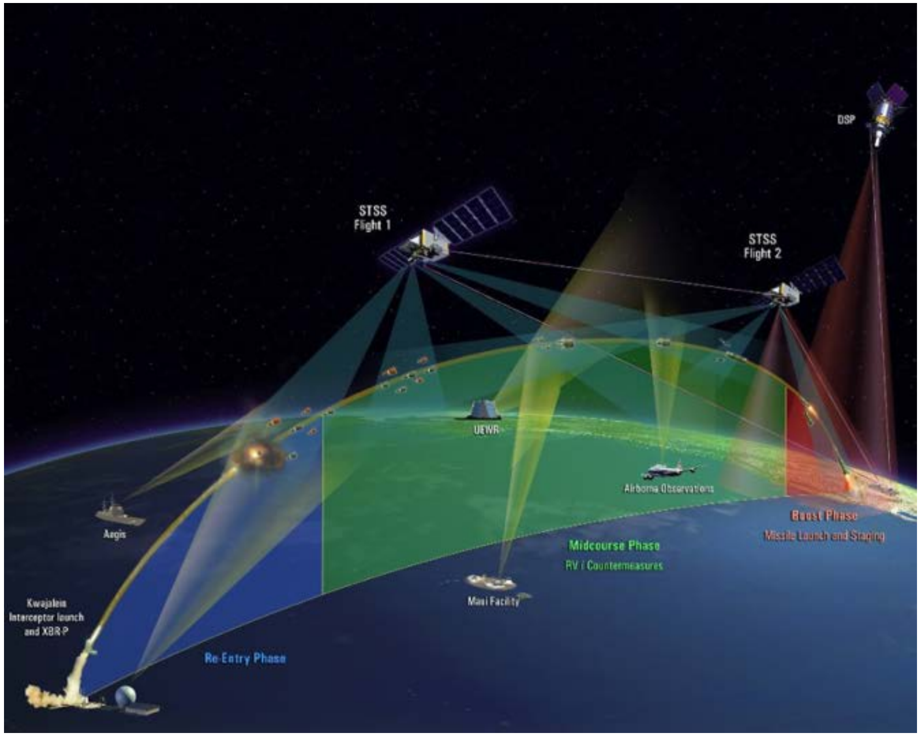
Security Engineering in a System of Systems Environment

G. Rebovich

J. Dahmann

G. Turner

August 2014



MITRE

Approved for Public Release; Distribution Unlimited. 13-3376

Topics

- **Background and Motivation**
- **Framework Overview**
- **Framework in Detail**
- **Potential Follow On Efforts**

Preamble

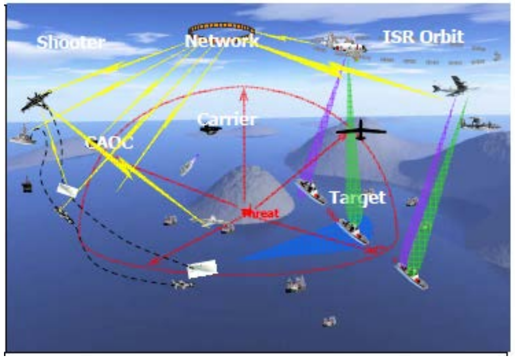
System: in general, the product of a Major Defense Acquisition

Example: F-35

Systems Security Engineering

- Identifies and contains risks to advanced technology and mission-critical system functionality from foreign collection, design vulnerability or supply chain exploit/insertion, and battlefield loss throughout the acquisition lifecycle
- Includes but is not limited to advanced cyber threats
- Includes but is not limited to assuring cyber technologies

System of Systems: a set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities



System of Systems Security Engineering

- Focus of this effort and briefing, especially for critical missions
- Question: Can system level SSE be extended to SoS to:
  - Identify SoS risks and mitigation approaches. *Example: SNC3 Modernization*
  - Provide improved context and rationale for individual system level security engineering. *Example: FAB-T terminal*

The Problem – SSE for SoS

- **DoD is addressing security in engineering of individual systems**
  - Major focus for acquisition – vulnerabilities of systems they field
  - Programs required "to identify mission-critical functions and components and manage their risk of compromise"
    - Includes hardware, firmware, software and information
- **Most missions supported by SoS with:**
  - Uneven levels of security protection among constituent systems (e.g., mix of legacy and newly developed systems) and
  - Additional vulnerabilities introduced by the SoS configuration rather than in constituent systems
- **Key question - how to address security of SoS in support of critical missions?**
  - Focus on mission impact of security threats to and vulnerabilities of supporting SoS, constituent systems, enabling infrastructure, and their interdependencies

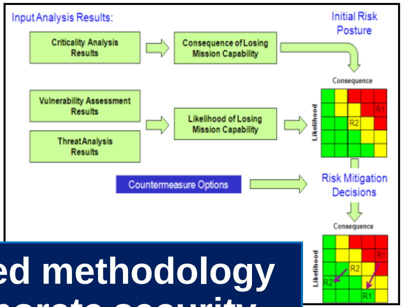
SSE Risk Based Methodology

- Identify critical system functionality and components, including information
- Assess threats and vulnerabilities of these components, including threats in the operational, program and development environments
- Identify and address counter-measure options for the system

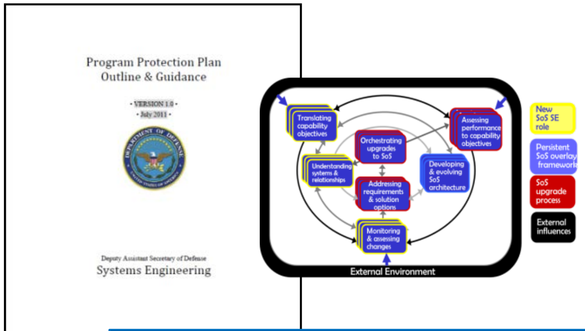
Can we apply the SSE Risk Based Methodology to systems engineering of SoS to assure mission success?

Approved for Public Release; Distribution Unlimited. 13-3376

SSE Policy and Guidance


Input Analysis Results:
Criticality Analysis Results
Consequence of Losing Mission Capability
Vulnerability Assessment Results
Likelihood of Losing Mission Capability
Threat Analysis Results
Countermeasure Options
Initial Risk Posture
Consequence
Likelihood
R1
R2
Risk Mitigation Decisions
Consequence
Likelihood
R1
R2

Risk based methodology to incorporate security considerations into the systems engineering


Program Protection Plan
Outline & Guidance
VERSION 1.0
July 2011
Deputy Assistant Secretary of Defense
Systems Engineering
Translating capability objectives
Orchestrating upgrades to SoS
Assessing performance to capability objectives
Understanding systems & relationships
Developing & evolving SoS architecture
Addressing requirements & solution options
Monitoring & assessing changes
External Environment
New SoS SE role
Persistent SoS overlay framework
SoS upgrade process
External influences

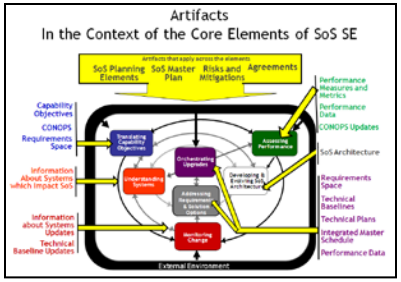
Can SE Guidance be extended to address SoS security consideration?

