SYSTEMS ENGINEERING RESEARCH CENTER

VIRGINIA TECH

STEVENS INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY®

UNIVERSITY of VIRGINIA

WRT-1033: Methods to Evaluate Cost/Technical Risk Opportunity Decisions for Security Assurance in Design

Tom McDermott (Stevens), Peter Beling (Va Tech)
Tim Sherburne, Ian Roessle, Stephen Adams (VT); Megan Clifford (Stevens)

Sponsor: OUSD(R&E)

WASHINGTON DC | VIRTUAL
NOV. 2-4 2021
ANNUAL SPONSOR RESEARCH REVIEW

Agenda

- Motivation
- Project Scope
- Outreach
- Mission Engineering
- Dynamic Simulation
- Formal Assurance
- Silverfish Case Study

TUTORIALS

DIGITAL ENGINEERING TUTORIAL
Dr. Mark Blackburn – Stevens Institute of Technology

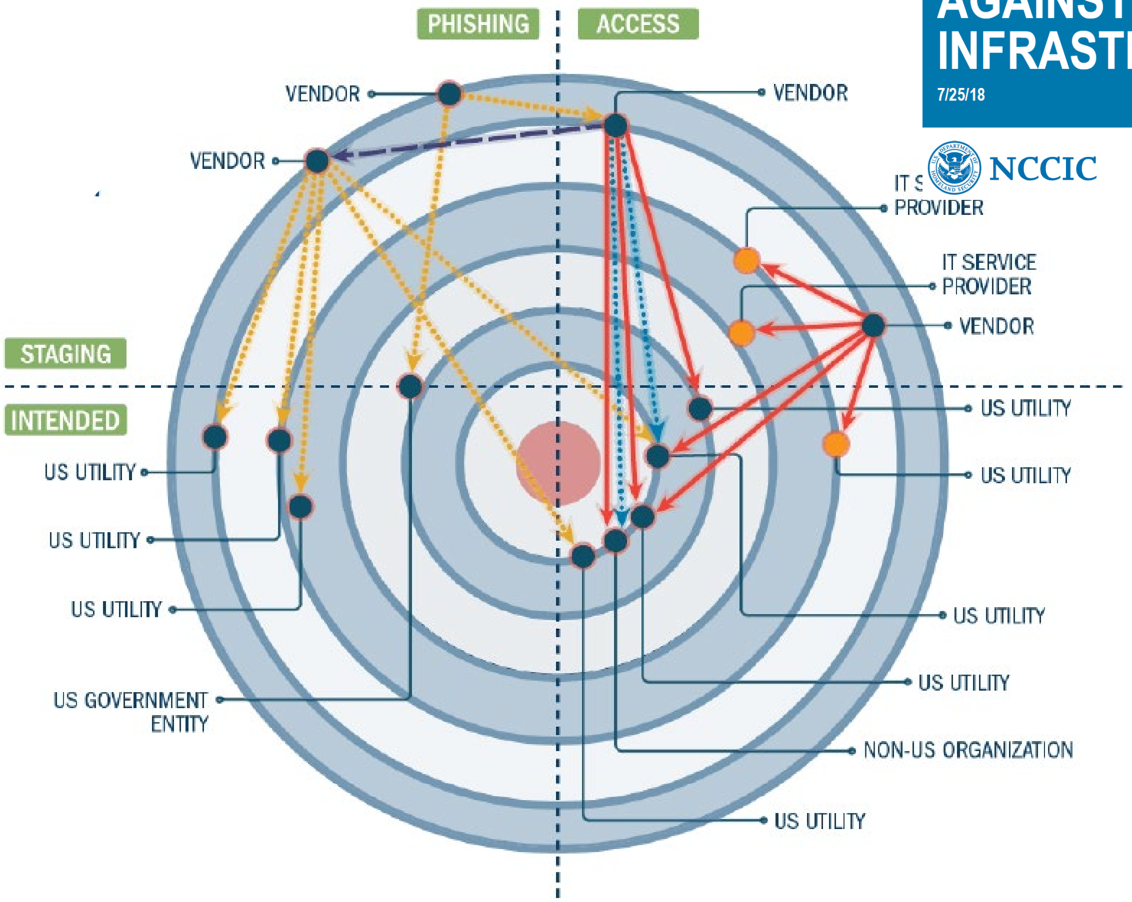
- Skyzer Surrogate Pilot Overview and MBSE Cost Model Use Case with Model Tour Demonstration

SECURITY ENGINEERING TUTORIAL
Dr. Peter Beling – Virginia Tech

- SERC Systems and Cyber Resilience Modeling

Motivation: Advanced Persistent Threat in Critical Systems

- Social Engineering
  - Research, data harvesting
- Physical Engineering
  - Components, network ops
- Vulnerabilities
  - Zero day
- Attacks
  - Exploits,
    prioritized loss scenarios
- Execute outcomes
  - Lack of predictive models
- Resilience
  - Design-in, test-in
  - Performance measures




TLP:WHIT

NCCIC | NATIONAL CYBERSECURITY & COMMUNICATIONS INTEGRATION CENTER

AWARENESS BRIEFING:

