SERC RESEARCH REVIEW 2023 | NOVEMBER 15, 2023

Digital Engineering Simulation (WRT-1043)

11/15/2023

Defense Acquisition University

Dr. Nicole Hutchison

This material is based upon work supported, in whole or in part, by the U.S. Department of Defense through the Systems Engineering Research Center (SERC) under Contract H98230-08-D-0171. The SERC is a federally funded University Affiliated Research Center (UARC) managed by Stevens Institute of Technology consisting of a collaborative network of over 20 universities. More information is available at www.SERCuarc.org

STEVENS INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY®



PI: Dr. Nicole Hutchison
Ms. Megan Clifford
Mr. David Long






VIRGINIA TECH

Co-PI: Dr. Peter Beling
Mr. Tim Sherburne
Dr. Paul Wach
Mr. Geoff Kerr

Georgia Tech Research Institute

Mr. Dalton Clark
Dr. Craig Arndt

Sponsor

DAU

Mr. David Pearson
Dr. Jim Roche
Mr. Rob Arthur
Dr. John Snoderly

Research Motivation

- DoD *Digital Engineering Strategy* (2018)
- Need to effectively train the acquisition workforce to meet challenges of digital transformation

History

STEDE
SIMULATION TRAINING ENVIRONMENT FOR DIGITAL ENGINEERING

Base Year

- Need exploration
- Initial architecture
- Case study identification
- Advisory Board Established
- Sponsor Relationships Established
- Lessons Learned Captured

Option Year 1

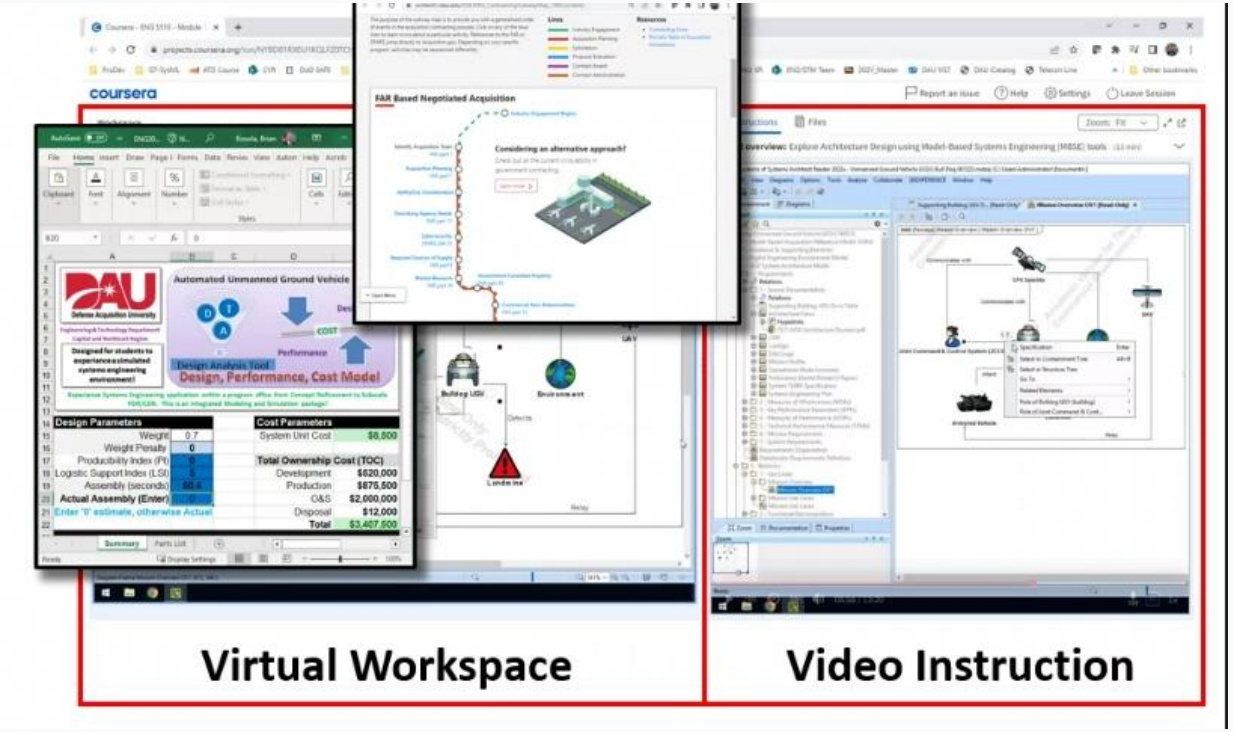
- Refined Architecture
- Draft “almanac” (Jupyter)
- Case Study Refinement
  - Bulldog / Firebird / Firedog
- Digital Systems Engineering Plan (dSEP)
- Mission Engineering and DE
- Digital Environment
- Simulation Training Environment Digital Engineering (STEDE)

