



WRT-1043
DAU DIGITAL
ENGINEERING
SIMULATION

Principal Investigator:

Dr. Nicole Hutchison, Stevens Institute of Technology

Co-Principal Investigators:

Dr. Dinesh Verma, Stevens Institute of Technology

Dr. Peter Beling, Virginia Tech

May 26, 2023

Sponsor: Defense Acquisition University (DAU)



The Networked National Resource to further
systems research and its impact on issues
of national and global significance

DISCLAIMER

Copyright © 2023 Stevens Institute of Technology, Systems Engineering Research Center

The Systems Engineering Research Center (SERC) is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology.

This material is based upon work supported, in whole or in part, by the U.S. Department of Defense through the Office of the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)) under Contract [HQ0034-19-D-0003, TO#0179].

Any views, opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense nor ASD(R&E).

No Warranty.

This Stevens Institute of Technology and Systems Engineering Research Center Material is furnished on an “as-is” basis. Stevens Institute of Technology makes no warranties of any kind, either expressed or implied, as to any matter including, but not limited to, warranty of fitness for purpose or merchantability, exclusivity, or results obtained from use of the material. Stevens Institute of Technology does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

This material has been approved for public release and unlimited distribution.

RESEARCH TEAM

Name	Organization	Labor Category
Nicole Hutchison	Stevens	Principal Investigator
Dinesh Verma	Stevens	Co-Principal Investigator
Peter Beling	Virginia Tech	Co-Principal Investigator
Craig Arndt	GTRI	Subject Matter Expert (SME)
David Long	Stevens	Subject Matter Expert (SME)
Philomena Zimmerman	Stevens	Subject Matter Expert (SME)
Tom McDermott	Stevens	Senior Research Associate
Molly Nadolski	Stevens	Research Associate
Tim Sherburne	Virginia Tech	Research Associate
Hoong Yan See Tao	Stevens	Research Project Manager
Paul Wach	Virginia Tech	Research Assistant Professor
Megan M. Clifford	Stevens	Research Associate
Dalton Clark	GTRI	MBSE Research Engineer
Geoff Kerr	Virginia Tech	Senior Research Associate

TABLE OF CONTENTS

DISCLAIMER.....	II
RESEARCH TEAM.....	II
TABLE OF CONTENTS.....	III
LIST OF FIGURES AND TABLES.....	IV
EXECUTIVE SUMMARY	V
1. INTRODUCTION.....	1
1.1 WHAT IS DIGITAL TRANSFORMATION?	1
1.2 CHALLENGES	3
1.3 TASKING.....	3
1.4 REPORT STRUCTURE.....	4
1. DEVELOPING THE CURRICULUM.....	5
2.1 DIGITAL ENGINEERING INTERMEDIATE CREDENTIAL.....	5
2.1.1 ENG 5510 – SysML	5
2.1.2 ENG 5520 – Model-Based Systems Engineering (MBSE).....	6
2.1.3 ENG 5530 – Digital Enterprise Ecosystem.....	7
2.2 SUPPORT ARTIFACTS FOR DE COURSEWARE AND MODULES	9
2.2.1 Firebird, Bulldog, and Firedog.....	9
2.2.2 Mission Engineering & Digital Engineering.....	15
2.2.3 Digital Environment and Ecosystem	16
2.2.4 Digital Systems Engineering Plan (dSEP).....	18
2.3 STEDE & TRACING INTERRELATIONSHIPS.....	22
2.4 SCRE.....	26
2.4.1 Silverfish with SysML SCRE.....	27
2. REVIEW AND FEEDBACK.....	30
3.1 DAU FACULTY REVIEWS.....	30
3.2 DIGITAL ENGINEERING ADVISORY BOARD REVIEWS.....	30
3.3 PUBLIC PRESENTATIONS.....	31
3. FUTURE WORK & CONSIDERATIONS.....	32
APPENDIX A: PUBLICATIONS AND PRESENTATIONS RESULTING FROM RESEARCH	34
APPENDIX B: CITED AND RELATED REFERENCES	35
APPENDIX C: DESCRIPTION OF ANCILLARY MATERIALS	36
APPENDIX D: OVERVIEW OF SCRE.....	38
D.1 DEVELOPMENT AND DEPLOYMENT OF SCRE	38
D.1.1 Cybersecurity and Cyber Resilience.....	38
D.1.2 SCRE Structure	39
D.1.3 Deploying the Credential	42
D.1.4 Digital Engineering in SCRE.....	42
D.2 OVERVIEW OF SCRE CREDENTIAL	43
D.2.1 Competencies/TLO/ELOs.....	45

D.2.2	CYB 5610.....	46
D.2.3	CYB 5610 Modules	48
D.3.3	CYB 5620	49
D.3.3.1	Supporting SERC Models and Efforts	53
D.3.4	CYB56XX.....	53
D.3.5	TRACEABILITY THROUGH MODULES, KNOWLEDGE REVIEW AND EXAM QUESTIONS, AND STORYBOARDS/MODELS	54
D.3.6	SCORE FUTURE DIRECTIONS AND NEEDS	54

LIST OF FIGURES AND TABLES

FIGURE 1.	MODEL-BASED OV-1 FOR THE FIREDOG MISSION	10
FIGURE 2.	FIREDOG MISSION THREAD (SEQUENCE DIAGRAM).....	10
FIGURE 3.	TRADITIONAL OV-1 FOR FIREDOG MISSION WITH NOTED MISSING CURRENT CAPABILITY FOR COMMUNICATION BETWEEN THE UAV (FIREBIRD) AND UGV (BULLDOG)	11
FIGURE 4.	INTERCONNECTIONS BETWEEN THE REQUIRED SYSTEM MODELS FOR FIREDOG PROGRAM	11
FIGURE 5.	GENERIC REPRESENTATION OF CONTINUOUS MODEL EVOLUTION.....	12
FIGURE 6.	LOW-FIDELITY MODEL OF THE COMMUNICATION BETWEEN FIREBIRD AND BULLDOG WITHIN THE CONTEXT OF THE FIREDOG MISSION	13
FIGURE 7.	VISUALIZATION OF THE FIREDOG V&V THREAD FOR LINK BUDGET ANALYSIS AGAINST THE REQUIREMENTS.....	14
FIGURE 8.	FIREBIRD-BASED TRACEABILITY FOR SATISFACTION AND ALLOCATION OF REQUIREMENTS	14
FIGURE 9.	EXPECTED EVOLUTION OF BULLDOG TO INCLUDE PLM AND PHYSICS-BASED SIMULATION	15
FIGURE 10.	CONCEPTUALIZATION OF THE CONTEXT AND RELATIONSHIPS FOR A DIGITAL ENVIRONMENT AND ECOSYSTEM.	16
FIGURE 11.	OV-1 FOR A NOTIONAL DIGITAL ENGINEERING ENVIRONMENT (DEE).....	17
FIGURE 12.	OVERVIEW OF SKYZER-BASED DIGITALIZATION OF THE SEP.....	19
FIGURE 13.	VISUALIZATION OF GENERIC SEPV4 DIGITIZATION AND DIGITALIZATION PLUS SPECIFIC EXAMPLE CONTENT FROM BULLDOG.21	
FIGURE 14.	STEDE CONTEXT	22
FIGURE 15.	CREDENTIAL META-MODEL.....	23
FIGURE 16.	COMPETENCY META-MODEL	24
FIGURE 17.	TAXONOMY META-MODEL	25
FIGURE 18.	STEDE DB IMPLEMENTATION OVERVIEW.....	26
FIGURE 19.	STEDE DB REPORT GENERATION EXAMPLE	26
FIGURE 20.	SECURE CYBER RESILIENCE ENGINEERING (SCORE) SysML META-MODEL.....	28
FIGURE 21.	CYBER RESILIENCE REQUIREMENTS METHODOLOGY	29
FIGURE 22.	THE DEVELOPMENT OF THE SCORE INITIATIVE.....	39
FIGURE 23.	BUILDING BLOCKS OF SCORE	40
FIGURE 24.	BREAKOUT OF LEVELS FOR SCORE CREDENTIALS	42
FIGURE 25.	SCORE TOOLBOX CONCEPT	45
FIGURE 26.	SCORE COMPETENCIES	45
FIGURE 27.	SNAPSHOT OF TRACED COMPETENCIES, TLOs, ELOs, AND DERIVED ELOs TO MATERIALS	46
FIGURE 28.	SNAPSHOT EXAMPLE OF BUILT STORYBOARD FOR CYB 5610	49
FIGURE 29.	STORYBOARDS FOR SCORE, CYB 5610 AND 5620	53

EXECUTIVE SUMMARY

Digital transformation is fundamentally changing the way acquisition and engineering are performed across a wide range of government agencies, industries, and academia. Digital transformation is characterized by the integration of digital technology into all areas of an organization, fundamentally changing operations and how results are delivered. It necessitates cultural change centered on alignment across leadership, strategy, customers, operators, developers, and designers.

The DoD acquisition workforce needs training to support their transition from current/traditional acquisition practices to digital engineering/acquisition. This report reflects the first option year (OY1) activities for the WRT-1043 SERC research task. The purpose of WRT-1043 is to provide support to the Defense Acquisition University (DAU) in developing new credentials to support the DoD acquisition workforce as it faces the challenges of digital transformation. In particular, the task supports the development of two new credentials in digital engineering (DE) and secure cyber resilient engineering (SCRE).

The DE credential consists of six courses that will give students the ability to generally function in a digital environment. This is the “intermediate” credential that will be relevant to almost all defense acquisition roles. DAU plans a future “advanced” credential that will be more targeted at modelers, engineers, and deeper analysts. For the intermediate credential, the six courses identified include:

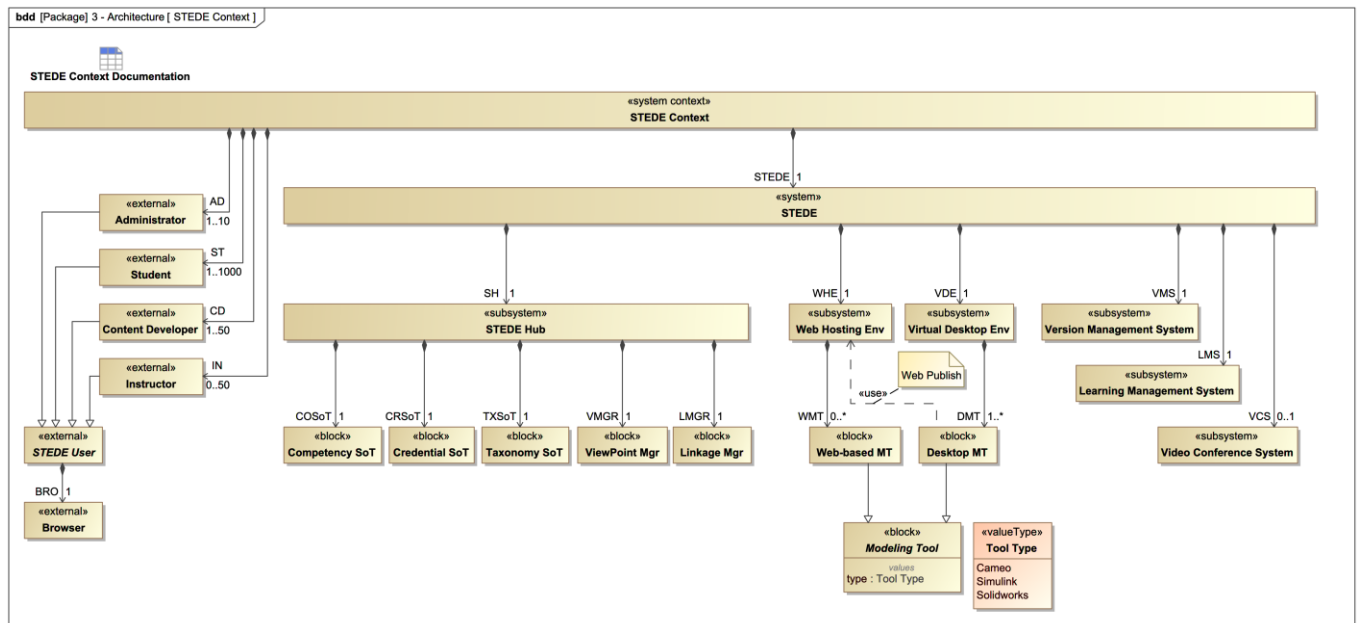
- Systems Modeling Language (SysML) – ENG 5510
- Model-Based Systems Engineering (MBSE) – ENG 5520
- Digital Enterprise Ecosystem – notionally ENG 5530
- Digital Engineering Technical Processes – notionally ENG 5540
- Digital Engineering Management Processes – notionally ENG 5550
- Digital Engineering Capstone – notionally ENG 5560

In OY1, the team supported the faculty teams developing ENG 5510 and 5520 and the team took the lead development role for ENG 5530. The following subsections detail these efforts. Once the full intermediate DE credential is launched, DAU has plans to develop an “advanced” credential for DE.

For the SCRE credential, the SERC team supported DAU on the development of three courses to address the needs of the workforce at the novice, beginner, and practitioner levels. These three courses will be folded into an introductory SCRE credential (level 1) and a practitioner SCRE credential (level 2), which will also encompass currently taught courses such as the Cyber Training Range. In the first course (CYB 5610), students will walk through models that adequately explain why SCRE is needed via an online-only training course. In the second course (CYB 5620), students will interact with and be led by an instructor through the models to better understand when and where throughout the lifecycle and phases. In the third course (CYB 56XX), students will actively work in the models themselves, but with an instructor able to help when needed.

In addition to the development of course materials, the team completed substantial modeling efforts in OY1. Models delivered to DAU as part of this task included:

- Firebird Model Updates (Firebird is based on the AFIT case study)
- Bulldog Draft Model (modeled based on a document-based DAU example)
- Firedog Draft Model (notional communication link between Firebird and Bulldog)
- A generic model of the DE environment
- Silverfish Model using SCRE meta-model profiles (utilized for the SCRE credential)
- Simulation Training Environment for Digital Engineering (STEDE) models and demonstration implementation (see figure below).



Overall, the team supported the development of six DAU courses across the DE and SCRE credentials, developed several models to support this training, and helped DAU think through the options for enabling students to be able to work directly with models in OY1.

In the upcoming option year 2 (OY2), the priorities will be to continue to develop courses for these credentials as well as to perform additional modeling to support these courses.

1. INTRODUCTION

Digital transformation is fundamentally changing the way acquisition and engineering are performed across a wide range of government agencies, industries, and academia. Digital transformation is characterized by the integration of digital technology into all areas of an organization, fundamentally changing operations and how results are delivered. It necessitates cultural change centered on alignment across leadership, strategy, customers, operators, developers, and designers.

In the U.S. Department of Defense (DoD), evidence across the Services and industry has affirmed digital transformation is critical for successful acquisition in an environment of increasing global challenges, dynamic threats, rapidly evolving technologies, and increasing life expectancy of systems currently in operation (Zimmerman et al., 2019). The DoD must continue to practice systems engineering efficiently and effectively to provide the best advantage for successful acquisitions and sustainment. Digital transformation will require the update of both acquisition and systems engineering practices to take full advantage of the digital power of computation, visualization, and communication throughout the lifecycle.

To meet the challenges and realize the benefits of digital transformation, the acquisition workforce must undergo significant transformation (U.S. DoD Digital Engineering Strategy 2018, Goal 5). This need stems from the growing use of digital engineering to represent complex systems throughout their lifecycle. Engineers, and perhaps in particular systems engineers, must be able to create, evaluate, and use digital engineering methods to specify, evaluate, and manage systems throughout the DoD acquisition process.

But this is no longer the realm of “engineers only.” As systems engineering and acquisition evolve, every individual who works within a digital environment needs digital literacy – the foundations required to interact with digital systems. Anyone who works in acquisition will have to navigate models, find information critical to their roles in models and the underpinning data, and make decisions based on this information.

This will not be an easy transition for the DoD acquisition workforce. A major shift in the way acquisitions is performed is needed. In addition to new processes, methods, and approaches and the need to build new skills, a major cultural shift will have to take place for the workforce to meet the challenges and realize the benefits of digital transformation.

1.1 WHAT IS DIGITAL TRANSFORMATION?

In the DoD, digital transformation is the transition from traditional acquisition and engineering approaches, which are heavily document- and event-driven, to an iterative, model-based, and data-driven approach that improves transparency and integration and allows improvements in existing processes. Full digital transformation requires both *digitization* and *digitalization*. **Digitization** is generally the easier of the two to tackle. When moving from a physically-printed document as the baseline to a PDF, that is a simple example of digitization: moving something in its existing form into a digital space. **Digitalization** is the adaptation of processes, methods, and approaches to better leverage computing technology for the capture, communication, visualization, and analysis of information (data). Digitalization does

not require that existing processes and artifacts be translated into an electronic environment, but rather that these be reviewed to determine where they can and should be updated to improve effectiveness, efficiency, and transparency in a digital environment. It is only with thoughtful consideration of both aspects that any organization can achieve true digital transformation.

Digital transformation in the Department requires an overhaul of two main elements: engineering and acquisition. In 2018, the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) published a *Digital Engineering Strategy*. This outlines the vision for digital engineering (DE) and five goals of the transition to a digitally based engineering and acquisition approach (U.S. DoD, 2018). DoD defines **digital engineering** as “an integrated digital approach that uses authoritative sources of system data and models as a continuum across disciplines to support lifecycle activities from concept through disposal” (U.S. DoD, 2018).

As the DoD transitions to digital engineering, the acquisition workforce must become literate in model-based and data-driven approaches; competent in digital models, methods, and tools; and competent with digital artifacts across the acquisition lifecycle. This is significant, as digital transformation and engineering impacts how the acquisition workforce will perform their job functions; the underlying data they will need, together with the data they will transform or generate; the digital artifacts that they will deliver; and their interaction and sharing of information across functional boundaries.

For the DoD to meet its vision as set out in the *Digital Engineering Strategy* (2018), the Department must embrace true digital transformation. It cannot simply continue to utilize the same document-based requirements and monolithic reviews with some model-based underpinnings. There must be thoughtful transformation of the existing processes to take advantage of what is possible in the digital space (digitalization). At the same time, not everything can be perfectly optimized to take advantage of digital capabilities, especially in the near term.

The research team has seen several examples of this already during the project. One of the most illustrative of these was a lack of trust in the ability to change one aspect of a model and have those changes flow throughout the rest of the model. This has long been touted as a benefit of model-based systems engineering (MBSE) – but in an acquisition context, this approach goes against many of the controls set in place. “But where is the configuration control board?” is a comment often heard when introducing traditional acquisition personnel to change management in DE. True digital transformation does not put a configuration control board, run exactly as it is done today, into a digital environment nor does it do away with configuration control entirely. Instead, it requires a considered blending of the two to optimize as far as is reasonable to maintain the rigor and control required – and no more.

One example of this was seen in previous work at the SERC with the Naval Air Systems Command (NAVAIR) on digital signoff (Blackburn et al., 2021). The ability to conduct reviews in a model and signoff elements as they are available and ready is a fundamental change from current Milestone review process (think preliminary or critical design reviews). The intent of Milestone A, B, and C reviews is to ensure that the system is meeting the quality and capabilities needed – that as planned, it should meet or exceed stakeholder requirements.

Digital transformation will embrace this approach but find ways to make it more efficient – and perhaps enable better utilization of techniques like agile and DevSecOps along the way.

The idea that this sort of validation and verification can happen throughout the lifecycle, literally allowing updates and approvals on a daily basis, is a paradigm shift for the majority of the DoD acquisition workforce. This is why a complex, realistic “case study” that allows acquisition personnel to experience these issues in a realistic simulated training environment will be beneficial to the workforce.