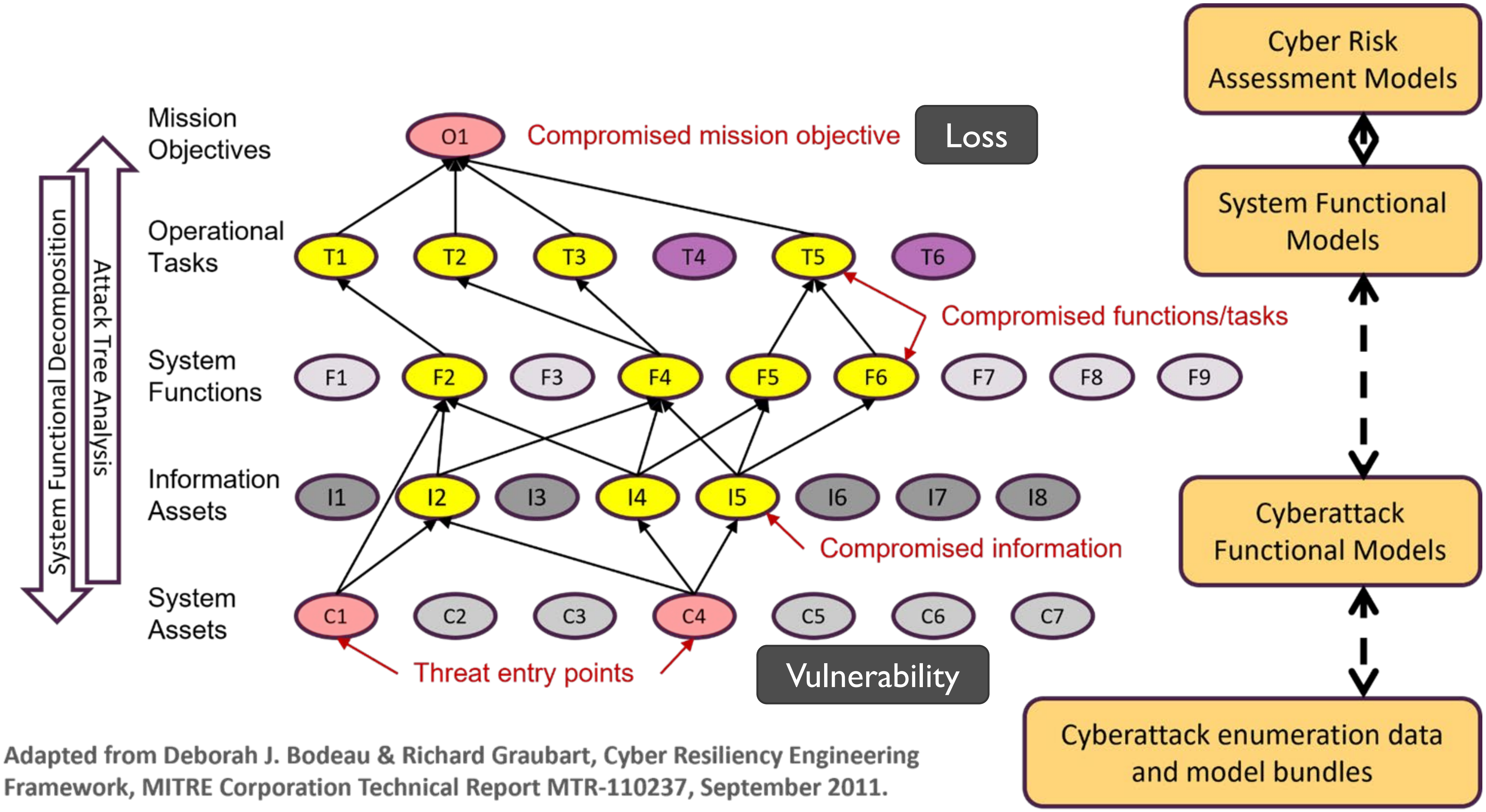
RUSSIAN ACTIVITY AGAINST CRITICAL INFRASTRUCTURE

7/25/18

NCCIC

Audio Information:
Dial-In: 888-221-6227

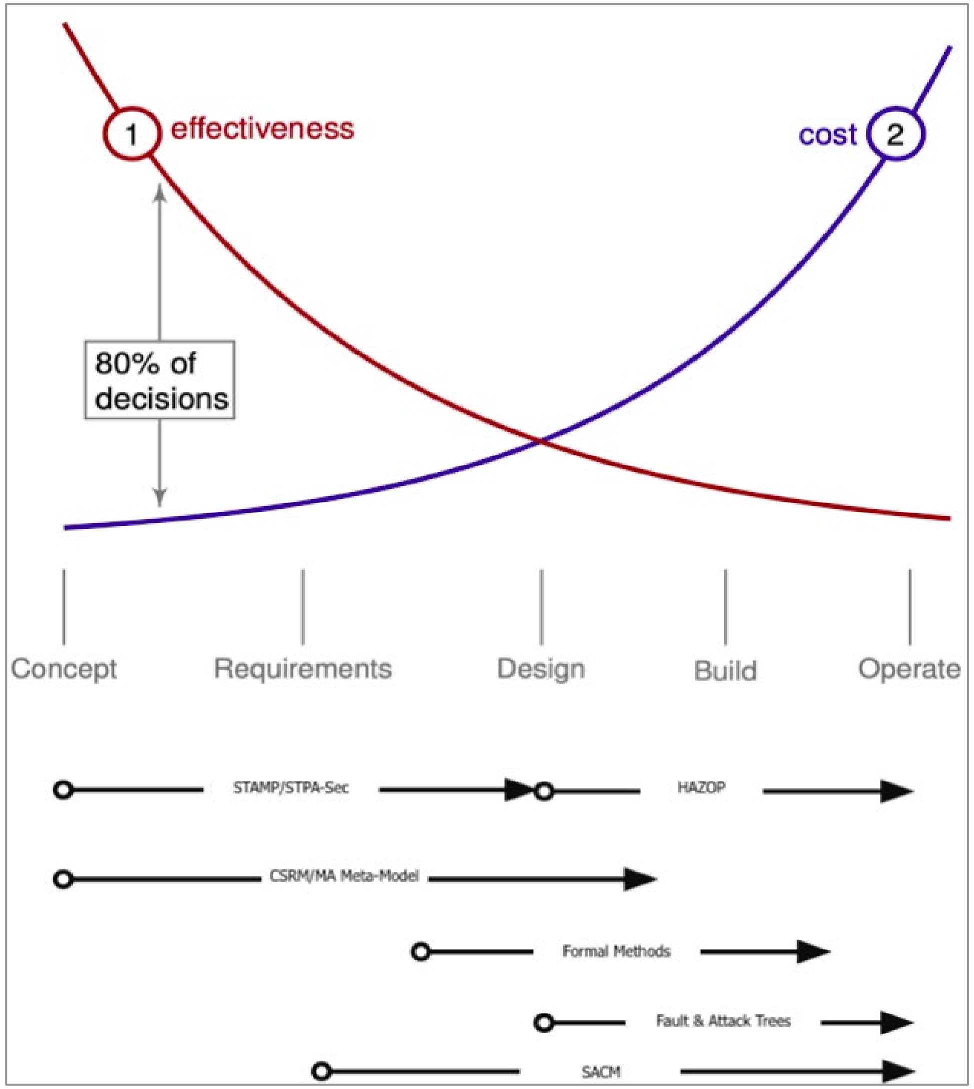
Functional Modeling in Cyber Resilience Engineering



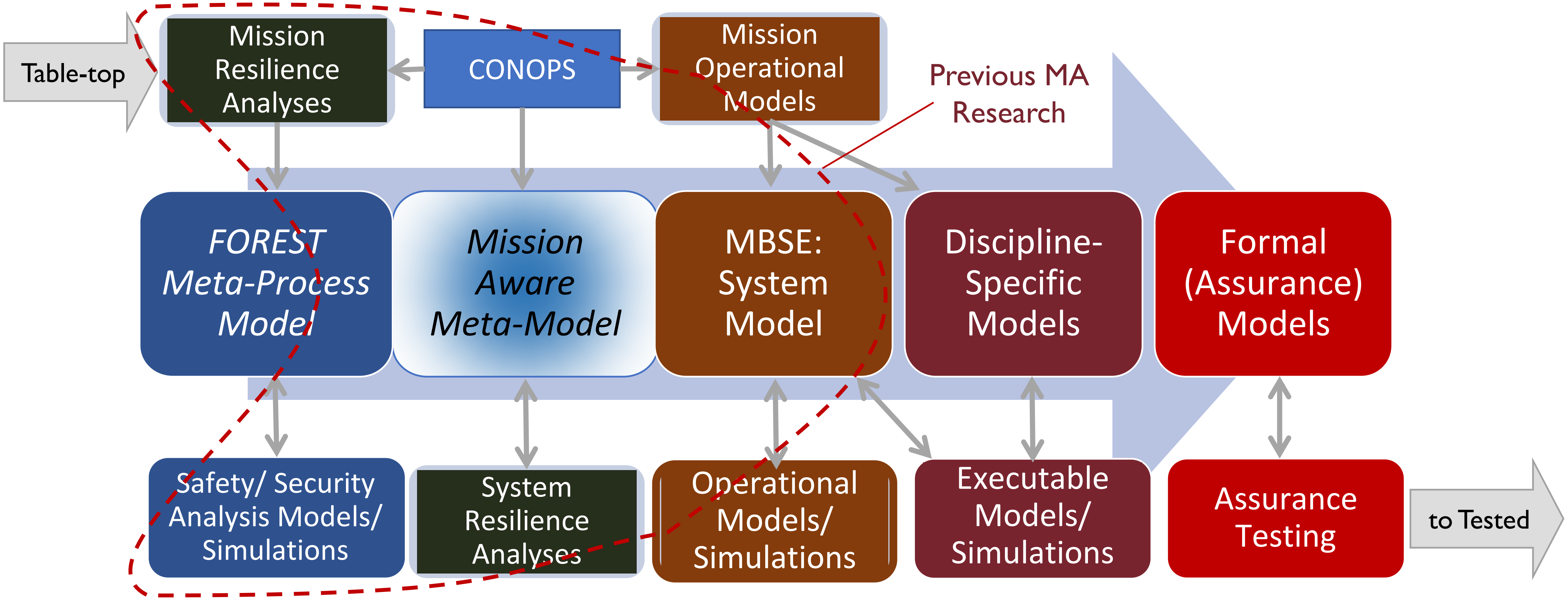
Adapted from Deborah J. Bodeau & Richard Graubart, Cyber Resiliency Engineering Framework, MITRE Corporation Technical Report MTR-110237, September 2011.

Approach: Resilience and Assurance Methodologies – full System Life Cycle

- Need rigorous methods and tools usable in all stages of the SE process
  - From Mission Engineering to Developmental & Operational Test
- Earlier focus on loss causation and resilience
- Later focus on risk management and assurance
- Continuous evaluation of assurance-related quality attributes