Current Year Taskings

- Support for DAU Credentials
  - Digital Engineering (DE)
  - Secure Cyber-Resilient Engineering (SCRE)
- Coordination with DAU Credentials
  - Systems Engineering (SE)
  - Mission Engineering (ME)
- Development of a Digital Twin

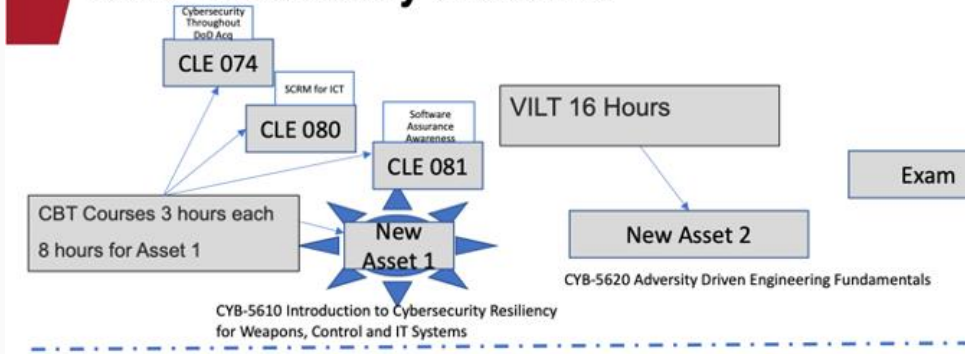
DAU Credentials: Digital Engineering

- 6 courses
  - SysML
  - MBSE
  - DE Environment
  - DE Technical Processes
  - DE Management Processes
  - Capstone

