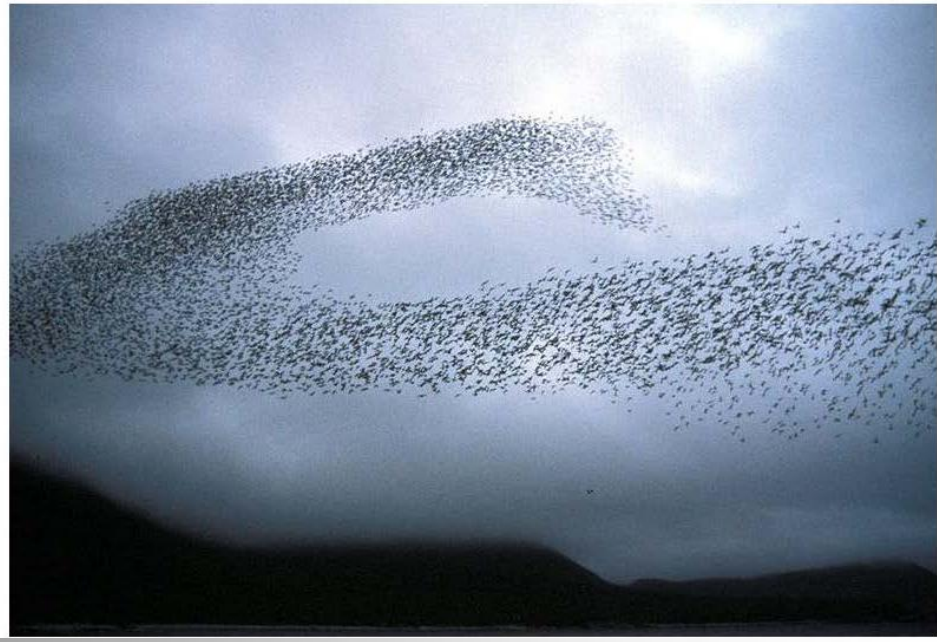
Complex Systems Engineering Applications for Future BMC2

Bonnie Young
Naval Postgraduate School
Professor, Systems Engineering
bwyoung@nps.edu
703-407-4531

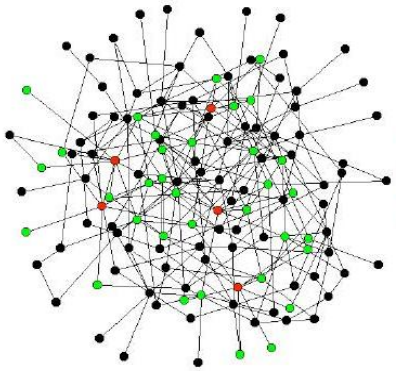
What makes a system complex?

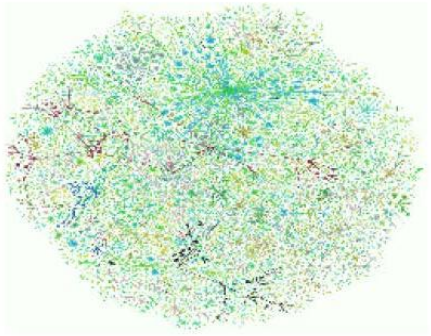
- # of decisions that have to be made regarding design
- Complexity of operational environment
- Degree of control (Centralized, decentralized, etc.)
- Complexity of objectives (#, inconsistency, etc.)
- Implications of design decisions less predictable
- Change at any level may have system-wide impacts
- Lateral influences stronger and more dominant than hierarchical relationships
- Risk dominated by system-level risk (rather than local risk)
- Small causes can have large effects

SWARMS



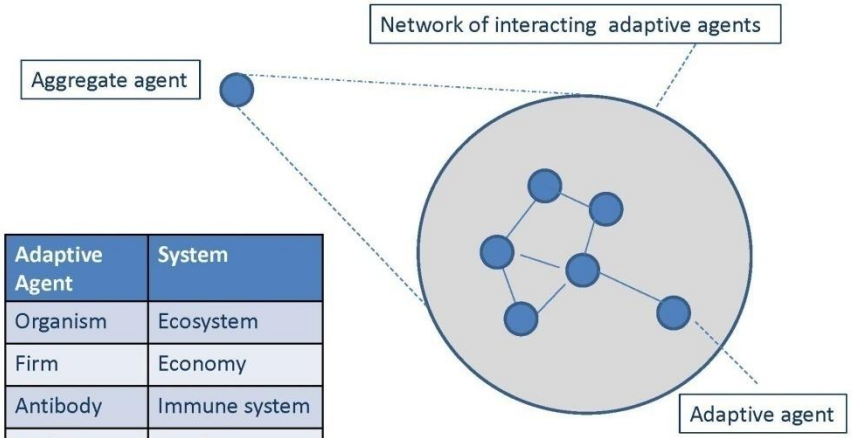
COMMS NETWORKS



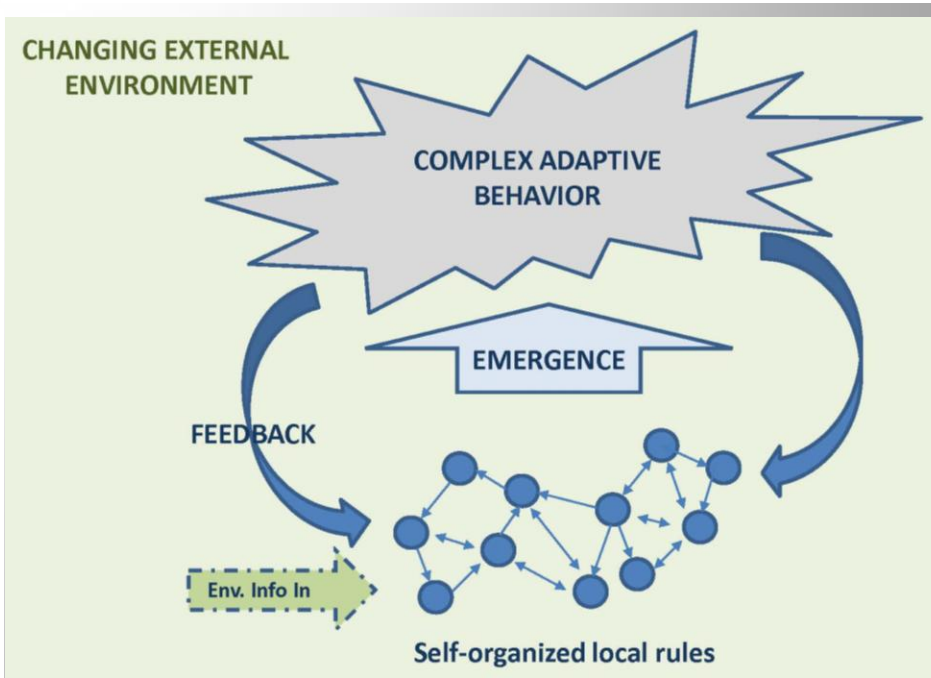


As yet, no one is studying how network interactions change over time...

AGENTS



Adaptive Agent	System
Organism	Ecosystem
Firm	Economy
Antibody	Immune system
Trader	Market
Department	Organization



Complexity vs. Complication

Degree of Independence

- In a **complicated system**, various elements that make up the system maintain a degree of independence from one another. Removing one element does not fundamentally alter the system's behavior apart from that which directly resulted from the piece that was removed.
- **Complexity** arises when the dependencies among the elements become important. Removing an element destroys system behavior to an extent that goes well beyond what is embodied in that element.

Inherent Nature

- Complexity is a deep property of a system, whereas complication is not.

Reducibility

- Complicated systems are reducible, whereas complex ones are not.

Complex Systems Engineering

- Why is there a need for Complex Systems Engineering?
- TSE = Traditional Systems Engineering
- CSE = Complex Systems Engineering

Traditional System	Complex System
Hierarchical Relationships dominate lateral influences	Lateral influences dominate hierarchical relationships
Cause and effect are relatively obvious and direct	Cause and effect are not obvious and direct; Small causes can have large effects
The implications of design decisions are relatively predictable	The implications of design decisions are much less predictable
Risks are dominated by the local risks in achieving the contributing parts	Risks are dominated by system risks, with unforeseen emergent properties
Influences on, and implications of, decisions tend to follow the local partitioning of the solution elements	Influences on, and implications of, decisions are much more difficult to bound and to establish

Emergence

- A classical systems principle
- Emergence holds that patterns and properties in a complex system will come about (emerge) through operation of the system
- These patterns and properties cannot be anticipated beforehand and are not capable of being deduced from understanding of system constituents or their individual properties

…also known as the "law of unintended consequences"

- Potential advantage: higher-level functionality emerging from engineered elements comprising a complex system
- Potential risk: possible emerging behavior that is unpredictable and unexpected