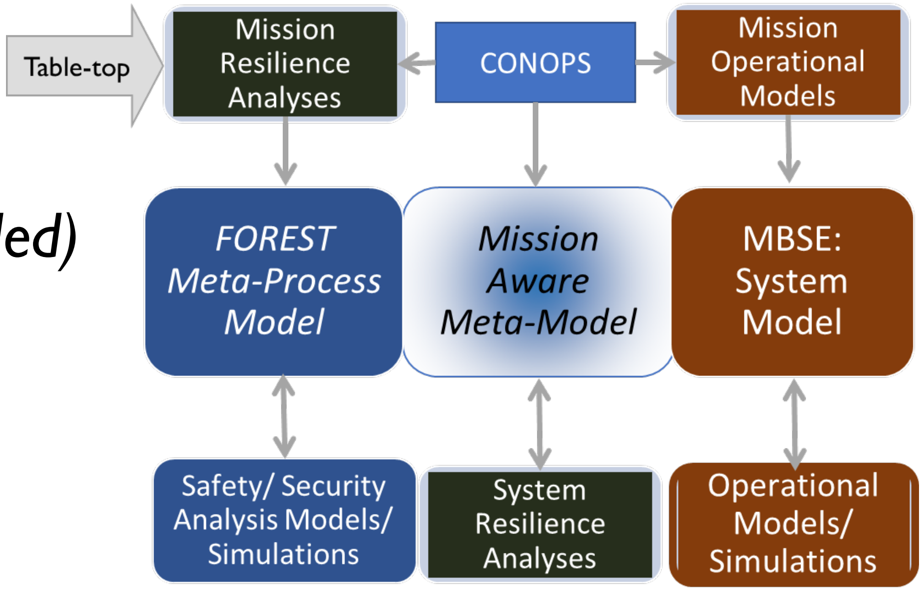


Project Scope

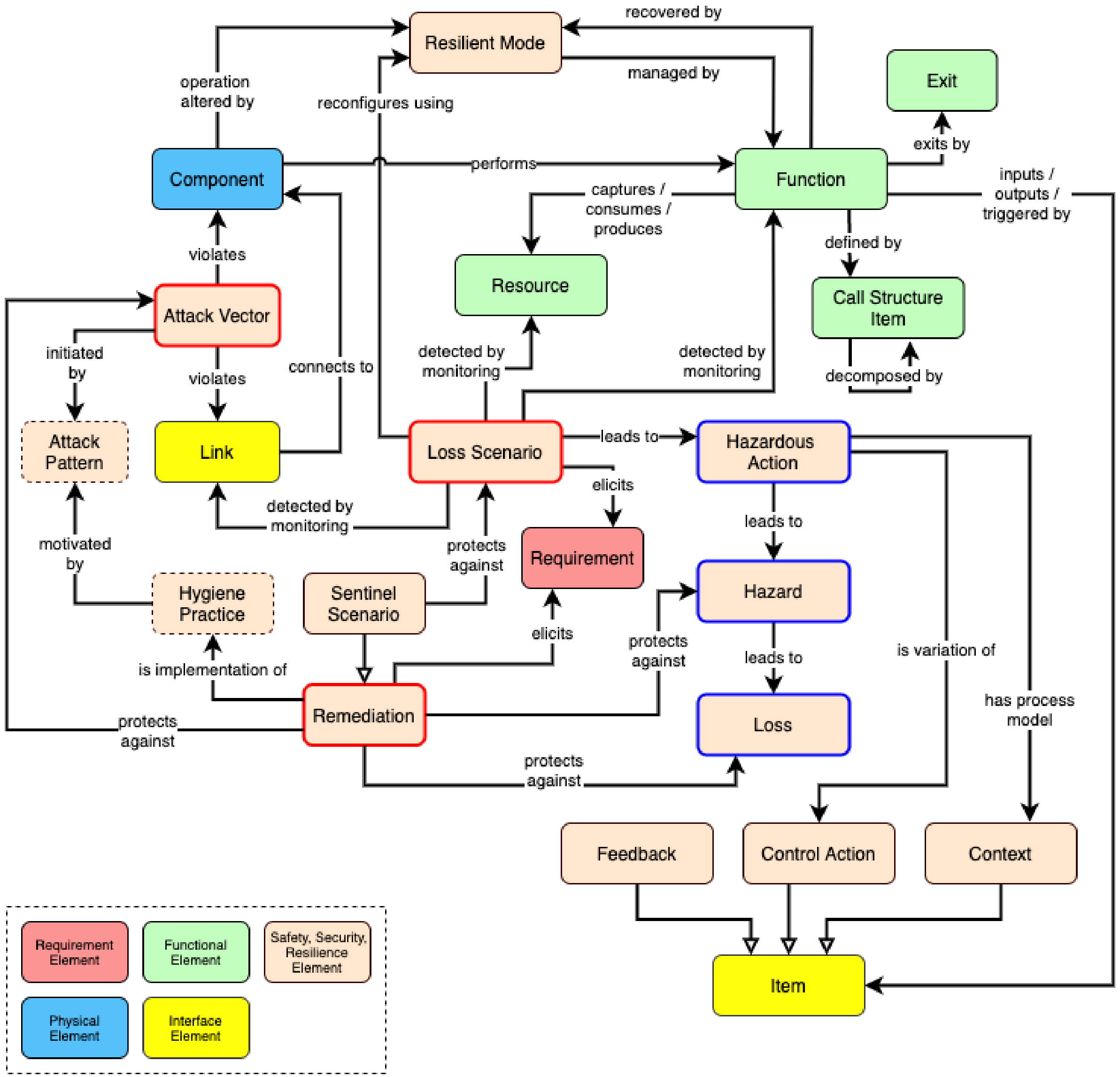


Mission Engineering

- The research shall:
  - Conduct a thorough analysis of the current Meta-Model and understand where levels are underserved by the data and information obtainable within the community to address specific **mission engineering** system capability needs.
  - *Development of FOREST & TREEs*
  - *Standardized model relationships*
  - *Integration of Cyber Survivability Attributes*
  - *Integration into cyber "table-tops" (experience needed)*
  - *Dissemination in tutorial form*
  - *Transition to DAU training*



Mission Aware Meta-Model: Necessary Information



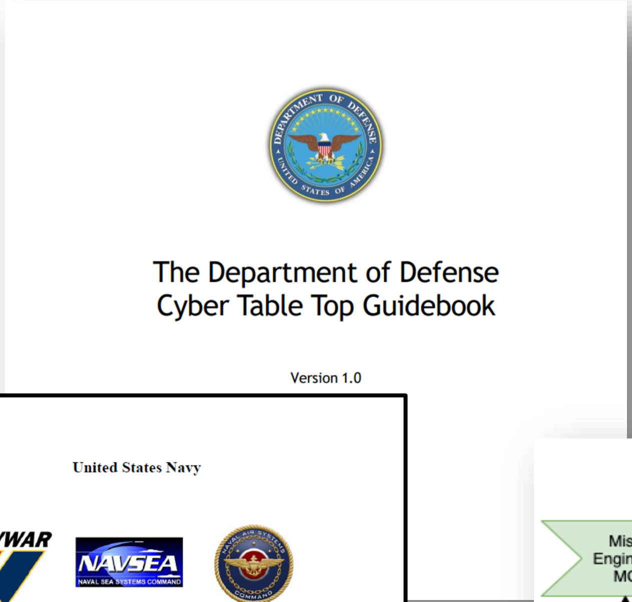
MISSION AWARE

CSRM Steps & Associated Meta-Model Entities:

1. System Description (Mission, Architecture, Behavior)
   - Use Case / Requirement
   - Component, Link
   - Function, Exit, Resource, Control-Action, Feedback, Context, Call Structure Item
2. Operational Risk Assessment
   - Loss, Hazard, Hazardous Action
3. Prioritized Resilience Solutions
   - Resilient Mode
4. Cyber Vulnerabilities Assessment
   - Loss-Scenario, Remediation, Elicited Requirements

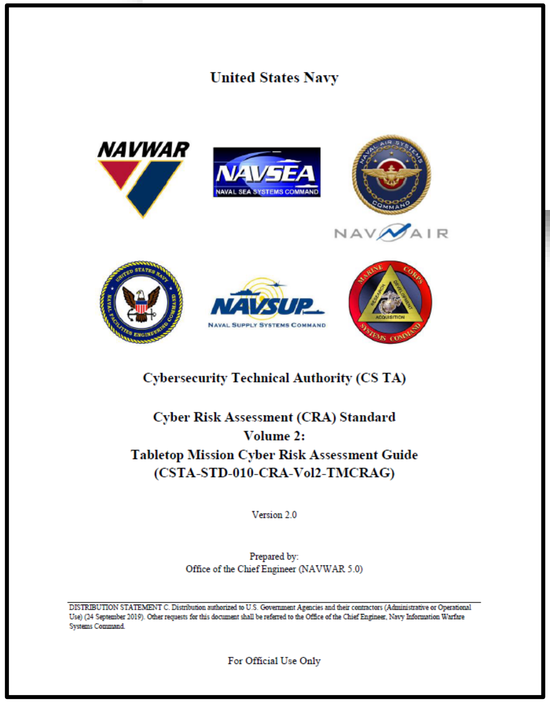
Typically determined in cyber table-top exercises (TTX)

Cyber TTX



The Department of Defense
Cyber Table Top Guidebook

Version 1.0



United States Navy

Cybersecurity Technical Authority (CS TA)

Cyber Risk Assessment (CRA) Standard
Volume 2:
Tabletop Mission Cyber Risk Assessment Guide
(CSTA-STD-010-CRA-Vol2-TMCRAG)