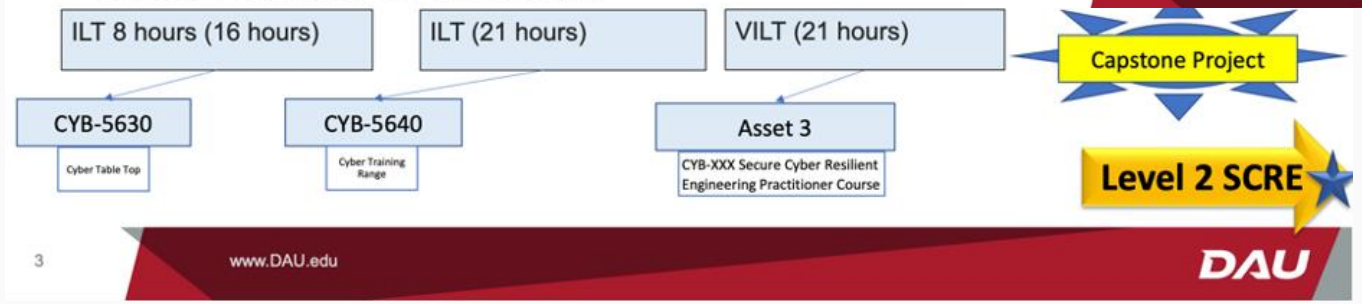


DAU Credentials: SCRE

SCRE Introductory Credential



SCRE Practitioner Credential



Cyber Resilience Techniques, approaches, and Patterns

FIGURE 1: CYBER RESILIENCY TECHNIQUES AND IMPLEMENTATION APPROACHES

NIST 800.160 vol 2

Mode / Pattern	Description	Attack Model Countered
Trusted Kernel or Guard	Creates a small control system within the CPS that independently monitors and/or manages all resource access.	Escalation, interruption attacks
Isolation	Creates an isolated runtime environment (sandbox) for the critical asset that is resistant against attacks.	Escalation, interruption attacks
Redundancy	Replicates the functionality of the critical asset in order to create multiple paths for high availability and fault tolerance in the case of individual function failures.	Attacks that disable individual instances of critical assets and functionality
Diversification	Produces functionally equivalent variations of binaries running in software critical assets. This is an enhancement of the redundancy countermeasure.	Coordinated attacks, zero-day attacks effective in identical binary copies of the critical assets
Physically Nonclonable Function	Secures the integrity and privacy of the messages in the system using a Physical Unclonable Function (PUF) that is hard to predict and duplicate.	Attacks that hijack the communication channels such as man-in-the-middle attacks
Obfuscation	Obscures the real meaning of data/signals/flows by making them difficult for an attacker to understand. It can use random sources of noise from the environment of the critical assets to increase the entropy.	Attacks that require knowledge of the inner workings of the system, its functions, and its mission
Parameter Assurance	Compares input data to a table of values in the system to check for large, unexpected deviations.	Attacks that manipulate data files or messages that are sent to the system
Data Consistency Checking	Verifies the source of a parameter change.	Attacks that use operator specific data entry
Limiting Circuits	Limits resource use (power, memory) to prevent overload.	Power System Attack

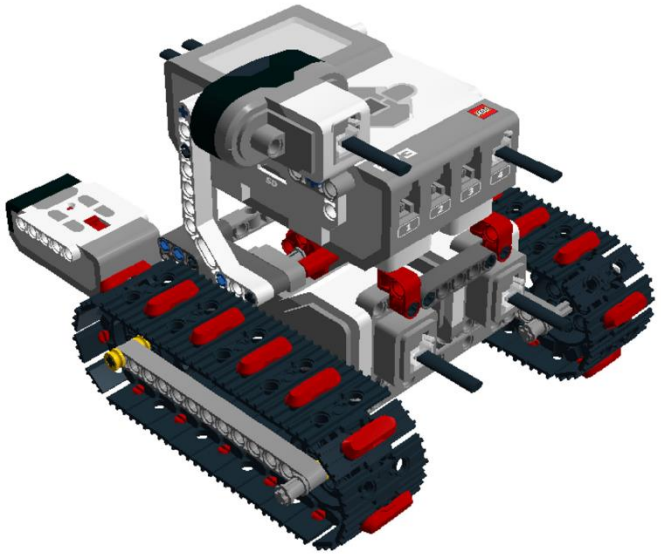
Resilience Modes and Detection Patterns (UVA, Siemens, SIT)

Development of a "Digital Twin": Bulldog

- DAU-created system for training (ENG 202) using traditional artifacts
- UGV – architected and designed in courses
- Implemented with Lego Mindstorms

Preferred Platform by criteria area:

Preliminary Results	Tracked Vehicle	Wheeled Vehicle	Hover Vehicle
Route Flexibility	X (e.g. off-road)		X (e.g. water, mud, ice)
Mobility		X	
Traction on Slopes	X		
Road Speed		X	X (e.g. water, mud, ice)
Logistics		X	
O&S Costs		X	
Payload Weight	X		
Maneuverability			
Transportability		X (e.g. tc	



