SYM-AM-23-104

Excerpt from the Proceedings

of the

Twentieth Annual Acquisition Research Symposium

Acquisition Research: Creating Synergy for Informed Change

May 10–11, 2023

Published: April 30, 2023

Disclaimer: The views represented in this report are those of the author and do not reflect the official policy position of the Navy, the Department of Defense, or the federal government.

The research presented in this report was supported by the Acquisition Research Program at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

Acquisition Research Program
Department of defense management
Naval Postgraduate School

Shifting Left: Opportunities to Reduce Defense Acquisition Cycle Time by Fully Integrating Test and Evaluation in Model Based Systems Engineering

Craig Arndt—currently serves as a principal research engineer on the research faculty of the George Tech Research Institute (GTRI) in the System Engi-neering Research division of the Electronic Systems Lab. Arndt is a licensed Professional Engineer (PE), and has over 40 years of professional engineering and leadership experience. Arndt holds engineering degrees in electrical en-gineering, systems engineering, and human factors engineering and a Masters of Arts in strategic studies form the U.S. Naval War college. He served as Professor and Chair of the engineering department at the Defense Acquisition University and as technical director of the Homeland security FFRDC at the MITRE Corporation. In industry he has been an engineering manager, director, vice president, and CTO of several major defense companies he is also a retired naval officer. [Craig.Arndt@gtri.gatech.edu]

Awele I. Anyanhun—is a senior research engineer in the MBSE Research and Application Branch at Georgia Tech Research Institute (GTRI). She is an INCOSE-Certified Systems Engineering Professional (CSEP) and Senior Member of IEEE with over 13 years' professional experience in architecting complex automotive, space, and defense system architectures. In her current role as a project director and systems architect, she provides thought leadership and systems engineering expertise on DoD-sponsored DE and MBSE projects. Anyanhun is an OMG-Certified Systems and Software Modeling Profes-sional, SysML-MBA, OCUP 2-MBA, and a UL-Certified Functional Safety Professional (UL-CFSP). Anyanhun has authored multiple conference and journal publications, and holds a PhD in Electrical Engineering with a con-centration in systems engineering. [Awele.Anyanhun@gtri.gatech.edu]

Jeremy Werner, PhD, ST—was appointed DOT&E's Chief Scientist in De-cember 2021 after initially starting at DOT&E as an Action Officer for Naval Warfare in August 2021. Before then, Werner was at Johns Hopkins Univer-sity Applied Physics Laboratory (JHU/APL), where he founded a data sci-ence–oriented military operations research team that transformed the analytics of an ongoing military mission. Werner previously served as a Research Staff Member at the Institute for Defense Analyses where he supported DOT&E in the rigorous assessment of a variety of systems/platforms. Werner received a PhD in physics from Princeton University where he was an integral contributor to the Compact Muon Solenoid collaboration in the experimental discovery of the Higgs boson at the Large Hadron Collider at CERN, the European Or-ganization for Nuclear Research in Geneva, Switzerland. Werner is a native Californian and received a bachelor's degree in physics from the University of California, Los Angeles where he was the recipient of the E. Lee Kinsey Prize (most outstanding graduating senior in physics). [jeremy.s.werner.civ@mail.mil]

Abstract

The reduction in cycle time for acquisition programs, or "Shift Left" is important to realizing the benefits of digital engineering (DE), as specifically addressed in the DOT&E Strategy update in 2022. Although DE has long held the promise of making programs faster, and achieving goals and priorities more efficiently, its effect on reduced acquisition cycle time is still difficult to identify and quantify. Furthermore, problem discovery during testing and evaluation (T&E) has been identified as a critical driver in the time it takes to develop systems and is said to have significant impact on the acquisition cycle time. Hence, a reduction in acquisition cycle time can be achieved through a systemic approach that positively impacts the time required to test systems while maintaining or reducing risk. Therefore, expanding the use of DE and model-based systems engineering (MBSE) to include test capability models creates the opportunity to improve testing and development of defense systems as well as reduce the defense acquisition life cycle time. To this end, this paper will present the quantitative results of a project that expands the use of MBSE within the test and evaluation space through the creation of a model-based test integration prototype. The results will show where and how test modeling can be used to impact acquisition decision making and reduce overall program schedule.

Keywords: Digital Engineering, MBSE, Test planning, Shift left

Introduction

The transformation from the historical, document-based acquisition system to digital engineering (DE) is resulting in some of the most significant changes to the way the DoD has engineered and developed weapon systems in decades. The shift to the use of DE will not only impact the DoD but the entire military-industrial complex. Coined by President Eisenhower in a 1961 address to the American people, the “military-industrial complex” includes the contractors that develop and manufacture our nation’s combat systems (History.com Editors, 2009).

In some ways, the transition to DE is the DoD’s reaction to the larger endeavor in the engineering community to reduce development time and cost by using digital data management technologies across development and manufacturing enterprises. In the DoD’s “Digital Engineering Strategy,” the DoD states that “current acquisition processes and engineering methods hinder meeting the demands of exponential technology growth, complexity, and access to information” (DoD, 2018). DoD leadership believes that DE will enable the DoD to meet the current and upcoming challenges to delivering new capabilities to the warfighters in support of the DoD’s numerous complex missions. To accomplish this, it is crucial to have a realistic DE strategy in place that can be implemented with new DE technologies while maintaining compliance with current acquisition policy and best practices.

In balancing these constraints against the opportunities of DE, several key goals and needs of the DoD must be considered. First the goal of the department acquisition activities is to deliver to the warfighters the best possible systems in a timely, cost-effective manner in order to maximize lethality and survivability. Second the different acquisition activities need to use and create data, information, and knowledge in a manner that improves critical processes already in the acquisition system and allows programs to be managed based on their risk profile and their impact to the existing and future operational use in concert with other operational systems and in the presence of future threats. In order to maximize the positive impact of DE and modeling we need to implement DE in a manner that specifically addresses speed, risk, and quality of decision making, across portfolios, in a manner responsive to relevant missions.

Background

The adoption of additional technologies or methodologies is often accompanied by a myriad of questions regarding the scope of adoption or degree of utilization of the introduced concept. Digital engineering is no different. Many of the original implementations of DE, and more specifically model-based systems engineering (MBSE), have focused on the development of models of requirements and the design of systems to meet these requirements. In many instances they lack a meaningful set of modes of the test process. This is problematic for a number of different reasons. First, because test and evaluation (T&E) are critical parts of the development life cycle accelerating the development of systems (a key goal for the DoD) cannot be properly addressed without detailed modeling of the T&E process. Additionally, the information and data that is collected during different parts of the T&E process (including developmental and operational test) is critical to making good decision about every aspect of a given program. In the *DOT&E Strategy Update 2022*, Nickolas Guertin, the Director of DoD Operational Test and Evaluation states the second strategy pillar of DOT&E strategy is “acceleration the delivery of weapons that work” and he points out that MBSE is needed to achieve this shift-left (DOT&E, 2022).

At the beginning of the development process essential mission requirements are identified as Key Performance Parameters (KPPs), key acceptance criteria, or Measures of

Effectiveness (MOEs), organizations typically use one or more of these terms for their essential mission requirements. All key stakeholders must agree to these KPPs or MOEs early in the life of the project, because these are the select few, critical, and non-negotiable criteria that the solution must satisfy to be acceptable. They represent the absolutely critical subset of measurable and observable capabilities and characteristics that the solution must meet. Developing KPPs, MOEs, or key acceptance criteria is a joint effort between the systems engineers and the key stakeholders. The DoD defines KPPs in the initial capabilities document and validates them in the capability description document. Defining KPPs often takes the collaboration of multiple stakeholders, but it is critical to providing focus and emphasis on complex multi-year multi-agency development programs.

Modeling of the testing capability, in this case the test ranges, is a key part of integrated program modeling. In modeling the system, the KPPs and the MOE define the test cases needed for the testing program. In order to demonstrate the modeling, we developed models for the test cases and for the testing capabilities of a generic electronic warfare system. The testing capabilities are modeled in the form of a test range model. For this project we developed a partial model of the Eglin range. The range model was used to capture specific capabilities of the range to be used in constructing the test use cases. The test range models the requirements, system design, and test cases. A risk model is then linked to the other models. In this way the risk model gets data from the other models, and can be used to aggregate the risks based on differences between the available test resources and the requirements for those resources in test execution.

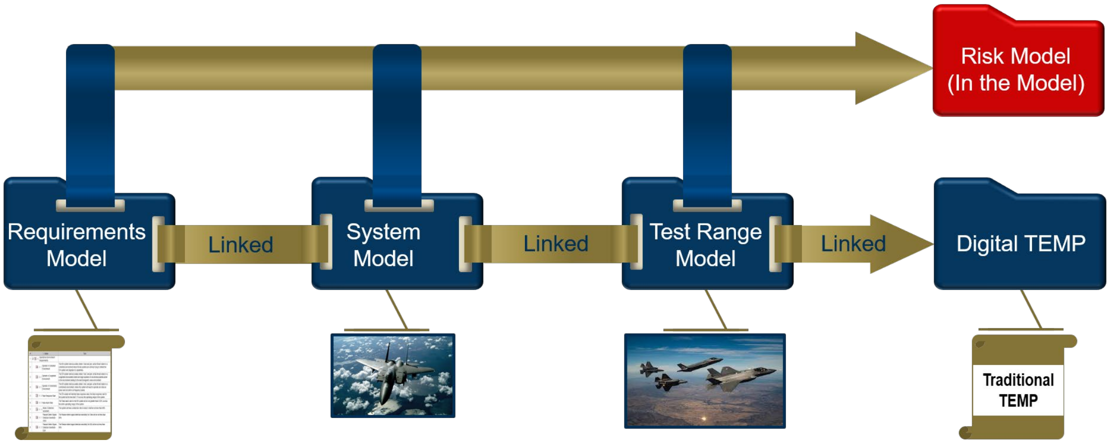


Figure 1. Life Cycle Modeling Structure

In addition to the need for greater use of modeling in T&E and the linking of these models to the larger set of requirements and systems models, there is a great need to look at the way risk is modeled as a function of the models that exist in DE processes. Risk in this context is inherently a function of different aspects of the program's ability to create and deliver a useful product to the field. Traditionally risk functions have focused only on the risk to the program of developing the end item product. The traditional risk approach also developed risks based on specific design risks. This approach has several shortcomings. First, this approach does not guarantee a comprehensive coverage of all possible risks. Second, the traditional approach has no specific way of addressing risk created in the testing program independent of the acquisition risk of different parts of the system. Third, the traditional approach to risk does not have a direct means of aggregating risk from the system's operational mission or operational environments. As a result, these three specific areas form the requirements set for the development of a new risk approach.

1. Develop a risk function that is comprehensive across all areas of the program.
2. It is critical that the risk function capture risks that are inherent to the testing of systems.
3. A risk function needs the ability to aggregate risk across different aspects of the program, specifically aggregate risks across mission areas and operational environments.

The development of more robust T&E and risk modeling generate the data, viability and insights needed to make decisions to accelerate acquisition programs.

Shifting Left: Applying an MBSE Approach to Test Planning, System Testing, and Evaluation

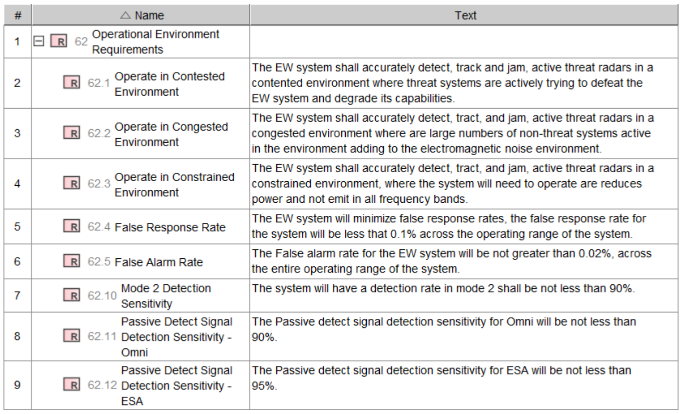
The power of system modeling to address the challenge of accelerating the acquisition process and reduce cycle time can be best demonstrated by a specific use case. In this use case we developed a representative set of models that captures requirements, system architecture, test range architecture, test cases, and risk functions. The use case shown in this section will demonstrate how test organizations can integrate and link together requirements models, system architecture/design models, test ranges, and system under test (SUT) models in order to reduce the time it takes to test systems while maintaining or reducing risk. In order to develop the system and test models in a form that would serve as a good example for future acquisition programs as well as to prototype the process of developing and linking the models, a simplified version (notional) of a real electric warfare (EW) system, the AN/ALQ-161A (Angry Kitten) electronic countermeasures system design for the B-1B bomber aircraft was chosen. The integrated model is composed of several independent models holding requirements, system architectures and test artifacts in self-contained modules that can be updated and augmented independently when new data is available. The EW use case was selected because of our ability to abstract it to more general defense acquisition and because there are several well understood missions that can demonstrate different risk profiles.

Specifying Requirements Modeling for Test

Requirements engineering is a vital part of the (model-based) systems engineering (SE) process because it defines the problem scope and links all subsequent system development, system testing, and risk analysis information to it (Dick, 2017). A set of exemplar requirements that capture the requirements of the system to be developed and tested, requirements of the test range(s) required for performing system tests, and testing requirements are captured in a requirements model and are further refined in the system architecture and test range infrastructure models. Highlighted in this section are the requirements sets for a specific capability of an EW electronic countermeasures system, the requirements sets for a test range that would be used to test the EW system capability, and the testing requirements. Requirements engineering constitutes the branch of SE that bridges the gap between the informal world of stakeholder needs—which in this context is representative of the test community and program office—and the formal world of a reduced cycle time for defense acquisition.

