18. Technical Risk Analysis – Exploiting the Power of MBSE

Despina Tramoundanis[1], Wayne Power[1] and Daniel Spencer[2]
[1]Weapons Systems Division, DSTO and [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)[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,

[17] DSTO, Technical Risk Assessment Handbook, Version 1.1, 2010

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
FEB 2013	**N/A**	**-**

4. TITLE AND SUBTITLE **Technical Risk Analysis â Exploiting the Power of MBSE â**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **1Weapons Systems Division, DSTO**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADA585222. Proceedings of the 2012 Model-Based Systems Engineering Symposium, 27 - 28 November 2012, DSTO Edinburgh, South Australia., The original document contains color images.

14. ABSTRACT
In his 2003 review into Defence procurement, Kinnaird recommended that for new acquisitions Defence undertake a âcomprehensive analysis of technology, cost and schedule risksâ and that âGovernment needs to be assured that adequate scrutiny is undertaken â¦.by DSTO on technology feasibility, maturity and overall technical riskâ. As a result, DSTO performs Technical Risk Assessments (TRA) to inform major acquisition decisions during the Requirements phase of the Capability Development process.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**22**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

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.

Presentation

UNCLASSIFIED – For Public Release

Australian Government
Department of Defence
Defence Science and Technology Organisation

Technical Risk Analysis: Exploiting the Power of MBSE

Despina Tramoundanis, DSTO (WSD)
Wayne Power, DSTO (WSD)
Daniel Spencer, Aerospace Concepts P/L

DSTO

UNCLASSIFIED – For Public Release

UNCLASSIFIED – For Public Release

Overview

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

DSTO

UNCLASSIFIED – For Public Release

Australian Government
Department of Defence
Defence Science and
Technology Organisation

Background

DSTO

UNCLASSIFIED – For Public Release

UNCLASSIFIED – For Public Release

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****'.*

DSTO

UNCLASSIFIED – For Public Release

UNCLASSIFIED – For Public Release

Technical Risk Assessment

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

UNCLASSIFIED – For Public Release

DSTO

UNCLASSIFIED – For Public Release

Australian Government
Department of Defence
Defence Science and
Technology Organisation

The Need

DSTO

UNCLASSIFIED – For Public Release

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

UNCLASSIFIED – For Public Release

UNCLASSIFIED – For Public Release

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

UNCLASSIFIED – For Public Release

UNCLASSIFIED – For Public Release

Australian Government
Department of Defence
Defence Science and Technology Organisation

Functional Risk Analysis (FRA)

UNCLASSIFIED – For Public Release

DSTO

UNCLASSIFIED – For Public Release

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

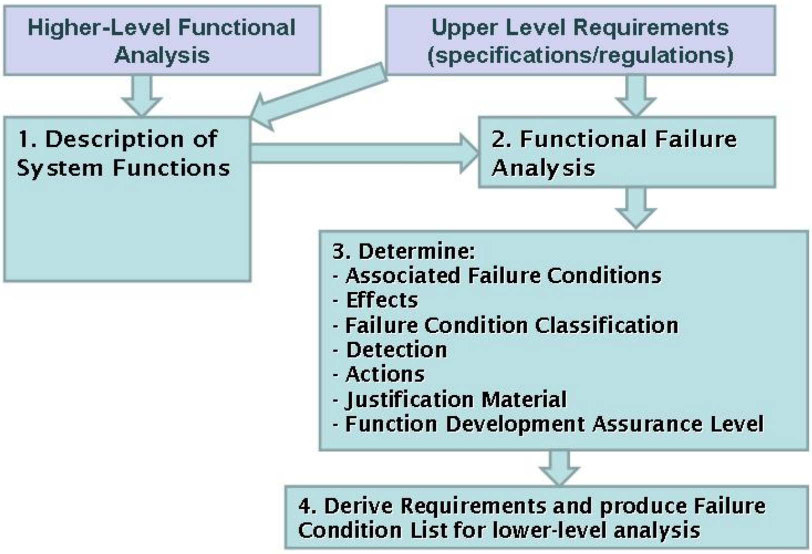
UNCLASSIFIED – For Public Release

DSTO

UNCLASSIFIED – For Public Release

Functional Hazard Assessment

(modified from SAE ARP4761)