Emergent Properties

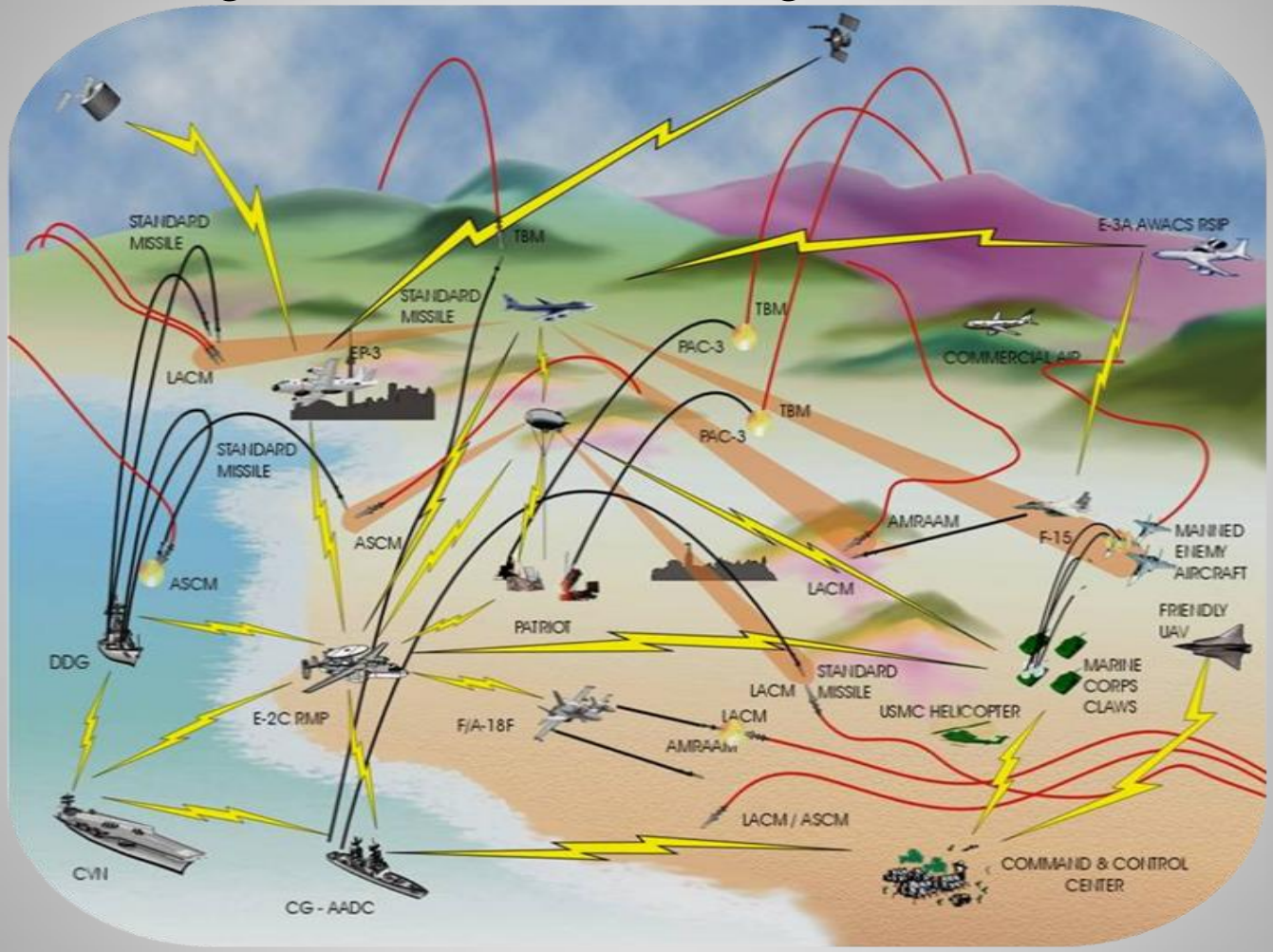
Emergent Properties in General:

- System-level properties exist only at the system level as it functions, being different from and existing beyond the constituent element properties
- System-level properties are not held by any of the isolated elements
- System-level properties are irreducible. They simply cannot be understood, explained, or inferred from the structure or behavior of constituent elements or their local properties
- Understanding the cause-effect relationships can only be established through retrospective interpretation. This renders traditional reduction-based analytic techniques incapable of useful predictions of emergent system-level behavior
- Emergent patterns are not adequately understood without the appreciation of the context within which the patterns exist

Emergent Properties for Future BMC2:

- Enhanced situational awareness (due to optimized sensor resource management) is an emergent property. As sensors are better allocated, the "picture" or information will improve. So it becomes a self-improving cycle of capabilities.
- Force-level capabilities, such as Integrated Fire Control (IFC)

Example: BMC2 as a Complex System of Systems



"...only complex systems can perform complex tasks" [Braha, Minai, & Bar-Yam, 2006]

Future BMC2

BMC2 is the command, control, and management of warfare assets.

Depending on the operational need, BMC2 can range from a single unit (platform) using only local resources to many distributed units functioning collaboratively for the benefit of the group (or Force).

The success of Joint combat operations depends on the individual capabilities of warfare resources (sensors, weapons, communications)

However…

A significant leap in operational capability (force multiplier) will result from achieving a <u>force-level warfighting paradigm</u> that optimizes the use of the resources for the needs of the force.

Future Collaborative BMC2

Shifting to a collaborative "big picture" system of systems arrangement for the BMC2 of the future

- This shift takes maximum advantage of the distributed warfare assets for the needs of the whole

- Example: collaborative BMC2 can select the best shooter (weapon system) from the Force of distributed firing units

Future BMC2 Vision

[1] Implement a System of Systems (SoS) architecture that distributes the “intelligence” among the warfare units

[2] Each warfare unit is a “system” within the SoS

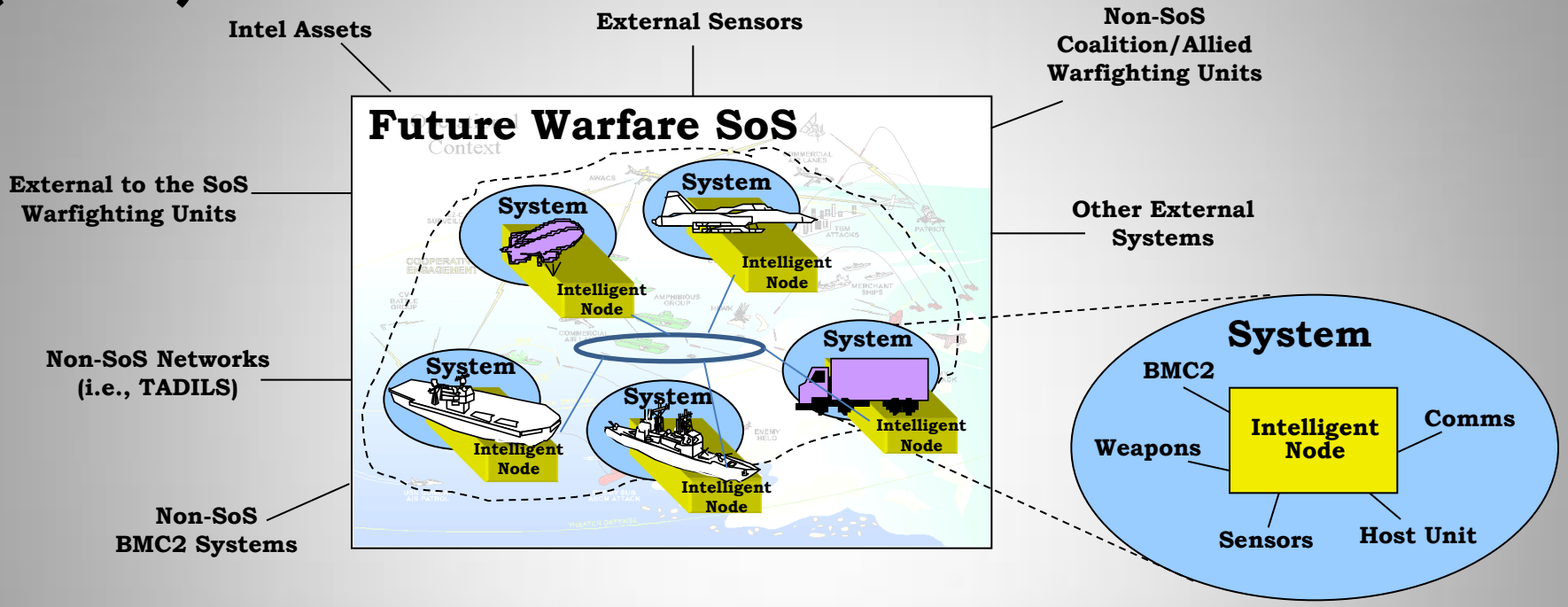
[3] Each system contains a common set of intelligent algorithms and processors

[4] All data and information is shared among the systems

[5] Each system within the SoS is empowered and equipped to operate as an intelligent agent—to make warfare decisions from a force-level perspective

