| Consistency | 1.4 |
| Insightfulness and Comprehensiveness | 1.1 |
| Effectiveness | 0.9 |
| Acceptability | 0.3 |
| Efficiency | 0.1 |
| Manageability | 0.1 |
| Adaptability and Scalability | 0.0 |
| Learnability | -0.1 |
| Supportability | -0.4 |

Estefan pointed out in his survey of MBSE methodologies (Estefan, 2008) that model traceability is a key outcome from modelling in an appropriate modelling language and that traceability is an especially noteworthy aspect of Vitech's CORE® methodology. A major aspect of justifiability as defined in Table 2 above is the traceability of risk evaluations back through the physical solutions to the system needs (system definition model) and requirements. It is not surprising then that this

attribute was rated as "Much Improved" given that the MB-TRA approach employed inherently includes traceability.

One of the key features of all MBSE techniques is that the emphasis is placed on evolving and refining an integrated model; a "well" from which everyone can draw (Ramos et al., 2012; Friedenthal et al. 2008; Estefan 2008). Thus model-based approaches intrinsically support information accessibility and the evaluators of Stakeholder Group 2 all believed that the MB-TRA approach demonstrated that accessing the capability definition model could be expected to provide "Much Improved" information accessibility.

Consistency arises from well-defined processes and well documented artefacts. All MBSE methodologies include processes and artefacts that are based on good systems engineering practices (Estefan, 2008) but these alone do not guarantee consistency between projects or within projects. Rather, Stakeholder Groups 2's strong response to this attribute reflects more their belief that the WSAF-based TRA methodology has the potential to produce "Improved" consistency, noting that the WSAF approach is well regarded with the TRA stakeholders consulted.

It is noteworthy that Stakeholder Group 2 evaluated the effectiveness and insightfulness and comprehensiveness of the MB-TRA approach as "Improved" because both of these two attributes benefit from a systematic guidance through the steps of the TRA process as espoused by the model-based approach. The assessments indicate that it is believed the MB-TRA approach will produce an improved TRA that will better meet practitioner and consumer needs alike, may help uncover more risk events, and support a more thorough analysis of risk drivers than would be expected through the current approach.

The evaluation was performed to address the research question "What is the potential value of a WSAF-based TRA Decision Support Tool system, in particular to the PSTA undertaking TRAs?" The overall evaluation indicates that a model-based approach would enhance TRA methodology because the improved quality of the TRA was considered to outweigh the slightly negative impact (on efficiency and learnability) of introducing the methodology.

Furthermore, the written comments of Stakeholder Group 2, particularly the general comments, were positive and supportive of further development of the methodology and they provided some useful insights on the direction this development should take.

- Firstly, there was overwhelming agreement amongst members of Stakeholder Group 2 that what is needed is an improved TRA methodology and not a tool suite per se. There was interest in having libraries of components with rich data sets that could contain such things as TRL values for components, obsolescence status, intended operating environment, and examples of successful application.
- Stakeholder views were divided on what should be automated in the TRA process. Some expressed a preference for more (technology, integration, risk) modelling whereas others preferred more automation of the process. Nonetheless, there was a consistent call for more "smarts" to perform analysis on the model and for decision support to prevent the assessor from making "real blunders".
- Future work was identified to extend the model-based support to combine risks and determine overall technical risk of each system option.

## CONCLUSION

The research project set out to investigate the potential of expanding the WSAF project definition paradigm and using the WSAF models as a basis for a model-based TRA methodology. The project was conducted within a formal constructive research framework and employed a critical reflective approach to encourage refinement of the intent of the project, the value model, and the constructive research methods. A demonstrable construct was produced, i.e. methodology elements such as a process description, tool components and models were developed to a degree of functionality and fidelity that was sufficient to show PSTAs and other TRA stakeholders what a model-based TRA

methodology might encompass and how it might supplement DSTO's established TRA process. The construct was evaluated by TRA subject matter experts against a formal value model developed within the constructive research framework. It was found that a model-based TRA methodology has the potential to provide improved outcomes compared to the current approach, especially in the areas of substantiating assertions made during TRA (justifiability); ease of searching and retrieving TRA-related information, intermediate artefacts and assessment rationale (information accessibility); and consistency of information and techniques applied in the TRA process within a single MCE project and across various projects (consistency).

