C2 ARCHITECTURES: The Persistent Challenge

Alexander H. Levis

18th ICCRTS

20 June 2013

Alexandria, VA

Outline

- A Little History
- The Persistent Challenges and the Elusive Next Best Thing
- Systems of Systems
- Service Oriented Architectures and Clouds
- Resilience
- A C2 Challenge: Integrated Courses of Action
- A Current Example
- Closure

A Little History: The Symposium

- In 1978 the first MIT/ONR Workshop on C2 was held in Cambridge, MA with the objective of creating a research community focused on C2
- In 1979, a workshop held at NDU articulated the need for a Science of Command and Control
- In 1987 the MIT/ONR Workshop was transformed into the Symposium on C2 Research sponsored by the Joint Directors of Laboratories and held at NDU and the Naval Postgraduate School
- In 1995 the scope was expanded and it became the C2 Research and Technology Symposium (CCRTS) sponsored by the Command and Control Research Program under Dr David Alberts
- Also in 1995 the International series was launched (ICCRTS) with both events integrated in June at the National Defense University
- From 1996 to 2006 the two series run in parallel for most of the time
- The CCRTS and the ICCRTS merged in 2007 and have continued in this form to this day

The Persistent Challenges

- Early on in these meetings, it was observed that C2 theory had to address three major challenges:
  - Coping with Uncertainty
    - Adversaries, missions, coalition partners, goals and objectives
  - Coping with Complexity
    - Net-centricity and Net-Enabled capabilities, Information sharing in a contested cyber environment, DIME and PIMEESI
  - Coping with Change
    - Transnational and non-state actors, technological change (e.g., PGMs, UAVs and UCAVs, cyber warfare), rapidly changing geo-political structure
- These challenges are still here and they keep accelerating

Many Solutions

- Every six or seven years*, a "next best thing" appears with the promise to address the daunting C2 problems
  - Examples:
    - C4ISR and DOD Architectures
    - Systems of Systems
    - Service Oriented Architectures
    - Cloud Computing
- And new concepts or "organizing principles" are articulated
  - Examples:
    - Net Centricity
    - Net Enabled Capabilities
    - Information Sharing
    - Communities of Interest
    - Collaboration

** Totally unscientific observation*

But Solutions Have Limitations

- However, as we start to go past the Powerpoint presentation and try to realize these concepts and design processes and systems we recognize that:
  - While the concepts are valid and worthwhile
  - Their applicability is usually limited
  - They often do not scale
  - They raise a host of new hard problems that need to be addressed

- A pervasive and persistent challenge is how to evaluate the designs based on such solutions
  - Functional Attributes (Performance evaluation: Accuracy, Timeliness, Throughput Rate, etc.)
  - Non Functional Attributes (Mission Assurance, Agility, Resilience, Security, Vulnerability, …)

System of Systems*

- **A system will be called a System of Systems (SoS) when:**
  - **The component systems achieve well-substantiated purposes in their own right even if detached from the overall system;**
  - **The components systems are managed in large part for their own purposes rather than the purposes of the whole;**
  - **It exhibits behavior, including emergent behavior, not achievable by the component systems acting independently;**
  - **[It is geographically distributed]**
  - **Component systems, functions, and behaviors may be added or removed during its use**

* Definition evolved from Maier, Sage, …

SoS Issues

- A System of Systems (SOS) poses novel engineering challenge.
  - Increasing complexity of the SOS Architectures
  - Need to reconfigure to meet unpredictable needs
- While we have extensive System theory expressed in many mathematical formalisms, it is based on the assumption that one can draw the system boundary and determine what is in, what is out, and what the interactions across the boundary are (a Physics-based point of view)
- The fifth attribute of an SoS violates that assumption
- Consequently, we do not have a mathematical theory for the Analysis and Design of Systems of Systems; we have ad-hoc approaches to their design and evaluation

SOSI: The Kluge

- **Assumptions:**
  - **The set of elements that compose the System of Systems changes over time**
  - **The elements are heterogeneous**
  - **The elements are at different stages of their lifecycle**
  - **The SOS defines a set of capabilities implemented by a selection of its elements**

- **Define a SOS Instance (SOSI) that is instantiated from a SOS**
  - **A SOSI is instantiated from available elements of the SOS based on the relationships described in the SOSI architecture**
  - **Each SOSI is unique**
  - **A SOSI provides a particular set of capabilities, a subset of the SOS capabilities**
  - **The SOSI is actually a System; we can analyze it and evaluate it**

Adaptability

- *Cohesion* - measure of the relatedness of inputs and outputs within a Node (a node contains one or more elements)
- *Coupling* - measure of the interdependence among Nodes
- *Adaptability* – the degree to which a SOSI or Node can change configuration

$$Adaptability = Cohesion^{-\alpha} Coupling^{-\beta} \qquad \alpha + \beta = 1$$

The inverse of the Cobb-Douglass production function is used

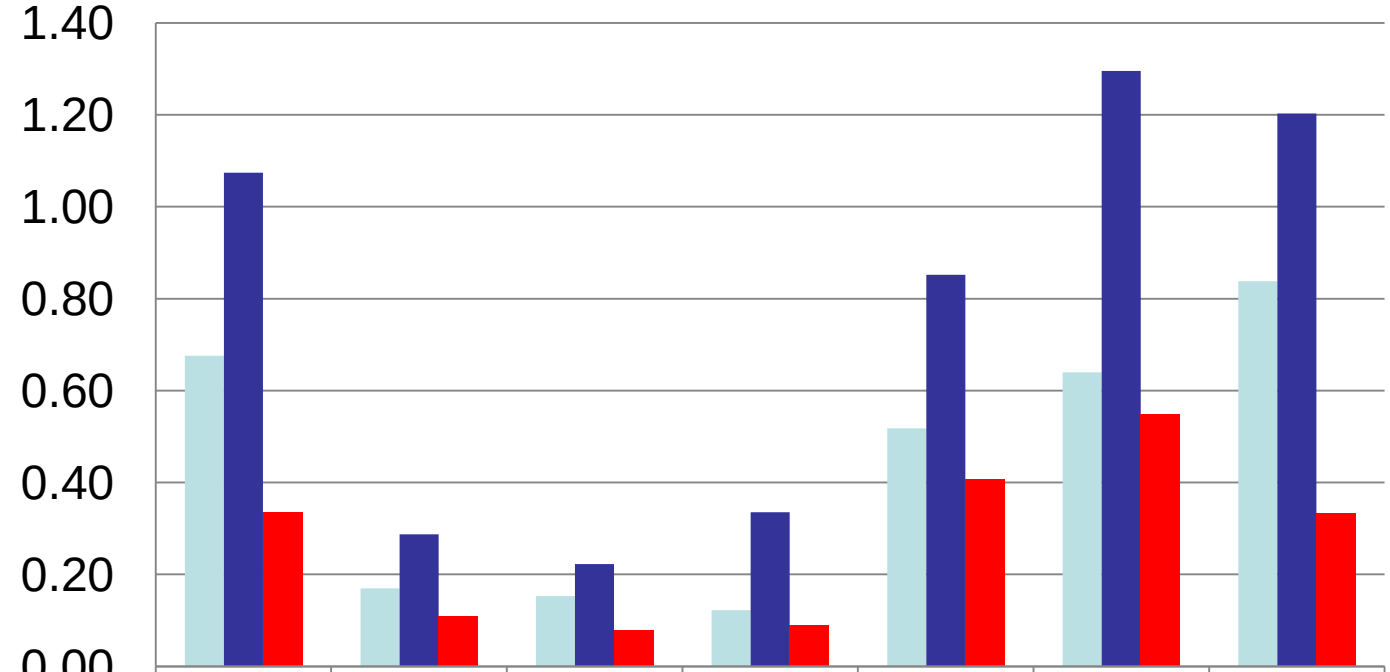
α and β are the elasticities of substitution