1.2 CHALLENGES

The DoD Acquisition System has long been based on documentation and stringent processes. During World War II, the DoD became the technological leader of the world, driving research, invention, innovation, and improvement across a variety of technologies. This leadership persisted for several decades. Today, the DoD plans for needed capabilities made of complex systems of systems (SoS), but as the complexity has increased and as technology development has become dominated by the commercial sector, the ability of the DoD to rapidly develop, acquire, and field defense capabilities has been dramatically reduced.

Historically, the acquisition system has been heavily invested in the “waterfall” or “v-model” methodology. This is a largely sequential approach to developing systems or capabilities—starting with high-level needs and requirements, then developing systems, testing and validating them, and finally delivering them. This is a logical approach, but tends to be overly methodical, bureaucratic, and slow. Data from 1997–2015 illustrates that the time for major defense acquisition programs to reach initial operational capability (IOC) from formal program initiation (Milestone B or C) has been about 7 years on average (OUSD(AT&L), 2016). As other countries accelerate the pace of their acquisitions, the United States needs the ability to more rapidly deliver critical initial capabilities and continue their refinement and augmentation.

1.3 TASKING

The DoD acquisition workforce needs training to support their transition from current/traditional acquisition practices to digital engineering/acquisition. This report reflects the first option year (OY1) activities for the WRT-1043 SERC research task. The purpose of WRT-1043 is to provide support to the Defense Acquisition University (DAU) in developing new credentials to support the DoD acquisition workforce as it faces the challenges of digital transformation. In particular, the task supports the development of two new credentials in digital engineering (DE) and secure cyber resilient engineering (SCRE). (See section 2, below.)

The original tasking for OY1 focused on the development of a training environment to support hands-on model navigation and manipulation by DAU students (see 2.2 Support Artifacts for DE Courseware and Modules). Over the period of performance, the focus shifted to primary support of the credentials, including the development of course content (section 2).

1.4 REPORT STRUCTURE

This report includes the following sections:

- **Developing the Curriculum** provides insight into the primary work conducted for this option year (OY1). It outlines the credentials supported, describes the research team's actions and results, and lays out the modeling work done in support of the credentials.
- **Technical Reviews** provides insight into the main review and feedback mechanisms used by the team, primarily DAU faculty reviews and reviews by the Advisory Board of subject matter experts (SMEs) created to support this task.
- **Future Directions** provides insights into the work for option year 2 (OY2) as currently planned.

Appendices A and B provide the publications generated from this research task and the works cited in this report, respectively.

In addition to the formal technical report (this document), the team is also providing ancillary materials, as outlined in Appendix C. Note that some ancillary materials were previously provided to the Sponsor via GitHub, DAU Teams, etc. However, versions of these materials are formally submitted along with this report as outlined in Appendix C.

Appendix D contains a detailed report on the SCRE credential development work.

1. DEVELOPING THE CURRICULUM

The primary focus of OY1 activities for WRT-1043 was support to DAU for the development of curriculum across two credentials: digital engineering (DE) and secure cyber resilient engineering (SCRE). This section provides an overview of the activities, while any content generated to support the courses can be found in the ancillary materials. Both of these credentials fall under the engineering and technical management (ETM) functional area for DAU. Each credential utilizes models to support student learning. The way the models are used within the courses is outlined in this section, as are the details about the models themselves, and the concept and modeling work for the Simulation Training Environment for Digital Engineering (STEDE).

2.1 DIGITAL ENGINEERING INTERMEDIATE CREDENTIAL

The DE credential consists of six courses that will give students the ability to generally function in a digital environment. This is the “intermediate” credential that will be relevant to almost all defense acquisition roles. DAU plans a future “advanced” credential that will be more targeted at modelers, engineers, and deeper analysts.

For the intermediate credential, the six courses identified include:

- Systems Modeling Language (SysML) – ENG 5510
- Model-Based Systems Engineering (MBSE) – ENG 5520
- Digital Enterprise Ecosystem – notionally ENG 5530
- Digital Engineering Technical Processes – notionally ENG 5540
- Digital Engineering Management Processes – notionally ENG 5550
- Digital Engineering Capstone – notionally ENG 5560

In OY1, the team supported the faculty teams developing ENG 5510 and 5520 and the team took the lead development role for ENG 5530. The following subsections detail these efforts. Once the full intermediate DE credential is launched, DAU has plans to develop an “advanced” credential for DE.

2.1.1 ENG 5510 – SysML

The team supported development of ENG 5510 in the following ways:

- Development of materials for the Block Definition Diagram (BDD) and the Internal Block Diagram (IBD) modules.
- Review of the Terminal and Enabling Learning Objectives (TLOs/ELOs) for the asset.
- Review of the initial script.
- Review of the storyboards as developed.

For both the BDD and IBD modules, the team coordinated with a faculty member to generate the materials for the script. These materials were then used by the instructional systems designer (ISD) to generate the storyboards. Team members also attended the weekly faculty meetings for ENG 5510 to provide feedback and insight based on other SERC-related tasks.

The materials developed can be found in Ancillary Materials SERC-2023-TR-007-A and SERC-2023-TR-007-B.

2.1.2 ENG 5520 – MODEL-BASED SYSTEMS ENGINEERING (MBSE)

The team supported the development of ENG 5520 in the following ways:

- Review of TLOs/ELOs for the asset.
- Review of the initial script.
- Review of storyboards as developed.
- Addition of materials to Module 4 (Model Validation and Quality).
- Creation of materials for Module 5 (Model-Based Metrics) including:
 - Script
 - Storyboards
 - Exercises
 - Models to support student exercises based on Firebird¹.

Team members also attended the weekly faculty meetings for 5520 to provide feedback and insight based on other SERC-related tasks.

The team was asked to develop module 5 (Model-Based Metrics) responding to the allocated TLOs/ELOs. The team identified three primary resources to ground the material in this module: *Practical Software and Systems Measurement Digital Engineering Measurement Framework* (June 2022), the SERC *Digital Engineering Metrics* report (June 2020), and the Digital Engineering Body of Knowledge (DEBoK). The resulting module introduces the what and why of model-based metrics, illustrates the translation of traditional metrics to a model-based environment, highlights additional metrics available through a model-based approach, and specifically addresses the critical topic of tracking technical performance measures.

To illustrate the fundamental concepts, the existing Firebird model was leveraged to the degree possible. Where necessary, the model was extended to support two exercises:

- **Requirements Traceability.** Sufficient requirements traceability was incorporated into the Firebird model to illustrate the satisfaction of requirements in a SysML model. The exercise introduces a simple SysML diagram to illustrate the model concepts for requirement traceability, shows a larger set of requirements using derived matrix views, and then expands to show that manual inspection is

¹Firebird is a model set developed by the Air Force Institute of Technology (AFIT). The main focus for ETM 5510 and 5520 is Firebird Virtual Vision (a subsystem). However, the SERC team also utilized requirements from the broader Firebird system to support some of the analysis activities.

impractical and error prone at scale. Custom reports leveraging the Cameo metrics modules were developed to generate a simple table showing current requirement satisfaction.

- **Architecture Completeness.** The Firebird model was extended to illustrate the growth in the number of activities as the program moves from initial functional requirements to use cases and activity diagrams as part of the systems engineering progression. Similar to the requirements traceability exercise, the student is progressively walked through a series of diagram views illustrating the base concept in a SysML model, a matrix view showing the allocation status of a subset of activities, and then an automated report to generate the current allocation metrics for the Firebird model.

The materials developed can be found in Ancillary Materials SERC-2023-TR-007-A, SERC-2023-TR-007-B, and SERC-2023-TR-007-C.

2.1.3 ENG 5530 – DIGITAL ENTERPRISE ECOSYSTEM

For the “Digital Enterprise Ecosystem” course, the SERC team was given the opportunity to develop materials from the beginning. The primary activities completed included:

- Creating Terminal and Enabling Learning Objectives (TLOs/ELOs).
- Creating an initial, comprehensive knowledge assessment bank to meet the TLOs/ELOs.
- Creating the initial module outline.
- Gathering feedback from the Advisory Board on the planned outline and responding to this feedback.
- Developing content for each module.
- Developing student exercises.
- Developing knowledge checks/assessment questions.
- Developing models to support the course.
- Briefing the 5530 materials to DAU faculty and the Advisory Board as it was developed and incorporating feedback (see Section 3, below).

The team was asked to take the Performance Outcomes (POs) provided to DAU by OSD and develop a set of TLOs/ELOs – outlining the knowledge and skills a student must develop or acquire in order to satisfy the POs. These went through iteration with DAU faculty. The team also developed an initial question bank intended to support assessment of the ELOs. (The POs, TLOs, and ELOs are found within the scripts and slide decks for 5530, found in SERC-2023-TR-007-A and SERC-2023-TR-007-B.)

In January 2023, the team was directed to refocus efforts to develop materials for 5530. Following an iterative process, the team developed a refined outline for the asset, an annotated outline, slide decks, and scripts. In February 2023 the team was asked to incorporate experiential Cameo learning as part of the course development. Starting in March

2023, the team delivered materials to DAU weekly and any feedback received from DAU was incorporated into the materials as they matured.

The curriculum for 5530 is currently broken into five modules (though these may be further divided once the team begins working with an ISD):

- **Module 1 – Introduction to the Digital Enterprise Environment.** This module introduces students to core terminology (infrastructure, environment, ecosystem, and enterprise), puts these concepts in the context of digital engineering and systems engineering more broadly, and introduces students to sample systems they will use in their exercises.
- **Module 2 – Understanding Models in the Context of Digital Engineering.** This module builds on the foundations of SysML and MBSE from previous courses and helps the students understand different types of models spanning multiple engineering domains, appreciate when and where those models are likely to be encountered, and begin to explore how the digital environment can support acquisition.
- **Module 3 – Applying Models and Data across the Acquisition Lifecycle.** This module illustrates different lifecycle models and walks students through examples of what they are used to seeing – generally, document-based artifacts – with examples of what these artifacts can transform into in a digitally-based approach. This includes an example of using continuous digital signoff instead of focusing on major milestone reviews.
- **Module 4 – Scoping the Digital Engineering Environment.** Once the students have seen models in action, this module takes a step back and introduces students to the data underpinnings of models and the role that data plays in a digital environment as well as critical considerations for data management and governance. Concepts to this point are then applied to designing the digital environment and the data needed to support it.
- **Module 5 – Controlling a Digital Environment and the Associated Policy, Standards, and Procedures.** This module expands the aperture from the “environment” to the broader ecosystem and enterprise, taking into account the bigger context of organization, policy, workforce, etc. This includes helping the students build familiarity with the key decisions for the digital ecosystem and giving them opportunities to make some of these decisions in a simulated environment.

The team was instructed to create ENG 5530 in a way that includes students engaging and interacting directly with models, rather than simply showing screen captures of models. In this case, DAU will be using Cameo and students will likely access Cameo using virtual desktops in the DAU Teams-based Digital Acquisition Learning Lab (DALL).

The exercises for 5530 involved the creation of new models, namely Bulldog and Firedog. Bulldog is based on a system used in the DAU Systems Engineering curriculum (SYS 202). To date, this had been a document-based exercise.

In the DE credential, the capstone project is intended to focus on Bulldog and the students will have been exposed to Firebird in ENG 5510 and 5520. Therefore, for ENG 5530, the team developed operational scenarios (“vignettes”) that outline the need to create a linkage between the two existing systems of Firebird and Bulldog, notionally named “Firedog” giving

the students a realistic feel for how models might be used to enhance mission level capability. The team developed initial models of Bulldog as well as models for Firedog. (These are described in more detail in Section 2.3).

The materials for ENG 5530 have been delivered incrementally in 2023, but the final versions are also being delivered concurrently with this report in SERC-2023-TR-007-A, SERC-2023-TR-007-B, SERC-2023-TR-007-C, and SERC-2023-TR-007-D.

2.2 SUPPORT ARTIFACTS FOR DE COURSEWARE AND MODULES

The team has developed a number of artifacts that support the execution of courseware and modules, namely:

1. Bulldog / Firebird / Firedog
2. Digital Systems Engineering Plan (dSEP)
3. Mission Engineering and DE
4. Digital Environment
5. Simulation Training Environment Digital Engineering

This section will walk through the development of each item and provide references to where the artifacts themselves can be found.

2.2.1 FIREBIRD, BULLDOG, AND FIREDOG

The team has developed a SoS context for exemplar systems (“case studies”) to support DAU’s DE credential. The SoS consists of three systems:

- Firebird – a UAV system based on the AFIT Firebird models
- Bulldog – a UGV system based on an existing document-based DAU exercise
- Firedog – a mission that requires engineering a communication link that allows data exchange between Firebird and Bulldog.

Accomplishments for this year include:

- Initialized digitization of Bulldog (text-based to model-based conversion)
- Updated Firebird model to include traceability and model completeness assessment (specific to 5520)
- Digitalized the Firedog mission model, initialized the interconnections to Bulldog and Firebird, modeled the Firedog DEE, and created a data continuum for varying fidelity of analytical models
- Modeled a generic DEE

The Firedog mission is characterized in Figure 1 as a model-based OV-1. This is a generic concept, independent of the selection of systems used to complete the mission.

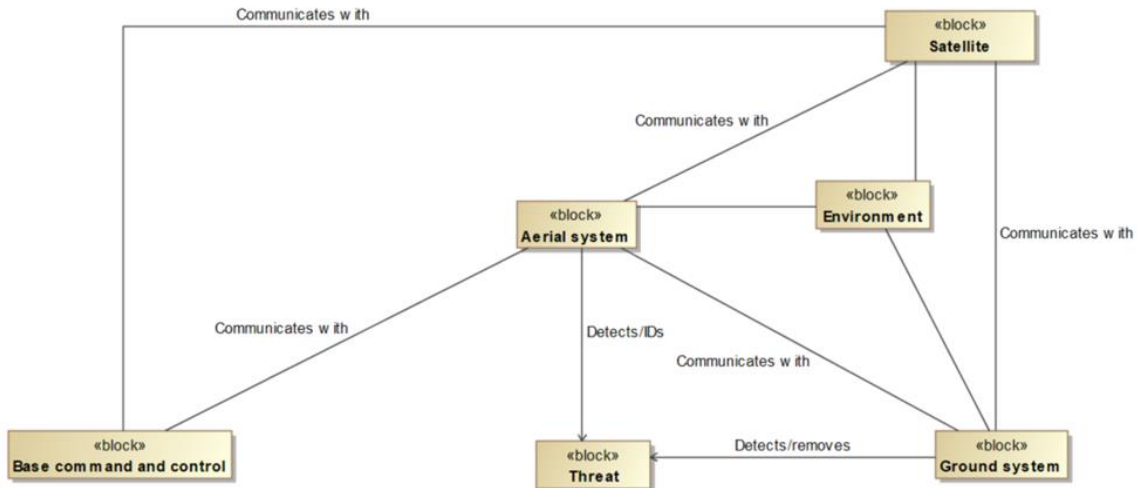


Figure 1. Model-based OV-1 for the Firedog Mission

A model-based mission thread, again independent of the selection of systems, is characterized in Figure 2. In the mission thread, (1) the command-and-control element provides tasking to the UAV, (2) the UAV surveils and detects threats, (3) the UAV notifies and tasks the UGV of a threat, (4) the UGV traverses a terrain and neutralizes the threat, (5) the UGV notifies the UAV of threat neutralization, and (6) the UAV notifies the command-and-control element of threat neutralization.

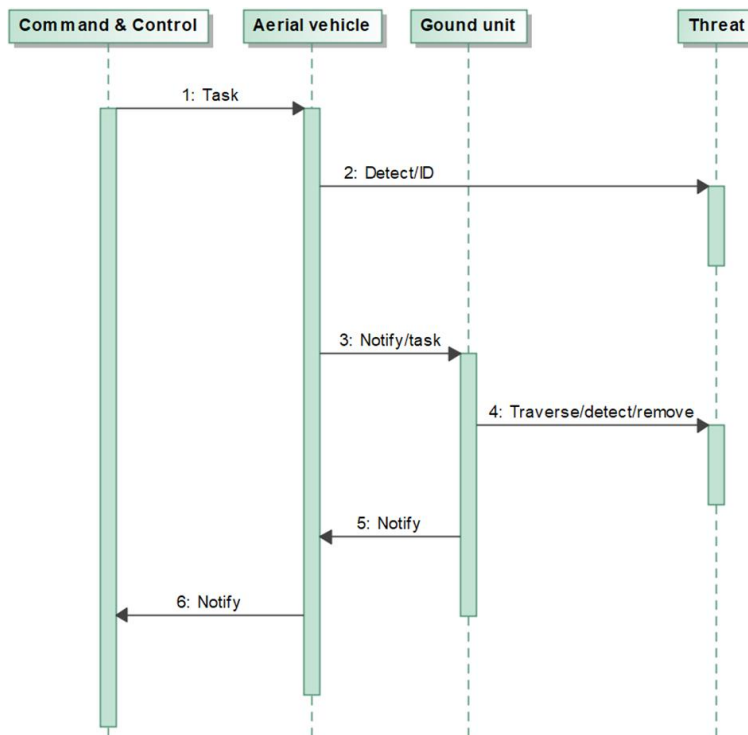


Figure 2. Firedog Mission Thread (Sequence Diagram)

Within the story arc, an (assumed) assessment concludes that the Firedog mission selects to use the Firebird UAV and the Bulldog UGV. As such, a traditional (cartoon) OV-1 shown in Figure 3 reveals the context specific information (e.g., generic blocks versus 4-wheeled vehicle). A challenge arises in the realization that the Firebird system does not currently include the capability to communicate with a UGV; and, therefore DE is leveraged to harmonize the models and data for the system of systems needed for success of the Firedog mission.

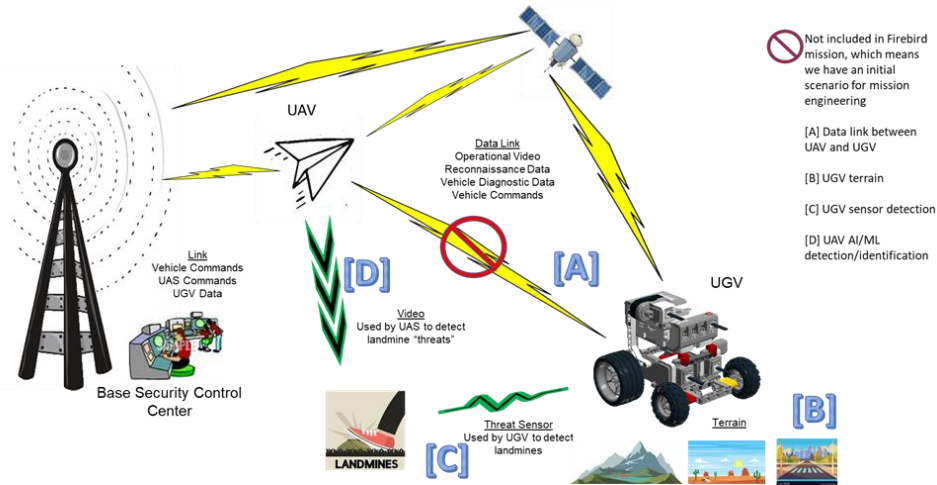


Figure 3. Traditional OV-1 for Firedog mission with noted missing current capability for communication between the UAV (Firebird) and UGV (Bulldog)

Therefore, within the Firedog program, the focus is on engineering the communication link between Firebird and Bulldog. This requires a set of four interconnected models: (1) a Firedog mission engineering model, (2) a Bulldog architecture model, (3) a Firebird architecture model, and (4) a link budget analytical model. A fifth model reflects the interconnections between the four system models as shown in Figure 4. Note, the blocks titled ModelCenter and Ansys HFSS reflect future evolution of the models to leverage of additional analytical environments.