## ACKNOWLEDGEMENTS

This project was a joint venture between DSTO and Shoal Group Pty Ltd and the researchers are grateful for the funding from both organisations and the support provided. The researchers would also like to acknowledge the invaluable assistance of over 20 TRA subject matter experts who invested their time and intellectual effort to ensure that the value model and the evaluation of the construct produced truly reflected the view of the PSTAs that perform technical risk assessments within DSTO.

## REFERENCES

ANAO (2013), *Capability Development Reform*, Commonwealth of Australia, ISBN 0 642 81399 X

Baldwin (2014), "Department of Defense Systems Engineering Panel"*, Conference on Systems Engineering Research*, March 31 2014, Los Angeles, USA.

Buede D.M. (2000), *The Engineering Design of Systems*, Wiley, 2000.

CMMI (2010), *CMMI® for Acquisition, Version 1.3 – CMMI-ACQ, V1.3*, CMU/SEI-2010-TR-032, Software Engineering Institute, Carnegie Mellon University.

Crnkovic G.D. 2010, "Constructive research and info-computational knowledge generation" in *Studies in Computational Intelligence, 2010*, Volume 314, Model-Based Reasoning in Science and Technology, Pages 359-380.

Cook S.C. et al. (2014), "Progress on using MBSE models as key information artefacts in project tendering", *Systems Engineering Tests and Evaluation Conference (SETE 2014)*, Adelaide, Australia.

Defence (2014), *Defence Capability Development Handbook 2014*, Commonwealth of Australia.

DSTO (2010), *Technical Risk Assessment Handbook*, Version 1.1, Defence Science and Technology Organisation, Commonwealth of Australia.

DSTO (2013), *Technical Risk Assessment Template,* version August 2013, Defence Science and Technology Organisation, Commonwealth of Australia.

Estefan J. (2008), *Survey of Model-Based Systems Engineering (MBSE) Methodologies*, INCOSE-TD-2007-003-01, INCOSE.

Finkelstein L. and Finkelstein A.C.W. (1983), "Review of design methodology", *IEE Proceedings*, Vol 130, Pt. A, No. 4.

Friedenthal S. et al. (2008). *Practical Guide to SysML: Systems Modeling Language*, Morgan Kaufmann Publishers, Inc.: San Francisco, CA.

ISO (2005), *Quality management systems – Fundamental and vocabulary*, International Standards Organization.

ISO (2009a), *ISO 31000:2009 Risk management—Principles and guidelines*, International Standards Organization.

ISO (2009b), *ISO Guide 73:2009 Risk management - Vocabulary*, International Standards Organization.

Jackson M.C. (2000), *Systems Approaches to Management,* Kluwer Academic.

Kalawsky R. S. at al (2013), "Bridging the gaps in a model-based system engineering workflow by encompassing hardware-in-the-loop simulation", *IEEE Systems Journal*, 1–13.

Keeney R.L. and von Winterfeldt D. (2009), "Practical value models", in *Advances in Decision Analysis: From Foundations to Applications,* Edwards W., Miles Jr. R.F., and von Winterfeldt D, Eds., Cambridge University Press, 232-252.

Kinnaird M., Early L., and Schofield B. (2003). *Defence Procurement Review 2003* (widely known as the Kinnaird Review), Commonwealth of Australia.

Kroeger T.A., Davidson N.J. and Cook S.C. (2014), "Understanding the characteristics of quality for software engineering processes: A Ground Theory investigation", *Information and Software Technology* 56, 252-271.

Logan P. (2011), "Model based capability definition", Tutorial, *SETE 2010,* Adelaide, Australia.

Logan P. and Harvey D. (2011), "Documents as information artefacts in a model based systems engineering methodology", *Proceedings of APCOSE 2011*, Korea.

Long, D. (2010), "A model-based SE roadmap for developing DoDAF 2.0 architectures", *SETE 2010*, Adelaide, Australia.

