Integration Risk Analysis in an MBSE Environment

Despina Tramoundanis, DSTO
despina.tramoundanis2@dsto.defence.gov.au

Wayne Power, DSTO
wayne.power@dsto.defence.gov.au

Daniel Spencer, Aerospace Concepts Pty Ltd
daniel.spencer@concepts.aero

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’ (Kinnaird 2003). As a result, the Defence Science and Technology Organisation (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 DSTO Technical Risk Assessment Handbook (TRAH) (DSTO 2010). These instructions provide guidance on the nature of technology and technical risks and the mechanics of assigning risk ratings and emphasise the importance of system integration risk as an important consideration in new capability projects.

In previous reported work (Tramoundanis et al 2012), the authors describe the Functional Risk Analysis (FRA) methodology and its application in a Model Based Systems Engineering (MBSE) environment to undertake system technical risk analysis. This paper demonstrates how FRA may be extended to conduct rigorous and robust Functional Risk Analysis for System Integration (FRASI). When applied as part of an MBSE approach, FRASI consists of the following:

- Utilisation of MBSE tool support to highlight redundancy, critical paths and key interfaces between systems of interest;
- Analysis of results produced by the tool in order to evaluate and focus on the key areas of system integration risk;
- A process, schema and language for recording results of FRA analysis in the MBSE model; and
- Utilisation of MBSE tool support to report on results of the FRA process.

This paper uses a generic weapon system example to illustrate the FRASI technique.

DSTO’s TECHNICAL RISK ASSESSMENT

Defence projects are often subject to high levels of technical complexity and risk, are extremely costly, and can take many years to realise (Helmsman 2010). A recent review of Australian project performance showed that technical risk “is the largest driver of post-approval [schedule] slippage”, and that “developmental and Australianised projects are, by definition less technically mature than [Military off the Shelf projects], and are far more likely to exceed original cost estimates” (Pappas 2009). Under the Kinnaird capability development process, the Chief Defence Scientist (CDS) provides an independent statement of the level of technical risk associated with projects via the Technical Risk Certificate (TRC). TRCs are based on Technical Risk Assessments (TRA)\(^1\) prepared

---

\(^1\) The TRA is preceded by a Technical Risk Indicator. The latter provides a high level assessment of the maturity of technologies inherent in candidate capability options and their associated technical risks and is used internally by Defence to support the down-selection of capability options to be taken to first pass consideration (Defence 2012).
by DSTO. Both the TRA and TRC are updated at each stage of the capability development process (Defence 2012).

DSTO’s assessment of project technical risk performs two key functions. First, the TRC provides government with independent advice on: the likelihood that the technologies inherent in a project will become fully mature within the endorsed project schedule; whether these technologies are fit for purpose; and what significant technical barriers there are to successful integration of the various elements of the system under acquisition and the wider ADO capabilities (DSTO 2010). Second, the TRA identifies technical risks and evaluates their likelihood and impact, evaluates the likely effectiveness of any planned risk treatment strategies, and proposes risk treatment strategies (DSTO 2010).

The DSTO TRA Handbook (TRAH) (DSTO 2010) outlines a five-step process as shown in Figure 1, and employs two ordinal scales, the Technology Readiness Level (TRL) and the System Readiness Level (SRL) which describe the maturity of individual technologies and the maturity of systems and their integration, respectively (DSTO 2010). The risk assessment process and procedures outlined in the TRAH are based on the Australian Standard for risk management (Standards Australia 2009) and include making separate assessments of the likelihood and consequence of an identified risk event. The likelihood and consequence ratings are then combined to generate a risk level.

| Step 1: Establish the context of use and the project objectives. |
| Step 2: Identify the sub-systems of the capability. |
| Step 3: For each sub-system, identify the key underlying technologies, their maturity (via TRLs), the likelihood that the technology will not mature in the time required by the project, the impact on the project’s objectives if the technology does not mature or achieve full potential, and hence the technology risks. |
| Step 4: Consider the integration of the sub-systems and the system (via SRLs), and identify the key technical risk sources in making the sub-systems and system function as an integrated whole, and then assess the likelihood that the sub-systems or system will not be integrated in time, the impact on the project’s objectives, and hence the technical risks. |
| Step 5: With the technology and system level risks identified, make an assessment of the overall level of technical risk to the project. |