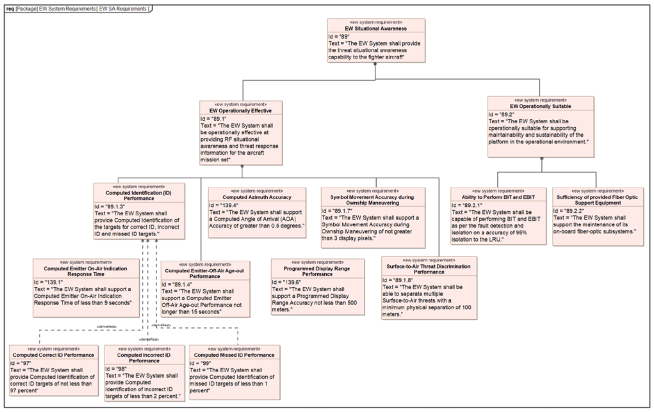
Specify the System of Interest (SoI) Requirements. The desired mission capabilities of the EW countermeasures system are first specified and modeled as system requirements. The system-level requirements describe the functions and quality attributes (non-functional requirements) the system must fulfill in order to satisfy the program office's needs. Functionally, the EW system is expected to operate optimally within several operational environments based on specific user-defined missions. A couple of operational environment requirements levied on the EW system are shown in Figure 2. For this exemplar model, the main mission capability expected of the EW countermeasures system is the ability to *provide situational awareness* during missions.

As highlighted in Figure 3, the high-level requirement *EW Situational Awareness* is decomposed into two main requirements: *EW Operationally Effective* and *EW Situationally Effective* ,which are further decomposed into atomic requirements that can be tested. Also captured in the requirements diagram are *Derived Requirements—Computed Correct ID Performance*, *Computed Incorrect ID Performance*, and *Computed Missed ID Performance* which are derived from the *Computed Identification (ID) Performance Requirement.* These mission requirements represent Key Performance Parameters (KPPs) or Measures of Effectiveness (MOEs) that are critical for the success of the mission and which a test range will need to have the capability to test.



#	△ Name	Text
1	⊟ R 62 Operational Environment Requirements	
2	R 62.1 Operate in Contested Environment	The EW system shall accurately detect, track and jam, active threat radars in a contented environment where threat systems are actively trying to defeat the EW system and degrade its capabilities.
3	R 62.2 Operate in Congested Environment	The EW system shall accurately detect, tract, and jam, active threat radars in a congested environment where are large numbers of non-threat systems active in the environment adding to the electromagnetic noise environment.
4	R 62.3 Operate in Constrained Environment	The EW system shall accurately detect, tract, and jam, active threat radars in a constrained environment, where the system will need to operate are reduces power and not emit in all frequency bands.
5	R 62.4 False Response Rate	The EW system will minimize false response rates, the false response rate for the system will be less that 0.1% across the operating range of the system.
6	R 62.5 False Alarm Rate	The False alarm rate for the EW system will be not greater than 0.02%, across the entire operating range of the system.
7	R 62.10 Mode 2 Detection Sensitivity	The system will have a detection rate in mode 2 shall be not less than 90%.
8	R 62.11 Passive Detect Signal Detection Sensitivity - Omni	The Passive detect signal detection sensitivity for Omni will be not less than 90%.
9	R 62.12 Passive Detect Signal Detection Sensitivity - ESA	The Passive detect signal detection sensitivity for ESA will be not less than 95%.

Figure 2. Operational Environment Requirements View



EW Situational Awareness
Id = "89"
Text = "The EW System shall provide the threat situational awareness capability to the fighter aircraft"

EW Operationally Effective
Id = "89.1"
Text = "The EW System shall be operationally effective at providing RF situational awareness and threat response information for the aircraft mission set"

EW Operationally Suitable
Id = "89.2"
Text = "The EW System shall be operationally suitable for supporting maintainability and sustainability of the platform in the operational environment."

Computed Identification (ID) Performance
Id = "89.1.3"
Text = "The EW System shall provide Computed Identification of the targets for correct ID, incorrect ID and missed ID targets."

Computed Azimuth Accuracy
Id = "139.4"
Text = "The EW System shall support a Computed Angle of Arrival (AOA) Accuracy of greater than 0.5 degrees."

Symbol Movement Accuracy during Ownship Maneuvering
Id = "89.1.7"
Text = "The EW System shall support a Symbol Movement Accuracy during Ownship Maneuvering of not greater than 3 display pixels."

Ability to Perform BIT and EBIT
Id = "89.2.1"
Text = "The EW System shall be capable of performing BIT and EBIT as per the fault detection and isolation on a accuracy of 95% isolation to the LRU."

Sufficiency of provided Fiber Optic Support Equipment
Id = "89.2.2"
Text = "The EW System shall support the maintenance of its on-board fiber-optic subsystems."

Computed Emitter On-Air Indication Response Time
Id = "139.1"
Text = "The EW System shall support a Computed Emitter On-Air Indication Response Time of less than 9 seconds"

Computed Emitter-Off-Air Age-out Performance
Id = "89.1.4"
Text = "The EW System shall support a Computed Emitter Off-Air Age-out Performance not longer than 15 seconds"

Programmed Display Range Performance
Id = "139.6"
Text = "The EW System shall support a Programmed Display Range Accuracy not less than 500 meters."

Surface-to-Air Threat Discrimination Performance
Id = "89.1.8"
Text = "The EW System shall be able to separate multiple Surface-to-Air threats with a minimum physical separation of 100 meters."

Computed Correct ID Performance
Id = "97"
Text = "The EW System shall provide Computed Identification of correct ID targets of not less than 97 percent"

Computed Incorrect ID Performance
Id = "98"
Text = "The EW System shall provide Computed Identification of incorrect ID targets of less than 2 percent."

Computed Missed ID Performance
Id = "99"
Text = "The EW System shall provide Computed Identification of missed ID targets of less than 1 percent"

Figure 3. EW System SA Requirements

Specify Test Range Requirements Views. For the purpose of this exemplar, the requirements captured as Test Range Requirements are limited to a specific test range capability as shown in Figure 4. To leverage MBSE as a means of positively impacting the time it takes to test systems, development of test range models is vital. Therefore, test range capability requirements are captured within the requirement model which enables traceability to both the test range infrastructure and the SoI requirements. For example, the *Probability of Target Identification Test Range Requirement* specifies that the test range of interest must be capable of testing whether an EW system correctly identifies target/threat systems with a confidence greater than or equal to 90%. The benefit of specifying test range requirements in model form is that it allows for a real-time gap and impact analysis of a test range's capability to test certain system capabilities and enables better test planning by organizations. Having such information readily available can help reduce the time needed to identify the appropriate test ranges needed to test specific systems/system capabilities.

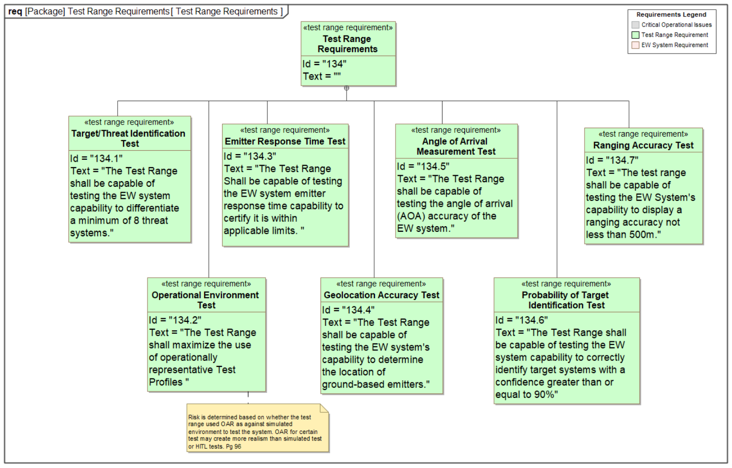

req [Package] Test Range Requirements[Test Range Requirements]
Requirements Legend
Critical Operational Issues
Test Range Requirement
EW System Requirement
«test range requirement» Test Range Requirements
Id = "134"
Text = ""
«test range requirement» Target/Threat Identification Test
Id = "134.1"
Text = "The Test Range shall be capable of testing the EW system capability to differentiate a minimum of 8 threat systems."
«test range requirement» Emitter Response Time Test
Id = "134.3"
Text = "The Test Range Shall be capable of testing the EW system emitter response time capability to certify it is within applicable limits. "
«test range requirement» Angle of Arrival Measurement Test
Id = "134.5"
Text = "The Test Range shall be capable of testing the angle of arrival (AOA) accuracy of the EW system."
«test range requirement» Ranging Accuracy Test
Id = "134.7"
Text = "The test range shall be capable of testing the EW System's capability to display a ranging accuracy not less than 500m."
«test range requirement» Operational Environment Test
Id = "134.2"
Text = "The Test Range shall maximize the use of operationally representative Test Profiles "
«test range requirement» Geolocation Accuracy Test
Id = "134.4"
Text = "The Test Range shall be capable of testing the EW system's capability to determine the location of ground-based emitters."
«test range requirement» Probability of Target Identification Test
Id = "134.6"
Text = "The Test Range shall be capable of testing the EW system capability to correctly identify target systems with a confidence greater than or equal to 90%"
Risk is determined based on whether the test range used OAR as against simulated environment to test the system. OAR for certain test may create more realism than simulated test or HITL tests. Pg 96

Figure 4. Notional Test Range Requirements View

Define Test Requirements and Test Objectives. Also captured as part of the requirements model are testing requirements and test objectives as shown in Figure 5 and Figure 6. Testing requirements also called critical operational issues (COI) outline the issues that are examined during testing and evaluation to determine the system's capability to perform the mission. An example of a testing requirement for the notional EW system is stated as *"Does the EW system provide effective situational awareness to the aircrew?"* It follows then that COIs represent the requirements by which the suitability of the system under test (SUT) will be assessed from a mission perspective. Capturing Test Objectives in a model-based format facilitate tracing of test objectives to system models and test range infrastructure, enabling test personnel to make key decisions in a timely manner.

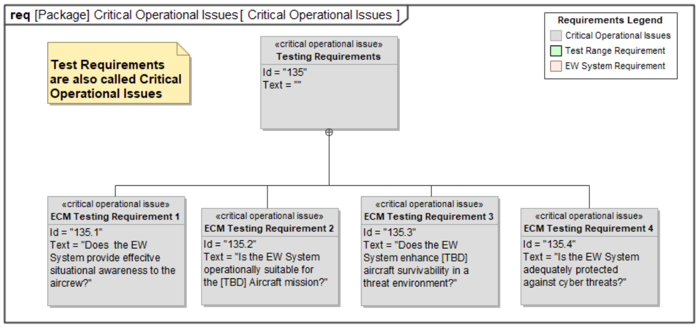

req [Package] Critical Operational Issues[Critical Operational Issues]
Test Requirements are also called Critical Operational Issues
«critical operational issue» Testing Requirements
Id = "135"
Text = ""
Requirements Legend
Critical Operational Issues
Test Range Requirement
EW System Requirement
«critical operational issue» ECM Testing Requirement 1
Id = "135.1"
Text = "Does the EW System provide effecitve situational awareness to the aircrew?"
«critical operational issue» ECM Testing Requirement 2
Id = "135.2"
Text = "Is the EW System operationally suitable for the [TBD] Aircraft mission?"
«critical operational issue» ECM Testing Requirement 3
Id = "135.3"
Text = "Does the EW System enhance [TBD] aircraft survivability in a threat environment?"
«critical operational issue» ECM Testing Requirement 4
Id = "135.4"
Text = "Is the EW System adequately protected against cyber threats?"

Figure 5. EW System Testing Requirement View

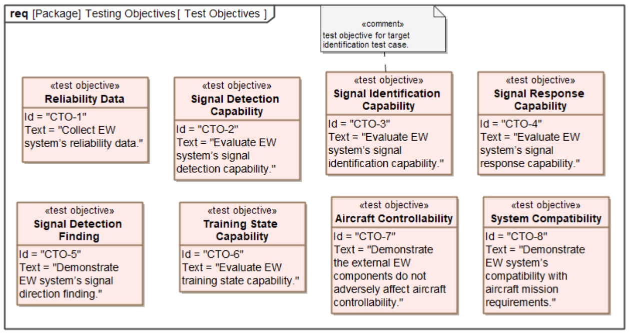

req [Package] Testing Objectives [Test Objectives]
«comment»
test objective for target identification test case.
«test objective»
Reliability Data
Id = "CTO-1"
Text = "Collect EW system's reliability data."
«test objective»
Signal Detection Capability
Id = "CTO-2"
Text = "Evaluate EW system's signal detection capability."
«test objective»
Signal Identification Capability
Id = "CTO-3"
Text = "Evaluate EW system's signal identification capability."
«test objective»
Signal Response Capability
Id = "CTO-4"
Text = "Evaluate EW system's signal response capability."
«test objective»
Signal Detection Finding
Id = "CTO-5"
Text = "Demonstrate EW system's signal direction finding."
«test objective»
Training State Capability
Id = "CTO-6"
Text = "Evaluate EW training state capability."
«test objective»
Aircraft Controllability
Id = "CTO-7"
Text = "Demonstrate the external EW components do not adversely affect aircraft controllability."
«test objective»
System Compatibility
Id = "CTO-8"
Text = "Demonstrate EW system's compatibility with aircraft mission requirements."

