SoS Architectures - Identifying Architecture, Engineering and Capability Challenges Early in the Lifecycle

Mike Gagliardi
Bill Wood
Tim Morrow

Software Solutions Conference 2015
November 16–18, 2015

Software Engineering Institute | Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0002994

Agenda

Background

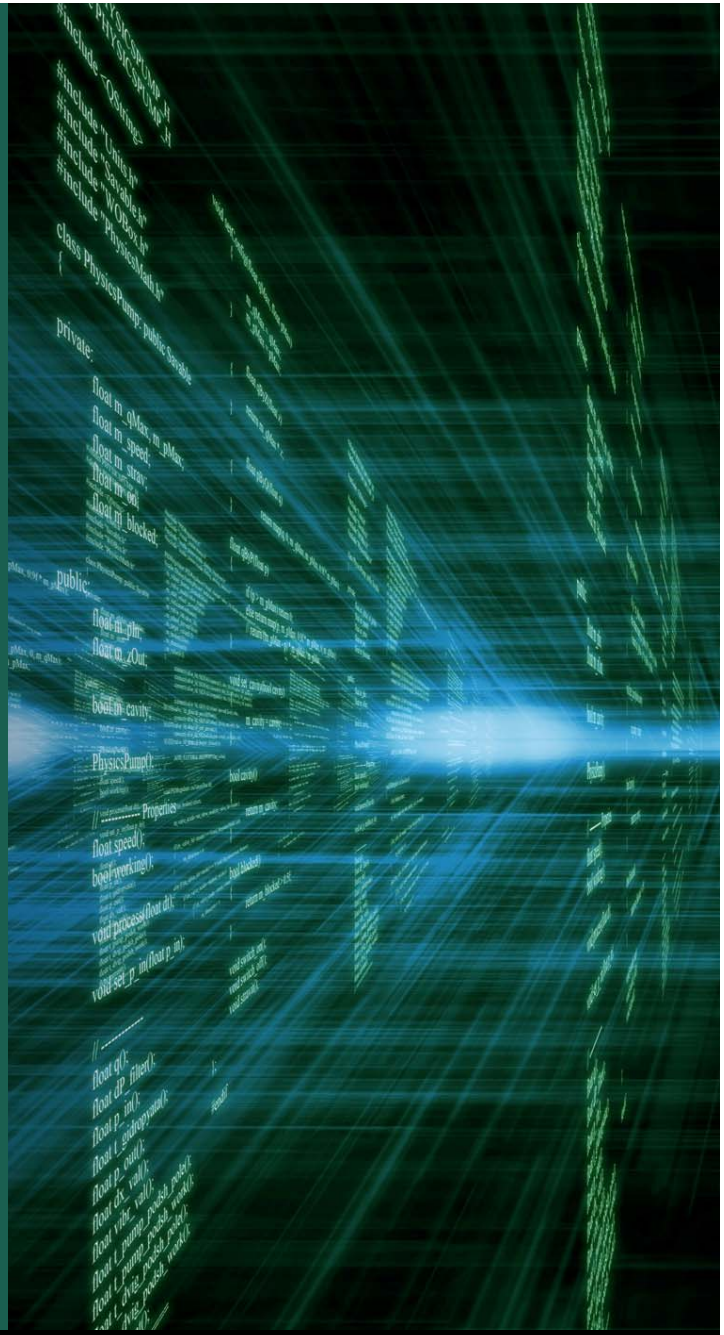
Mission Thread Workshop

Legacy System Architecture Evaluation in SoS Context

Lessons Learned

Application in Acquisition Context

Background



Problem

Integration and operational problems arise due to inconsistencies, ambiguities, and omissions in addressing quality attributes between system and software architectures. This is further exacerbated in an SoS architecture.

Example quality attributes: **performance/responsiveness, security, availability, reliability, usability, testability, safety, interoperability, maintainability, sustainability, force modularity, spectrum management.**

Functionality and capability are critically important, but the architecture must be driven by the quality attributes. Specifying and addressing quality attributes early and evaluating the architecture to identify risks is key to success.

The Need for Augmented End-to-End Mission Threads in DoD SoS Architecture Definition

DoDAF provides a good set of architectural views for an SoS architecture. However, it inadequately addresses cross-cutting quality attribute considerations.

System use cases focus on a functional slice of the system.

More than DoDAF and system use cases are needed to ensure that the SoS architecture satisfies its cross-cutting quality attribute needs.

SoS end-to-end mission threads augmented with quality attribute considerations are needed to help define the SoS Architecture and then later evaluate the SoS architecture and constituent system/software architectures.

Definitions (DoD Context)

Vignette: A description of the geography, own force structure and mission, strategies and tactics, the enemy forces and their attack strategies and tactics, including timing. There may be associated Measures of Performance (MOP) and Measures of Effectiveness (MOE). A vignette provides context for one or more *mission threads*.

Mission Thread: A sequence of end-to-end activities and events beginning with an opportunity to detect a threat or element that ought to be attacked and ending with a commander's assessment of damage after an attack. C4ISR for Future Naval Strike (Operational)

Sustainment: A sequence of activities and events which focus on installation, deployment, logistics and maintenance.

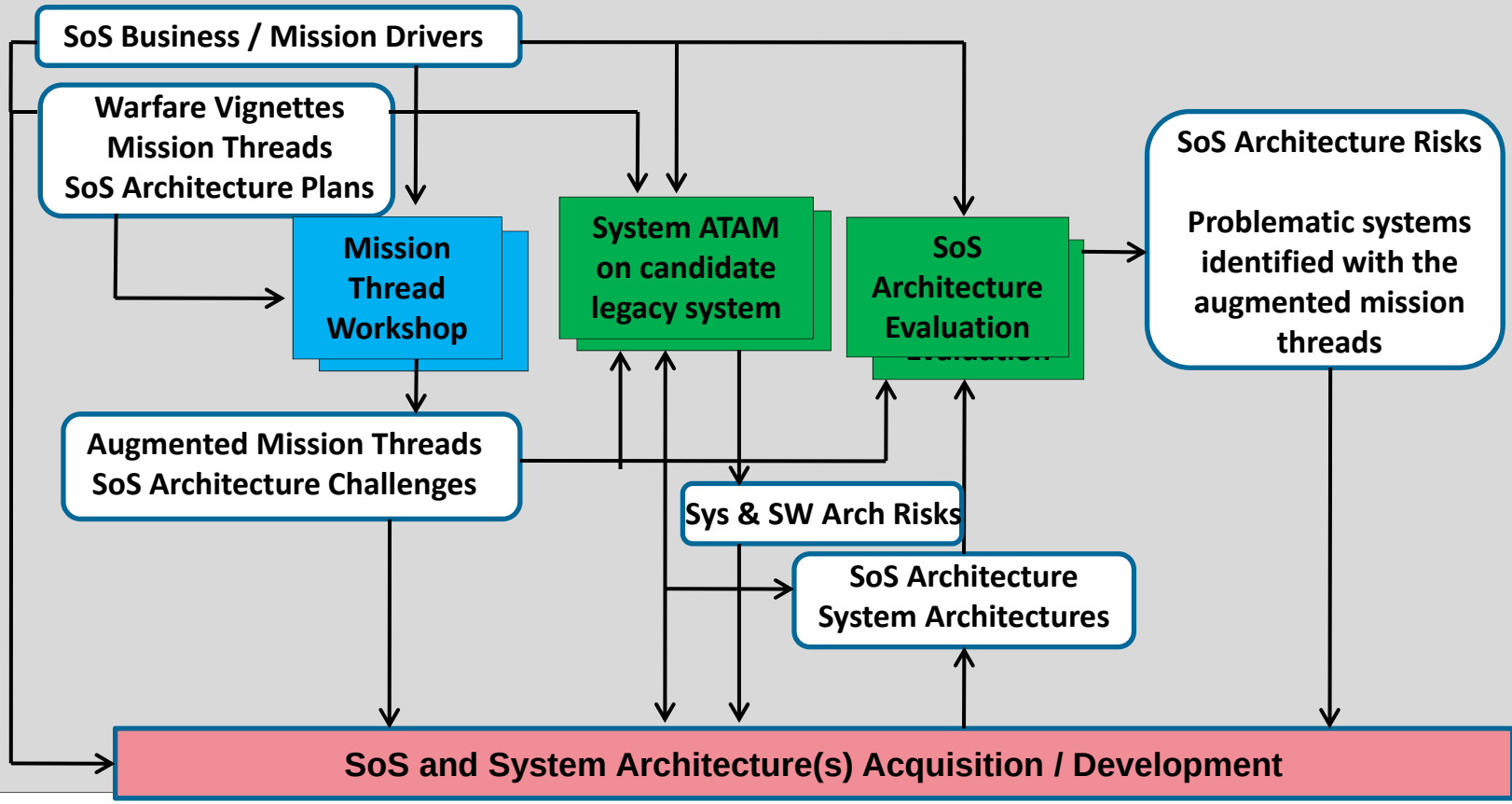
Development: A sequence of activities and events that focus on re-using or re-engineering legacy systems and new adding capabilities