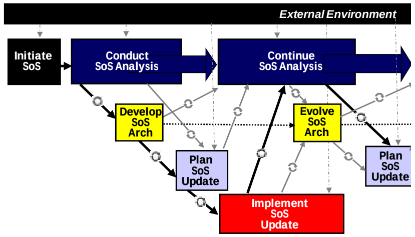
- **System level program protection planning**
  - Requires every program "to identify mission-critical functions and components and manage their risk of compromise [1]."
  - Risk based methodology
    - Identifying critical system components
    - Assess threats and vulnerabilities of these components
    - Identify and address countermeasure options for the system
- **Guidance for systems engineering for SoS is relatively silent on security**
  - The 2008 *Systems Engineering Guide for Systems of Systems* provides DoD guidance to systems engineers. It identifies seven core elements of SoS SE, but
    - "…. more work is needed to better understand the role of SE in SoS in areas not addressed in this guide. This understanding will enable one to better address SE issues that go beyond the initial class of SoS addressed here. These areas include:
      - Systems assurance issues posed by SoS"

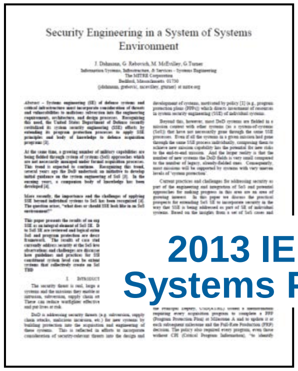
[1] Critical Program Information (CPI) Protection Within the Department of Defense, DoD Instruction 5200.39, 2008.

Baselining SoS SSE Practice

Can SoS SE extend to SSE & is there evidence that it is happening?


Artifacts
In the Context of the Core Elements of SoS SE
Artifacts that apply across the elements
SoS Planning Elements
SoS Master Plan
Risks and Mitigations
Agreements
Capability Objectives
CONOPS
Requirements Space
Information About Systems which Impact SoS
Information about Systems Updates
Technical Baseline Updates
Translating Capability Objectives
Understanding Systems
Orchestrating Upgrades
Addressing Requirements & Solution Options
Monitoring Change
Developing & Evolving SoS Architecture
Assessing Performance
Performance Measures and Metrics
Performance Data
CONOPS Updates
SoS Architecture
Requirements Space
Technical Baselines
Technical Plans
Integrated Master Schedule
Performance Data
External Environment





Security Engineering in a System of Systems Environment

J. Dahmann, G. Rebovich, M. McEvilley, G Turner
Information Systems, Infrastructure, & Services - Systems Engineering
The MITRE Corporation
Bedford, Massachusetts 01730
{jdahmann, grebovic, mcevilley, gturner} at mitre.org

2013 IEEE Systems Paper

- **Logically extended SoS SE guidance to incorporate SSE**
  - For systems, DoD has extended SE to include SSE for program protection; can the same be done for SoS and missions?
  - Drafted extensions to SoS SE artifacts and implementers' view to address security
- **Baselined SoS SSE state-of-practice**
  - Via practitioner interviews with MITRE SE teams working at the SoS level
  - In cases where SoS SE is being applied, determined how SoS security considerations are being addressed
- **Compared current practices and logical extensions**
  - **General lack of attention – seen as system level issue**
    - Focus on systems not end to end SoS and mission
    - Little attention to in-service system protection
  - **Little evidence of extensions in practice**
    - SoS architectures do not typically include security
    - Security not typically incl. in formal SoS agreements
    - End-to-end security risk management not addressed

Purpose of Presentation

- **Present an ‘actionable engineering framework’ for conducting SSE of SoS for critical missions**
- **Focused on the following questions:**
  - How should risks to a SoS/mission be assessed risks so they can be countered?
  - Can the approach being pursued for systems be adapted for SoS?
  - What type of SSE analysis provides the logical foundation for implementation of SoS SSE?
  - How to identify effective approaches to SoS SSE analysis and implementation for priority missions?

Framework Purpose and Users

- **Purpose**
  - Provide a structured systems engineering approach to addressing security for SoS supporting missions
  - Provide technical grounding for investments in security to improve the likelihood of successful mission outcomes
- **Users**
  - Organizations responsible for delivery of technically sound mission capabilities
    - Systems engineering offices responsible for SoS
    - DoD Components or Commands with mission or portfolio responsibility
    - Organizations with specific tasking to address risk in critical missions
  - Decision makers responsible for system improvement investments

Driving Factors (1 of 3)

- **Increased recognition of persistent threat and its potential impact on mission outcomes, particularly for critical missions**
  - Problem and need for attention at mission/SoS level are increasing despite lack of attention to this point
  - Goes beyond information assets to include whole system considerations
- **Progress made with protecting systems is proceeding but considerable residual risk given the large legacy component of inventory and complex system interdependencies in SoS supporting missions**
  - Protecting new systems is important, but it may not be sufficient or effective to assure missions

Driving Factors (2 of 3)

- **Missions predominantly supported by already fielded systems - improvements in security need to realistically consider operational system configurations**
  - Understanding the current systems and operations is key to assessing risk and investments in systems to improve assurance
  - Framework needs to bridge the operational and systems acquisition/engineering communities

Acquisition

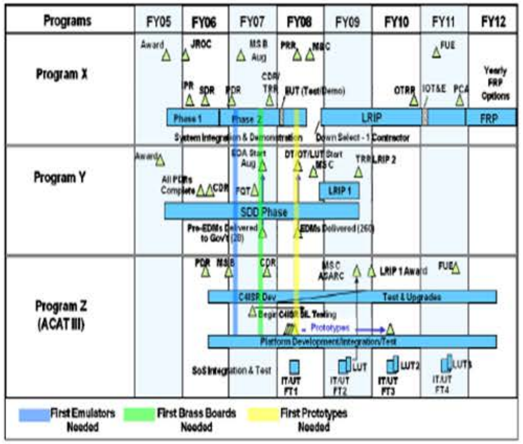
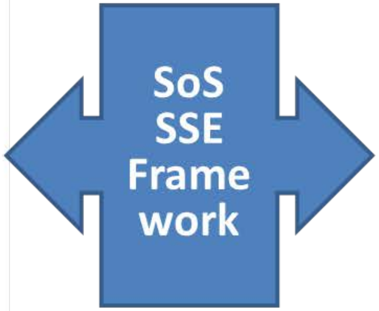


Figure 3.5-1 System-of-Systems Schedule (optional) (sample)
Note: Include an as-of date – time sensitive figure



Operations

Driving Factors (3 of 3)