Each system within the SoS is an intelligent agent

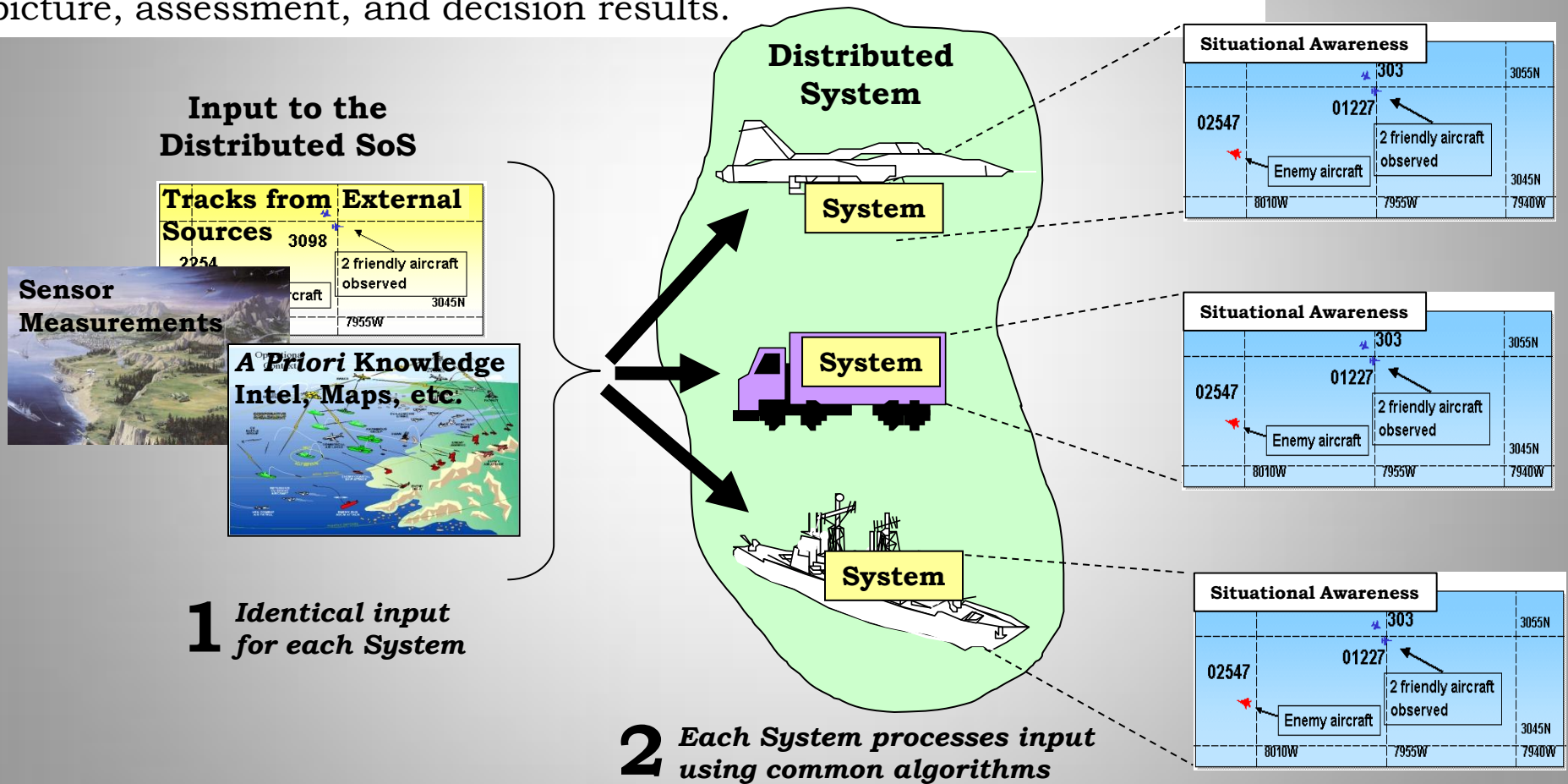
Future Warfare System of Systems (SoS)



- The warfare resources are considered the "systems"; the SoS will be the collaborative utilization and employment of them for the good of the whole.
- Each warfighting unit implements an "intelligent node" with identical/ common processing to perform BMC2 functionality.
- A "system" is defined as the intelligent node integrated with a unit's warfare resources.
- The distributed systems interact (collaborate/communicate) by sharing information with all other systems over a network.

Common Processing Philosophy

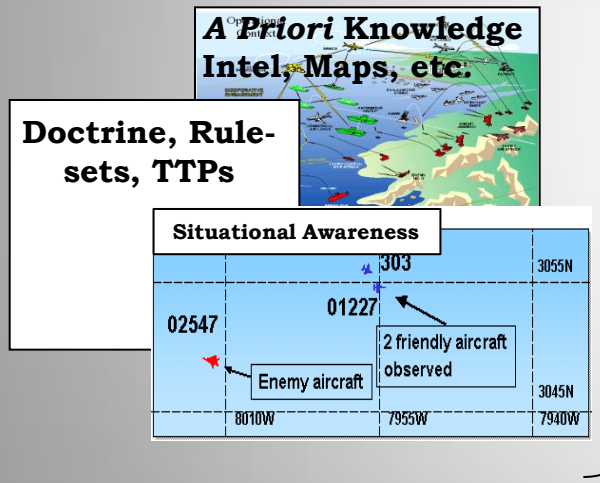
The philosophy, simply stated, is that common processing algorithms provided with identical data & information input will produce identical picture, assessment, and decision results.



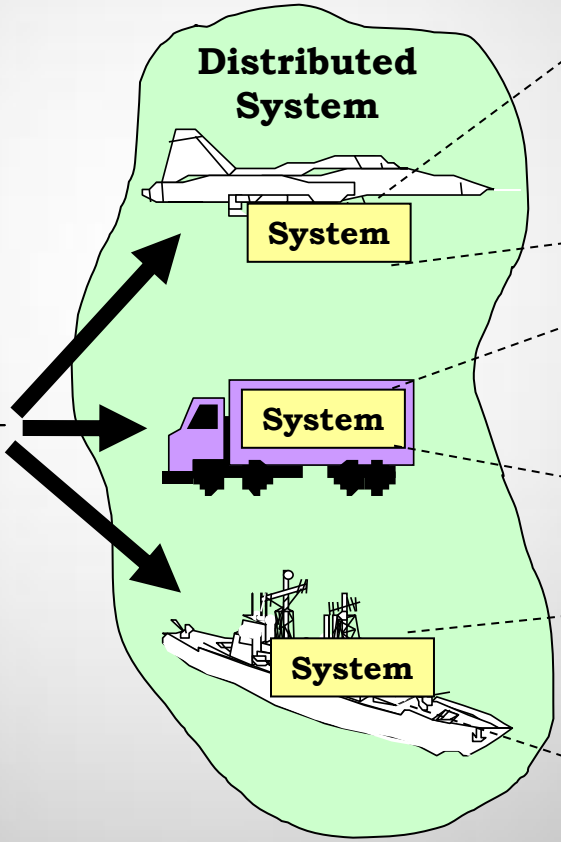
Common Processing for BMC2

Take the "Common Processing" Philosophy One Step Further:
Equip each system with common decision-making and advanced data fusion algorithms, which when fed identical track pictures (or data sets), allows each to produce identical resource tasking recommendations.

Input to the Distributed System

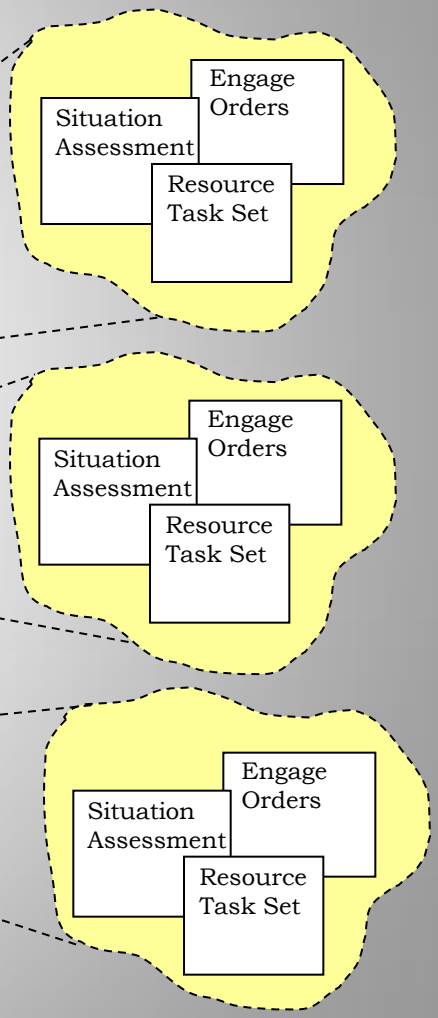


1 ***Identical input for each System***



2 ***Each System processes input using common algorithms***

System Products



3 ***Each System produces identical results***

Emergent Capabilities (Payoffs)

Integrated Fire Control (IFC) refers to the participation and coordination of multiple non-collocated warfare assets in tactical engagements of enemy targets

- IFC is the ability to develop fire control solutions from information provided by remote sensors
- IFC expands the weapon's effective kinematic range by removing dependency on range limits of the local sensors
- Future advances in aerospace warfare depend largely on IFC – the collaborative use of distributed warfare assets for time-critical aerospace engagements.

Payoffs of Future BMC2 Collaboration:

- Improved chance of interception (by selecting the optimal engagement geometry)
- Selection of the best shooter from the distributed warfare assets
- Expansion of the battle space to the effective kinematic ranges of the weapons
- Removes dependency on range limits of the organic/dedicated sensors
- Improved economy of weapon resources (by reducing redundant shots)
- Faster reaction times (earlier launch decisions possible)
- Sharing engagement control – forward pass
- Off-board engagement support for guidance relay and target illumination
- Enhanced defense against complex threat environments (sophisticated or significant numbers of aerospace targets) – IFC may be a necessity for victory

Exploring the Complexity of Future BMC2

Definitions of Complexity

First Definition of Complexity: "…a system in which large networks of components with no central control and simple rules of operation give rise to complex collective behavior, sophisticated information processing, and adaptation via learning or evolution."

- Complexity in future BMC2 systems dependent on:
  - # of participating warfare assets
  - complexity of operational environment
  - level of collaboration (& interoperability) achieved
  - Achievement of a decentralized architecture to empower elements and avoid central control
- Sophisticated information processing inherent in future BMC2
- Adaptation achieved through predictive capabilities—threat prediction, dynamic planning, etc.

