Training the DoD Acquisition Workforce in Secure Cyber Resilient Engineering:

Using a Storyboard and Model Based Systems Engineering Approach in the Defense Acquisition University Credential Program

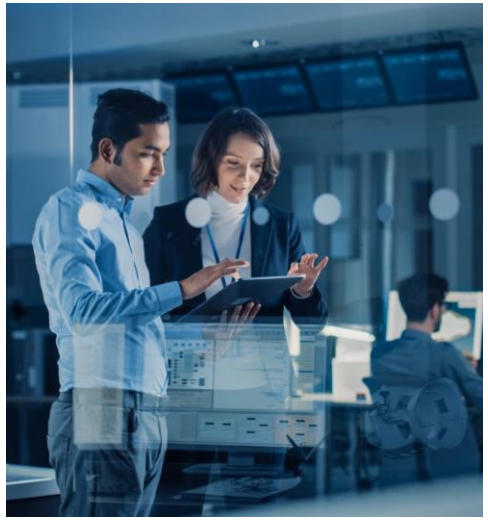
Mr. Paul E. McMahon, Mr. Burhan Adam
Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)
Dr. Aaron Jacobson
Professor of Cybersecurity
Defense Acquisition University (DAU)

NDIA Systems and Mission Engineering Conference
Norfolk, VA
October 29, 2024

Agenda

- Background
- Requirements & Defense Acquisition University (DAU) Secure Cyber Resilient Engineering (SCRE) Credential Program
- About the Story
- Setting the Story Stage and Last Year at the Conference
- Examples of Processes & Principles Used in the Story
- Examples of Improved/Added Wording in SCRE Competency Tasks
- Deeper Dive into the DAU Courses
- Next Steps & Questions
- Points of Contact

Background



- **About this Presentation:** Progress update on OUSD(R&E) collaboration with DAU on DAU's SCRE Credential Program using a Storyboard and Model Based Systems Engineering (MBSE) Approach
- **Purpose of Storyboard:** Demonstrate through easy-to-understand examples the 28 SCRE Competency Tasks in the 6 DoD Acquisition Workforce SCRE Competencies
- **Purpose of Presentation:** Update on how Storyboard and Model Based Systems Engineering (MBSE) being used within the SCRE Credential Program
- **Story Perspective:** Lead Systems Engineer and Team

Not giving you a new methodology, but rather additional tools to help the lead engineer and team increase their job efficiencies

Requirements & DAU SCRE Credential Program

- **Requirements: Demonstrate 6 SCRE Competencies**
  - Acquire Cyber Awareness — *Introductory*
  - Adversity-Driven Requirements Derivation — *Intermediate*
  - Analysis of Adversity — *Intermediate*
  - Adversity-Driven Design — *Advanced*
  - Adversity-Driven Design Realization — *Advanced*
  - Adversity-Driven Test, Evaluation & Verification & Validation — *Advanced*

More on credential requirements later

- **SCRE Credential New Courses**
  - CYB 5610 Introduction/Awareness — Online, 4 hours
  - CYB 5620 Adversity-Driven Fundamentals, Instructor led, 2 days
  - CYB 5621 SCRE Practitioner Credential — Future

Credential
Introductory
Intermediate
Advanced

Where applicable, parts of the storyboard are used throughout the 3 courses

About the Story

- **The System:** Silverfish is a fictional set of unmanned ground vehicles (UGV) controlled by a single remote operator
- **Purpose of System:** To deter and prevent adversaries from trespassing into a designated geographic area near a strategic sensitive area
  - The system in our story is being upgraded for use in hostile enemy environments where the risk to friendly troops exists
- **Program in Story:** The program is planning to reuse the existing legacy Silverfish system, which includes some, but not all, of the requirements necessary for the new system

One new requirement: Ensure new system is cyber resilient. Other new requirements: Add mine detector and laser designator to target mobile enemy vehicles

Setting the Story Stage

- The lead systems engineer has the responsibility together with their team, in accordance with Department of Defense Instruction (DoDI) 5000.83, to conduct SCRE including "deriving stakeholder adversity driven concerns to protect against unacceptable loss" which will be used as an input to the requirements derivation process and the "definition of protect-oriented design constraints consistent with existing agreements and regulations."

At this conference last year, we provided a few simple examples of how the lead engineer achieves their responsibilities

Examples of Processes & Principles Used in the Story

- System Theoretic Process Analysis for Security (STPA-Sec): Top-down, loss-based approach that identifies unacceptable losses
  - Used to demonstrate Principles/Techniques*: Loss/Hazard Analysis, Protective System Control, Loss Scenarios
- Assurance Case: A structured argument that demonstrates that a stated claim is, or will be, satisfied
  - Used to demonstrate Competency Task: Develop “credible & compelling arguments" for added features
  - Used to demonstrate Principles/Techniques*: Redundancy, Diversity, Encryption, Anomaly Detection, Alerts, Distributed Privilege
- Risk Assessment: Includes tradeoffs conducted to ensure agreed criteria in story met and protections are commensurate
  - Used to demonstrate Principle/Technique*: Commensurate Protection