UNCLASSIFIED – For Public Release

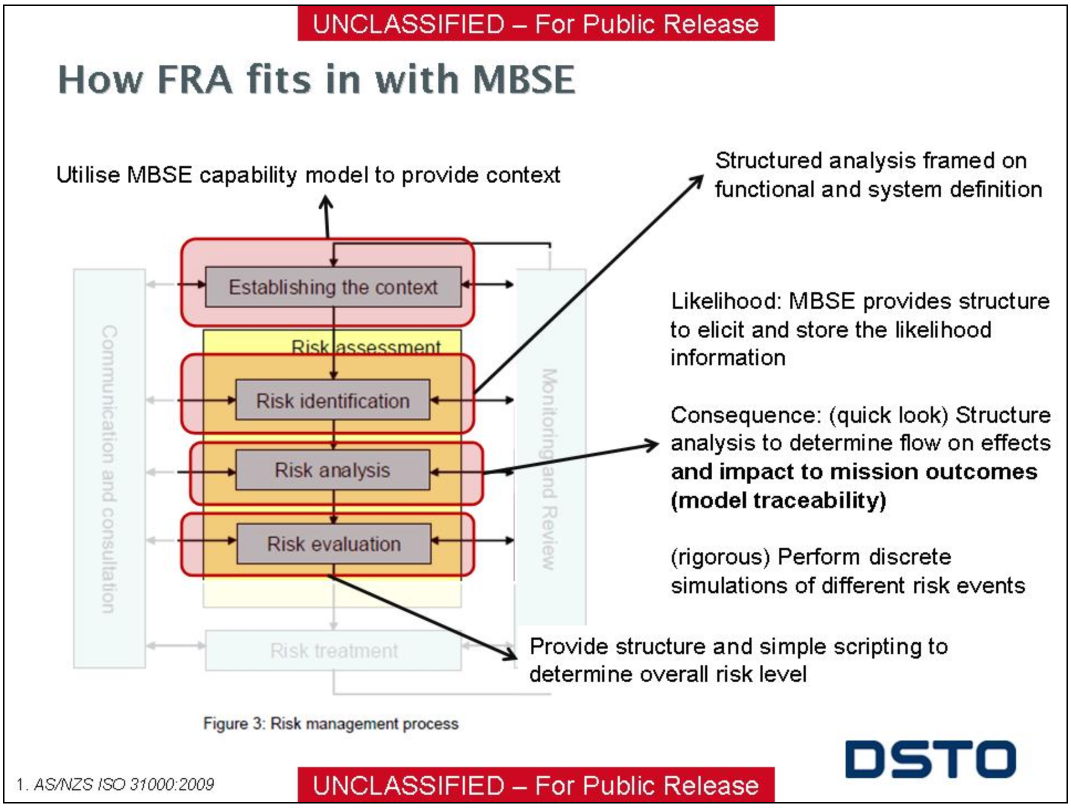
UNCLASSIFIED – For Public Release

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)

UNCLASSIFIED – For Public Release


UNCLASSIFIED – For Public Release
Australian Government
Department of Defence
Defence Science and Technology Organisation
Applying FRA as part of an MBSE methodology
DSTO
UNCLASSIFIED – For Public Release


UNCLASSIFIED – For Public Release
How FRA fits in with MBSE
Utilise MBSE capability model to provide context
Structured analysis framed on functional and system definition
Establishing the context
Risk assessment
Risk identification
Risk analysis
Risk evaluation
Risk treatment
Communication and consultation
Monitoring and Review
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
1. AS/NZS ISO 31000:2009
DSTO
UNCLASSIFIED – For Public Release

UNCLASSIFIED – For Public Release

Required model state

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

Required for EFFBD representation

If a materiel system does not exist:

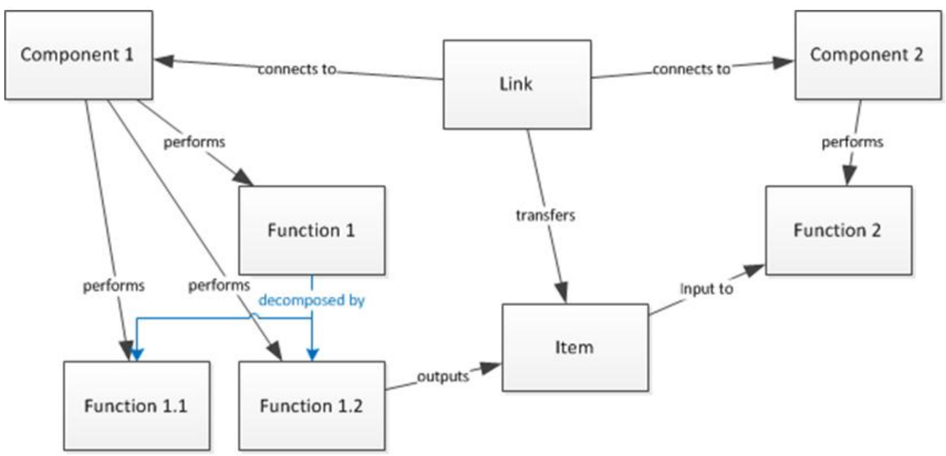
- Perform risk analysis on available technologies to perform functions
- Identify *indicative risk areas* in achieving functional and operational outcomes due to technology maturity issues
- Repeat FRA when the materiel system is known.