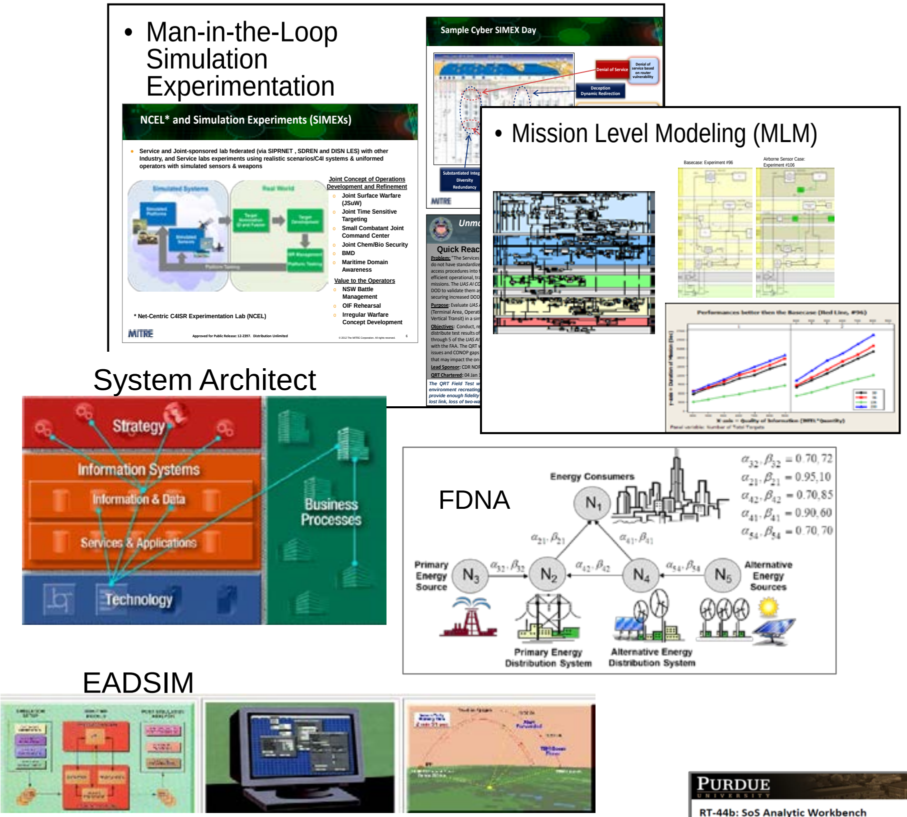
- **SoS and their support to missions combined with the operational context and threats constitutes a complex environment which challenges the application of system-level approaches to SSE**
  - Important to consider this complexity when identifying security improvements to account for unintended effects, missing actions and to assure desired impact
- **Growing inventory of approaches to addressing system security risks**
  - Engineering framework is needed to provide the structure to leverage these in an SoS/mission context

Developing the Framework

- **A growing number of techniques to improve mission assurance and many increasing in maturity**
  - Security specific approaches
    - Take a somewhat specialized view depending on their original purpose
      - Largely focused on cyber and operations - may be extensible to broader applications
    - Tend to assume an understanding of the mission, systems, dependencies and, to some degree, vulnerabilities
  - More general SoS/Mission analysis approaches
    - Generally no specific security features, but provide approaches to represent and analyze missions, including dependencies
      - Explicitly represent systems
      - Less capability to represent specific threats and effects, but provide tools to assess mission impacts of threat effects in operational terms
    - Offer a possible tool set for important aspects of the problem
      - ‘SoS’ criticality analysis: Impact of loss or subversion of a system element on the mission outcome
      - Countermeasure tradeoffs: Assessment of alternative investments in protection of system elements and impact on mission outcome
- **Piloted promising techniques**
  - Used DoD test case; created common set of tasks; engaged SMEs for piloting
  - Focused on proposed application of techniques to SSE analysis as basis for framework development

Approved for Public Release; Distribution Unlimited. 13-3376

Promising Techniques – General Analysis



- Man-in-the-Loop Simulation Experimentation

NCEL* and Simulation Experiments (SIMEXs)

- Service and Joint-sponsored lab federated (via SIPRNET , SDREN and DISN LES) with other Industry, and Service labs experiments using realistic scenarios/C4I systems & uniformed operators with simulated sensors & weapons

Joint Concept of Operations Development and Refinement
- Joint Surface Warfare (JSuW)
- Joint Time Sensitive Targeting
- Small Combatant Joint Command Center
- Joint Chem/Bio Security
- BMD
- Maritime Domain Awareness

Value to the Operators
- NSW Battle Management
- OIF Rehearsal
- Irregular Warfare Concept Development

* Net-Centric C4ISR Experimentation Lab (NCEL)

Approved for Public Release: 12-2397. Distribution Unlimited © 2012 The MITRE Corporation. All rights reserved. 6

Sample Cyber SIMEX Day

- Mission Level Modeling (MLM)

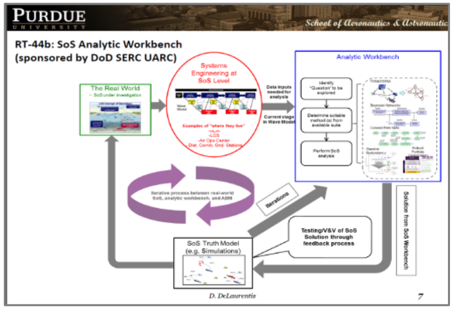
System Architect

FDNA

EADSIM

Simulated Systems
Real World
Platform Tasking
Denial of Service
Deception
Dynamic Redirection
Substantiated Integrity
Diversity
Redundancy
Quick Reaction
Basecase: Experiment #96
Airborne Sensor Case: Experiment #106
Strategy
Information Systems
Information & Data
Services & Applications
Technology
Business Processes
Energy Consumers
N_1
N_2
N_3
N_4
N_5
α_{21}, β_{21}
α_{41}, β_{41}
α_{32}, β_{32}
α_{42}, β_{42}
α_{54}, β_{54}
$\alpha_{32}, \beta_{32} = 0.70, 72$
$\alpha_{21}, \beta_{21} = 0.95, 10$
$\alpha_{42}, \beta_{42} = 0.70, 85$
$\alpha_{41}, \beta_{41} = 0.90, 60$
$\alpha_{54}, \beta_{54} = 0.70, 70$
Primary Energy Source
Alternative Energy Sources
Primary Energy Distribution System
Alternative Energy Distribution System

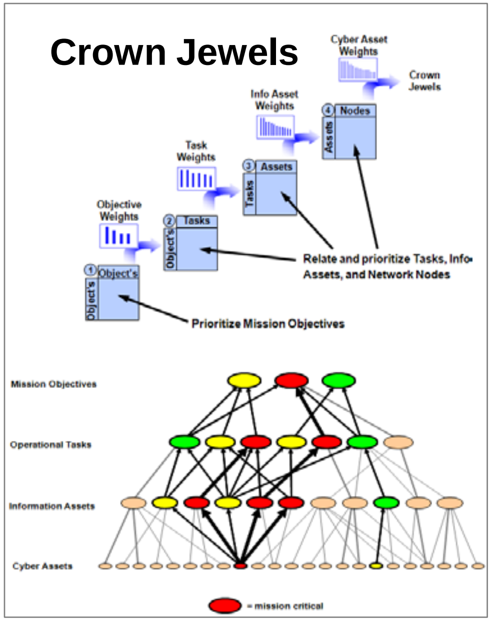
- Architecture Tools
  - Systems Architect
- Process Models
  - BPMN/Mission Level Modeling
- Constructive mission-level simulations
  - Extended Air Defense Simulation
- Virtual simulations
  - Joint Semi-Automated Forces
- Man-in-the-Loop Experimentation
  - Canadian Forces Warfare Centre
- Dependency Analyses
  - Functional Dependency Network Analysis (FDNA)