*Reference: Loss Control Design Principles & Protection Nucleus Cyber Resilience Weapons Systems (CRWS) White Paper
Note: *Similarities to 14 techniques in NIST 800-160 v2 & Cyber Survivability Attributes (CSAs)*

Examples of improved/added wording in SCRE Competency Tasks

- Change word “protection” to “loss”
  - Example: Acquire and develop awareness, insights, and skills necessary to specify, design, and realize systems given the **loss** concerns
- Changing phrase “record and report” to “use”
  - Example: **Use** adversity related tech data for decision-making.
- Change word “optimal” to “sufficient”
  - Example: Select a system design that is **sufficient** in achieving security/resilience objectives”
- Change word “optimal” to “appropriate”
  - Example: Select **appropriate (informed by cost, schedule, performance objectives**) methods/processes for security and resilience

SCRE Learning Paths

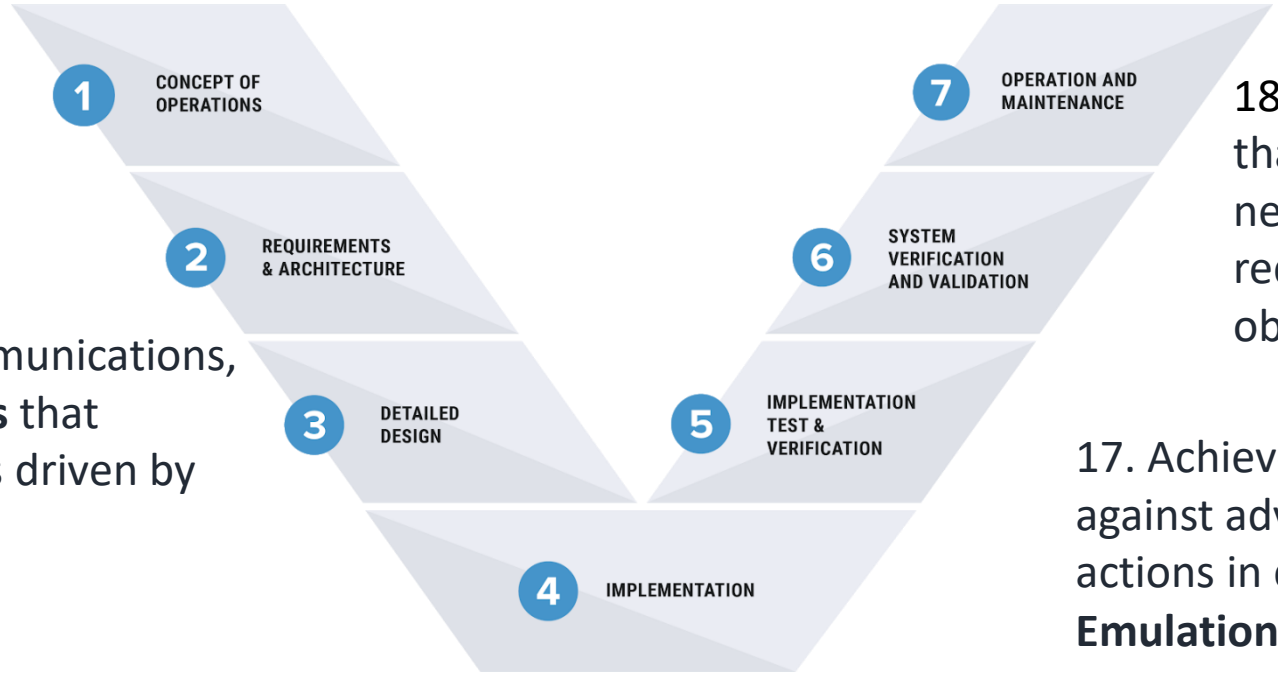
CCYB-003 Introductory SCRE Learning Path	CCYB-004 Intermediate SCRE Learning Path	CCYB-005 Advanced SCRE Learning Path
• CLE-074 Cybersecurity throughout DoD Acquisition CLE 074 | www.dau.edu • CLE-080 Supply Chain Risk Management for Information Communications and Technologies (ICT) CLE 080 | www.dau.edu • ENG-0810 Software Assurance ENG 0810 | www.dau.edu • CYB-5610 Introduction to Cybersecurity and Resiliency of Weapons, Control and IT Systems CYB 5610 | www.dau.edu • Credential Capstone (Fielded)	• CYB-5630V Cyber Table-Top CYB 5630V | www.dau.edu • CYB-5640 CYB 5640 | www.dau.edu or CYB-5640V CYB 5640V | www.dau.edu Basic Cyber Training Range with Enterprise IT and Weapon System • CYB-5620V Adversity Driven Engineering CYB 5620V | www.dau.edu • Credential Capstone (Fielded)	• Critical Infrastructure Cyber Training Range - New • CYB-5621 SCRE Engineering • Credential Capstone Not Deployed

Paradigm shift to ensure weapon systems, IT systems, and Control systems are Secure and Resilient to fight through a cyber-attack.
CCYB-003 credential provides the DoD professional with the foundational elements of SCRE within the DoD.
CCYB-004 credential provides an intermediate level look at adversarial cyber threats to DOD networks, weapon systems, and Industrial Control Systems leveraging a loss-based system engineering approach using hands-on Cyber Training Ranges and MBSE Cyber