- High Adaptability: Low Cohesion within Nodes, Low Coupling among them
- Medium Adaptability: Low Cohesion within Nodes, High Coupling among them or High Cohesion within Nodes, Low Coupling among them
- Low Adaptability: High Cohesion within Nodes, High Coupling among them

Example: ESG

- A Naval Expeditionary Strike Group reconfiguring its C2 to address an unexpected Humanitarian Assistance / Disaster relief mission
- Three Architecture Patterns:
  - Peer to Peer (PtP)
  - Centralized (CS)
  - Service Oriented Architecture (SOA)
- Three configurations of the SOSI that contains 19 elements
  - Alt 1: Six Nodes
  - Alt 2: Eight Nodes
  - Alt 3: Four nodes
- The architectures were designed, executable models derived and analysis and simulations carried out

Adaptability

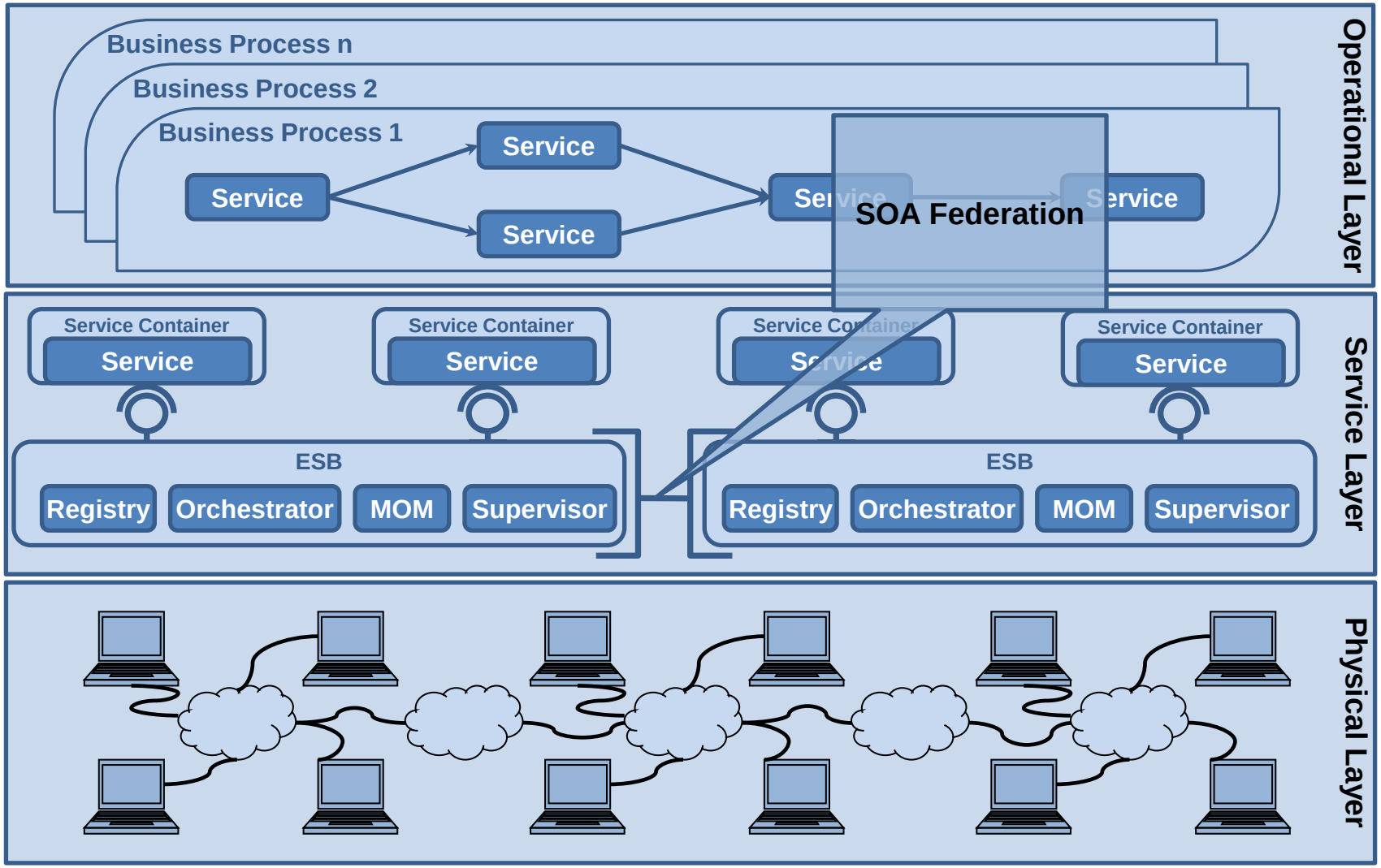


	P2P	CS1	CS2	CS3	SOA1	SOA2	SOA3
Alt 1	0.68	0.17	0.15	0.12	0.52	0.64	0.84
Alt 2	1.07	0.29	0.22	0.34	0.85	1.30	1.20
Alt 3	0.33	0.11	0.08	0.09	0.41	0.55	0.33

