SPECIAL REPORT FCDD-AMS-24-01

MBSE FOR ASSESSING CYBER SURVIVABILITY: LESSONS LEARNED FROM A DEVELOPMENTAL WEAPON SYSTEM (POSTER)

C. Daniel Colvett
Software, Simulation, Systems Engineering and Integration Directorate
Combat Capabilities Development Command
Aviation & Missile Center

And

Janice F. Dyer, Juliana J. Burge, and Elijah G. Evans
DESE Research Inc.
315 Wynn Drive
Huntsville, Alabama, 35805

February 2024

APPROVED FOR PUBLIC RELEASE

DISCLAIMER

THE FINDINGS IN THIS REPORT ARE NOT TO BE CONSTRUED AS AN OFFICIAL DEPARTMENT OF THE ARMY POSITION UNLESS SO DESIGNATED BY OTHER AUTHORIZED DOCUMENTS.

TRADE NAMES

USE OF TRADE NAMES OR MANUFACTURERS IN THIS REPORT DOES NOT CONSTITUTE AN OFFICIAL ENDORSEMENT OR APPROVAL OF THE USE OF SUCH COMMERCIAL HARDWARE OR SOFTWARE.

REPORT DOCUMENTATION PAGE

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED	
		START DATE	END DATE
February 2024	Poster Presentation (Final)		

4. TITLE AND SUBTITLE
MBSE for Assessing Cyber Survivability: Lessons Learned from a Developmental Weapon System (Poster)

5a. CONTRACT NUMBER	5b. GRANT NUMBER	5c. PROGRAM ELEMENT NUMBER
W9124-P-19-9-0001		
5d. PROJECT NUMBER	**5e. TASK NUMBER**	**5f. WORK UNIT NUMBER**

6. AUTHOR(S)
C. Daniel Colvett, Janice F. Dyer, Juliana J. Burge, and Elijah G. Evans

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Cyber Technologies Integration Division; Software, Simulation, Systems Engineering and Integration Directorate; Aviation and Missile Center; U.S. Army Combat Capabilities Development Command ATTN: FCDD-AMS-UCC Redstone Arsenal, AL 35898-5000	SR-FCDD-AMS-24-01

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
Distribution Statement A: Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
(See next page)

15. SUBJECT TERMS
MBSE, MOSA, MBCRA, Weapon System Assurance, WSA, Criticality Analysis, ACAD, Cyber Survivability, Mission Critical Functions, Digital Engineering, System Security Engineering, Risk Assessment

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT	b. ABSTRACT	C. THIS PAGE		
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAR	

19a. NAME OF RESPONSIBLE PERSON	19b. PHONE NUMBER *(Include area code)*

STANDARD FORM 298 (Rev. 5/2020)
Prescribed by ANSI Std. Z39.18

ABSTRACT

Model Based Systems Engineering (MBSE) is considered an enabler for rapid transition of technology, allowing for agile product development and adaptation to changing operational conditions and system requirements. The U.S. Army is increasingly requiring digital integration between Program Offices and Contractors through MBSE to meet Department of Defense (DoD) demands for modernization and optimization. MBSE is also a crucial element in the Army's strategy for executing the Modular Open System Approach (MOSA) required for major defense acquisition programs. This presentation explores the relationship between MBSE and MOSA as it relates to the ability of warfighting systems to prevent, mitigate, recover from, and adapt to adverse cyber events that could impact mission critical functionality in a multi-domain operations (MDO) environment. The authors argue that the capabilities and outputs of MBSE—both during system development and later life cycle phases—should be harnessed by Programs seeking to meet cyber survivability key performance parameters (KPPs). This presentation presents lessons learned from using real world MBSE artifacts from a developmental weapon system as inputs to an assurance capability for cyber risks to weapon systems during the Technology Maturation & Risk Reduction (TMRR) phase of an aviation platform. Early-phase models supplied by the Government and Contractors contained data allowing the authors to perform a cyber survivability requirements analysis and the initial steps of a Criticality Analysis (CA). Just as executing MBSE does not profoundly change the fundamental systems engineering process, the authors found that the additional use of models does not change the core cybersecurity assessment processes; rather, it enhances analyses by providing operational context and traceability across elements and stakeholders, and allowing for more thorough and actionable analysis at a phase when hardware and software design changes are cost effective and do not interfere with mission execution. Further, the authors foresee potential for MBSE-informed cyber survivability assessment methods to be applied to today's modern battlefield where critical data are shared between enterprise platforms and components.