SCRE - Engineering Activities

13. Awareness to specify, design, and realize systems considering protection concerns within contested cyberspace

14. Generate system, communications, and network **requirements** that accurately reflect concerns driven by contested cyberspace



15. Adversity-driven **technical data** about system, communication, and network behaviors and outcomes that is sufficient to inform life cycle engineering, programmatic, and risk decisions

16. Effective **design** for realization that is effective against adversarial and non-adversarial actions in cyberspace (FOREST** Trees, Sentinels, Assurance Cases)

17. Achieve design intent for effectiveness against adversarial and non-adversarial actions in cyberspace (**Simulations, Emulations)**

18. Develop evidence to substantiate that the system, communications, and network design fulfils its specified requirements and its mission objectives in cyberspace

* Numbers 13-18 refer Engineering & Technical Management Functional Area Tier 2 Competencies assigned to SCRE

** FOREST stands for Framework for Operational Resilience in Engineering and System Test

DoD Cyberspace Workforce Framework (DCWF)

In addition to the ETM Career Field

CYBER IT
OPR: DoD CIO

- (411) Technical Support Spec.
- (421) Database Administrator
- (431) Knowledge Mgr.
- (441) Network Operations Spec.
- (451) Systems Administrator
- (632) Systems Developer
- (641) Systems Requirements Planner
- (651) Enterprise Architect
- (661) Research & Development Spec.
- (671) System Testing & Evaluation Spec.

CYBERSECURITY
OPR: DoD CIO

- (521) Cyber Def. Infrastructure Support Spec
- (622) Secure Software Assessor
- (631) Information Systems Sec. Developer
- (652) Security Architect
- (462) Control Systems Security Specialist

CYBER EFFECTS
OPR: PCA

- (112) Mission Assessment Spec.
- (121) Exploitation Analyst
- (131) Target Developer
- (132) Target Network Analyst
- (141) Warning Analyst
- (321) Cyber Operator
- (332) Cyber Operations Planner
- (333) Partner Integration Planner

Three unlisted Cyber Work Roles are not for public release (CUI)

INTEL (CYBER)
OPR: USD(I&S)

- (151) Multi-Disciplined Language Analyst
- (111) All-Source Analyst
- (311) All-Source Collection Mgr.
- (312) All-Source Collection Requirements Mgr.
- (331) Cyber Intelligence Planner

AI/DATA
OPR: CDAO

- (902) AI Innovation Leader
- (733) AI Risk & Ethics Specialist
- (623) AI/ML Specialist
- (672) AI Test & Evaluation Specialist
- (753) AI Adoption Specialist
- (903) Data Officer
- (424) Data Steward
- (653) Data Architect
- (624) Data Operations Specialist
- (423) Data Scientist
- (422) Data Analyst

SOFTWARE ENG
OPR: R&E

- (621) Software Developer
- (628) Software/Cloud Architect
- (461) Systems Security Analyst
- (627) DevSecOps Specialist
- (625) Product Designer User Interface (UI)
- (626) Service Designer User Experience (UX)
- (806) Product manager
- (673) Software Test & Evaluation Specialist

CYBER ENABLERS (OPR: DoD CIO)
Support/facilitate the functions of other Cyber Workforce Categories

Leadership: (732) Privacy Compliance Mgr.; (751) Cyber Workforce Dev. & Mgr.; (752) Cyber Policy & Strategy Planner; (901) Executive Cyber Leader

Training & Education: (711) Cyber Instructional Curriculum Developer; (712) Cyber Instructor

Legal/Law Enforcement: (211) Forensics Analyst; (221) Cyber Crime Investigator; (731) Cyber Legal Advisor

Acquisition: (801) Program Mgr.; (802) IT Project Mgr.; (803) Product Support Mgr.; (804) IT Investment/Portfolio Mgr.; (805) IT Program Auditor

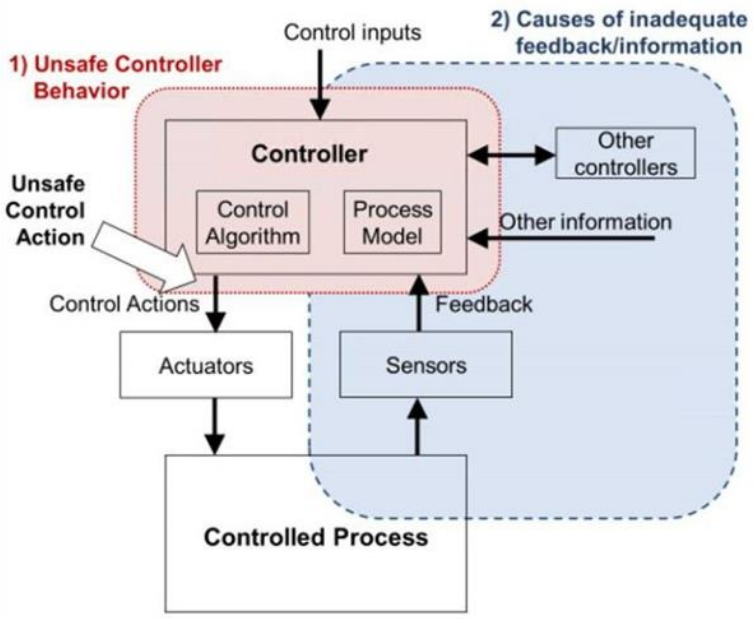
Ref DoDD 8140.01

ETM = Engineering Technical Management

Ref: Elements Map (NIPR) (cyber.mil)