Acquisition: A sequence of activities and events that focus on the acquisition of elements of an SoS, and the associated contracts and governance

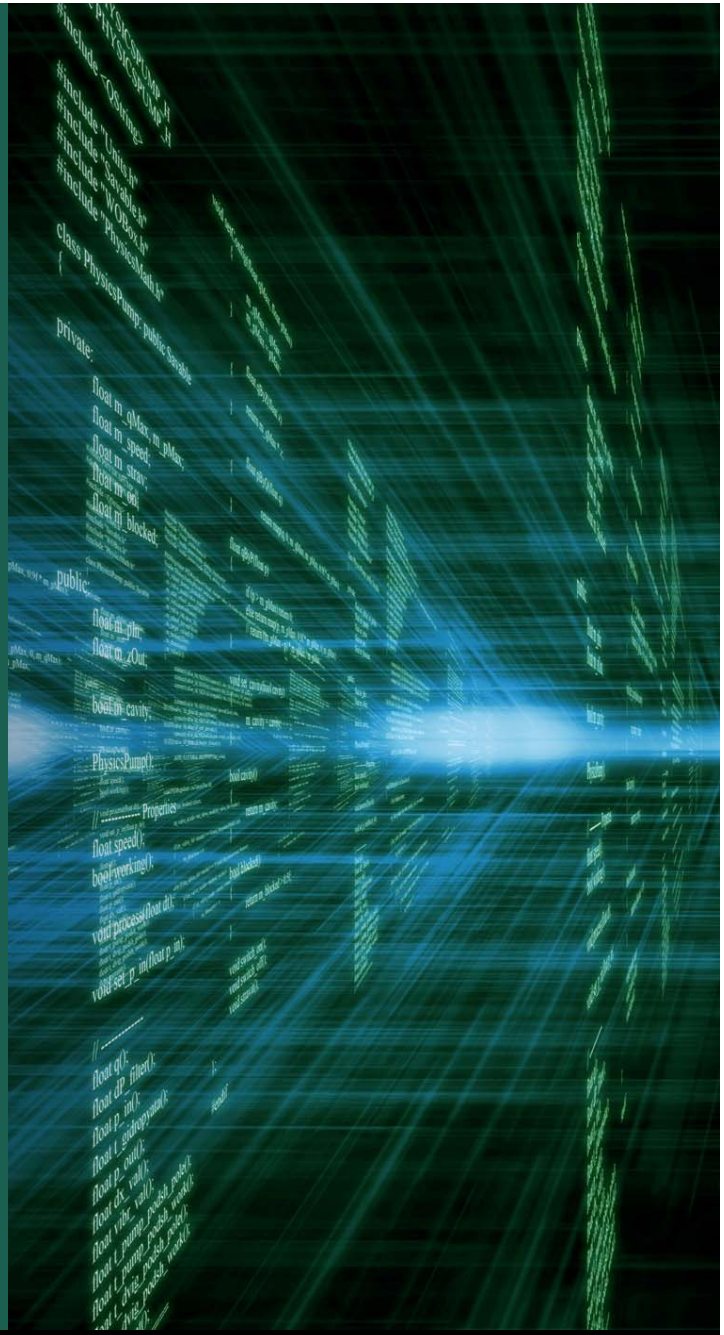
These have been applied to Enterprise Architectures as well

SoS Architecture Quality Attribute Specification and Evaluation Approach

- Early elicitation of quality attribute considerations
- Early candidate legacy system architecture evaluation
- Early identification and mitigation of architectural risks



Mission Thread Workshop



Purpose

The Mission Thread Workshop (MTW) is a facilitated, stakeholder-centric workshop whose purpose is to elicit and refine end-to-end quality attribute, capability, and engineering considerations for SoS mission threads.

The MTW identifies significant SoS challenges, which are architecturally significant questions that are distilled from the architecture, engineering, and capability issues identified in a qualitative analysis of the augmented mission threads. The SoS challenges have the potential to turn into risks if they are not addressed during SoS architecture development.

The augmented mission threads and SoS challenges serve as inputs to developing the SoS architecture, evaluating the SoS architecture and the constituent system and software architectures, and V&V of the SoS against test/use cases derived from the augmented mission threads.

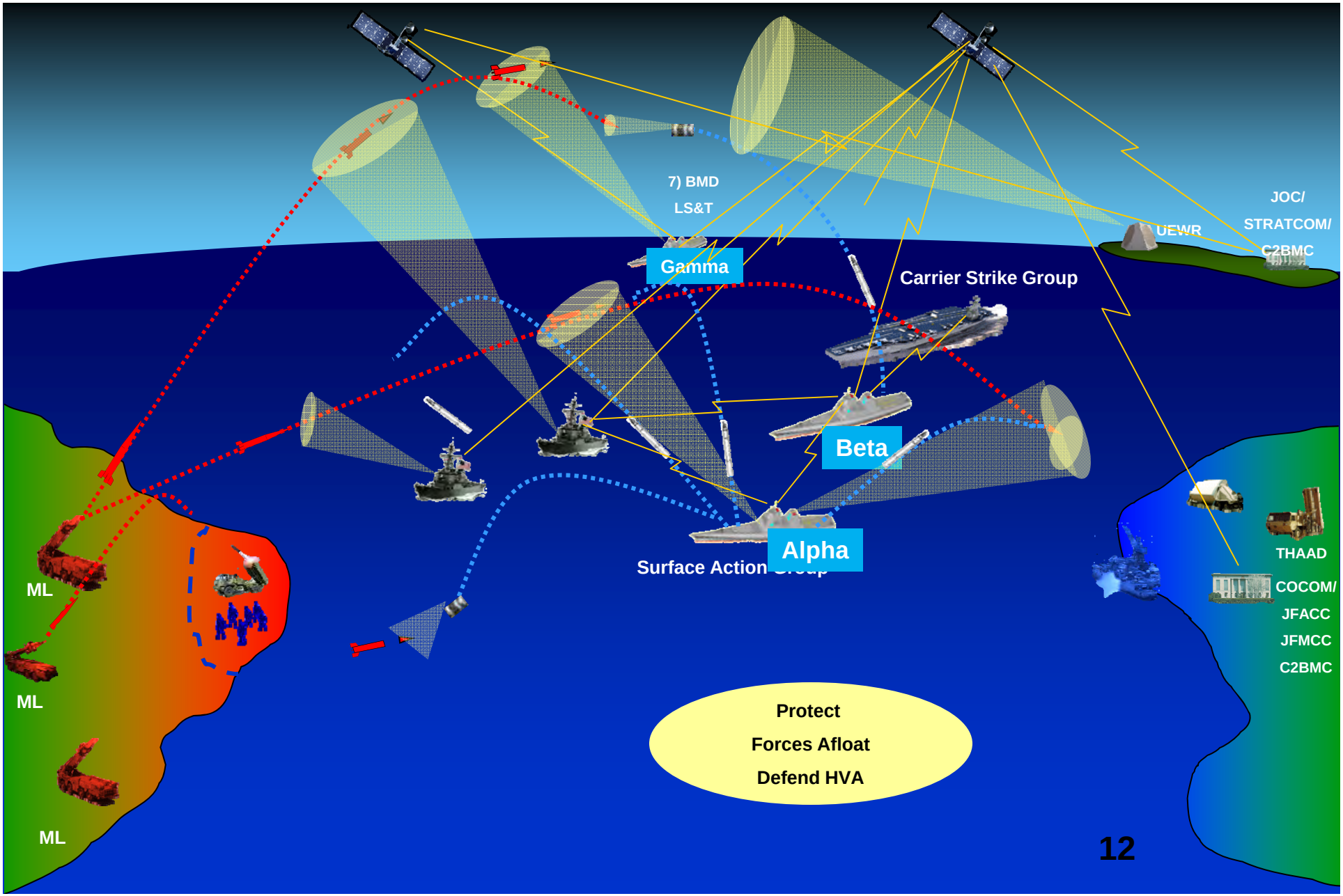
Vignettes Are the Starting Point – Example Wording

Two ships (Alpha and Beta) are assigned to integrated air and missile defense (IAMD) to protect a fleet containing two high-value assets (HVA). A surveillance aircraft SA and 4 UAVs are assigned to the fleet and controlled by the ships. Two UAVs flying as a constellation can provide fire-control quality tracks directly to the two ships. A three-pronged attack on the fleet occurs:

- 20 land-based ballistic missiles from the east
- 5 minutes later from 5 aircraft-launched missiles from the south
- 3 minutes later from 7 submarine-launched missiles from the west.

The fleet is protected with no battle damage.