Figure 6. EW System Test Objectives View

EW Countermeasures System Architecture Definition

The approach taken in the development of the EW countermeasures notional architecture was to first define the conceptual or black box architectural view of the system which entailed defining the EW system as a black box, and capturing its operational domain. This approach enabled the identification of external interfaces and specification of high level (black box) test cases. Once the conceptual view of the system had been defined, the next step taken was to develop the logical or white box architectural view of the system. This section highlights some of the architectural views created as part of the system architecture definition. The views which comprise both behavioral and structural depictions of the system architecture facilitate the development of test cases for the EW countermeasures system. In order to simplify the modeling and make the process more generalizable for multiple programs, the decision was made to use only unclassified information.

Identify SOI Capabilities and Specify Conceptual Architecture. Two main capabilities of an EW countermeasures system include its ability to *provide situational awareness* to the pilot and *execute self-protection*. The situational awareness capability is the focus for this exemplar model, and hence, most architectural views and artifacts presented here are skewed to this capability with all other aspects either abstracted out or simplified. Figure 7 depicts the *Perform RF Source ECM* capability as a use case of the RF Electronic Countermeasures System. The combined behavior of the use cases, *provide situational awareness* and *execute self-protection,* represent the overall behavior of the *Perform RF Source ECM* capability. Identified primary actors include the *pilot* and *aircraft* while secondary actors (systems) have been identified as EW Threats and Enemy EW Systems. A significant benefit of an MBSE approach is the ability to determine very early in the system acquisition cycle which test resources are required to test a certain system/capability. In the case of the EW countermeasures system, it is apparent that in order to perform a live test of the *provide situational awareness* capability, the test range used should have the capabilities that represent an Enemy EW system. The high-level *perform RF Source ECM* scenario view depicted in Figure 8 highlights the interactions between the SoI and external systems (i.e., enemy threat and radar systems) within its operational domain, while Figure 9 highlights a structural view of the EW countermeasures system domain. Also specified at this level are MOEs of the SoI.

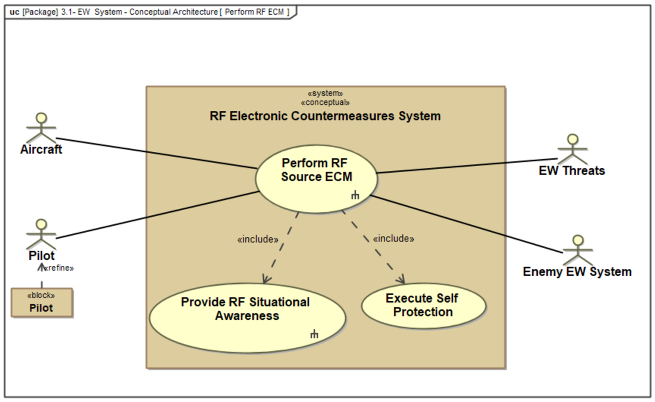

uc [Package] 3.1- EW System - Conceptual Architecture [Perform RF ECM]
«system»
«conceptual»
RF Electronic Countermeasures System
Aircraft
Pilot
«refine»
«block»
Pilot
Perform RF Source ECM
«include»
«include»
Provide RF Situational Awareness
Execute Self Protection
EW Threats
Enemy EW System

Figure 7. Perform RF Source ECM Capability View

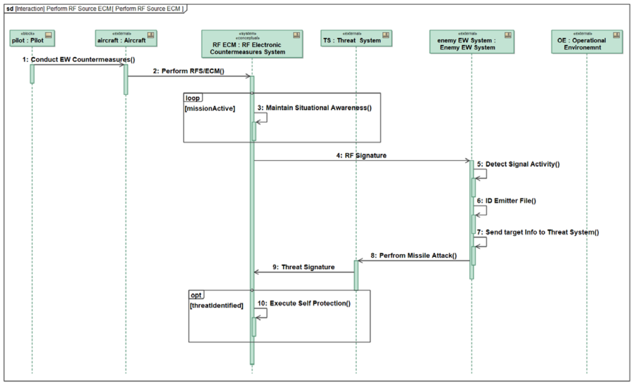

sd [Interaction] Perform RF Source ECM[Perform RF Source ECM]
«block»
pilot : Pilot
«external»
aircraft : Aircraft
«system»
«conceptual»
RF ECM : RF Electronic Countermeasures System
«external»
TS : Threat System
«external»
enemy EW System : Enemy EW System
«external»
OE : Operational Environemnt
1: Conduct EW Countermeasures()
2: Perform RFS/ECM()
loop
[missionActive]
3: Maintain Situational Awareness()
4: RF Signature
5: Detect Signal Activity()
6: ID Emitter File()
7: Send target Info to Threat System()
8: Perfrom Missile Attack()
9: Threat Signature
opt
[threatIdentified]
10: Execute Self Protection()

Figure 8. Perform RF Source ECM Scenario View

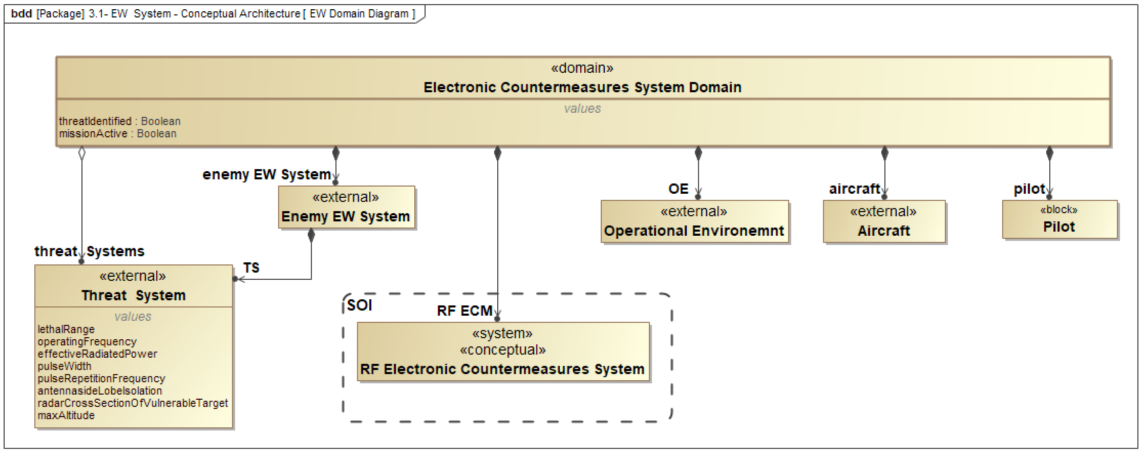


Figure 9. Electronic Countermeasures System Domain View

Develop Logical Architecture Views. The process of developing the logical architecture for the EW system begins with defining the functional/behavior architectural view, identifying logical subsystems, developing a configuration view, and finally allocating the functions (actions) to logical/structural subsystems. Portrayed in Figures 10 and 11 are the logical configuration view portraying the interconnections between subsystems and structural decomposition (hierarchy) view of the exemplar EW countermeasures system.

Additionally, the logical architecture view shown in Figure 12 portrays the allocation of system functions to logical subsystems using swimlanes. The EW system's functional hierarchy / decomposition view is shown in Figure 13.

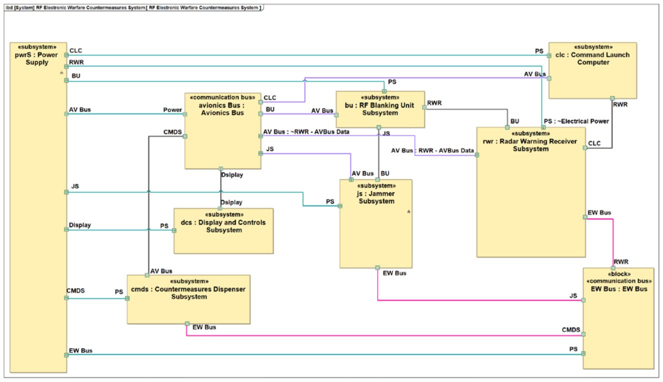

ibd [System] RF Electronic Warfare Countermeasures System[RF Electronic Warfare Countermeasures System]
«subsystem» pwrS : Power Supply
CLC
RWR
BU
AV Bus
JS
Display
CMDS
EW Bus
«subsystem» clc : Command Launch Computer
PS
AV Bus
RWR
«communication bus» avionics Bus : Avionics Bus
Power
CMDS
CLC
BU
AV Bus : ~RWR - AVBus Data
JS
Dsiplay
«subsystem» bu : RF Blanking Unit Subsystem
PS
AV Bus
RWR
JS
«subsystem» rwr : Radar Warning Receiver Subsystem
BU
PS : ~Electrical Power
AV Bus : RWR - AVBus Data
CLC
EW Bus
«subsystem» js : Jammer Subsystem
AV Bus
BU
PS
EW Bus
«subsystem» dcs : Display and Controls Subsystem
Dsiplay
PS
«subsystem» cmds : Countermeasures Dispenser Subsystem
AV Bus
PS
EW Bus
«block» «communication bus» EW Bus : EW Bus
RWR
JS
CMDS
PS

Figure 10. EW System Logical Configuration View

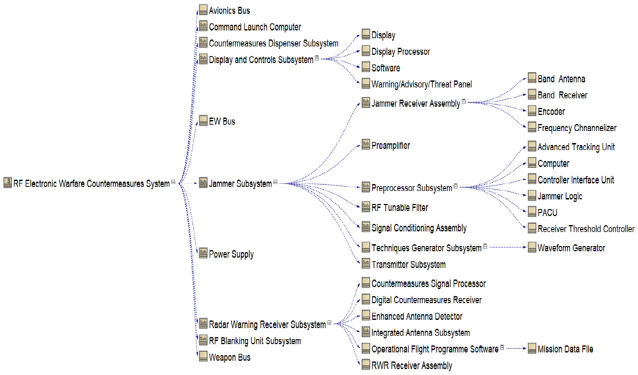

RF Electronic Warfare Countermeasures System
Avionics Bus
Command Launch Computer
Countermeasures Dispenser Subsystem
Display and Controls Subsystem
EW Bus
Jammer Subsystem
Power Supply
Radar Warning Receiver Subsystem
RF Blanking Unit Subsystem
Weapon Bus
Display
Display Processor
Software
Warning/Advisory/Threat Panel
Jammer Receiver Assembly
Preamplifier
Preprocessor Subsystem
RF Tunable Filter
Signal Conditioning Assembly
Techniques Generator Subsystem
Transmitter Subsystem
Countermeasures Signal Processor
Digital Countermeasures Receiver
Enhanced Antenna Detector
Integrated Antenna Subsystem
Operational Flight Programme Software
RWR Receiver Assembly
Band Antenna
Band Receiver
Encoder
Frequency Chnannelizer
Advanced Tracking Unit
Computer
Controller Interface Unit
Jammer Logic
PACU
Receiver Threshold Controller
Waveform Generator
Mission Data File

Figure 11. EW System Structural Decomposition View

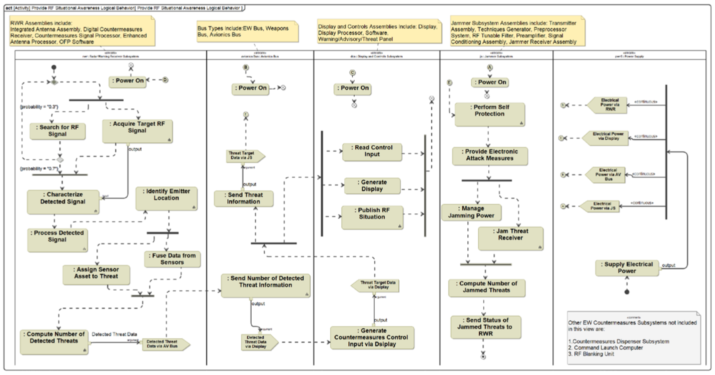

act [Activity] Provide RF Situational Awareness Logical Behavior[Provide RF Situational Awareness Logical Behavior]
RWR Assemblies include: Integrated Antenna Assembly, Digital Countermeasures Receiver, Countermeasures Signal Processor, Enhanced Antenna Processor, OFP Software
Bus Types include:EW Bus, Weapons Bus, Avionics Bus
Display and Controls Assemblies include: Display, Display Processor, Software, Warning/Advisory/Threat Panel
Jammer Subsystem Assemblies include: Transmitter Assembly, Techniques Generator, Preprocessor System, RF Tunable Filter, Preamplifier, Signal Conditioning Assembly, Jammer Receiver Assembly
: Power On
{probability = "0.3"}
: Search for RF Signal
: Acquire Target RF Signal
output
{probability = "0.7"}
: Characterize Detected Signal
: Identify Emitter Location
: Process Detected Signal
: Fuse Data from Sensors
: Assign Sensor Asset to Threat
: Compute Number of Detected Threats
Detected Threat Data
Detected Threat Data via AV Bus
: Power On
Threat Target Data via JS
output
: Send Threat Information
: Send Number of Detected Threat Information
output
Detected Threat Data via Dsiplay
: Power On
: Read Control Input
: Generate Display
: Publish RF Situation
Threat Target Data via Dsiplay
output
: Generate Countermeasures Control Input via Dsiplay
: Power On
: Perform Self Protection
: Provide Electronic Attack Measures
: Manage Jamming Power
: Jam Threat Receiver
: Compute Number of Jammed Threats
: Send Status of Jammed Threats to RWR
Electrical Power via RWR
Electrical Power via Display
Electrical Power via AV Bus
Electrical Power via JS
«continuous»
: Supply Electrical Power
output
Other EW Countermeasures Subsystems not included in this view are:
1.Countermeasures Dispenser Subsystem
2. Command Launch Computer
3. RF Blanking Unit