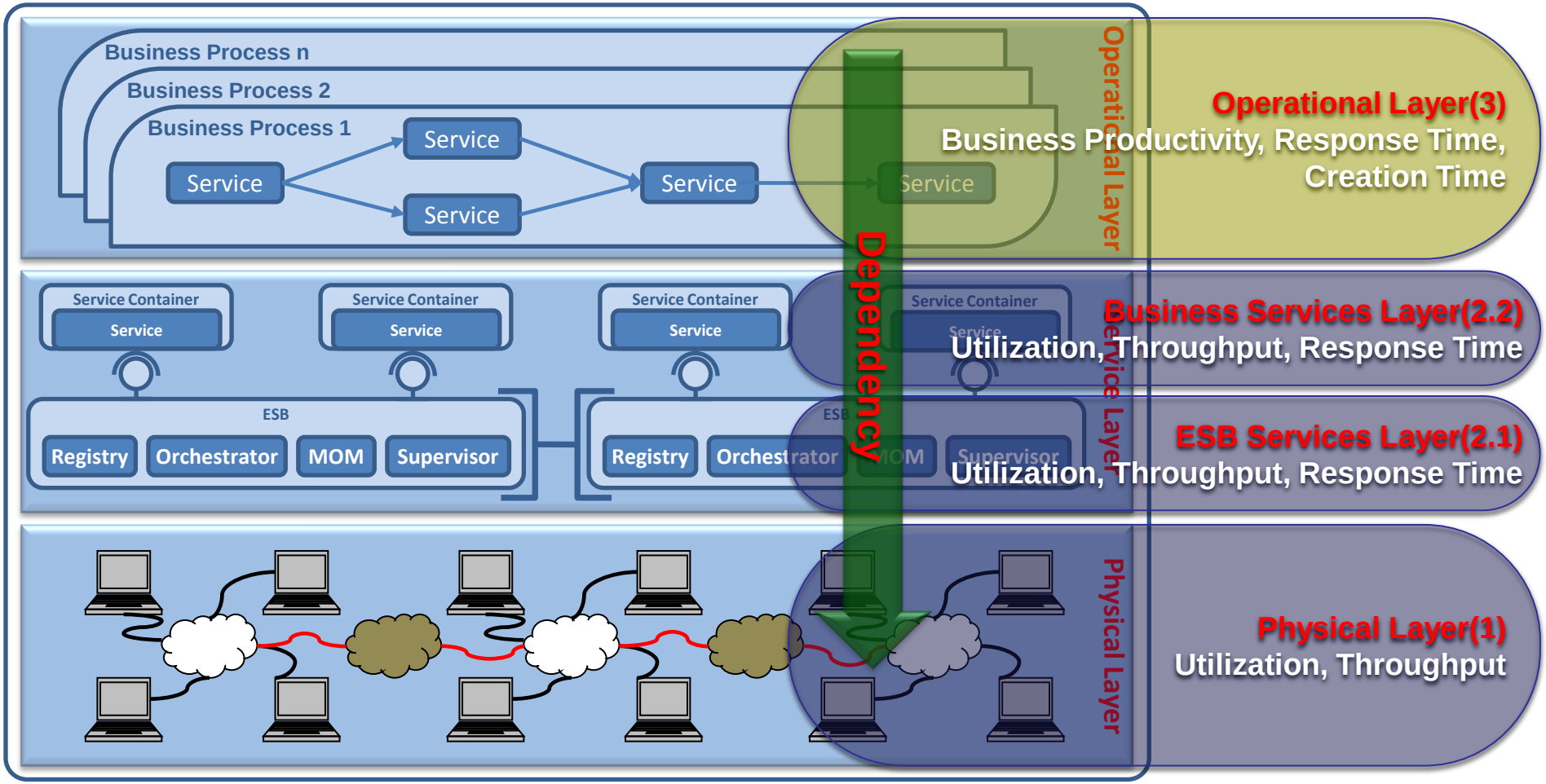
Service Oriented Architectures

- SOA is an architecture for building applications as a set of loosely coupled black-box components orchestrated to deliver a well-defined level of service by linking together processes.
- These *loosely coupled* components can be combined and recombined in different ways
- SOA should support Net-Centric Concepts or Net-Enabled Capabilities by:
  - Populating the Net Enabled Environment with new capabilities
  - Utilizing existing Net Enabled capabilities
  - Accommodating un-anticipated users
  - Promoting the use of Communities of Interest (COIs)
  - Supporting shared infrastructure
- An essential enabler of a SOA is meta-data (it is the currency of SOA)
- However, different meta-data sets lead to different SOAs that then need to be federated
- Key issue: Quality of Service (an evaluation issue)

SOA Federation Environment



Analysis & Evaluation of the Hybrid Executable Model, 2

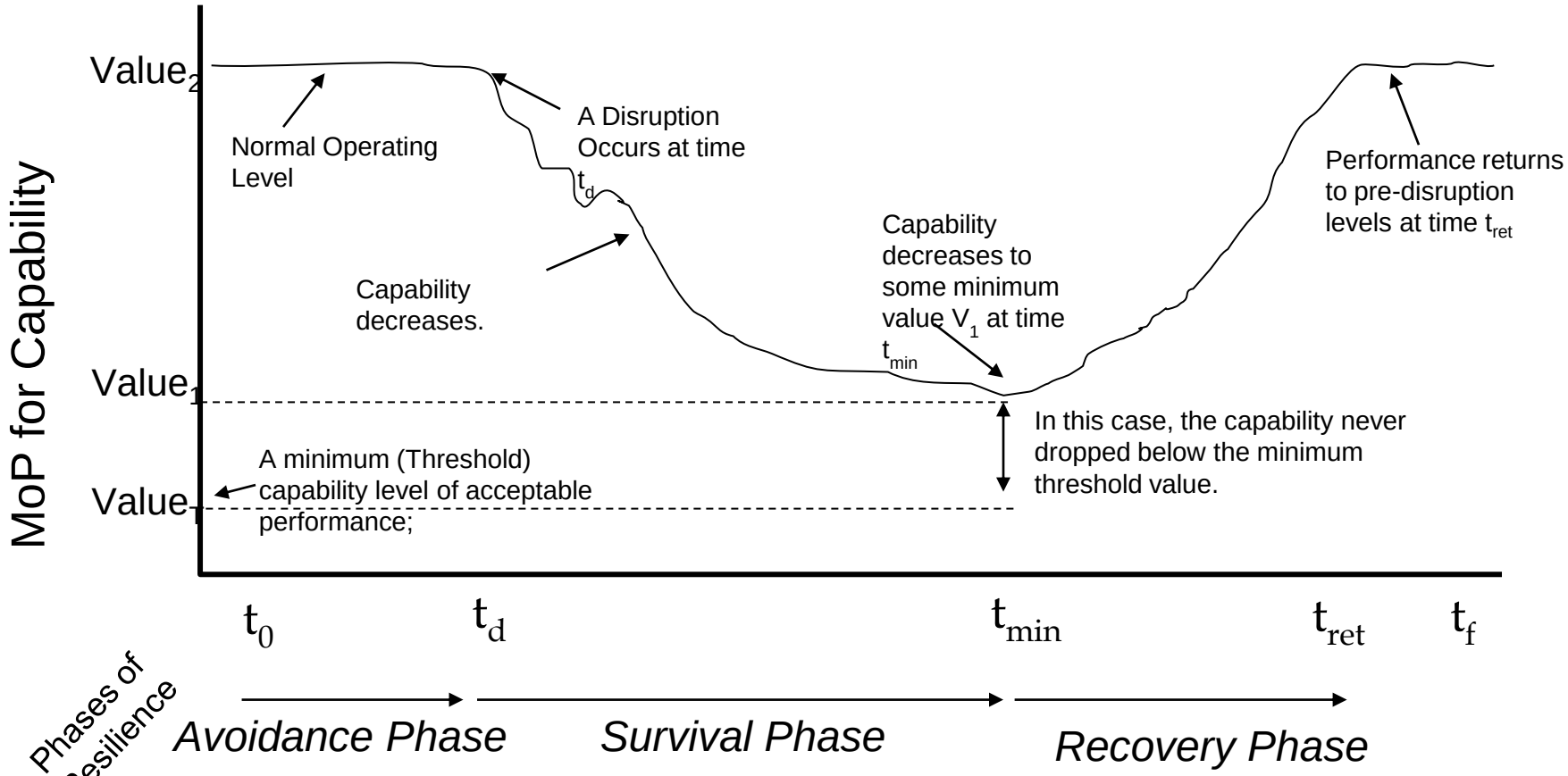


The Challenge

- Meta-data is not universal; rather Communities of Interest define their own meta-data
- Some meta-date is common by agreement, but much is not (semantic differences)
- Consequently, we cannot integrate SOAs; we need to federate them so that we can exploit service availability across SOAs (a sort of cross-domain issue)
- That brings in a whole new level of necessary infrastructure that increases complexity and degrades the Quality of Service
- A key component of SOA is the orchestrator (or workflow manager) that needs to deal with semantic issues for the valid interconnection (inter-operation) of services when crossing COIs.
  - Think of creating workflows in which Apple apps and Android apps inter-operate in complex ways
  - Think cloud computing across clouds!

Resilience and Time

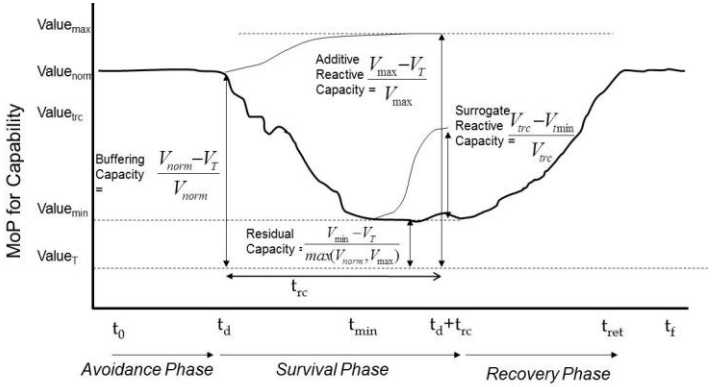
Resilience is the ability to "avoid, survive and recover from disruption"