Air and Missile Defense (AMD) OV-1 Example



Mission Threads Flow from Vignettes – Example (Non-Augmented)

1. 20 land-based missiles launched - X minute window
2. Satellite detects missiles - cues CMDR
3. CMDR executes re-planning – reassigns Alpha and Beta
4. Satellite sends track/target data - before they cross horizon
5. Ships' radars are focused on horizon crossing points

…

N Engagement cycle is started on each ship

N+1. Aircraft are detected heading for fleet

N+2. SA detects missile launches – tells CMDR

N+3. CMDR does re-planning - UAVs are re-directed

N+4. FCQ tracks are developed from UAV inputs

Mission Thread Workshop - Objective

To augment a set of end-to-end System of Systems (SoS) mission threads with quality attribute and engineering considerations with the stakeholders.

To capture at each step of the mission thread AND each SoS quality attribute

- the engineering considerations from diverse stakeholders
- the quality attribute concerns associated with the mission thread
- the applicable use cases for the different nodes and/or systems

To develop technical challenges associated with the threads, and to aggregate the challenges over a number of MTWs

Outputs will inform and drive SoS Architecture Decisions.

MTW Stakeholders

Example Stakeholders:

- Architects – SoS, (System, Software – especially for identified legacy systems)
- Requirements
- Engineering
- Test and Evaluation
- Sustainment
- Modeling and Simulation
- Integration
- CONOPs and operational analysts
- Operational Commanders, Operators, Users
- Logistics and Sustainment
- Training

Augmentation Process – Per Mission Thread

Two Passes over the Mission Thread:

1) For each event in the mission thread:
   - Elicit quality attribute considerations. Capturing any engineering issues, assumptions, challenges, additional use cases and mission threads (with QA context etc.)
   - Capture any capability and/or mission issues that arise.

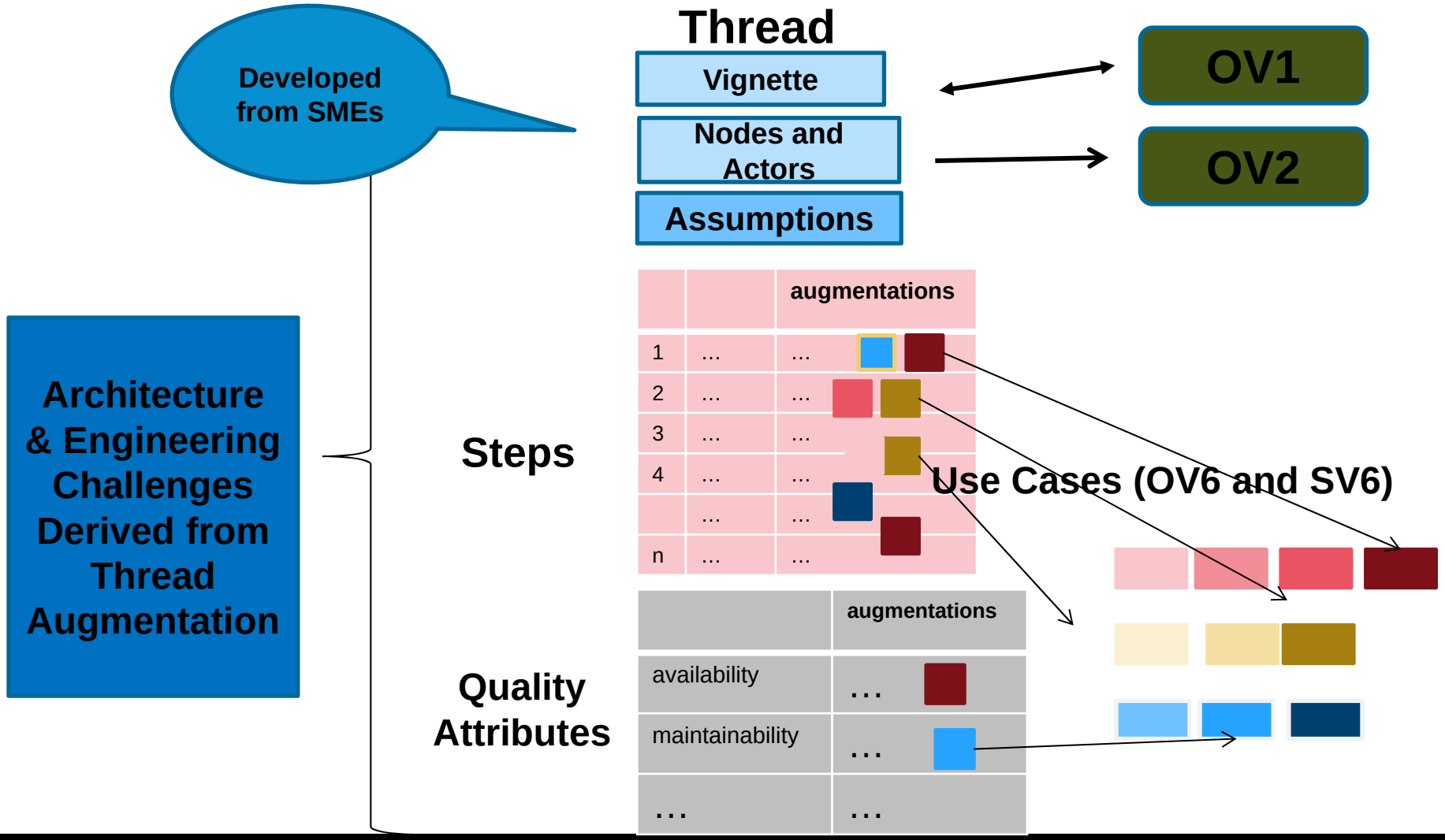
2) For each Quality Attribute - elicit any over-arching quality attribute considerations
   - Capturing any over-arching assumptions, engineering issues, challenges, additional use case and mission threads (with QA context) etc.
   - Capture any capability and/or mission issues that arise.

Capture any MT extensions for later augmentation

Capture Parking Lot issues – for organization, programmatic, non-technical issues that arise (will not be further pursued in the MTW).

Stakeholder Inputs are Key.

Mission Thread
(augmented via the Mission Thread Workshop)



Nodes, Actors and Assumptions Augmentation

Name	Protect Fleet Assets against Cruise Missile Attacks
Vignette (Summary Description)	Two ships (Alpha and Beta) are assigned to air defense (AD) to protect a fleet containing two high-value assets (HVA). A surveillance aircraft (SA) and four UAVs (two pairs) are assigned to the fleet and controlled by the ships (Alpha and Beta). A pair of UAVs flying as a constellation can provide fire-control quality (FCQ) tracks directly to the two ships. A two-pronged attack on the fleet occurs: • five aircraft-launched missiles from the Southeast • three minutes later seven submarine-launched missiles from the Southwest. The fleet is protected with no battle damage.
Nodes Actors	• two ships (Alpha and Beta) • four UAVs • two HVAs • one SA • five enemy aircraft and their missiles • seven enemy submarines and their missiles

Assumptions	• Enemy aircraft are flying along a route normally used for training, and suddenly change direction and head for the fleet. They are being tracked.
	• The submarines are undetectable until they fire their missiles.
	  • *No sonabouys are deployed, but they could be in a new vignette.*
	• The vignette is not concerned with counter-attacking the enemy aircraft or submarines.
	• It is not a wartime situation; ships are at battle condition 3.
	• Sea state is 3.
	• Ships' readiness condition is YOKE.
	• Alpha controls two UAVs and Beta two other UAVs.
	  • *Each ship has two organic UAVs.*
	• During normal operations the UAVs have separate non-overlapping areas of regard (AORs).
	• The SA has an area of regard that will detect both the launched missiles.
	• The Air Defense Commander (ADC) is on-board Alpha.
	• *Alpha ship's Helo is in the air.*
	• *Both ships are aware that a potentially hostile country has some fighter aircraft conducting training missions nearby.*