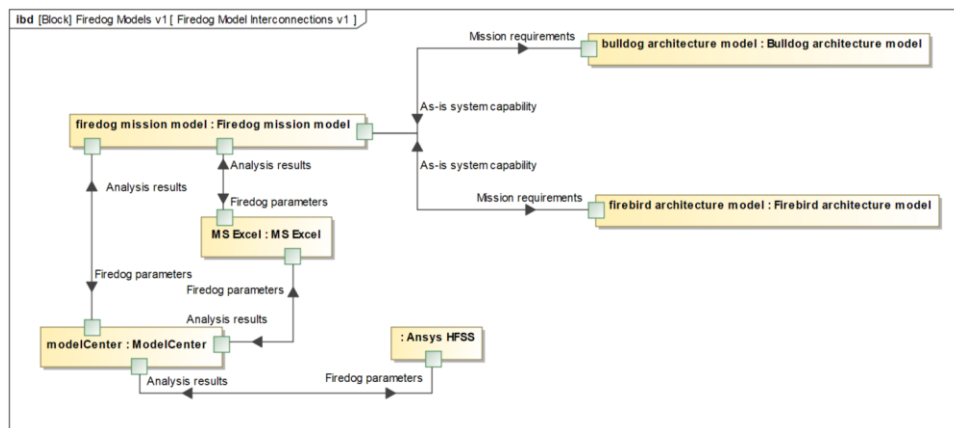


Figure 4. Interconnections between the Required System Models for Firedog Program

Note, the models are intended to evolve as the program advances; and, some models may exist within an MBSE tool, while others may exist within other tools such as a physics-based tool. Figure 5 is used to visualize an example of the continuous evolution of models.

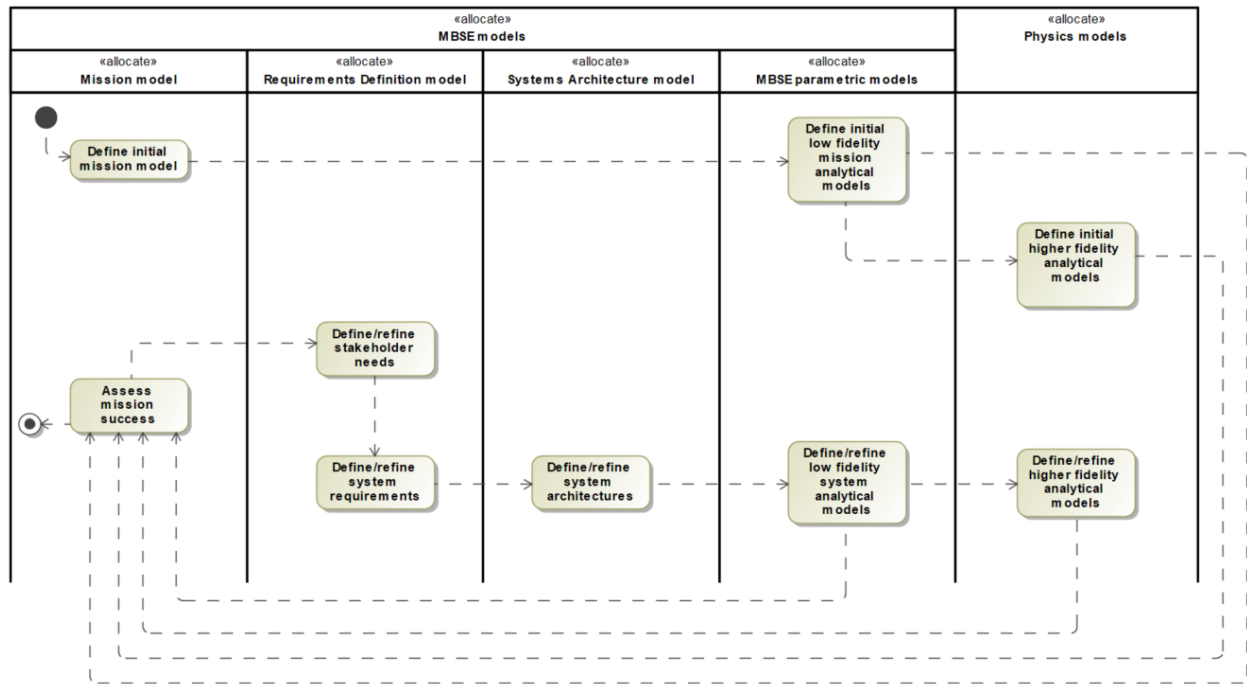


Figure 5. Generic representation of continuous model evolution

The team exemplified that evolution in Firedog. Early models, specifically within MBSE tools, are likely to be descriptive of behavior and provide low-fidelity analysis. For example, an activity diagram, shown in Figure 6, characterizes the expected system of systems behavior between the Firebird UAV and the Bulldog UGV. Through use of simulation of the activity diagram, analysis of the communication between Firebird and Bulldog would be limited to displaying the existence of exchanges of threat data (Firebird to Bulldog) and assessment (Bulldog to Firebird).

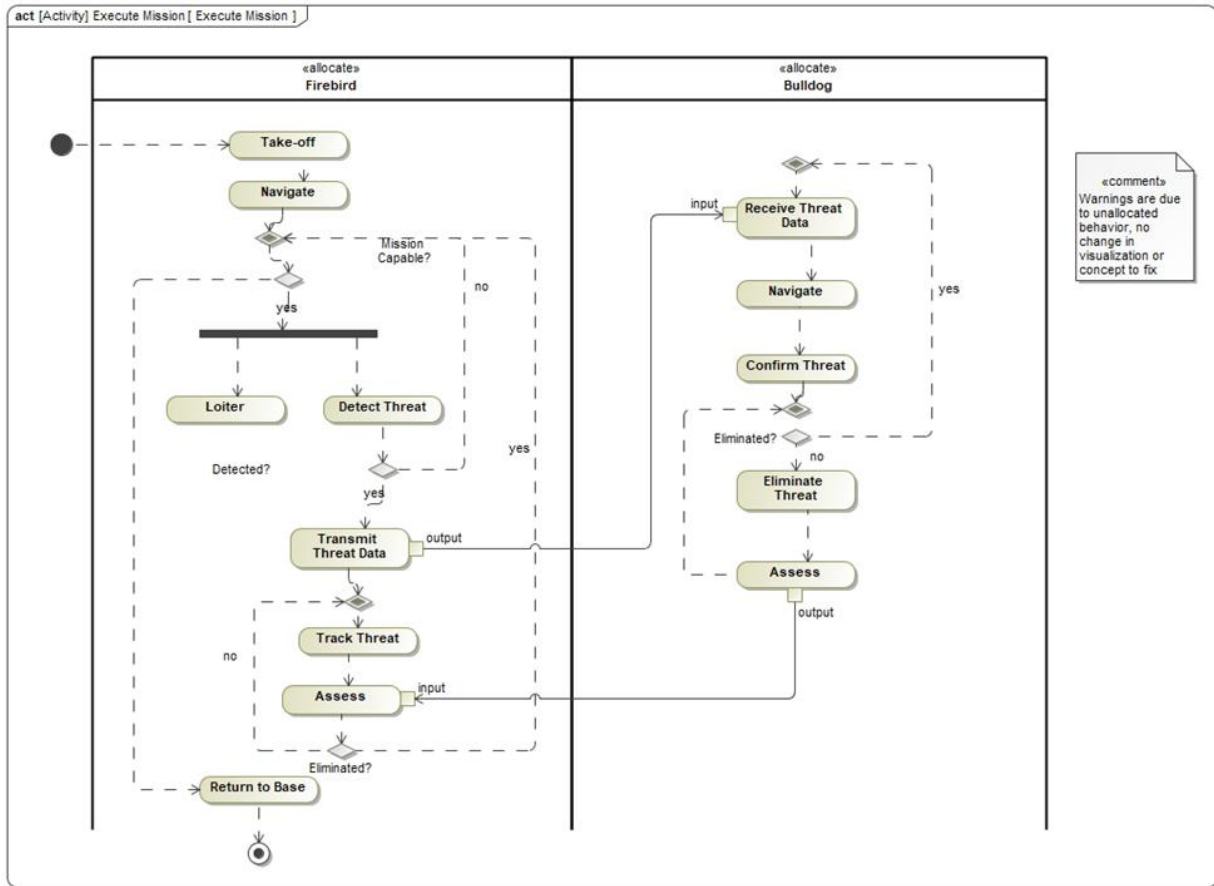


Figure 6. Low-fidelity model of the communication between Firebird and Bulldog within the context of the Firedog Mission

As the next evolution of analytical capability, more detailed models should be expected. In the case of Firedog, a Microsoft Excel file was interconnected with the Firedog mission model. The mission model provides the requirements set, which bounds the output of the analytical model, and provides the input parameters, which bound the range of analysis for two sets of system of systems alternatives. The analytical model accepts the input parameters, computes the output parameters for the alternatives, and provides the output back to the Firedog mission model. Figure 7 provides a visualization of the analytical V&V thread.

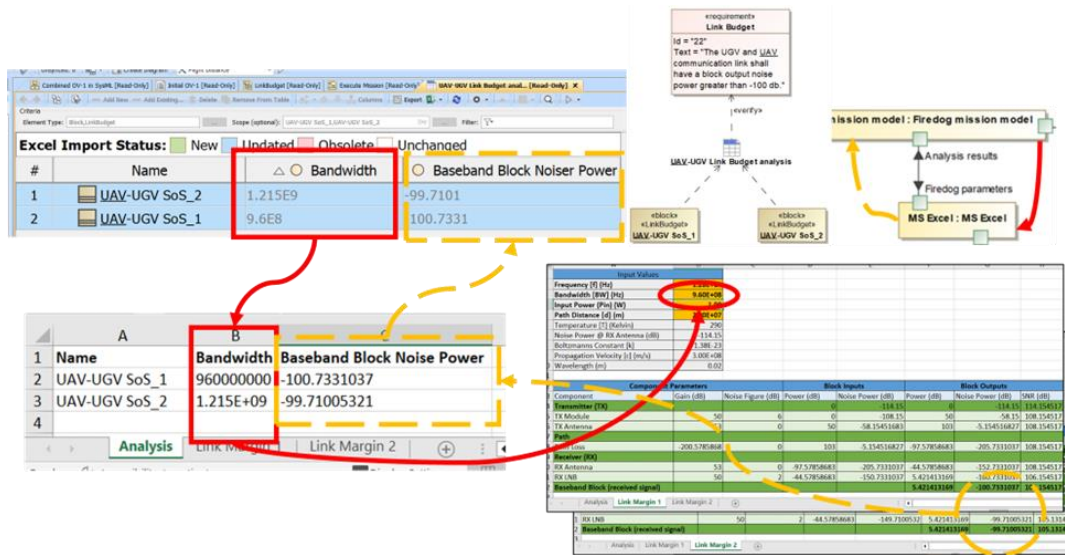


Figure 7. Visualization of the Firedog V&V thread for link budget analysis against the requirements

The team used MS Excel to demonstrate the interactions between connected models. Higher fidelity analytical models, such as with Ansys HFSS, should be expected as the program advances. Additionally, the supporting DEE should be expected to evolve to support the desired analysis of the system of interest.

Demonstration of requirements satisfaction as well as decomposition and allocation of functionality is another expected capability. In Figure 8, an example tabulation of requirements satisfaction and function allocation is shown, based on the Firebird system. As part of the curriculum in development for DAU, students are exposed to perform manual and automated calculation of the percent completion of satisfaction to highlight the value of model-based metrics.

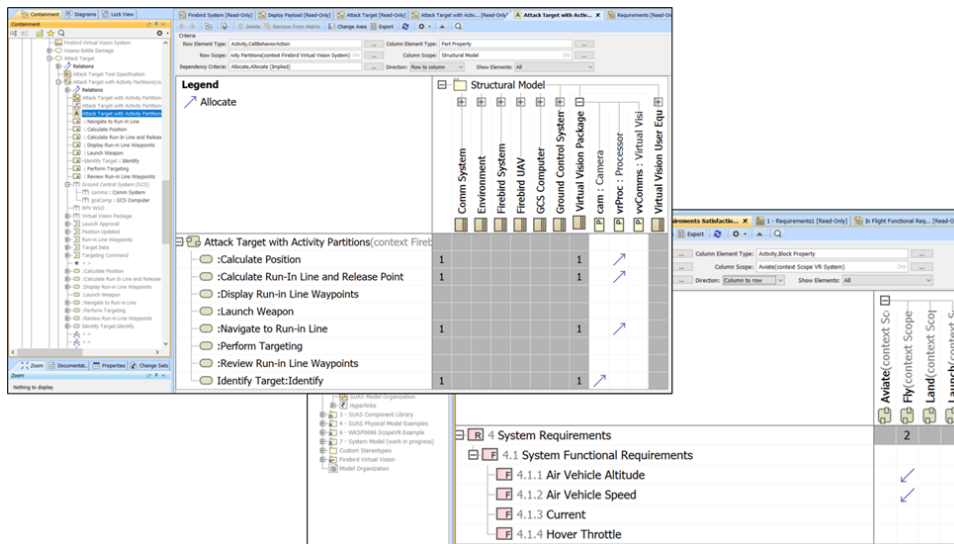


Figure 8. Firebird-based traceability for satisfaction and allocation of requirements

A general expectation in practice is that model-based metrics such as the percentage completion should be automated. In the MBSE tool selected for the Firedog case study, Cameo/Catia, this is not inherent as an out-of-the-box capability. Rather, the capability was constructed by the SERC team. The construct of such analytical capabilities should be considered in the selection of MBSE tools.

Overall, the Firedog case study is expected to evolve with the DAU sponsored project and other SERC/AIRC research. An AIRC team is leveraging Firedog to transform T&E to include integrated testing, joint testing, V&V uncertainty quantification, T&E for AI/ML, and normalization of a digital approach a TEMP and T&E planning. Additionally, an expectation set by DAU is to harmonize the DE curriculum with Systems Engineering and Mission Engineering curriculum, which the SERC team expects to be based on Firedog. Much of Bulldog, at the time of drafting this report, still exists as textual documents. The digital form of Bulldog is a much-anticipated growth area. For example, the SERC team explored integration of MBSE with product lifecycle management (PLM) and simulation through the use of LEGO-based software. Figure 9 is used to show an exemplar for MBSE/PLM integration in regard to Bulldog. The Firedog models were provided to the SERC team by partners external to this research. To further the utility of Firebird, the SERC team recommends cleaning up the model to provide more cohesive views that are more representative of what a member for the workforce should expect.

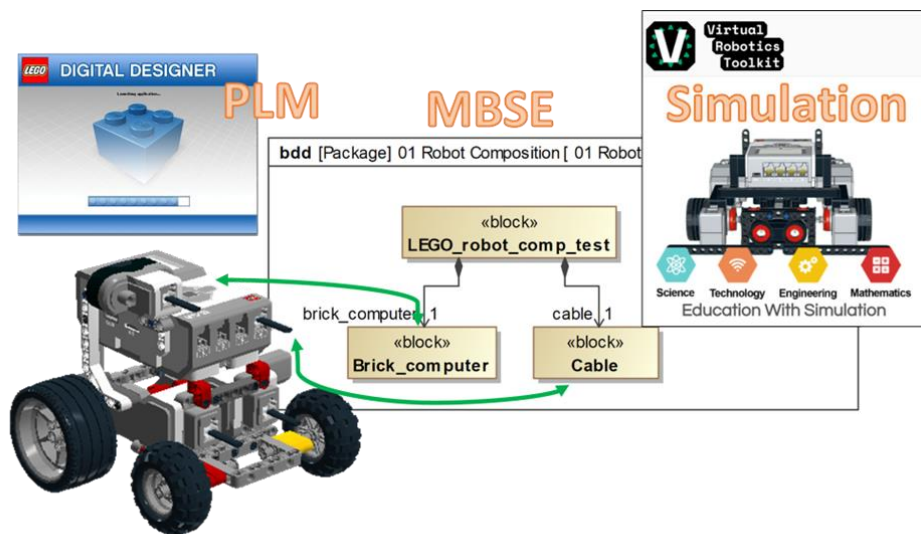


Figure 9. Expected evolution of Bulldog to include PLM and physics-based simulation

2.2.2 MISSION ENGINEERING & DIGITAL ENGINEERING

Overlap exists with the curriculum necessary to train the workforce on Mission Engineering (ME) and DE. Direction was given to the SERC team to coordinate with the team developing the ME credential, led by Dr. Jim Moreland, Old Dominion University (ODU). The two teams have held coordination meetings and the outcomes of the meetings included plans for basing the ME curriculum on the story arc and models created for the DE credential as well as having the ME team review any mission threads or models generated for the DE credential. The

primary goal of coordination is to ensure that both credentials are aligned and properly represent one another (i.e., the way the DE credential references ME is consistent with the ME credential and vice versa).

The notional plan is for the ME credential to leverage the Firedog mission developed for the DE credential. The Firedog mission is defined in detail in Section 2.2.4. To summarize, the Firedog mission revolves around a SoS that includes command base, satellite, unmanned aerial vehicle (UAV – Firebird), unmanned ground vehicle (UGV – Bulldog), a communication link between the two (Firebird and Bulldog), and a threat that must be neutralized. The ME credential team would like to include further mission analysis and development of further mission threads for Firedog, which could be used to support the ME credential. These additions are a potential activity for the next funding year of this SERC research task.

Additionally, the SERC and the Acquisition Innovation Research Center (AIRC) are both working on related tasks that build on Bulldog, such as digital transformation for T&E, which are expected to be complementary to and available for use as part of the DAU credentials for both DE and ME.

2.2.3 DIGITAL ENVIRONMENT AND ECOSYSTEM

Deploying DE on a program requires a fit-for-purpose set of tools and connecting infrastructure to support the desired activities through the acquisition lifecycle. The infrastructure helps to weave together or provide the connective tissue between tools and data, which creates the digital environment. That environment can then link into other types of tools (e.g., engineering versus program management) or other environments to form the broader ecosystem. All of this exists within an enterprise, which sets the foundational rules and context for everything from infrastructure through the ecosystem. This is illustrated in Figure 10.

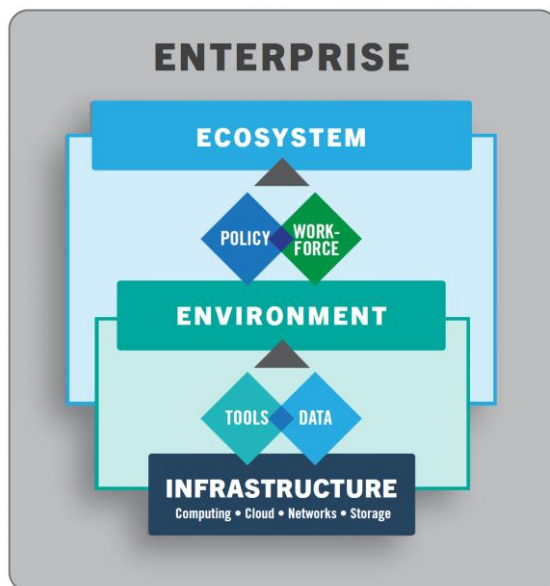


Figure 10. Conceptualization of the context and relationships for a digital environment and ecosystem.

To help illustrate the concepts and support the DE credential, the team conceptualized a digital engineering environment (DEE), illustrated in Figure 11.