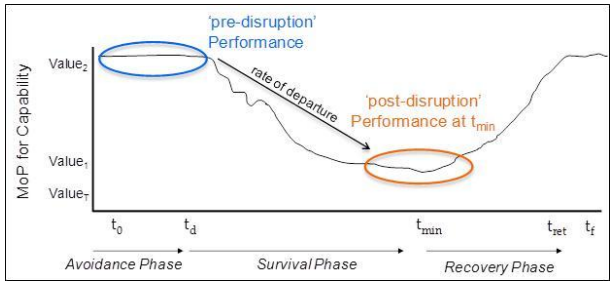


An evaluation of resilience must consider time

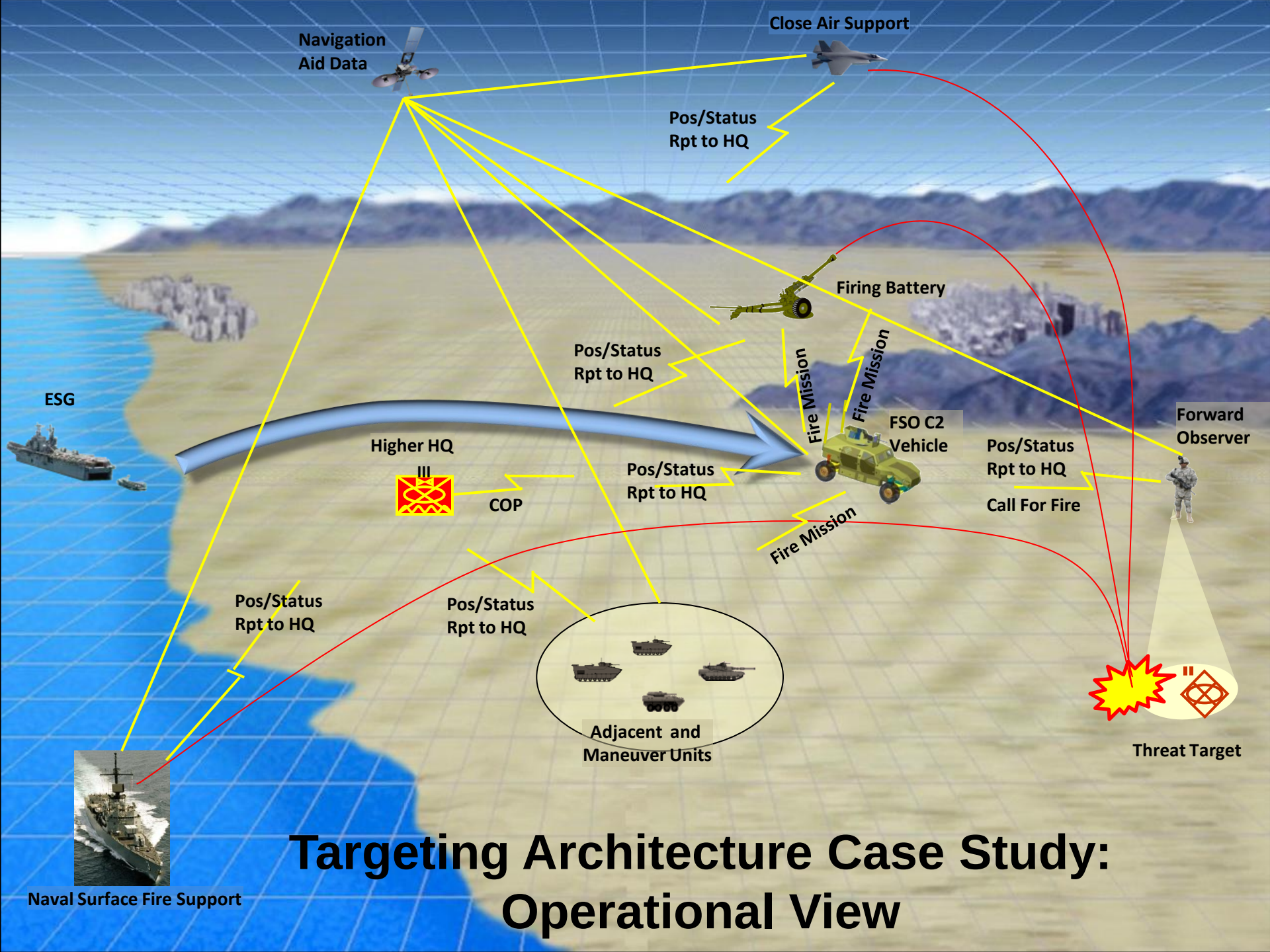
Resilience Measures

Concept	MOP
Capacity "The ability to operate at a certain level of capability as defined by a given measure"	Buffering Capacity
	Reactive Capacity
	Residual Capacity
Tolerance "the ability to degrade gracefully after a disruption"	Rate of Departure
	Fault Tolerance
	Point of Failure Tolerance
Flexibility "the ability of a system to reorganize its elements to maintain its capabilities"	Cohesion
	Common Use
	Proportion of Use





$$Tol_{RD} = \frac{\left[\frac{L_p \cap L_r}{L_p}, t_d\right] - \left[\frac{L_p \cap L_r}{L_p}, t_{\min}\right]}{t_{\min} - t_d}$$