Step by Step Augmentation

Mission Steps	Description	Engineering Considerations, Issues, Challenges
1	Alpha develops the air defense plan (ADP) and rules of engagement (ROE) and sends them to Beta. The plan assigns to Alpha the area of regard (AOR) to the west, and Beta the AOR to the east. Alpha configures surveillance and weapons systems to support eastern engagements.	1. *How much is pre-defined and how much is done manually?* 2. *ROE dictates a "shoot-look-shoot" defense.* 3. *How is this communicated to Beta? Using the fleets NRTC: near real-time communications*
2	The SA aircraft detects that the five enemy aircraft have changed course and are heading towards the fleet at low altitude.	1. *The enemy aircraft are within the area of regard (AOR) of the SA sensors. The SA has been tracking these aircraft and sending tracks to Alpha and Beta.* 2. *Need a "fleet" SA use case*
3	SA informs both Alpha and Beta of the change.	1. *Within X seconds of detecting the change* 2. *Using the Global Information Grid (GIG). Is the GIG usable for tactical near real-time data? Probably not!* 3. *Need a use case on assigning the UAVs to track the aircraft at this point*
4	Alpha (and Beta) go to General Quarters	1. *ADC informs the captain who orders general quarters* 2. *Using Internal Communications*
5	SA detects that missiles have separated from the enemy aircraft and informs Alpha and Beta.	*Within X seconds*
6	Alpha assigns its two UAVs to track the missiles.	1. *The legacy Defensive Engagement System (DES) cannot use external tracks to form a FCQ track.* 2. *Within X seconds* 3. *Does the ADC have to do this manually?* 4. *Would they start tracking automatically if the missiles were within their AOR?* 5. *Would they have been tracking the aircraft?*
7	The two Alpha controlled UAVs send FCQ tracks for the five missiles to both Alpha and Beta.	1. *The two UAVs can re-direct their payload to do this within YY seconds. (use case)* 2. *It takes XX seconds for the FCQ tracks to stabilize.* 3. *What is the comms between UAVs and*

Over-Arching Quality Attribute Augmentation

Name of QA (filled in during Preparation phase)	**Considerations** (This column will be filled in during the Augmentation Phase)
Performance (P)	1. *The airspace de-confliction latency is heavily dependent on the number of aircraft within the strike paths.* 2. *The timeline function from missile detection at specific distance from target until point of impact, including detection by both UAVs, engagement assignments, missile launching sequence, and fly out times has not been analyzed in detail!*
Availability/ Reliability (AV)	1. *What if both UAVs cannot maneuver to their respective AORs in time?* a. *They will probably have to wait until they are within the ship's radar to fire.* b. *Is this a manual decision? (tradeoff with automation)* 2. *What if the ship/missile communications fails?* a. *It will probably have to fire another intercept missile!* b. *Can the other ship try to control the missile?* 3. *What if Alpha/Beta Comms fails?* a. *Revert to a pre-defined separate engagement.* 4. *What if Beta does not acknowledge engagement assignments? Revert to what was defined in ROE or assume that it will follow received orders or take some other option?* a. *A degraded Mode Use Case needs to be developed.* 5. *Degraded modes of operation have not been detailed yet.* 6. *Loss of comms. to SA.* a. *After initial detection and UAV coverage, it does not matter.* b. *Before initial detection, the UAVs will provide some coverage, but will probably have some unmonitored areas.* c. *What happens when missile goes beyond line-of-sight radar coverage?* 7. *What if one of the UAVs is deemed non-functional during operations?*
Accuracy (Ac)	1. *If the tracks are relayed (see Interoperability item 2) what if they are not sufficiently accurate? Will they be?* 2. *Given multiple relay hops, how will accuracy be impacted? (Performance / accuracy tradeoff implications). How can shared resources be managed to bound latencies in this environment?*
Interoperability (In)	1. *Can a UAV that is assigned and controlled by one ship be re-assigned and controlled by another ship dynamically? (Degraded mode future support?)* 2. *Can FCQ information be transferred in real time from Alpha to Beta in order to target one of the missiles?*

Outputs

Individual MTWs

- Augmented Mission Threads (.doc, using MTW template)
  - Over-arching quality attribute augmentations for the mission thread
  - Capability and mission augmentations to the mission thread
  - Quality attribute augmentations for each event in the mission thread
  - Identified mission/additional use cases (with context) and mission threads

- Challenges (briefing, vetted with sponsor)
  - Architectural, capability and mission challenges derived from the mission thread augmentations. Rolled up from the augmentation.
  - The MTW team will roll up challenges from the data and provide an out-brief of the challenges.
  - Any candidate legacy system architecture that may require architecture evaluation.

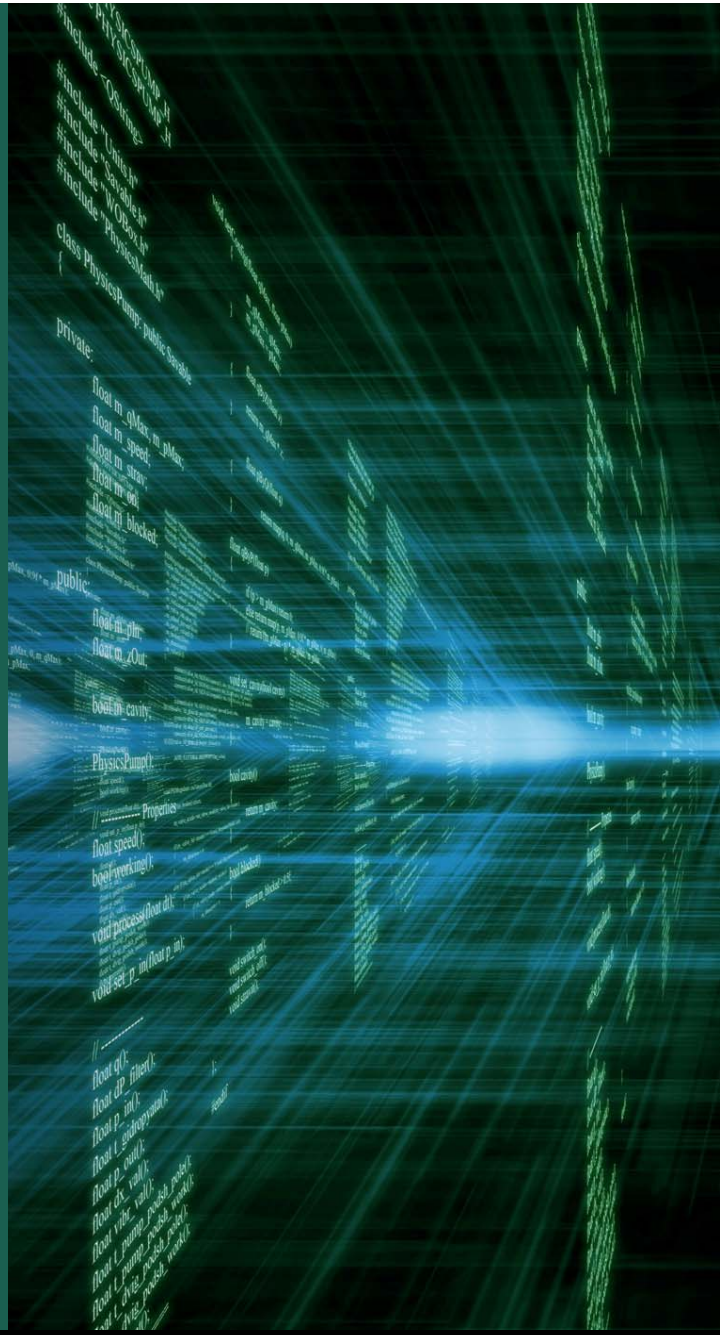
Upon completion of series of MTWs (briefing, vetted with sponsor):

- SoS challenges derived and rolled up from the mission thread augmentations; upon completion of the series of mission thread workshops for the SoS.

Mission Thread Workshops - Numbers to Date

Client	Description	MTWs	Vignettes	Mission Threads	Stakeholders
A	IRAD New platform/capability	1	1	2	8
B	New Naval Ship	13	17	37	>200
C	Battle Command	6	3	4	>100
D	Maritime Detection	2	4	4	30
E	NSF	1	3	3	15
F	Air Force Program	1	1	1	10
G	Other Govt Agency	3	10	10	>50
H	Cyber-Security	4	8	8	>50

Cyber-Security Considerations



Four Mission Threads Supporting Enterprise Architecture Development and Cyber-Security

Situational Awareness

Revolves around developing situational awareness information for different levels among the organizations which make use of XYZ. The development is based on the Situational Awareness Reference Model identified in the book "Cyber Situational Awareness: Issues and Research published by Springer which identifies four functions: Perception, Comprehension, Projection, and Resolution.

Indicator Expansion

Focuses on indicator expansion (process of taking an indicator and improving, enhancing and/or deriving additional indicators related to the initial indicator) used by XYZ analysts, and the automation of such tasks. The expansion includes primitives, discoveries, and external and internal shared inputs as resources.

Analysts Collaboration

Follows the workflow of a submission of an incident by a D/A analyst to the collaboration with XYZ Analysts to develop a response Tactics, Techniques, and Procedures (TTP) package addressing the D/A's situation. The response is successfully vetted through XYZ's indicator process and is supplied to D/A operations. Once the response is installed, the D/A analyst verifies the incident is being successfully addressed.

Continuity of Operations

Focuses on all hazard continuity of operations from the perspective of the XYZ Enterprise. A significant event occurs that invokes incident response protocols and subsequent system failover recovery mechanisms. Resources are redistributed, reconfigured alternate facilities are commissioned and full Mission Essential operational capability is resumed within 12 hours of the incident.