DSTO

UNCLASSIFIED – For Public Release

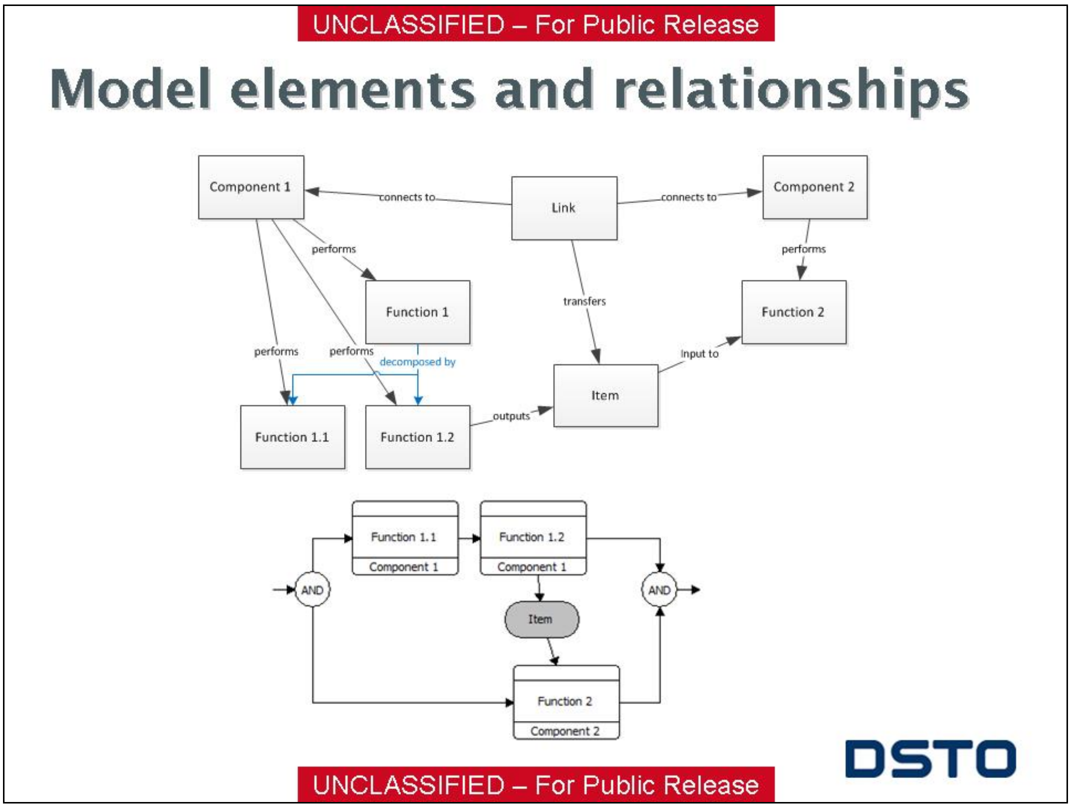
UNCLASSIFIED – For Public Release

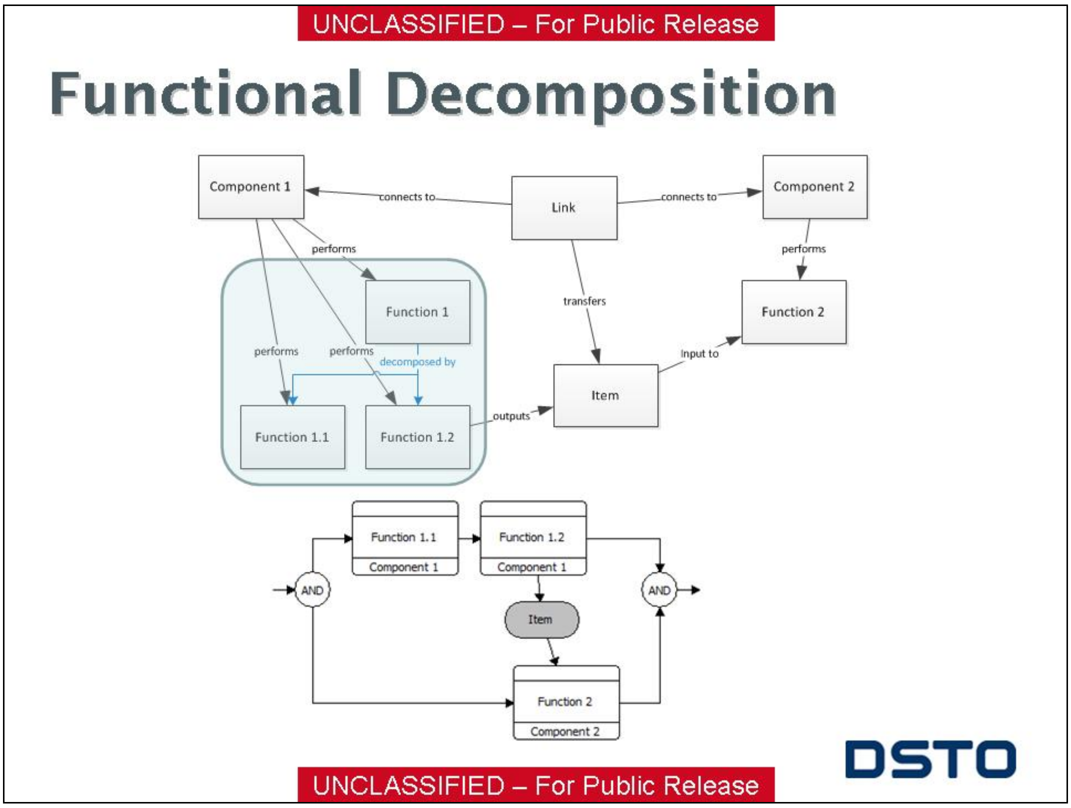
Model elements and relationships

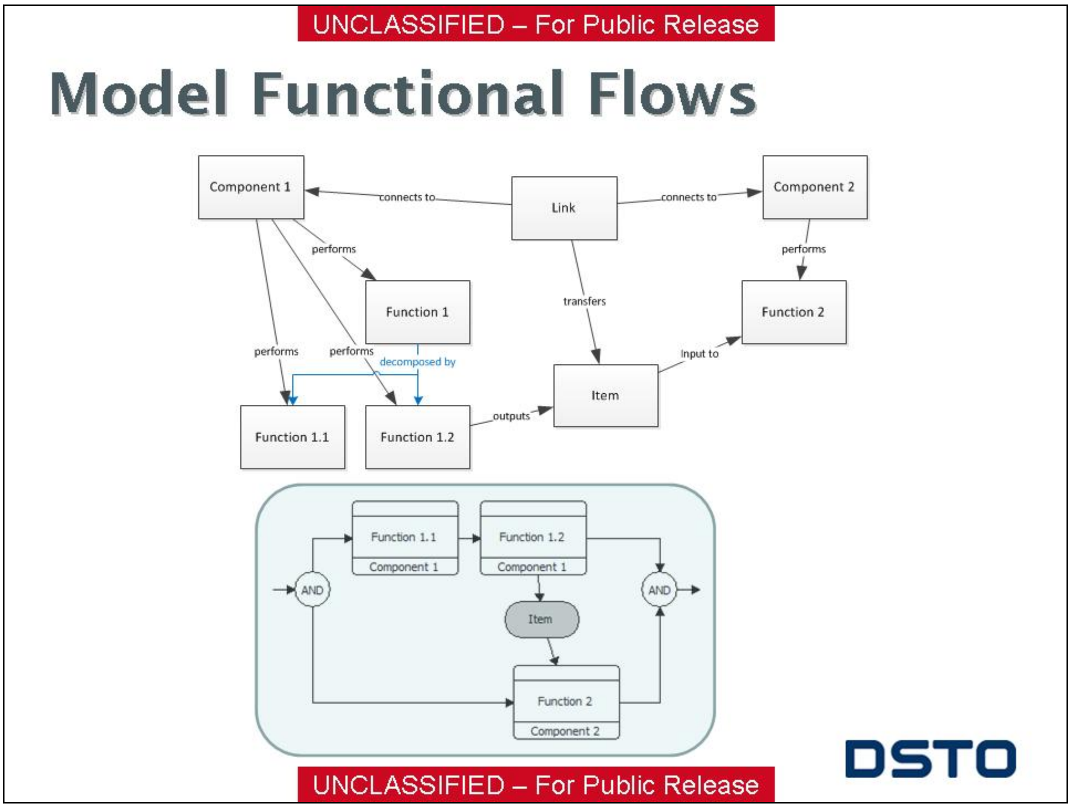


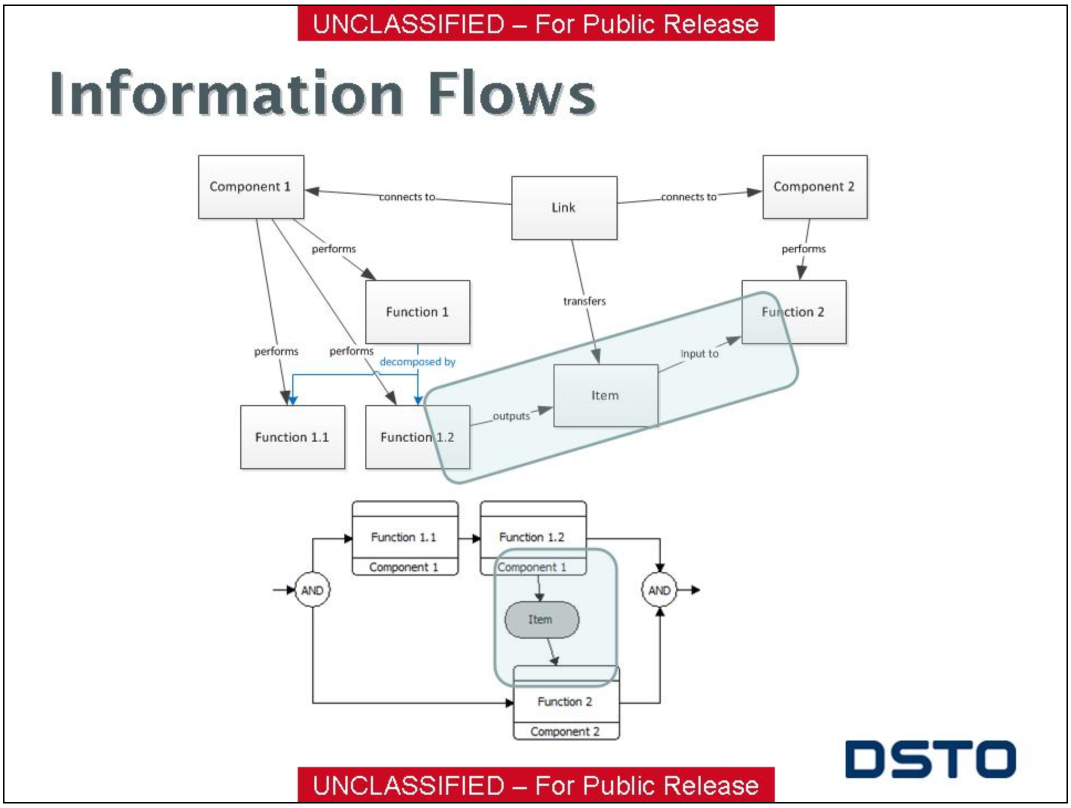
DSTO

UNCLASSIFIED – For Public Release


UNCLASSIFIED – For Public Release
Model elements and relationships
Component 1
connects to
Link
connects to
Component 2
performs
performs
Function 1
transfers
Function 2
performs
performs
decomposed by
Input to
Item
outputs
Function 1.1
Function 1.2
Function 1.1
Component 1
Function 1.2
Component 1
AND
AND
Item
Function 2
Component 2
DSTO
UNCLASSIFIED – For Public Release


UNCLASSIFIED – For Public Release
Functional Decomposition
Component 1
connects to
Link
connects to
Component 2
performs
performs
Function 1
transfers
Function 2
performs
performs
decomposed by
Input to
Item
outputs
Function 1.1
Function 1.2
Function 1.1
Component 1
Function 1.2
Component 1
AND
AND
Item
Function 2
Component 2
DSTO
UNCLASSIFIED – For Public Release


UNCLASSIFIED – For Public Release
Model Functional Flows
Component 1
connects to
Link
connects to
Component 2
performs
Function 1
transfers
performs
Function 2
performs
performs
decomposed by
Item
Input to
Function 1.1
Function 1.2
outputs
Function 1.1
Component 1
Function 1.2
Component 1
AND
AND
Item
Function 2
Component 2
DSTO
UNCLASSIFIED – For Public Release


UNCLASSIFIED – For Public Release
Information Flows
