Investigating Alternative Concepts of Operations for a Maritime Security System of Systems

INCOSE 2012

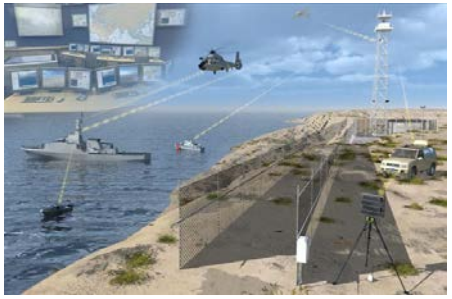
Presented by: Prof. Daniel E. Hastings

Brian Mekdeci
Dr. Donna H. Rhodes
Dr. Adam M. Ross
Prof. Daniel E. Hastings

Maritime Security Systems of Systems

Problem

- Stakeholders want to monitor and protect a particular Area of Interest (AOI)
  - Narrow straight, where a large volume of ships pass through
- Stakeholders want a system that:
  - Detects, identifies boats
  - Intercepts “bad guys”
- Common SoS problems:
  - Diverse, interconnected assets
  - System is subject to various “disturbances”



Constituent systems

- Manned patrol aircraft
- Unmanned aerial vehicles (UAVs)
- Supporting radar towers
- Command Center
- Manned patrol boats

Problem: What will be the “best” system of systems when considering performance, survivability and cost?

© 2012 Massachusetts Institute of Technology

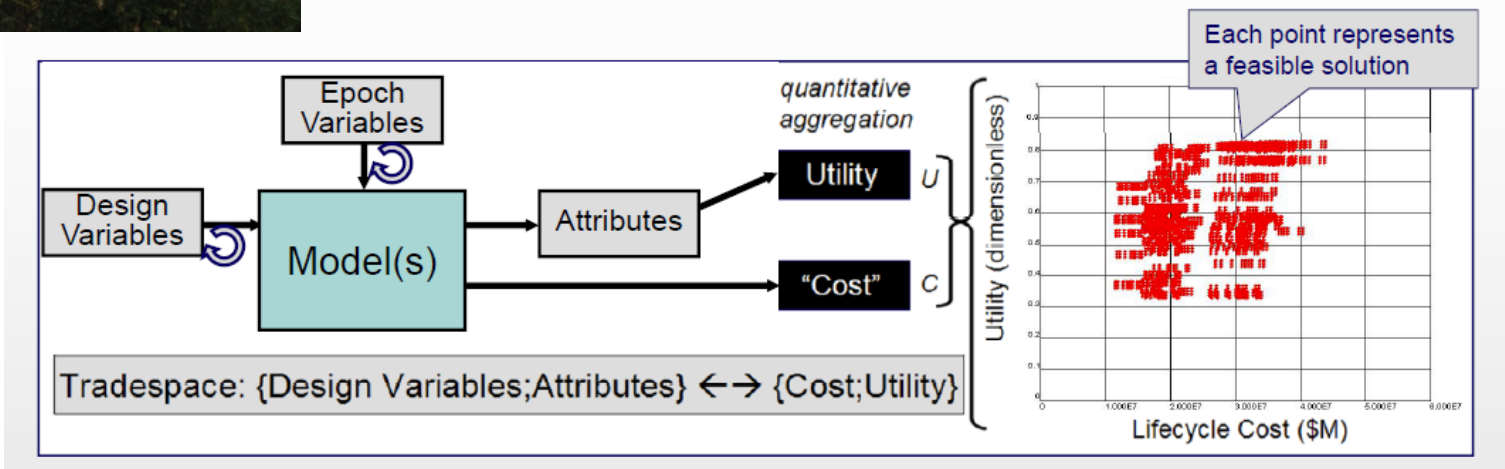
Large-Scale, Time-Critical, Geospatial Systems of Systems

