18. Technical Risk Analysis – Exploiting the Power of MBSE

Despina Tramoundanis\textsuperscript{1}, Wayne Power\textsuperscript{1} and Daniel Spencer\textsuperscript{2}
\textsuperscript{1}Weapons Systems Division, DSTO and \textsuperscript{2}Aerospace Concepts

Abstract

In his 2003 review into Defence procurement, Kinnaird recommended that for new acquisitions Defence undertake a ‘comprehensive analysis of technology, cost and schedule risks’ and that ‘Government needs to be assured that adequate scrutiny is undertaken ….by DSTO on technology feasibility, maturity and overall technical risk’. As a result, DSTO performs Technical Risk Assessments (TRA) to inform major acquisition decisions during the Requirements phase of the Capability Development process.

Instructions for preparing the TRA are found in the Technical Risk Assessment Handbook (TRAH)\textsuperscript{17}. These instructions provide useful guidance on the nature of technology and technical risks and means for risk discovery and assessment.

The current TRA development practice has several shortcomings, including:

- Existing templates do not necessarily fit every type of acquisition project.
- At the early stages of capability definition, before a materiel solution has been selected, system decomposition is not always possible.
- The level of discipline and rigour applied to risk analysis is variable depending on the skills of individuals.
- System integration risk does not receive adequate coverage.
- The TRA is a stand-alone document meaning that the risk analysis is not necessarily integrated with the capability definition.
- It is not easy to see how risks in one part of the system impact risks in other parts of the system that may be directly or indirectly coupled.

To address several of these shortcomings, this paper introduces the concept of Functional Risk Analysis (FRA) conducted within a Model Based Systems Engineering (MBSE) environment. FRA is a rigorous technique used to explore potential effects of functional failures or degradation that result from insufficient technical readiness, both within and between parts of a system and across system interfaces. (FRA is analogous to Functional Hazard Analysis, a technique applied in the aerospace domain.) The underlying method of FRA uses an Enhanced Functional Flow Block Diagram (EFFBD) representation of the system functionality and follows the following procedure:

1. Perform the following steps on each function in turn:
   a. Define the purpose and behaviour of the function.
   b. Consider the technologies inherent in the function and the potential failure modes that may result based on an understanding of the technology readiness,

\textsuperscript{17} DSTO, Technical Risk Assessment Handbook, Version 1.1, 2010
In his 2003 review into Defence procurement, Kinnaird recommended that for new acquisitions Defence undertake a comprehensive analysis of technology, cost and schedule risks and that Government needs to be assured that adequate scrutiny is undertaken by DSTO on technology feasibility, maturity and overall technical risk. As a result, DSTO performs Technical Risk Assessments (TRA) to inform major acquisition decisions during the Requirements phase of the Capability Development process.
e.g., ‘complete loss of function’, ‘degraded performance’, ‘incorrect operation (e.g., high, low, fast, slow etc ...)’.

c. Represent functional failure modes within MBSE model.

2. Simulate or interrogate the functional model to assess the potential impact of functional failures on downstream functions and guide detailed system analysis.

3. Record in the MBSE model the identified risks (i.e., the potential effect in terms of severity and probability of occurrence).

Once the physical system has been designed or selected, the FRA procedure can be repeated using the system architecture to assess and explore the effects of component failures or degradation that result from insufficient system readiness. The results of the FRA are recorded in the MBSE model from which the TRA report is auto-generated via the running of scripts. This paper will use a generic weapon system example to illustrate the FRA technique.

**Presenter Biography**

**Despina Tramoundanis** was a Royal Australian Air Force Armaments Engineer for 20 years before joining DSTO’s Weapons Systems Division. She is currently the S&T advisor for a Ground-Based Air and Missile Defence project. Her current research interests include development of the Whole-of-System Analytical Framework, a Model-Based Capability Engineering methodology for the provision of cross-Defence modeling, simulation, analysis and Capability Development activities. She holds a Bachelor of Engineering (Chemical) from Monash University, an MSc in Explosives Engineering from Cranfield University (UK), a Master of Defence Studies from UNSW and a Master of Defence Operations Research from UNSW.