Figure 1: DSTO Technical Risk Assessment Process (DSTO 2010)

The TRAH delineates between technical risks and issues by observing that technical issues reportable by DSTO are existing conditions or circumstances “that prevent the capability option achieving the objectives of the project” (DSTO 2010). Such issues are termed fitness-for-purpose issues and are those existing attributes of a capability system which affect achievement of the desired operational capability. Defence often acquires commercial or military-off-the-shelf equipment in an effort to reduce project risk. The TRAH cautions that technical risks may reside in the operation of such systems in novel ways, in new environments, or with different interfacing systems and may present risks. Off-the-shelf acquisitions may also exhibit technical fitness-for-purpose issues by their nature. Such issues potentially will impact system functional and non-functional performance.

WHY MBSE-ASSISTED TECHNICAL RISK ASSESSMENT?

An MBSE methodology has been employed within Defence to support capability requirements definition on several projects (Robinson et al 2010). For these projects, the full extent of existing project knowledge is contained in the model, including strategic guidance, capability missions, operating concepts, employment scenarios, user needs, capability requirements etc. The capability definition documents are generated by running scripts which interrogate the model. Accordingly, the MBSE environment provides DSTO analysts a single source of knowledge that is traceable and readily accessible. This helps overcome any potential for basing a technical risk analysis on incomplete,
inconsistent or dated information. Further, a technical risk assessment conducted within an MBSE environment is directly traceable to the capability definition so that any changes in the latter will cue a review of the risk analysis.

Notably, the MBSE capability definition also includes the full operational context, satisfying the very first step in the DSTO TRA process as shown in Figure 1 without the need for further effort by the DSTO analyst. The MBSE model also contains functional flows which provide another important benefit: complex Defence systems are often reconfigurable for specific missions and hence the system architecture may change depending on the employment scenario and the criticality, and hence the risk consequence, of particular system functions and components may change for different missions and employment scenarios. These aspects are readily represented in and analysed via the functional flows in the model so that the analyst’s effort and the potential for interpretational error is reduced. Content for inclusion in the TRA document can be produced directly from the model by running scripts, in a similar way as capability definition documents are automatically generated from the model.

Finally, integrating the TRA content into the MBSE environment makes it immediately accessible to all project staff and for other purposes. For instance, the TRA content may be used for the generation of project risk logs and risk management plans. It may also be used for the development of the Test Concept Document and the project Test and Evaluation Master Plan.

AVAILABLE TECHNIQUES AND TOOLS

Risk Identification and Assessment Methods

Several methods are available for structured risk identification; some relying on a work breakdown structure and others relying on system capabilities, requirements and processes (Conrow 2003). Several of these methods were reviewed and are described briefly below. Each of these methods focuses on the identification and early analysis of risks. Additionally, as will be seen, each of these methods conducts risk analysis based on system functions and processes.

Model-based Behaviour Tree Safety Risk Assessment

A model-based approach to safety risk assessment has been proposed by (Lindsay et al 2012) which involves developing a behaviour tree (BT) model from a set of natural language requirements, identifying hazards and then determining which functional failures and system hazards are of interest. The BT is then extended to include the events that might contribute to hazards and is used to check if the hazard conditions are reachable.

OMG System Assurance Architecture Risk Analysis

The Object Management Group’s (OMG) System Assurance Task Force has investigated the use of analysing architecture risk using the DoDAF (Calloni 2011). By employing a common model they suggest that all information elements (including risks, threats and vulnerabilities) can be collated and more adequately managed. They also describe how architectures can be used to underpin a “systematic methodology for identifying” and analysing risks (Calloni 2011).