DRAFT

BULL DOG UNMANNED GROUND VEHICLE (UGV) SYSTEM – ACAT II

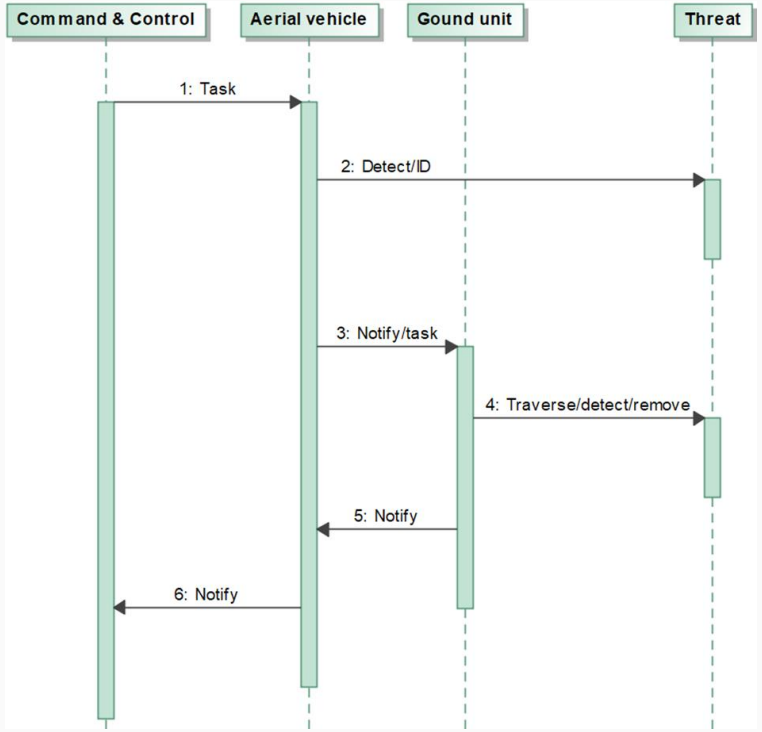
SYSTEMS ENGINEERING PLAN VERSION 3.5

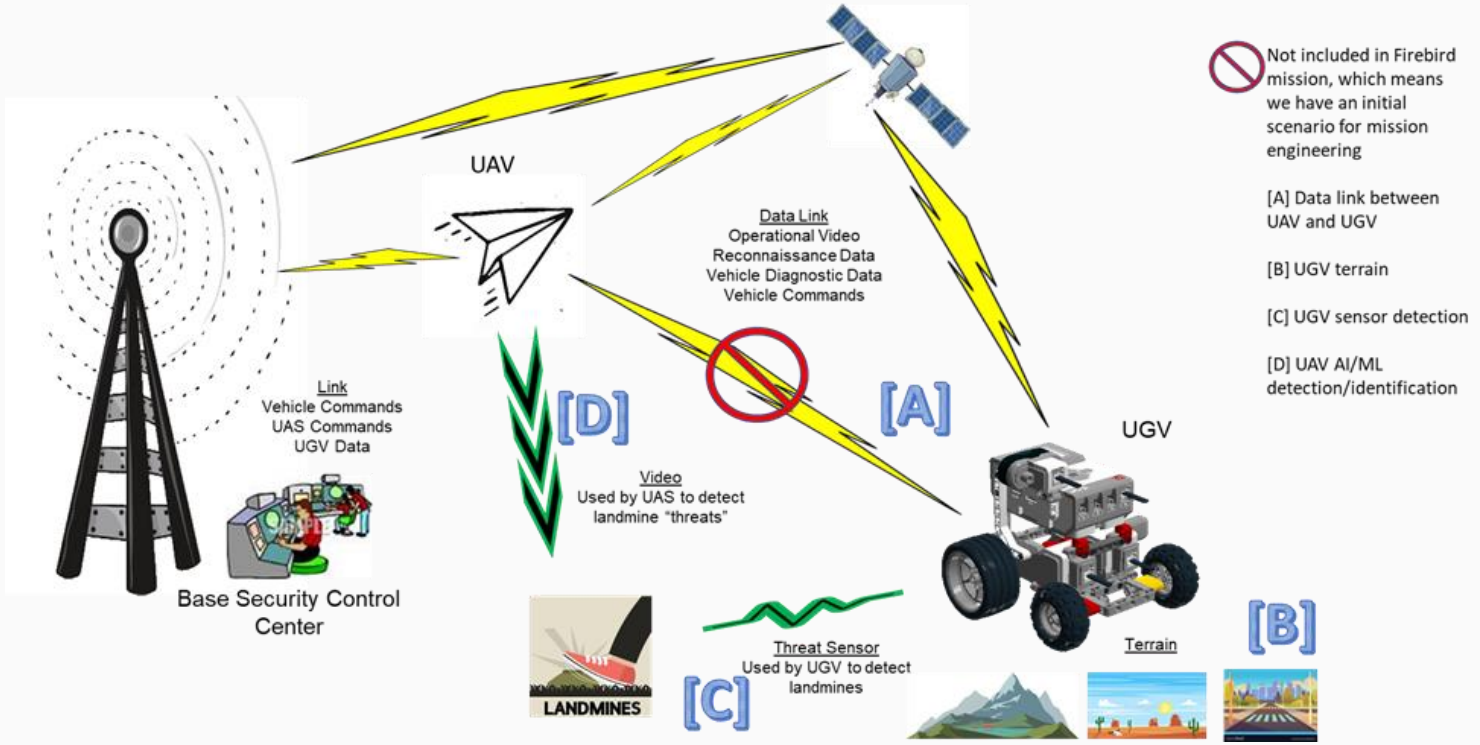