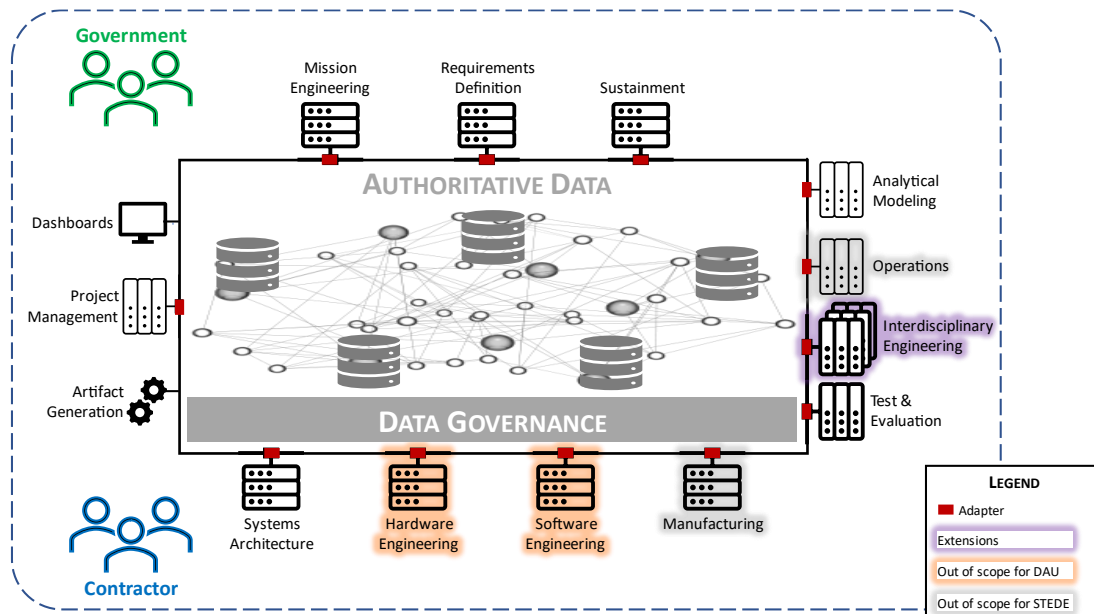


Figure 11. OV-1 for a Notional Digital Engineering Environment (DEE)

The notional DEE reflects the cumulative industry and academic experience of the team. The DEE elevates from specific tools to broader domains and concerns. While not exhaustive, the OV-1 reflects a potential scope from mission through architecture and design to T&E and operations and sustainment. It also reflects the engagement of both government and contractor without specific allocation to either party.

The OV-1 for the DEE is indicative of classes of tooling and the underlying authoritative data necessary to perform DE on a major program. Interdisciplinary engineering is highlighted to reflect that additional classes of tools should be added to the environment based upon the needs of the program. SCRE would be one such example.

The notional DEE plays a foundational role in the content of ENG 5530. It provides a framework for the discussion of classes of models in DE, the corresponding data underpinning these models, and the tools in a DEE. The notional DEE can be further leveraged as ENG 5540 and ENG 5550 are developed.

At this time, the DEE is only notional. However, as DAU moves forward and deploys the DE curriculum, it will be advantageous to incorporate student experiences in a multi-tool environment to clearly demonstrate the concepts and benefits of DE. Such an environment must be scaled to the learning objectives and the available infrastructure. The research team conceptualized and began architectural modeling of an environment specifically intended for academic instruction or training. This work was suspended based on the priority placed on development of ENG 5530 content but can easily be restarted in follow on work. It is

envisioned that the DEE will guide the instantiation of a suitable instructional multi-tool environment at DAU.

2.2.4 DIGITAL SYSTEMS ENGINEERING PLAN (dSEP)

This section is focused on digital (acquisition) artifacts, primarily the digital Systems Engineering Plan (dSEP). Here the term “artifact” is used in reference to items, traditionally delivered during system development in the format of a textual document, that are expected to be deliverable as a visualization of underlying data (e.g., model) through digital transformation.

As an example of the challenge of preparing the workforce for digital transformation, when drafting a Systems Engineering Plan (SEP), a student from the U.S. DoD workforce will use the SEP template and criteria as defined by policy, currently SEP version 4 (SEPV4). (U.S. DoD, 2021). The SEPV4 defines a document structure and the content for each section. The content includes items such as title page, signature approval page, program technical definition, and program technical management. While much of the content serves a similar intent to the previous version (SEPV3 (U.S. DoD, 2017)), SEPV4 requires content specific to digital transformation such as *technical data management* and a new appendix section entirely dedicated to defining a *digital engineering implementation plan*. Despite the new digital transformation-specific content required for a SEP, there is no specific guidance on the digital format for a SEP; rather, it gives the appearance of an expectation for a text-based format instead of a digital one.

Progress made over the last year includes:

- Assessment of the conversion of Skyzer to be consistent with current policy
- Progress and planning toward creating digital outlines, models, and templates of a SEP with the intention of using Bulldog as a means to compare text-based to digital formats
- Feedback from government, industry, and academia on digital artifacts through the advisory board, publications, and presentations

Planned activities for next year include:

- Incorporation into DAU curriculum
- Iterating on the digital outlines, models, and templates
- Soliciting and incorporating further feedback government, industry, and academia

Although the focus of this section is largely on the dSEP, some additional artifacts being explored by the SERC include the TEMP, RFI, and CDD. A notable finding, thus far, is that current policy requirements do not account for the digital format of a SEP. We expect to continue to share progress with the community in future venues.

The remainder of this section focuses on insights to the assessment of adhere of Skyzer to policy for the SEP and followed by progress on and planning for the use of Bulldog as the basis of a dSEP.

Skyzer

Digital acquisition artifacts are viewed from the perspective of the acquisition and system life cycles. As the system progresses through the acquisition lifecycle, the artifacts are also

expected to evolve. Much of the current DE ecosystem used by the SERC team consists of MBSE models constructed around key exemplar systems as well as dashboards constructed from the data that originated in the MBSE models and analytical models. Referring back to Figure 11 to frame an example, the dashboard may be Confluence, which visualizes authoritative data that originated in another tool, such as an architecture (MBSE) tool. The approach used by the SERC team leveraged previous efforts and currently existing constructs where possible and created new material where necessary.

Some available digital acquisition artifacts based on the Skyzer UAV model (Blackburn et al., 2021) were used and new digital acquisition artifacts were created based on the Bulldog UGV model (see section 2.3.5). Skyzer was created to demonstrate the art of the possible in regards to digital transformation specific to Systems Engineering. Figure 12 provides an overview of the Skyzer-based digitalization of the SEP.

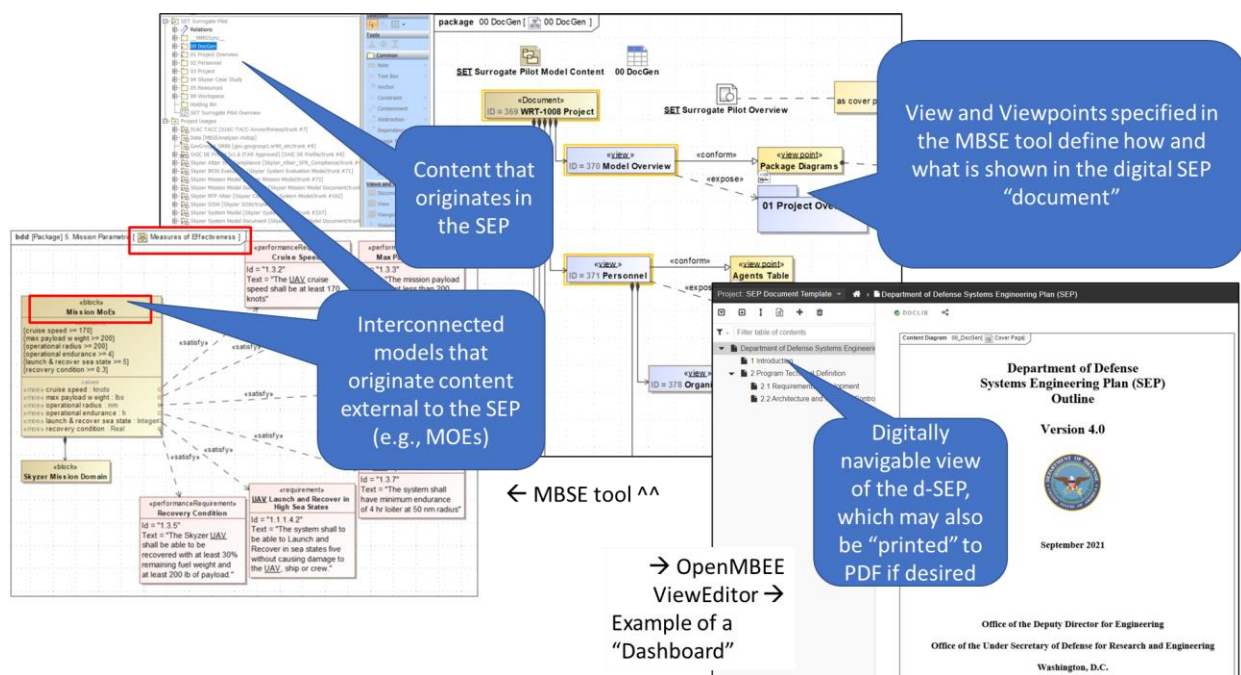


Figure 12. Overview of Skyzer-based Digitalization of the SEP

One insight the team gained is in regard to origination of data that constitutes the SEP. The Skyzer SEP consists of many parts. One set of parts, the MBSE models, serves the purposes of ME, requirements definition, system architecture, and program management components. As shown in the folder structure at the upper left of Figure 12, some content originated as part of the creation of the Skyzer SEP, while other content, such as the mission model, is interconnected to the Skyzer SEP and provides externally originated content. In summary, some data will originate as part of the inception of a SEP, while other data will originate from sources external to the SEP.

Another part of the Skyzer SEP is a dashboard (shown in the lower right of Figure 3), which is external to the MSBE tool and is intended to communicate from the authoritative data. Skyzer leverages OpenMBEE (OpenMBEE, 2022) for this purpose, although other Wiki-type tools such as Confluence® may also be used. OpenMBEE consists of a profile (DocGen) to

extend the MBSE language, Systems Modeling Language (SysML), and a dashboard referred to as the “ViewEditor”.

An insight gained from using DocGen was that the MBSE model structure may not be the desired structure of the digital artifact. DocGen enables customization of the data that exists in the MBSE models to specific stakeholder expectations, through the use of Views and Viewpoints.

An insight from using the ViewEditor is that not all individuals will need to directly access the MBSE tools. For example, the decision authority approver of the SEP may only navigate the content in the ViewEditor dashboard, rather than going directly into the MBSE tool. In the Skyzer example, while much of the SEP content may be created in the MBSE tool, the “digital sign-off” of the decision authority originates in the ViewEditor dashboard, which in turn is fed back into the MBSE tool.

This dashboard approach illustrates the ability to communicate data from an authoritative source, in a way that is easier for human consumption and supports management of the data by non-engineers.

While the above provided the SERC team with insights to the realization of a dSEP, assessment of the Skyzer SEP as to its adherence to policy was still necessary. The team assessed alignment of Skyzer against the requirements for SEpv4. While Skyzer contains much of the scope necessary for SEpv4, there is much SEP policy-driven content that is not present in Skyzer. For example, the Skyzer SEP does not have a DE Implementation Plan. As a result of these gaps, the team began exploring alternatives to Skyzer, with the intent of taking lessons learned from Skyzer and applying the lessons a dSEP based on Bulldog.

Bulldog

Bulldog is the name of an existing exercise used in DAU’s SE curriculum (SYS 202, specifically). In SYS 202, it is a UGV that is designed and built using either Lego Mindstorms kits (in person) or Lego Digital Designer (online). Students get the opportunity to work through trade spaces in the design, go through verification and validation (V&V activities), and make technical decisions that include considerations for cost. This is a rich set of exercises with an existing dataset. The team worked with DAU to begin modeling Bulldog earlier in OY1, but the higher-level bulldog models are used in ENG 5530 (see section 2.1.2 ENG 5520 – Model-Based Systems Engineering (MBSE), above).

Bulldog provides the basis for the next steps to explore digital artifacts. Because Bulldog currently exists largely as a set of text-based artifacts, an initial baseline for comparison to digital artifacts exists. Examples of the Bulldog text-based artifacts include the Capability Development Document (CDD) and a SEP. The SEP is based SEpv3, rather than SEpv4. Progress was made toward capturing the Bulldog SEP as a model consistent with SEpv3. Although the SEP will not be consistent with the current policy requirements, it is important to provide realistic examples that compare a text-based SEP to a d-SEP, as these types of examples are critical to support training and help students apply lessons in their own context. The team has begun mapping the existing SEP materials for Bulldog against SEpv4, which will provide a point of additional comparison especially useful for programs that began to

digitalize earlier under the SEpv3 guidance. This is illustrated in Figure 4. To fully understand the planned work, it is important to note the use of the following terms in Figure 13:

- **Outline** references the criteria for what should be included in a SEP(v4), which is currently defined in text-based form in (U.S. DoD, 2021) and which is in the process of being converted to a digital format as an MBSE model.
- **Model** is used to mean the set of MBSE models that define much of the content as well as the Dashboard, which is filled with data specific to the system being acquired such as Bulldog.
- **Template** is used as a suggested means of meeting a defined data need via a specified set of language, framework, and views; which is currently based on SysML.

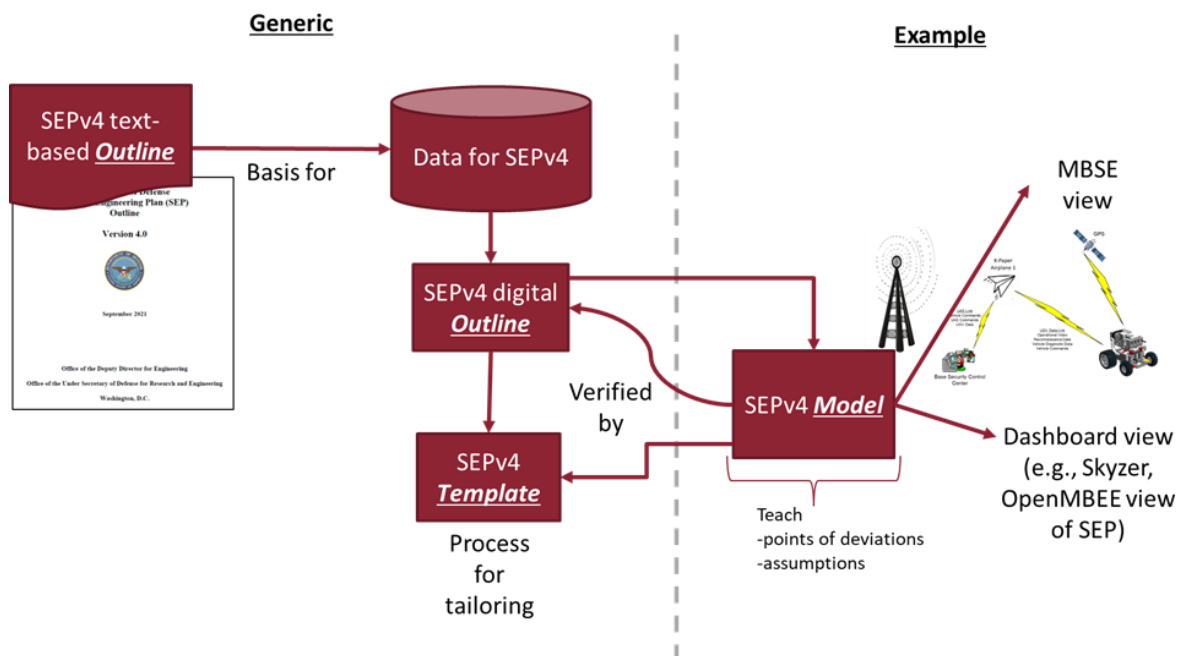


Figure 13. Visualization of Generic SEpv4 Digitization and Digitalization plus Specific Example Content from Bulldog

The plan going forward is to have generic content that includes the SEpv4 text-based outline, SEpv4 digital outline, and the SEpv4 template; and, specific example with populated content such as a Bulldog SEpv4 model. The need for continuous improvement is expected, which is why the feedback arrows, marked with the “verified by” indicator, are present in Figure 13, from the model to the outline and template. Furthermore, it is expected that the current policy may not contain the right guidance or direction necessary for the digital transformation of acquisition artifacts. Feedback from the modeling efforts to the policy is necessary to move from a *digitized* SEP to a *digitalized* SEP.

From a pedagogical perspective, students will need to be familiar with the SEpv4 text-based outline, digital outline, model(s), and template. The combination provides the foundation to help students think through the digital transformation of the SEP and can support the training necessary to empower the defense workforce. The SEpv4 digital outline has been created and the SEpv4 model based on Bulldog is currently in progress. The SEpv4 template will be

the last step and will be developed iteratively with the SEpv4 model, which is why it is suggested in Figure 13 that teaching from the SEpv4 model will require showing students points of deviation and assumptions made when creating the SEpv4 model. Lastly, in parallel, the digital outline and model of Bulldog for SEpv3 is currently in progress; which will enable students to see an example of a digitization of the text-based to digital SEP in a one-for-one comparison.

2.3 STEDE & TRACING INTERRELATIONSHIPS

During the base year of this project, work was initiated on the Simulation Training Environment for Digital Engineering (STEDE) architecture. During OY1, the architecture was further refined via MBSE representations (see Figure 14 Figure 14). During curriculum development for OY1 (see Section 1 - Developing the Curriculum), it became clear that a formalized definition of credential and competency concepts would be useful for team understanding and for consistent application of those concepts.

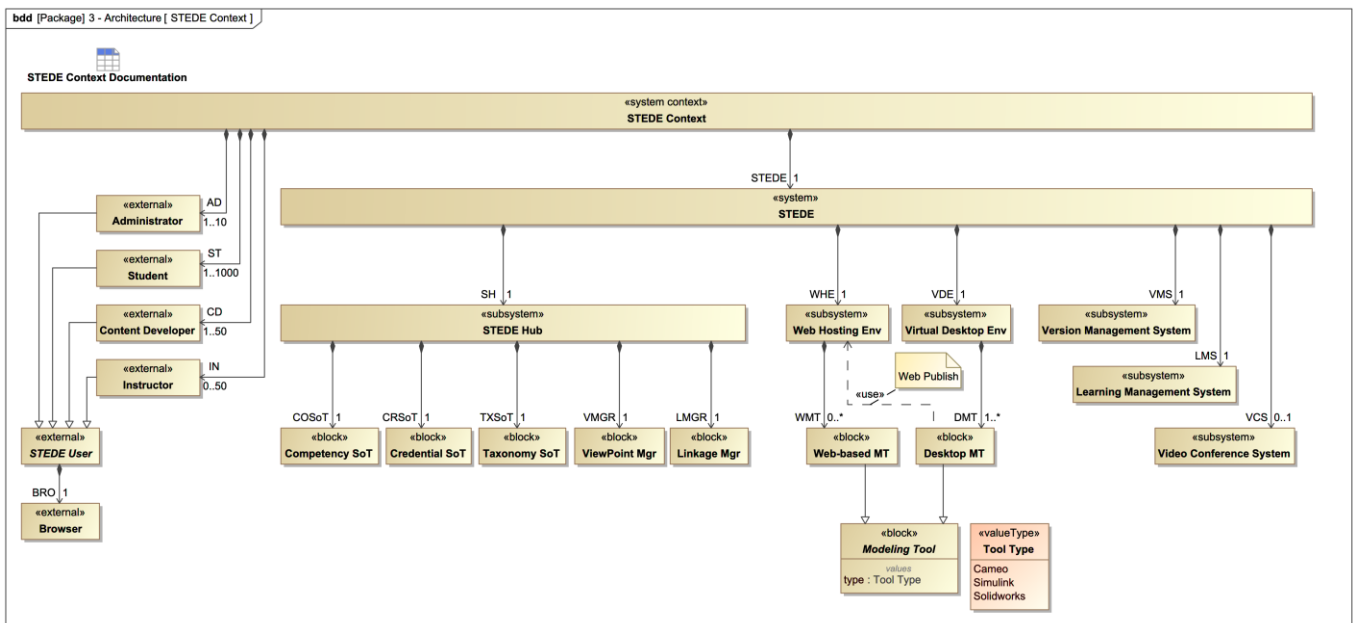


Figure 14. STEDE Context

The meta-model for the Credential source of truth is captured in Figure 15. Key concepts include:

- The hierarchical relationship between Credential, Package (Course or Textbook), and Section (Module or Chapter)
- The notion of ordered Credential pre-requisites
- The notion that Sections contain a set of activities and that activities may involve Case Study models using various DE tool types. Sections are intended to be self-contained and reusable.