Failure Mode and Effect Analysis (FMEA)

The Failure Mode and Effect Analysis (FMEA) technique identifies all potential failure modes, the effects of these failures and the mechanisms causing them (ISO/IEC 2009). Failure modes are defined as observable divergences from the design intent of the system. When considered against the designed functions of a system, failures result from the inability of the system as a whole to perform the function.

Steps in the FMEA process include breaking the system down into components, then functions of each of these components. For each of these functions, every conceivable failure is considered. The risk analyst must determine the mechanisms that might produce these modes of failure and the potential effects of the failure amongst other considerations. FMEA can be applied as either a qualitative or quantitative approach.
FMEA is a comprehensive and detailed technique, with a significant amount of material available to support the analyst.

**Hazard and Operability Studies (HAZOP)**

A Hazard and Operability Study (HAZOP) is a very structured and systematic approach to risk identification and determination of consequences (ISO/IEC 2009). HAZOP was initially developed for the chemical industry, and has been further developed as a more general hazard analysis procedure. The concepts of the HAZOP process can be applied to general Risk Management, and is most useful early in the design stages for a system.

It is similar to the FMEA process in the identification of failure modes, causes and consequences. In addition to the FMEA process described above, HAZOP provides some useful “guidance words” that can be used to help the analyst classify failures. These guidance words are to be used against every parameter on each defined system function, and prompt the analysts to consider functional failure modes that may not have been considered otherwise. The result of the HAZOP process is a qualitative risk assessment.

**Functional Hazard Analysis (FHA)**

As defined in the Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment (SAE ARP 4761), Functional Hazard Analysis is a comprehensive technique used in aircraft design to identify system functional failure conditions and analyse the consequences of these failures.

The FHA process is designed for safety-critical systems and was developed for the civil aviation industry. Techniques used in FHA can be applied to identify system failures, whether or not the system is safety-critical. When applying similar techniques, it is important that the level of detail in the process is appropriate to the level of risk of the system being analysed.

Figure 2: Simplified Functional Hazard Assessment process for a generic system (modified from (SAE ARP 4761))

Similar to the techniques described above, FHA is based on an initial functional decomposition of the system. A system-level FHA is a qualitative assessment of risk relevant to a system. The FHA is performed iteratively on the system, working from system-level down to sub-systems, and becoming more refined as the system is defined.

Figure 2 shows a simplified version of the FHA process, modified to cover a generic system of interest. The starting point for analysis of the system is the highest-level requirements, including any
regulations applicable to the system being designed. As can be seen in this flowchart, lower-level (sub-system) requirements can be derived from the output of the system-level FHA, which incorporates the safety and reliability of the system directly into the system design.

Technology Maturity Measures and Calculators

Defence has adopted the use of TRLs and SRLs to assess the maturity of technologies and systems. The use of TRLs and SRLs, first pioneered on NASA programs, is now widely used by the US and UK defence departments (US DoD 2011, UK MoD 2013, Fernandez 2010). Several other readiness levels are used in the US including: Manufacturing Readiness Level, Integration Readiness Level (Sauser & Forbes 2009 and Sauser & Ramirez-Marquez 2009) and Software Readiness Level among others (Bilbro 2007). The Advancement Degree of Difficulty (AD2) measure developed by NASA and used in some parts of the US Defense Department (NASA 2009a, NASA 2009b, Bilbro 2008), combines these other measures into a single index which describes what is required to progress a system, sub-system or component to a higher TRL.

In the US and UK defence organisations, the use of these technology maturity measures is supported by tools (Nolte et al 2003) which are generally process-based, best practice systems engineering models that lead the assessor through a series of questions about whether particular steps in the product development process have been completed successfully. The assessor’s responses are entered into a spreadsheet tool which then generates a TRL, SRL or AD2. The Technical Risk Identification and Mitigation System (TRIMS) is another such tool (DAU 2013, Willcor 2009).