SUPPORTING MILESTONE A AND TECHNOLOGY MATURATION AND RISK REDUCTION

NOVEMBER 7, 20XX

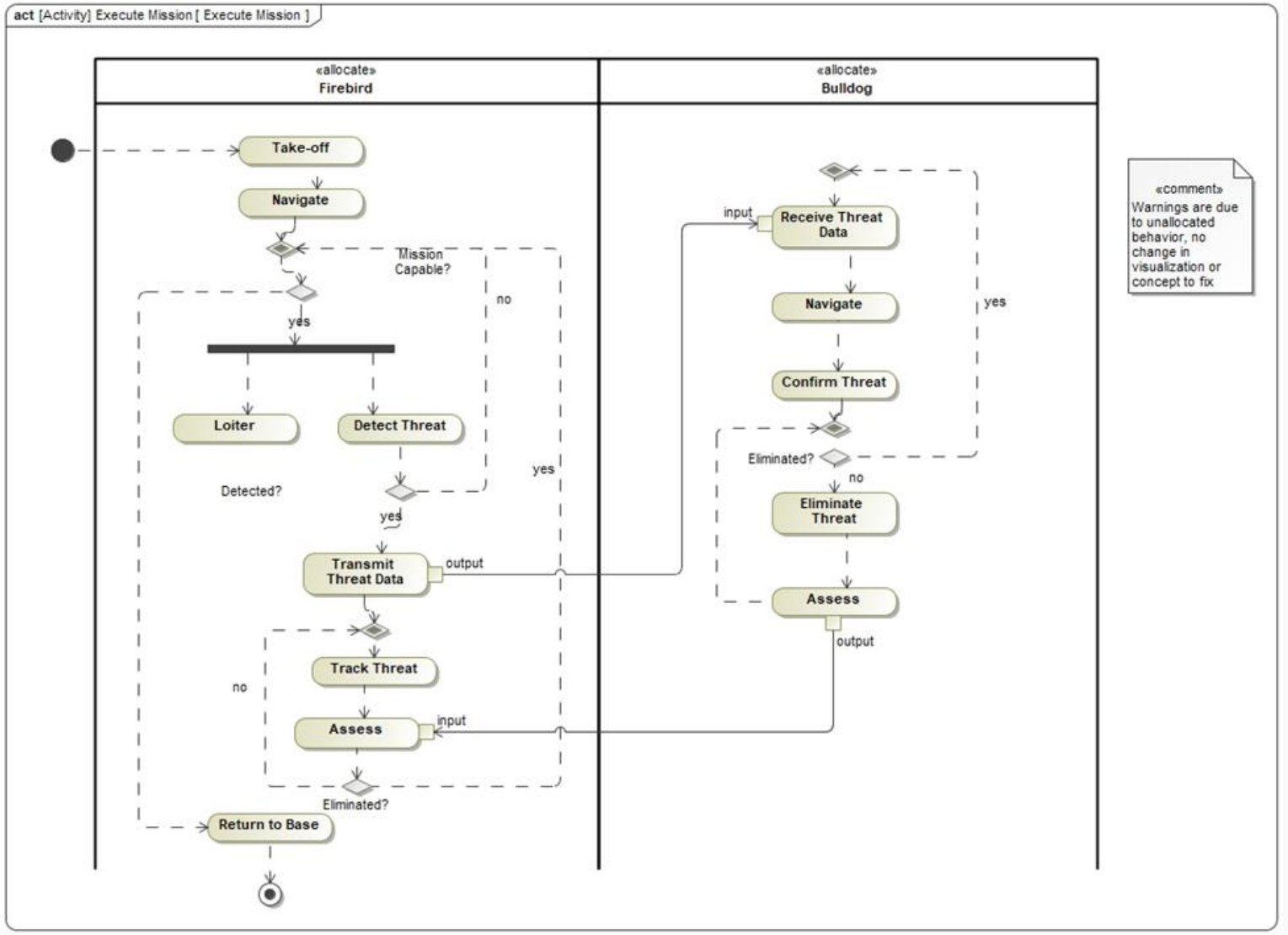
(Adapted for Academic Purposes)