Definitions of Complexity (cont.)

Second Definition: "…a system that exhibits nontrivial emergent and self-organizing behaviors."

- Nontrivial emergent behavior is the central objective and payoff of creating a networked collaborative BMC2 system of systems
- Emergent behavior would include: utilization of warfare resources at the force-level and shared situational awareness
- Self-organization refers to the ability of the components of a complex system to create organized behavior without an internal or external controller.
- Future warfare resources could self-organize given adaptable BMC2 rules/procedures and the ability to self-form collaborative systems of systems

Characteristics of Complex Systems

Common characteristics of complex systems. To what extent does the future BMC2 system of systems have these characteristics?

- Complex Collective Behavior
- Signaling & Information Processing
- Adaptation
- Design Decisions
- Complex Objectives
- Complex Operational Environment
- System Changes
- Lateral Influences
- System Risk
- Unforeseen Emergent Properties

Complex Collective Behavior

The collective action of the large numbers of components gives rise to the complex, hard-to-predict, changing patterns of behavior

The overall behavior of collaborative warfare resources would change in response to the complex operational environment and hard-to-predict in terms of which action might be taken by each individual element

Signaling & Information Processing

Complex systems produce and use information and signals from their internal and external environments

Information production, sharing, and usage is key for collaborative BMC2. Types of information include: sensor data, environmental data, intelligence, health & status information

Adaptation

Complex systems adapt—they change their behavior to improve their changes of survival or success through learning or evolutionary processes

Adapting to a constantly changing operational environment

- Future warfare threat environments will be complex and constantly changing.
- Additionally, the SoS itself will be constantly changing as its systems join and leave the SoS; as systems move; and as warfare resources change in time
- Therefore, the future BMC2 SoS will constantly find itself in unique and changing circumstances.
- Future BMC2 SoS behavior is adaptive as it responds to the threat environment and seeks to best utilize all of its warfare resource elements.

Characteristics of Future BMC2 Adaptation

- Adaptation can occur at system-level and force-level.
- Adaptation takes the form of changes to rules of operation/engagement, etc., doctrine, TTP's
- Adaptation can also take the form of the creation of new SoS's; acquiring additional systems into the SoS; dropping systems from a SoS

Design Decisions

For complex systems, a significantly large number of decisions have to be made regarding design, and typically the implications of design decisions are less predictable

Future BMC2 is based on a multitude of design decisions:

- micro-level (for each warfare resource)
- element level (integrating multiple warfare resources on platforms)
- the macro level (designing the system of systems architecture and force-level decision process)

Examples: common processing software, communications, decision process that governs resource allocation, interactions, and responses to the threat environment

The outcome of the future BMC2 system is the response of the warfare resources to the operational mission. Based on the design complexity and the complexity of the operational environment, this outcome is necessarily unpredictable, unique, and changing in time.

Complex Objectives

Complex systems have a large number of objectives and the objectives are generally inconsistent or changing.

Mission objectives include:

- Meeting the operational needs of different warfare areas based on threat present (i.e., air and missile defense, surface warfare, subsurface warfare, cruise missiles, asymmetric warfare, special operations, etc.)
- Addressing a set of objectives that are changing in time (priorities among threat change as combat environment unfolds)
- Meeting the operational objectives of individual platforms as well as those at the force-level

Conflicting objectives can arise from either of these types of mission objectives

Complex Operational Environment

Complex systems exist to operate in complex operational environments. The complexity of the operational environment may be a result of adverse environments, widely varying environments, or environments that cause challenging missions.

The operational environment for future BMC2 operations is envisioned to be highly complex and could include a combination of multiple and fast-moving air, missile, land, and space-based threats.

The threat may be sequential or simultaneous and may come from various directions

Threats may include unmanned vehicles, swarms of manned or unmanned vehicles, asymmetric attacks, or unconventional attacks disguised as a non-threat

Complexity in BMC2 Operations

Ultimately, every moment in the operational life of the BMC2 system will be unique.

All aspects are changing:

- Threats
- Participating warfare resources/units
- Status/health/capabilities of warfare resources
- Locations of units, threats, etc.
- Threat/mission priorities
- Rules governing resources and actions

System Changes

For complex systems, change at any level may have system-wide impacts and small causes may have large effects.

Changes include: inputs to the system; changes in the health or status of warfare resources, or the addition or deletion of participating warfare resources to a system of systems.

Inputs include: operational environment data (sensor data, intel, weather/maps, weapon loads and status, health and status of warfare resources, etc.), changes in operating rules (TTPs, rules of engagement, decision rules, etc.), and operator input

System-wide impacts; or force-level emergent capabilities include: identification of new threats, changes to tasking priorities, selection of best shooter, etc.)

Therefore, system changes and changes to inputs can impact the force-level emergent capabilities of the envisioned future BMC2 SoS

Lateral Influences

In complex systems, lateral influences are stronger and more dominant that hierarchical influences

- Empowering individual warfare units (systems) as intelligent agents with the force-level BMC2 capability (to arrive at force-optimized tasking for warfare resources) creates an emphasis on lateral influences over vertical

"In its highest state, shared context and understanding is implicit and intuitive between hierarchical and lateral echelons of command, enabling decentralized and distributed formations to perform as if they were centrally coordinated. When achieved, **these practices result in decentralized formal decision-making throughout the force**, leading implicitly to the opportunity to gain advantageous operational tempo over adversaries."

"Decentralization will occur beyond current comfort levels and habits of practice."

- Quotes from CJCS Paper on Joint Force 2020 (April 2012)

System Risk

In complex systems, risk is dominated by system-level risks, rather than lower level risks in achieving the contributing parts.

For the future BMC2, the risk shifts from individual warfare resources operating independently, to the collaborative system of systems.

Lower level risks, such as whether an individual warfare asset will function properly become less of an issue as the number of participating warfare resources participate

The risk shifts to system-level concerns, such as:

- whether information is being communicated properly
- whether situational awareness is shared and accurate
- whether the force-level decision process for tasking resources is behaving properly

Unforeseen Emergent Properties

Complex systems exhibit unforeseen or hard-to-predict emergent properties.

If such properties are truly unforeseen, then it remains to be seen whether the future BMC2 system of systems will behave in unpredictable ways

Since weapon systems are involved, it is imperative that modeling and testing occur to investigate unforeseen emergent properties

BMC2 Complexity Principles

Principles that Apply to Complex Systems

- System Holism Principle
- Darkness Principle
- 80-20 Principle
- Law of Requisite Variety
- Redundancy of Resources Principle
- Sub-optimization Principle
- Relaxation Time Principle
- Redundancy of Potential Command Principle

System Holism

A system has holistic properties not manifested by any of its parts and their interactions: vertical emergence. System holism widely known as "the whole is greater than the sum of its parts"

- Holistic properties of future BMC2 systems: force-level capabilities made possible through the collaborative interactions of their parts

- Examples: enhanced and shared situational awareness, distributed sensor and weapon management for force-level needs; integrated fire control

Darkness Principle

The darkness principle in complexity is the concept of ***incompressibility****: no system can be known completely. The darkness principle implies that members of a complex system do not have knowledge of the system as a whole: they will always be in the shadow of the whole.*

"Each element in the system is ignorant of the behavior of the system as a whole, it responds only to information that is available to it locally. This point is vitally important. If each element "knew" what was happening to the system as a whole, all of the complexity would have to be present in that element."

For future BMC2 with the existence of common processing resident in each warfare element and shared information, each element of the complex system gains a complete understanding of the whole system. This implies that the system complexity is present in each element. Thus, the darkness principle does not apply in the decentralized BMC2 architecture envisioned.

80-20 Principle

According to the 80-20 principle, in any large complex system, 80% of the output will be produced by only 20% of the system.

This principle can be evaluated in terms of future BMC2 in two different ways:

(1) The point of collaborative BMC2 is to best coordinate distributed warfare assets. So, the output of the system—the decisions or commands to task resources (or launch weapons) will reduce the number of tasked resources to a smaller fraction. As an example, the optimum weapon can be selected to engage a target; rather than each weapon system independently defending against a threat.

(2) On the other hand, for the envisioned BMC2 system, each node in the network is performing identical processing to develop the force-level tasking of the warfare resources. So, from this perspective, the decision outputs are being generated at each participating common node. So, from this perspective, 100% of the output is produced by 100% of the system. Thus, a significant amount of redundancy is designed into the decentralized architecture that is envisioned.

Law of Requisite Variety

- *"Control can only be obtained if the variety of the controller is at least as great as the variety of the situation to be controlled.*
- *A variation: "…every good regulator of a system must contain a complete representation of that system."*

The future BMC2 system complies with this complexity principle. With common processors, each warfare element attains information superiority through the common operational picture which contains shared situational awareness, health and status information of the warfare resources, and identical rule sets. So, each warfare element is empowered with the variety of the situation and therefore has the ability to "control" (or arrive at the optimum resource tasking solution) warfare assets at the force-level.

Redundancy of Resources Principle

Maintenance of stability under conditions of disturbance requires redundancy of critical resources

System stability is a concern for the future BMC2 system. Disturbances include:

- an overload of information or data
- false or corrupt data
- outages/communication failures
- a threat environment so complex that the number of resource tasks overloads the decision prioritization process
- delays that could slow the tasking process down to the point where the reaction time is not met

System redundancy that could address these types of disturbances include :

- redundant links (communication paths)
- the redundancy of the common processors at each element
- the ability to synchronize information among elements

Sub-optimization Principle

If each subsystem, regarded separately, is made to operate with maximum efficiency, the system as a whole will not operate with utmost efficiency. And the reverse: if the whole is made to operate with maximum efficiency, the comprising subsystems will not operate with upmost efficiency. Another way to think about this: parts in isolation behave differently from parts that are connected to a system and/or an environment

The sub-optimization principle readily applies to the BMC2 system. If individual warfare platforms are considered subsystems, then it is easy to imagine that if the platforms are each operating as they would in isolation; then given threats in the environment, each would fire weapons to engage the targets.