Figure 12. EW System Logical Architecture View

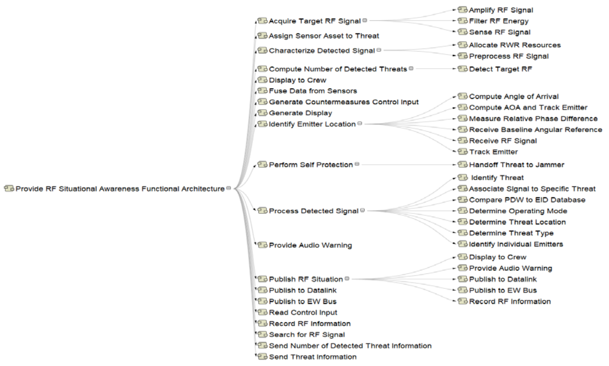
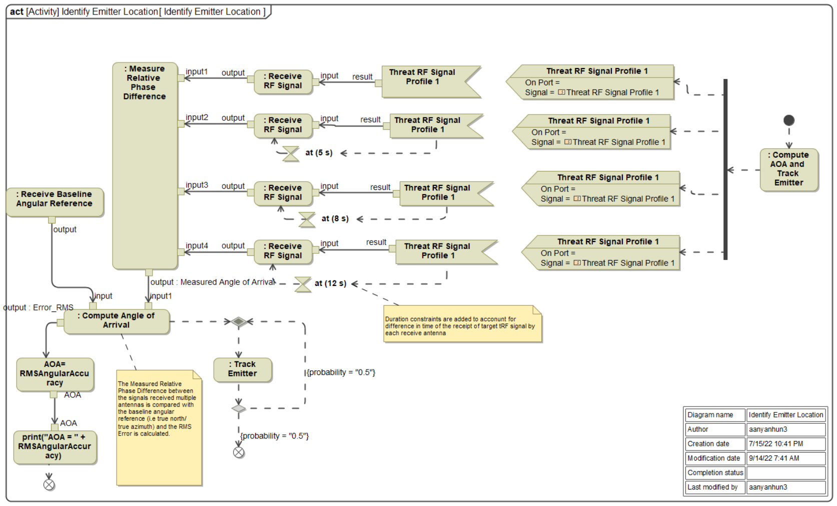


Figure 13. EW System Functional Decomposition View

Furthermore, shown in Figures 14 and 15 are simplifications of the behavior of two EW system functions: *Identify Emitter Location* and *Compute Number of Detected Threats.* They represent key functionality of the EW system needed to *provide situational awareness* to the pilot and other subsystems onboard the aircraft. Identification and modeling of these system capabilities inform the program office and test planners during the early phases of system development of tests that would need to be performed on the system and can enable early testing via simulation of the system model before it is actually built. This approach greatly limits the tendency to develop systems that do not satisfy stated requirements, thereby reducing the overall acquisition cycle time in the event that design rework is required.

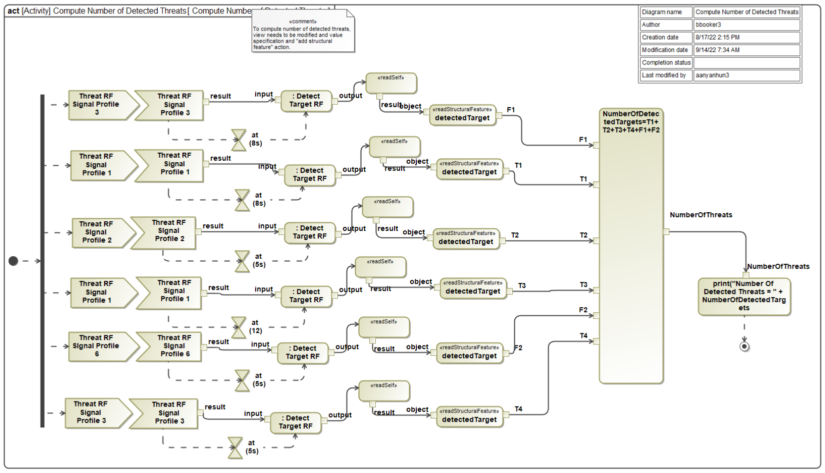

act [Activity] Identify Emitter Location[Identify Emitter Location]
: Measure Relative Phase Difference
input1
output
input2
input3
input4
: Receive RF Signal
input
result
Threat RF Signal Profile 1
at (5 s)
at (8 s)
at (12 s)
Threat RF Signal Profile 1
On Port =
Signal = Threat RF Signal Profile 1
: Compute AOA and Track Emitter
: Receive Baseline Angular Reference
output
output : Measured Angle of Arrival
input
input1
output : Error_RMS
: Compute Angle of Arrival
AOA= RMSAngularAccuracy
AOA
AOA
print("AOA = " + RMSAngularAccuracy)
: Track Emitter
{probability = "0.5"}
{probability = "0.5"}

Duration constraints are added to acconunt for difference in time of the receipt of target tRF signal by each receive antenna

The Measured Relative Phase Difference between the signals received multiple antennas is compared with the baseline angular reference (i.e true north/ true azimuth) and the RMS Error is calculated.

Diagram name	Identify Emitter Location
Author	aanyanhun3
Creation date	7/15/22 10:41 PM
Modification date	9/14/22 7:41 AM
Completion status	
Last modified by	aanyanhun3

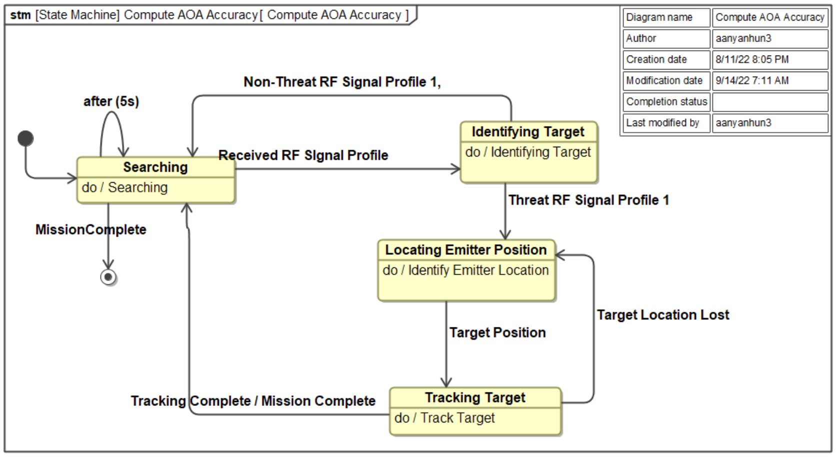
Figure 14. Identify Emitter Behavior View



act [Activity] Compute Number of Detected Threats[Compute Number of Detected Threats]
«comment»
To compute number of detected threats, view needs to be modified and value specification and "add structural feature" action.
Threat RF Signal Profile 3
Threat RF Signal Profile 1
Threat RF Signal Profile 2
Threat RF Signal Profile 6
result
input
: Detect Target RF
output
«readSelf»
result
object
«readStructuralFeature» detectedTarget
at (8s)
at (5s)
at (12)
F1
F2
T1
T2
T3
T4
NumberOfDetectedTargets=T1+T2+T3+T4+F1+F2
NumberOfThreats
print("Number Of Detected Threats = " + NumberOfDetectedTargets

Diagram name	Compute Number of Detected Threats
Author	bbooker3
Creation date	8/17/22 2:15 PM
Modification date	9/14/22 7:34 AM
Completion status	
Last modified by	aanyanhun3

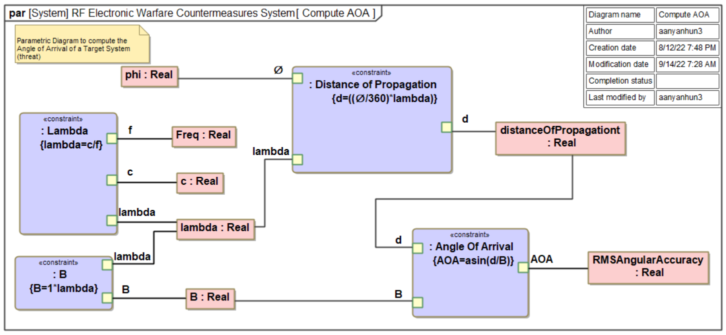
Figure 15. Compute No. of Detected Threats Behavior View



stm [State Machine] Compute AOA Accuracy[Compute AOA Accuracy]
after (5s)
Searching
do / Searching
Non-Threat RF Signal Profile 1,
Received RF SIgnal Profile
Identifying Target
do / Identifying Target
Threat RF Signal Profile 1
Locating Emitter Position
do / Identify Emitter Location
Target Location Lost
Target Position
Tracking Target
do / Track Target
Tracking Complete / Mission Complete
MissionComplete

Diagram name	Compute AOA Accuracy
Author	aanyanhun3
Creation date	8/11/22 8:05 PM
Modification date	9/14/22 7:11 AM
Completion status	
Last modified by	aanyanhun3

Figure 16. EW System Behavior View



par [System] RF Electronic Warfare Countermeasures System[Compute AOA]
Parametric Diagram to compute the Angle of Arrival of a Target System (threat)
phi : Real
Ø
«constraint»
: Distance of Propagation
{d=((Ø/360)*lambda)}
d
distanceOfPropagationt : Real
«constraint»
: Lambda
{lambda=c/f}
f
Freq : Real
c
c : Real
lambda
lambda : Real
«constraint»
: B
{B=1*lambda}
B
B : Real
«constraint»
: Angle Of Arrival
{AOA=asin(d/B)}
AOA
RMSAngularAccuracy : Real

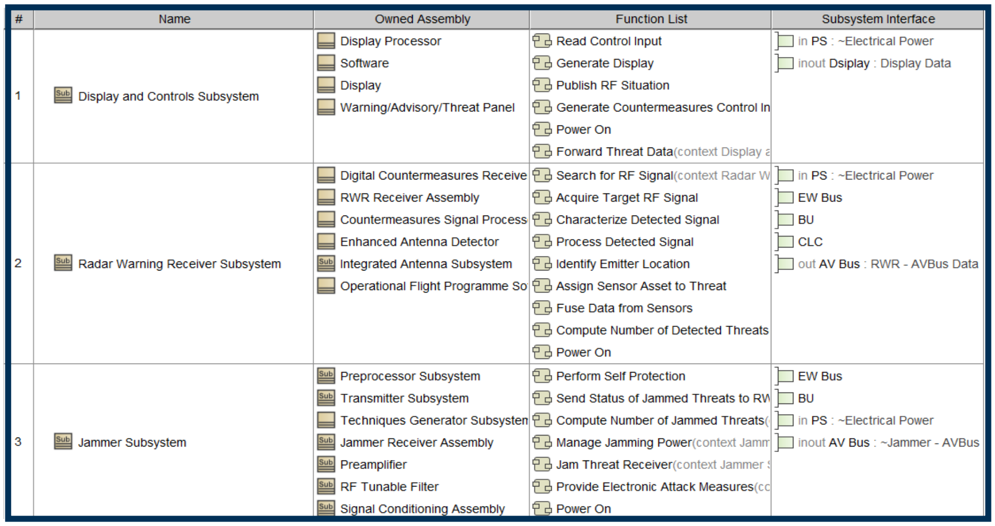
Diagram name	Compute AOA
Author	aanyanhun3
Creation date	8/12/22 7:48 PM
Modification date	9/14/22 7:28 AM
Completion status	
Last modified by	aanyanhun3

Figure 17. Angle of Arrival Parametric View

In addition, developed within the system architecture model are the views highlighted in Figure 16 which portrays the system behavior using a *state machine* and a system performance analysis view created to compute the angle of arrival (AOA) which is shown in Figure 17. The AOA is a system property that was specified as a measure of effectiveness in the *conceptual* architecture. Development of these system views are critical since they are used during model-based testing activities.

Curate Key Traceability Views. During the model-based development of the EW countermeasures system architecture, several model views and artifacts are created which describe the system from multiple perspectives such as structural, behavioral, interfaces, data, etc., and varying levels of fidelity. These views explicitly portray existing relationships between model elements, however, there also exist implicit relationships between some model elements that are not captured in these model views but which are crucial to understanding the system. Identifying and capturing these implicit relationships enable the performance of impact analysis, regression analysis, and promote the understanding of how these relationships impact system behavior and by extension test results. As reported by Konigs et al., "traceability allows changes to be propagated efficiently while implications can be detected easily based on relations between multiple artifacts" (2012). Highlighted in Table 1 are traceability views which portray existing explicit/implicit relationships between model data.

Table 1. EW System Traceability View Mapping Structure to Function



#	Name	Owned Assembly	Function List	Subsystem Interface
1	Display and Controls Subsystem	Display Processor Software Display Warning/Advisory/Threat Panel	Read Control Input Generate Display Publish RF Situation Generate Countermeasures Control In Power On Forward Threat Data(context Display a	in PS : ~Electrical Power inout Dsiplay : Display Data
2	Radar Warning Receiver Subsystem	Digital Countermeasures Receive RWR Receiver Assembly Countermeasures Signal Process Enhanced Antenna Detector Integrated Antenna Subsystem Operational Flight Programme So	Search for RF Signal(context Radar W Acquire Target RF Signal Characterize Detected Signal Process Detected Signal Identify Emitter Location Assign Sensor Asset to Threat Fuse Data from Sensors Compute Number of Detected Threats Power On	in PS : ~Electrical Power EW Bus BU CLC out AV Bus : RWR - AVBus Data
3	Jammer Subsystem	Preprocessor Subsystem Transmitter Subsystem Techniques Generator Subsysten Jammer Receiver Assembly Preamplifier RF Tunable Filter Signal Conditioning Assembly	Perform Self Protection Send Status of Jammed Threats to RW Compute Number of Jammed Threats(Manage Jamming Power(context Jamm Jam Threat Receiver(context Jammer Provide Electronic Attack Measures(cc Power On	EW Bus BU in PS : ~Electrical Power inout AV Bus : ~Jammer - AVBus

Develop Test Range Capability Architecture

A test capability model can be described as a model-based representation of all test resources required to enable the testing of a given set of systems/capabilities. The test range infrastructure is a key part of the model-based integrated test prototype and consists of the testing capabilities required to test an EW countermeasures system. In this section, aspects of a notional test range model based on the Eglin test range (Eglin Customer Guide, 2021) will be presented. The test range model captures the system capabilities the test range is capable of testing, test range test resources, its structural composition, and test operational environments. Development of the test range model begins with the identification and definition of the capabilities of the test range.