Component 1
connects to
Link
connects to
Component 2
performs
Function 1
transfers
performs
Function 2
performs
performs
decomposed by
Item
Input to
Function 1.1
Function 1.2
outputs
Function 1.1
Component 1
Function 1.2
Component 1
AND
AND
Item
Function 2
Component 2
DSTO
UNCLASSIFIED – For Public Release

UNCLASSIFIED – For Public Release

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)**

UNCLASSIFIED – For Public Release

DSTO

UNCLASSIFIED – For Public Release

3. Consider upstream causes of functional failure

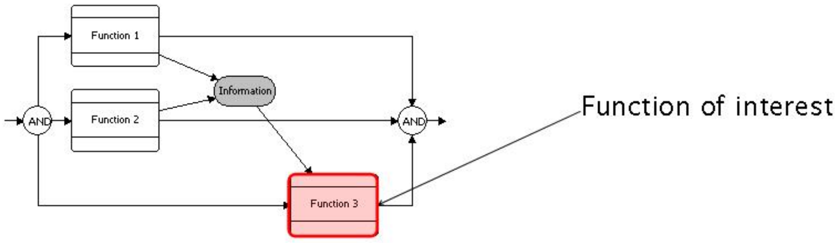
- Use tool support to produce report on "success path"
- Start from chosen function, consider:
  - *"triggered by"* items: Will always impact flow
  - *"inputs"* items: May affect quality of flow
- For the items collected, consider the other functions they are *"output from"*:
  - If multiple *"output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

UNCLASSIFIED – For Public Release

DSTO

Upstream risk patterns

Redundancy – decreased likelihood



DSTO

4. Consider downstream effects of functional failure

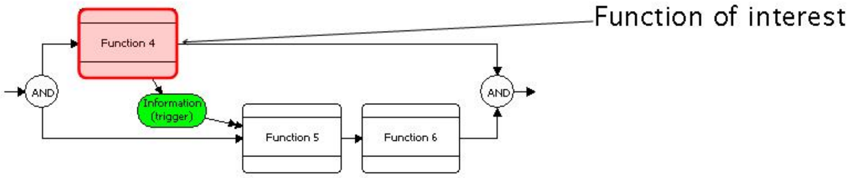
- Use tool support to produce report on "success path"
- For each function, consider the items it *"outputs"*
- For each item, consider:
  - *"triggers"* functions: May impact flow, but also need to consider if other functions are able to output this item
  - *"input to"* functions: May affect quality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