Examining the reverse implies that if the system is made to operate at maximum efficiency at the force-level, then the warfare platforms will not be operating at maximum efficiency. This situation would be the intent; since fewer weapons would have to be fired and sensors could share in the creation of the common operational picture.

Relaxation Time Principle

System stability is possible only if the system's relaxation time is shorter than the mean time between disturbances

Application of this principle to the future BMC2 system is critical to the success and stability of the system:

- the speed of communications, processing, decision-making, synchronizations, and generation of resource tasking.
- the tempo of the "disturbances" on threats must be understood: the speed, location, and numbers of threats and the resulting system reaction times necessary to address the threats.
- the correlation between the system tempo and the threat tempo—ensuring there is a built-in time for "relaxation" or processing necessary to stabilize in between

Redundancy of Potential Command

In any complex decision network, the potential to act effectively is conferred by an adequate concatenation of information. This means that to "control" a complex system we must at first have a sufficiently good representation of it.

The future BMC2 system of systems upholds this principle. One of the major outcomes is shared situational awareness among the distributed warfare nodes. This constitutes the adequate concatenation of information or self-knowledge of the operational environment and the system itself.

CSE Applications for BMC2

Designing Complex Man-Made Systems

"Many engineering applications, such as real-time decision support, communications and control, are reaching the point where classical methods are no longer feasible for reasons of system interdependencies and complexity." [Bar-Yam, 2004]

"As systems become increasingly large and must seamlessly interoperate with other systems in ways that were never envisioned, system engineers are bumping into the limits of the tenets, principles, and practices traditionally used in systems engineering." [Brian White, 2001]

CSE does not "…primarily seek to produce predictable, stable behavior within carefully constrained situations, but rather to obtain systems capable of adaptation, change, and novelty—even surprise!" [Braha, Minai, and Bar-Yam, 2006]

Complex Systems Engineering

- Why is there a need for Complex Systems Engineering?
- TSE = Traditional Systems Engineering
- CSE = Complex Systems Engineering

Traditional System	Complex System
Hierarchical Relationships dominate lateral influences	Lateral influences dominate hierarchical relationships
Cause and effect are relatively obvious and direct	Cause and effect are not obvious and direct; Small causes can have large effects
The implications of design decisions are relatively predictable	The implications of design decisions are much less predictable
Risks are dominated by the local risks in achieving the contributing parts	Risks are dominated by system risks, with unforeseen emergent properties
Influences on, and implications of, decisions tend to follow the local partitioning of the solution elements	Influences on, and implications of, decisions are much more difficult to bound and to establish

CSE Methods

How can we deal with complexity in a predictable way?

1. Identify when a system and/or its solution is complex
2. Determine level of complexity (or relative complexity)
3. Determine when enough SE has been done; and when level of confidence in design (and predictable behavior) is acceptable [Calvano, 2004]

Adopt an evolutionary paradigm for CSE that involves rapid parallel exploration and a context designed to promote change through competition between design/implementation groups with field testing of multiple variants. [Bar-Yam, 2003]

1. Design the environment and processes by which the system is going to be created (not designing the system itself).
2. Design components of the system for the system as a whole.
3. Design a set of rules about how components engage with one another and the process of change.

[White, 2001]

"Highly integrated systems exhibit more complex interactions across the system than earlier, simpler systems. In the highly integrated system, the designer must consider effects on all parts of the system. We are therefore engineering at the systems level more fundamentally than ever; as opposed to introducing subsystems into an evolved, well-precedented system structure." [Calvano, 2004]

CSE Considerations

- Design until an acceptable degree of confidence is met
- Attempt to deal with complexity in a predictable way
- Engineer at the system level—gain an understanding of the whole and emphasize lateral interactions rather than hierarchical
- Adopt an Evolutionary Paradigm with rapid parallel exploration and competition between design/implementation groups to test multiple variants
- Utilize best practices from TSE and CSE:

"[Traditional] systems engineering and complex system engineering live together. Treating them separately doesn't make any sense. CSE builds on the capabilities of TSE but has its own unique perspective of focusing on the system environment." [White, 2001]

Should CSE methods be considered for future BMC2?

- The complexity characteristics of future BMC2 pose serious challenges that may exceed the limits of TSE
- Complexity in the objectives results in a BMC2 system of systems that is hard to bound
- Generating a well-defined set of mission objectives and system requirements is very challenging
- There is much complexity involved in design decisions (large scope and unpredictability of design decision outcomes)

Taking Advantage of Complexity

In addition to trying to cope with the scope and complexity of the future BMC2 system, engineering strategies must also strive to ensure designs take advantage of the benefits that complexity offers.

- Designs should not limit features such as redundancy, sub-optimization, and the 80-20 principle

- These may seem wasteful, inefficient, and costly; but they may be the key to the stability and response times necessary to function in a complex environment

- Benefits also include adaptation, self-organization, and agility

Conclusions

- Future BMC2 has many characteristics of complexity and follows many principles of system complexity
- The system engineering of future BMC2 should adopt a mix of CSE and TSE methods
- SE approaches adopted should not limit or constrain the benefits of the complex nature of the future BMC2 system

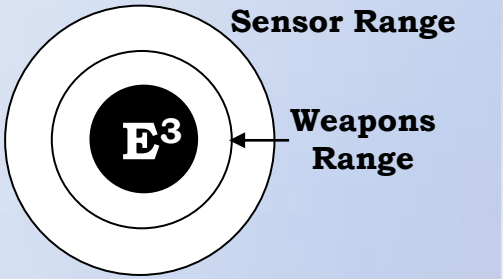
Future Explorations

- Understand and quantify the BMC2 system tempo, the threat environment tempo, and analyze and compare the tempos to identify disconnects
- Determine what a sufficient level of systems engineering completeness would be – develop a strategy to determine when the level of confidence in the design is acceptable
- Study the 80/20 principle as it applies to BMC2. What percentage of the system output will be produced by what percentage of the system?
- Predict and understand emergent properties
- Study the overall system stability against “disturbances” – is there enough redundancy and sub-optimization to compensate for disturbances?
- Study what sufficiency in representation (situational awareness) is required to support action (resource tasking).

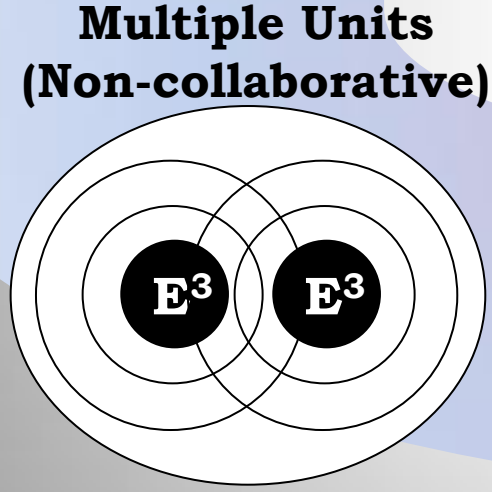
In conclusion, the potential complex threat environment of the future and the mission need to provide defensive measures and tactical responses have created a need for a future BMC2 system that can perform complex tasks. And, only a complex BMC2 system can perform complex BMC2 tasks!

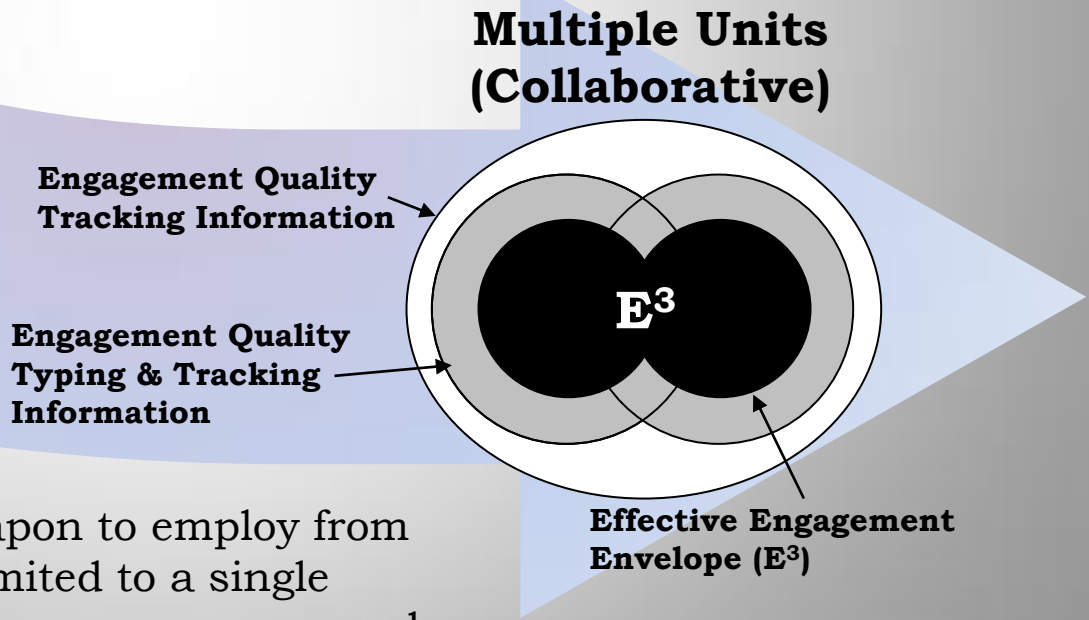
Back-Ups

Improved Engagements



The "effective engagement envelope" will greatly expand as the shift takes place from a single warfighting unit using only local sensor and weapon resources to a system of collaborating warfighting units. The shared sensor data will enhance situational awareness; thereby extending the detection envelope and improving the reaction time of weapons deployment—which will extend the effective range of engagements.