Version 2.0

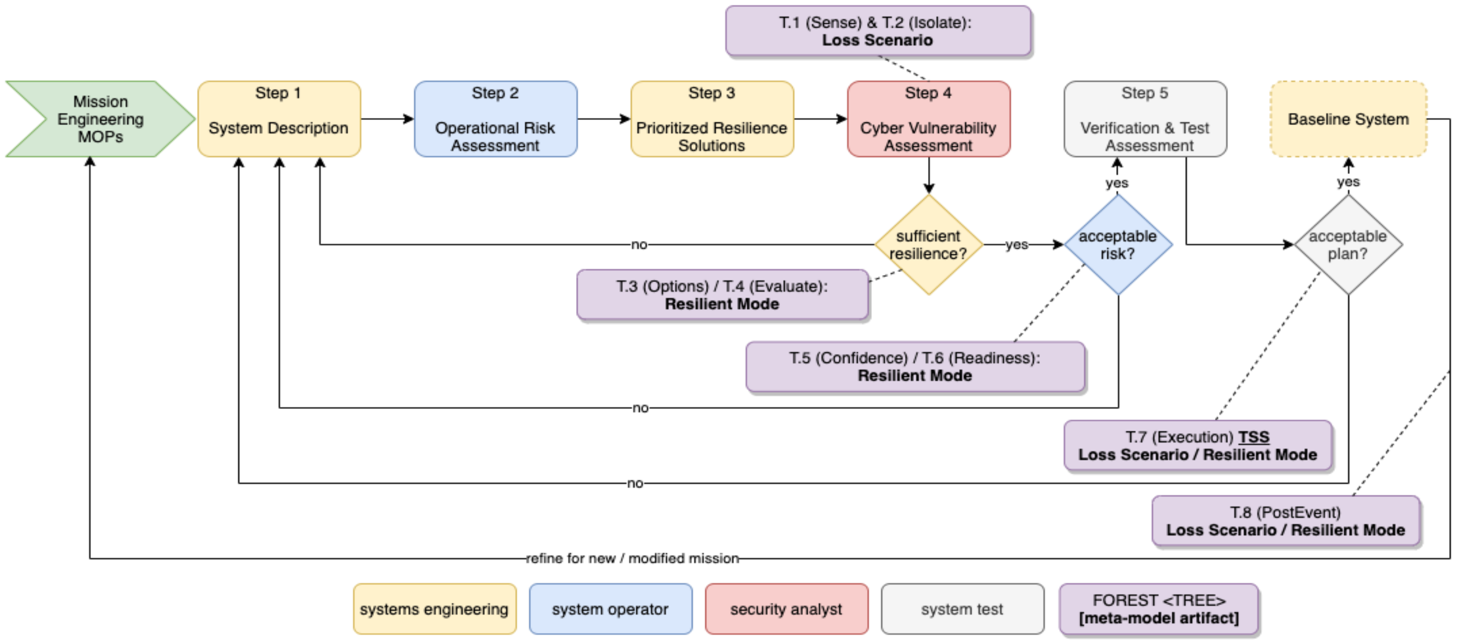
Prepared by:
Office of the Chief Engineer (NAVWAR 5.0)

DISTRIBUTION STATEMENT C. Distribution authorized to U.S. Government Agencies and their contractors (Administrative or Operational Use) (24 September 2019). Other requests for this document shall be referred to the Office of the Chief Engineer, Navy Information Warfare Systems Command.

For Official Use Only

Issues:

- Identifying definitive system information/ architecture
- Timely and relevant intelligence community support
- Finding the right people
- Need to be doing much earlier in engineering V



Example Cyber Vulnerability Assessment

Remediation	is implementation of: Hygiene Practice	protects against: Attack Vector
REM.CH.MON.1:Forensic Logging	CPP.LO.1:Log, audit, or monitor systems	SF.CAPEC.122:Privilege Abuse
REM.CH.PRO.1:Deployment Account	CPP.AC.1:Eliminate Default Access CPP.AC.2:Physical or Procedural Access CPP.AC.3:Require Authentication CPP.AD.1:Minimize administrative privileges CPP.UI.1:Unique Identifiers	SF.CAPEC.122:Privilege Abuse
REM.RES.DEF.1:Link encryption	CPP.BD.1:Control and protect information	LS.1:Manipulated Fire Command LS.2:Situational Injection RR.CAPEC.94:Radio Relay Man in the Middle RR.CAPEC.117:Radio Relay Interception
REM.RES.DEF.2:Voice only command and control		CC.CAPEC.607:Command and Control Jamming
REM.RES.DEF.3:Sentinel: Field - OBS: Measured Boot	CPP.CM.1:Manage configurations	LS.4:Tampered Deployment
	CPP.CM.3:Constrain installation	OBS.CAPEC.439.CONFIG:Obstacle Configuration Modification during Distribution
	CPP.SI.1:Inventory software	OBS.CAPEC.439.MALWARE:Obstacle Malware during Distribution
	CPP.VU.1:Vulnerability detection	OBS.CAPEC.439.SW:Obstacle Software Modification during Distribution
REM.RES.DR.1:Sentinel: Vehicle - Weapon Mis-Fire		FC.CAPEC.438:Fire Control Modification during Manufacture LS.1:Manipulated Fire Command
REM.RES.DR.2:Sentinel: Vehicle - Weapon Delay Fire		FC.CAPEC.438:Fire Control Modification during Manufacture LS.5:Delayed Fire Command
REM.RES.DR.3:Sentinel: Field - Situational Delay		IR.CAPEC.438:IR Modification during Manufacture LS.3:Situational Delay
REM.RES.DR.4:Sentinel: Field - Situational Injection		LS.2:Situational Injection RR.CAPEC.594:Radio Relay Injection
REM.RES.HARD.1:Isolate fire control and sit-		H.1:Weapon mis-fire.

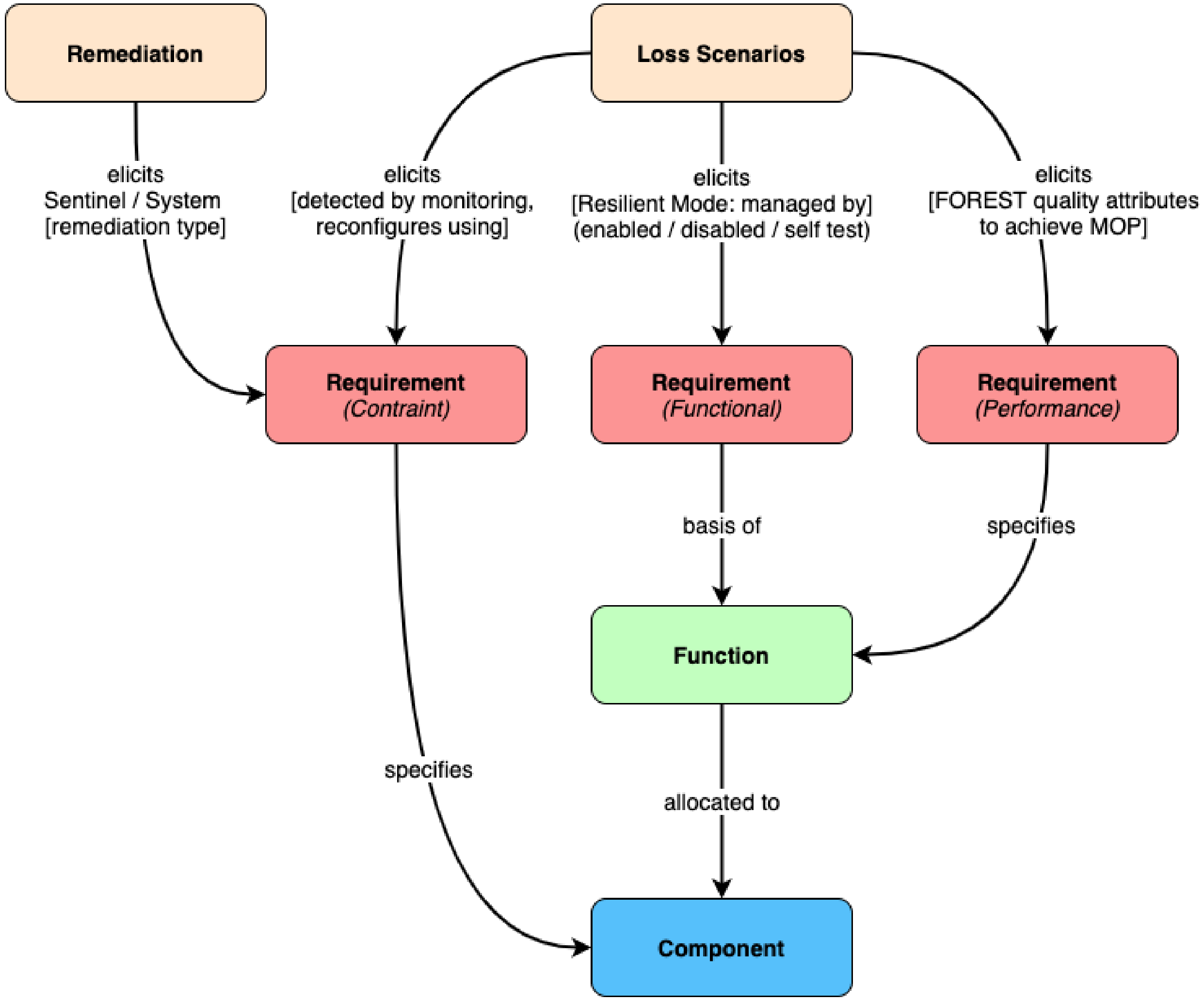
Remediation Types:

- Hygiene Practice
- Diverse Redundancy
- Defensive / Hardening

Silverfish Example Loss Scenarios

Loss Scenario	leads to: Hazardous Action	reconfigures using: Resilient Mode
LS.1:Manipulated Fire Command	HCA.1:Incorrect Fire	RM.2:Diverse Redundant Fire Control
LS.2:Situational Injection	HCA.2:No Fire	RM.1:Diverse Redundant Radio Relay
LS.3:Situational Delay	HCA.2:No Fire	RM.1:Diverse Redundant Radio Relay RM.3:Diverse Redundant IR Sensors RM.5:Operator Reposition
LS.4:Tampered Deployment	HCA.3:Unable to set Location	RM.4:Obstacle Restore
LS.5:Delayed Fire Command	HCA.2:No Fire	

Metamodel: Elicited Requirements



Elicited Requirement Types:

- Constraints
- Functional
- Performance

Cyber Survivability Engineering (Steve Pitcher J-6)

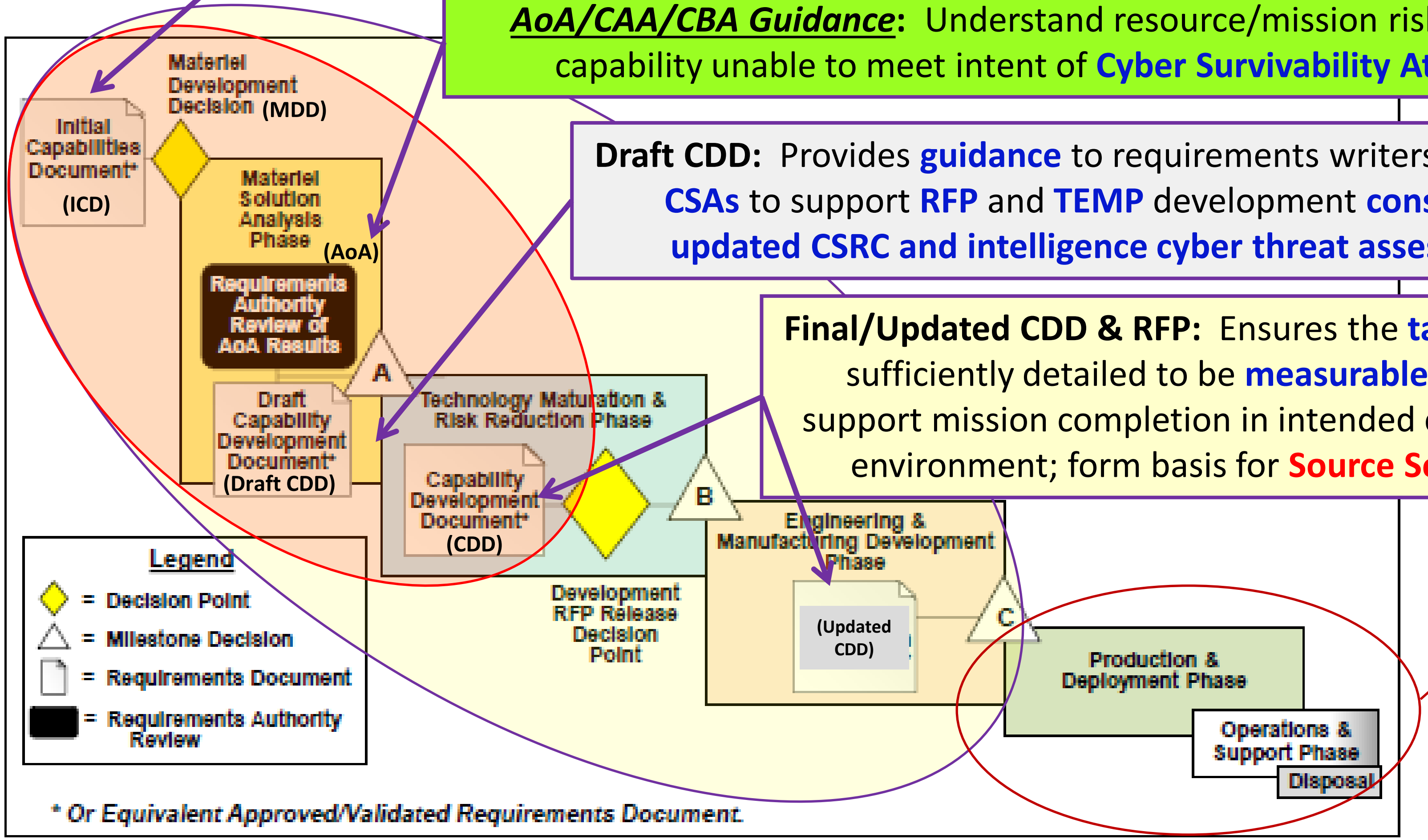
ICD: **Cyber Survivability Risk Category (CSRC) summary statement** incorporates an unclassified **projected cyber threat** and **mitigations** before formal threat assessment

AoA/CAA/CBA Guidance: Understand resource/mission risk implications if capability unable to meet intent of **Cyber Survivability Attributes (CSAs)**

Draft CDD: Provides **guidance** to requirements writers on **tailoring of CSAs** to support **RFP** and **TEMP** development **consistent with the updated CSRC and intelligence cyber threat assessment** at MS A

Final/Updated CDD & RFP: Ensures the **tailored CSAs** are sufficiently detailed to be **measurable and testable** to support mission completion in intended cyber-contested environment; form basis for **Source Selection Criteria**

AoA: Analysis of Alternatives
CAA: Course of Action Analysis
CBA: Capability Based Assessment



Gap to address

Generally Independent of Design Lifecycle Considerations

CSA Top-Level Requirements

KPP	CSA Number	Description
Prevent	CSA-01	Control Access
	CSA-02	Reduce System's Cyber Detectability
	CSA-03	Secure Transmissions and Communications
	CSA-04	Protect System's Information from Exploitation
	CSA-05	Partition and Ensure Critical Functions at Mission Completion Performance Levels
	CSA-06	Minimize and Harden Attack Surfaces
Mitigate	CSA-07	Baseline and Monitor Systems and Detect Anomalies
	CSA-08	Manage System Performance if Degraded by Cyber Events
Recover	CSA-09	Recover System Capabilities
Adapt	CSA-10	Actively Manage System's Configuration to Achieve and Maintain an Operationally Relevant Cyber Survivability Risk Posture (CSRP)

*MITRE, Relationships Between Cyber Resiliency Constructs and Cyber Survivability Attributes (CSA), 2019

CSA	Req Number	Description
CSA-07	CSA.07.1	The system shall monitor operational parameters, boundaries, and configuration controls.
	CSA.07.2	The system shall analyze performance through a baseline comparison to detect anomalies and attacks.
	CSA.07.3	The system shall generate and store logs.
CSA-08	CSA.08.1	The system shall alert users of detected anomalies and attacks.
	CSA.08.2	The system shall provide capabilities to shed non-mission-critical functions, systems/sub-systems, and interfaces.
	CSA.08.3	The system shall maintain mission-critical functions in a cyber contested operational environment during/after observed anomaly(ies).
	CSA.08.4	The system shall maintain safety-critical functions in a cyber contested operational environment during/after observed anomaly(ies).
	CSA.08.5	The system shall fail secure when mission-critical functions are no longer operational in a contested environment.
	CSA.08.6	The system shall maintain flight-critical functions in a cyber contested operational environment during/after observed anomaly(ies).
CSA-09	CSA.09.1	The system shall provide the capability to recover to a known state in near real time.
CSA-10	CSA.10.1	The system shall have the capability to update scans to ensure appropriate, applicable requirements are captured (e.g. STIGS, SRG, etc.) for: (a) hardware (b) software (c) firmware
	CSA-10.2	Actively manage System's Configurations to achieve and maintain an Operationally Relevent Cyber Survivability Risk Posture (CSRP).