Cyber Security Mission Threads Focused on End-to-End Attacks

Four more specific attack focused deep dive end-to-end Mission Threads (They preferred to call them “Scenarios”).

- A cloud-based attack against an agency
- Exploiting a Client - “Watering Hole” attack against an agency
- Exploiting a Server - A SQL injection attack against an agency
- A social engineering attack on D/A’s local agency network

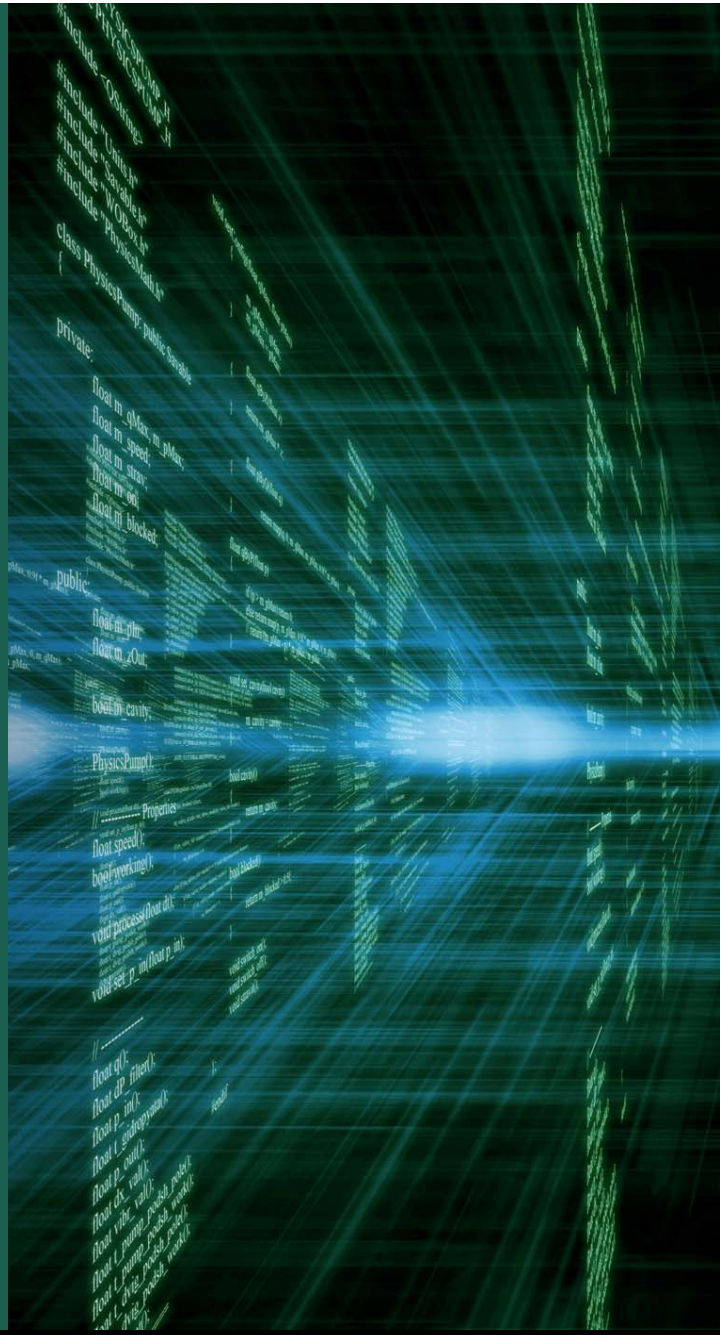
These threads were used to answer the questions:

- How did they get in?
- What did they do once in?

Many of the challenges and gaps pertained to “data visibility and fusion, SLA, MOAs”

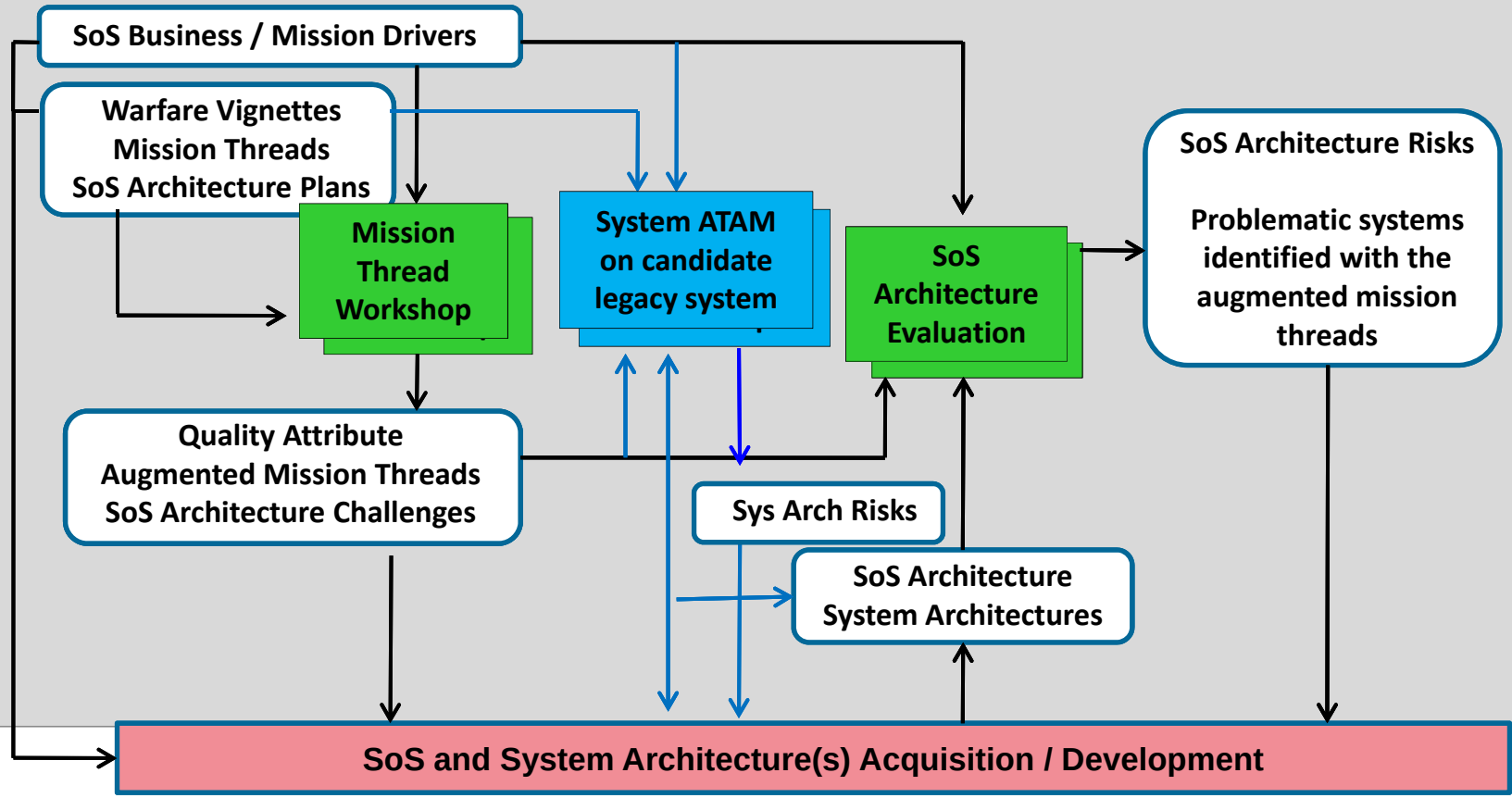
Many other MTWs have augmented existing mission threads with cyber-security considerations.