The ability to select the optimum weapon to employ from across the force (rather than being limited to a single unit) will improve the economy of weapons resources and the probability of effective engagements.

Future BMC2 Information Architecture

Characteristics:

- High bandwidth, Secure, Reliable
- Timely sharing of data and information among units
- Adaptable to accept or drop units
- Employ authentication measures to ensure authoritative data sources

Information Architecture Capabilities

Objectives for Information Sharing:
Based on Force-centric de-centralized architecture
• Allows warfare resources to be managed according to Force-level needs (rather than unit-centric needs)
• Manages network to enable special data distribution needs during engagements. (higher data rate or throughput)

Information Dissemination Capabilities:
• Determines needs of information-recipient users or decision nodes (data advertisements/ subscriptions)
• Tracks data availability
• Establishes routing paths & maintains connectivity
• Optimizes bandwidth usage
• Determines feasibility of transmission/checks link status
• Sends and receives commands to/from remote link managers to control, manage, & synchronize transmission
• Transmits data/information according to local/remote synchronized commands

Information Exchange Required:
• Associated Measurement Reports
• Resource information: HSCC
• C2 Datasets (Doctrine, TTPs, plans, manual commands)
• Resource Tasking Requests
• Resource Commitment "Handshakes"

Data Exchange Characteristics:
• Supports real-time exchange of sensor measurement data
• Broadcast/Multicast/Point-to-Point
• Non-real-time traffic for operations control
• Link monitoring
• Quality of Service delivery
• Data integrity and confidentiality
• Bandwidth allocation/monitoring
• Data dissemination prioritization (for time-sensitive data or bandwidth constraints)
• Ad hoc nodal topology (nodes can easily join or leave network)
•Interfaces with Tactical Data Links (TDLs)

Shared SA Data Processing & Fusion

Shared SA relies on:
Data processing and data fusion algorithms to assess and develop a representation of the real situation

Situation Assessment Capabilities

Tracking & Combat ID
- Pixel/Signal-level association
- Object kinematics
- Object characterization
- Object kinematics prediction

Object Context Assessment
- Estimate object relations
- Refine object ID & typing based on group behavior
- Provide physical context for track picture
- Discrimination, kill assessment
- Maintain defended assets picture

Environment Assessment
- Develop & maintain environmental picture (weather, mapping, jamming, etc.) for Area of Interest (AOI)

C2 Situation Assessment
Assessment & Adoption of Blue Force BMC2 inputs
- Ensure peer promulgation of commands
- Translate BMC2 inputs into system operating rules, constraints, & parameters

Processing Evaluation
- Assessment of processing performance
- Unit health & status assessment

Warfighting Resource Assessment
Assessment of sensors, weapons, & warfighting units
- Health & status assessment
- Configuration & capability maintenance

Threat Evaluation
- Identify, evaluate, & prioritize threats

SA Certification
- Assessment of track quality
- Assessment of track ID confidence
- Certification of fire control quality SA

Force Readiness Assessment
Fusion of assessments
- Determination of overall readiness of warfighting forces

SoSE

A need exists for new approaches for engineering SoS's because of:

(1) An exponential rise in the demand, accessibility and proliferation of information
(2) Increasing requirements for interdependence between systems that have previously been conceived, developed, and deployed as independently functioning systems
(3) Demands for engineering solutions willing to trade completeness for accelerated deployment
(4) Holistic solutions that exist beyond technical resolution

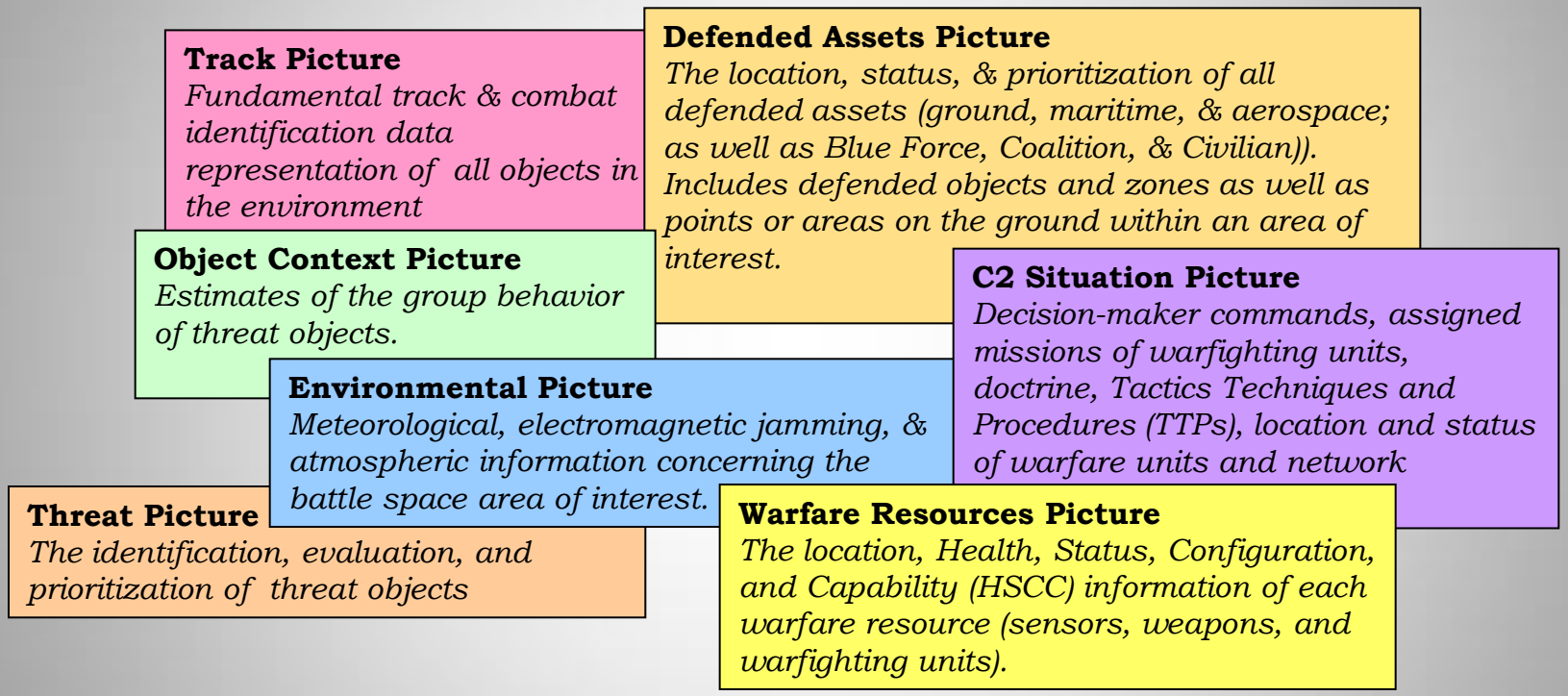
Methodology vs. Process

There are 6 primary conditions that suggest a methodology may be preferable to traditional SE approaches (processes) for SoS's:

1. **Turbulent Environmental Conditions** (environment is highly dynamic, uncertain, rapidly changing)
2. **Ill-defined Problem Conditions** (in dispute, not readily accessible, or lack of consensus)
3. **Contextual Dominance** (the technical "hard" aspects are overshadowed by the contextual "soft" (circumstances, conditions, factors) aspects)
4. **Uncertain Approach** (path of how "best" to proceed is indeterminate)
5. **Ambiguous Expectations and Objectives** (inability to establish measure of success or system objectives)
6. **Excessive Complexity** (system boundaries are expansive such that the level of complexity is beyond the capabilities of traditional SE approaches)

Shared Situation Awareness

… is key because each unit needs identical, complete, accurate, & timely awareness (knowledge) of the operational situation.



Shared Situation Awareness (SA) is the ability of distributed units (systems) to gain an understanding of the totality of the operational environment including the tactical situation, the threat, the defended assets, the readiness of warfighting resources, and command and control constraints within which the systems must operate.

Distributed Resource Management...