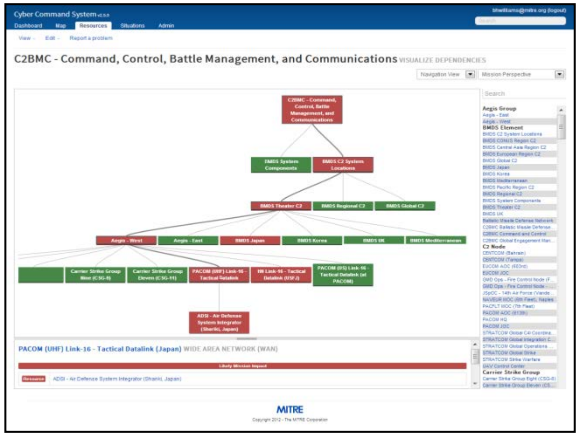
PURDUE UNIVERSITY
School of Aeronautics & Astronautics
RT-44b: SoS Analytic Workbench (sponsored by DoD SERC UARC)
Systems Engineering at SoS Level
The Real World
Examples of "where they live"
Analytic Workbench
Data inputs needed for analysis
Current stage in Wave Model
Identify "Question" to be explored
Determine suitable method(s) from available suite
Perform SoS analysis
Iterations
Testing/V&V of SoS Solution through feedback process
SoS Truth Model (e.g. Simulations)
Solution from SoS Workbench
D. DeLaurentis
7

Also SERC SoS Analysis Workbench and Toolset

Promising Techniques – Security Specific



Map-the-Mission Prototype

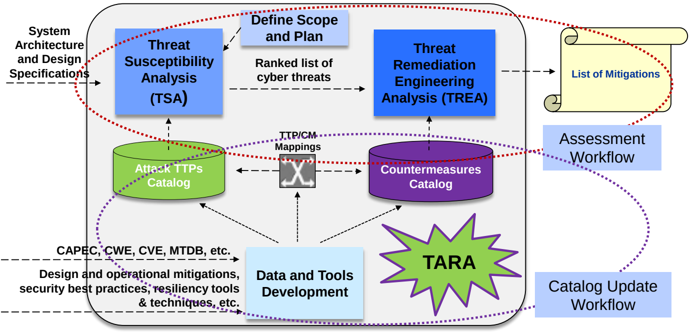


C2BMC - Command, Control, Battle Management, and Communications VISUALIZE DEPENDENCIES

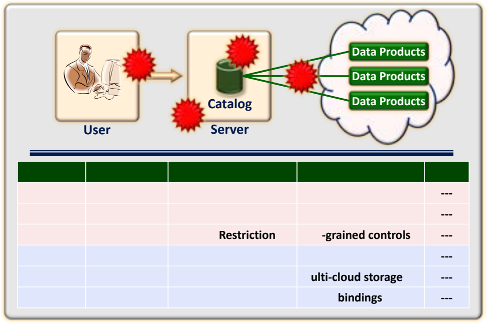
PACOM (UHF) Link-16 - Tactical Datalink (Japan) WIDE AREA NETWORK (WAN)

Resource ADSI - Air Defense System Integrator (Shariki, Japan)

Copyright 2012 - The MITRE Corporation

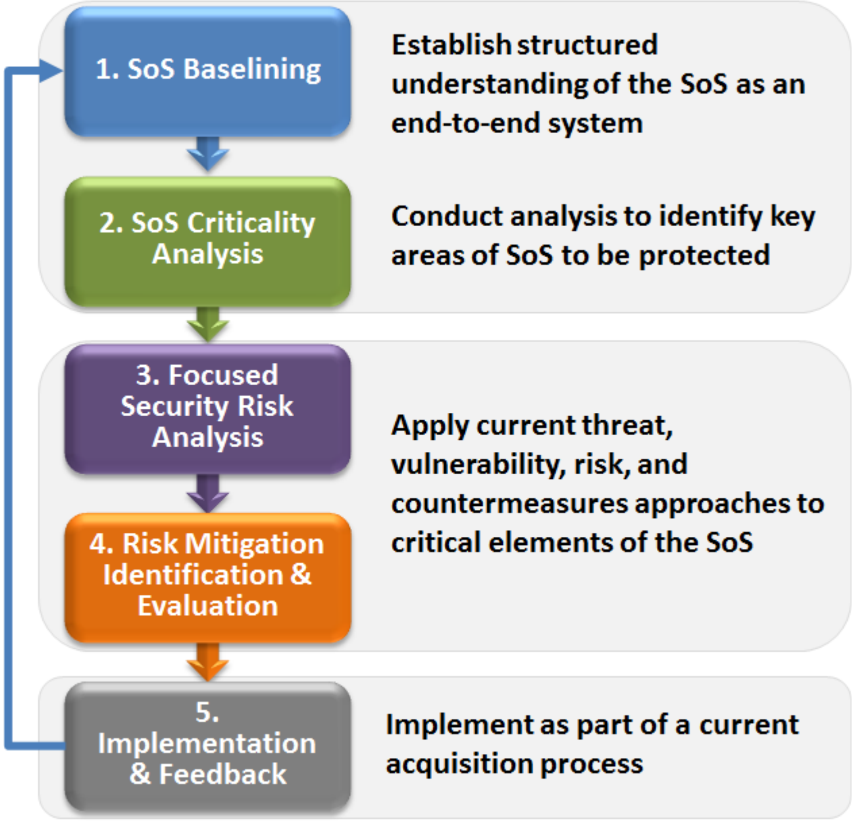

System Architecture and Design Specifications
Threat Susceptibility Analysis (TSA)
Define Scope and Plan
Ranked list of cyber threats
Threat Remediation Engineering Analysis (TREA)
List of Mitigations
Assessment Workflow
Attack TTPs Catalog
TTP/CM Mappings
Countermeasures Catalog
CAPEC, CWE, CVE, MTDB, etc.
Design and operational mitigations, security best practices, resiliency tools & techniques, etc.
Data and Tools Development
TARA
Catalog Update Workflow

RAMBO



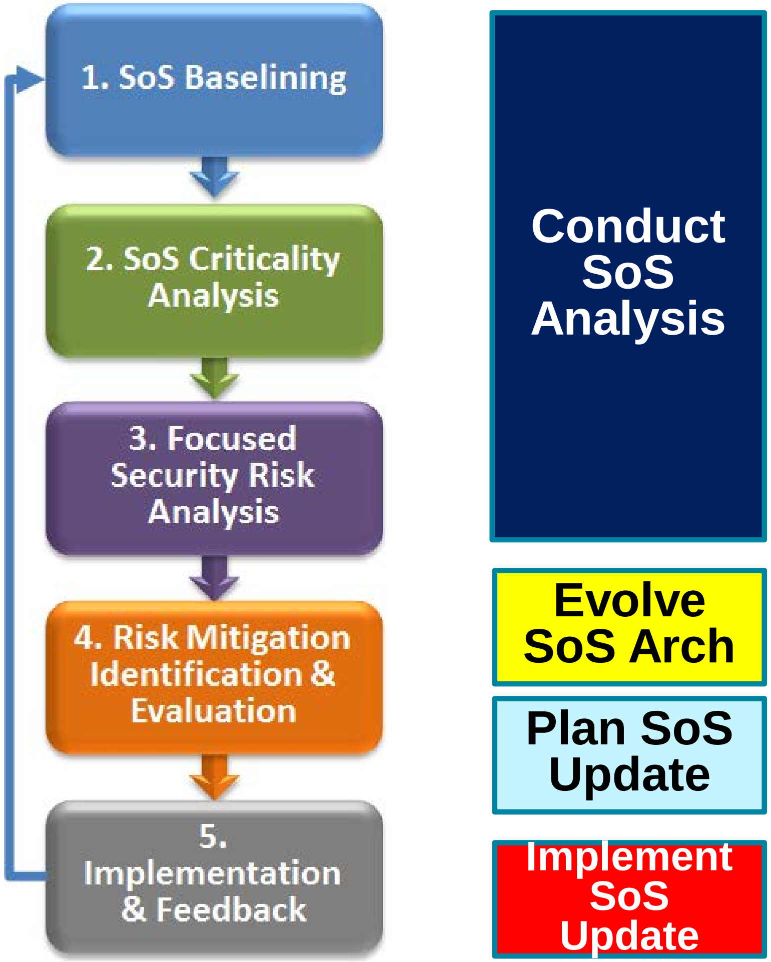
- **Cyber protection and resiliency frameworks**
  - Several approaches address ways to examine an operational environment to identify key IT assets in an operational mission context
    - Crown Jewels Analysis
    - Map The Mission
  - Others apply to addressing approaches to address cyber risks
    - Threat Assessment & Remediation Analysis (TARA)
    - Resilient Architectures for Mission and Business Objectives (RAMBO)