While it is reasonable for DSTO to adopt the TRL and SRL concepts, introduction of the associated calculators would create more problems than it solves in that the data required to populate them is significant and not readily available before tender submissions are received. Informal discussions with DSTO staff has identified that the unavailability of data is already a significant impediment to performing TRAs. This problem would be increased manifold if the TRL and SRL calculators were to be introduced. Additionally, the use of the calculators in the US and UK is to shape developmental projects whereas DSTO’s role is to inform decision makers of technical risks associated with acquisition projects.

There is a need therefore, for a form of aid to DSTO staff that at once exploits their technical and analytical expertise and provides systems engineering rigour, without adding unnecessarily to the requirement for data that may not be readily available. In addition, this form of aid should not rely on the availability of a system breakdown because, as was noted earlier, this is often not available until tenders are received and not helpful for reconfigurable systems.

PROPOSED APPROACH – FUNCTIONAL RISK ANALYSIS (FRA)

To that end, the Functional Risk Analysis (FRA) methodology was developed for employment as part of an MBSE methodology and offers a rigorous, structured means of undertaking technical risk analysis (Tramoundanis et al 2012). In common with the risk identification and analysis methods reviewed previously, the FRA commences with a system functional breakdown. Indeed, the FRA process is a modified and simplified FMEA process, following the procedures of FHA and drawing on guidance words in a similar fashion to HAZOP.

The present work extends FRA to system integration risk analysis. It is important to note that FRA is a rigorous method that has been developed to aid DSTO staff in identifying technical risks and assessing their likelihood and impact, as required by the TRAH (DSTO 2010). The output of the FRA is a candidate list of risks and a first indication of the risk levels. These results require further qualitative or quantitative analysis by subject matter experts in order to provide a final risk assessment.

Required MBSE Model State

Before FRA techniques can be employed, the MBSE model of the capability system being analysed requires a certain level of maturity. FRA was developed to provide a mechanism for assessing technical risk in the absence of detailed system definitions. FRA is performed commencing with the functional and item flow (which could include data or physical entities etc.) description of the system. This enables the analyst to assess risk, prior to the selection of a materiel solution. In other words,
while what the system needs to do is understood, the nature of the physical system is unknown. Therefore, at commencement, FRA requires the model to be mature in the following areas:

- Functional decomposition,
- Functional flow, and
- Item and control flow.

The MBSE capability definition model used to produce a complete Operational Concept Document and Function and Performance Specification for a Defence acquisition project will have functions decomposed to a level of detail required for system definition (CDG 2011). However, this functional decomposition may not include a full model of the functional behaviour, as this is not necessarily required at this stage of the capability development process.

In order to complete an MBSE-supported risk analysis process as described in this paper, there is a need to develop the functional flows to a sufficient level to capture the system behaviour in all employment scenarios, including the item exchanges.

To create this behaviour model, internal scenarios can be developed from the functional decomposition. It is important that within these internal scenarios, all items being exchanged are modelled in order to fully define the system behaviour. As per all analysis, the quality of the risk analysis is largely dependent on the quality of the model structure and content (“garbage in, garbage out”).

**FRA Process**

The FRA methodology as described previously by the authors (Tramoundanis et al 2012), adapts a Failure Mode and Effect Analysis (FMEA) process to derive the steps summarised in Figure 3. This section describes the process within the FRA methodology.

![Figure 3: FRA Process](image)

**Step 1 – Determine analysis objectives**

This step is crucial in determining the overall objectives of the analysis and to determine the appropriateness of the FRA methodology to the task. FRA should be applied when the objective of the analysis is to identify, classify and treat risks related to technical readiness (Tramoundanis et al 2012). This applies for individual and integrated systems.