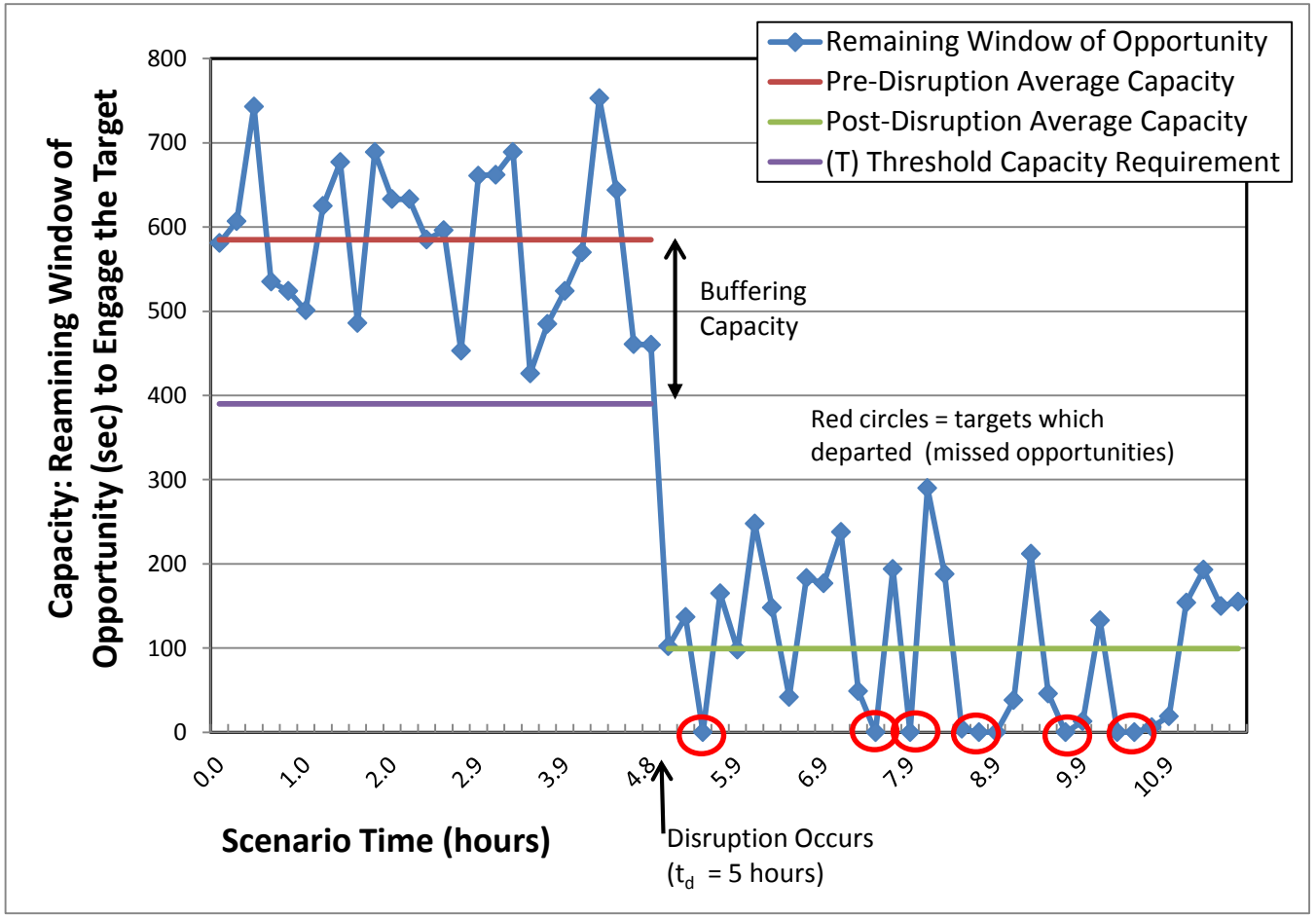


Targeting Architecture Case Study: Operational View

Targeting Architecture: Scenario and Disruption

- Examine the resilience of the capability to 'Coordinate and Synchronize Fire Support' to disruption of the 'geo-positioning navigation aid signals (GPS)' in early entry operations (of what, to what, under what conditions)
- Cyber attack to the GPS satellite constellation scrambled the GPS signal, rendering it useless
- Loss of GPS affects the fire support process from end to end (FO self-location, target location, clearance of fires, and allocation of weapons)
- Each portion of the fire support team can still complete the process, but the process transitions to pre-GPS era methods which require much longer times to complete. Soldier common task standards for times to manually complete tasks, vs. GPS enabled times are used
- No backup is available to offset this loss except for the older manual approaches (i.e., no reactive capacity exists to this disruption)

Capacity


Remaining Window of Opportunity
Pre-Disruption Average Capacity
Post-Disruption Average Capacity
(T) Threshold Capacity Requirement
Capacity: Reamining Window of Opportunity (sec) to Engage the Target
800
700
600
500
400
300
200
100
0
Buffering Capacity
Red circles = targets which departed (missed opportunities)
0.0
1.0
2.0
2.9
3.9
4.8
5.9
6.9
7.9
8.9
9.9
10.9
Scenario Time (hours)
Disruption Occurs
(t_d = 5 hours)

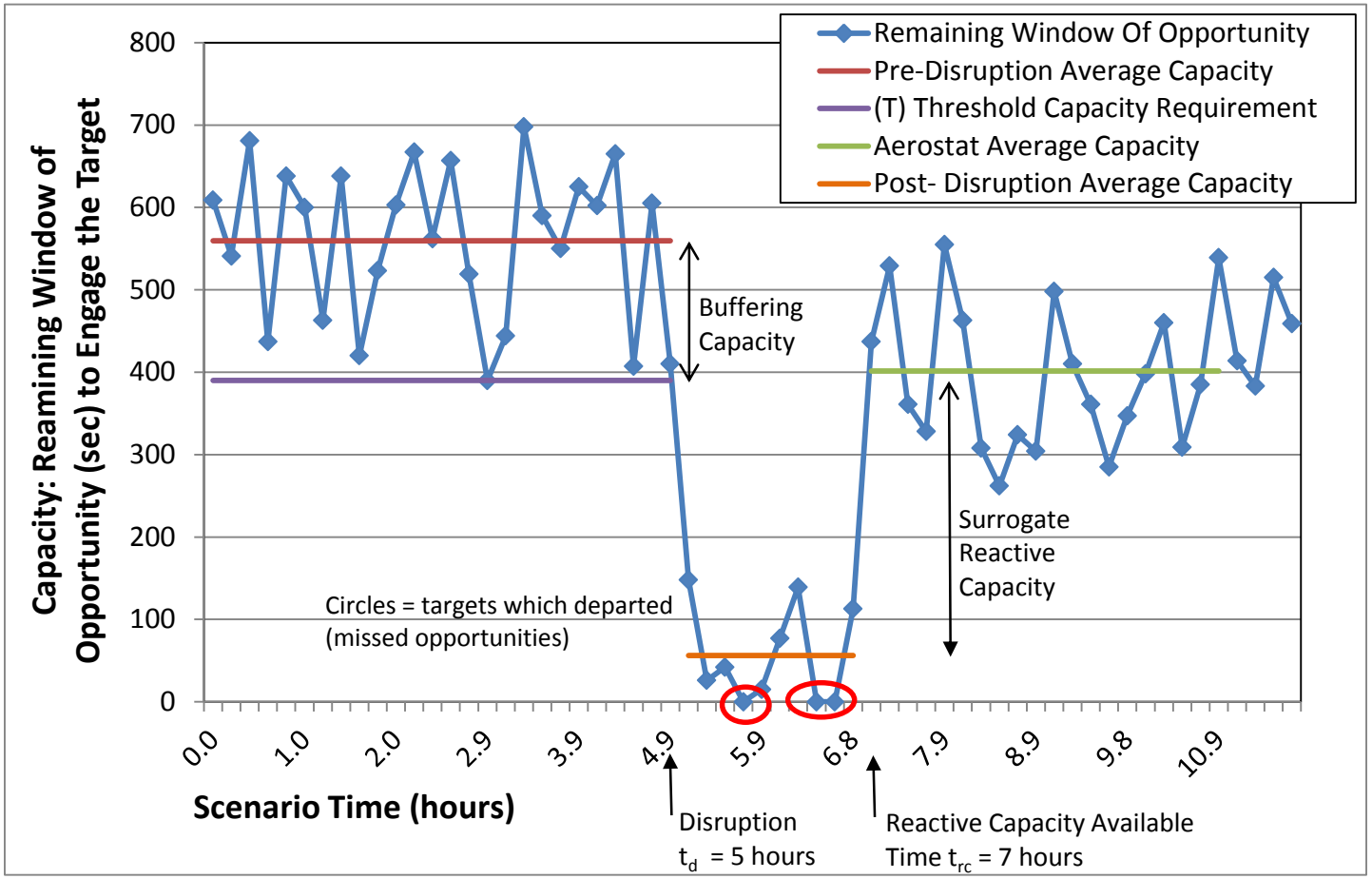
GPS Alternative: An Aerostat

- **Fire Support Community understands its vulnerability to loss of GPS – what can be done?**
- **Aerostats can be used as a limited alternative to GPS.**

- **Approach:**
  - **Modify the architecture to reflect Aerostat reactive capacity.**
  - **Reflect the architectural modifications into the executable model**
  - **Repeat the analysis of appropriate resilience measures**
  - **Apply the revised results into the resilience evaluation framework**

Aerostat Reactive Capacity

- The aerostat returns performance to meet requirements
- However, there is a window of severe vulnerability
- Issue: Static performance analysis vs. dynamic performance analysis