... is key to enabling and optimizing the use of distributed resources for collaborative BMC2 and integrated fire control

Distributed Resource Management

Engagement support strategy after launch
- Forward pass (preferred eng control option)
- Remote guidance relay (preferred sensor arrangement)
- Remote target illumination (preferred sensor support)

Selective engagement
- Selection of best option if multiple engagement options along the threat trajectory exist

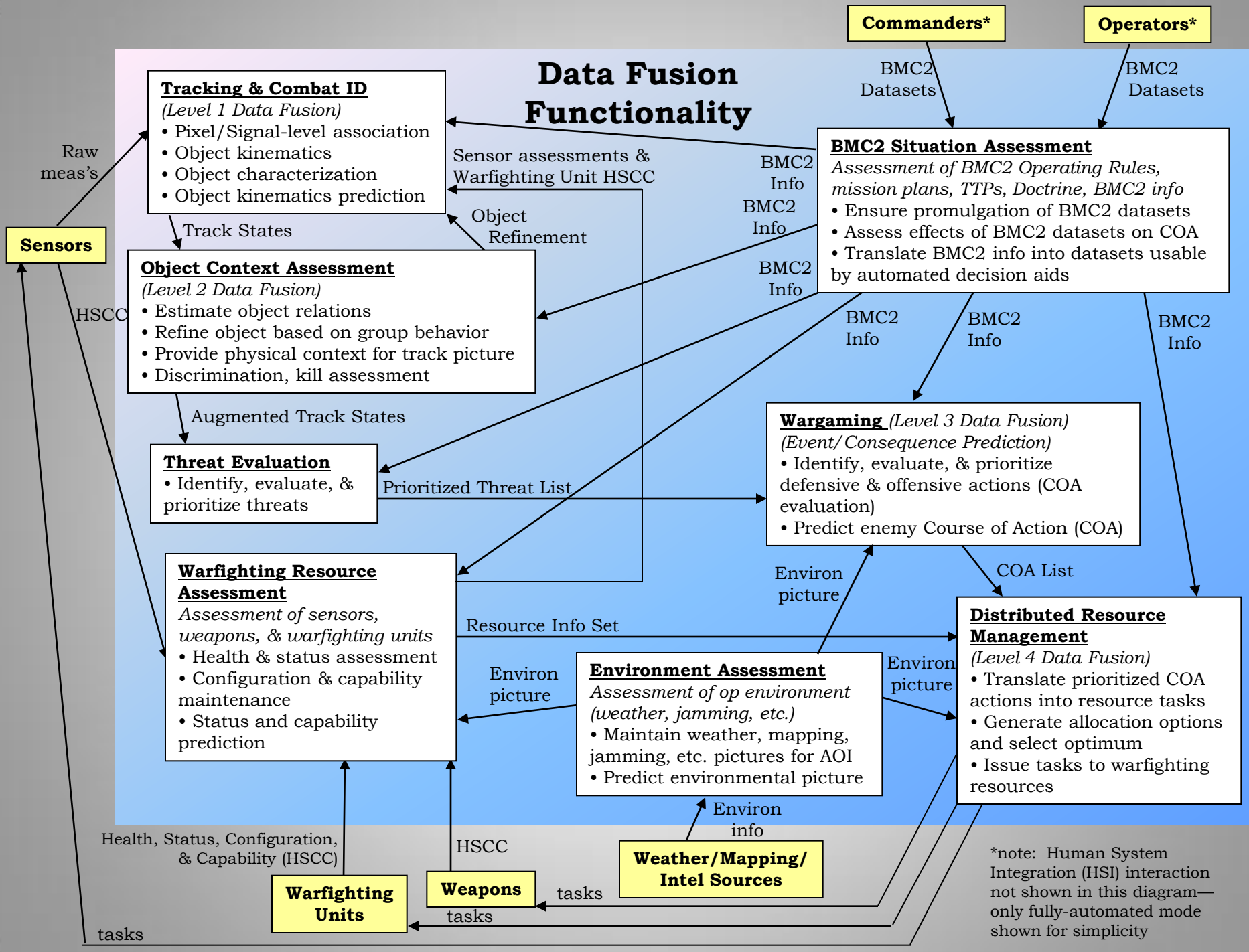
Launch determination
- Receive threat determination
- Assess engageability of weapon options
- Determine intercept probability
- Decide to launch (or not)

Engagement support strategies
- Threat detection/cue
- Fire Control Quality data availability
- Sensor tasking/commitment
- Preferred sensor arrangement

Weapon-target pairing
- Preferred shooter determination
- Engageability of weapon options

- Based on the use of automated decision aids to determine and recommend optimum uses of warfare resources
- Using identical automated decision aids on distributed units enables decisions to be made in a timely manner to support time-critical engagement operations.
- Each distributed unit uses distributed resource management (DRM) to determine tasks for all resources within the operational environment
- Resident operators can override resource tasking recommendations for local resources; thus command authority is upheld.

Data Fusion Functionality



Knowledge & Decision Products

Example Products of Data Fusion Process:

- Preferred shooter determination
- Weapon-Target Pairing
- Sensor Support for Engagements
- Engagement Control Strategy (i.e., forward pass)
- Engagement Preferences (intercept geometry)
- Sensor tasking to support better situational awareness
- Unit tasking to reposition warfare units
- Identification of gaps in defense and recommendations to close gaps
- Threat identifications and prioritizations
- Awareness of SoS warfare resources: health, status, configuration, and configuration (HSCC)
- Situational awareness – object identification and characterization, map overlays, weather overlays, etc.

Example: each distributed unit uses "common" algorithms to produce identical Force-level engagement recommendations. Therefore, each unit arrives at the same conclusion that a particular weapon has the best shot and that a particular sensor (not necessarily collocated with the weapon) can best track and/or illuminate the target.

Situation Prediction Capability

… is key for determining that a threat requires defensive measures—taking into account possible ramifications (Effects Based Operations)

Situation Prediction Functionality

Environment Prediction
- Predict weather for AOI
- Predict possible jamming/clutter

Resource Projection
Prediction of sensors, weapons, & unit performance
- Availability & capability prediction

Wargaming – Event/Consequence Prediction
Prediction of sensors, weapons, & unit performance
- Predict threat
- Predict & evaluate enemy COA & intent
- Identify, evaluate & prioritize blue force COA
- Evaluate effects of C2 inputs on blue force COA
- Analyze historical trends

Force Projection
Prediction of Force Readiness
- Prediction of overall force readiness & capabilities

- Projects the current situation into the future to estimate the enemy Course of Action (COA) and potential impact of the blue force's planned actions.
- Develops and assesses alternative futures or hypotheses concerning the current situation and possible COAs.
- Assigns quantitative confidence values to potential COAs
- Enables collaborative planning, effective resource management, and dynamic replanning

Warfare Planning Capability

… is key to predicting operational situations that require defensive measures (such as collaborative fire control)

Built-in planning prior to operations is a key enabler of Distributed Resource Management:

- Establishing prioritization schemes for missions, threats, defended areas, weapons, tactics
- Establishing rule sets to guide resource behavior for tactical and strategic operations
- Establishing parameters to control engageability calculations, target-weapon pairing, target identification/threat evaluation, & sensor tasking
- Establishing decision logic

Deliberate Planning is the predetermination of resource utilization

Defense Planning - "Macro" Planning

- Assigning resources to missions
- Allocating areas/zones within theater
- CINC priorities
- Identifying critical assets

Defense Design – "Micro" Planning

- Specific TTPs
- Rule sets
- Initialization parameters
- Correlation Track Quality Values

Dynamic Planning is the modification of plans during operations

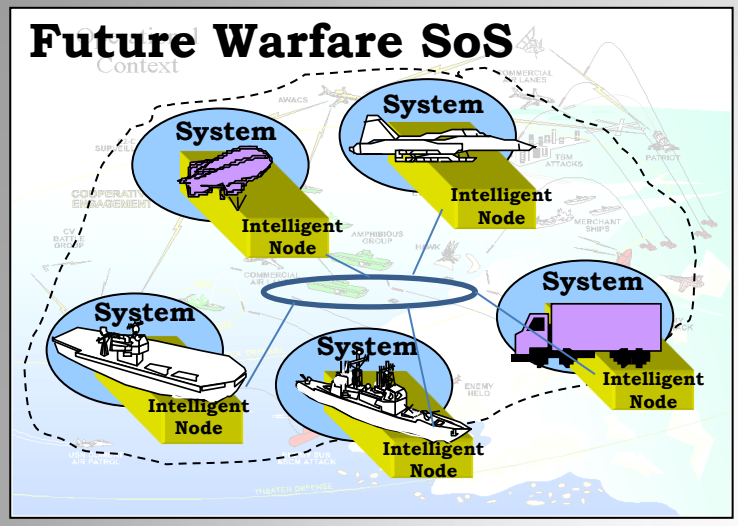
Dynamic Planning Functions:

- Replanning – dynamic creation of new plan
- Refinement of plan
- Reassignment of resources
- Ad hoc operations
- Alteration of rule sets
- Reset of parameters
- Reestablishing prioritization

Why Dynamic Planning is Useful:

- Plan implementation needs to reflect reality
- Resources change (things break, resources become unavailable)
- Enemy prediction never 100% accurate (unexpected events, enemy COAs, & threats)

SoS Design Characteristics



- Each constituent system can operate independently or as a collaborating member of an SoS
- Individual systems may enter and exit SoS's
- Multiple SoS's may exist
- Multiple warfare mission areas can be addressed by single or multiple SoS's
- Constituent systems have the ability to "self-organize"

- Each constituent system is "intelligent": has a replicated (identical or shared) situational awareness and arrives at replicated decisions for BMC2
- Lateral influences dominate vertical (hierarchical) influences
- SoS adaptation is possible, encouraged, and necessary
- SoS must be robust (resilient to external forces)
- Emergent capabilities are projected to include the force-level optimization of the use of the assets and enhanced situational awareness across the force
- SoS must maintain a strong self-identity

Independent Operation of Constituent Systems

- Each constituent system can operate independently or as a collaborating member of an SoS
  - Each system is empowered as an intelligent agent and is fully-equipped to operate independently as operationally necessary
- Individual systems may enter and exit a SoS
  - Examples: Mobile systems (aircraft, ships, etc.) may move into (or out of) the range of an SoS; system degradation or destruction may result in a system exiting an SoS
  - Systems need to get caught up to speed upon entering a SoS (data/information download and synchronization)
  - SoS must acknowledge systems that join – "handshake"
  - Systems must provide information concerning their warfare resources and SA knowledge to SoS upon entering
- Constituent systems have the ability to "self-organize"
  - Each system, empowered as an intelligent agent, can form a SoS with other systems as the operational mission/environment require

SoS Robustness

- Future warfare SoS's must be robust (resilient to external forces)
- Robustness refers to resilience to changes in understanding, interpretation, and context
- Perturbation for SoS is inevitable, may not be known beforehand, and emergent patterns/properties may develop in response

- Methods of achieving SoS robustness through design:
  - Knowledge of operational environment (SA)
  - Internal SoS monitoring
  - Design flexibility to respond to anticipated SoS deviations
  - Feedback to adjust over the mission performance of the SoS

SoS Communications

Communications, within and external to the SoS, are essential to ensure solution viability in the face of emergence.