**Step 2.1 – Identify function of interest and failure modes**
The FRA process adopts a systematic approach to identifying risks related to each individual function and item transfer within the system (Tramoundanis et al 2012). This step consists of identifying the function of interest as the starting point of analysis, and determining the failure modes of this function. Consideration of the failure modes should include all key output parameters of the function. The function of interest should be analysed to determine the various ways in which it may fail to meet its designed intent. To support the analyst in this process, some guidewords for consideration against these parameters have been included in Table 1 below. An example showing these guidewords as applied to a missile function named “Receive target updates”, as part of a generic Ground-Based Air Defence (GBAD) system is used to demonstrate the use of these guidewords (the GBAD example is explained further in the following sections).

<table>
<thead>
<tr>
<th>Guidewords</th>
<th>Example of use on &quot;Receive target updates&quot; function</th>
</tr>
</thead>
<tbody>
<tr>
<td>No / Not / None:</td>
<td>Function &quot;receive target updates&quot; doesn't run: Missile continues on pre-determined course.</td>
</tr>
<tr>
<td>Opposite / Reverse:</td>
<td>N/A</td>
</tr>
<tr>
<td>As well as:</td>
<td>Multiple target updates received, with conflicting information: May need to have some deconfliction.</td>
</tr>
<tr>
<td>Part of:</td>
<td>Partial target data received: Is the partial data useful?</td>
</tr>
<tr>
<td>More / Higher / Excessive:</td>
<td>N/A</td>
</tr>
<tr>
<td>Less / Lower / Not Enough:</td>
<td>Target updates are not received often enough to accurately track the target.</td>
</tr>
<tr>
<td>Other than / Replaced by:</td>
<td>Incorrect/false target data updates received: Need to verify information?</td>
</tr>
<tr>
<td>Elsewhere:</td>
<td>N/A</td>
</tr>
<tr>
<td>Early:</td>
<td>N/A</td>
</tr>
<tr>
<td>Late:</td>
<td>Delays in receiving target data: Missile continues on pre-determined course.</td>
</tr>
<tr>
<td>Before:</td>
<td>Updates received in wrong sequence.</td>
</tr>
<tr>
<td>After:</td>
<td>As above.</td>
</tr>
<tr>
<td>Slow:</td>
<td>The frequency of target updates is too slow: Missile may run out of time to change course.</td>
</tr>
<tr>
<td>Fast:</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Table 1: Demonstration of guiding words used to explore functional failure modes

Although all functions should be investigated, the functions that should be the focus of the analysis should be those of critical importance to the overall mission objective or those likely to fail. If the
function of interest has a high likelihood of failure, the effort should be concentrated on Step 2.3, identification of downstream effects. If the function of interest has a high impact of failure, concentrate the analysis effort on Step 2.2, identification of upstream mechanisms.

Note, steps 2.2 and 2.3 are repeated for each identified function of interest.

**Step 2.2 – Identify upstream mechanisms (causes)**

For each function of interest, the potential external influences on performance are assessed. This focuses on identifying what potential causes of failure exist outside of the function of interest. This step is crucial for mission critical functions (i.e. what are the likely causes of that function underperforming or failing?). The model interrogation capabilities of MBSE tools can be used to trace the information and logical flow that result in, control, or input to the function of interest. This can be achieved by specifying the “upstream” relationships of interest and allowing the tool to trace these relationships through the model. The output of this can be used to assist the analyst in understanding the influences on the function of interest and the risks as a result.

Figure 4 below shows the functional flows for an example GBAD system. The red highlighting in this diagram shows the logical path from the target “Guide to intercept point” function (highlighted blue) tracing back to “upstream” elements in the flow. Figure 5 illustrates an example upstream traceability diagram of this function, as generated by the MBSE tool.

![Figure 4: Enhanced Functional Flow Block Diagram (EFFBD) highlighting upstream traceability](image-url)
Figure 5: Upstream traceability diagram for exemplar GBAD system function

Step 2.3 – Identify downstream effects (impact on system performance)

For each function of interest, determine the potential impact of the function failing on other key (and/or critical) system functions. This step is crucial for functions that have a high likelihood of failure. This step is similar to step 2.2, employing the MBSE tool’s model interrogation capabilities, but to trace the flow on effects of the function of interest. This is achieved by specifying the “downstream” relationships of interest and allowing the tool to trace these relations through the model. The output of this can be used to guide the analyst in the understanding of the impact of the function of interest failing (or degrading in performance) and analysing the resulting risks.