CYB-5610V Cybersecurity & Resiliency for Weapons, and IT Systems

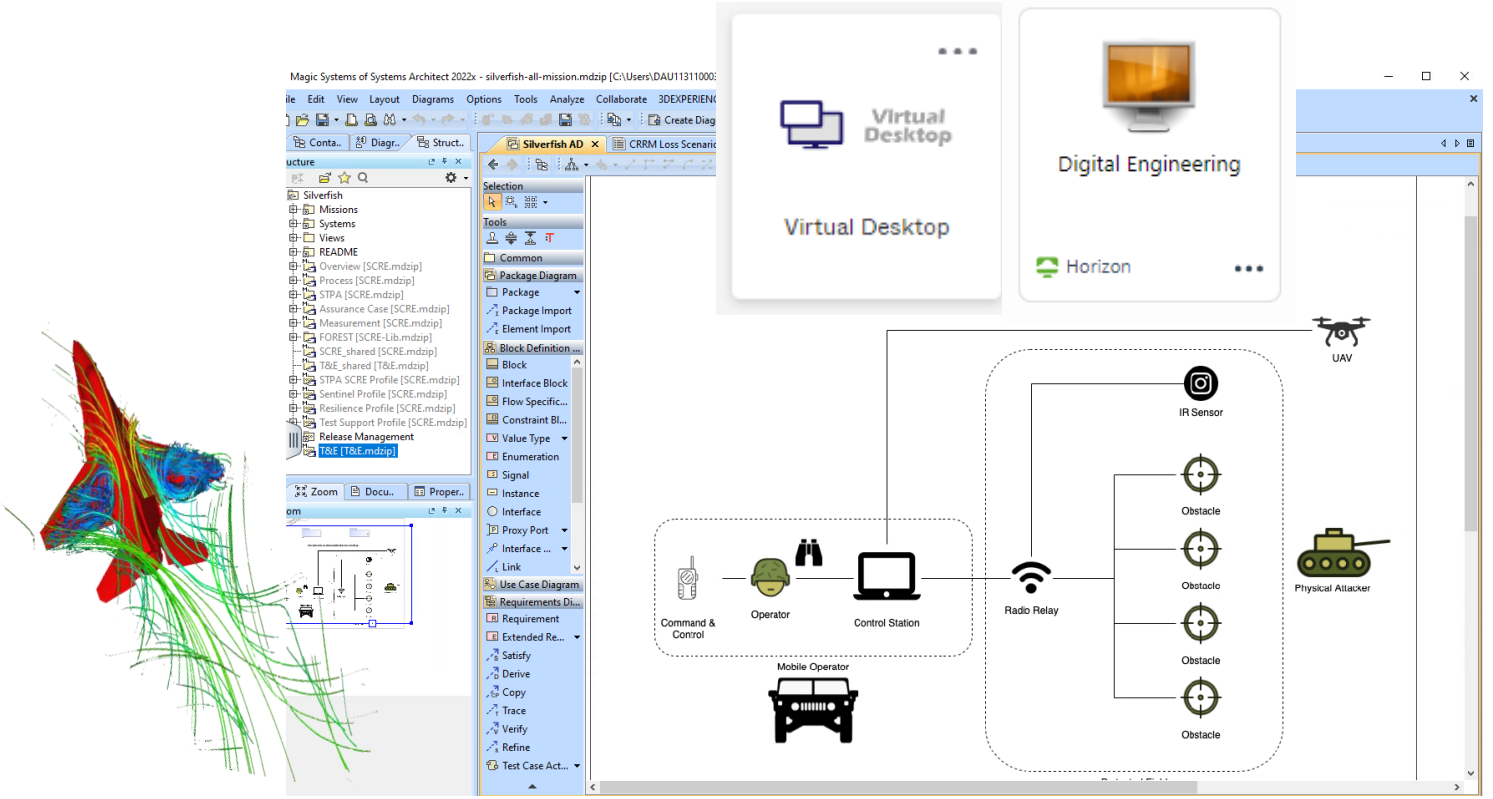
- Gain expertise in the fundamental principles of SCRE with DAU's online training opportunities
- The Cybersecurity & Resiliency for Weapons, Control and Information Technology (IT) Systems course, offers an important paradigm to ensure systems can fight through a cyber attack. [CYB 5610 | www.dau.edu](www.dau.edu)
- Mindset change to Engineering-in Security and Resiliency by addressing adversity



CYB-5620V – Adversity Driven Engineering

The DAU infrastructure incorporates the Model Based Systems Engineering (MBSE) environment to offer a structured, visual, and simulated learning experience, effectively preparing trainees for real-world cyber challenges. The course is a ground-breaking new approach to teaching Cyber. This Virtual instructor-led course uses a MBSE tool to provide a realistic problem space for incorporating security and resiliency into the engineering process. This course combines many realistic examples from UAVs to Critical Infrastructure pipelines, to IT Enterprise Systems.