MBSE for Assessing Cyber Survivability: Lessons Learned from a Developmental Weapon System

BACKGROUND

Model-Based Systems Engineering (MBSE)

- Acquisition programs are adopting Digital Engineering (DE) ecosystems with MBSE at their core
- Models are integrated representations of system requirements, behaviors, structure (physical and logical), properties, and interconnections
- MBSE provides traceability between domains, including cyber security and survivability

Modular Open Systems Approach (MOSA)

- MOSA establishes business objectives and technical practices for weapon systems allowing components to be incrementally added, removed, or replaced
- **MBSE supports DoD goals for MOSA**: rapid innovation, flexibility, interoperability, upgradeability, easier sustainment, resource reduction
- The **system architecture model** is the basis for decomposition on which MOSA relies
- Architectures govern internal and external interfaces for integrated systems
- Reference and enterprise architecture frameworks facilitate standardization and reusable requirements, profiles, models, standards, interfaces, libraries, etc.

Army Cyber Assessments

- DoD calls for conducting **Mission Based Cyber Risk Assessments (MBCRAs)**, with an emphasis on starting *early* and *iterating*
- The **Army Cyber Acquisition Discipline (ACAD)** integrates cyber into planning, design, and acquisition phases to maximize survivability and resiliency
  - Mandates performing the Joint Staff's **Cyber Survivability Endorsement (CSE)** Process
  - Calls for *early* and *continuous* cyber and engineering risk-reduction activities to support **all-domain operations**

Model elements and digital artifacts can support required cyber assessment activities by providing inputs to analyses—and potentially allow assessment findings to be fed back into the model.

MIL-HDBK-539 *Department of Defense Handbook: Digital Engineering and Modeling Practices* provides guidance on MBSE, interrelated MOSA statutory requirements, and cybersecurity analyses

PROJECT & TEAM

- **Customer:** A Project Management Office within one of the Army's six modernization priorities
- **Goal:** Help program meet *cyber survivability* key performance parameters (KPPs)
- **Objective:** Analyze MBSE artifacts during the Technology Maturation & Risk Reduction (TMRR) phase
- **Method:** Early-phase Weapon System Assurance (WSA) (customized MBCRA activities)
- **Requirement/Guidance:** Army Cyber Acquisition Discipline (ACAD)
- **Personnel:** DEVCOM AvMC cyber risk analysts (<u>not</u> modelers)
- **Inputs:** (1) Government Furnished Information (GFI) models for the enterprise architecture framework & platform, (2) Early-phase models produced by Performers

RESULTS

Requirements Analysis

The GFI models included system specifications and Program requirements for cyber, allowing for a **security engineering assessment of requirements** (ACAD-required task)

- Security Controls library for Family of Systems (FoS)
- Cyber-relevant System Performance Specifications (SPS)
- Airworthiness Qualification Plan (AQP) deliverables (cyber-relevant reports/plans, including Risk Management Framework (RMF) artifacts)
- Cyber Security Analysis Specifications (23 assessments/analyses total)
- Design Constraints (i.e., platform architecture/modeling requirements) for:
  1. Cyber components/part types
  2. Security properties of components
  3. Cyber survivability and security attributes of data flows
  4. Applicable NIST 800-53 controls (baseline and overlays) identified by GFI
  5. Applicable Cyber Survivability Attributes (CSAs) and Lower-Level Requirements (LLRs) identified by GFI
  6. Cybersecurity analysis specifications/activities and reports

Fig 1. Snippets of GFI Containment Tree showing packages containing requirements for the system and the model

The requirements alone are not enough to determine whether a resultant system will be "cyber survivable"—that is highly dependent on a Performer's ability to *understand* the requirements and implement them *appropriately*.