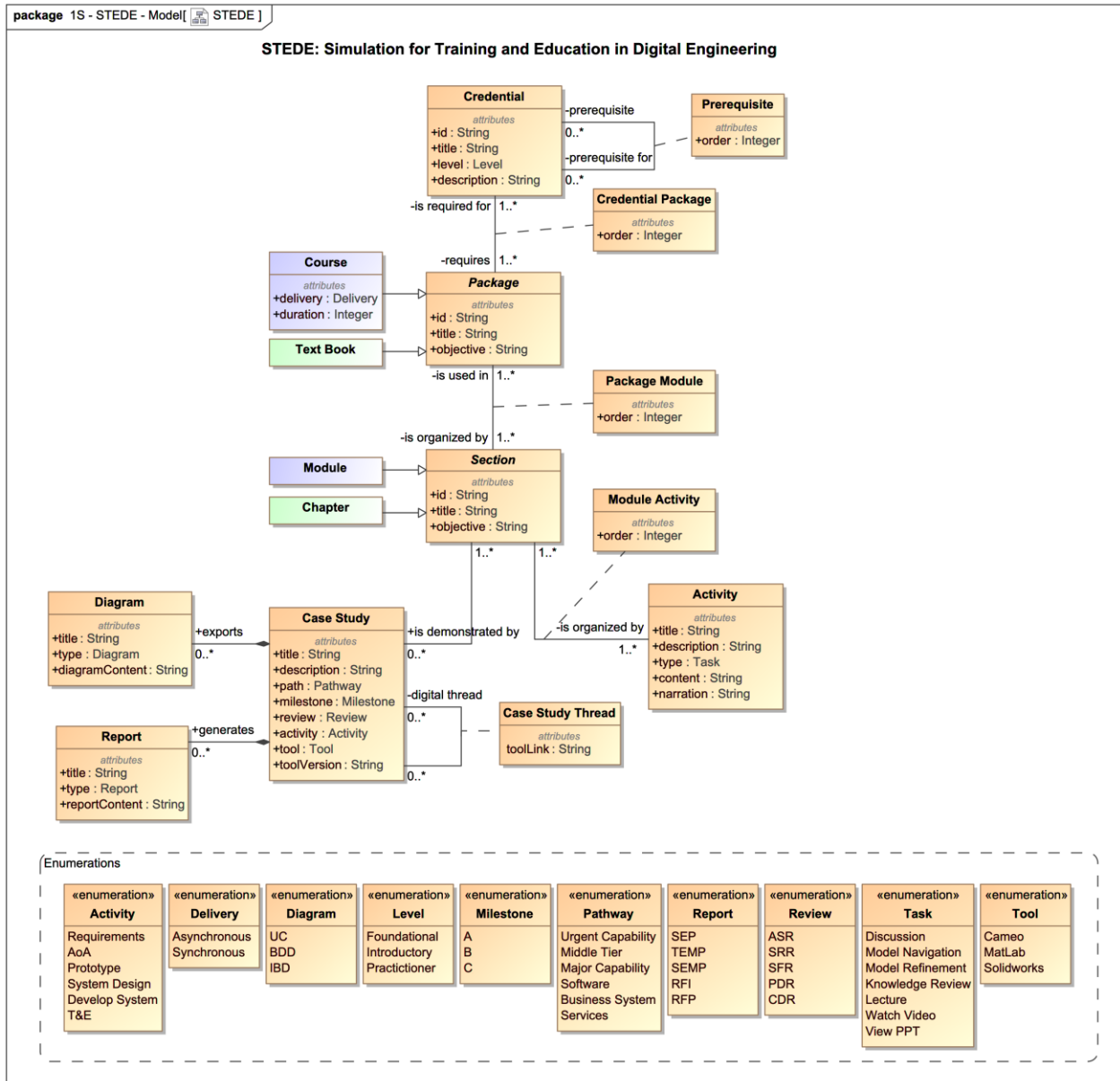


Figure 15. Credential Meta-Model

The meta-model for the competency source of truth is captured in Figure 16. Key concepts include:

- The hierarchical relationship between Competency, Performance Outcome, TLO and ELO.
- The notions that Competencies are satisfied by Credentials, Performance Outcomes are satisfied by Packages, and ELOs are satisfied by Sections.
- The notion that an Exam is made up of a set of questions, that Credentials are evaluated by an Exam, and that TLOs are evaluated by one or more questions.

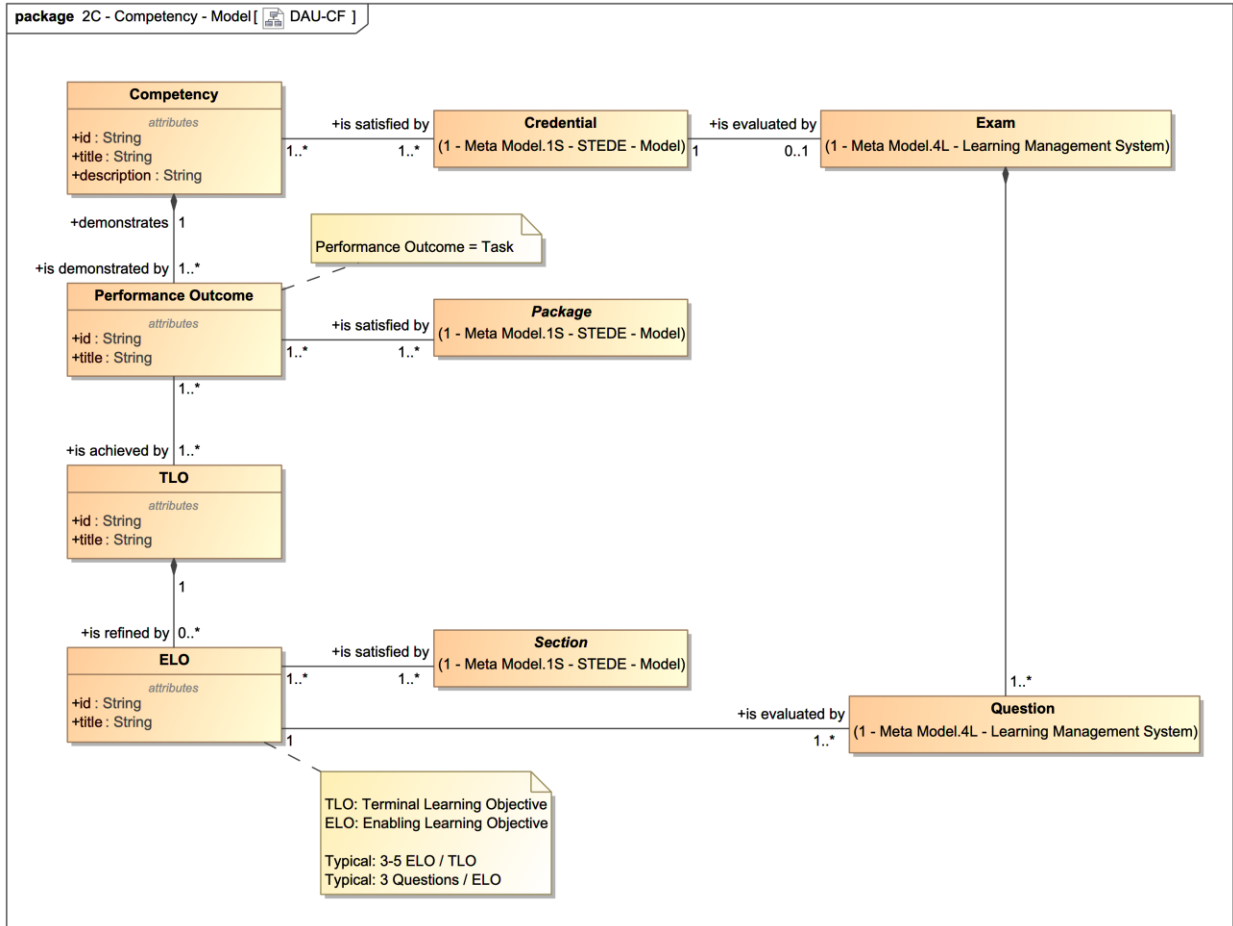


Figure 16. Competency Meta-Model

Finally, the meta-model for the taxonomy source of truth is captured in Figure 17. Key concepts include:

- For training consistency, packages that use a specialized language, e.g., Secure Cyber Resilience Engineering (SCRE), it is important to document that language via a Taxonomy.
- The taxonomy provides a definition of key concepts and how those concepts relate to one another.

The full Cameo STEDE model is delivered as an addendum to this report summary (see Appendix C: Description of Ancillary Materials for details).

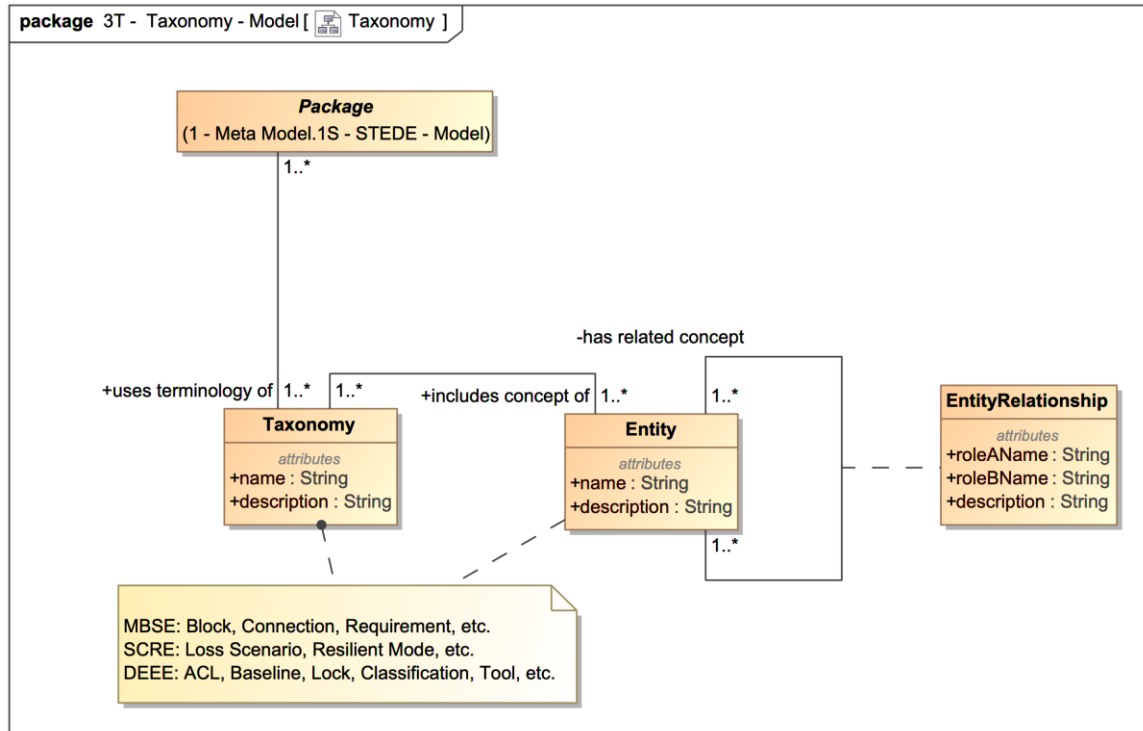


Figure 17. Taxonomy Meta-Model

To test and evolve the meta-models above, a demonstration STEDE implementation was built using an SQLite DB with a Jupyter Notebook user interface (see Figure 18). The “create-db” notebook performs the following:

- Creates the DB Schema per the meta-model definition,
- Partially populates the DB with instances per the curriculum being developed for DE and SCORE, and
- Creates a few interesting DB views which join tables of interest into an integrated view.

The “query-db” notebook demonstrates how a tabular web view can visualize the DB views.

Finally, the “report-db” notebook (Figure 19) demonstrates how the same underlying DB can be used to generate reports and documents. In this case, a LaTeX extension is used to generate and format tables which are previewed as a pdf document.

The STEDE demonstration implementation is delivered as an addendum to this report summary (see Appendix C: Description of Ancillary Materials for details) and is also available at: <https://github.com/tsherburne/stede-db>.

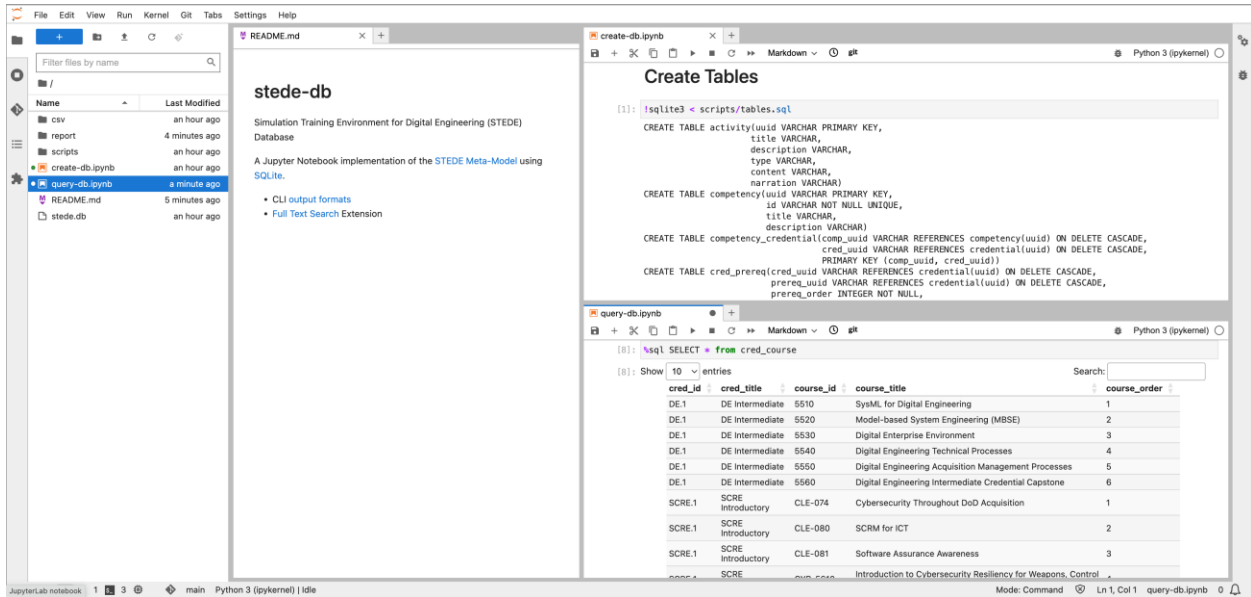


Figure 18. STEDE DB Implementation Overview

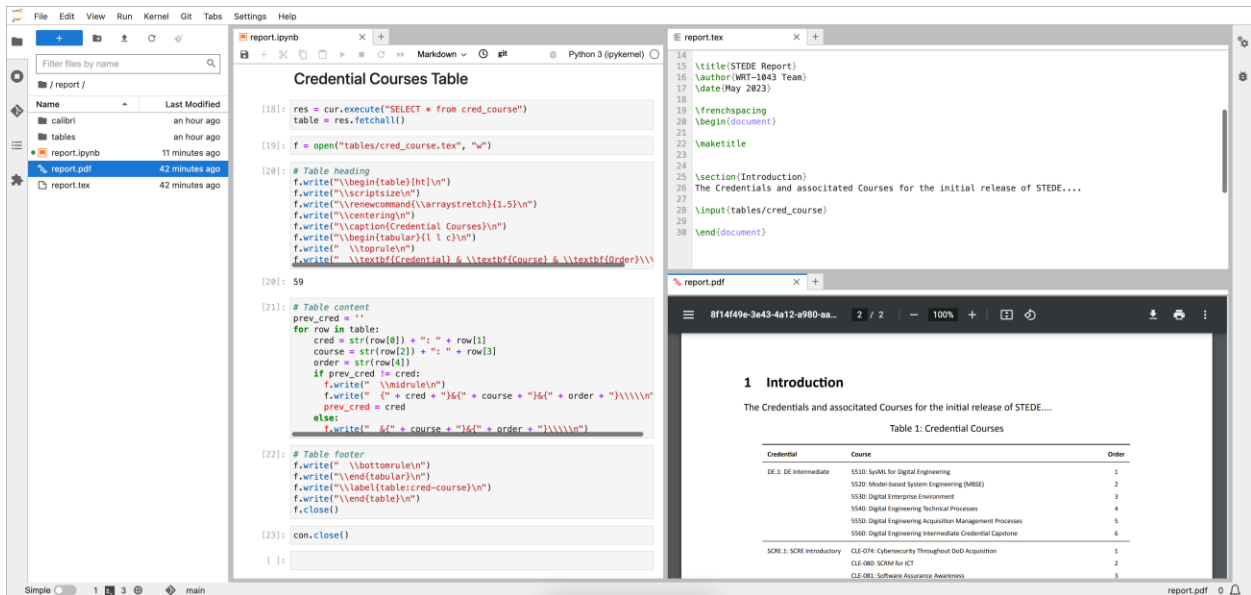


Figure 19. STEDE DB Report Generation Example

2.4 SCRE

As a part of the Digital Engineering task, the SERC team was also asked to develop and help deploy a credential focusing on Secure Cyber Resilient Engineering (SCRE). The Systems Security Directorate, in the Office of Science and Technology Program Protection (STPP) under the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) realizes cybersecurity and cyber resilience as a critical pillar in defense related engineered systems. However, it has also been noted that a developed, holistic approach to

integrating the varying aspects of cyber into the engineered design is lacking – especially at the early stages of development. Therefore, the motivation for designing in resilience and system security, specifically relating to cyber, is being actualized. Especially considering digital engineering, where potential vulnerabilities may be elucidated most optimally through the proposed practices. SCORE is the term used for the systems engineering practice that achieves the objectives of weapon system security and cyber resilience, and the Defense Acquisition University has taken on the task to develop a credential that can strengthen the workforce through three added courses.

Further information on the development and deployment of the SCORE credential can be found in Appendix D. In addition, any further information, or demonstrations of the materials, can be access through Dr. Aaron Jacobson (aaron.d.jacobson@dau.edu), Dr. Peter Beling (beling@vt.edu), Timothy Sherburne (sherburne@vt.edu), or Megan M. Clifford (mcliffor@stevens.edu).

2.4.1 SILVERFISH WITH SysML SCORE

During OY1, DAU directed that all case study models are to be built using the SysML meta-model and the Cameo modeling tool. An important case study for SCORE is Silverfish, which was previously developed using GENESYS (the Vitech modeling tool) and meta-model. Silverfish was converted to SysML and further refined during OY1.

A top-level view of the SCORE meta-model is shown below (Figure 20**Error! Reference source not found.**). As part of the migration, the team has identified the Object Management Group (OMG) Risk Analysis and Assessment Modeling Language (RAAML) specification for standardized support of the Systems Theoretic Process Analysis (STPA) methodology. The SCORE meta-model is partitioned between the standard SysML profile, RAAML profile, and Virginia Tech (VT)-defined SCORE profile for the “sentinel” and “resilience” concepts.