Lukka K. (2000), "The key issues of applying the constructive approach to field research" in Reponen, T. (ed.) *Management expertise for the new millennium*, In commemoration of the 50th anniversary of the Turku School of Economics and Business Administration. Publications of the Turku School of Economics and Business Administration, Series A-1:2000.

Midgley G. (2000), *Systemic Intervention: Philosophy, Methodology and Practice*, Kluwer Academic.

Moon T. et al. (2004), *Technical Risk Assessment of Australian Defence Projects*, DSTO-TR-1656, Defence Science and Technology Organisation, Commonwealth of Australia.

Moon T., Smith J. and Cook S.C. (2005), "Technology Readiness and Technical Risk Assessment for the Australian Defence Organisation", *SETE 2005,* Brisbane, Australia.

Pappas G. (2009), *2008 Audit of the Defence Budget*, (widely known as the Pappas Review), McKinsey and Company.

Pahl G. et al. (2007), *Engineering Design – A Systematic Approach*, Springer-Verlag London.

Power W. and Robinson K. (2010), "Golf warfare: demonstrating how analytical frameworks can drive the course of complex capability analysis", *SETE 2010*, Adelaide, Australia.

Ramos A.L., Ferreira J.V. and Barcelo J. (2012), "Model-based systems engineering : an emerging approach for modern systems. *IEEE Transactions on SMC*, 42(1), 101–111.

Robinson K. and Graham D. (2010). "An improved methodology for analysis of complex capability", *SETE 2010*, Adelaide, Australia.

Robinson K. et al. (2010), "Demonstrating model-based systems engineering for specifying complex capability", *SETE 2010*, Adelaide, Australia.

Tramoundanis D., Power W. and Spencer D. (2013), "Integration risk analysis in an MBSE environment." in *Proceedings of SETE 2013*, 1–16, Canberra Australia.

## BIOGRAPHIES

***Stephen Cook*** is a systems engineering advisor at Shoal Group Pty Ltd where he works on a variety of research and system definition projects. Until June 2014 has was the Professor of Systems Engineering at the University of South Australia where he led a number of research concentrations in the field. Preceding this he accumulated twenty years of industrial R&D and SE experience spanning aerospace

and defence communications systems in both DSTO and industry. His research interests focus on the development of MBSE practices, the SE of large-scale defence capabilities, and relating complexity theory to SE practice and organisational improvement. He remains active in academic circles though his adjunct professorships at the University of Adelaide, the University of South Australia, and Loughborough University, UK. Prof Cook is a past President of the Systems Engineering Society of Australia, an INCOSE Fellow, a Fellow of Engineers Australia, a Fellow of the Institution of Engineering and Technology (UK), and a Member of the Omega Alpha Association.

***Axel Bender*** is a Group Leader and Project S&T Advisor at the Defence Science and Technology Organisation (DSTO). In these roles, he is leading interdisciplinary science teams in support of Army modernisation and Defence capability development. His research publications span a variety of disciplinary fields such as risk management, strategic planning, operations research, multi-objective optimisation, natural computing, artificial life, theoretical biology, non-pertubative quantum chromodynamics, formal languages, and fleet management. His current research interests are in the justifiability of decision support analysis, computational red teaming, and complex systems design for robustness and adaptability.

***Daniel Spencer*** is a systems engineer and the MBSE practice lead at Shoal Group Pty Ltd. He has over a decade of experience in design and development of systems solutions across a broad range of industries, both in Australia and the United Kingdom. Dan holds a Bachelor of Engineering in Information Technology and Telecommunications from the University of Adelaide. He has been working with Australian Defence and other government clients developing and refining tools and methods for a repeatable and comprehensive MBSE method, while using this approach for real-world capability definition and development projects.

***Michael Waite*** is a systems engineer with experience in the leadership and project management of large, complex socio-technical projects. Michael has demonstrated experience in the application of systems thinking techniques and has a keen interest in model-based approaches to conceptual design and systems engineering. Michael is currently the Chief Operating Officer and a Senior Systems Engineer at Shoal Group Pty Ltd an engineering consultancy specialising in the definition and design of large-scale complex system capabilities.