Example Elicited Requirements - System

Requirement	Type	elicited by: LS
SF.600.1:Silverfish shall provide fire control action monitor.	Constraint	LS.1:Manipulated Fire Command
SF.600.2:Silverfish shall provide fire control timing monitor.	Constraint	LS.5:Delayed Fire Command
SF.600.3:Silverfish shall provide situational sensor report consistency monitor.	Constraint	LS.2:Situational Injection
SF.600.4:Silverfish shall provide situational sensor report timing monitor.	Constraint	LS.3:Situational Delay
SF.600.5:Silverfish shall provide measured boot monitor.	Constraint	LS.4:Tampered Deployment
SF.600.10:Silverfish shall provide component self test operations.	Functional	LS.1:Manipulated Fire Command LS.2:Situational Injection LS.3:Situational Delay LS.4:Tampered Deployment LS.5:Delayed Fire Command
SF.600.11:Silverfish shall provide fire control redundancy management controls.	Functional	LS.1:Manipulated Fire Command LS.5:Delayed Fire Command
SF.600.12:Silverfish shall provide fire control self test operations.	Functional	LS.1:Manipulated Fire Command LS.5:Delayed Fire Command
SF.600.13:Silverfish shall provide IR sensor redundancy management controls.	Functional	LS.2:Situational Injection LS.3:Situational Delay
SF.600.14:Silverfish shall provide obstacle restore management controls.	Functional	LS.4:Tampered Deployment
SF.600.15:Silverfish shall provide radio relay redundancy management controls.	Functional	LS.2:Situational Injection LS.3:Situational Delay LS.5:Delayed Fire Command
SF.600.16:Silverfish shall provide situational aware self test operations	Functional	LS.2:Situational Injection

Elicited System Requirement Sources:

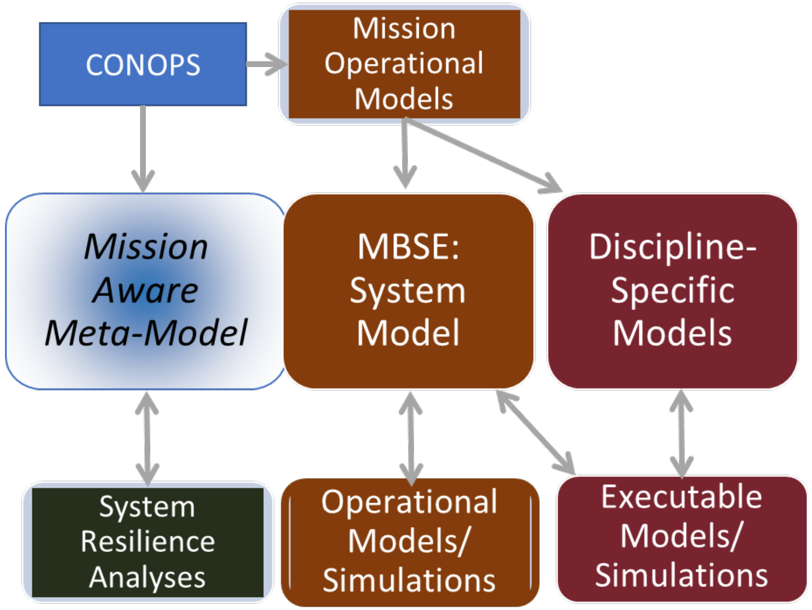
- Loss Scenarios
  - Enable Sensing / Isolation by Sentinel
  - Associated Resilient Mode Management (enable / disable / self-test)
- Remediation
  - Provides Sentinel for protection against Loss Scenario

Remediation	protects against: LS/AV	elicits: Requirement
REM.RES.DR.1:Sentinel: Vehicle - Weapon Mis-Fire	FC.CAPEC.438:Fire Control Modification during Manufacture LS.1:Manipulated Fire Command	MA.100.1.1:The vehicle Sentinel shall protect against manipulated fire commands.
REM.RES.DR.2:Sentinel: Vehicle - Weapon Delay Fire	FC.CAPEC.438:Fire Control Modification during Manufacture LS.5:Delayed Fire Command	MA.100.1.2:The vehicle Sentinel shall protect against delayed fire.
REM.RES.DR.3:Sentinel: Field - Situational Delay	IR.CAPEC.438:IR Modification during Manufacture LS.3:Situational Delay	MA.100.2.2:The field Sentinel shall protect against situational delay.
REM.RES.DR.4:Sentinel: Field - Situational Injection	LS.2:Situational Injection RR.CAPEC.594:Radio Relay Injection	MA.100.2.1:The field Sentinel shall protect against situational injection.

Dynamic Simulations

- The research shall:
  - Work with Meta-Model to initiate a framework for **patterns**: system models and threat models to produce scalable graph structures for system analysis.

  - *Extended the MA meta-model to support specification of simulation constructs*
  - *Developed an extensive set of MA resilience metrics - demonstrated in the Silverfish model*
  - *Standardized resilience patterns*
  - *MBSE tools still lack necessary integration with event-driven and activity-based simulation tools*