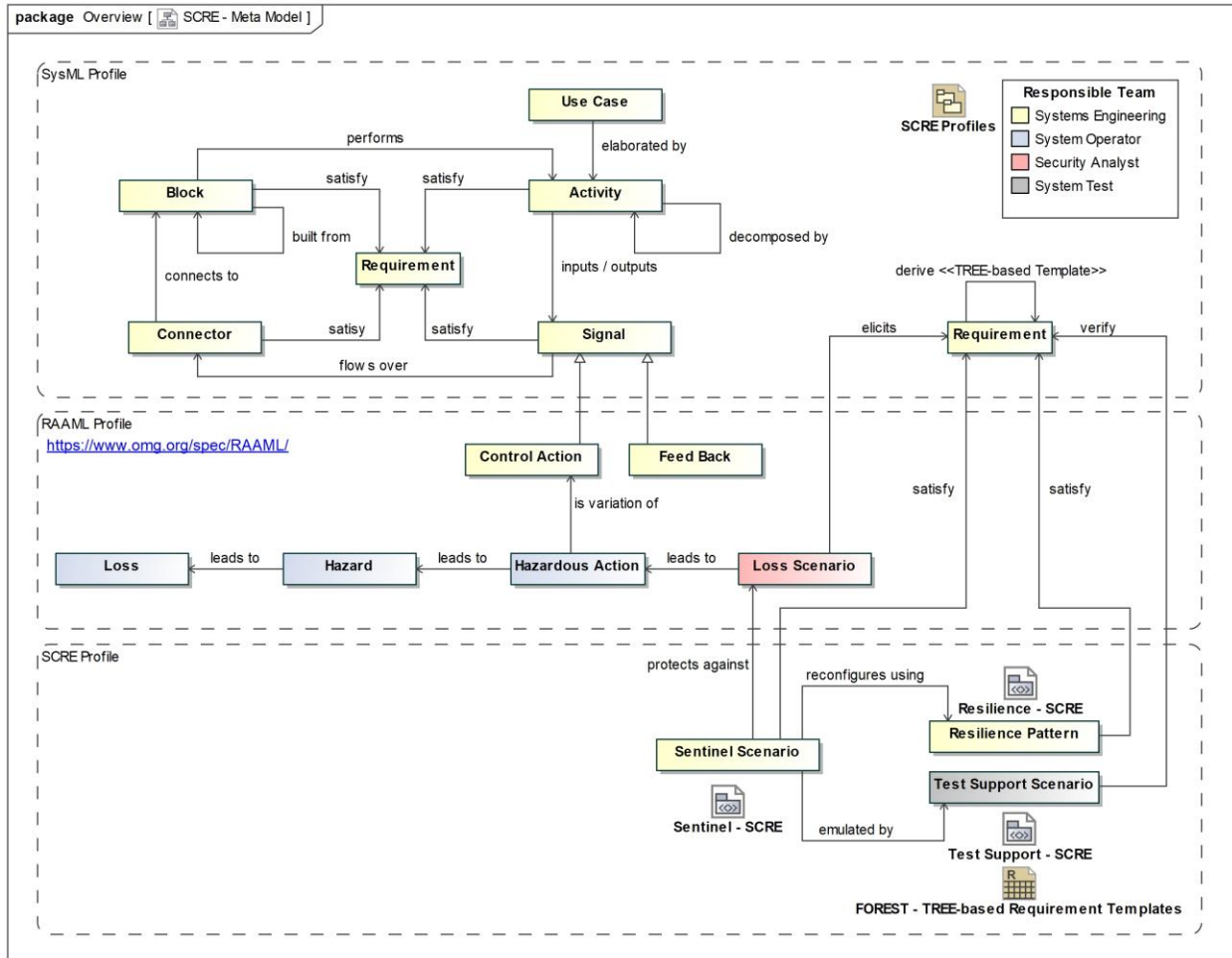


Figure 20. Secure Cyber Resilience Engineering (SCRE) SysML Meta-Model

The Cyber Resilience Requirements Methodology (CRRM) is illustrated in Figure 21. The Silverfish case study is modeled according to the CRRM using the SCRE meta-model. A brief description of the model artifacts produced at each step include:

- System Description
 - Use Cases, Activity Diagrams (with Signals [Control Action or Feedback] between Activities), BDD, and IBD (with Connectors and message flow between Blocks)
- Hazard Analysis
 - STPA Losses, Hazards and Hazardous Actions
- Loss Scenario Assessment
 - STPA Loss Scenarios and elicited resilience Requirements
- Resilience Architecture

- Sentinel Scenarios that protect against Loss Scenarios, reconfigure using Resilience Patterns, and are emulated by a Test Support System which verify elicited resilience requirements.

The full Silverfish model and SCRE meta-model are delivered as addendums to this report summary (see Appendix C: Description of Ancillary Materials for details).

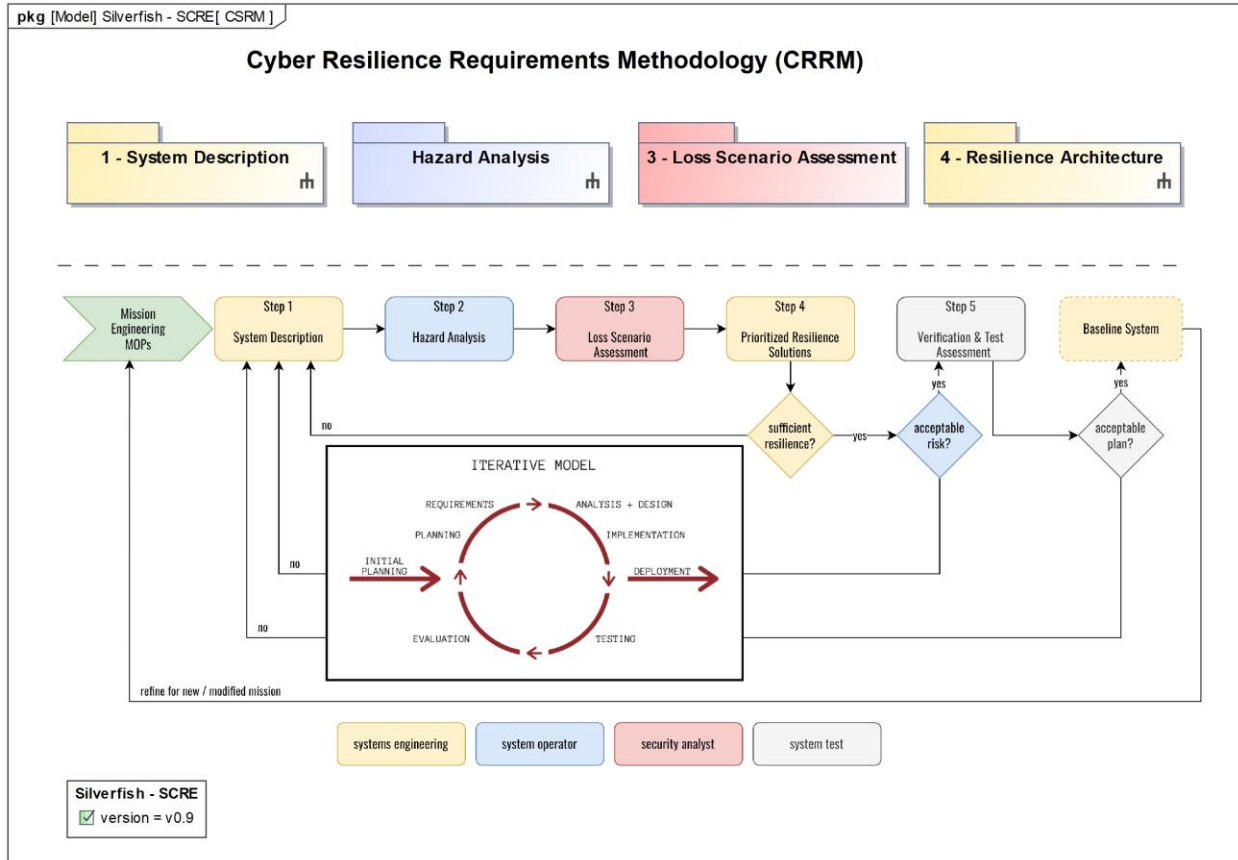


Figure 21. Cyber Resilience Requirements Methodology

2. REVIEW AND FEEDBACK

A critical component for successful research tasks is open collaboration with the sponsor and review by the broader community. This section briefly outlines the major review and feedback processes utilized in OY1.

3.1 DAU FACULTY REVIEWS

The SERC team conducted a monthly review with DAU faculty members. During this review, the team would present the status of current work and faculty members would provide review and feedback. The team would update materials based on that feedback.

In addition, team members have attended meetings for ENG 5510 and 5520 and CYB 5610 each week, providing close coordination with faculty.

3.2 DIGITAL ENGINEERING ADVISORY BOARD REVIEWS

There are opportunities to usher in the necessary breakthroughs for digital transformation to advance the DoD's technical edge. DAU is entrusted to develop digital engineering curriculum that will prepare individuals and organizations for the evolving digital engineering needs of DoD. The purpose of the Advisory Board is to gain insight into current practices, challenges, and needs from the esteemed board's perspective. Another goal of the Advisory Board is to continue expanding the curriculum and approach to best equip the workforce for engagement and execution of digital engineering. Eleven Advisory Board members across industry, government, Federally Funded Research Development Centers (FFRDCs), and academia serve in this capacity to guide and validate the research and deployment of the curriculum.

As of report publication, the Advisory Board consists of:

Name	Organization
J. Kyle Hurst	U.S. Air Force
Jason Cook	U.S. Army
LTC David Bates	U.S. Space Force
Lori Zipes	U.S. Navy
Phil Zimmerman	OUSD(R&E) (Retired)
Ryan Noguchi	Aerospace Corporation
Azad Madni	University of Southern California
Steven Ardito	NASA Jet Propulsion Lab (JPL)
Phil Anton	Acquisition Innovation Research Center (AIRC)
Mike Jones	Applied Physics Lab (APL)
Ed Kraft	University of Tennessee

Past Advisory Board members included Chris Schreiber (Lockheed Martin), Victoria Cuff (formerly OUSD(A&S)), and John Day (NASA JPL).

The Advisory Board met bi-monthly, conducting eight workshops during OY1. The Advisory Board provided detailed feedback and insights based on their experiences and organizations. Key agenda items for these meetings have included:

- Discussion of Needs and Most Critical Skill Gaps
- Living Digital Textbook for Digital Engineering
- STEDE/Digital Engineering Textbook
- Architecture
- Digital Artifacts
- Experiences with DE: Challenges and Bright Spots
- Critical Scenarios for Training
- Review of Curriculum Materials (ENG 5510, 5520, and 5530)
- Digital Engineering Ecosystem: Minimum Viable Ecosystem
- Digital Engineering Ecosystem: Minimum viable set of data and tools to support educational experiences
- Mission Threads
- Model Interoperability
- SCRE Credential
- DE/MBSE Style Guides

The feedback from Advisory Board members has been critical for improving the research and the team's support of DAU's curriculum. The team published a paper about the role of the Advisory Board in the 2023 IEEE Systems Conference (SysCon), which was presented to an international audience in April 2023. (See Tao et al. 2023)

The slides and minutes (including any working materials captured in Miro) from each Advisory Board meeting can be found in the SERC-2023-TR-007-F ancillary materials.

3.3 PUBLIC PRESENTATIONS

In addition to the formal reviews by DAU and the Advisory Board, the team published several conference papers in OY1. At each event, the team received questions and feedback from the audience and often in follow-up from the events. This feedback also informed the evolution of the materials. See Appendix A for a full list of publications.

3. FUTURE WORK & CONSIDERATIONS

This section outlines the expected scope of work for the next year (option year 2 (OY2)). The priorities identified by the sponsor for future work are:

1. Development and deployment support to ENG 5530
2. Development and deployment support to CYB 5610
3. Development and deployment support to CYB 5620
4. Collaborate on the development of a digital twin for a selected system.
5. Collaboration with Mission Engineering Credential courses to include selection of appropriate models and supporting curriculum.
6. Collaboration with Systems Engineering Credential courses to include selection of appropriate models and supporting curriculum.
7. Development and Deployment support to CYB XXXX-Cyber Resilient Engineering Practitioner course

Sections 2 describes the ENG 5530 and CYB 56XXX series courses and Appendix D provides additional context. Next year's expected tasks include continued iterations between the SERC and DAU teams to develop, refine, and review the course material. The development of the Bulldog and Firebird case studies will be key to addressing the sponsor's priorities for next year. Pathways for this development are discussed below.

Completing the digitization of existing Bulldog artifacts and digitalizing Bulldog where no artifacts currently exist will be a top priority. This comprehensive process will ensure that all relevant materials are available in a digital format, facilitating accessibility and ease of use. Conforming the Firebird model to a designated style guide will be another crucial task. The project will actively align the Firebird model with the selected style guide to enhance its coherence and improve comprehensibility. This will enable students to better understand and engage with the model, further advancing their learning experiences.

Expanding the Firedog case study is a key objective for the upcoming year. The project aims to incorporate physics-based modeling and simulation techniques to enrich the study. The goal in actively integrating these methods is to improve the fidelity of the analytical models used, transitioning from basic MS Excel-based models to more powerful tools such as Python, Matlab, Ansys HFSS, and MDAO. This approach will enhance the accuracy of the analysis and provide valuable support for mechanical engineering aspects.

To foster a more comprehensive DEE, the plan for next year includes incorporating the updates and improvements made to Bulldog and Firebird. The DEE will serve as a central platform for the project's artifacts and tools, with the goal of providing seamless integration and accessibility to all stakeholders involved.

Next year's work will incorporate the updates into the curriculum to ensure that students benefit from the advancements. This will involve integrating the updated Bulldog and Firebird artifacts, models, and case study materials into the curriculum framework. Such integration

would provide a foundation for support of higher-level classes including the capstone experience.

Several updates are recommended to further enhance the educational value of the Firedog case study. First, the project proposes advancing the analytical models from MS Excel to more sophisticated modeling tools such as Python, Matlab, Ansys HFSS, and MDAO. This transition will allow students to delve deeper into the subject matter and perform more comprehensive analyses, particularly in the realm of mechanical engineering.

Additionally, Bulldog will undergo notable expansion. The suggested plan includes converting all text-based artifacts to model-based artifacts, providing a more intuitive and visual representation of Bulldog's components. A detailed architecture model(s) for Bulldog should be constructed to capture its intricate structure and design. Physical and digital representations based on platforms like LEGO EV3, Arduino, and/or Raspberry Pi will be incorporated to enrich the learning experience. Finally, the project will develop lifecycle appropriate artifacts to support developmental and operational testing and evaluation (T&E) activities, allowing students to gain practical insights into the project's life cycle.

APPENDIX A: PUBLICATIONS AND PRESENTATIONS RESULTING FROM RESEARCH

2023:

Wach, P., Clark, D., Kerr, Geoff, Long, D., Clifford, M., Arndt, Cl., Sherburne, T., See Tao, H. Y., McDermott, T., Verma, D., Beling, P., Hutchison, N. (2023). "Advancing Education on Digital Artifacts." Conference on Systems Engineering Research (CSER), 16-17 March 2023, Hoboken, NJ.

See Tao, H. Y., Hutchison, N., Clifford, M., Kerr, G., Beling, P., Sherburne, T., Wach, P., Long, D., Arndt, C., Verma, D., & McDermott, T. A. (2023). "Challenges and Opportunities in the Digital Engineering Simulation Curriculum Development." IEEE International Systems Conference, 17-20 April 2023, Vancouver, Canada.

2022:

Beling, P. (2022). "Operational Cyber Resilience in Engineering and Systems Test." DATAWorks (Defense and Aerospace Test and Analysis Workshop), 26 April 2022, Alexandria, VA.

See Tao, H. Y., Hutchison, N., Beling, P., Arndt, C., Blackburn, M. R., Sherburne, T., Wach, P., Long, D., Verma, D., & McDermott, T. A. (2022). "Initial Development of a Roadmap for Digital Engineering Simulations Curriculum." IEEE International Systems Conference, 2022, pp. 1-7. doi: 10.1109/SysCon53536.2022.9773836.

Hutchison, N., See Tao, H. Y., Clifford, M., Burley, C., Wach, P., Sherburne, T., Beling, P., Arndt, C., McDermott, T. A., Blackburn, M. R., Long, D., & Verma, D. (2022). "Digital Transformation in Acquisition: Using Modeling and Simulation to Advance the State of Practice." INCOSE International Symposium, 25-30 June 2022, Detroit, MI.

Wach, P. (2022). "Simulation Training Environment for Digital Engineering (STEDE)." NDIA Systems and Mission Engineering Conference, 3 November 2022, Orlando, FL.

Hutchison, N., & Pearson, D. (2022). "Digital Transformation in Acquisition: Using Modeling and Simulation to Advance the State of Practice." Presentation at the 2022 SERC Sponsor Research Review, 16 November 2022, Washington, D.C.

2021:

Hutchison, N., & Wach, P. (2021). "DAU Digital Engineering Simulation." Presentation at the 2021 SERC Sponsor Research Review, 4 November 2021, Washington, D.C.

Beling, P. (2021). "SERC Systems and Cyber Resilience Modeling." Security Engineering Tutorial, 3 November 2021, Washington, D.C.

Blackburn, M. R. (2021). "Skyzer Surrogate Pilot Overview and MBSE Cost Model Use Case with Model Tour Demonstration." Digital Engineering Tutorial, 3 November 2021, Washington, D.C.

APPENDIX B: CITED AND RELATED REFERENCES

Blackburn, et al. (2021). Transforming Systems Engineering through Model-Centric Engineering. Hoboken, NJ: Systems Engineering Research Center, Stevens Institute of Technology. SERC-2021-TR-012. 2021.

Bloom, B. S. (1956). Taxonomy of educational objectives: Cognitive and affective domains. New York: David McKay.

DoDI 8500.01 (2019). Department of Defense Instruction 8500.01 on Cybersecurity. Retrieved May 25, 2023 from

https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/850001_2014.pdf

NIST 800-160 V2 (2021). Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. Retrieved May 25, 2023 from

<https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final>

OpenMBEE (2022). "Open Model Based Engineering Environment." Retrieved Dec 9, 2022, from <https://www.openmbee.org/>.

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistic OUSD(AT&L), *Performance of the Defense Acquisition System 2016 Annual Report*, U.S. Department of Defense, October 24, 2016, pp. 45–46.

<http://www.acq.osd.mil/fo/docs/Performance-of-Defense-Acquisition-System-2016.pdf>,

also <https://www.dtic.mil/docs/citations/AD1019605>

U.S. DoD (2017). Systems Engineering Plan (SEP) Outline Version 3.0. Retrieved May 25, 2023 from <https://ac.cto.mil/wp-content/uploads/2020/08/SEP-Outline-3-0.docx>

U.S. DoD (2018). DoD Digital Engineering Strategy (2018), Washington, DC, June 2018.

Retrieved from <https://ac.cto.mil/wp-content/uploads/2019/06/2018-Digital-Engineering-Strategy-Approved-PrintVersion.pdf>

U.S. DoD (2021). Department of Defense Systems Engineering Plan (SEP) Outline Version 4.0. Retrieved May 25, 2023 from <https://ac.cto.mil/wp-content/uploads/2021/10/SEP-Outline-4.docx>

See Tao, H. Y., Hutchison, N., Clifford, M., Kerr, G., Beling, P., Sherburne, T., Wach, P., Long, D., Arndt, C., Verma, D., & McDermott, T. A. (2023). "Challenges and Opportunities in the Digital Engineering Simulation Curriculum Development." IEEE International Systems Conference, 17-20 April 2023, Vancouver, Canada.

Zimmerman, Phil, Tracee Gilbert, Frank Salvatore 2019. "Digital Engineering Transformation across the Department of Defense," *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 16(4), October 2019.

APPENDIX C: DESCRIPTION OF ANCILLARY MATERIALS

The following is a list of all ancillary materials provided along with this report. As agreed to by DAU, these materials were delivered into the DAU Teams environment.