"Channels" are proposed as a method for SoS communication:

Operations Channel – direct exchange between SoS subsystems
Coordination Channel – to monitor regulatory mechanisms for SoS standardization
Algedonic Channel – a direct link between subsystems and the SoS level for identification of high level threats
Command Channel – for high-level direction throughout the SoS
Audit or Operational Monitoring Channel – to examine SoS disturbances/health
Environmental Screening Channel – continuous monitoring of trends, patterns, and events in the environment
Resource Bargain-Accountability Channel – negotiation between the SoS and the constituent subsystems concerning resource distribution
Dialog Channel – to support the examination and interpretation of SoS decisions, actions, and events
Learning Channel – the detection and correction of SoS errors
Informing Channel – routine transmission of information throughout the SoS
Identity Channel – to support the exploration of the essence of the SoS – the purpose, mission and character

Context

Context – the circumstances, factors, conditions, and patterns that both enable and constrain a complex system solution; it's deployment; and it's interpretation

- For the future warfare SoS, the context can dominate the solution space (even more so than technical aspects)

- Context is a critical consideration for developing SoS's

- Context considerations for SoS's: technical, operational, human/social, managerial, organizational, policy, political

Multiple Objectives

Pluralism – the characteristic of having multiple purposes and objectives in play at the individual, entity, and enterprise levels.

- Differences in purposes may become sources of conflict at various points in the development of the SoS.
- The assumption that an SoS has a singular set of agreed-upon requirements and shared understandings may be questionable
- This is problematic for SE approaches based on rational-logical assumptions of objective/requirement alignment
- For SoS's, pluralism suggests that different objectives may be pursued in response to patterns and properties that manifest through SoS operation

SoS Requirements Specification

- Due to emergence and adaptation, the system design of an SoS can only be partially specified in advance of system operation

- Overspecification of system-level requirements is:
  (1) wasteful of scarce resources necessary to monitor and control system level performance
  (2) reduces subsystem autonomy, which in turn restricts the agility and responsiveness of the system to compensate for environmental shifts.
  (3) fails to permit subsystem elements to self-organize based on their contextual knowledge, understanding, and proximity to the operating environment.

Boundaries

Boundaries in an SoS are ambiguous, fluid, and negotiable.

- They provide the criteria for what is included and excluded from an SoS
- Boundaries may form around geographic, time, spatial, or conceptual delineations
- SoS boundaries may shift radically; particularly in the early formation of the problem domain; and also during operations
- SoS boundary shifts should be expected and embraced

SoS Self-Identity

- Maintenance of a strong SoS identity is key to SoS viability, robustness, and continued existence
- There may be many decisions, actions, and interpretations necessary for an SoS to function in the face of changing objectives, operational missions, perturbations, etc.
- Thus, a stabilizing force is required that acts as a reference point for consistency in decisions, actions, and interpretations
- A strong SoS self-identity is the driving force that establishes the set of characteristics that is the essence of the SoS

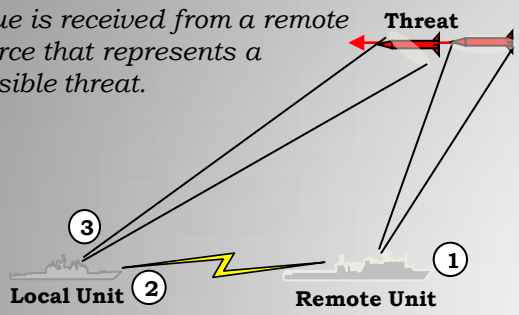
In conclusion, this presentation is intended to raise questions that will lead to further study. Here are some topics of interest:

- Study the application of SoS systems engineering (SoSE) & complex systems engineering (CSE) as methodologies
- Understand and quantify the BMC2 system tempo, the threat environment tempo, and analyze and compare the tempos to identify disconnects
- Determine what a sufficient level of SE completeness would be—develop a strategy to determine when the level of confidence in the design is acceptable
- Study the SoS against disturbances – is there enough redundancy and sub-optimization to compensate for disturbances?
- Understand the interplay between complex SoS's and their context/environments

IFC Variants

Precision Cue

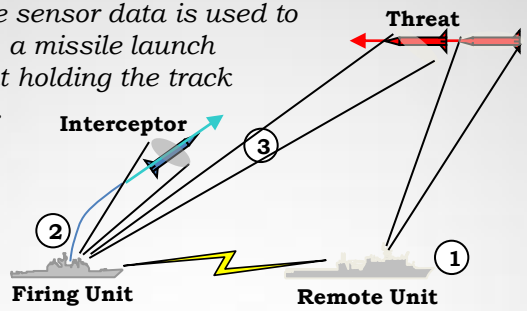
A cue is received from a remote source that represents a possible threat.



1. Remote sensor detects threat.
2. Local unit receives cue.
3. Local unit tasks local sensor to detect and track threat.

Launch on Remote

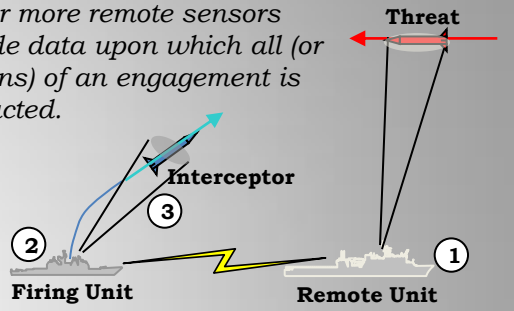
Remote sensor data is used to initiate a missile launch without holding the track locally.



1. Remote unit provides FCQ threat data.
2. Firing ship launches interceptor based on remote threat data.
3. Local unit tasks local sensor to provide FCQ threat data for remainder of post-launch engagement cycle.

Engage on Remote

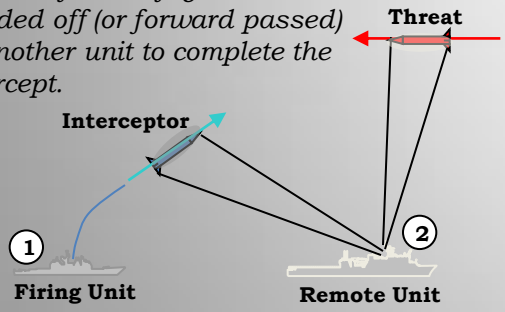
One or more remote sensors provide data upon which all (or portions) of an engagement is conducted.



1. Remote unit provides FCQ threat data.
2. Firing ship launches interceptor based on remote threat data.
3. Remote unit continues to control engagement (compute & provide interceptor guidance, etc.) based on remote data.

Forward Pass

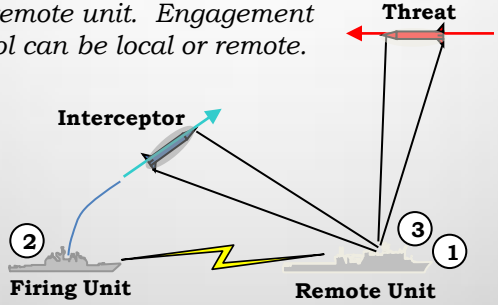
Control of the in-flight missile is handed off (or forward passed) to another unit to complete the intercept.



1. Firing Unit launches interceptor & passes engagement control to Remote Unit
2. Remote Unit takes over engagement control – tracks threat, passes guidance to interceptor, and illuminates threat when necessary

Remote Fire

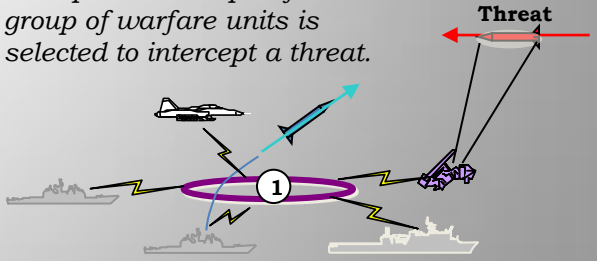
The decision to launch is made by a remote unit. Engagement Control can be local or remote.



1. Remote unit makes decision that firing ship should launch.
2. Firing ship launches interceptor.
3. Remote unit (in this example) controls engagement (threat tracking, interceptor guidance, etc.).

Preferred Shooter Determination

The optimum weapon from a group of warfare units is selected to intercept a threat.



1. The best shooter is selected based on optimum engagement geometry and engageability determination. PSD can be performed in conjunction with any of the other IFC variants. PSD is, in effect, Force-centric weapon-target pairing.