	Taxi Service	Emergency Response (911)	Joint Task Force	Maritime Security
Bounded Area of Interest	Yes (city)	Yes (city)	Yes (battlefield)	Yes (coastal area)
Components	Central dispatch, taxicabs	Central dispatch, police, fire, ambulance	Command center, troops, tanks, artillery, bombers, etc.	Command center, UAVs, patrol boats, etc.
Geographically Separation	Yes	Yes	Yes	Yes
Location-Driven Events	Yes	Yes	Yes	Yes
Context changes	Traffic, weather, city bylaws, fuel prices, major events, etc.	Traffic, weather, city bylaws, fuel prices, major events, etc.	Weather, hostile forces, fuel prices, political events, technology upgrades, etc.	Traffic, weather, city bylaws, fuel prices, major events, politics, technology upgrades etc.
Heterogeneous Systems	No	Yes	Yes	Yes
Authority	Virtual	Collaborative	Acknowledged	Directed

© 2012 Massachusetts Institute of Technology

Design of Complex Systems

- Complex systems are expensive to design, test, build, operate, maintain
  - Important to get design right early in lifecycle
- Tradespace studies are helpful for decision makers to evaluate thousands of potential designs
- Analysis is often biased towards physical design variables
  - Modeling with physics equations highlights physical variables
  - Changing physical design variable is often just parameter changes
    - Changing an operations variable often requires new models, assumptions
  - Enumerated design choices are often determined from the availability



Source: Ross, A.M., McManus, H.L., Rhodes, D.H., Hastings, D.E., and Long, A.M., "Responsive Systems Comparison Method: Dynamic Insights into Designing a Satellite Radar System," AIAA Space 2009, Pasadena, CA, September 2009.

© 2012 Massachusetts Institute of Technology

Operational Variables

- Operational variables are important to consider because
  - They are often faster to implement than form changes
    - Increasing survivability against disturbances
  - They have a significant impact on performance and other “-ilities”
  - May be the only way a decision maker can change a system during it’s lifecycle
    - Form may be fixed after implementation
    - Particularly true for SoS where there are constituent systems
  - Often the less costly way to make changes
    - Physical design options require something physical
      - Materials, transportation, storage, installation, power
  - Strongly correlated with form options
    - Cannot have a CONOPs without form.
    - Having a form that is able to accommodate CONOPs variations is probably a good thing