- SERC-2023-TR-007-A: Slide decks for
 - A.1 ENG 5520
 - A.2 ENG 5530
 - A.3 CYB 5610
 - A.4 CYB 5620
- SERC-2023-TR-007-B: Scripts for
 - B.1 ENG 5520
 - B.2 ENG 5530
 - B.3 CYB 5610
- SERC-2023-TR-007-C: Models, Model Views, Model Tracking
 - C.1 Firebird Model Updates (SERC-2023-TR-007-C.1 Firebird_2023-05-15.mdzip)
 - C.2 Bulldog Draft Model (SERC-2023-TR-007-C.2 Bulldog_Concise_2023-05-15.mdzip)
 - C.3 Firedog Draft Model (SERC-2023-TR-007-C.3 Firedog_Mission_Model_2023-05-15.mdzip)
 - C.4 Generic DEE model utilizing Firedog (SERC-2023-TR-007-C.4 Firedog_DE_Environment_2023-05-15.mdzip)
 - C.5 Silverfish Model using SCRE meta-model profiles (SERC-2023-TR-007-C.5 Silverfish-SCRE.7z)
 - C.6 STEDE model (SERC-2023-TR-007-C.6a STEDE.mdzip) and demonstration implementation (SERC-2023-TR-007-C.6b stede-db-0.1.tar.gz)
 - C.7 SE for d-Artifacts (SERC-2023-TR-007-C.7a SE for d-Artifacts.mdzip), SEP(v4) template (SERC-2023-TR-007-C.7b SEP Document Template.mdzip), SEpv3 template (SERC-2023-TR-007-C.7c SEpv3 Template.mdzip), Extract of views from mapping of adherence of Skyzer to SEpv4 required content (SERC-2023-TR-007-C.7d Skyzer SEpv4 test.pptx)
- SERC-2023-TR-007-D: Explanatory Documents

- D.1 5530 Wireframes (SERC-2023-TR-007-D.1 Wireframes.pptx)
- D.2 5530 Wireframes Excel Sheet (SERC-2023-TR-007-D.2 5530_model_wireframe.xlsx)
- D.3 Analytical Model Link Budget (SERC-2023-TR-007-D.3 Analytical_Model_LinkBudget.xlsx)
- D.4 Unique Model Views (SERC-2023-TR-007-D.4 Unique model views.pptx)
- SERC-2023-TR-007-E: Quick Start Guide (SERC-2023-TR-007-E WRT-1043_OY1QuickStartGuide.docx)
- SERC-2023-TR-007-F: Advisory Board
 - F.1 Advisory Board Presentations
 - F.2 Advisory Board Minutes
- SERC-2023-TR-007-G: Draft Videos
 - G.1 Digital Engineering Environment (SERC-2023-TR-007-G.1 DE Environment.mp4)
 - G.2 Digital Sign Off (SERC-2023-TR-007-G.2 Digital sign-off.mp4)
 - G.3 Cyber Terms (SERC-2023-TR-007-G.3 CyberSurvResSecTerms.mp4)
 - G.4 Circuit Breaker Example (SERC-2023-TR-007-G.4 MissionFocusedwithCircuitBreakerExample.mp4)

APPENDIX D: OVERVIEW OF SCORE

D.1 DEVELOPMENT AND DEPLOYMENT OF SCORE

The Systems Security Directorate, within the Office of Science and Technology Program Protection (STPP) under the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)), is actively pursuing the establishment of secure cyber resilient engineering practices. Secure Cyber Resilient Engineering (SCORE) refers to a systems engineering approach that effectively addresses the objectives of ensuring weapon system security and cyber resilience. This practice considers the challenges associated with operational domains such as air, land, maritime, space, and cyberspace, as well as the cyber-physical characteristics of weapon systems.

In fiscal year 2015, the Department of Defense (DoD) faced the imperative to enhance the resiliency of weapon systems and strengthen their cybersecurity during the design phase. Consequently, the need arose to define standards and identify engineering best practices for incorporating cyber resiliency into weapon systems. In 2017, the DoD acquisition policy outlined in document 5000.02 underwent revision, affording an opportunity to assign responsibility for engineering practices to the workforce. Specifically, the Technology and Program Protection directive (5000.83) transferred this responsibility from program managers to S&T managers and the engineering workforce, thereby presenting a chance to clarify the cyber-related considerations for the engineering workforce.

Launched in 2018 as a response to the call for integrating cyber into engineering practices, Secure Cyber Resilient Engineering (SCORE) aims to establish consistent methodologies, risk assessment procedures, and analysis approaches. Its objective is to incorporate secure cyber resilience principles into the engineering process from the outset. By equipping the systems security engineering workforce with the knowledge of designing systems and capabilities that are less vulnerable to cyber attacks and more resilient in the face of adversity, the risk of weapon systems being compromised by cyber events can be significantly reduced. Cyber resilience, distinct from simply focusing on minimizing the risk of cyber intrusions and attacks, involves the ability of a system to adapt to changing conditions and quickly recover from disruptions. SCORE practices encompass the necessary skills to specify, design, and implement systems while addressing the protection concerns arising in contested cyberspace. These protection concerns span the entire life cycle of the system, encompassing its enabling and supporting systems, the technology, data, and technical information associated with it, as well as maintenance, logistics, and the supply chain.

D.1.1 CYBERSECURITY AND CYBER RESILIENCE

Cybersecurity focuses on preventing adversaries from accessing system operations, while cyber resilience acknowledges the difficulty in easily thwarting advanced adversaries due to undetected vulnerabilities and weaknesses in system software. In the

event of a successful attack resulting from persistent threats, organizations must ensure the continuity of their essential functions despite any adverse impacts. Cyber resilience is defined as the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources. Operational resilience, as defined in DoDI 8500.01, is the system’s ability to resist, absorb, recover from, or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of capability to perform mission-related functions. Thus, resilience is concerned with assuring mission capability in the face of successful attacks. Achieving high levels of mission assurance can require a focus on enhancing cyber and operational resilience by incorporating engineered mechanisms and processes specifically designed to help the system recover from the attack.



Figure 22. The Development of the SCRE Initiative

Measuring the resilience of a system poses challenges. It requires intentional testing that introduces adversities capable of causing harm, destruction, or loss of mission-related functions during operation. Testing should encompass the measurement of system attributes, performance, and resulting effects, while considering the actions needed to resist, absorb, recover from, or adapt to the adversities.

Cyber resilience plays a crucial role in ensuring the continuity of essential functions in the presence of advanced adversaries and undetected vulnerabilities. It complements traditional cybersecurity measures by emphasizing anticipation, withstanding, recovery, and adaptation to adversities. Measurement of resilience requires intentional testing and evaluation of system attributes, performance, and defender actions. By prioritizing cyber resilience and implementing improved evaluation methods, organizations can enhance mission assurance and sustain critical operations despite persistent threats and successful cyber attacks.

D.1.2 SCRE STRUCTURE

The concept of Secure Cyber Resilient Engineering (SCRE) encompasses the integration of security and protection considerations throughout the lifecycle of military systems

operating in both physical and cyberspace domains. It encompasses a range of standards, specifications, methods, practices, techniques, and data requirements that are explicitly tailored to address security aspects in systems engineering activities and associated artifacts. The focus is on addressing both malicious and non-malicious adversity.

The fundamental idea behind SCRE is to enhance the resilience of weapon systems by providing them with a fight-through capability even when under attack. The goal is to "engineer in" resilience during the design phase and ensure its preservation throughout operations. Resilience can be thought of in terms of the loss of critical functions, the speed at which those functions can be restored, the magnitude of the functional loss, and the speed of recovery. It emphasizes the critical functions of the mission and the ability to absorb and recover from attacks.

SCRE can be described in terms of a discrete methodology whose building blocks (see Figure 23) can be translated into course modules for instructional purposes. One of these elements is Mission Aware, which provides a framework for architecting resilience and identifying engineering tradeoffs. Mission Aware focuses on incorporating engineered mechanisms for detecting and responding to potential cyber-attacks. Model-based systems engineering (MBSE) techniques can be employed during the early phases of conceptualization and requirements to specify patterns for these engineered mechanisms, which then inform requirements, architectural design, and verification and validation activities. Mission Aware is primarily applicable to cyber-physical systems, such as vehicles and weapons systems.

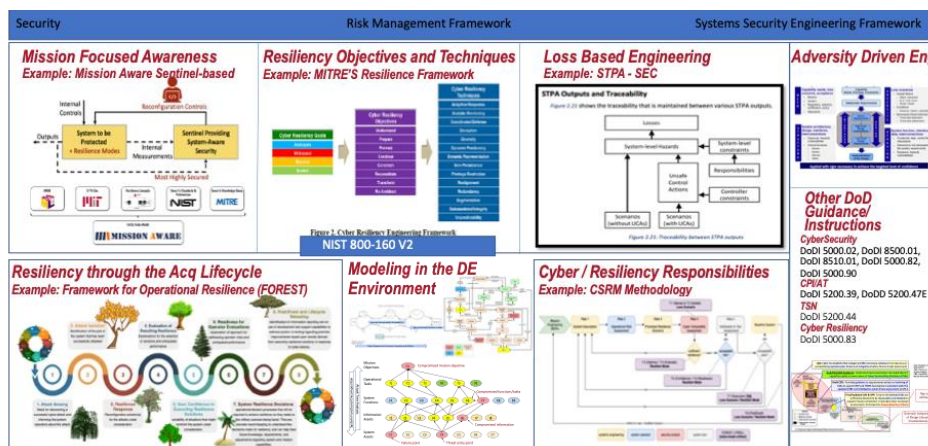


Figure 23. Building Blocks of SCRE

SCRE adopts a loss-based and adversity-driven engineering perspective that facilitates streamlined consideration of system functions that are critical and cannot be lost. The Cyber Security Requirements Methodology (CSRM) is introduced as a means of identifying resilience requirements during the initial design phase of physical system programs. CSRM provides a framework for implementing cyber defense and resilience solutions, as well as security-based software engineering solutions. Systems Theoretic Process Assessment (STPA) and STPA for Security (STPA-Sec) take a holistic approach

to considering hardware, software, and the operational environment in which systems interact and operate, in contrast to tactics-based, bottom-up approaches of other cybersecurity methodologies.

In summary, SCRE encompasses the integration of security and protection considerations throughout the lifecycle of military systems. It aims to engineer resilience into systems, enabling them to maintain critical functions even under attack. The course provides a comprehensive understanding of SCRE through various building blocks, including Mission Aware, CSRM, and STPA-Sec, each addressing specific aspects of resilience and cybersecurity. By adopting these methodologies, practitioners can enhance the resilience and security of systems, particularly in cyber-physical domains.

The Framework for Operational Resilience in Engineering and System Test (FOREST) is a comprehensive approach to enhancing cyber resilience as part of system development and testing. This methodology can be applied to any system-level resilience concerns and is not limited to just cybersecurity. Resilience is a crucial aspect of a system's functionality and thus requires a systematic evaluation of the system's various components under attack or disruption. This evaluation leads to the development of functional requirements and functional views of cyber resilience processes in an MBSE tool. The methodology comprises two main components, FOREST, a meta-process model, and Mission Aware, a reference architecture meta-model. These elements are used in the decision-making process for security and related resilience in capability development, utilizing a standard risk-based approach for cybersecurity requirements development. The FOREST methodology can be implemented early in system development, so that resilience, specifically cyber resilience, techniques can be introduced in early design phases and carried throughout the system lifecycle so when in operation, the system has baked-in resilience with traceable reasoning that can enable adaptation to evolving threats.

There are multiple aspects of the SCRE credential that bear on course design. This reporting period, SERC supported DAU on the development of three courses to address the needs of the workforce at the novice, beginner, and practitioner levels (see Figure 24). These three courses will be folded into an introductory SCRE credential (level 1) and a practitioner SCRE credential (level 2), which also encompasses currently taught courses, such as the Cyber Training Range. In the first course, the students will be walked through models that adequately explain why SCRE is needed via an online-only training course. The second course will have the students interact with and be led by an instructor through the models to better understand when and where throughout the lifecycle and phases. The third course will have students actively work in the models themselves, but with an instructor able to help when needed. This sandbox approach will provide the exposure needed to build confidence in each student. Especially in those that do not have a background in cyber, resilience, control engineering, or model-based systems engineering.

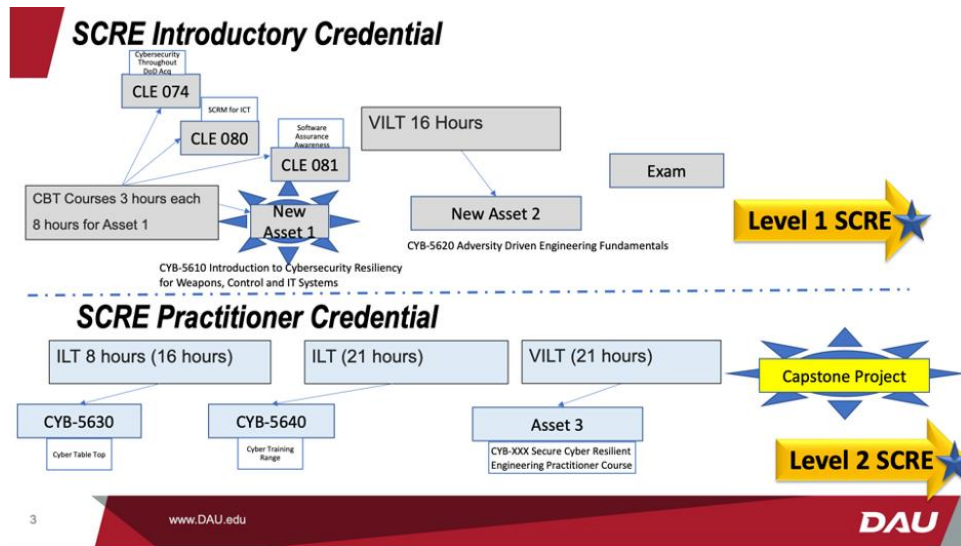


Figure 24. Breakout of Levels for SCRE Credentials

D.1.3 DEPLOYING THE CREDENTIAL

SERC researchers Tim Sherburne and Megan Clifford, in conjunction with DAU LAM Dr. Aaron Jacobson, created a Digital Almanac to illustrate the materials, discern gaps, and provide vision for enabling a student to work with live models while being guided on pertinent information. Unfortunately, most personnel from DAU cannot access due to firewall issues, however, it was necessary for leading discussions with faculty, potential SCRE students, and DoD driving forces. Dr. Jacobson is seeking to have GitHub and Jupyter Notebooks/Google Collaboratory notebooks be made available.

The Digital Almanac includes methodologies, frameworks, practices, and tools from the SCRE toolbox discussed below. It also has two working, real-time models within the Jupyter notebooks. The notebook is designed to walk through cyber resilience tasks – illustrating the CONOPS, system descriptions, control structure, risks, vulnerability assessments, and then designing in resiliency patterns. The exercises provide an example of how the SCRE curriculum can be achieved through the case study and its assets in model-based systems engineering.

The artifacts can be found at: https://colab.research.google.com/github/tsherburne/de-textbook/blob/main/content/01_SCRE_DE_Textbook.ipynb

D.1.4 DIGITAL ENGINEERING IN SCRE

The SCRE curriculum enables digital engineering. It has been designed so that it can properly teach MBSE and show the interoperability and connectivity amongst various ongoing efforts within a use case to achieve resilience. The research team reviewed the

ongoing SE Mod research task at SERC and noted that some of the pain points outlined in the project were being addressed (SERC research task report can be found [on the SERC website](#)). For instance, the SCRE courses start to mitigate the lack of use cases and exemplars with metrics.

The efforts of SCRE will continue to address needs and benefits for the wider efforts.

D.2 OVERVIEW OF SCRE CREDENTIAL

SCRE addresses the protection concerns of contested cyberspace that spans the entire life cycle of the system. This includes the entire life cycle of technology, data, and information associated with the system, which includes the maintenance, logistics, and supply chain. The SCRE courses aim to teach and foster aptitude in its participants and students towards a solution to achieve resilience using the same systems engineering processes that are commonly used when considering the systems attributes of safety, reliability, and survivability. The goal is to design in resilience, and develop measurable cyber requirements alongside performance, safety, and other “-ility” requirements while using common mitigation and recovery capabilities, regardless of cause.

At the time when the SCRE team joined the course production effort, the DAU Initial Design Solutions (IDS) documents were complete. In addition, the competencies and their terminal and enabling learning objectives were also written (TLO/ELOs). The SERC team then helped create derived ELOs to better trace specific learning capabilities and their artifacts throughout the courses. It also created a learning environment that promotes understanding through a build of information, rather than siloed modules and learning. This was done through an assessment of the courses by the SERC team. The assessment was then shared with the Learning Asset Manager (LAM). From there, the content and updated ELOs were iterated to ensure congruency. This was initially done through a shared Word document and Excel spreadsheet on Google Drive.

After the parallel iterations and assessments, the team decided that making the credentials as modular as possible would maximize the opportunity to make future changes economically. The modular design also enables the student to revisit specific, small sections of the course to better understand the content. In addition, the DAU and SERC team ran several exercises with existing material to ensure that the material was correct for the course and able to be threaded throughout each course and its corresponding modules. As this was done, the team created storyboards, by way of PowerPoint, scripts to go with the material (in the PowerPoint and separated to a Word document), drafts of video content (done through Celtx and PowerPoint), and knowledge review and exam questions.

The course development and levels are as follows:

- CYB 5610
 - Bloom's Level 1: Remember (Bloom 1956)

- The course will be static, foundational material for understanding with a walkthrough of various models.
- It is online learning and between four and six hours.
- The learning objective is that upon completion of the course, the DoD professional will be able to explain the foundational elements of SCRE within the DoD.
- CYB 5620
 - Bloom's Level 2: Understand (Bloom 1956)
 - The course will be more dynamic, with instructor-led "play" within the models.
 - This is a hybrid of online learning and instructor lead for two days.
 - The learning objective is that upon completion of this course, the DoD professional will be able to explain the elements of SCRE within the DOD based on provided scenarios.
- CYB 56XX
 - Bloom's Level 3: Apply (Bloom 1956)
 - This course will be dynamic with the ability to navigate and build models.
 - It is online and instructor lead training for two and a half days.
 - The learning objective will be that the DoD personnel will be able to apply principles that are crucial for successful secure cyber resilient engineering implementation and sustainment.

The DAU/SERC team recognizes that the solution space for achieving SCRE must be tailorable and that there are several methodologies to achieve the task at hand. Therefore, the team created a SCRE toolbox concept (Figure 25) to provide greater clarity on the areas and methodologies necessary to achieve SCRE, acknowledging that there are several frameworks, processes, and tools to achieve secure cyber resilience. There are also several significant DoD guidance documents, instructions, and white papers relevant to the credential.



Figure 25. SCRE Toolbox Concept

D.2.1 COMPETENCIES/TLO/ELOS

The competencies for the courses are outlined in Figure 28 below. CYB-5610 covers competency 13, while CYB-5620 covers competencies 13 through 15. The final course, CYB-56XX, will cover competencies 16 through 18.

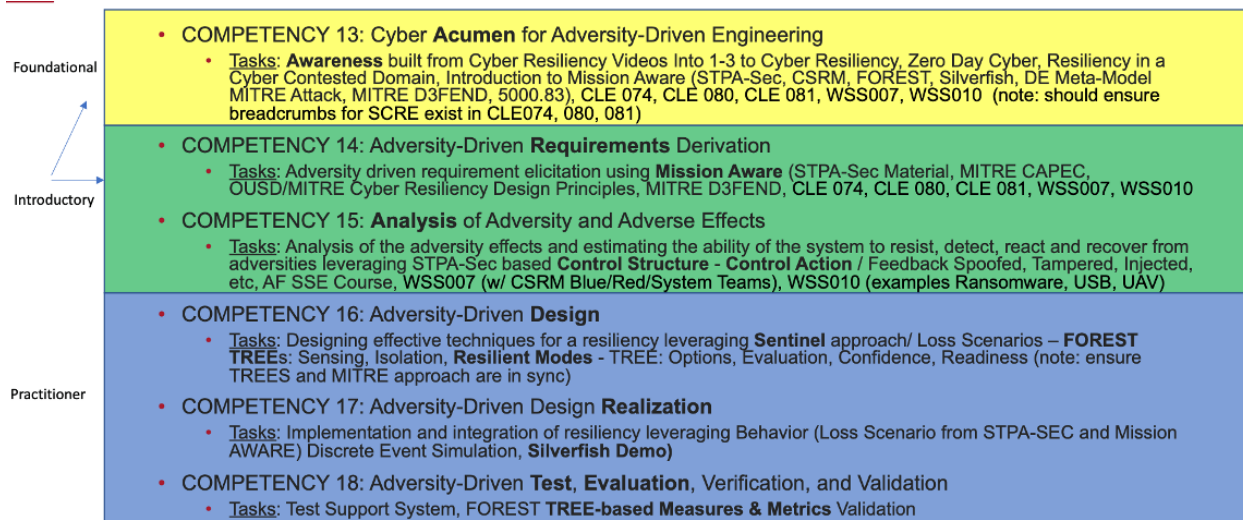


Figure 26. SCRE Competencies

The DAU and SERC teams, as previously mentioned, continue to work within the competencies, TLOs, and ELOs – continuously trace the materials and exercises to ensure the directives are being met.