The Framework at a Glance


1. SoS Baselining
Establish structured understanding of the SoS as an end-to-end system
2. SoS Criticality Analysis
Conduct analysis to identify key areas of SoS to be protected
3. Focused Security Risk Analysis
4. Risk Mitigation Identification & Evaluation
Apply current threat, vulnerability, risk, and countermeasures approaches to critical elements of the SoS
5. Implementation & Feedback
Implement as part of a current acquisition process

- **Puts SSE into an SE and SoS context**
- **Explicitly addresses front-end processes to:**
  - Define SoS in operations in a structured way
  - Identify critical components based on an analysis of impacts to mission objectives
- **Supports the application of current security analysis and mitigation approaches**
- **Leverages**
  - Growing inventory of approaches to address risks to systems &
  - Current processes to identify & address changes in systems to support mission success
- **Recognizes that mission security improvements must focus on operational needs and risks of fielded systems**
- **Targeted changes can then be identified and implemented**
  - In fielded system elements with greatest impact on mission outcomes
  - As part of ongoing acquisitions or system upgrades

SoS SSE Relationship to SoSE Wave Model



1. SoS Baselining

2. SoS Criticality Analysis

3. Focused Security Risk Analysis

4. Risk Mitigation Identification & Evaluation

5. Implementation & Feedback

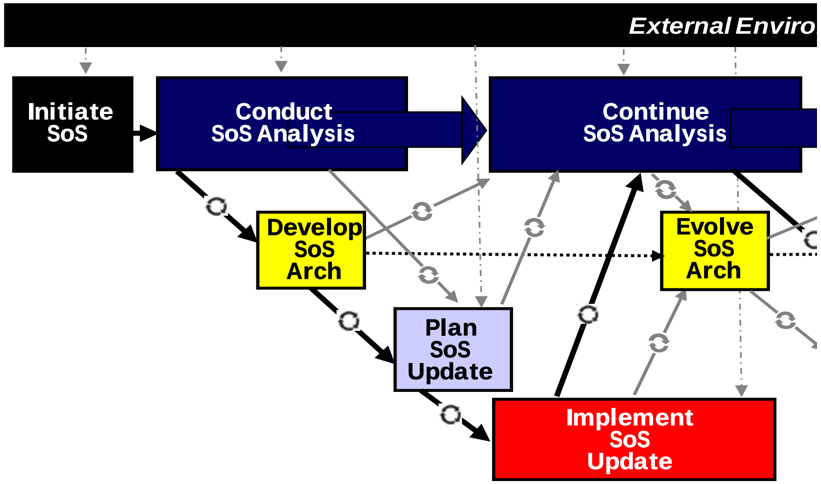
Conduct SoS Analysis

Evolve SoS Arch

Plan SoS Update

Implement SoS Update

SoS SSE Framework is a tailoring of the SoSE Wave Model



External Enviro

Initiate SoS

Conduct SoS Analysis

Continue SoS Analysis

Develop SoS Arch

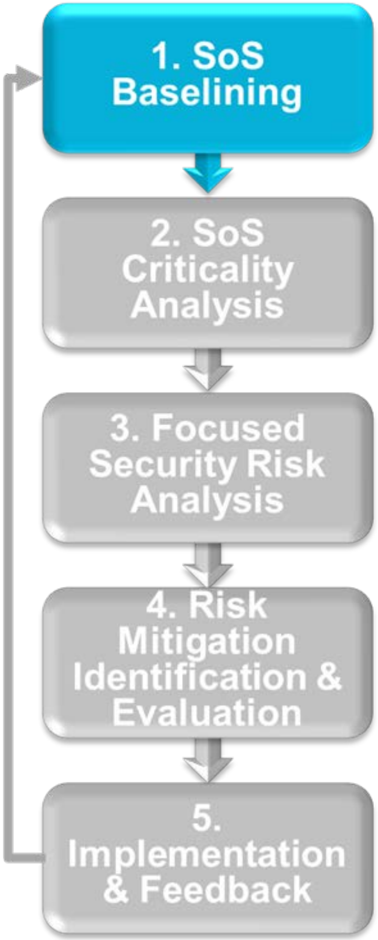
Evolve SoS Arch

Plan SoS Update

Implement SoS Update

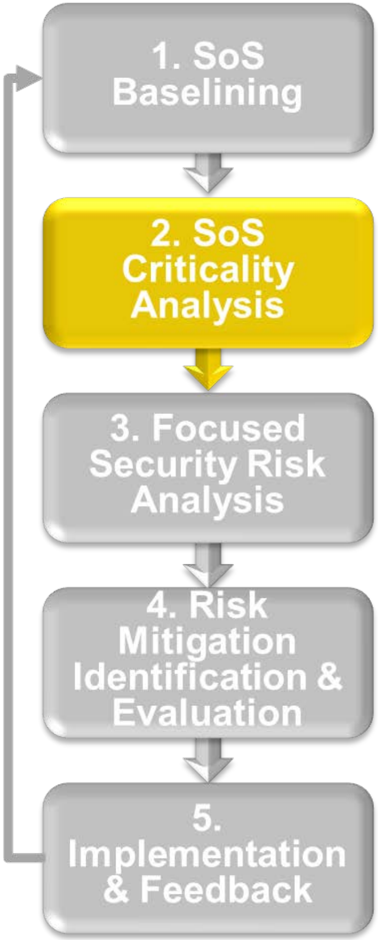
Implementation of SSE would ideally be done as part of SoSE

SoS Baselining

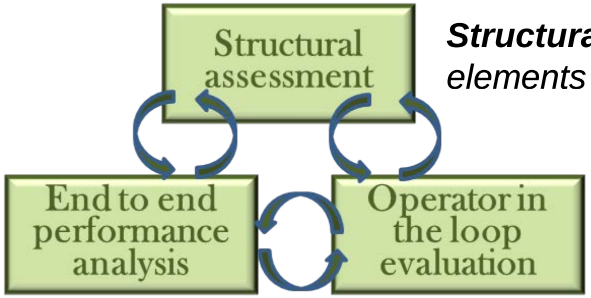

1. SoS Baselining
2. SoS Criticality Analysis
3. Focused Security Risk Analysis
4. Risk Mitigation Identification & Evaluation
5. Implementation & Feedback