Virtual Instructor Led Training



This course provides an environment for the student to interpret Mission Driven requirements based on the System Theoretic Process Analysis to address the loss of a given mission in a Cyber Contested environment. **For more information: Aaron.Jacobson@DAU.edu**

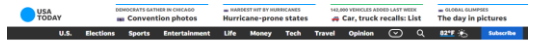
UAV = Unmanned Aerial Vehicle

Learn SCRE with us using MBSE!

Supported MBSE Training with Hands-on CTRs

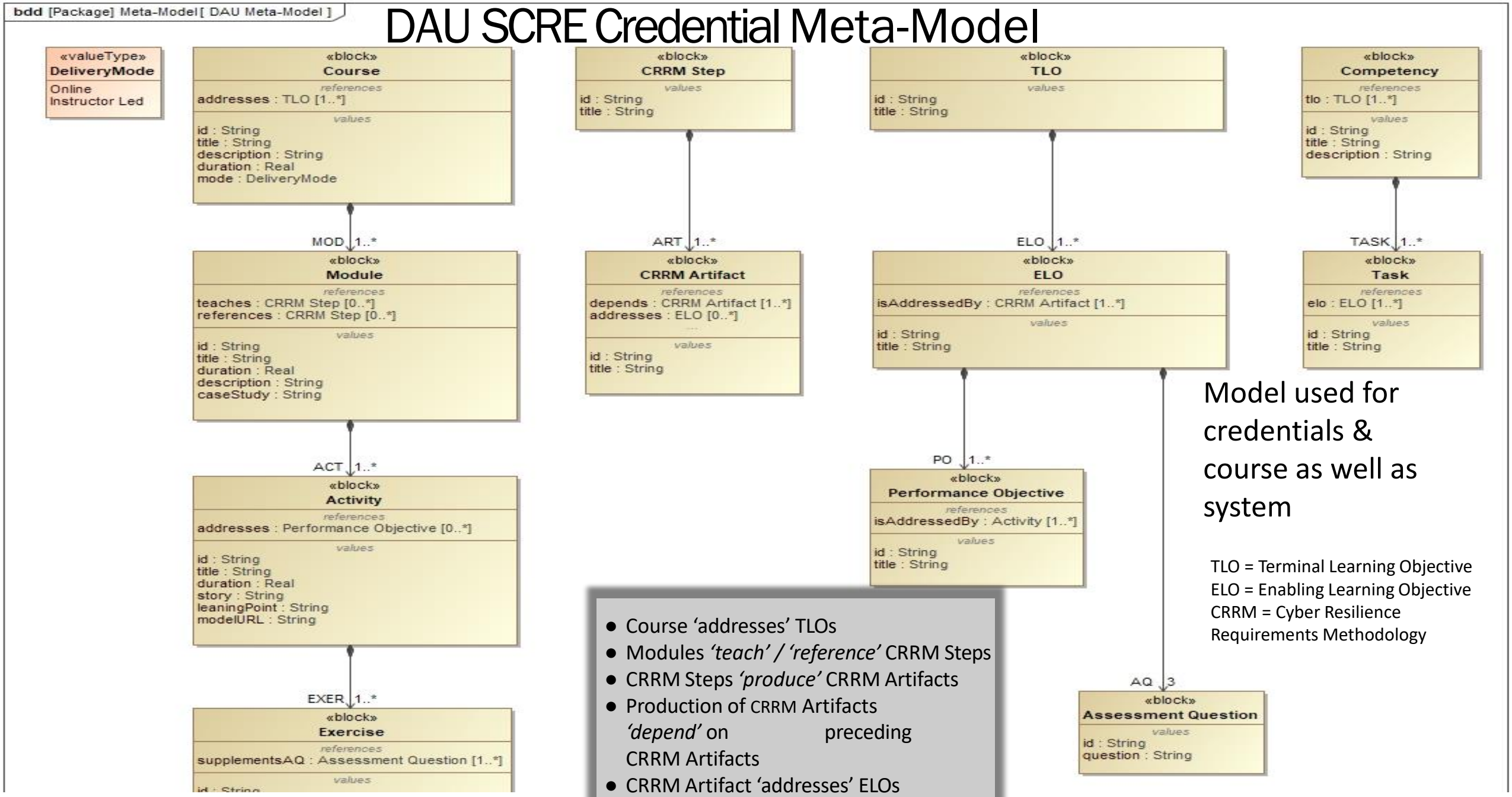
- The Cyber Training Range – hands on laboratory exploration of cyber threats to Critical Infrastructure Systems, Aviation Systems, and Enterprise IT Systems
- Embedded attacks include UAS* Datalink jamming, ICS* Modbus attacks, buffer overflow attacks, Embedded Device security, and Mil-std 1553 and MAVLINK sniffing, spoofing, and attacking
- Workshops are deployed as virtual self paced workshop with office hours available for support, instructor led workshops, and classroom workshops designed for students to develop cyber countermeasure design requirements, design solutions and testing approaches to improve security and resiliency in the modern cyber contested battlefield, leveraging Capture the Flag assessments