DSTO

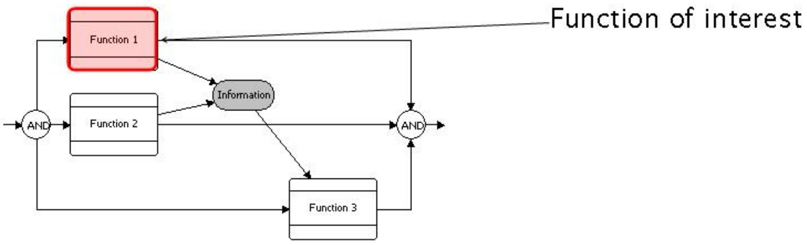
UNCLASSIFIED – For Public Release

Downstream risk patterns

Critical path – significant consequence



Redundancy – decreased consequence



UNCLASSIFIED – For Public Release

UNCLASSIFIED – For Public Release

Analyse 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

UNCLASSIFIED – For Public Release

5. Analyse and record resulting risk

Likelihood	Consequence/Impact		
	Minor	Moderate	Major
More Than Likely	MEDIUM	HIGH	HIGH
Less Than Likely	LOW	MEDIUM	HIGH
Unlikely	LOW	LOW	MEDIUM

TRAH Risk Likelihood / Impact Matrix

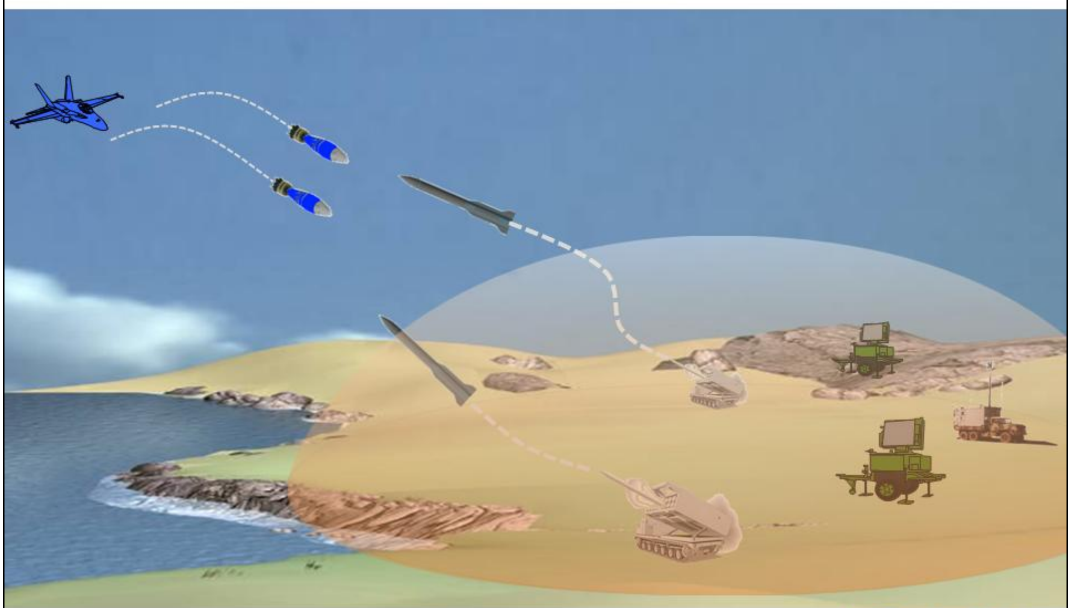
1. *Technical Risk Assessment Handbook*, Project and Requirements Division, DSTO, 2010