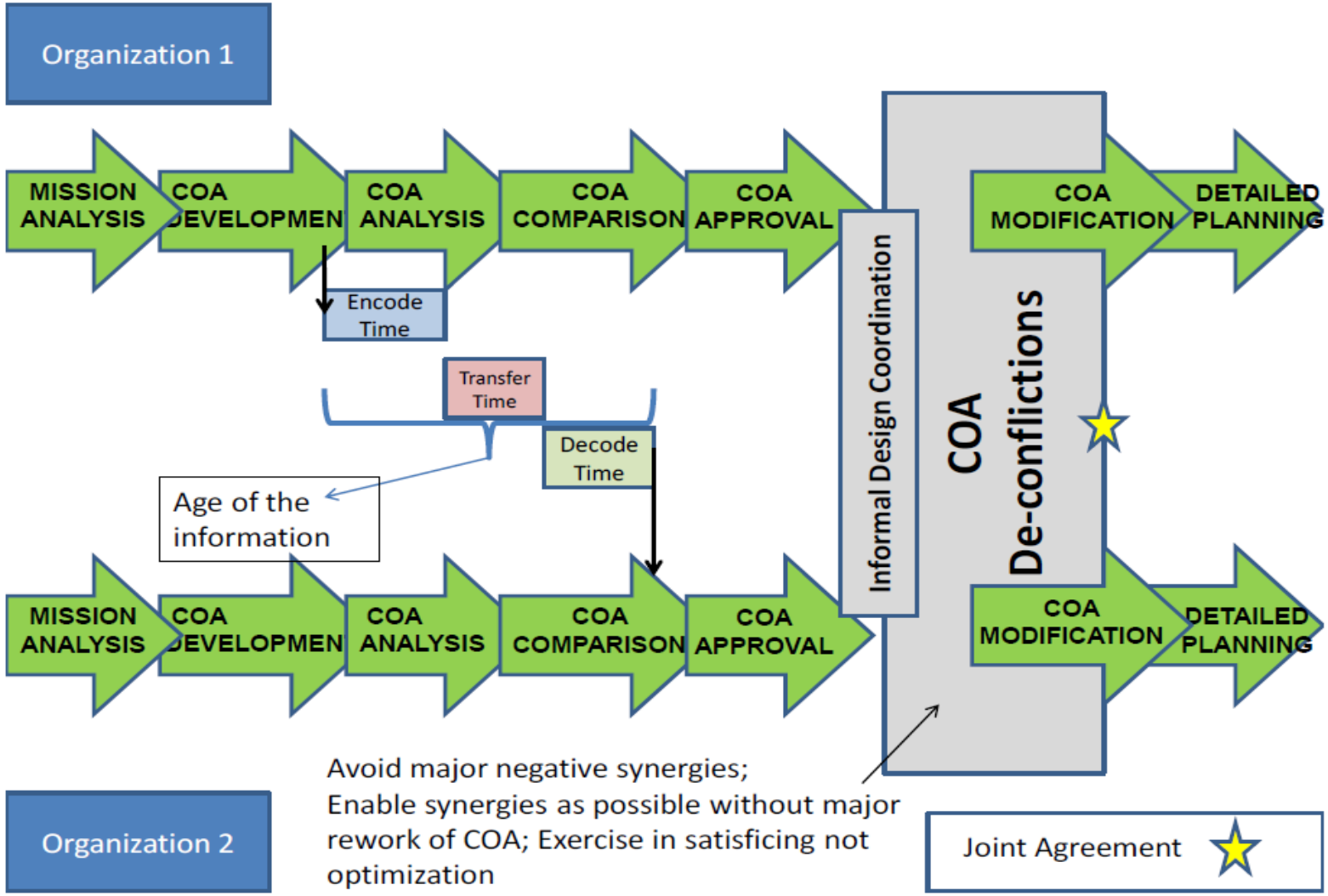


Integrated Courses of Action (Cross-Domain)

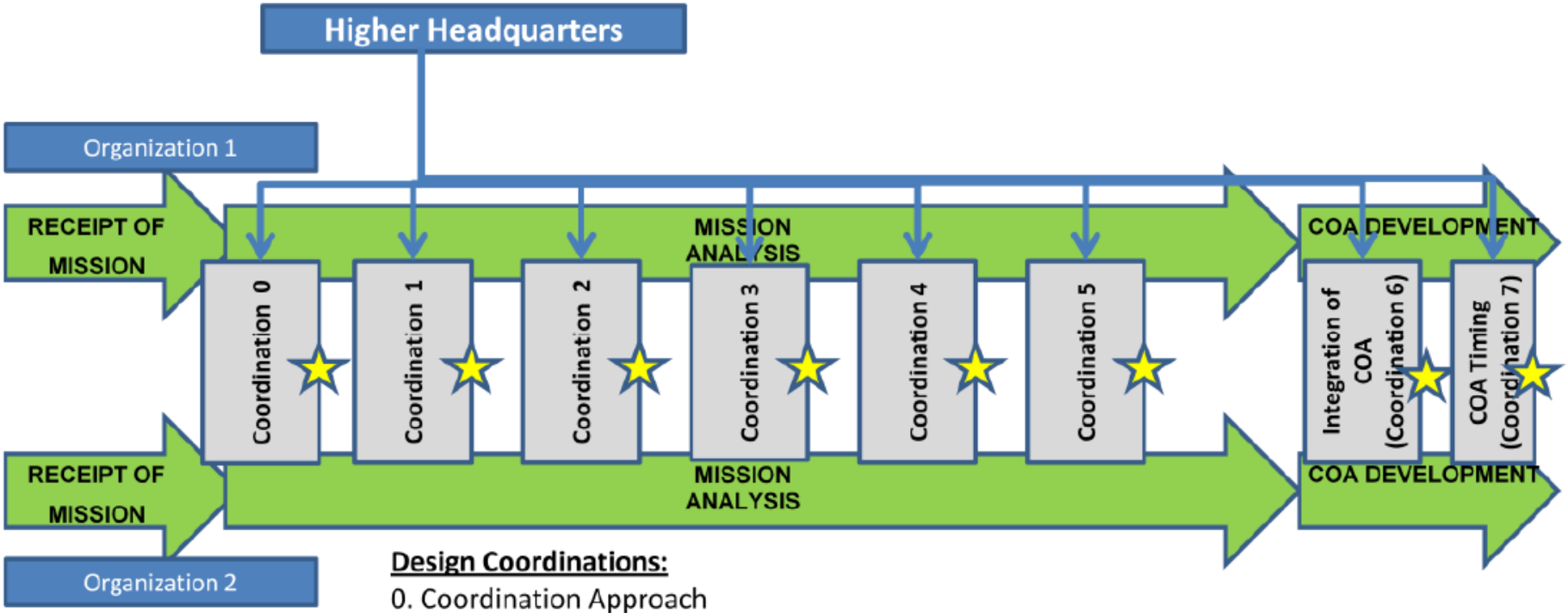
Integrated COA – A COA in which all participating entities act as one organization in pursuit of common goal(s); A COA in which no higher estimation of performance can be obtained by changing the actions taken and action timing in each involved domain

- **Current C2 enterprise processes cannot produce integrated Courses of Action (COAs) within the desired timeframes for planning**
  - **Time-constrained Crisis Action Planning results in COAs which are not fully integrated adding more risk to military operations**
  - **Lack of a method to discover and agree upon cross-domain effects makes mutual adjustment between domains very difficult**
  - **Commanders are often required to perform (mental) COA integration themselves during decision making**

Current De-Confliction Approach



Co-Design or Collaborative Approach



Design Coordinations:

0. Coordination Approach
1. Objective(s) and metric(s)
2. Key Influencers of objective(s)
3. Adversary and environment potential actions
4. Organizations' (Domains') potential actions
5. System structure (interactions, constraints, synergies)
6. Integrated COA
7. Integrated COA Timing

Joint Agreement ★

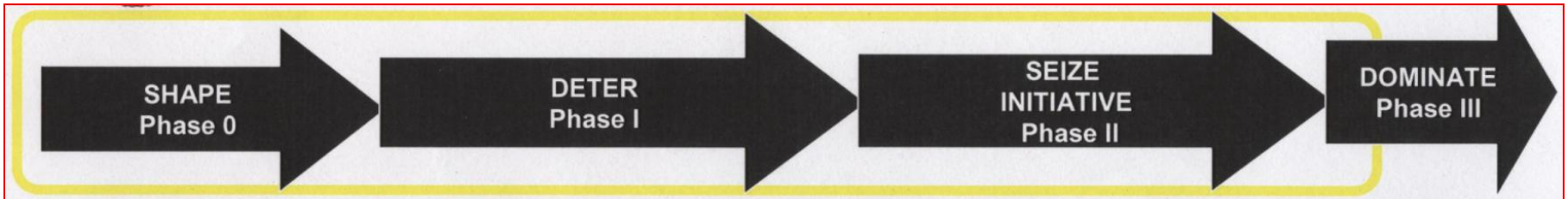
Illustrative Results

- **Maintain prescribed tempo**

Approach Used	Combined COA Type	Process Times (With Iteration Efficiency) (CPN Model)		COA Performance (Probability of Goal Node Being True) (Pythia Model)		
		Minutes	Hours	Coalition OBJs Met	Coalition Losses Avoided	Leader Agrees to Leave Power
New Approach	Integrated COA	3007	50.11	0.802	0.9	0.85
Current Approach Level 2	De-conflicted Level 2	2968	49.46	0.56	0.67	0.59
Current Approach	De-conflicted	2860	47.66	0.394	0.45	0.43
No Coordination	Combined Domain COAs	2610	43.5	0.28	0.32	0.295