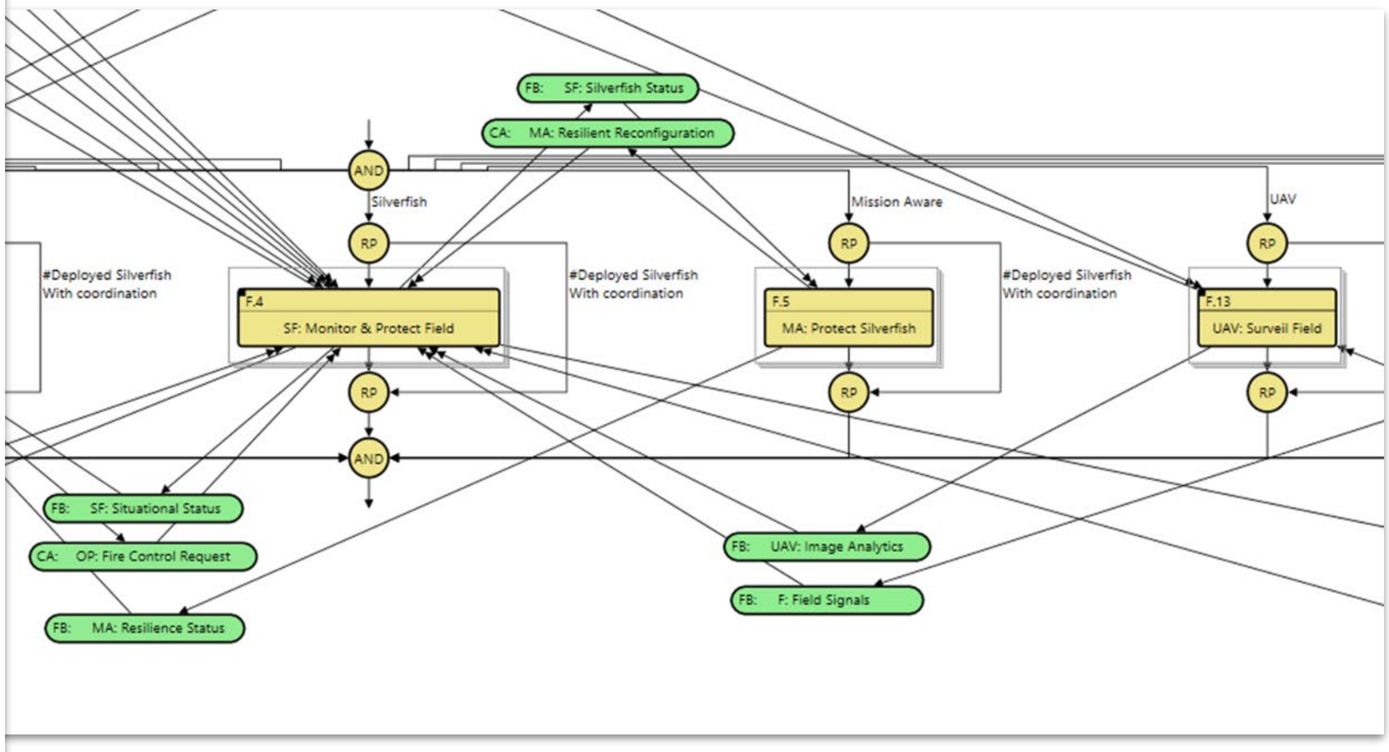


Example System Behavior (Functions) via Control Structure

System Function	Description	decomposed by: Function	triggered by: Control Action
F.4.10:SF: Fire	Select and fire one or more munitions for one or more obstacles.	F.4.10.1:CS: Input Fire Munition Command F.4.10.2:RR: Transfer Fire Munition Command F.4.10.3:OBS: Initiate Fire Munition	OP.1.1:OP: CA: L1-Fire
F.4.10.1:CS: Input Fire Munition Command	Process operator input to fire one or more munitions for one or more obstacles, manage munition fire state, and wireless transmit fire command to selected munitions.		OP.1.1.1:CS: L2-Operator Fire Control Action
F.4.10.2:RR: Transfer Fire Munition Command	Wirelessly transfer munition fire commands from control station to obstacles.		OP.1.1.2:RR: L2-Transfer Fire Control Action
F.4.10.3:OBS: Initiate Fire Munition	Detonate selected mentions and update munition state to fired.		OP.1.1.3:OBS: L2-Initiate Fire Control Action
F.4.13:SF: Monitor Field	Monitor field for physical attackers (human or vehicle) by fusing UAV, IR, Acoustic and Seismic sensor analytics.	F.4.13.1:UAV: Report UAV Analytics F.4.13.2:LAN: Transfer UAV Analytics F.4.13.3:IR: Report IR Analytics F.4.13.4:OBS: Report Acoustic & Seismic Analytics F.4.13.5:RR: Transfer Acoustic & Seismic & IR Analytics F.4.13.6:CS: Perform Situational Fusion	F.1.1:F: FB: L1-Sensor Signature
F.4.13.1:UAV: Report UAV Analytics	Periodically report UAV sensor analytics.		F.1.1.6:UAV: Sensor Feedback
F.4.13.2:LAN: Transfer UAV Analytics	In vehicle transfer of sensor data.		F.1.1.3:LAN: Sensor Transfer Feedback
F.4.13.3:IR: Report IR Analytics	Periodically report IR sensor analytics.		F.1.1.2:IR: Sensor Feedback
F.4.13.4:OBS: Report Acoustic & Seismic Analytics	Periodically report Obstacle sensor analytics.		F.1.1.4:OBS: Sensor Feedback
F.4.13.5:RR: Transfer Acoustic & Seismic & IR Analytics	Wirelessly transfer sensor data.		F.1.1.5:RR: Sensor Transfer Feedback
F.4.13.6:CS: Perform Situa-	Fuse sensor data into an integrated situa-		F.1.1.1:CS: Sensor Feedback

System Function Examples:

- Graphical Control Structure vs. Tabular View
- Decomposition of Functions
- Triggered by Control Actions / Feedback



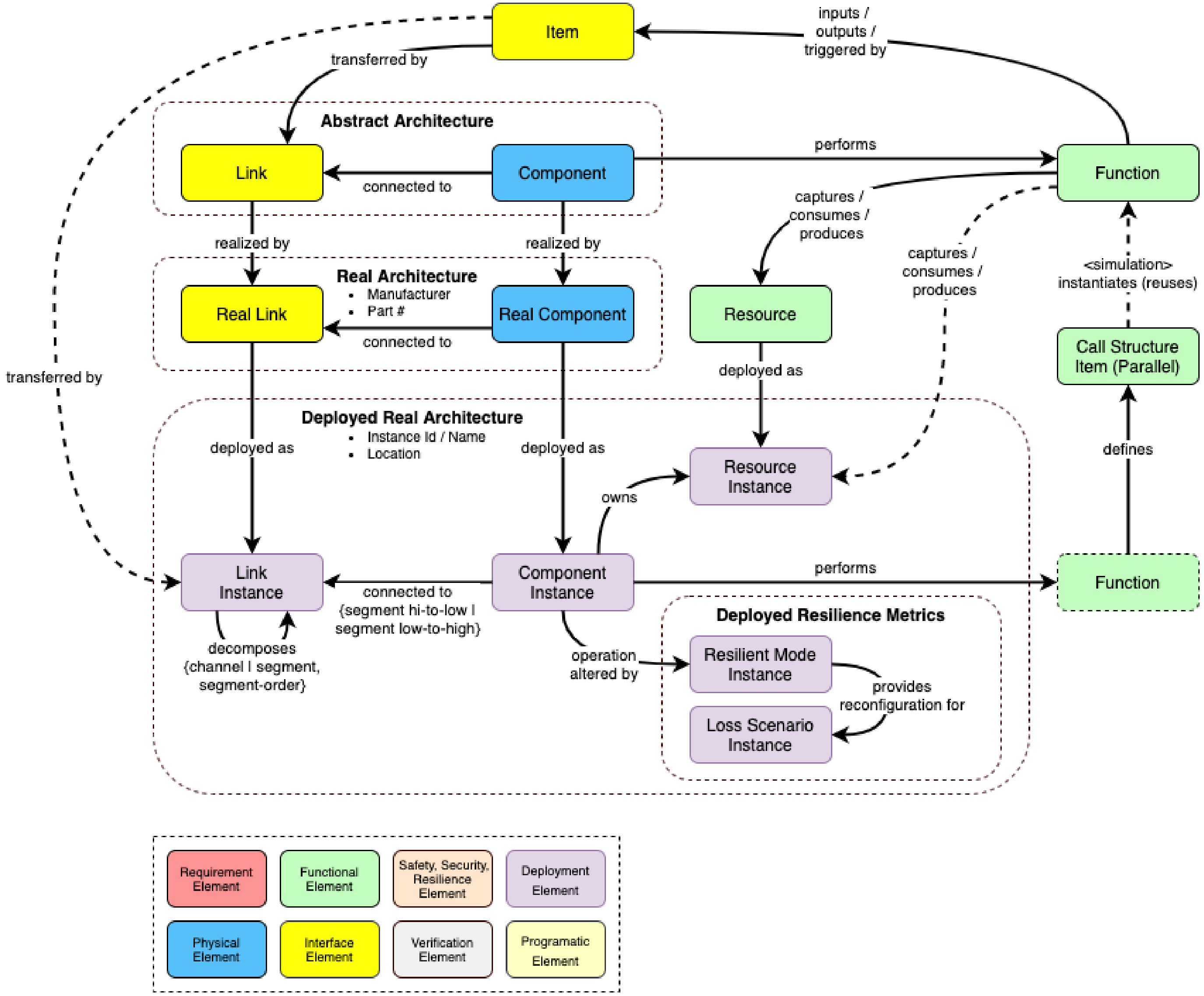
Simulation – Fault Injection

Mission Aware Monitor Design Pattern	MBSE Fault Injection Simulation Technique
Resource Introspection (cpu, battery, queue depth, etc.)	Attacker - consumes / produces *Resource*
Information Exchange Delay	Attacker - modifies *Link* capacity / delay
Parameter Modification	Attacker - modifies data store *Item*
Changing Control Action (modify / drop / inject)	Attacker - modifies input/output *Item*
Changing Feedback (modify / drop / inject)	Attacker - modifies input/output *Item*
Behavior Timing (speedup, slowdown)	Attacker - modifies *Function* execution / timeout duration
Illogical Behavior	Attacker - modifies *Function* exit path probability

Resilience Evaluation Scenarios

- Issues:
  - Limited simulation capability within existing MBSE tools
  - Interoperability with dynamic simulation tools

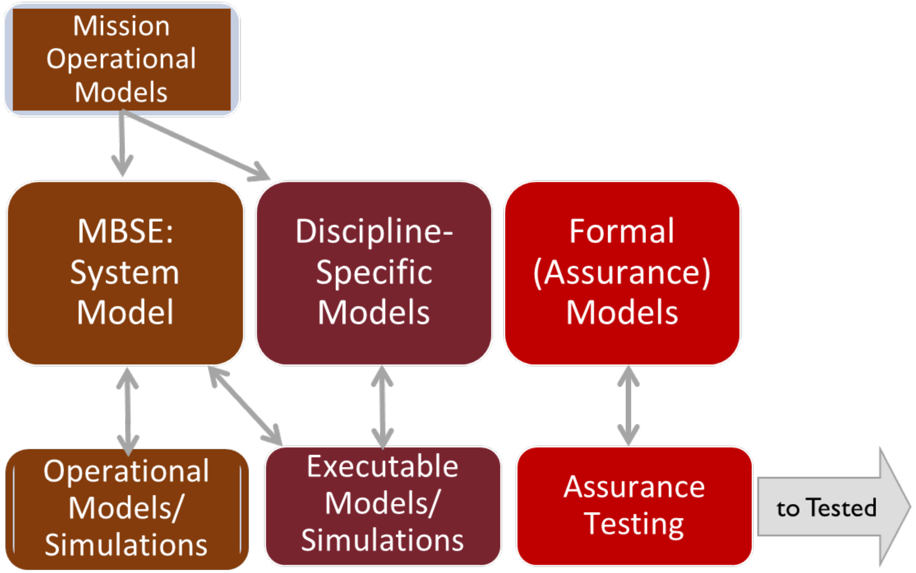
Meta Model Extension – Functional Simulation



Element	Entity	Description
Physical	Component	A component is an abstract term that represents the physical or logical entity that performs a specific function or functions.
	Real Component	A component that realizes an abstract physical entity with a known manufacturer & part number that performs a specific function or functions. Performance characteristics may vary between different realizations (manufactures) of real components.
Interface	Link	A link is the abstract physical implementation of an interface that connects Components
	Real Link	A physical link that realizes an abstract link and connects Real Components.
	Item	An item represent flows within and between functions. An item is an input to or an output from a function.
Functional	Function	A function is a transformation that accepts one or more inputs (items) and transforms them into outputs (items).
	Call Structure Item	Recursive call structure, for example, select, parallel, loop, for each function.
	Exit	An exit identifies a possible path to follow when a processing unit completes.
	Resource	A resource is an element, for example, power, MIPS, interceptors, that the system uses, captures, or generates while it is operating.
Deployment	Component Instance	An instance of a real component with a name & serial number, deployed at a specific location.
	Link Instance	An instance of a real link which connects deployed components.
	Resource Instance	An instance of a resource that is owned by a deployed component.