**Wayne Power** graduated with honours from the Queensland University of Technology (QUT) with a Bachelor of Engineering (Aerospace Avionics), minor in Systems Engineering. He has spent the last six years working in Weapons Capability Analysis within DSTO’s Weapons Systems Division (WSD). His work in WSD has included weapon system integration modelling and analysis, but the major focus of his work has revolved around researching and developing the Whole-of-System Analytical Framework (WSAF). The WSAF employs a Model-Based Systems Engineering approach for the provision of cross-Defence modelling, simulation, analysis and Capability Development activities.

**Daniel Spencer** works as a systems engineer for Aerospace Concepts 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 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.
Overview

- Brief background
- The need
- What is Functional Risk Analysis (FRA)?
- FRA Implementation in an MBSE environment
- An example
Kinnaird (2003):

For new acquisition Defence should undertake a ‘comprehensive analysis of technology, cost and schedule risks’

‘Government needs to be assured that adequate scrutiny is undertaken ... by DSTO on technology feasibility, maturity and overall technical risk’.
Technical Risk Assessment

- Pre-1\textsuperscript{st} Pass: TRI
- 1\textsuperscript{st} Pass & 2\textsuperscript{nd} Pass: TRA
- Technical Risk Assessment Handbook (TRAH)
- TRA templates
- Based on
  - Technical Readiness Levels (TRLs)
  - Risk assessment matrix
Shortcomings

- TRA templates do not fit every type of acquisition
- Work only with materiel solutions
- Quality depends on the skills of individuals
- Inadequate analysis of:
  - System integration risk
  - Risk coupling
- TRA is a stand-alone document

The Need

A rigorous technique to explore the potential effects of functional failures and performance degradation that result from insufficient technical readiness, both within and between parts of a system and across system interfaces
What is FRA?

A rigorous technique used with an MBSE methodology to explore the potential effects of functional failures and performance degradation that result from insufficient technical readiness of a system and its interfaces

Application of Functional Hazard Assessment methods to risk analysis
Functional Hazard Assessment
(modeled from SAE ARP4761)

1. Description of System Functions
2. Functional Failure Analysis
3. Determine:
   - Associated Failure Conditions
   - Effects
   - Failure Condition Classification
   - Detection
   - Actions
   - Justification Material
   - Function Development Assurance Level
4. Derive Requirements and produce Failure Condition List for lower-level analysis

FRA Procedure Overview

- Commence with a functional decomposition of the capability system and include the system interfaces.
- Define the purpose and behaviour of each system function.
- Consider potential failure modes of each function eg loss or degradation of function
- Determine the effect of each failure on system function and operational / mission outcomes
- Identify, analyse and record the risks (impact and likelihood)
Applying FRA as part of an MBSE methodology

How FRA fits in with MBSE

Utilise MBSE capability model to provide context

Structured analysis framed on functional and system definition

Likelihood: MBSE provides structure to elicit and store the likelihood information

Consequence: (quick look) Structure analysis to determine flow on effects and impact to mission outcomes (model traceability)

(rigorous) Perform discrete simulations of different risk events

Provide structure and simple scripting to determine overall risk level

Figure 3: Risk management process
Required model state

- Functional decomposition defined
- Functional flows modelled
- Information flows modelled and connected to functions

If a materiel system does not exist:
- Perform risk analysis on available technologies to perform functions
- Identify indicative risk areas in achieving functional and operational outcomes due to technology maturity issues
- Repeat FRA when the materiel system is known.