*ICS = Industrial control system *UAS = Unmanned Aircraft System



Complementary hands-on activities support SCRE learning

DAU SCRE Credential Meta-Model



- Course ‘addresses’ TLOs
- Modules *‘teach’ / ‘reference’* CRRM Steps
- CRRM Steps *‘produce’* CRRM Artifacts
- Production of CRRM Artifacts *‘depend’* on preceding CRRM Artifacts
- CRRM Artifact ‘addresses’ ELOs

Model used for credentials & course as well as system

TLO = Terminal Learning Objective
ELO = Enabling Learning Objective
CRRM = Cyber Resilience Requirements Methodology

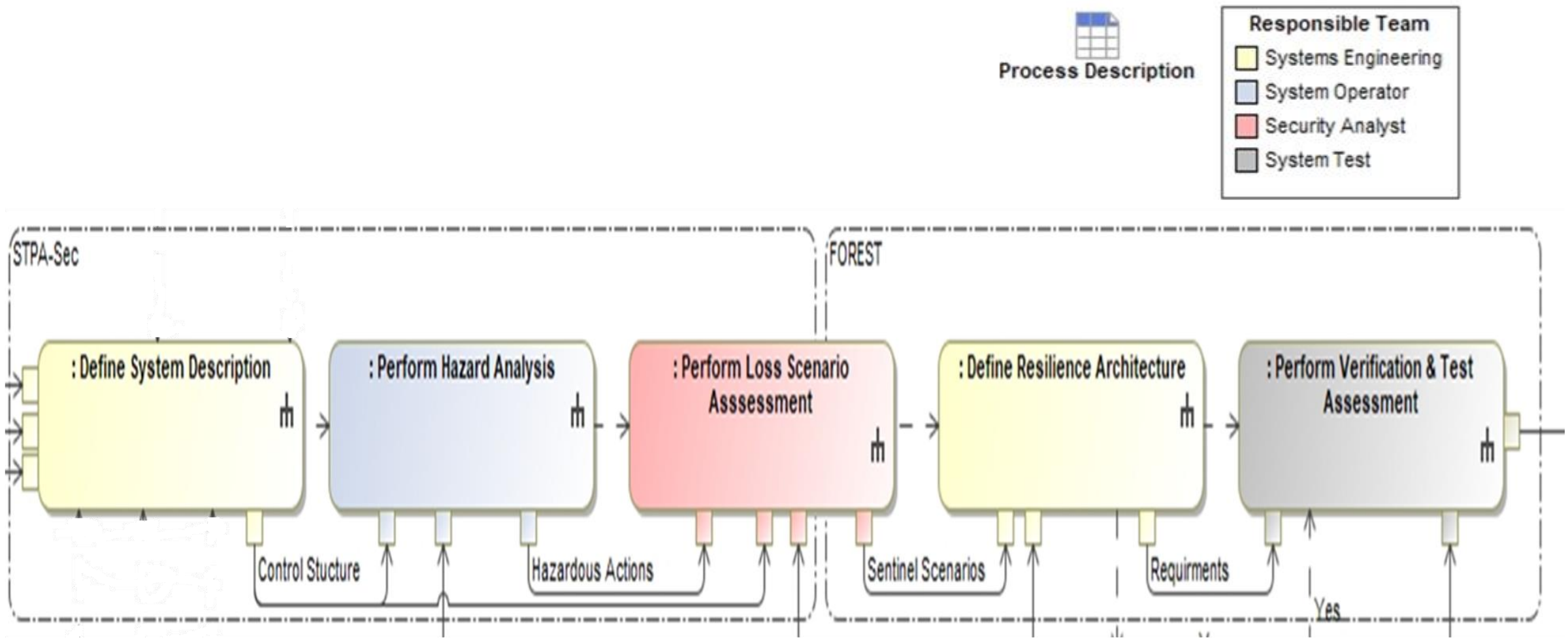
Cyber Resilience Requirements Methodology (CRRM) Artifacts