Bulldog (cont)

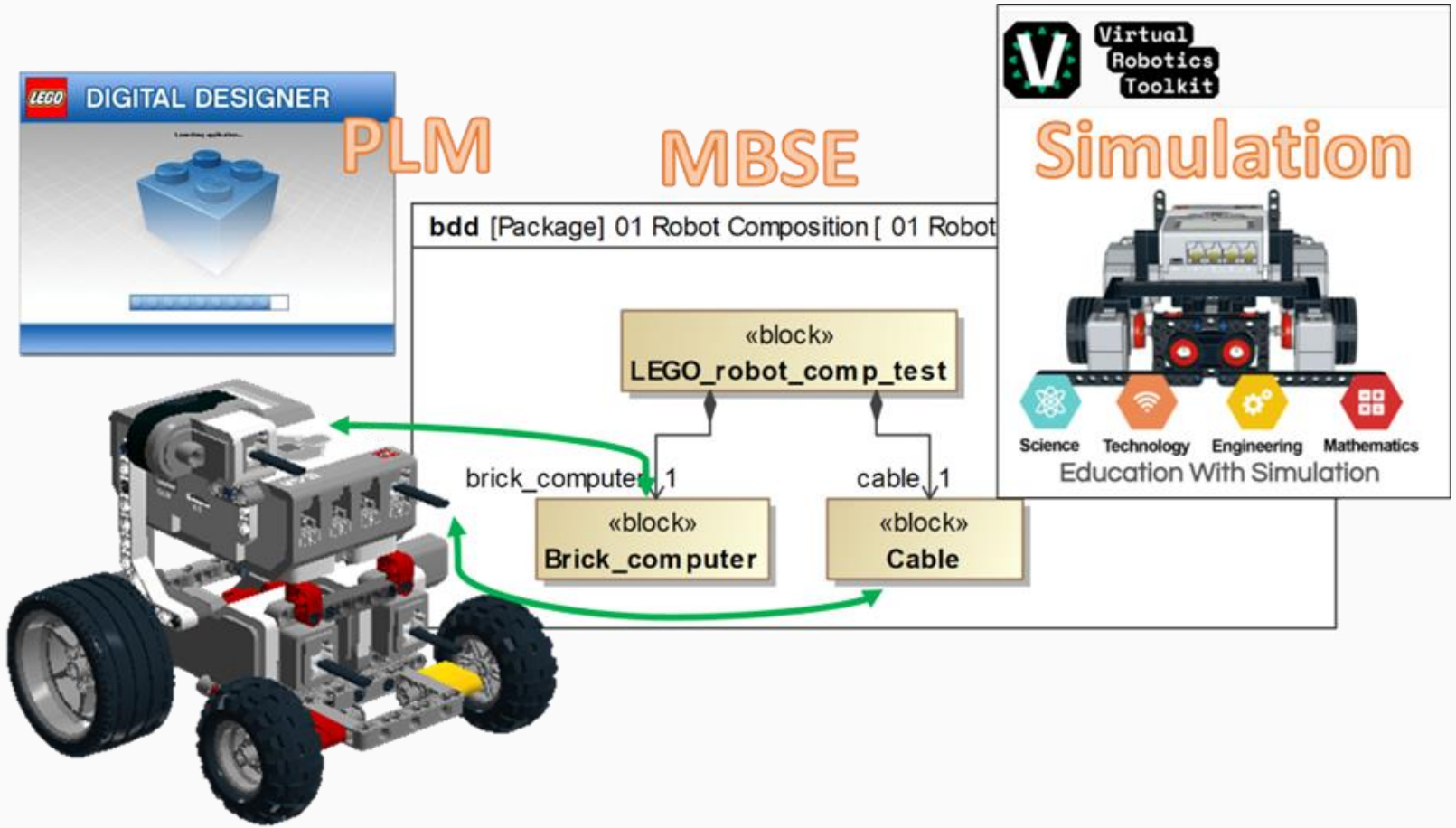




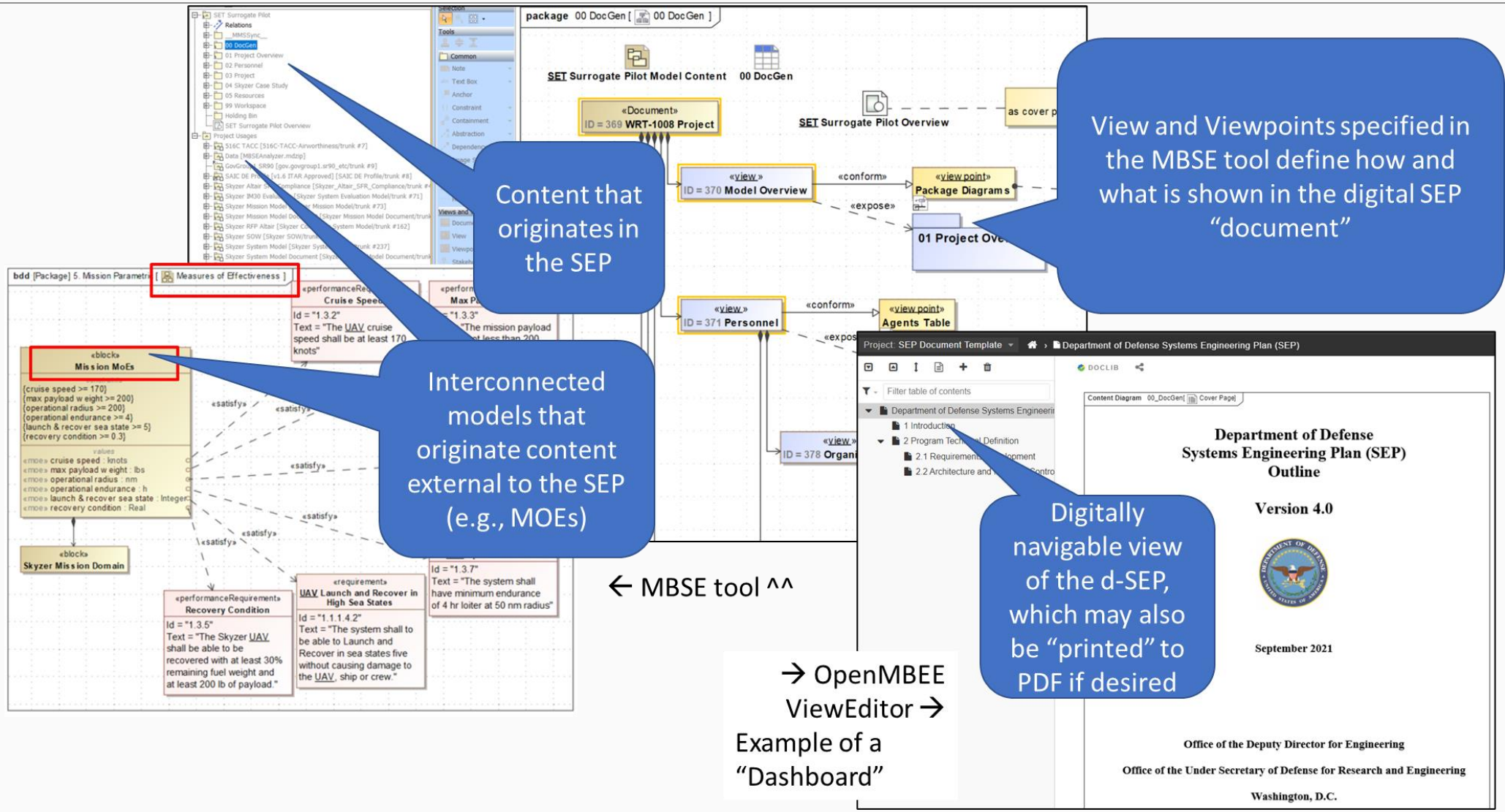
Bulldog (cont)



Bulldog (cont)



Artifacts: Digital SEP



Future Directions

- Completion of SysML and MBSE Courses
- Development/Pilot of DE Environment Course
- Delivery of SCRE courses
- Delivery of Bulldog

Thank you

Stay connected with SERC Online:

Email the presenter: Nicole Hutchison

nicole.hutchison@stevents.edu

Email the research team:

paulw86@vt.edu