Identify Test Range Capabilities. The first step taken in the development of the model-based test range was to identify the test range capabilities. Test range capabilities in this work refer to the types/kinds/categories/forms of tests a test range is capable of executing. The Eglin Test and Training Complex (ETTC) has a total of 45 test capabilities (Eglin Customer Guide, 2021), some of which are shown in Figure 18. Specifically, the test capabilities of interest for this model prototype shown in the use case diagram highlighted in Figure 19 is the *Perform EW Countermeasures Test* capability and the *Perform RF Source*

Countermeasures Test. Once capabilities have been identified and defined as part of the test range model, next steps entail the development of the test range infrastructure's architecture.

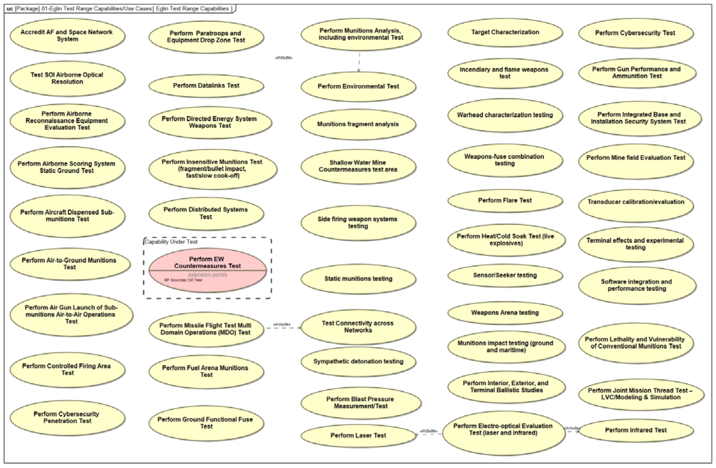

uc [Package] 01-Eglin Test Range Capabilities/Use Cases[Eglin Test Range Capabilities]
Accredit AF and Space Network System
Test SOI Airborne Optical Resolution
Perform Airborne Reconnaissance Equipment Evaluation Test
Perform Airborne Scoring System Static Ground Test
Perform Aircraft Dispensed Sub-munitions Test
Perform Air-to-Ground Munitions Test
Perform Air Gun Launch of Sub-munitions Air-to-Air Operations Test
Perform Controlled Firing Area Test
Perform Cybersecurity Penetration Test
Perform Paratroops and Equipment Drop Zone Test
Perform Datalinks Test
Perform Directed Energy System Weapons Test
Perform Insensitive Munitions Test (fragment/bullet impact, fast/slow cook-off)
Perform Distributed Systems Test
Capability Under Test
Perform EW Countermeasures Test
extension points
RF Sources CM Test
Perform Missile Flight Test Multi Domain Operations (MDO) Test
Perform Fuel Arena Munitions Test
Perform Ground Functional Fuse Test
«include»
Perform Munitions Analysis, including environmental Test
Perform Environmental Test
Munitions fragment analysis
Shallow Water Mine Countermeasures test area
Side firing weapon systems testing
Static munitions testing
«include»
Test Connectivity across Networks
Sympathetic detonation testing
Perform Blast Pressure Measurement/Test
Perform Laser Test
«include»
Target Characterization
Incendiary and flame weapons test
Warhead characterization testing
Weapons-fuse combination testing
Perform Flare Test
Perform Heat/Cold Soak Test (live explosives)
Sensor/Seeker testing
Weapons Arena testing
Munitions impact testing (ground and maritime)
Perform Interior, Exterior, and Terminal Ballistic Studies
Perform Electro-optical Evaluation Test (laser and infrared)
«include»
Perform Cybersecurity Test
Perform Gun Performance and Ammunition Test
Perform Integrated Base and Installation Security System Test
Perform Mine field Evaluation Test
Transducer calibration/evaluation
Terminal effects and experimental testing
Software integration and performance testing
Perform Lethality and Vulnerability of Conventional Munitions Test
Perform Joint Mission Thread Test – LVC/Modeling & Simulation
Perform Infrared Test

Figure 18. List of Eglin Test Center Test Capabilities

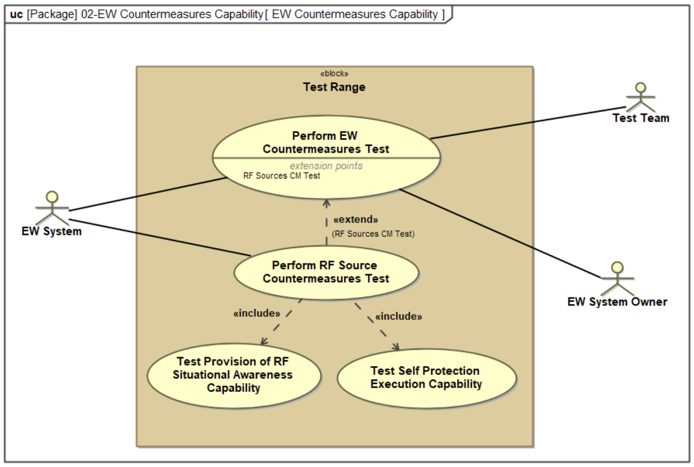

uc [Package] 02-EW Countermeasures Capability[EW Countermeasures Capability]
«block»
Test Range
Perform EW Countermeasures Test
extension points
RF Sources CM Test
Test Team
EW System
«extend»
(RF Sources CM Test)
Perform RF Source Countermeasures Test
EW System Owner
«include»
«include»
Test Provision of RF Situational Awareness Capability
Test Self Protection Execution Capability

Figure 19. Perform EW Countermeasures Test

Specify Test Range Infrastructure. The test range model infrastructure shown in Figure 20 specifies specific aspects of a test range required for performing an EW Countermeasures Test. Range infrastructure include *Test Instrumentation, EW Threat Systems, EW Non-Threat Systems,* and *Air Threat Defense Systems*. Additionally, the EW threat systems view portrayed in Figure 21 highlights several types of radar threat systems that form part of the test environment configuration while test resources captured in Figure 22 are also used as part of the test configuration. The capture of these test range resources and their properties within the test range model enables the construction of holistic and integrated test case configurations.

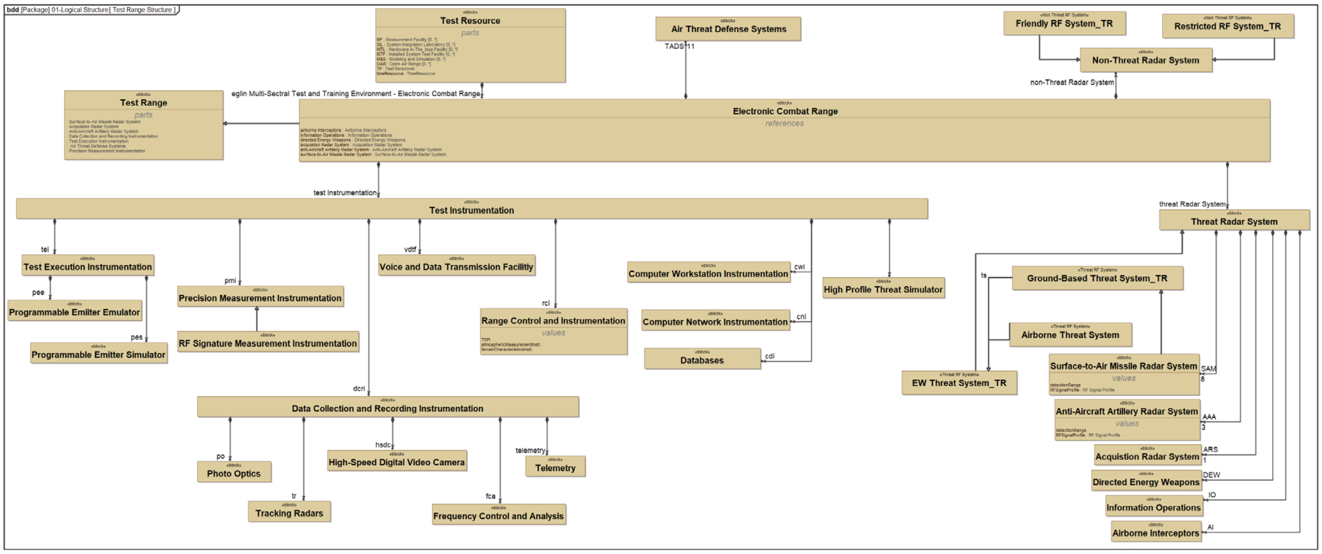

bdd [Package] 01-Logical Structure[Test Range Structure]
Test Resource
Air Threat Defense Systems
TADS
Friendly RF System_TR
Restricted RF System_TR
Non-Threat Radar System
non-Threat Radar System
Test Range
eglin Multi-Sectral Test and Training Environment - Electronic Combat Range
Electronic Combat Range
test Instrumentation
Test Instrumentation
threat Radar System
Threat Radar System
tei
Test Execution Instrumentation
vdtf
Voice and Data Transmission Facilitiy
pee
Programmable Emitter Emulator
pmi
Precision Measurement Instrumentation
Computer Workstation Instrumentation
cwi
High Profile Threat Simulator
ts
Ground-Based Threat System_TR
pes
Programmable Emitter Simulator
RF Signature Measurement Instrumentation
rci
Range Control and Instrumentation
Computer Network Instrumentation
cni
Airborne Threat System
Databases
cdi
EW Threat System_TR
Surface-to-Air Missile Radar System
SAM
dcri
Data Collection and Recording Instrumentation
Anti-Aircraft Artillery Radar System
AAA
hsdc
High-Speed Digital Video Camera
telemetry
Telemetry
po
Photo Optics
Acquistion Radar System
ARS
Directed Energy Weapons
DEW
tr
Tracking Radars
fca
Frequency Control and Analysis
Information Operations
IO
Airborne Interceptors
AI

Figure 20. Notional Test Range Infrastructure View

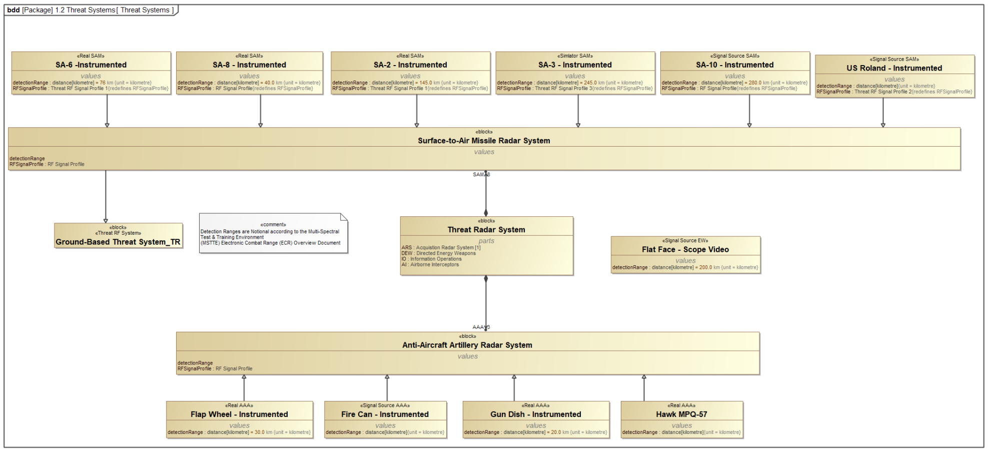

bdd [Package] 1.2 Threat Systems[Threat Systems]
SA-6 -Instrumented
SA-8 - Instrumented
SA-2 - Instrumented
SA-3 - Instrumented
SA-10 - Instrumented
US Roland - Instrumented
Surface-to-Air Missile Radar System
Ground-Based Threat System_TR
Detection Ranges are Notional according to the Multi-Spectral Test & Training Environment (MSTTE) Electronic Combat Range (ECR) Overview Document
Threat Radar System
Flat Face - Scope Video
Anti-Aircraft Artillery Radar System
Flap Wheel - Instrumented
Fire Can - Instrumented
Gun Dish - Instrumented
Hawk MPQ-57

Figure 21. Test Range Threat Radar Systems View

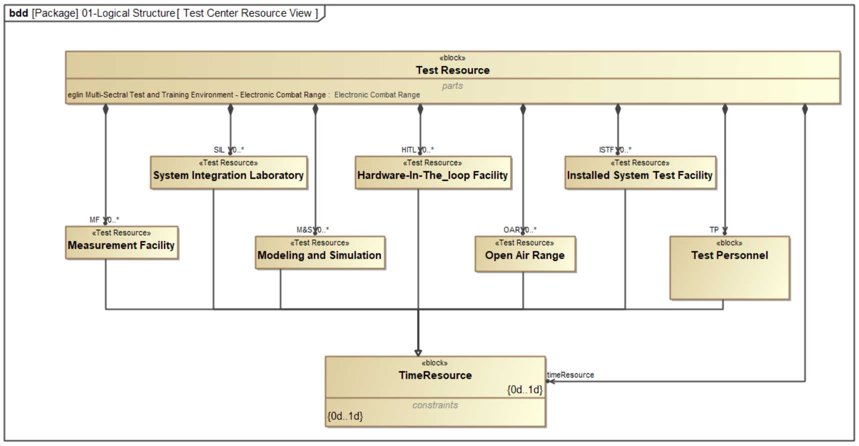


Figure 22. Test Range Test Resources View

Consequently, the capture and definition of test range artifacts in model form plays a crucial role in *test planning* by providing information on available test range resources, in *testing* by enabling model execution of test cases early in the system development life cycle, and in identifying *test risks* relating to test range resource availability.