Persistent Challenges

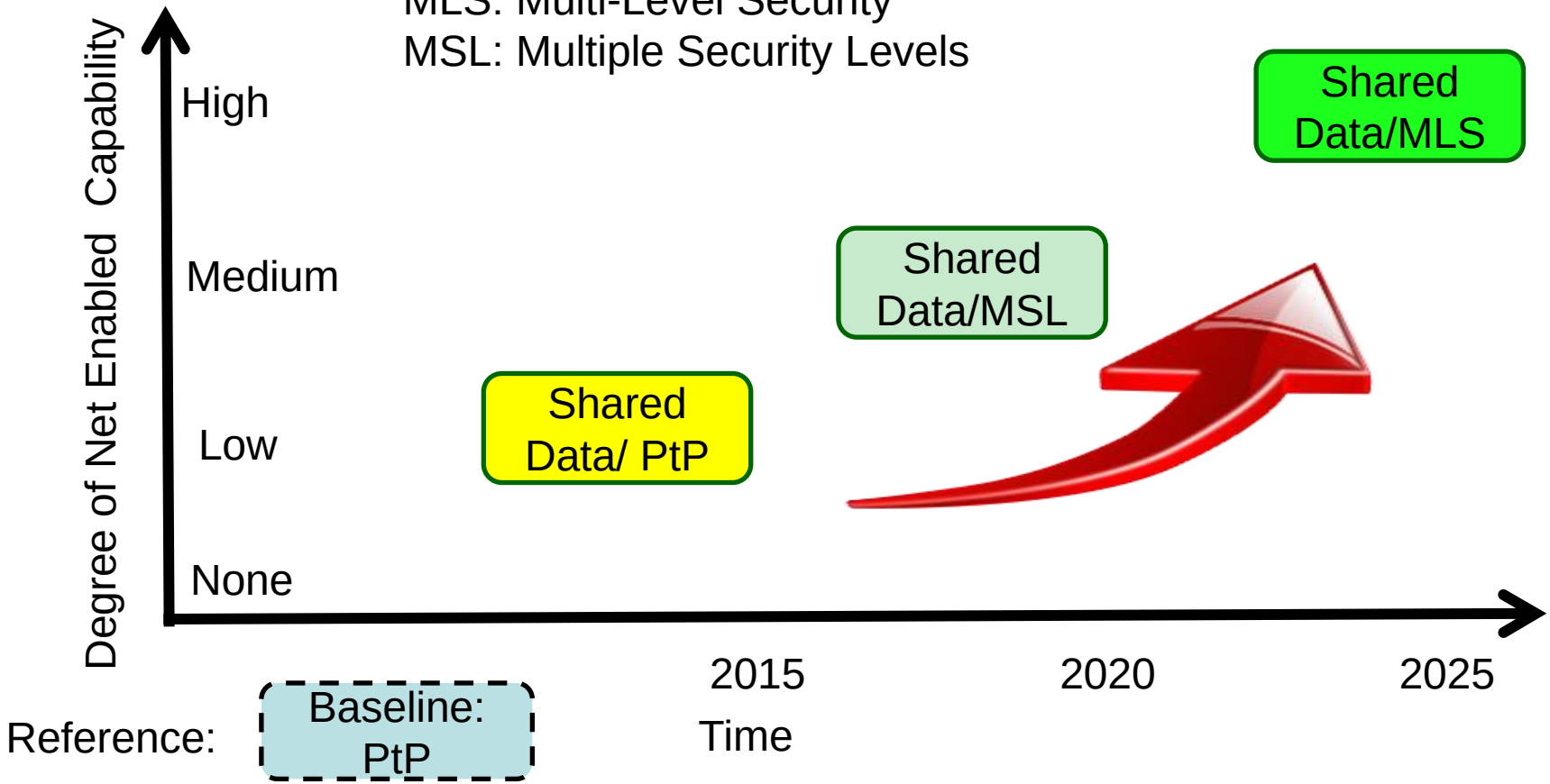
Four Use Cases



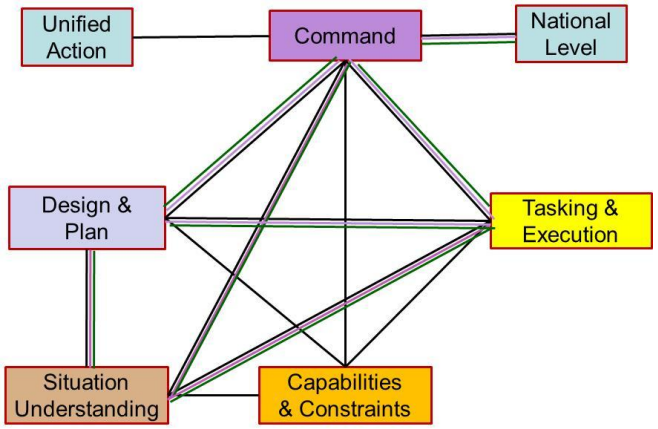
Shape, Prevent, Prepare	Crisis response, Stabilize, De-escalate		Seize Initiative; Achieve Freedom of Action in Global Commons; Defeat Adversary
USE CASE 1: Day to Day Operations	**USE CASE 2: Prevent Adverse Activity**	**USE CASE 3: Non-Nuclear Attack**	**USE CASE 4: Nuclear Attack**
• End Condition: Maintained Strategic situational awareness and cognition of force readiness • Trigger Event(s): 1) External taskings (UCP, JSCP, etc.) 2) GCC/External requests 3) CCIR/PIR event	• End Condition: Adversary action is prevented/ deterred and Command returns to Day to Day Operations • Trigger Event(s): Indications & warning indicate imminent adverse activity or "act of nature"; however no overt activity has occurred	• End Condition: Minimize effect of attack & prevent further attacks • Trigger Event(s): Kinetic attack, non-kinetic attack (asymmetric attack), or perceived attack against national interests/allies	• End Condition: End Attack on conditions favorable to US and Allies • Trigger Event(s): Valid indications of major strategic attack on US interests or Allies; Missile or Missiles inbound; Radiological detonation

Architecture Evolution

PtP: Point to Point
SD: Shared Data
MLS: Multi-Level Security
MSL: Multiple Security Levels