Legacy System Architecture Evaluation in SoS Context



Legacy System Architecture Evaluation - Early

- Early elicitation of quality attribute considerations
- Early identification and addressing of architecture challenges
- Early identification and mitigation of architectural risks (e.g. candidate legacy system/software architecture evaluation)



Purpose of the System ATAM

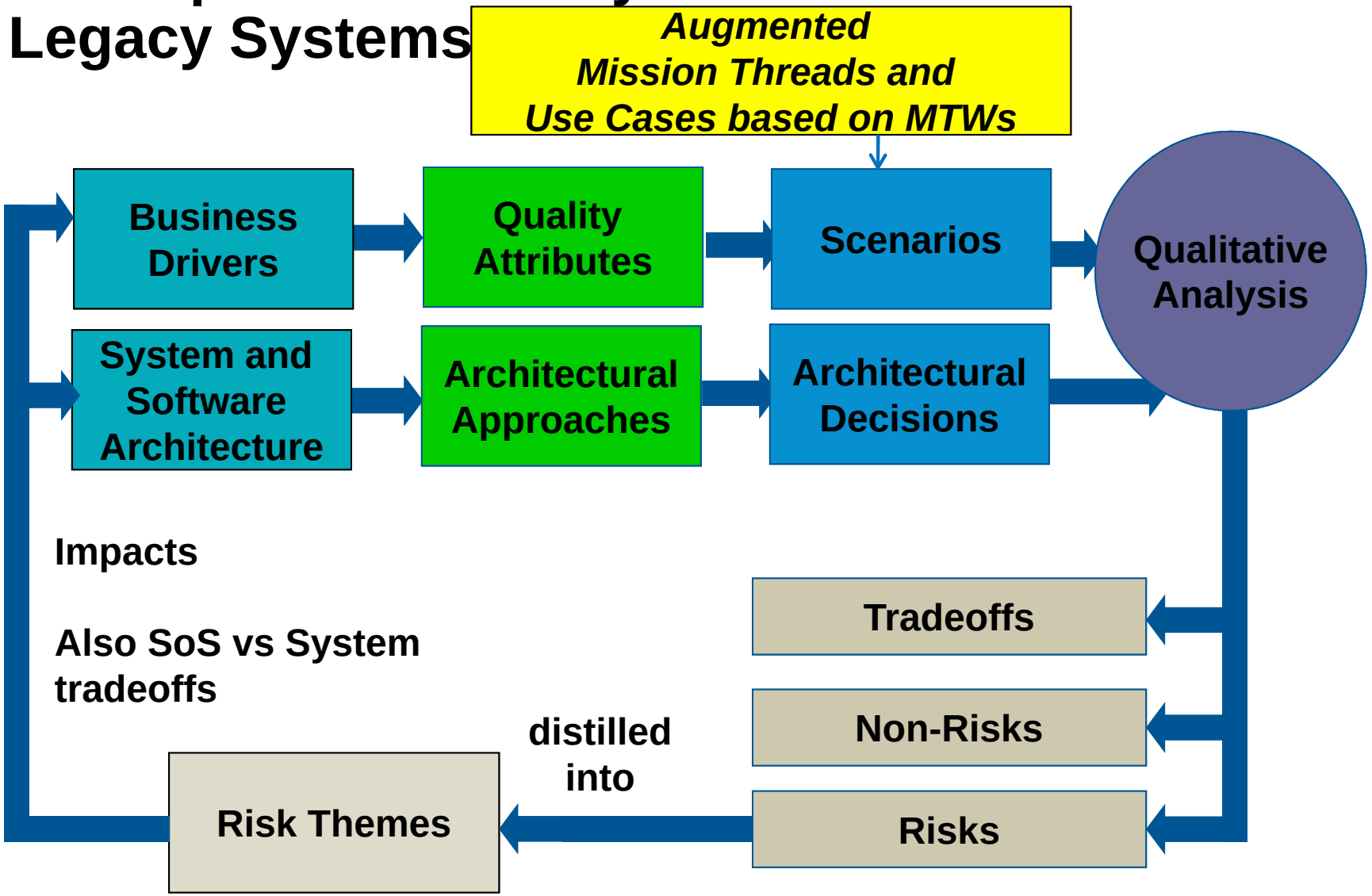
The System ATAM is a method that helps stakeholders ask the right questions to discover potentially problematic architectural decisions.

Purpose is to assess the consequences of **system and software architectural** decisions in light of quality attribute requirements and business goals; and to identify architectural risks.

The purpose is **NOT** to provide precise analyses; the purpose **IS** to discover risks created by architectural decisions.

Discovered risks can then be made the focus of mitigation activities. Tradeoffs can be explicitly identified and documented

Conceptual Flow of System ATAM Variant for Legacy Systems



Using the augmented mission threads to seed the system architecture evaluation

Issues from augmented mission thread identified in the MTW:

- The Defensive Engagement System may not be able to support the deconfliction timeline for 5 incoming missiles.
- The Defensive Engagement System may not have the capability to acknowledge Beta's acceptance of its assignment of 2 missiles.
- Is the Defensive Engagement System capable of sending track updates to the interceptor missiles that Beta had launched within the intercept timeline?

In preparation, the System ATAM lead meets with SoS and appropriate system architects to discuss what is in and out of scope concerning the system under analysis and if appropriate documentation exists.

Agreement is reached on the scenarios (based upon the augmented mission threads) with the understanding that additional scenarios can be added during the legacy system architecture evaluation.

Examples of Scenarios

Scenarios address both system and software aspects. Consist of Stimulus, Environment and Response.

Growth scenarios

- *The Defensive Engagement System (DES) is able to support de-confliction of 7 incoming missiles using own-ship and external information within 5 seconds.*
- *An upgraded DES is able to reduce the confliction time by 40% of 7 incoming missiles with no loss of existing functionality.*

Exploratory scenario

- *The DES is able to operate at up to 80% of its time budget for de-confliction of 7 incoming missiles with 8 coalition UAVs and 3 coalition helicopters operating in its vicinity.*

Stakeholders and Evaluators

Stakeholders will consist of:

- System Architects of relevant, associated systems to system under evaluation
- SoS Architects who know the total system and how the system under evaluation is envisioned to fit in
- Relevant stakeholders of the system under evaluation in the areas of requirements, development, T&E, sustainment, M&S

ATAM evaluators will look to identify/expose potential system and software architecture risks, with the help of the stakeholders. Subject matter experts may be used on the evaluation team, if necessary.

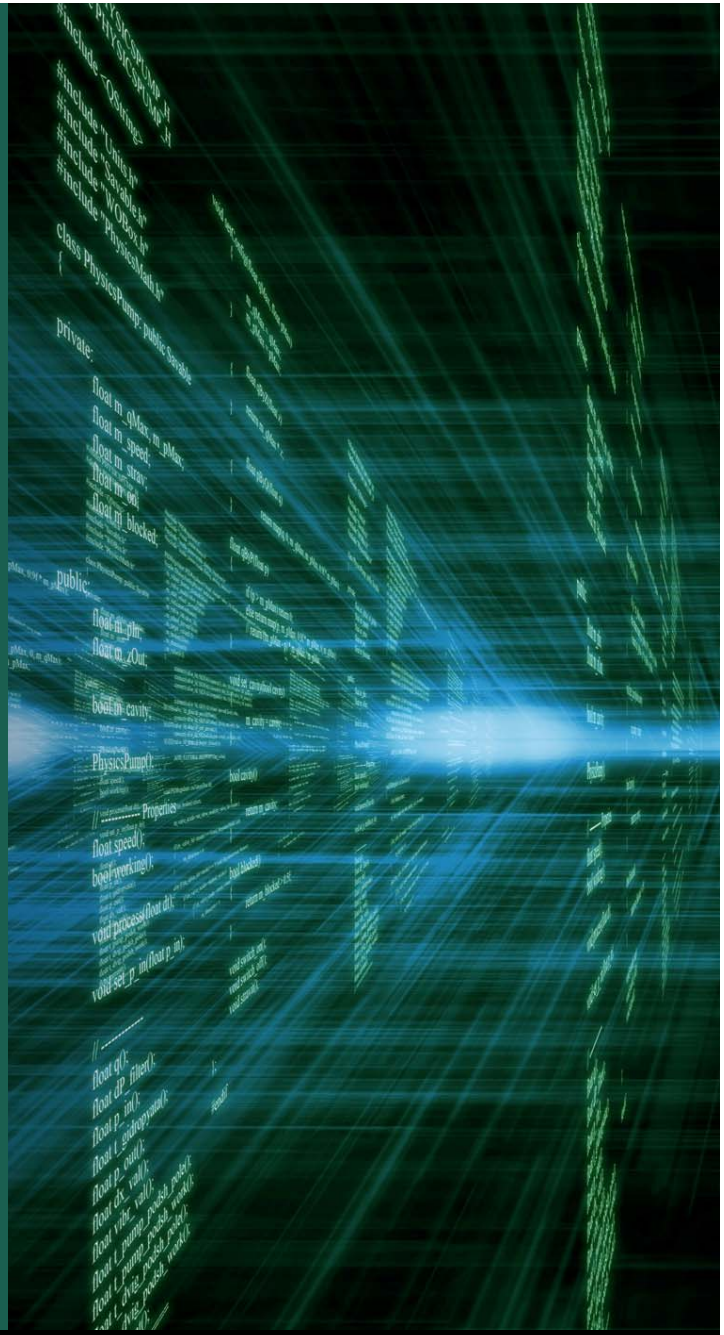
Walk-through of a scenario derived from augmented MT

The Defensive Engagement System (DES) is able to support de-confliction of 7 incoming missiles using own-ship and external information within 5 seconds.

- System architect identifies that currently DES can support 3 incoming missiles with 25% spare capacity within the latency bounds given the existing hardware.
- The software architect reveals that the system has a monolithic software architecture which is tightly coupled to the existing hardware.
- The architect identifies that upgraded hardware is available for the system which will provide the needed performance upgrade, but the software will need to be re-designed to take advantage of the upgrade.

SoS and DES architects and managers negotiate how to proceed based on architectural risks identified and associated risk mitigation options.