Test Range Operational Environment Definition. A very important aspect of test range model definition involves specifying the various operational environments required for performing specific types of EW system tests. Shown in Figure 23 is a high-level structural view of the Test Range Operational Environment. As shown, the test range operational environment is grouped into two main categories: *Test Range Electromagnetic Operational Environment* (EMOE) and *Test Range Geophysical Environment*. Of importance for this exemplar however, are the EW countermeasures system operational environments, namely, congested environment, contested environment, and constrained environment types respectively. Defining these environments as part of the test range test capability are necessary to enable testing of the EW system to verify that the EW system requirements can be satisfied as well as enable the mapping of risk to the specific system operational environments.

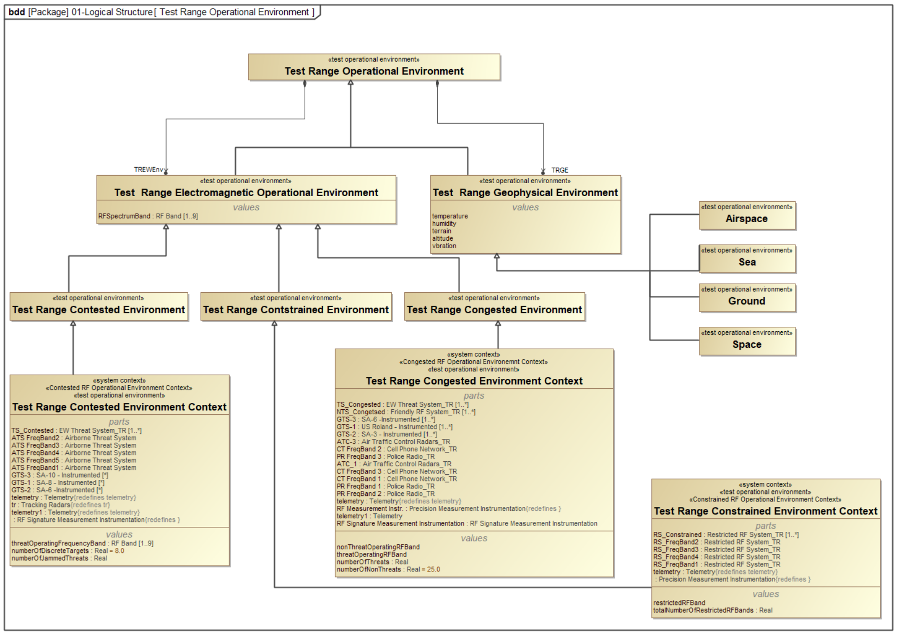

bdd [Package] 01-Logical Structure[Test Range Operational Environment]
«test operational environment»
Test Range Operational Environment
TREWEnv
TRGE
«test operational environment»
Test Range Electromagnetic Operational Environment
values
RFSpectrumBand : RF Band [1..9]
«test operational environment»
Test Range Geophysical Environment
values
temperature
humidity
terrain
altitude
vbration
«test operational environment»
Airspace
«test operational environment»
Sea
«test operational environment»
Ground
«test operational environment»
Space
«test operational environment»
Test Range Contested Environment
«test operational environment»
Test Range Contstrained Environment
«test operational environment»
Test Range Congested Environment
«system context»
«Contested RF Operational Environment Context»
«test operational environment»
Test Range Contested Environment Context
parts
TS_Contested : EW Threat System_TR [1..*]
ATS FreqBand2 : Airborne Threat System
ATS FreqBand3 : Airborne Threat System
ATS FreqBand4 : Airborne Threat System
ATS FreqBand5 : Airborne Threat System
ATS FreqBand1 : Airborne Threat System
GTS-3 : SA-10 - Instrumented [*]
GTS-1 : SA-8 - Instrumented [*]
GTS-2 : SA-6 -Instrumented [*]
telemetry : Telemetry{redefines telemetry}
tr : Tracking Radars{redefines tr}
telemetry1 : Telemetry{redefines telemetry}
: RF Signature Measurement Instrumentation{redefines }
values
threatOperatingFrequencyBand : RF Band [1..9]
numberOfDiscreteTargets : Real = 8.0
numberOfJammedThreats : Real
«system context»
«Congested RF Operational Environemnt Context»
«test operational environment»
Test Range Congested Environment Context
parts
TS_Congested : EW Threat System_TR [1..*]
NTS_Congetsed : Friendly RF System_TR [1..*]
GTS-3 : SA-6 -Instrumented [1..*]
GTS-1 : US Roland - Instrumented [1..*]
GTS-2 : SA-3 - Instrumented [1..*]
ATC-3 : Air Traffic Control Radars_TR
CT FreqBand 2 : Cell Phone Network_TR
PR FreqBand 3 : Police Radio_TR
ATC_1 : Air Traffic Control Radars_TR
CT FreqBand 3 : Cell Phone Network_TR
CT FreqBand 1 : Cell Phone Network_TR
PR FreqBand 1 : Police Radio_TR
PR FreqBand 2 : Police Radio_TR
telemetry : Telemetry{redefines telemetry}
RF Measurement Instr. : Precision Measurement Instrumentation{redefines }
telemetry1 : Telemetry
RF Signature Measurement Instrumentation : RF Signature Measurement Instrumentation
values
nonThreatOperatingRFBand
threatOperatingRFBand
numberOfThreats : Real
numberOfNonThreats : Real = 25.0
«system context»
«test operational environment»
«Constrained RF Operational Environment Context»
Test Range Constrained Environment Context
parts
RS_Constrained : Restricted RF System_TR [1..*]
RS_FreqBand2 : Restricted RF System_TR
RS_FreqBand3 : Restricted RF System_TR
RS_FreqBand4 : Restricted RF System_TR
RS_FreqBand1 : Restricted RF System_TR
telemetry : Telemetry{redefines telemetry}
: Precision Measurement Instrumentation{redefines }
values
restrictedRFBand
totalNumberOfRestrictedRFBands : Real

Figure 23. High-Level Test Range Operational Environment View

Test Range Infrastructure Traceability. Creating traceability views of test range resources such as the test instrumentation infrastructure, threat systems, and air defense systems serve as crucial model data views which enable test planning and testing activities using the *model-based test-integrated system* prototype. Figure 24 highlights several explicitly and implicitly identified relationships among test range infrastructure artifacts.

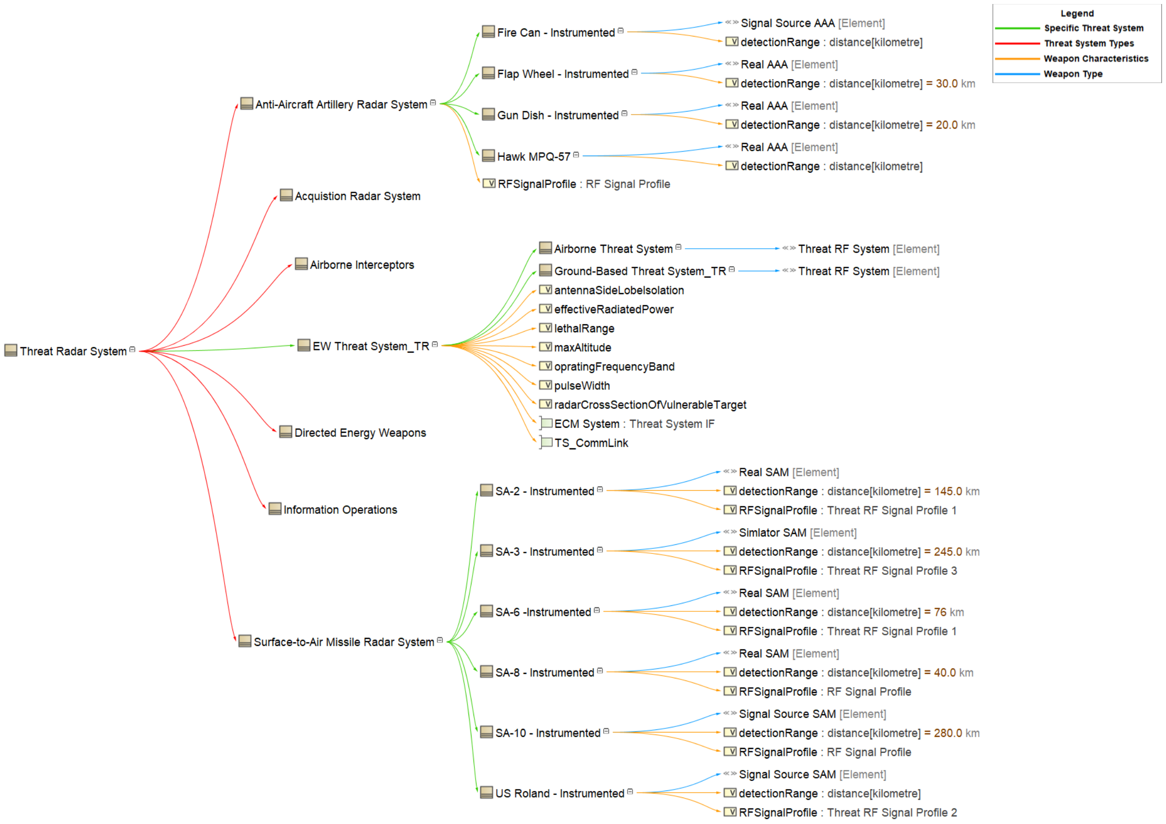

Legend
Specific Threat System
Threat System Types
Weapon Characteristics
Weapon Type
Threat Radar System
Anti-Aircraft Artillery Radar System
Fire Can - Instrumented
«» Signal Source AAA [Element]
detectionRange : distance[kilometre]
Flap Wheel - Instrumented
«» Real AAA [Element]
detectionRange : distance[kilometre] = 30.0 km
Gun Dish - Instrumented
«» Real AAA [Element]
detectionRange : distance[kilometre] = 20.0 km
Hawk MPQ-57
«» Real AAA [Element]
detectionRange : distance[kilometre]
RFSignalProfile : RF Signal Profile
Acquistion Radar System
Airborne Interceptors
EW Threat System_TR
Airborne Threat System
«» Threat RF System [Element]
Ground-Based Threat System_TR
«» Threat RF System [Element]
antennaSideLobeIsolation
effectiveRadiatedPower
lethalRange
maxAltitude
opratingFrequencyBand
pulseWidth
radarCrossSectionOfVulnerableTarget
ECM System : Threat System IF
TS_CommLink
Directed Energy Weapons
Information Operations
Surface-to-Air Missile Radar System
SA-2 - Instrumented
«» Real SAM [Element]
detectionRange : distance[kilometre] = 145.0 km
RFSignalProfile : Threat RF Signal Profile 1
SA-3 - Instrumented
«» Simlator SAM [Element]
detectionRange : distance[kilometre] = 245.0 km
RFSignalProfile : Threat RF Signal Profile 3
SA-6 -Instrumented
«» Real SAM [Element]
detectionRange : distance[kilometre] = 76 km
RFSignalProfile : Threat RF Signal Profile 1
SA-8 - Instrumented
«» Real SAM [Element]
detectionRange : distance[kilometre] = 40.0 km
RFSignalProfile : RF Signal Profile
SA-10 - Instrumented
«» Signal Source SAM [Element]
detectionRange : distance[kilometre] = 280.0 km
RFSignalProfile : RF Signal Profile
US Roland - Instrumented
«» Signal Source SAM [Element]
detectionRange : distance[kilometre]
RFSignalProfile : Threat RF Signal Profile 2

Figure 24. Traceability View of Test Range Threat Radar Systems

System Under Test (SUT) and Test Case Modeling

A key aspect of the *model-based test-integrated system* prototype is the development and modeling of test cases and test case configurations for the system under test (SUT). In order to perform model-based testing within the MBSE environment, test cases and the test scenario configuration need to be defined for the SUT. In the context of this work, the test configuration describes the testing context for the SUT and comprises the SUT, test resources, test personnel, test case, and the system requirements that need to be satisfied. The test community and program offices can use this model-based test configuration to inform decision making regarding availability of test range resources and the system requirements that need to be satisfied by the SUT per (mission) test case. The test configuration pattern shown in Figure 25 is an abstract representation of a test context and depicts the components required for test case execution and the relationships between them.

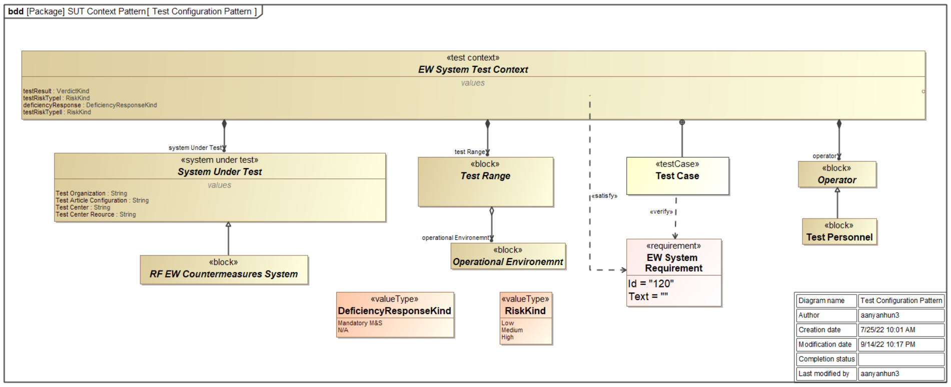


Figure 25. Model-Based Test Configuration Pattern

Execute Test Case Model and Capture Results. The model view portrayed in Figure 26 is an example of an implementation of the test configuration pattern shown in Figure 25. The model view shown represents the test context for the EW countermeasures system *Angle of Arrival Test Case*. It can be noted that the operational environment in which the system is being tested is designated as a specific contested operational environment. Test range resources listed as part of the contested environment include multiple threat radar systems, telemetry, and RF signature measurement instrumentation. Also captured as test scenario participants are test personnel, the requirement being tested, the SUT, and the test case artifact. Results gotten from the execution of the AOA test case context are captured in the test instance specification table shown in Table. 2.