Step 2.4 – Analyse and record overall risk

Once the upstream and downstream causes and effects have been analysed for all functions of interest, this information is correlated to determine the overall risks. The upstream analysis informs the likelihood aspect of the risk, while the downstream effects inform the consequence/impact of the risk. Thus, FRA enables the analysis and recording of inter-functional risks and risks coupled between functions (see Figure 6 for example).

Once the potential influences on, and effects of functional failures have been identified, the MBSE model can be used to capture the resulting risk, and trace them through to the affected mission outcomes. Guided by the diagrams generated by the tool in steps 2.2 and 2.3, the analyst is able to identify and record potential functional risks within the system. Figure 6 illustrates an example upstream risk affecting the function of interest, Guide to intercept point (highlighted blue). These risks indicate that there are potential consequences, caused by data transfer, which may indirectly affect the performance of the critical function Guide to intercept point. The structured process enabled by the tools traceability diagrams guided the analyst to identify potential origins of risks which we not directly linked to the function of interest.
Additional to the guidance provided to the analyst, the MBSE tool can be used to help summarise the risk information captured. Figure 7 is a functional risk traceability diagram generated by the MBSE tool once the risks had been recorded. Thus, the benefits from using MBSE tools to support risk analysis go beyond the identification process.

Application of FRA to System Integration (FRASI)

Figure 8 illustrates the extension of the FRA process to analysing system integration risk. The following discussion describes the steps shown in Figure 8. Note that steps 1 and 2 are identical with those described above for the FRA process.

**Step 3 – Allocate functions (with identified risks) to system solutions**

Now that the inter-function risks have been identified independently of the potential system solutions, an objective analysis of the system integration risk, with respect to the proposed system solutions can be assessed. This requires the allocation of the functions to the systems/components comprising the system solution options. The functions may be allocated to systems within the capability boundary or to systems provided by interdependent capabilities.
Step 4 – Identify functional system integration risks (based on system allocation)

The allocation of functions to the proposed system solutions enables the analyst to determine which of the previously identified functional risks are to be treated as system integration risks (which are the responsibility of the lead system integrator), and those that remain functional risks (which are the responsibility of the prime contractor providing the systems). Risks which cross the boundary between systems provided in the solution become system integration risks, while those that remain within the system solution boundary are functional risks.

The example solution proposal illustrated in Figure 9 consists of an integration of two different systems (a Battle Management System (BMS) and a separate Launcher / Missile package). Thus, *Risk 1*, which crosses the system boundaries, becomes flagged as a system integration risk which the systems integrator must mitigate, while *Risk 2* is contained within the Launcher / Missile system boundary and remains the responsibility of the system provider. Both risks still remain, but they are treated differently and can be the responsibility of different organisations.
Figure 9: Example Partial System Solution resulting in system integration risk

The previous example illustrates how performing FRA then allocating the functions to the proposed system solutions can help identify system integration risks at the functional level. By utilising MBSE tools, the functional risks that result in system integration risks can be automatically reported through a model interrogation script. However, although the process so far has identified system integration risks as a result of the functional description of the system, further system integration risks may exist.

**Step 5 – Utilise risk library and other risk analysis techniques to identify other system integration risks**

Once the functional system integration risks have been identified, it is important to identify any other, non-functional, system integration risks that may exist. One of the benefits of employing a common MBSE environment is the ability to generate libraries as projects are completed. The system integration risk checklist, described later, can be utilised to assist in this process.

**Step 6 – Update risk library**

Finally, once the system integration risk analysis has been complete, the MBSE model risk library can be updated with any new risks assessed as appropriate for reuse. These libraries are maintained as individual project models which can be imported into a new project as required and maximises the retention of knowledge between projects.