DSTO

UNCLASSIFIED – For Public Release

UNCLASSIFIED – For Public Release

Example – Ground Based Air Defence

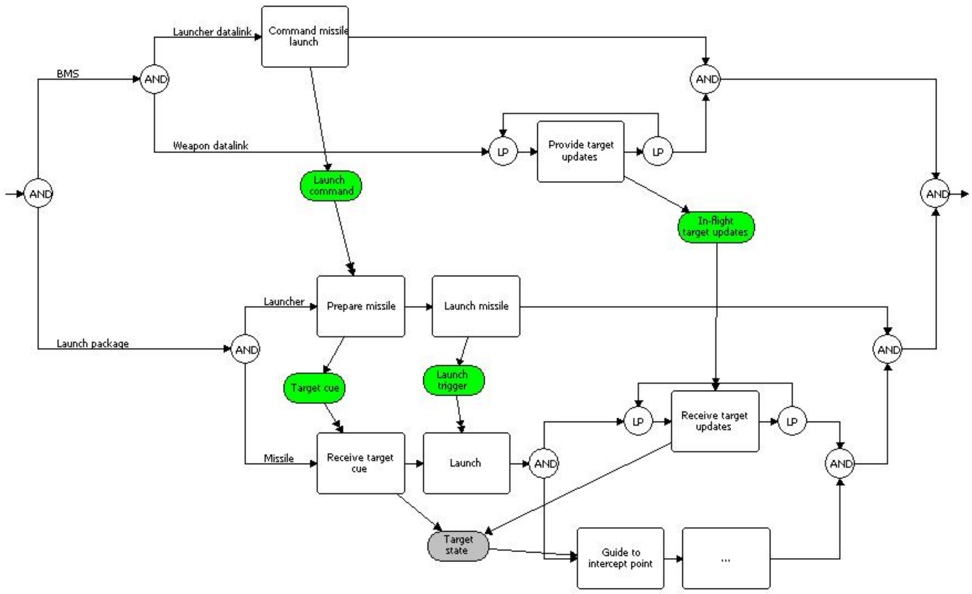


DSTO

UNCLASSIFIED – For Public Release

UNCLASSIFIED – For Public Release

Example – Ground Based Air Defence



UNCLASSIFIED – For Public Release

DSTO

UNCLASSIFIED – For Public Release

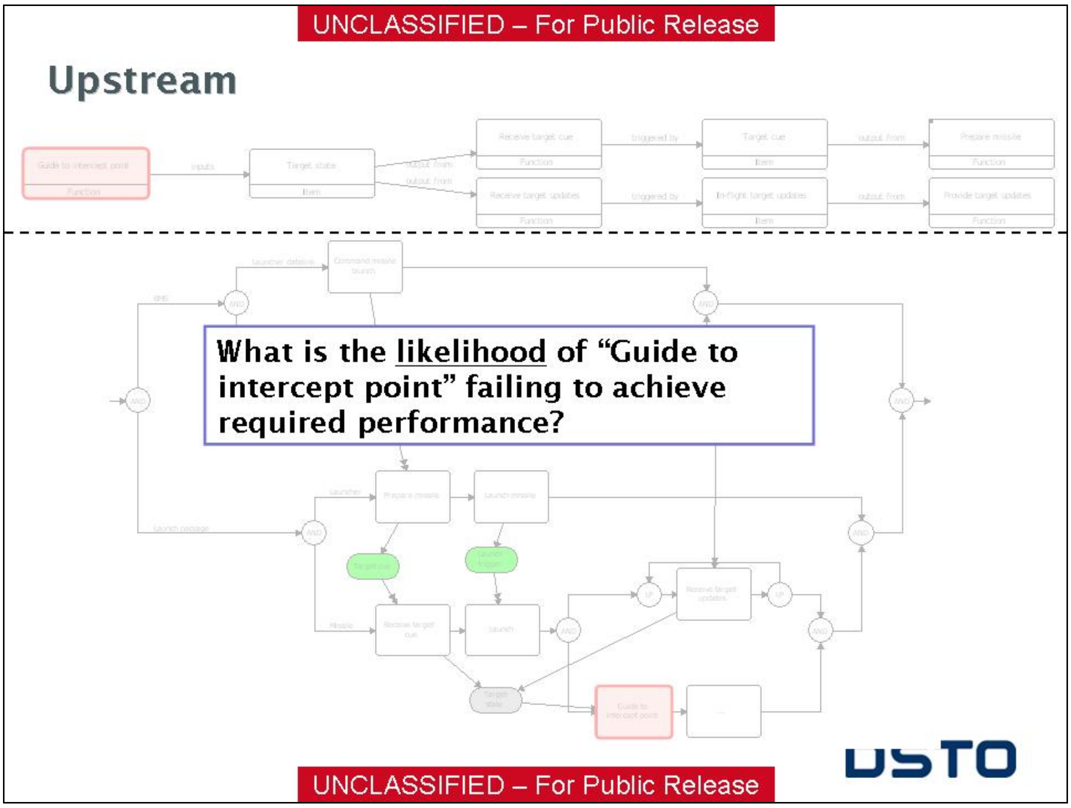
Upstream functional traceability

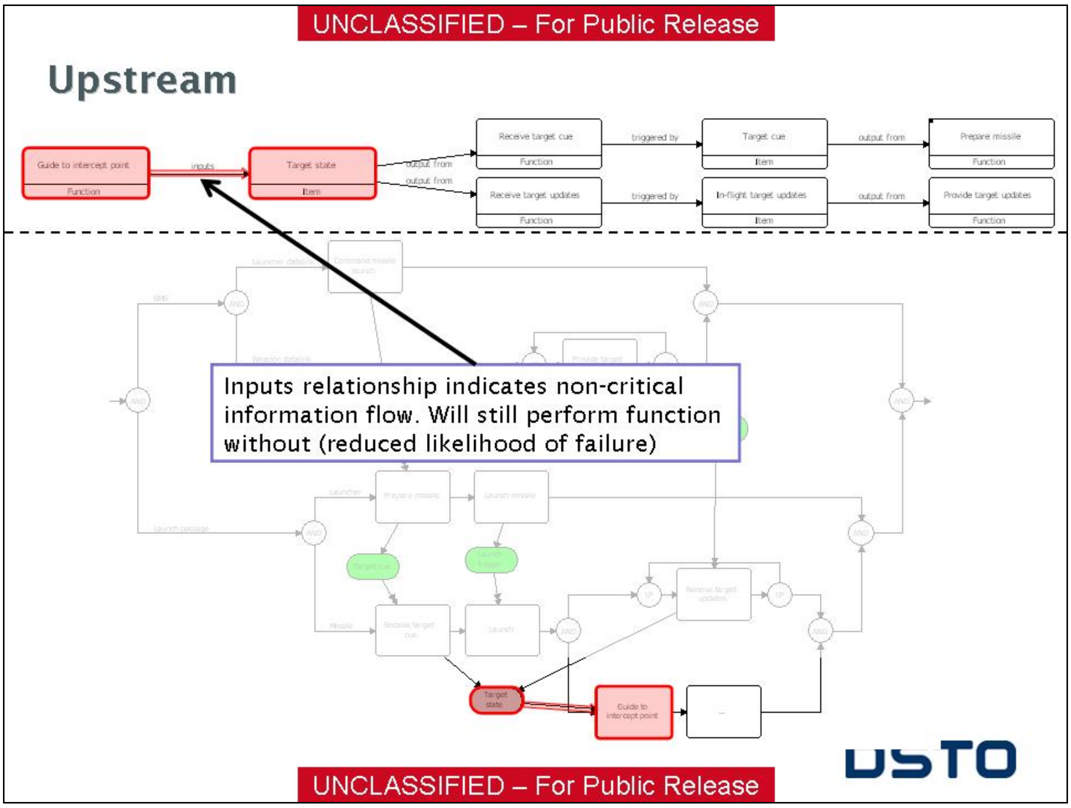
To guide the analyst in understanding the potential influences on critical functions

