USD(R&E)

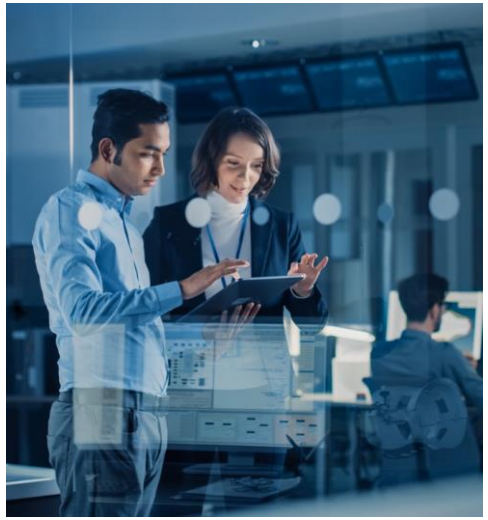
Training the DoD Acquisition Workforce in Secure Cyber Resilient Engineering (SCRE): A Storyboard Approach Being Integrated into the Defense Acquisition University (DAU) Credential Program

Mr. Paul E. McMahon, Mr. Burhan Adam
Office of the Under Secretary of Defense for Research and Engineering
National Defense Industrial Association Systems and Mission Engineering Conference
October 16-19, 2023

Agenda

- Background
- Requirements & DAU SCRE Credential Program
- About the Story & A Few Simple Examples
- Examples of Processes & Principles used in the Story
- Adversity Driven Scenarios & Risk Assessment in the Story
- Assurance Case Process in the Story
- Another Example Principle & Competency Task in the Story
- Next Steps & Questions
- Point of Contact

Background



- **About this Presentation:** Shortened version of the Storyboard being integrated into DAU's Secure Cyber Resilient Engineering (SCRE) Credential Program
- **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:** Highlight example learning points, principles, and processes used in the story
- **Story Perspective:** Lead Systems Engineer and Team

Not giving you a new methodology, but rather additional tools to help lead engineer and team become more effective in doing their job

Requirements & DAU SCRE Credential Program

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

- **SCRE Credential Program**
  - CYB 5610 Introduction/Awareness—On-line, 4-6 hours
  - CYB 5620 Adversity-Driven Fundamentals, Instructor led, 2.5 days

  Introductory Credential

  - CYB 5630 SCRE **Practitioner Credential -- future**

Parts of the storyboard are used in all 3 courses at appropriate level for the course

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
  - System in our story is being upgraded for use in hostile enemy environments where there exists risk to friendly troops
- **Program in Story:** Program is planning to reuse the existing legacy Silverfish system which has some, but not all of the requirements needed 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

- As the lead systems engineer you have the responsibility together with your team, in accordance with DoDI 5000.83 to conduct Secure Cyber Resilient Engineering (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."

Learning Points – 2 of the 28 SCRE Competency Tasks:

Deriving Stakeholder Adversity Driven Concerns to Protect Against…

Defining Protect-Oriented Design Constraints…

A Few Simple Examples How Lead Engineer Achieves their Responsibilities

Competency Task	Derive stakeholder adversity-driven concerns to protect against unacceptable loss	Define protect-oriented design constraints … consistent with existing agreements, regulations
Story	Lead engineer sets up stakeholders meeting to elicit concerns… • loss of friendly troops • loss ability to complete mission • loss of technology	Lead engineer defines design constraints: • monitor laser designator for malfunction • provide operator malfunction alerts • provide backup system • monitor mine detector for malfunction • encrypt data on board Silverfish
Learning Point	Loss concerns are based on stakeholders' valuations of assets.	Protection-oriented design constraints could be regulations or derived requirements