**System Integration Risk Interface Analysis Checklist**

Analysts undertaking system integration risk analysis need to have a comprehensive understanding of the systems’ interfaces to ensure that all risks are identified and assessed. Very often system interface definitions are not available at the time that a TRA is performed because the interface definition documentation only becomes available as a contract deliverable. Therefore, there is value in

---

2 Note that “Target Cue” is derived from “Launch Command” information.
developing a checklist categorising the various forms of interfaces possible to aid the analyst. This checklist can reside as a library in the MBSE model and can be developed progressively as more is understood about the system under acquisition. There is some literature available on interface definition and this can be used to generate such a checklist. One example of this is the NASA training document (NASA 1997) where the basic forms of interfaces are defined to be: electrical / functional, mechanical / physical, software and supplied services. These have been adapted to produce an aide memoire to assist analysts in identifying all interface aspects that should be considered as sources of risk. A section of this integration analysis aid is illustrated in Table 2.

<table>
<thead>
<tr>
<th>Mechanical / physical interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Compatibility of size, shape, mass, mass distribution, point loads, centre of gravity (consider potential for variations with time and use – e.g. fuel usage and centre of gravity shift)</td>
</tr>
<tr>
<td>• Availability of space for access for operation, maintenance and observation / inspection (assess availability, accessibility, location and size)</td>
</tr>
<tr>
<td>• Compatibility of concentricity, parallelism, perpendicularity, straightness</td>
</tr>
<tr>
<td>• Material compatibility, consider all material properties including mechanical, optical, thermal, chemical, electrical, acoustic, surface properties.</td>
</tr>
<tr>
<td>• Vibration, sound and heat transmission (planned and incidental) compatibility</td>
</tr>
<tr>
<td>• Hard points (number, locations, dimensions and load strength) for tie down and handling</td>
</tr>
</tbody>
</table>

Table 2: Example of interface risk analysis aid for mechanical / physical interface

CONCLUSION

FRA is designed to be a rigorous approach to support the technical risk assessment process in defining risks and how they affect the functionality of the mission system. FRASI is an extension of FRA to help identify which of these functional risks can be classified as system integration risks (those that cross the proposed system solution boundaries) and require mitigating by the lead system integrator. The Functional Hazard Assessment inspired FRASI methodology, when underpinned by an MBSE environment, is a useful tool to assist in the identification of system integration risks and assess (and record) their potential impact on system functionality. There are several benefits, to different stakeholders, in using an MBSE based FRASI methodology. Some of the key benefits are:

- Use of existing capability and system information resident in the MBSE capability model means that there is less potential for error. Typically, the system information required for risk assessments is either developed independently by DSTO or based on static, potentially out of date information. By utilising the knowledge within the same MBSE model, both the risk analyst and the capability developer / system engineer are using the same information, reducing the potential for error or conflict and reducing the effort required to translate textual information into functional flow diagrams. This develops a single source of truth.

- Further, because under FRASI the risk analysis is integrated into the MBSE environment, the risk analysis is embedded in the capability definition and its implications, on things such as mission objectives, are evident at all times. Importantly, in the event of any change in the project, the update of the TRA is not a case of starting from a blank page, the traceability of the information inherent in the MBSE model provides a means of identifying those parts that
need updating versus those that can stand unchanged. A fresh TRA report may be generated at any point as the risk analysis is updated by running the relevant scripts.

- Additionally, this integrated MBSE environment, and its inherent traceability of functions to mission objectives, provides a more rigorous means of analysing capability fitness for purpose.

- FRASI provides a method for identifying technical risk in situations where the system breakdown has not yet been developed or where such a breakdown might not be appropriate.

- FRASI is a methodology for improving the rigour of the analysis, enhancing the robustness of the resulting TRA.

- The FRASI process guides the risk analyst to better understand the potential for risk coupling and system integration risk.

REFERENCES


**BIOGRAPHIES**

**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 modelling, 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.