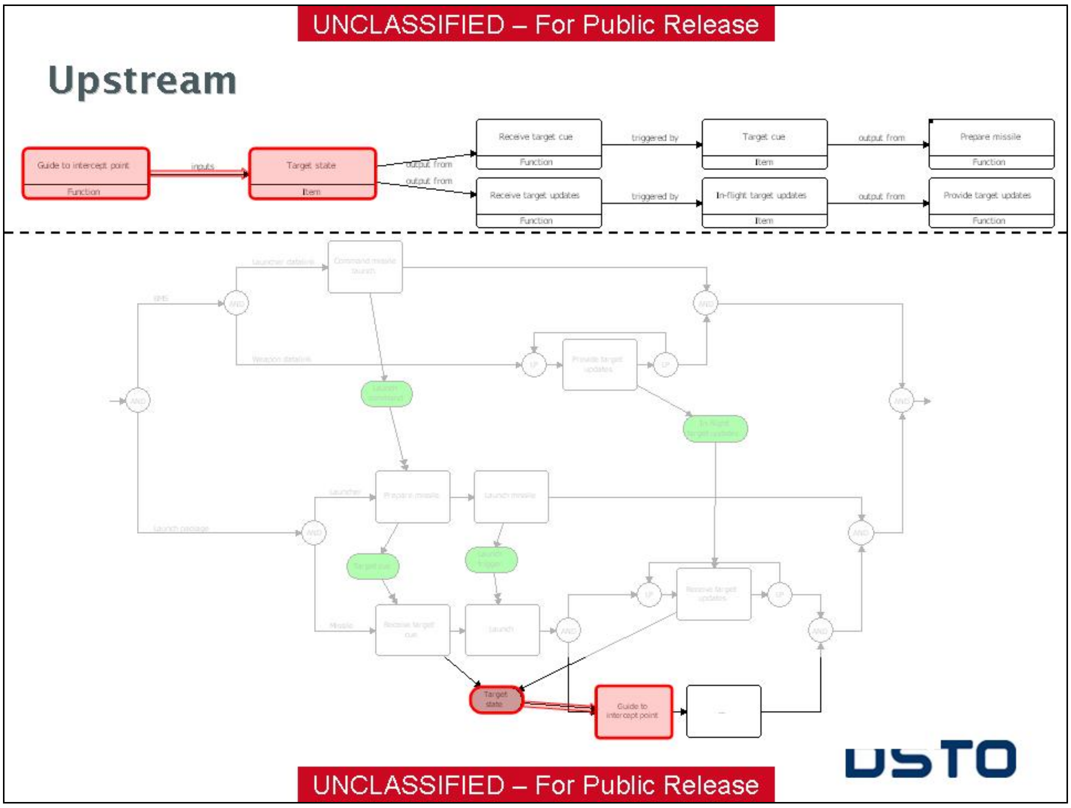
What's the likelihood of failure?

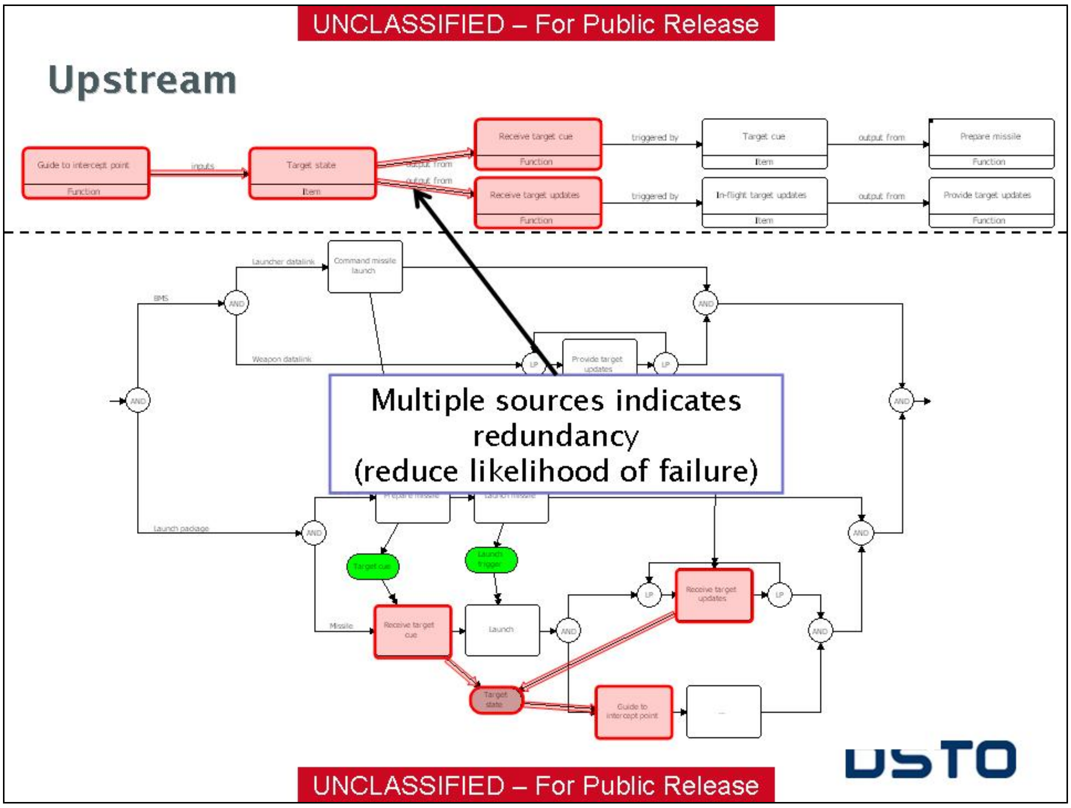
UNCLASSIFIED – For Public Release

DSTO


UNCLASSIFIED – For Public Release
Upstream
What is the likelihood of “Guide to intercept point” failing to achieve required performance?
DSTO
UNCLASSIFIED – For Public Release