Examples of Processes Used in the Story

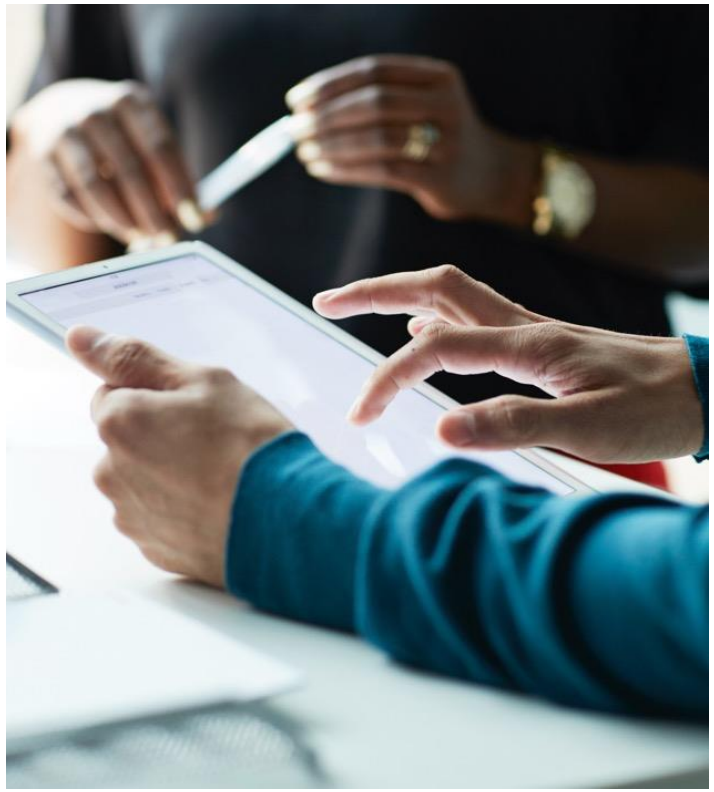
- STPA-Sec: System Theoretic Process Analysis for Security– Top-down loss-based approach that identifies unacceptable losses
  - Used to demonstrate Principles/Techniques*: Loss/Hazard Analysis, Protective System Control, Loss Scenarios
- Assurance Case: A structured argument that demonstrates that a 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)*

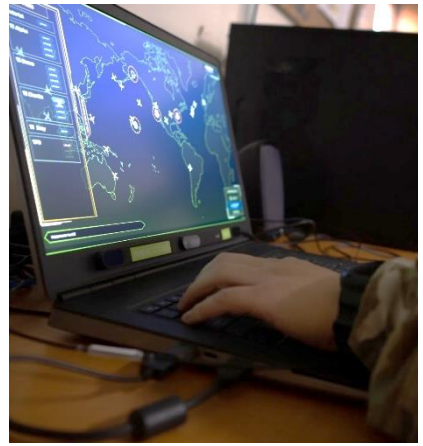
Continuing with the Story: Adversity-Driven Scenarios and Risk Assessment

- Now that you (as the lead engineer with your team) have a list of proposed protection-oriented design constraints and derived requirements, before conducting further requirements break-down, or design (which is what you traditionally might have done), you need to develop Adversity-Driven Scenarios and conduct a Risk Assessment in support of your proposed list of design constraints and derived requirements.



Developing Adversity Driven Scenarios through System Theoretic Process Analysis –Security

- One way to develop adversity driven scenarios-- although not necessarily the only way– is through the use of System Theoretic Process Analysis – Security (STPA-SEC)
- System Theoretic Process Analysis– Security (STPA-Sec) is a top-down, loss-based approach that identifies unacceptable losses, and hazards that might cause those losses.
- We are going to walk through (at a high level) a simplified example of the STPA-Sec process for the Silverfish.



Simplified 4 Step STPA-Sec Process

1. Problem Framing

- Includes identifying unacceptable losses & hazards (states) leading to those losses

2. Model Control Structures

- Includes assigning responsibilities to controllers, including feedback

3. Identify Hazardous Control Actions

- Can be not providing a control action, or too early, too late, or stopping too soon

4. Identify Loss Scenarios

- Includes identifying what part of the architecture in the scenario is responsible to ensure unacceptable things don't happen

Step 1 Applied to Silverfish

Step 1: We identify three unacceptable losses:

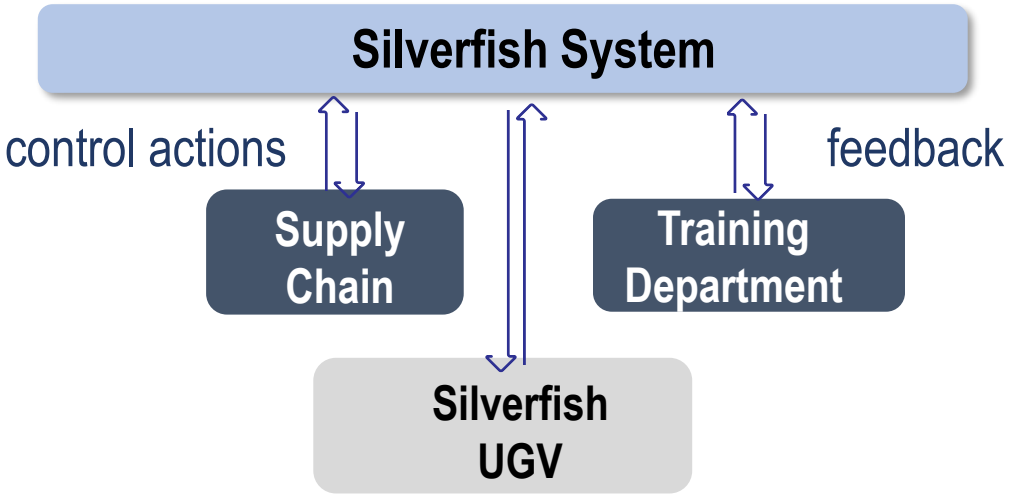
- Loss of friendly troops
- Loss of Silverfish ability to complete mission
- Loss of technology