- **Objective: Understand current configuration of SoS elements and their role in mission execution**
  - Mission & enabling infrastructure systems, links & interfaces
- **Growing number of approaches to addressing mission resilience to persistent threats**
  - To apply them requires a good understanding of the current ‘brownfield’ mission situation
  - May be straightforward when SoSE exists; if not, may require investments
- **Actions**
  - Understand mission CONOPS & outcomes, including end-end functionality & performance measures, describe current systems, links and their relationships; SoS dynamics; environments that support mission outcomes
- **Result/product is a technical foundation for analysis of critical elements, security risks and mediations**
- **Variety of approaches for defining and representing SoS/Mission**
  - I&I baselining tools based on mission threads and system data from OT
  - Standards-based BPM techniques to represent activities & sequential relationships
  - Architecture tools (e.g., DoDAF) for depicting systems & relationships
  - Model-based approaches (e.g., UML, SysML) to represent SoS elements, behaviors and relationships

SoS Criticality Analysis


1. SoS Baselining
2. SoS Criticality Analysis
3. Focused Security Risk Analysis
4. Risk Mitigation Identification & Evaluation
5. Implementation & Feedback

- **Objective: Identify key elements of the SoS essential to mission outcomes independent of any threats to them**
  - Mission & enabling infrastructure systems, links & interfaces
  - Helps align protection priorities with mission outcomes
- **Comprehensive protection of end-to-end SoS is not tractable**
  - Need a way to identify critical SoS elements and manage complexity
- **Identification of critical elements done independent of their risks or threats**
- **Various representation and analysis approaches can be applied**
  - Describe current systems, links and their relationships; SoS dynamics; environments that support mission outcomes
- **SoS Criticality Analysis consists of 3 interacting activities**

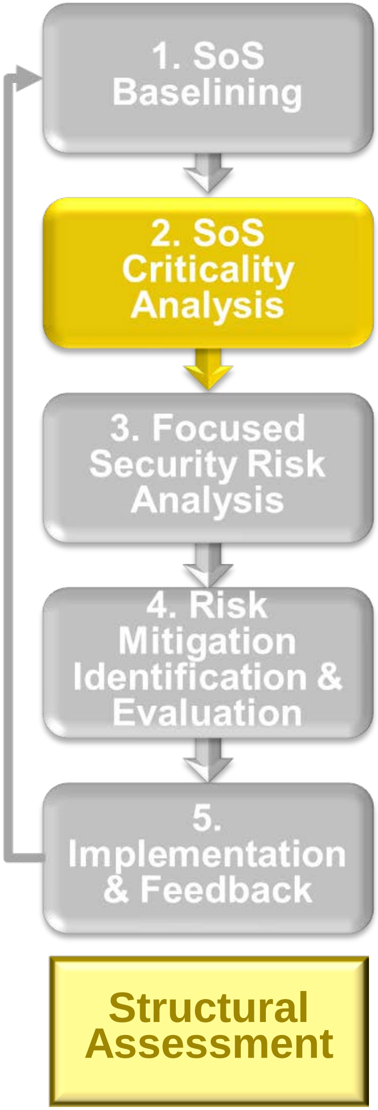

Structural assessment
End to end performance analysis
Operator in the loop evaluation

***Structural assessment** to identify critical elements and their interrelationships*

***Operator in the loop** evaluation for a realistic perspective on critical elements*

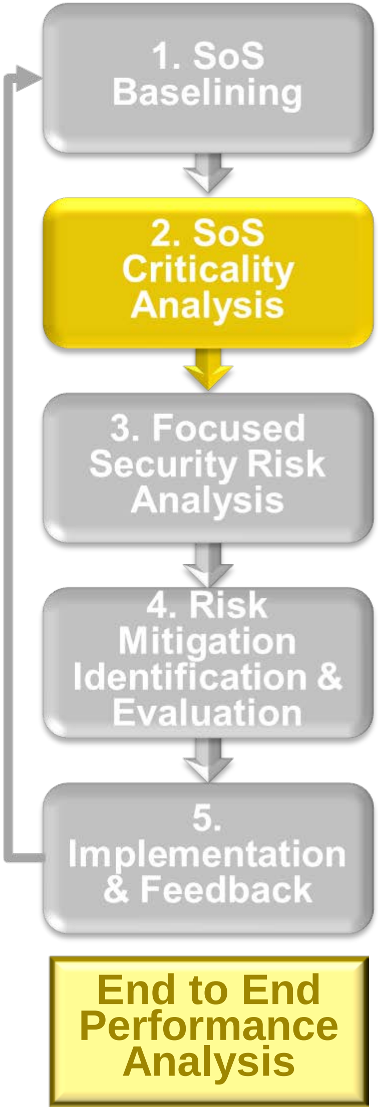
***End-to-end performance analysis** to understand SoS behavior & effects on mission outcomes of loss of, incursions or disruptions to critical elements*

SoS Criticality Analysis: Structural Assessment


1. SoS Baselining
2. SoS Criticality Analysis
3. Focused Security Risk Analysis
4. Risk Mitigation Identification & Evaluation
5. Implementation & Feedback
Structural Assessment

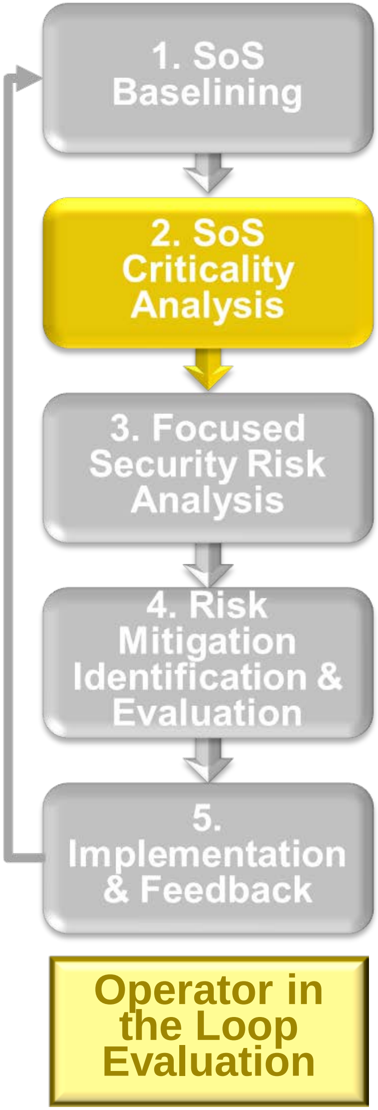
- **Objective: Identify SoS elements clearly critical or clearly not critical to mission as a starting point**
- **Actions**
  - Define end-to-end system flows and dependencies required for mission execution (drawing on SoS Baselining)
  - Based on analysis of SoS architecture, identify elements clearly on critical path for mission success
  - Also, identify those elements that, based on limited dependencies, redundancies, etc., can be ruled out from critical path
- **Results/products: Initial identification of SoS elements critical to mission outcomes**
- **Candidate tools & technical approaches**
  - Lessons learned from operations/user inputs; require validation via other methods.
  - BPMs support analysis of flows and paths through nodes and dependencies
  - DoDAF data for structural description of mission elements and relationships
  - Tools like System Architect for analysis of SoS elements
  - FDNA or other methodologies to model and measure the operational effectiveness of a mission network if one or more entities degrade or fail

SoS Criticality Analysis: End-to-End Performance Analysis


1. SoS Baselining
2. SoS Criticality Analysis
3. Focused Security Risk Analysis
4. Risk Mitigation Identification & Evaluation
5. Implementation & Feedback
End to End Performance Analysis