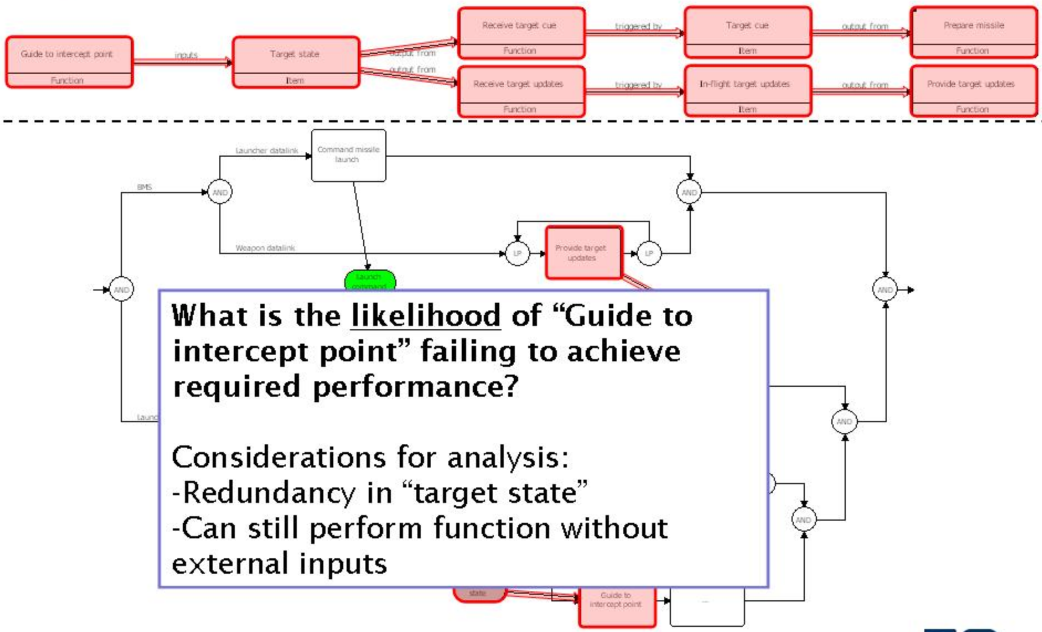

UNCLASSIFIED – For Public Release
Upstream
Guide to intercept point
Function
inputs
Target state
Item
output from
output from
Receive target cue
Function
triggered by
Target cue
Item
output from
Prepare missile
Function
Receive target updates
Function
triggered by
In-flight target updates
Item
output from
Provide target updates
Function
Inputs relationship indicates non-critical information flow. Will still perform function without (reduced likelihood of failure)
Target state
Guide to intercept point
...
DSTO
UNCLASSIFIED – For Public Release


UNCLASSIFIED – For Public Release
Upstream
Guide to intercept point
Function
inputs
Target state
Item
output from
output from
Receive target cue
Function
triggered by
Target cue
Item
output from
Prepare missile
Function
Receive target updates
Function
triggered by
In-flight target updates
Item
output from
Provide target updates
Function
Target state
Guide to intercept point
...
UNCLASSIFIED – For Public Release
DSTO


UNCLASSIFIED – For Public Release
Upstream
Guide to intercept point
Function
inputs
Target state
Item
output from
output from
Receive target cue
Function
triggered by
Target cue
Item
output from
Prepare missile
Function
Receive target updates
Function
triggered by
In-flight target updates
Item
output from
Provide target updates
Function
Launcher datalink
Command missile launch
BMS
AND
Weapon datalink
LP
Provide target updates
Multiple sources indicates redundancy
(reduce likelihood of failure)
Launch package
Target cue
Launch trigger
Missile
Receive target cue
Launch
Receive target updates
Target state
Guide to intercept point
...
UNCLASSIFIED – For Public Release
DSTO

UNCLASSIFIED – For Public Release

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

DSTO

UNCLASSIFIED – For Public Release

UNCLASSIFIED – For Public Release

Downstream functional traceability

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

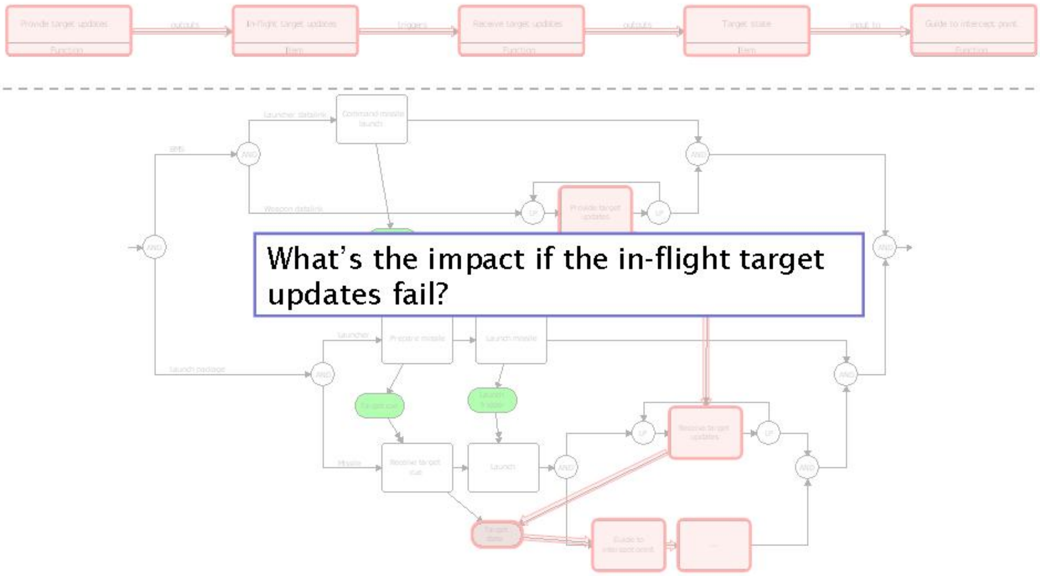
What's the consequence of failure?

DSTO

UNCLASSIFIED – For Public Release

UNCLASSIFIED – For Public Release

Downstream



UNCLASSIFIED – For Public Release

UNCLASSIFIED – For Public Release

Benefits of methodology/ Conculsions

Issues with current practice	FRA Benefit
TRA templates do not fit every type of acquisition	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.
Need to assume a materiel solution	FRA can be applied to a functional description of a system using knowledge of available technologies (pre-2nd pass) and is repeated for physical systems at 2nd Pass.
Quality depends on the skills of individuals	Provides a rigorous process to assist in the analysis of whole of system technical risk
Inadequate analysis of: System integration risk Risk coupling	Process guides analyst through the potential influence of technologies on other systems and sub-systems. Focus is on potential impact of integration risk
TRA is a stand-alone document	Analysis performed in and risks recorded in the same model OCD and FPS definitions. Completely traceable: a single source of truth.

UNCLASSIFIED – For Public Release

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 fitness-for-purpose)
- Can extend FRA process to system assessment
- Resulting derived requirements can be traceable back to the analysis process

UNCLASSIFIED – For Public Release

DSTO