Lessons Learned



MTW – Initial Results - 1

The MTW and SoS Arch Evaluation methods adopted by a Navy and Army SoS programs and integrated into their architecture development process

Many of the identified challenges drove early risk mitigation activities (e.g. prototyping, EDM, white papers, modeling and simulation).

Many new use cases and additional mission threads identified. The QA considerations will be included in the use cases.

Excellent vehicle to promote communication between architects and stakeholders.

Capability and Mission Challenges were identified as well as Architectural Challenges.

MTW – Initial Results - 2

SoS Architecture and Guidelines document is needed. Developed a template for use on Army and Navy SoS Programs.

Supports programs' DoDAF architecture development efforts. Normalized the OV-1s and informed and drove many subsequent DoDAF views (e.g. OV-5, OV-2, OV-3, OV-4, OV-6c, SV-5a, SV-4a, SV-1, SV-3)

3rd Party facilitation by the MTW facilitators enabled the leads to think about and participate in the discussions rather than trying to lead/control the meetings

Method worked for non-software elements, as well as software-intensive elements

MTW Experiences – 1

Conducted a total of 35 MTWs (over 90 mission threads augmented), each MTW is a 1.5 day meeting

Plan 4 MTs per MTW, but expect to augment 3.

Expect 25-30 stakeholders to want to participate per MTW. Benefits from strong facilitation and independent 3rd party leadership.

Clients developed very good first pass vignettes and MTs after initial introduction.

Criteria for MT selection include: New capability, High perceived risk, proposal differentiators, etc.

DoDAF OV-1's were sufficient level of documentation going into the MTWs

MTW Experiences - 2

Mission thread step elaboration focused on:

- Command authority, network communications, step constraints
- Manned vs Automated, timelines, planning considerations
- Availability, Survivability, and Security considerations
- Readiness, environmental conditions, start up/shut down
- New capabilities/extensions, don't be limited by current capabilities
- CONOPS considerations
- Assumption clarifications and issues

Extensions

- Clients built some initially
- Added them as we go (to sideline discussions)

MTW Experiences - 3

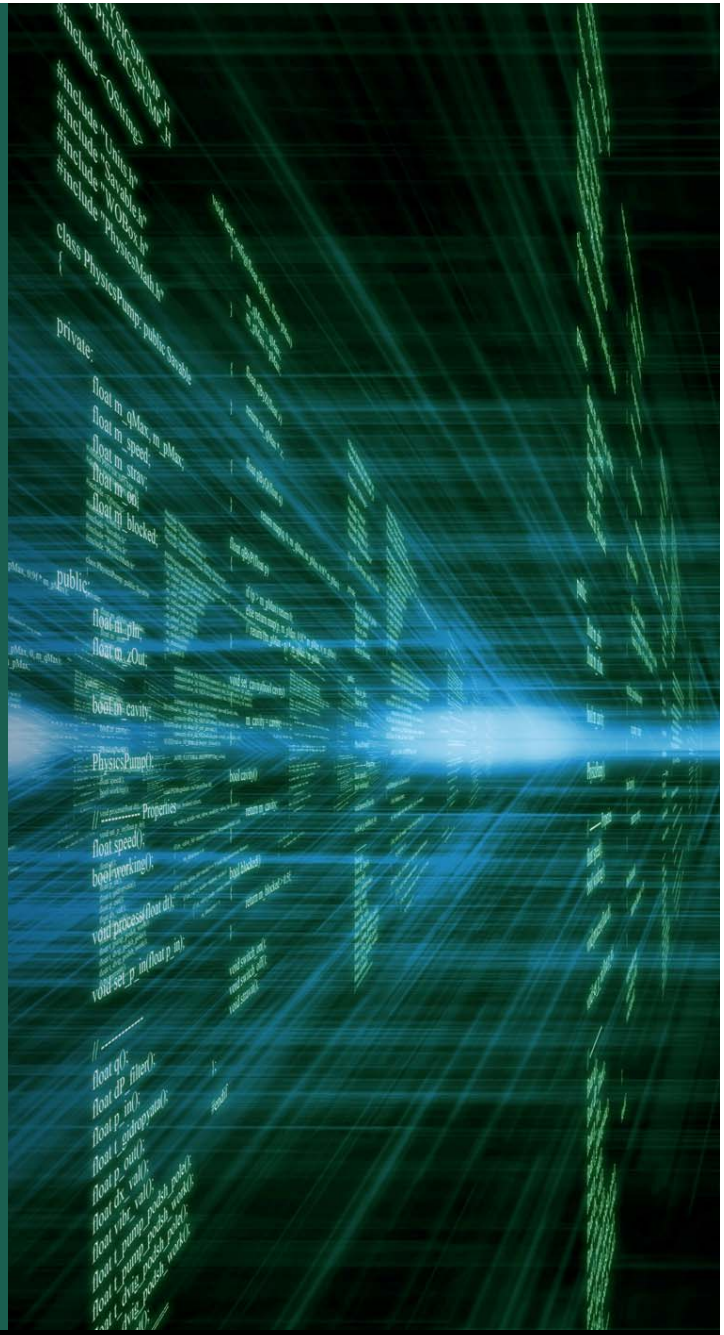
Quality Attributes Considerations:

- Timeline decomposition often built into thread (weeks to seconds)
- Availability/ Degraded Operation / Resource Management under-developed
- Focus on operational MTs, separate MTW for development and support
- Over-arching MT pass collects much of the QA considerations
- Identified additional use cases and MTs (e.g. survivability)

Challenges:

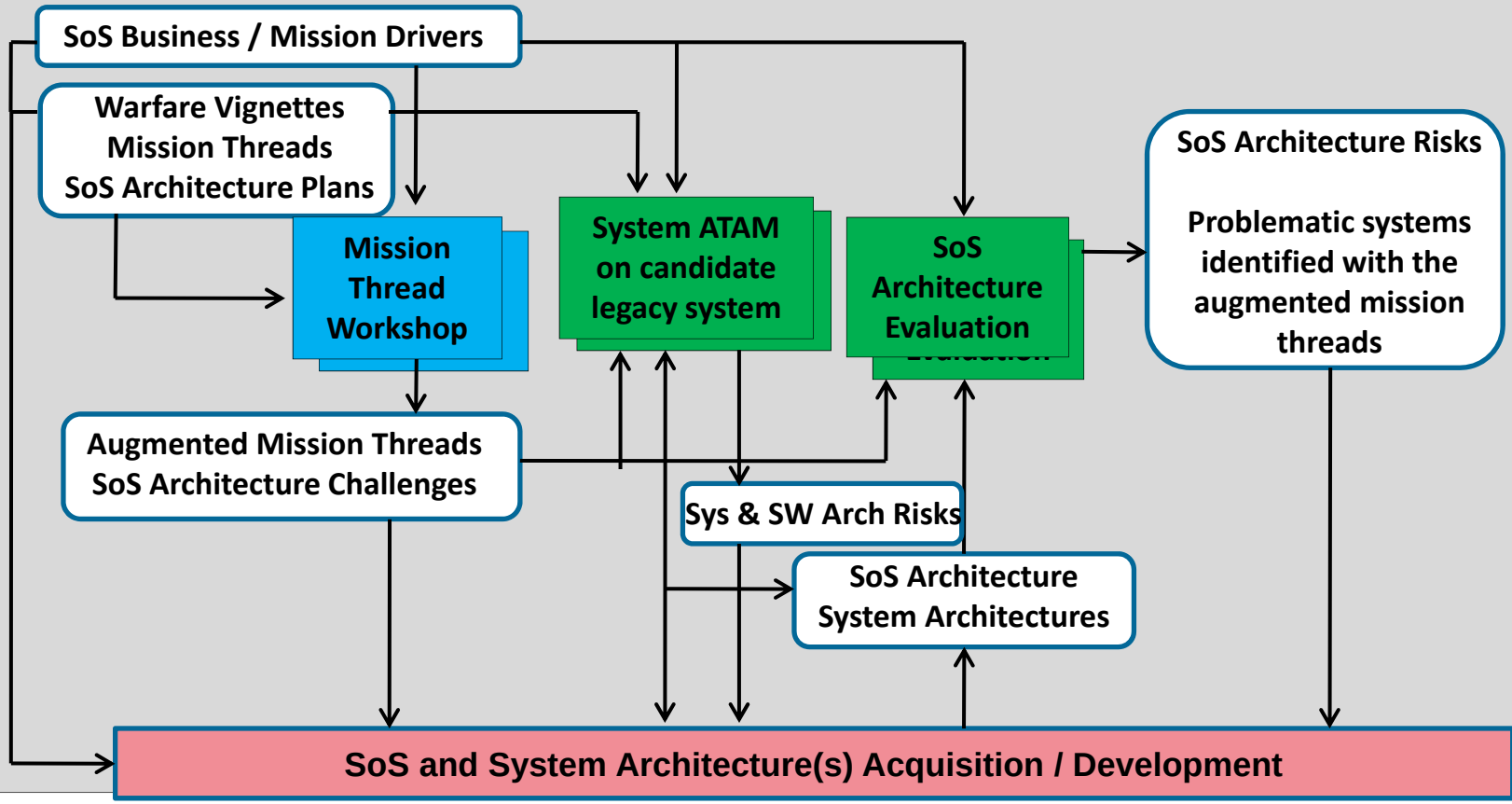
- Some challenges need to be kicked up to the SoS architecture level to address, while others need to be addressed by systems engineering
- Drives an SoS Architecture and Guidelines Document