Model elements and relationships

- Component 1 connects to Component 2
- Function 1 performs and decomposes into Function 1.1 and Function 1.2
- Function 2 transfers inputs to Item, which in turn outputs to Function 2
- Link connects to both component 1 and component 2.
Model elements and relationships

Functional Decomposition
FRA Process
(Modified FMEA Process)

1. Determine objectives
   - To identify, analyse and evaluate risks related to technical
     readiness
2. Identify starting points for analysis (*mode*)
3. Identify *upstream mechanisms* (causes)
4. Identify *downstream effects* (impact on system
   performance and mission outcomes)
5. Analyse and record overall risk (*trace to affected
   mission outcomes*)

3. Consider upstream causes of functional failure

- Use tool support to produce report on “success path”
- Start from chosen function, consider:
  - “*triggered by*” items: Will always impact flow
  - “*inputs*” items: May affect quality of flow
- For the items collected, consider the other functions
  they are “*output from*”:
  - If multiple “*output from*”: Redundancies in path
- Continue backwards through the success path
Upstream risk patterns

Redundancy – decreased likelihood

4. Consider downstream effects of functional failure

- Use tool support to produce report on “success path”
- For each function, consider the items it “outputs”
- For each item, consider:
  - “triggers” functions: May impact flow, but also need to consider if other functions are able to output this item
  - “input to” functions: May affect quality of flow
- Continue forward through the success path
Downstream risk patterns

Critical path – significant consequence

Redundancy – decreased consequence

Analyze and record resulting risk

- Create technical risk element in the model, related to the Function / Item / Link analysed
- Record risk ratings (likelihood, consequence) and mitigation strategies
- Output Technical Risk documentation from the model

- Risk can result in a design decision and derived Requirement
5. Analyse and record resulting risk

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Consequence/Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Minor</td>
</tr>
<tr>
<td>More Than Likely</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>Less Than Likely</td>
<td>LOW</td>
</tr>
<tr>
<td>Unlikely</td>
<td>LOW</td>
</tr>
</tbody>
</table>

TRAH Risk Likelihood / Impact Matrix

Example - Ground Based Air Defence
Upstream functional traceability

To guide the analyst in understanding the potential influences on critical functions

*What’s the likelihood of failure?*
What is the likelihood of “Guide to intercept point” failing to achieve required performance?

Inputs relationship indicates non-critical information flow. Will still perform function without (reduced likelihood of failure)
Multiple sources indicates redundancy (reduce likelihood of failure)
**Upstream**

What is the likelihood of “Guide to intercept point” failing to achieve required performance?

Considerations for analysis:
- Redundancy in “target state”
- Can still perform function without external inputs

**Downstream functional traceability**

To guide the analyst in understanding the potential impact of a system component underperforming

*What’s the consequence of failure?*
**Downstream**

What's the impact if the in-flight target updates fail?

**Benefits of methodology/Conclusions**

<table>
<thead>
<tr>
<th>Issues with current practice</th>
<th>FRA Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRA templates do not fit every type of acquisition</td>
<td>Focus of risk analysis is on a model of the capability of interest, not on a document template. Documentation is derived from the risk analysis, not the other way around.</td>
</tr>
<tr>
<td>Need to assume a materiel solution</td>
<td>FRA can be applied to a functional description of a system using knowledge of available technologies (pre-2\textsuperscript{nd} pass) and is repeated for physical systems at 2\textsuperscript{nd} Pass.</td>
</tr>
<tr>
<td>Quality depends on the skills of individuals</td>
<td>Provides a rigorous process to assist in the analysis of whole of system technical risk</td>
</tr>
<tr>
<td>Inadequate analysis of: System integration risk Risk coupling</td>
<td>Process guides analyst through the potential influence of technologies on other systems and sub-systems. Focus is on potential impact of integration risk</td>
</tr>
<tr>
<td>TRA is a stand-alone document</td>
<td>Analysis performed in and risks recorded in the same model OCD and FPS definitions. Completely traceable: a single source of truth.</td>
</tr>
</tbody>
</table>
Additional Benefits / conclusions

Resulting benefits from using MBSE for risk analysis:
- Capture and trace risks and issues to mission objectives
- Capture non-technical risks/issues (such as fitness-for-purpose)
- Can extend FRA process to system assessment
- Resulting derived requirements can be traceable back to the analysis process