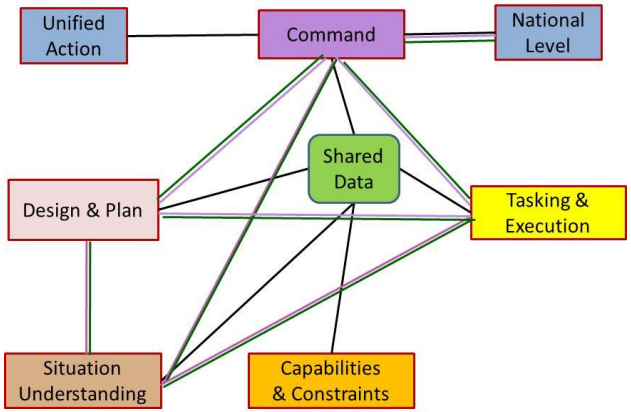


Comparison of the Four Architectures



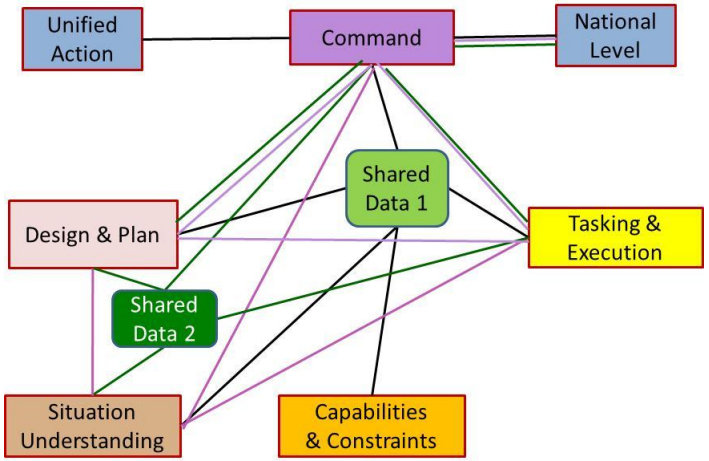
Baseline: Point to Point

1



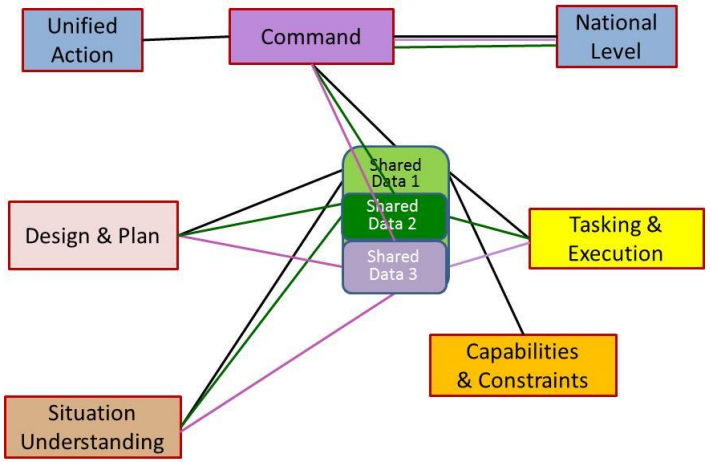
Shared Data / PtP for security

2



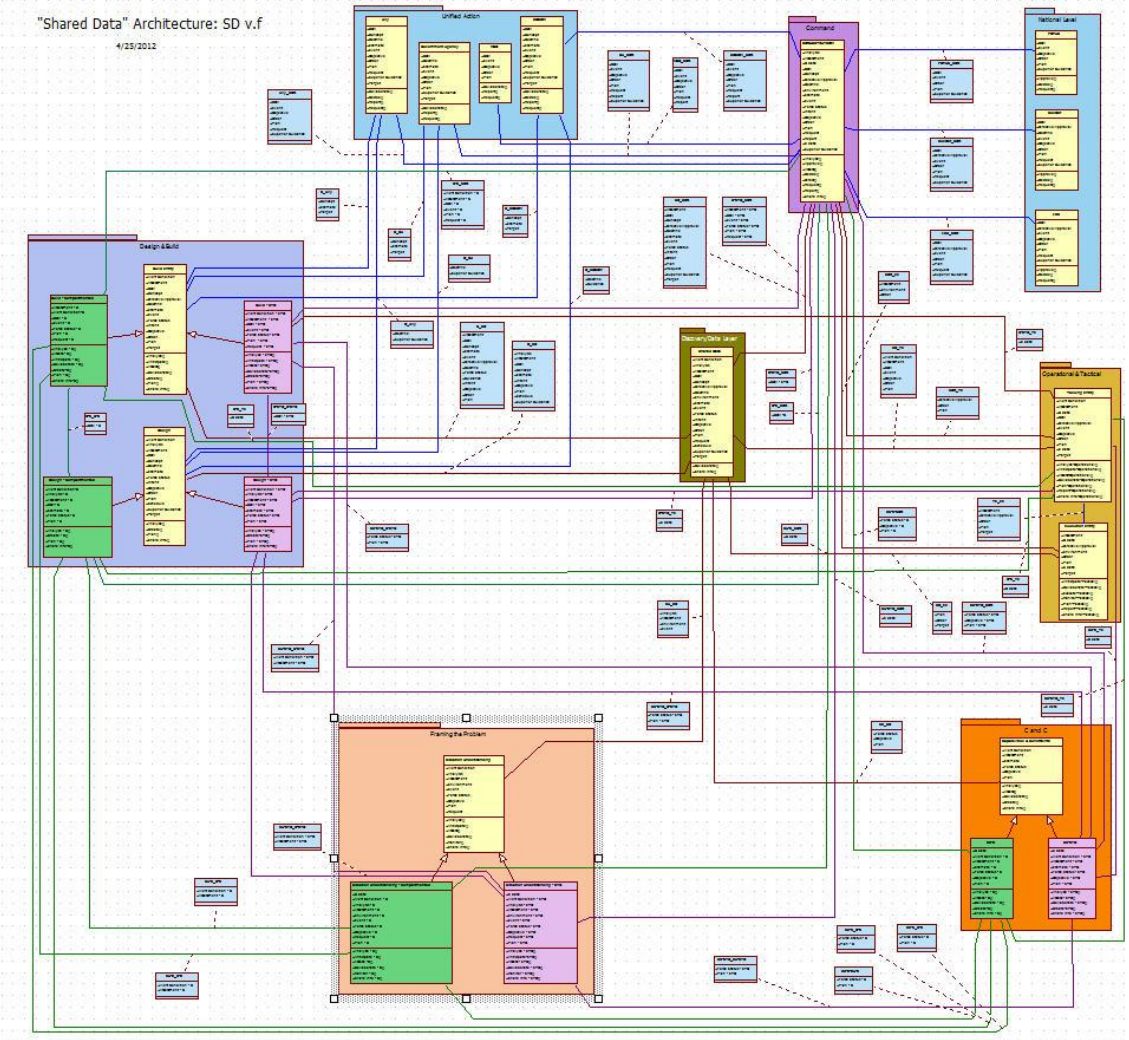
Shared Data at Multiple Security Levels

3



Multi-Level Security

Example Architecture



The Challenges

- Enable Information Sharing at different levels of classification
- Enable collaboration while maintaining security levels
- Not all collaboration schemes are created equal. How do we design the appropriate collaboration architecture for each Community of Interest?
- Some experimental and Modeling and Simulation data exist rom the ELICIT program (see The Agility Advantage by David Alberts) but more, problem focused experimentation is needed
- USSTRATCOM is launching a Campaign of Experimentation to address these issues
  - Processes will need to adapt
  - Systems will need to be modified
  - Behaviors will need to change

Some Questions

- **Have the original goals that launched these conferences been met?**
  - **Yes, a Research and development community has evolved; Command and Control is now in the public consciousness**

- **Is Command and Control a viable, challenging research field?**
  - **Yes, and the challenges are getting harder. We need new theories (and empirical data) to address the impact of information technology on processes and on human (operator and commander) behavior**

- **Do we understand the difference between C2 and C4I?**
  - **Yes, most of the time, but there is still the tendency to jump to system solutions without fully assessing the need to change the processes**

Closure

- **In 1987, at the first Symposium on C2 Research, I gave a plenary speech on the Quest for a C2 theory that started with the opening lines from *Ithaca* by the Greek poet, K. Kavafy:**

  "When you start on your journey to Ithaca, then pray that the road is long, full of adventure, full of knowledge,"

- **The talk ended with these lines from the same poem:**

  "Ithaca has given you the beautiful voyage, without her you would not have taken the road. … and with so much experience you have gained, you must surely have understood what Ithacas mean."

- **Twenty six years later, looking back at what the C2 community has contributed to the warfighter and the promise it holds for addressing the continuously evolving (and persistent) challenges, it is clear that *it is the journey and not the destination* that we should cherish**
- **And the journey promises to be "*long*, *full of adventure, full of knowledge*"**