	A	B	C	D	E	F	G	H
1	Key							
2	Denotes New ELOs with specific, traceable materials.							
3	Can be addressed, but maybe not wholly							
4	Denotes ELOs that will be accomplished at a later date.							
5	Competency TITLE, OUSD TLO	OUSD ELOS	Competency Performance Outcomes, ISD DAU	DERIVED ELOs (OUSD, DAU, SERC)	Corresponding Modules	Assessment Questions	Source	Source 2
6	<p>COMPETENCY 13 TITLE: Cyber Acumen for Adversity-Driven Engineering</p> <p>Acquire awareness and insights necessary to specify, design, and realize systems considering protection concerns within contested cyberspace span and considering the entire system life cycle.</p>	<p>1.1 Appraise/differentiate the purpose of principles/techniques for secure cyber resilient systems</p> <p>1.2 Identify/differentiate assets that provide secure resilient systems</p>	<p>Task 13.A: Appraise and differentiate the purpose and application of principles, concepts, and techniques for design of trustworthy secure and resilient systems, networks, and communications. (SCRE)</p> <p>Task 13.B: Identify and differentiate technologies, components, products, and services that provide secure</p>	<p>13.A.1 Student can identify difference between system assurance and system resilience.</p> <p>13.A.2 Student can identify directives where specific cyber issues are addressed (Guides, GAO reports)</p> <p>13.A.3 Student can determine statement that best identified how early cyber resiliency should be addressed in a system.</p> <p>13.B.1 Identify the security techniques that make up secure resilient systems 800-160 techniques.</p>	<p>0, 1</p> <p>0</p> <p>0, 1</p>	<p>13.A.1. Student can identify difference between system assurance and system resilience. The system resilience is agnostic to the particulars of attacks but assumes _____. (Answer: attacks will happen) (Exam)</p> <p>Multiple choice</p> <p>Fill in the blank</p> <p>Alternative: worded "but assumes attacks will _____" (Answer: happen)</p> <p>System assurance is defined as _____. (OR)</p> <p>Multiple choice</p> <p>To be effective in resilience engineering, you must be able to reason about _____ and _____. (Exam)</p> <p>Multiple choice</p> <p>System assurance is a _____ property while system resilience is a _____ property. (OR)(Exam)</p> <p>Multiple choice.</p> <p>Fill in the blank.</p> <p>In system assurance, the system "functions as _____" and is _____ of exploitable vulnerabilities." (OR)</p> <p>Multiple choice</p> <p>Fill in the blank</p> <p>System resilience is defined as _____. (OR)</p> <p>Multiple choice</p> <p>13.A.2. Student can identify directives where specific cyber issues are addressed (Guides, GAO reports) in the GAO, the National Cyber Security Director summarized the vision, challenge, path, and urgency to improve the nation's security. What was the vision? (Answer: the Office's goal is to engage in cyberspace such</p>	<p>Darty Video</p> <p>GAO Reports</p> <p>Acquisition Process Charts, Policies</p>	<p>a. Intro to Cyber F Resiliency Module 3 d. CROWS_Cyb (8042) e. Resilie f. Zero Day for Cy https://www.youtu ps://www.youtu</p>

Figure 27. Snapshot of Traced Competencies, TLOs, ELOs, and Derived ELOs to Materials

D.2.2 CYB 5610

The CYB 5610 course is designed to offer fundamental training for individuals new to the field of cybersecurity and resilience. Its primary objective is to equip DoD professionals with the foundational elements of SCRE and the requisite skill set to develop system protections within contested cyberspace throughout the entire system life cycle. The course targets individuals involved in decision-making, contract development, financial oversight, and other essential functions related to system acquisition. As the concept of resilience becomes increasingly foundational, the course is designed to evolve alongside emerging needs. It adopts a modular format, facilitating easy execution of updates to the course materials.

When designing the course, several assumptions were considered. Firstly, it was recognized that some participants may have no prior exposure to cyber, cyber resilience, or loss-driven engineering. Secondly, there may be participants who lack familiarity or understanding of digital engineering concepts. Thirdly, the asynchronous learning format employed in the course limits the opportunity for interactive and critical thinking exercises. Additionally, it was assumed that students would have the ability to access and navigate hyperlinks within the course materials to explore examples crucial for their comprehension of the subject matter and objectives.

CYB 5610 addresses the objectives outlined by OUSD TLOs in Task 13 (detailed listed below). It aims to enable participants to develop awareness, insights, and skills necessary for specifying, designing, and realizing systems within contested cyberspace. This includes understanding protection concerns associated with the computational, communication, and physical aspects (i.e., cyber-physical characteristics) of systems. The course emphasizes that protection concerns related to contested cyberspace span the entire life cycle of the system, its enabling and supporting systems, as well as the life

cycle of technology, data, and information associated with the system. It also encompasses considerations regarding maintenance, logistics, and the supply chain.

In summary, the CYB 5610 course provides foundational training in cybersecurity and resilience, with a specific focus on Secure Cyber Resilient Engineering (SCRE). It caters to DoD professionals involved in system acquisition and equips them with the necessary skills to address protection concerns within contested cyberspace throughout the system life cycle. The course accommodates various backgrounds and learning needs, ensuring that participants without prior exposure to related concepts can fully engage and benefit from the materials. The course aligns with the OUSD TLOs, specifically Task 13, by addressing the comprehensive protection concerns associated with contested cyberspace and cyber-physical characteristics of systems.

OUSD ELOs:

- 1.1 Appraise/differentiate the purpose of principles/techniques for secure cyber resilient systems
- 1.2 Identify/differentiate assets that provide secure resilient systems
- 1.3 Identify/differentiate attack methods/strategies used to produce adverse system effects
- 1.4 Identify/differentiate system vulnerabilities
- 1.5 Appraise/differentiate methods/approaches to provide confidence in secure resilient systems
- 1.6 Provide credible compelling argument for assurance of a secure cyber resilient system

The Initial Design Solution (IDS) document provided by DAU listed performance outcomes needed from CYB-5610 that is in alignment with the above DoD TLOs and ELOs. The performance outcomes for Task 13 are as follows:

1. Student identifies various techniques for designing secure and resilient solutions by utilizing modern techniques throughout the product lifecycle. (Task 13.A)
2. Student Identifies applicable emergent cyber solutions, principles, concepts, and techniques. (Task 13.B)
3. Student summarizes and differentiates the adverse conditions that impact traditional system, networks, and communication deficiencies. Student formulates appropriate requirements. (Demonstrate he/she can find weaknesses) (Task 13.C)
4. Student gives examples of exposure and likelihood of susceptibilities. The student will develop the skills needed to conduct vulnerability assessments. (Task 13.D)
5. Student will describe the needs of the organization and ability to achieve secure and resilient systems. Student will distinguish between various defensive approaches and determine best approaches given organization's constraints. (Task 13.E)

6. Outline risk mitigation strategies to the Adaptive Acquisition framework and cyber activities throughout the acquisition lifecycle (engineering V) to show complete Cyber traceability of all requirements to include Test and Evaluation. (Task 13.F)

As it states in Special Publication 800-160 volume 2 from the National Institute of Standards and Technology, “If you don’t have awareness of cyber-attacks, then you don’t know when to enact a resilient mode.” The first course within the credential enables foundational understanding and awareness of cyber-attacks.

D.2.3 CYB 5610 MODULES

The CYB 5610 course consists of five modules that cover various aspects of SCRE and its application in weapon systems. Throughout the design and iteration of these modules, careful consideration was given to the included materials, with a focus on addressing potential missing areas. As the course evolved, the team actively sought feedback from key stakeholders, including the DAU faculty, the WRT-1043 Advisory Board, the Cyber Resilient Weapon Systems panel, and INCOSE. These engagements helped shape the course and confirmed the team’s alignment with industry standards and best practices.

The introduction module provides an overview of SCRE policy and the core components of SCRE. It sets the foundation for understanding the importance of resilience and its application in the context of weapon systems. Module 1 delves into the threats faced in the cyber domain, emphasizing the need to move beyond a perimeter-based approach to achieve resiliency.

Module 2 focuses on terminology, examining its relevance to weapon systems, IT systems, and control systems. It highlights the interconnectedness of these domains and the importance of ensuring that all members of the acquisition workforce understand their roles and contributions to achieving cyber resiliency.

In Module 3, various frameworks are explored, including Mission Aware Terminology, Loss Based Engineering, MITRE DEFEND, NIST 800-160 V2, RMF, and the Cyber Survivability attributes. This module provides insights into integrating resiliency into the acquisition lifecycle, including incorporating resiliency requirements into contracts.

The final module takes students through a practical example that leverages Model-Based Systems Engineering (MBSE) to demonstrate how resilience modes and remediations can be integrated into the control flow of a system. This module provides a hands-on experience, reinforcing the application of SCRE concepts in real-world scenarios.

Throughout the course development process, the team utilized PowerPoint storyboards to capture the distinctive derived Expected Learning Outcomes (ELOs) (see Figure 28). This robust format facilitated collaboration and ensured that each team member had the opportunity to contribute and reach consensus on the course’s forward steps, guaranteeing that the course is designed to provide optimal capabilities for the students.

CVB-5610, Workshop

Derived ELOs, Task 13.A

Task 13.A: Student identifies various techniques for designing secure and resilient solutions by utilizing modern techniques throughout the product lifecycle.

- 13.A.1** Student can identify difference between system assurance and system resilience.
- 13.A.2** Student can identify directives where specific cyber issues are addressed (Guides, GAO reports).
- 13.A.3** Student can determine statement that best identified how early cyber resiliency should be addressed in a system.

Derived ELO	Module(s) Addressed	SOURCE Material*
13.A.1	0, 1	Darty Video (SERC)
13.A.2	0	GAO Reports
13.A.3	0, 1	Acquisition Process Charts, Policies

*Source material noted is the largest portion of source material where the Derived ELO is addressed. The answers can come from other portions of the course content, too.

Knowledge Review and Exam Questions

- 13.A.1. Student can identify difference between system assurance and system resilience.
 1. The system resilience is agnostic to the particulars of attacks but assumes _____. (Answer: attacks will happen) (Exam)
 - Multiple choice
 - Fill in the blank
 - Alternative: worded "but assumes attacks will _____." (Answer: happen)
 2. System assurance is defined as _____. (KR)
 - Multiple choice
 3. To be effective in resilience engineering, you must be able to reason about _____, _____, and _____. (Exam)
 - Multiple choice
 4. System assurance is a _____ property while system resilience is a _____ property. (KR)(Exam)

Figure 28. Snapshot Example of Built Storyboard for CYB 5610

D.3.3 CYB 5620

For CYB 5620, there will be several approaches to the learning modules. The student will find requests in the model as opposed to updating the model, which will cause the student to find and answer multiple-choice questions after analyzing the model. In addition, there will be a completed model, traversed to the Cyber Resilience Requirements Model (CRRM), with then pieces removed for students to acknowledge and update themselves.

The course will be delivered in two days of course time and is outlined below, with the assumed prerequisites being a digital engineering primer and CYB 5610:

1. What is a pipeline?
 - a. Overview of oil and gas pipeline infrastructure
 - b. Understanding the importance of cyber resiliency in pipeline operations.
2. Model of the pipeline components, functions, behaviors
3. Pipeline - Just attacked by Fuzzy Bear attacker named Sven.
 - a. Discuss scenarios of what would be a global threat.
 - b. Risk analysis techniques for identifying and assessing security risks in pipeline systems.
 - c. Incorporating risk analysis into the STPA SEC framework.

4. Main Objective: Learn STPA SEC
 - a. Detailed explanation of the STPA SEC process and its components
 - b. System boundary definition and identification of security-related hazards
 - c. Functional analysis and identification of potential security threats
5. Model of the pipeline components, functions, behaviors, and **adversity**
 - a. Defining security requirements and objectives based on system functions and hazards.
 - b. Mapping security requirements to system elements and components
 - c. Ensuring compliance with applicable regulations and standards.
 - d. Identification and evaluation of security controls to mitigate threats and vulnerabilities.
 - e. Selection and implementation of appropriate countermeasures for pipeline security.
 - f. Integration of security controls into the pipeline infrastructure and operational processes.

Here is an example of a written scenario for use in the course:

Loss: Manipulated Sensors
Attack Method: Use MITRE ATTACK

A threat actor named Sven, employed by Fuzzy Bear, hatched a nefarious plan to disrupt the operations of a highly advanced ground-based system called Silverfish. Equipped with knowledge of the MITRE ATT&CK framework, Sven meticulously studied the vulnerabilities and attack vectors inherent in the system.

Under the cover of darkness, Sven began the initial phase of his attack: reconnaissance. He scoured open-source intelligence, scrutinized technical documentation, and observed the drone's behavior during routine operations. Sven sought to identify weaknesses that he could exploit to gain control over the drone's vital functions.

Armed with valuable intelligence, Sven moved on to the next stage of his plan—weaponization. Drawing upon his deep understanding of the MITRE ATT&CK framework, he crafted a meticulously designed payload capable of exploiting specific vulnerabilities within the drone's firmware and communication protocols. This payload would serve as the key to infiltrating the drone's defenses and gaining unauthorized access.

With his weaponized payload prepared, Sven initiated the delivery phase. Through cunning social engineering techniques and carefully crafted

phishing emails, he targeted the drone's operators and maintenance personnel. His goal was to trick them into unwittingly executing the payload, thus providing him with a foothold within the drone's system.

Once inside, Sven maneuvered to establish command and control over the drone. He carefully navigated the drone's network, leveraging various MITRE ATT&CK techniques such as privilege escalation and lateral movement to gain deeper access and control over critical subsystems. His ultimate aim was to manipulate the system's controls and sensor data, rendering it ineffective or even hazardous.

As Sven manipulated the drone's systems, the drone's operators grew suspicious of its erratic behavior. They initiated their incident response protocols, activating monitoring systems and analyzing network traffic for anomalies. Their expertise in the MITRE ATT&CK framework allowed them to quickly recognize the signs of an ongoing attack, and they focused their efforts on identifying the source and mitigating the threat.

The operators successfully isolated the compromised sections of the drone's network, cutting off Sven's access and preventing further damage. They meticulously analyzed the attack, identifying the MITRE ATT&CK techniques employed by Sven and developed countermeasures to safeguard against future similar attacks.

Sven's attempt to compromise the ground-based system had been thwarted, thanks to the expertise of the engineering team. They understood the criticality of cyber resiliency and are prepared to thwart attacks and implemented continuous monitoring of their system with robust incident response capabilities.

Model Exercises:

Participants will engage in a practical MBSE exercise where they will apply Adversity driven engineering methodologies to a simulated oil and gas pipeline. The project will involve identifying and analyzing security risks, developing security requirements, and designing an effective, secure, and cyber-resilient approach for the pipeline system. By the Module, participants will possess a solid understanding of adversity-driven engineering applied to a control system and will be equipped with the skills necessary to systematically analyze security risks, design robust security measures, and ensure other control systems and systems such as Enterprise IT systems and Weapon systems are secure and resilient from adversity.

Exercise 1 (30 minutes)

- Class walks through the oil and gas pipeline infrastructure
- Discuss Model of the pipeline components, functions

Exercise 2 (30 minutes)

- Discuss behaviors and adversity.
- Show specific instance of where the specific attack occurred in the control flow
- Discuss Risk analysis techniques for identifying and assessing security risks in pipeline systems.

Exercise 3 (2 hours)

- Defining security requirements and objectives based on system functions and hazards.
- Mapping security requirements to system elements and components
- Ensuring compliance with applicable regulations and standards (e.g., map to 5000.83, RMF, ZT, CSAs)
- Identification and evaluation of security controls to mitigate threats and vulnerabilities.
- Selection and implementation of appropriate countermeasures for pipeline security (e.g., 800-160v2r1)
- Integration of Resiliency controls into the pipeline infrastructure and operational processes

There are several defined MBSE examples that DAU will be integrating into course work (e.g., Silverfish, oil/gas pipeline, UAV, Bulldog, Photon Torpedo). One or more will be visible across most of the modeling centric courses; however, for SCRE, the Silverfish and oil/gas pipeline models are the most mature.

Module development is still underway for CYB 5620, but storyboards that address the DoD tasks and competencies have been developed (see Figure 29).



SCRE Storyboard
Presentation for DAU
focusing on
Competency Areas 13, 14,
& 15
Silverfish Update, Apr 17,
2023


Storyboard focus areas for this presentation	Setting the storyboard stage
<ul style="list-style-type: none"> • SCRE Competency Areas focusing on: <ul style="list-style-type: none"> • 13 Cyber Acumen for Engineering • 14 Adversity-Driven Requirements Derivation • 15 Analysis of Adversity and Adverse Effects <p><small>Added as update 13C, 14C April 17, 2023, Slide 32</small></p> <p><small>Focus of the stories in this presentation provide examples of 9 of the 17 Competency tasks in the 3 Competency areas</small></p>	<ul style="list-style-type: none"> • In this story we want to explain how your effort as a Lead Systems Engineer, together with your team, is affected. • What we are going to be giving you in this story are examples of additional tools that can help you do your job more effectively specifically in the area of ensuring the system to be developed is adequately cyber-resilient given the cost, schedule and performance requirements for your program. • In the past, too often, the type of thinking presented in this storyboard has been an after-thought rather than integrated and "tasked-in" through the normal weapons systems engineering process. 

Figure 29. Storyboards for SCRE, CYB 5610 and 5620

D.3.3.1 SUPPORTING SERC MODELS AND EFFORTS

The SERC has provided materials, use cases, scripts, videos, methods, processes, and tool understanding for the support and design of the courses. It also helped that each member of the team has taught some aspect, whether through coursework, conferences, or briefs, the materials chosen and available for development.

D.3.4 CYB56XX

CYB 56XX is designed for the practitioner. While it is can be difficult to achieve Bloom’s Level 3 in online training, the assumption is that the student is not only exposed to modeling and cyber within the course but is already a practitioner to some extent. Therefore, the course is equipping the student with a better understanding of how to design in cyber resilience as far to the “left” of the vee-model as possible, i.e., as early in the lifecycle as is feasible. The target audience is the DoD professionals that are planning to implement SCRE and be able to apply crucial principles for implementation and sustainment.

The immediate need is the completion of the two previous courses; however, the team has outlined some pertinent information concerning the course and have been able to identify areas where the storyboards best suit this credential over the other two.

D.3.5 TRACEABILITY THROUGH MODULES, KNOWLEDGE REVIEW AND EXAM QUESTIONS, AND STORYBOARDS/MODELS

The DAU and SERC teams created a shared drive to work collaboratively and efficiently on the materials for the credential. Documentation in the storyboards and Excel spreadsheets ensured the derived ELOs were addressed in the various modules and that there is traceability to the source material within each. Every knowledge review and exam question are also traced to the source material and its specific module. This has been completed in totality for CYB-5610 and initiated for CYB-5620. The workflow will continue into the final CYB-56XX course.

D.3.6 SCRE FUTURE DIRECTIONS AND NEEDS

The DAU and SERC teams are currently working with the course designers and video production teams provided by DAU. The teams meet weekly and provide updates their respective tasks. Support for workshops and the launch of the credentials are needed, specifically with technical designers and leaders contracted by DAU.