Formal Models and Assurance Testing

- The research shall:
  - Connect MA MBSE Meta-Model to Army/DARPA research on formal modeling and validation of computer information flows and software code execution.
  - *Connection remains primarily a manual process*
  - *Conversion of functional system view to structural software simulation difficult to support in existing tools*
  - *Core features of MA Metamodel – controller architecture and behavioral (activity) diagrams – do not translate easily between SysML tools and AADL*
  - *Gap remains in behavioral-structural specification and assurance testing*
  - *Sentinel functions (at least) and resilient modes should use assured design approaches*



Cyber Assured Systems Engineering (CASE)

CUI

(U) CASE Tool Capabilities

(CUI) Adversarial analysis of system architecture to **derive requirements** for cyber-resiliency

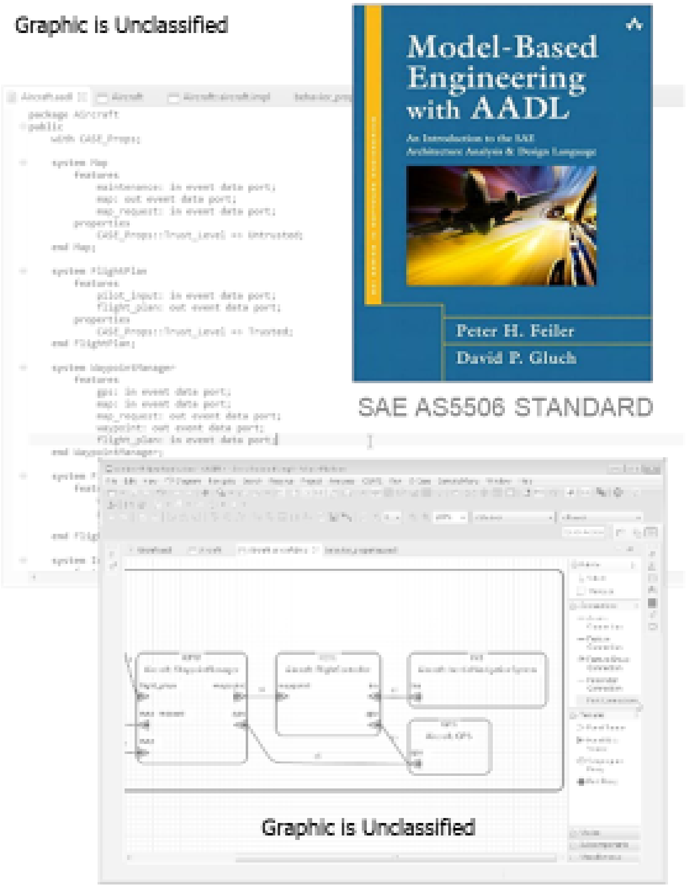
(U) Integrated **model-based systems engineering** tool suite based on Architecture Analysis & Design Language (AADL) models

(U) Transform system design to satisfy **cyber-resiliency** requirements

(U) Generate new **high-assurance components** from formal specifications

(U) Verify system design using **formal methods** and document evidence/compliance with assurance case

(U) Generate **software integration code** directly from verified architecture models, targeting multiple operating systems (including seL4)



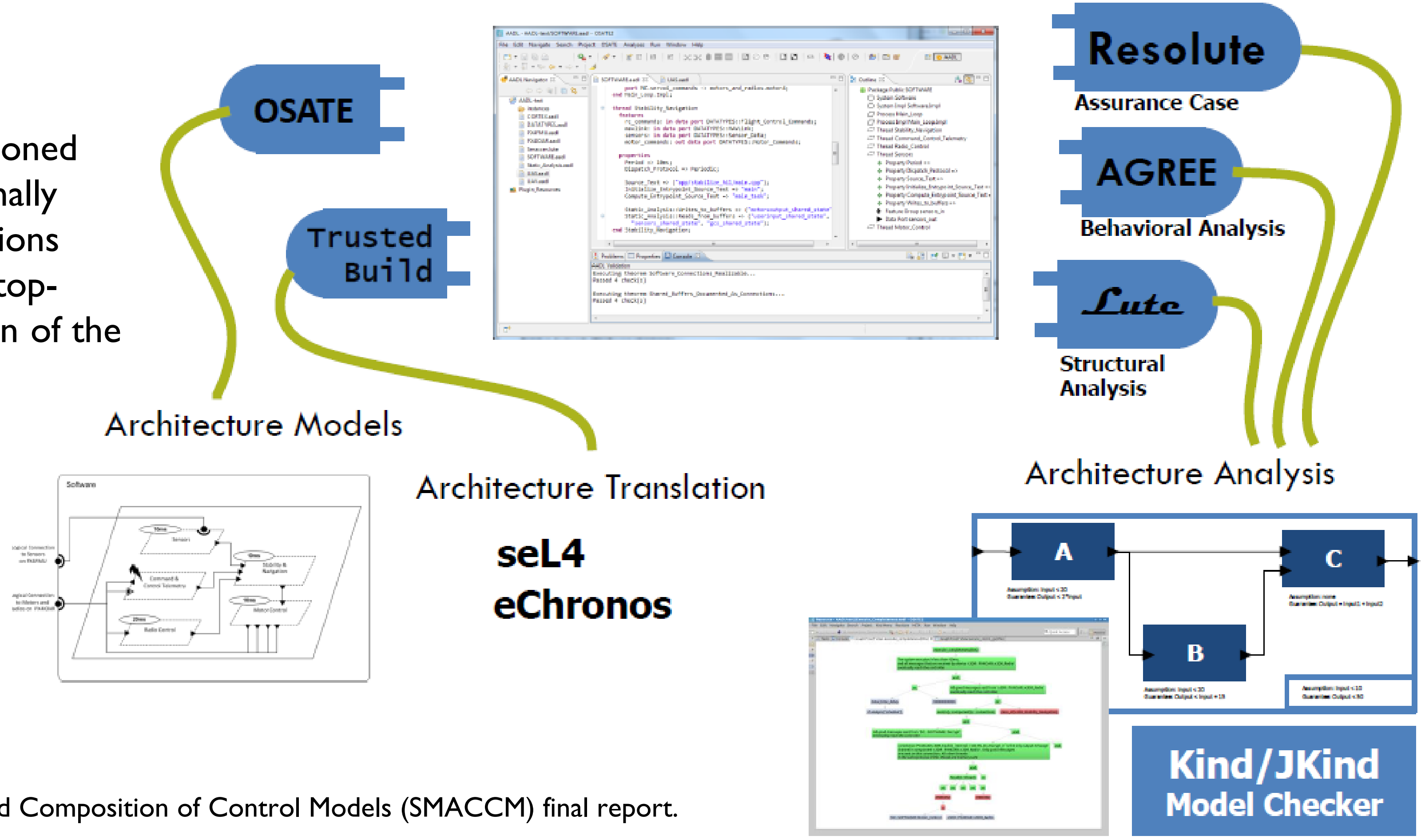
Distribution A. Approved for public release: distribution unlimited.

4

DARPA HACMS/CASE Program Toolset

The approach is based on the use of formal assume-guarantee contracts

verification is partitioned into a series of formally proven sub-verifications integrated into the top-down decomposition of the system in AADL



Resolute generates assurance cases from AADL models

AGREE proves behavioral properties using modern Satisfiability Modulo Theories (SMT)-based model checkers.

Secure Mathematically-assured Composition of Control Models (SMACCM) final report.

Questions?