The SUT requirements traceability view shown in Figure 27, highlighting implicit relationships that may exist between the artifacts of the integrated test model prototype. Moreover, such traceability views allow planned or unplanned change implications to be quantified and assessed.

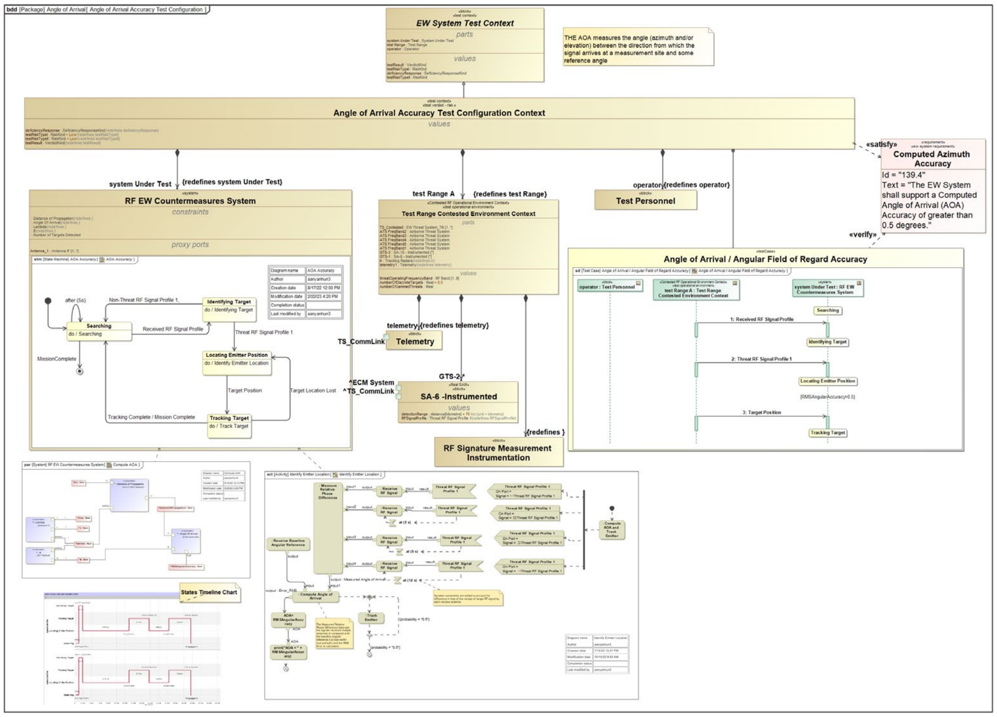
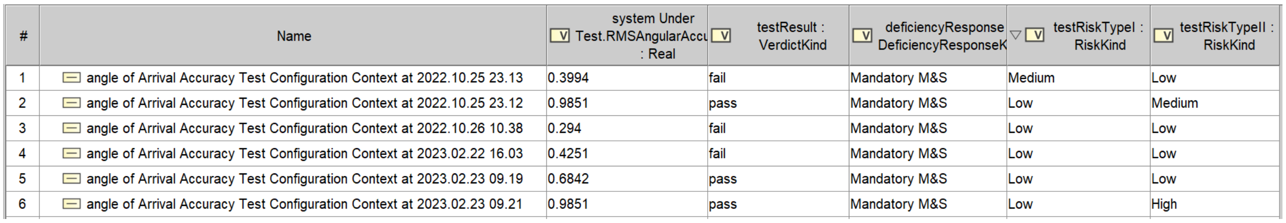

bdd [Package] Angle of Arrival[Angle of Arrival Accuracy Test Configuration]
EW System Test Context
parts
values
THE AOA measures the angle (azimuth and/or elevation) between the direction from which the signal arrives at a measurement site and some reference angle
Angle of Arrival Accuracy Test Configuration Context
values
«satisfy»
Computed Azimuth Accuracy
Id = "139.4"
Text = "The EW System shall support a Computed Angle of Arrival (AOA) Accuracy of greater than 0.5 degrees."
«verify»
system Under Test
{redefines system Under Test}
RF EW Countermeasures System
constraints
proxy ports
test Range A
{redefines test Range}
Test Range Contested Environment Context
parts
values
operator
{redefines operator}
Test Personnel
Searching
do / Searching
after (5s)
Non-Threat RF Signal Profile 1
Identifying Target
do / Identifying Target
Received RF Signal Profile
Threat RF Signal Profile 1
Locating Emitter Position
do / Identify Emitter Location
MissionComplete
Target Position
Target Location Lost
Tracking Complete / Mission Complete
Tracking Target
do / Track Target
telemetry
{redefines telemetry}
TS_CommLink
Telemetry
GTS-2
^ECM System
^TS_CommLink
SA-6 -Instrumented
values
{redefines }
RF Signature Measurement Instrumentation
Angle of Arrival / Angular Field of Regard Accuracy
operator : Test Personnel
test Range A : Test Range Contested Environment Context
system Under Test : RF EW Countermeasures System
Searching
1: Received RF Signal Profile
Identifying Target
2: Threat RF Signal Profile 1
Locating Emitter Position
[RMSAngularAccuracy>0.5]
3: Target Position
Tracking Target
States Timeline Chart

Figure 26. EW System Angle of Arrival Accuracy Testing Context

Table 2. Angle of Arrival Accuracy Test Execution Results for the EW System



#	Name	system Under Test.RMSAngularAccu : Real	testResult : VerdictKind	deficiencyResponse DeficiencyResponseK	testRiskTypeI : RiskKind	testRiskTypeII : RiskKind
1	angle of Arrival Accuracy Test Configuration Context at 2022.10.25 23.13	0.3994	fail	Mandatory M&S	Medium	Low
2	angle of Arrival Accuracy Test Configuration Context at 2022.10.25 23.12	0.9851	pass	Mandatory M&S	Low	Medium
3	angle of Arrival Accuracy Test Configuration Context at 2022.10.26 10.38	0.294	fail	Mandatory M&S	Low	Low
4	angle of Arrival Accuracy Test Configuration Context at 2023.02.22 16.03	0.4251	fail	Mandatory M&S	Low	Low
5	angle of Arrival Accuracy Test Configuration Context at 2023.02.23 09.19	0.6842	pass	Mandatory M&S	Low	Low
6	angle of Arrival Accuracy Test Configuration Context at 2023.02.23 09.21	0.9851	pass	Mandatory M&S	Low	High

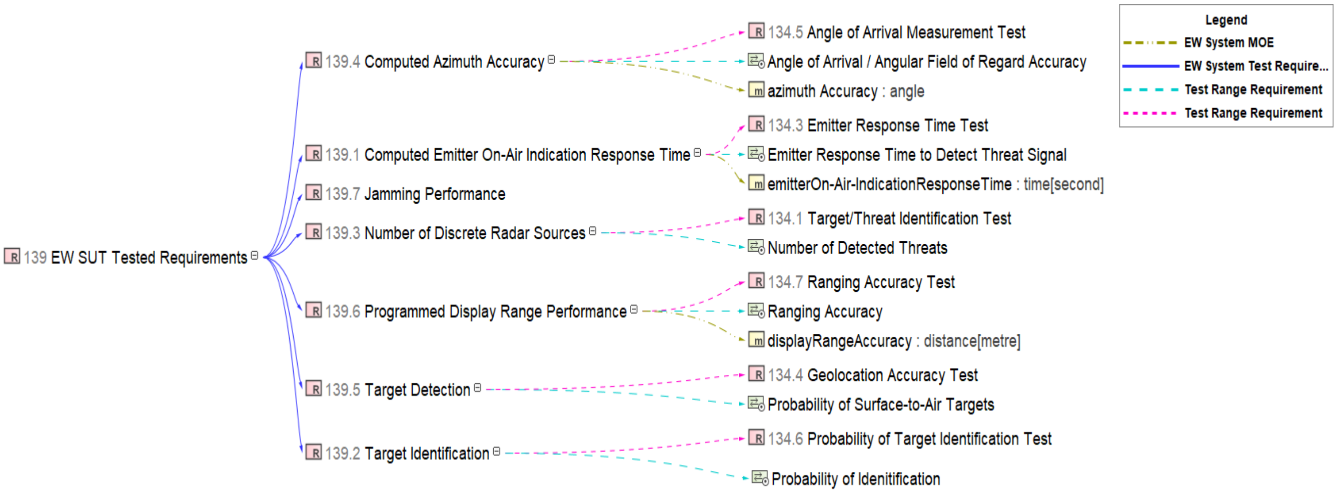

139 EW SUT Tested Requirements
139.4 Computed Azimuth Accuracy
139.1 Computed Emitter On-Air Indication Response Time
139.7 Jamming Performance
139.3 Number of Discrete Radar Sources
139.6 Programmed Display Range Performance
139.5 Target Detection
139.2 Target Identification
134.5 Angle of Arrival Measurement Test
Angle of Arrival / Angular Field of Regard Accuracy
azimuth Accuracy : angle
134.3 Emitter Response Time Test
Emitter Response Time to Detect Threat Signal
emitterOn-Air-IndicationResponseTime : time[second]
134.1 Target/Threat Identification Test
Number of Detected Threats
134.7 Ranging Accuracy Test
Ranging Accuracy
displayRangeAccuracy : distance[metre]
134.4 Geolocation Accuracy Test
Probability of Surface-to-Air Targets
134.6 Probability of Target Identification Test
Probability of Idenitification
Legend
EW System MOE
EW System Test Require...
Test Range Requirement
Test Range Requirement

Figure 27. Test-Related Artifacts Traceability View

A key benefit of the model-based test integrated system prototype concept is that it enables the execution and analysis of multiple user defined missions and operational environment test configurations in a minimum amount of time. As a consequence, this testing prototype provides quantifiable value to program offices and the test community through its ability to impact the defense acquisition cycle time positively by enabling program offices to make informed decisions regarding system tests and associated risk in a timely manner.

Development and Modeling of the Risk Function

Program risk in the context of this project is inherently a function of different aspects of the program's ability to create and deliver a useful product to the field. Traditionally risk functions have focused only on the risk to the program of developing the end item product. The traditional risk approach also developed risks based on specific design risks. This approach has several short comings. First, this approach does not guarantee a comprehensive coverage of all possible risks. Second, the traditional approach has no specific way of addressing risk created in the testing program independent of the acquisition risk of different parts of the system. Third, the traditional approach to risk does not have a direct means of aggregating risk from the system's operational mission or operational environments. As a result, these three specific areas form the requirements set for the development of a new risk approach.

1. Develop a risk function that is comprehensive across all areas of the program.
2. It is critical that the risk function capture risks that are inherent to the testing of systems.

3. A risk function needs the ability to aggregate risk across different aspects of the program, specifically aggregate risks across mission areas and operation environments.

Additionally, the risk function must be compatible with the system modeling functions.

Elements of the Risk Function

In developing the comprehensive risk function, it was determined assessing risk on each requirement represented a means of assessing risk on all parts of the system in a comprehensive way. Undoubtedly, linking risk to the system requirements addressed several different issues. First, the requirements are modeled as a part of the MBSE process and are therefore part of the integrated engineering model of the system. Second, by linking the risk to the requirements, it is assured that the evaluation of all possible risks in the system is done in a comprehensive way. The requirements, if specified correctly and unambiguously, describe all the different aspects of the system and its operations including its different missions and operating environments.

Therefore, for a given mission and operational environment, a program's risk can be aggregated and evaluated by combining the system requirements specified for the system operations based on a given mission and operational environment. Functionally, this approach allows for different weighting of factors to the individual risks so that the overall risk profile for a given mission can reflect the different priorities of the mission. To effectively model testing risks, a test-based risk function was developed which addresses the risks inherent in the testing infrastructure's ability to completely test system requirements, and the risk of the testing infrastructure's ability to replicate future operational environments during system test. Specifically, the three risk categories defined in the test-based risk function include:

- Type 1 Test Risk: the ability to test to the requirements.
- Type 2 Test Risk: the reliability of the testing to validate the operational environment (confidence in test).
- Implementation Risk: the risk of being able to design and build the system to meet its requirements. This could be viewed as the traditional risk function (cost, schedule, and performance risks).