#	CRRM Step.id	CRRM Step.title	CRRM Artifact.ART.id	CRRM Artifact.ART.title
1	CRRM.1	System Description	CRRM.1.ART.1	Mission / System Purpose (Use Case Model)
			CRRM.1.ART.2	Subsystem Hiearchy (Block Definition Diagram)
			CRRM.1.ART.3	Use Case Realizations (Activity Diagram)
			CRRM.1.ART.4	Mission / System Control Structure (Internal Block Diagram)
			CRRM.1.ART.5	Control Action / Feedback Inventory (Table)
2	CRRM.2	Hazard Analysis	CRRM.2.ART.1	Blue Team: Prioritized Mission / System Losses [to be avoided] (Table)
			CRRM.2.ART.2	Mission System Hazard States [leads to Loss] (Table)
			CRRM.2.ART.3	Hazardous Control Actions (HCA) [leads to Hazard] (Table)
3	CRRM.3	Loss Scenario Assessment	CRRM.3.ART.1	Loss Scenario: Control Structure Analysis [leads to HCA] (Table)
			CRRM.3.ART.2	Red Team: Loss Scenario Risk Analysis (Table)
			CRRM.3.ART.3	Assurance Cases [reduce Likelihood of LS] (Table)
			CRRM.3.ART.4	Sentinel Scenarios [reduce Consequence of LS] (Table)
			CRRM.3.ART.5	Tradespace: Assurance Case elicted Requirements (Table)
4	CRRM.4	Resilience Architecture	CRRM.4.ART.1	Resilient: Subsystem Hiearchy (Block Definition Diagram
			CRRM.4.ART.2	Sentinel Scenario Realizations (Activity Diagram)
			CRRM.4.ART.3	Resilient: Mission / System Control Structure (Internal Block Diagram)
			CRRM.4.ART.4	Resilient: Control Action / Feedback Inventory (Table)
			CRRM.4.ART.5	Tradespace: Architectural Sentinel Scenario elicted Requirements (Table)
			CRRM.4.ART.6	Tradespace (Blue Team): FOREST-based Sentinel Scenario elicted Requirements (Table)
5	CRRM.5	Verification & Test Assessment	CRRM.5.ART.1	Assurance: Test Cases (Table)
			CRRM.5.ART.2	Resilience: Test Cases (Table)
			CRRM.5.ART.3	Tradespace: Test Case eliced Requirement for Test Support (Table)
			CRRM.5.ART.4	Tradespace: Resilience Simulation to refine FOREST Requirements (Table)

Overarching process. Houses learning objectives.

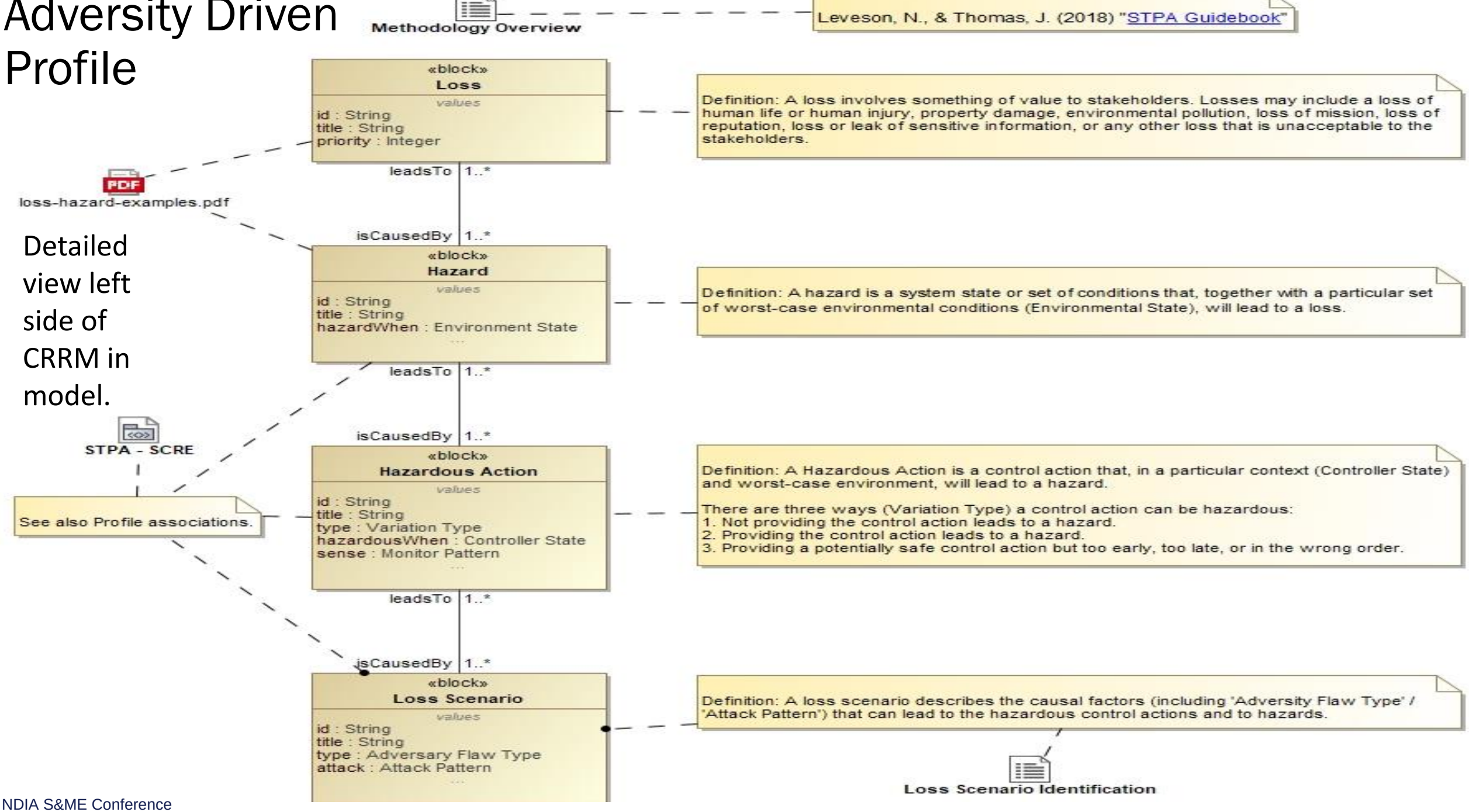
Implemented in model. Completely functional.