Criticality Analysis (CA)

CA is an ACAD-required task and key to successful execution of MBCRA. Involves end-to-end functional decomposition and identification of components critical to system mission (CCs). **Data found in both the GFI and Performer models contributed to an *initial* CA.** Outputs included:

- Mission Statement + 4 operational activity missions
- 5 high-level Mission Critical Functions (MCFs)
- ~50 *logical* subsystems mapped to one or more MCFs

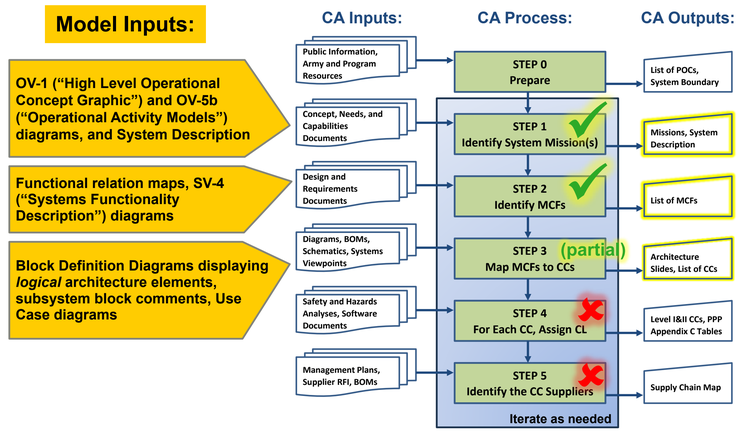

Fig 2. TMRR phase model inputs to an initial CA allowed for completion of Steps 1 and 2, and *partial* completion of Step 3

CHALLENGES & OPPORTUNITIES

CHALLENGE	OPPORTUNITY
01 DE Environment Access and Resources Logistical challenges obtaining access to models; missing model dependencies; lack of understanding of how framework, enterprise, and system models "fit" together	**01** Instructions for obtaining and opening models, briefings on models and stakeholder expectations, availability of MBSE subject matter experts (SMEs)
02 Difficulty Navigating and Understanding Models as Non-MBSE SMEs Steep learning curve understanding what models conveyed and how to navigate and interpret them	**02** Tailored training on three pillars of MBSE (modeling language, modeling tool, and modeling method)
03 Variances in Performer Approaches to Model Structure Inconsistencies in structural organization of model (e.g., containment tree) and in levels of detail and relationships between diagrams	**03** Collaborate with modelers and requirements authors to develop methods and metrics to systematically navigate and evaluate models
04 Logical versus Physical Early-phase logical representations of the system do not supply data typically used in MBCRA activities	**04** MBCRA practitioners capitalize on MBSE as an *operational* enabler; identify ways to affect engineering decisions earlier

CONCLUSION

- **Inputs to and context for MBCRA activities** can be found in logical architecture diagrams, requirements models, and interdependency and traceability features
- **Contextualized understanding** of missions, threats, and critical components and functions helps:
  - Focus resources (cyber and engineering)
  - Define cyber assessment objectives
  - Save time, money, and technical expertise
- Push for open systems architectures and standardized comprehensive infrastructures creates opportunities and inputs for **early, iterative, and frequent cyber analysis**
- While *early-phase* models present **limitations to the way cyber is traditionally assessed** (e.g., threat modeling, attack path analysis, controls verification), potential exists for MOSA-oriented architecture framework models and model elements to be used to **conduct threat analyses and cyber assessments at the Multi-Domain Operations (MDO) level**

FOR FURTHER INFORMATION:
U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND AVIATION & MISSILE CENTER:
AvMC.ARMY.MIL

POINT OF CONTACT:
Dr. Daniel Colvett
usarmy.redstone.devcom-avmc.mbx.wsa@army.mil

U.S. ARMY