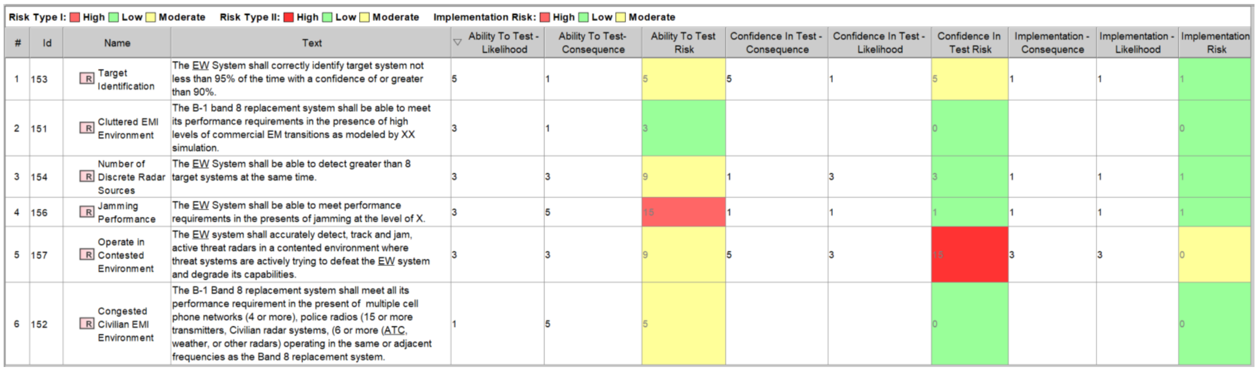
Use of the Risk Function to Determine a Mission-Based Risk Profile

Operational environments and missions of interest contribute to the risk of a given system not being able to perform as designed, or as needed during operations. The risk function provides the ability to roll up the risk for the different test cases. In particular, the test risks allow the program office and test community to assess whether the testing resources available at a given test range can effectively test the system requirements to the levels expected in the operational environment for different missions of interest.

Mapping of the risk function characteristics to specific operational environments and user defined missions can be accomplished in one of two ways. The first involves using the system requirements to describe a specific mission. *Given that the complete set of requirements contain all requirements necessary for a given system to perform all required missions under all specified operating conditions, it follows that a subset of the requirements can be selected which describe a specific mission and operating environment*. While the second involves the use of the system's operational testing requirements. *In this method, the testing requirements and test cases for a specific mission are linked to the risk model to capture risks from the mission of interest.* The risks can then be aggregated to form a mission-based risk profile.

A demonstration of the mission-based risk profile developed for the EW countermeasures system and created within the *model-based test-integrated system* prototype is portrayed in Table 3, Table 4, and Table 5. In this example, the mission-based risk profile is created by mapping the set of requirements of the EW countermeasures system needed to perform a user-defined mission within specific contested, congested, and constrained environments. As shown in the congested, contested, and constrained risk function tables, values for the *Likelihood* and *Consequence* of each risk type are entered into the tables following which the value for each risk type is then automatically computed and given the necessary risk color based on the computed value.

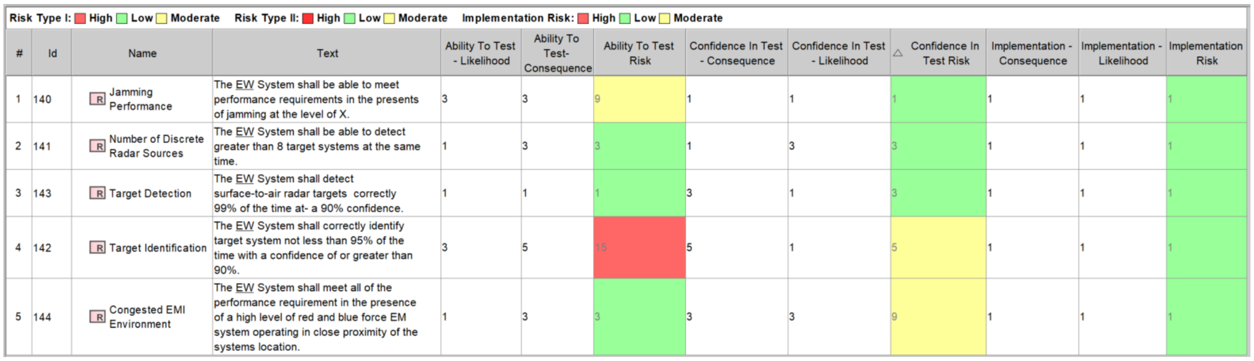
Table 3. Contested Environment Mission-Based Risk Function for the EW Countermeasures System



Risk Type I: 🟥 High 🟩 Low 🟨 Moderate Risk Type II: 🟥 High 🟩 Low 🟨 Moderate Implementation Risk: 🟥 High 🟩 Low 🟨 Moderate

#	Id	Name	Text	▽ Ability To Test - Likelihood	Ability To Test- Consequence	Ability To Test Risk	Confidence In Test - Consequence	Confidence In Test - Likelihood	Confidence In Test Risk	Implementation - Consequence	Implementation - Likelihood	Implementation Risk
1	153	R Target Identification	The EW System shall correctly identify target system not less than 95% of the time with a confidence of or greater than 90%.	5	1	5	5	1	5	1	1	1
2	151	R Cluttered EMI Environment	The B-1 band 8 replacement system shall be able to meet its performance requirements in the presence of high levels of commercial EM transitions as modeled by XX simulation.	3	1	3			0			0
3	154	R Number of Discrete Radar Sources	The EW System shall be able to detect greater than 8 target systems at the same time.	3	3	9	1	3	3	1	1	1
4	156	R Jamming Performance	The EW System shall be able to meet performance requirements in the presents of jamming at the level of X.	3	5	15	1	1	1	1	1	1
5	157	R Operate in Contested Environment	The EW system shall accurately detect, track and jam, active threat radars in a contented environment where threat systems are actively trying to defeat the EW system and degrade its capabilities.	3	3	9	5	3	15	3	3	0
6	152	R Congested Civilian EMI Environment	The B-1 Band 8 replacement system shall meet all its performance requirement in the present of multiple cell phone networks (4 or more), police radios (15 or more transmitters, Civilian radar systems, (6 or more (ATC, weather, or other radars) operating in the same or adjacent frequencies as the Band 8 replacement system.	1	5	5			0			0

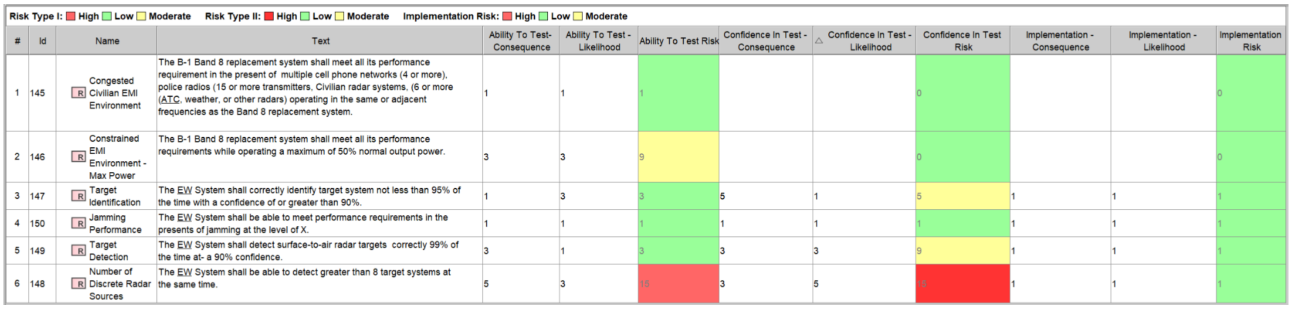
Table 4. Congested Environment Mission-Based Risk Function for the EW Countermeasures System



Risk Type I: 🟥 High 🟩 Low 🟨 Moderate Risk Type II: 🟥 High 🟩 Low 🟨 Moderate Implementation Risk: 🟥 High 🟩 Low 🟨 Moderate

#	Id	Name	Text	Ability To Test - Likelihood	Ability To Test- Consequence	Ability To Test Risk	Confidence In Test - Consequence	Confidence In Test - Likelihood	△ Confidence In Test Risk	Implementation - Consequence	Implementation - Likelihood	Implementation Risk
1	140	R Jamming Performance	The EW System shall be able to meet performance requirements in the presents of jamming at the level of X.	3	3	9	1	1	1	1	1	1
2	141	R Number of Discrete Radar Sources	The EW System shall be able to detect greater than 8 target systems at the same time.	1	3	3	1	3	3	1	1	1
3	143	R Target Detection	The EW System shall detect surface-to-air radar targets correctly 99% of the time at- a 90% confidence.	1	1	1	3	1	3	1	1	1
4	142	R Target Identification	The EW System shall correctly identify target system not less than 95% of the time with a confidence of or greater than 90%.	3	5	15	5	1	5	1	1	1
5	144	R Congested EMI Environment	The EW System shall meet all of the performance requirement in the presence of a high level of red and blue force EM system operating in close proximity of the systems location.	1	3	3	3	3	9	1	1	1

Table 5. Constrained Environment Mission-Based Risk Function for the EW Countermeasures System



Risk Type I: 🟥 High 🟩 Low 🟨 Moderate Risk Type II: 🟥 High 🟩 Low 🟨 Moderate Implementation Risk: 🟥 High 🟩 Low 🟨 Moderate

#	Id	Name	Text	Ability To Test- Consequence	Ability To Test - Likelihood	Ability To Test Risk	Confidence In Test - Consequence	△ Confidence In Test - Likelihood	Confidence In Test Risk	Implementation - Consequence	Implementation - Likelihood	Implementation Risk
1	145	R Congested Civilian EMI Environment	The B-1 Band 8 replacement system shall meet all its performance requirement in the present of multiple cell phone networks (4 or more), police radios (15 or more transmitters, Civilian radar systems, (6 or more (ATC, weather, or other radars) operating in the same or adjacent frequencies as the Band 8 replacement system.	1	1	1			0			0
2	146	R Constrained EMI Environment - Max Power	The B-1 Band 8 replacement system shall meet all its performance requirements while operating a maximum of 50% normal output power.	3	3	9			0			0
3	147	R Target Identification	The EW System shall correctly identify target system not less than 95% of the time with a confidence of or greater than 90%.	1	3	3	5	1	5	1	1	1
4	150	R Jamming Performance	The EW System shall be able to meet performance requirements in the presents of jamming at the level of X.	1	1	1	1	1	1	1	1	1
5	149	R Target Detection	The EW System shall detect surface-to-air radar targets correctly 99% of the time at- a 90% confidence.	3	1	3	3	3	9	1	1	1
6	148	R Number of Discrete Radar Sources	The EW System shall be able to detect greater than 8 target systems at the same time.	5	3	15	3	5	15	1	1	1

Discussion

As many parts of the DoD are moving to SysML-based MBSE and digital engineering to manage their programs, there is significant opportunity to leverage the power of these tools for test and evaluation. The test program for any DoD system is vital to ensure the future performance of the system. However, testing can be very costly and time consuming on projects and may not produce high confidence. Modeling will increase the program and test organizations ability to more effectively plan and manage the test program and to ensure that all data collected on systems during contract or test, developmental test, and operational test is captured and used to its best advantage. The current system level risk approach does not adequately capture test risk or how changes to the test program and the requirements will impact overall system risk. More robust risk analysis will positively impact test planning and acquisition outcomes.

This work has demonstrated that test risk can be effectively modeled within a MBSE model and directly related to requirements and the design of the system. In addition, this work has proposed a risk function that addresses the DoD's need for a risk function that can be focused on modeling directly as a function of mission profile and an operating environment. The development of integrated system modeling to include the full acquisition life cycle, particularly the testing of systems, will be a major advancement in the development of the practice of model-based systems engineering and is critical to the use of MBSE in the acquisition community going forward. Results of this work demonstrate the ability to directly link the program requirements and design directly to the ability to test and test planning and develop risk functions dependent on both the system and the ability to effectively test the system.

In order to get the maximum benefits for the use of MBSE in the development of systems for the DoD we investigated the creation of an advanced risk function to include traditional risk functions (cost, schedule and performance, likelihood, and consequence) as well as linking risk to testing and requirements. In addition, the model-based risk functions were designed as a function of requirements in order to allow for defining specific missions (based on a set of requirements) and looking at the risks as a function of the mission and operation profile (environment and threats) for that defined mission.

Conclusion

The model-based test risk function is a new development that will give the program offices and test organizations better visibility into the critical aspects of program performance during the development and testing life cycle of the program. By expanding the use of model-based systems engineering and digital engineering to include more of the program life cycle, the DoD can gain better visibility into the management of these programs. The use of these digital models also provides the means necessary to better look across portfolios of developmental programs and existing systems for portfolio management, mission and threat analysis, and long-term campaign planning.

The Expansion of MBSE and DE in DoD acquisition to fully include the different aspects of T&E and risk management creates several significant advantages in managing programs and portfolios. Greater knowledge of risk and the data needed to inform decision making all along the acquisition life cycle will allow for the acceleration of DoD programs in a manner consistent with reasonable risk taking and data driven decision making that will result in more rapid fielding the highly capable systems.

References

Dick, J., Hull, E., Jackson, K., Dick, J., Hull, E., & Jackson, K. (2017). Requirements engineering in the problem domain. *Requirements Engineering*, 113–134.

DoD. (2018). *Digital Engineering Strategy*. Office of the Deputy Assistant Secretary of Defense for Systems Engineering.

DOT&E. (2022). *Office of the Director, Operational Test and Evaluation strategy update—Strategic pillars*. FINAL DOTE 2022 Strategy Update 20220613.pdf (osd.mil)

History.com Editors. (2009). *President Eisenhower warns of Military-Industrial Complex*. History.com, A&E Television Networks. https://www.history.com/this-day-inhistory/eisenhower-warns-of-military-industrial-complex

Königs, S. F., Beier, G., Figge, A., & Stark, R. (2012). Traceability in systems engineering–Review of industrial practices, state-of-the-art technologies and new research solutions. *Advanced Engineering Informatics*, *26*(4), 924–940.

Range Operations & Sustainment 96T/XPO. (2021). *96th Test Wing Customer Guide.* https://www.eglin.af.mil/Portals/56/documents/Customer%20Guide%202021.pdf

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net