- **Objective: Understand SoS behavior and effects of loss of, incursions or disruptions to critical elements on mission outcomes**
- **Actions**
  - Identify **appropriate model of simulation** to represent missions, scenarios which reflect the mission context, and mission objectives including measures of performance and effectiveness
    - May be discrete event simulations (e.g. EADSIM, JIMM), agent based models, or other operations/systems analysis environments used to address other mission level issues in the particular mission areas
  - **Represent** the end-to-end mission thread, including systems and their behaviors, in a realistic operational context to simulate the mission in a selected set of scenarios
  - **Run series of excursions**
    - Base case to assess nominal mission performance and effective
    - A series of excursions where changes in the critical SoS elements are made to evaluate the impacts on mission performance and effectiveness
    - Design of experiments may be needed, when a large number of critical elements, to scope the set of excursion needed to identify key elements for detailed analysis
    - Facilities such as MEG could be employed to support these analysis
- **Results/Products: Set of priority SoS elements to be addressed for the security risk to the mission, supported by an understanding of the mission consequences of impacts to these elements**
  - May indicate the need for added structural analysis or provide data needed for certain structural analysis techniques (e.g. FDNA)

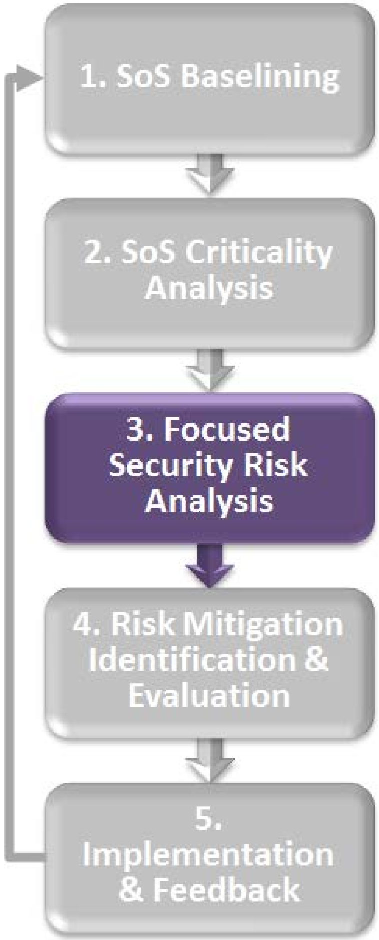
SoS Criticality Analysis: Operator in the Loop Evaluation


1. SoS Baselining
2. SoS Criticality Analysis
3. Focused Security Risk Analysis
4. Risk Mitigation Identification & Evaluation
5. Implementation & Feedback
Operator in the Loop Evaluation

- **Objective: Obtain a realistic perspective on critical elements in an operational context**
  - Puts a spotlight on the real-time, human dimension of potential solutions or workarounds not illuminated by other analytical approaches
  - Gain insights only available when working directly with the system user
- **Actions**
  - Collect and analyze data on critical elements identified in the structural and performance analyses, with a focus on the human elements of the operation
  - OIL techniques range from observing operations or operational exercises to collecting, analyzing and assessing data from structured experiments
- **Results/Products: Set of priority SoS elements to be addressed for the security risk to the mission**
  - May indicate a need for additional structural or performance analyses

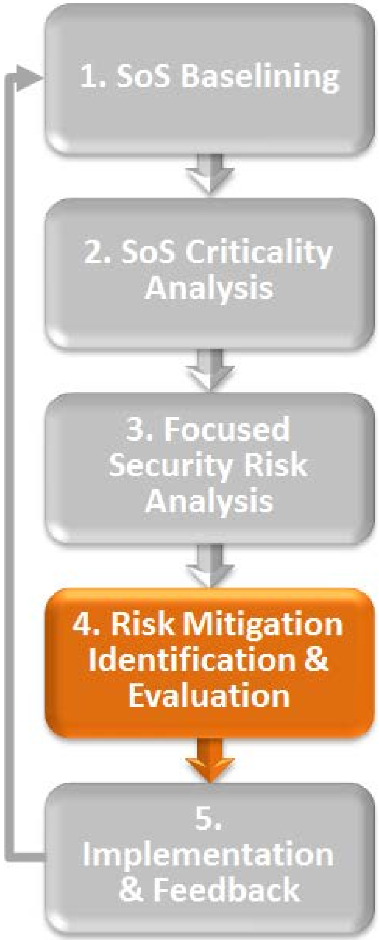
Approved for Public Release; Distribution Unlimited. 13-3376

Focused Security Risk Analysis


1. SoS Baselining
2. SoS Criticality Analysis
3. Focused Security Risk Analysis
4. Risk Mitigation Identification & Evaluation
5. Implementation & Feedback

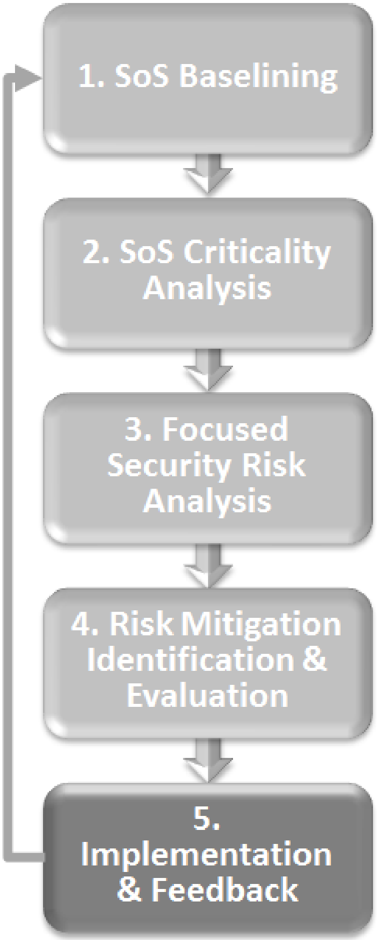
- **Objective: Determine whether elements critical to the mission are really at risk or are adequately protected**
  - Mission & enabling infrastructure systems, links and interfaces
- **Approach**
  - Employ currently available system-level threat, vulnerability and impact analysis techniques
  - Threat assessment determines threats to a critical element in the particular mission context
  - Vulnerability assessment determines how protected an element is to a threat, using PPP results as tested
- **Results/Products**
  - Characterization of the nature and severity of the security risks for each critical system element
  - Basis for establishing priority areas to improve assurance of mission outcomes

Risk Mitigation Identification and Evaluation


1. SoS Baselining
2. SoS Criticality Analysis
3. Focused Security Risk Analysis
4. Risk Mitigation Identification & Evaluation
5. Implementation & Feedback

- **Objective: Identify, evaluate and recommend a suite of risk mitigation changes to the SoS**
- **Approach**
  - Identify options for addressing risks and evaluate them for impact on mission outcomes, technical feasibility, affordability, etc., including dependencies among composite solution options
    - Identification draws on growing knowledge base of countermeasures, best practices and design patterns
    - Evaluation leverages methods used to identify critical SoS elements to assess predicted impact of options, including composite set of options
    - Selection depends on system-level considerations (technical feasibility and cost, system development plans, & capacity for change)
  - Assessing right mix of mitigations to provide desired assurance
    - May require additional analysis using criticality analysis methods
    - Other portfolio analysis approaches to understand mix of investments to achieve best ROI or mission outcome value
- **Results/Products**
  - Plan for composite set of changes to systems to improve security of SoS to achieve mission outcomes