Three system level hazards that can lead to unacceptable losses:

- Laser designator malfunction
- Mine detector malfunction
- Silverfish remote vehicle captured by enemy/reverse engineered

Step 2 & 3 Applied to the Silverfish

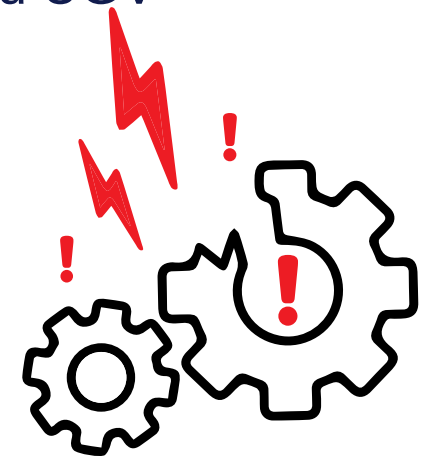
Step 2: Model Control Structures - Protective System Control (PSC): Ensure outcomes only as authorized & intended



Assign Controller responsibilities:
1. Supply Chain – Example: Monitor subcontracted Laser Designator
2. Training Department – Examples: Testers, Silverfish Operators
3. Silverfish UGV – Example: Encrypt data at rest

Step 3: Identify hazard control actions:

- ⚠ Not adequately vetting subcontractor
- ⚠ Not adequately training testers and UGV Operator
- ⚠ Not encrypting data “at rest” on board UGV



Step 4: Identify Silverfish Loss Scenarios & related facts informing-- risk assessment & credible and compelling arguments

Silverfish Loss Scenario	Assumptions	Likelihood facts	Consequence
1: Laser designator malfunction due to malicious activity in supply chain	Laser designator subcontracted to contractor X	Sub X team member vetting process concern	All Scenarios Unacceptable to Stakeholders
2: Mine detector malfunction caused unintentionally by poor testing	All mine detector testing done by prime	Assessment of training dept feedback surveys	
3: Vehicle captured by enemy & On-board data reverse engineered - technology loss	On board data not encrypted on legacy system	No plan to encrypt on board data	
4: Laser designator malfunction/ Operator waits too long to engage backup	Operators adequately training in alerts	Operator training Assessment	

Assumptions and facts informing likelihood used in risk assessments, also provide example of SCRE Competency Task "Collect sufficient data insight Into adversity"

Assurance Case Process Demonstrated in Story

Assurance Case: Structure Argument to Demonstrate a Claim

Silverfish Assurance Case Top Level Claim:
The system is adequately cyber resilient if risk of each scenario moderate or low

Rationale for Top level claim:
In story stakeholders agree on criteria to maintain risk of 7 unacceptable loss scenarios to moderate or lower

Initial Risk Assessment results indicate 3 of the 7 Loss Scenarios are currently assessed at a moderate or below level, while 4 of the 7 Loss Scenarios are currently assessed at a high level.

In this Storyboard we provide rationale for added protection measures to bring all loss scenarios into the moderate or below level to meet the agreed criteria for a sufficiently cyber resilient system.

This is example of SCRE Competency Task:
"Provide credible & compelling argument based on quality of evidence.."

Another Example Principle & Competency Task Demonstrated in Story

- **Risk of operator missing or mis-interpreting an alert**
  - Use of an AI requiring concurrence prior to engaging Laser Designator backup
  - Demonstrates "Distributed Privilege" Technique

- **However, requiring concurrence could delay the decision putting friendly troops at higher risk**
  - As a result, the lead engineer adds derived requirement allowing AI override if specified certification achieved by Operator
  - Demonstrates SCRE Competency Task "altering design to reduce risk inherent in selected design"

Next Steps & Questions

- **Next Steps**
  - Continue to collaborate with the Defense Acquisition University (DAU) on the integration of the Storyboard into the SCRE Credential Program

- **Questions**
  - ????

Points of Contact

- **Further questions about the SCRE Storyboard:**
  - Mr. Paul E. McMahon, Paul.E.McMahon6.ctr@mail.mil
  - Mr. Burhan Adam, Burhan.y.Adam.civ@mail.mil