Methodology - CRRM Process (STPA SEC + Security, Awareness, Assurance, Resiliency)

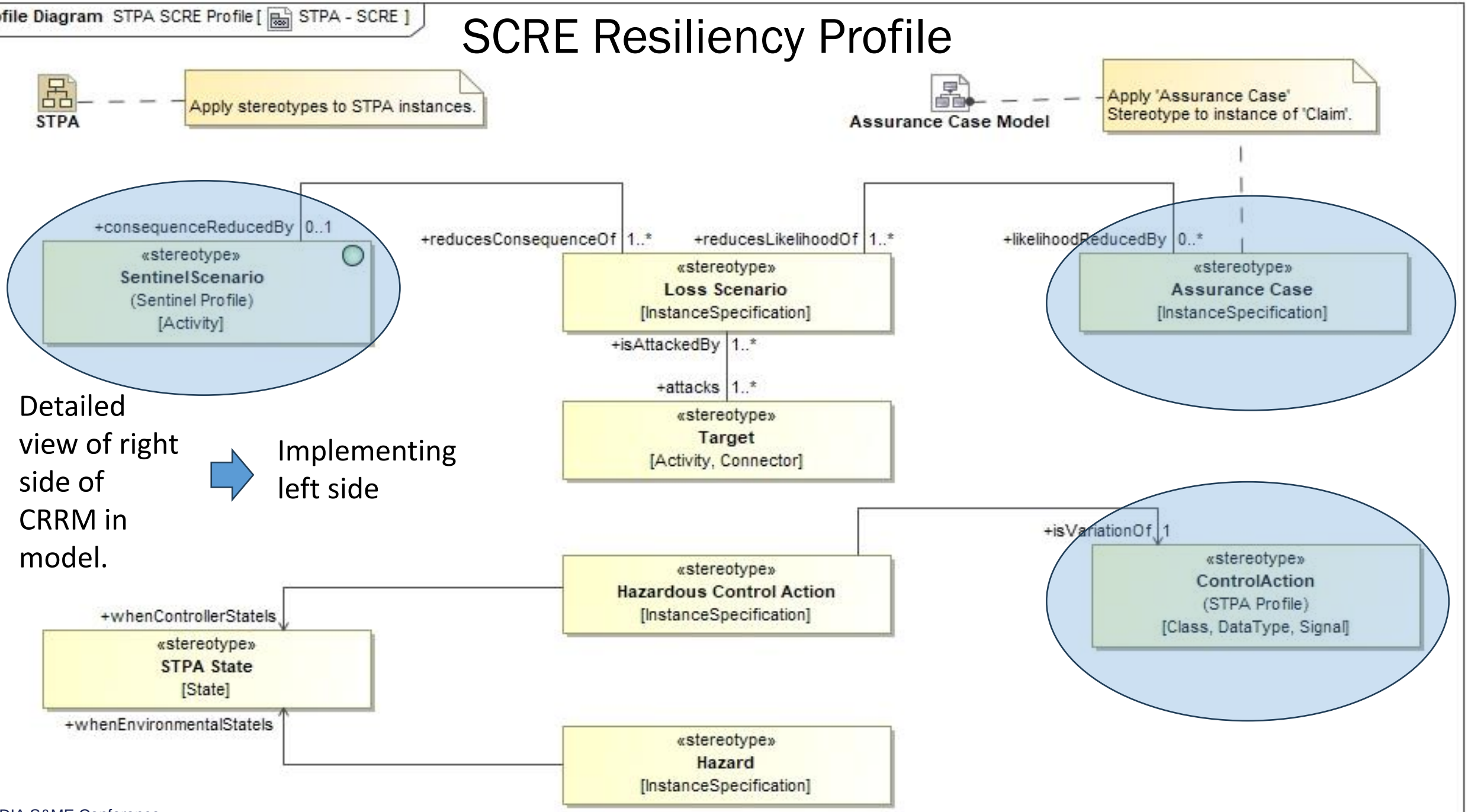


Adversity Driven Profile

Detailed view left side of CRRM in model.



SCRE Resiliency Profile



Next Steps & Questions

- **Next Steps**
  - Continue to collaborate between the DAU and OUSD R&E on the integration of the Storyboard Resiliency Verification and Validation into CCYB-005 Advanced SCRE Credential
- **Questions**

Points of Contact

- **Further questions about the SCRE Credential Program:**
  - Mr. Paul E. McMahon, Paul.E.McMahon6.ctr@mail.mil
  - Mr. Burhan Adam, Burhan.y.Adam.civ@mail.mil
  - Dr. Aaron Jacobson, Aaron.Jacobson@dau.edu