Application in Acquisition Context

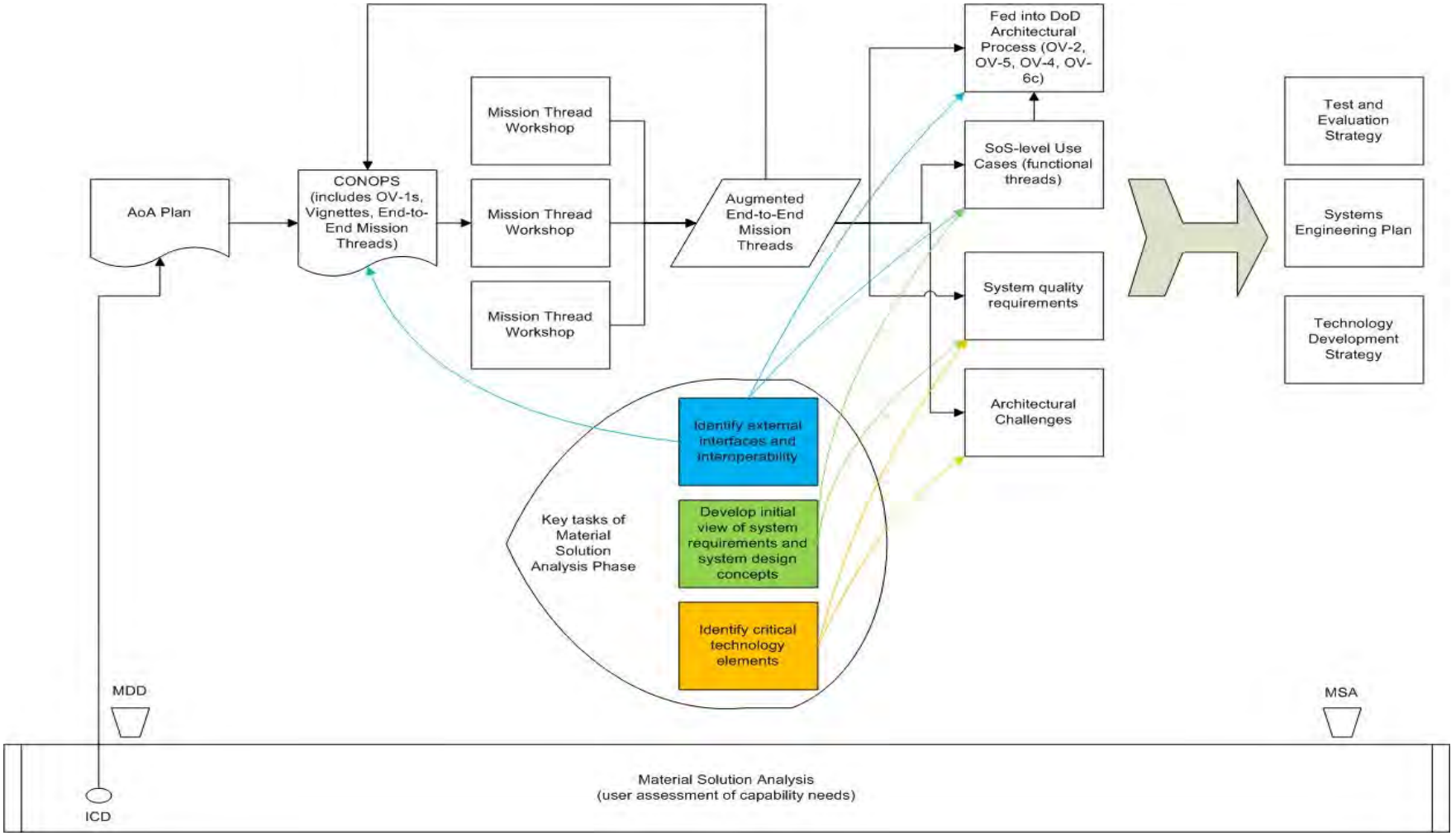


SoS Architecture Quality Attribute Specification and Evaluation Approach

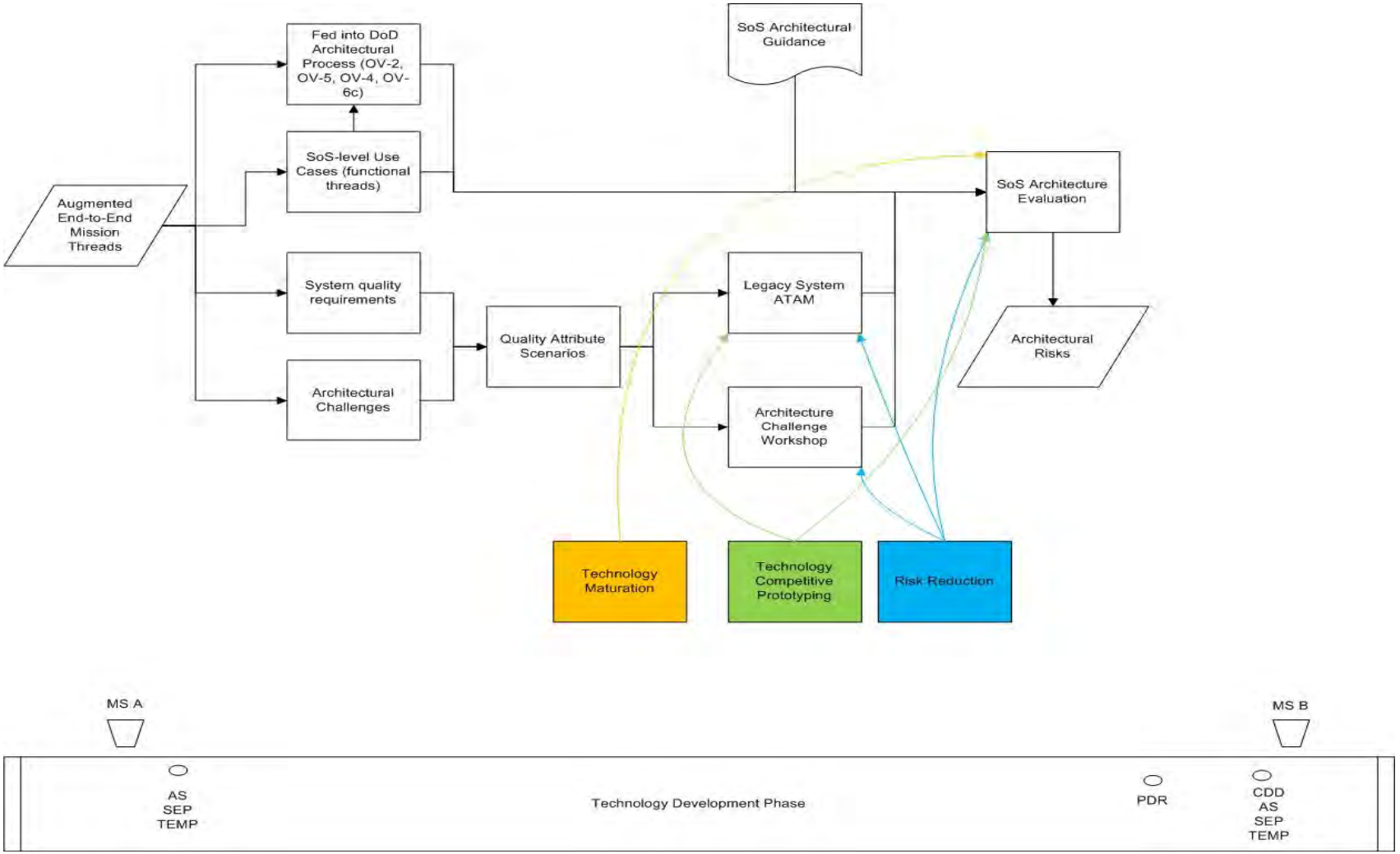
- Early elicitation of quality attribute considerations
- Early candidate legacy system architecture evaluation
- Early identification and mitigation of architectural risks



Material Solutions Analysis Phase



Technology Development Phase



Contact Information

Mike Gagliardi

Principal Engineer

Software Engineering Institute

Office: 412-268-7738

Email: mjg@sei.cmu.edu