Implementation and Feedback


1. SoS Baselining
2. SoS Criticality Analysis
3. Focused Security Risk Analysis
4. Risk Mitigation Identification & Evaluation
5. Implementation & Feedback

- **Objective: Execute the changes to systems resulting from preceding steps to improve mission outcomes**
  - Includes planning, implementation, integration and testing of changes and their impact on the SoS and mission assurance
  - Usually accomplished as part of system development, upgrade or technology refresh
  - Feedback an ongoing process
- **Approach**
  - Implementation is part of the normal system acquisition processes
  - SoS-level action is to monitor implementation for issues that could impact SoS
    - Example: identification of technical issues in one system that could impact another and mitigations to assure continuity of operations
  - Changes in systems are reflected in an updated SoS baseline
- **Results/Products**
  - Updates to systems to increase security of end-to-end SoS and reduce risk to mission outcomes

SoS SSE Framework as Bridge between Acquisition/Engineering and Operations

Acquisition

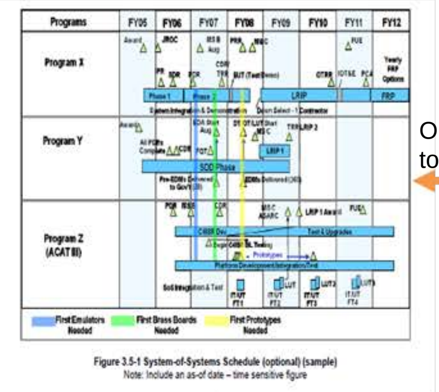
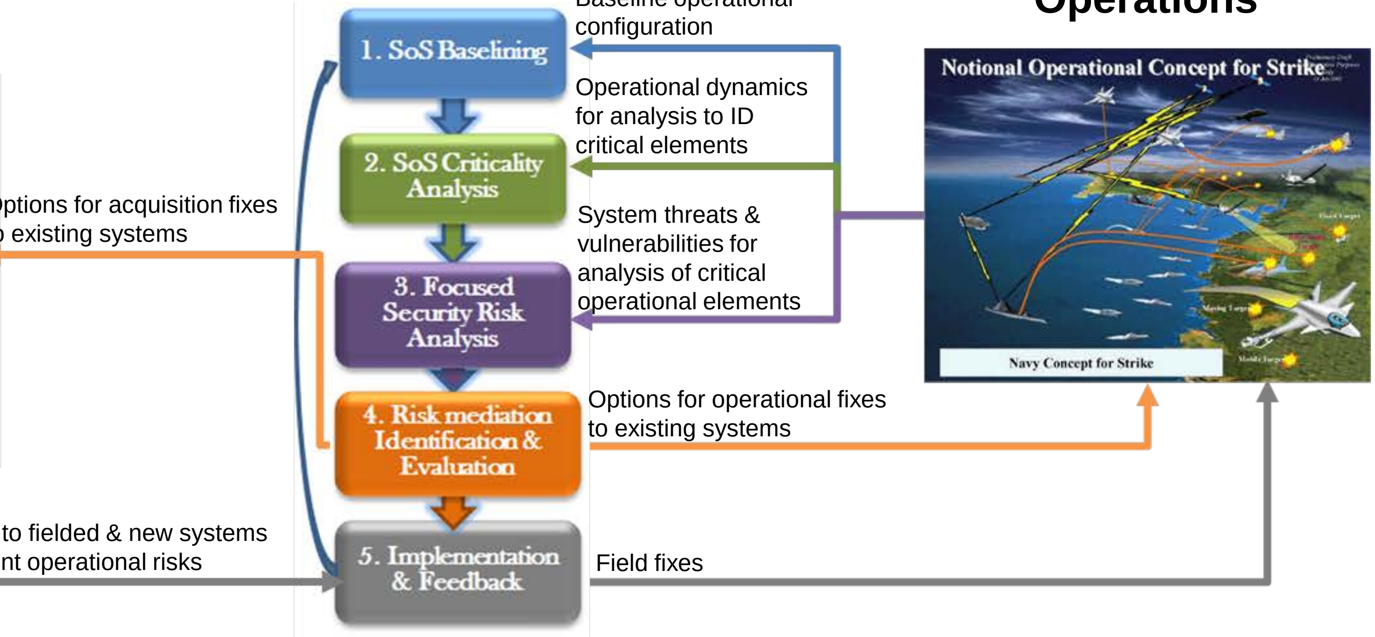


Figure 3.5-1 System-of-Systems Schedule (optional) (sample)
Note: Include an as-of date – time sensitive figure

Operations


1. SoS Baselining
2. SoS Criticality Analysis
3. Focused Security Risk Analysis
4. Risk mediation Identification & Evaluation
5. Implementation & Feedback
Notional Operational Concept for Strike
Navy Concept for Strike

Baseline operational configuration

Operational dynamics for analysis to ID critical elements

System threats & vulnerabilities for analysis of critical operational elements

Options for acquisition fixes to existing systems

Options for operational fixes to existing systems

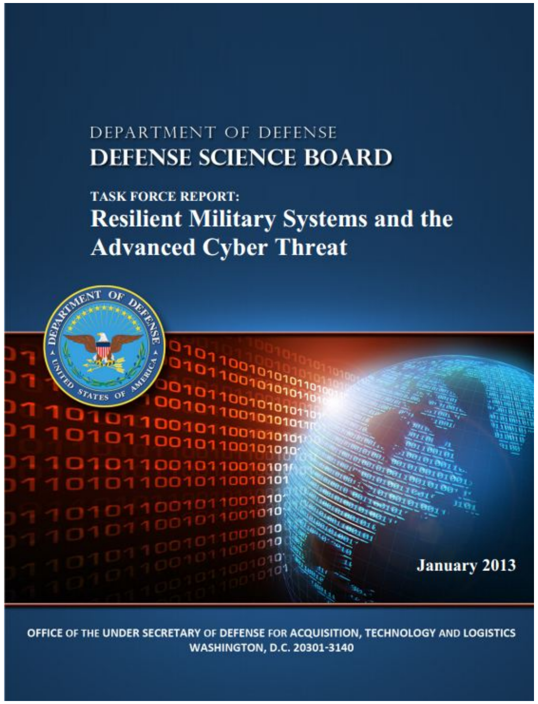
Implement fixes to fielded & new systems to address current operational risks

Field fixes

Implement "fixes" to fielded and new systems vs. current operational risks

Potential Follow On Efforts

- **NDIA SE Division SoS and SSE committees collaboration**
  - Based on the presentation at the October NDIA SE Conference & December NDIA SE Division discussions
- **Conduct pilots**
  - Vet framework with SoS programs interviewed in SoS SSE baselining activity
  - Possibly in key DoD mission area security engineering initiatives
  - Develop greater insight into mix of approaches to support SoS SSE in different situations
  - Determine data needs, sources and strategies
- **Inform in-progress refinements to DoD Program Protection Planning and Trusted Systems and Networks (TSN) processes**
- **Inform systems engineering research investments**



DEPARTMENT OF DEFENSE
DEFENSE SCIENCE BOARD

TASK FORCE REPORT:
Resilient Military Systems and the
Advanced Cyber Threat

January 2013

OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY AND LOGISTICS
WASHINGTON, D.C. 20301-3140

Contact Information

George Rebovich

Director, Systems Engineering Practice Office

The MITRE Corporation

Bedford, MA, USA 01720

Email: grebovic@mitre.org