© 2012 Massachusetts Institute of Technology

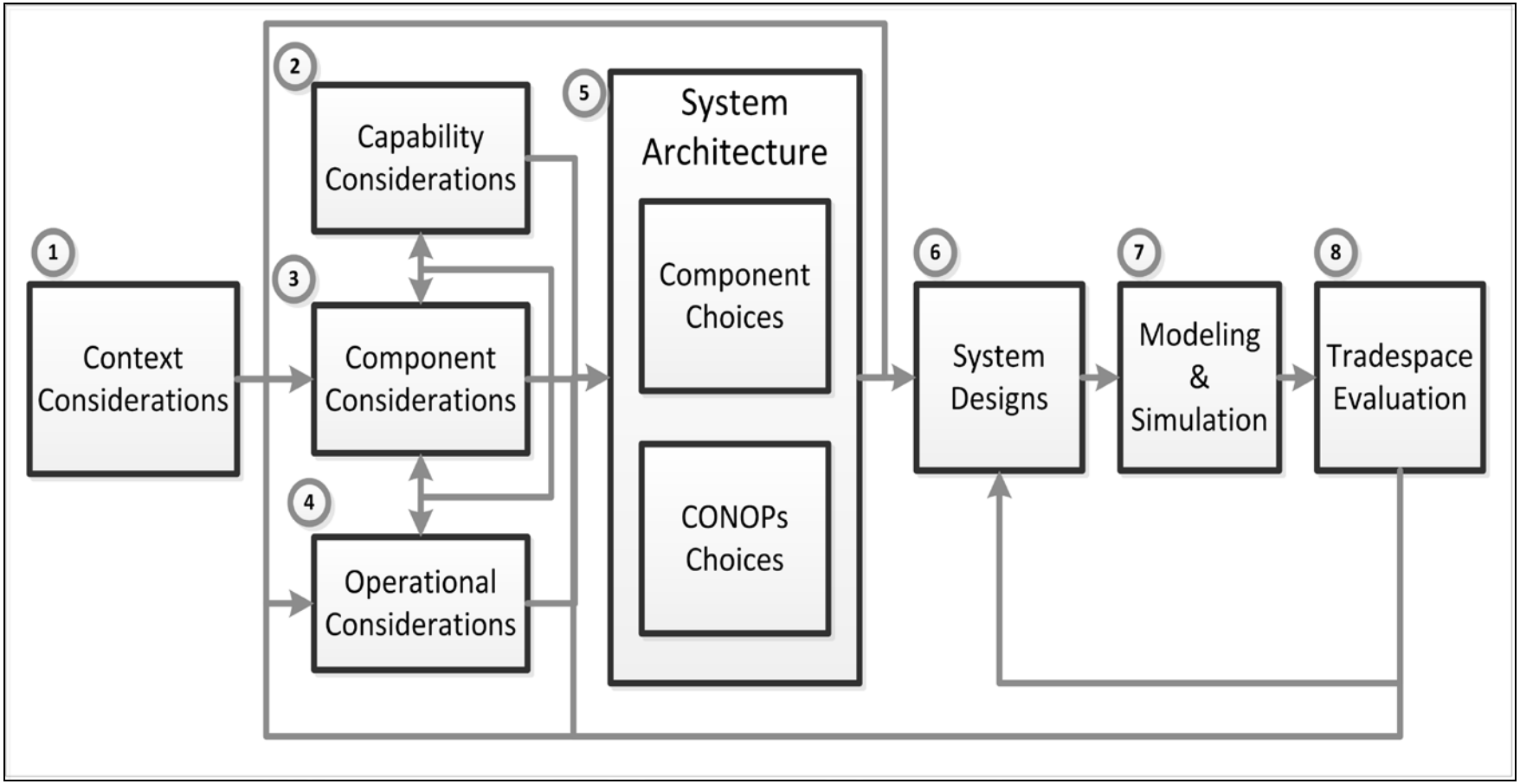
Having a Form That Allows Multiple CONOPs

Some ways in which system architects can increase CONOPs, without changing form

- Margin
  - Having the ability to do more, allows you to do more
  - Examples
    - Physical attributes (lift, power, etc.)
    - Resources (fuel, manpower, etc.)
    - Communication bandwidth
- Implementing a communication interface
  - Even if vehicle is initially designed to operate solo, design it to be able to send / receive communications with other constituent systems

© 2012 Massachusetts Institute of Technology

Steps for Generating Operational Variables



© 2012 Massachusetts Institute of Technology

Context Considerations

- Recognize the relevant exogenous data and constraints that make up the context under which the maritime security system is expected to function
- Maritime Security Example
  - Large Scale AOI
  - Location Dependence
    - Events occur at specific geographical locations
  - Time Criticality
    - Time is of the essence
  - Terrorist Attack
    - Some ships will appear to be civilian, only to change their behavior close to port and act dangerously

© 2012 Massachusetts Institute of Technology

Capability & Component Considerations

Capability Considerations

Determine the high-level capabilities required to satisfy the stakeholder needs.

For maritime security:

- Three main tasks
  - Detection
  - Identification
  - Boarding

Component Considerations

Component that can provide the required capabilities are considered.

- Component selection may be limited by what's available, inherited.

Issues affecting component considerations in maritime security:

- Limited sphere of influence
- Redundant capabilities
- Geographical separation
- Mobile Components

© 2012 Massachusetts Institute of Technology

Operational Considerations

By looking at context, capabilities and components, some operational considerations should be apparent.

Operations is how the components use their capabilities, to satisfy mission objectives, given a particular context.

For maritime security, some operational considerations include

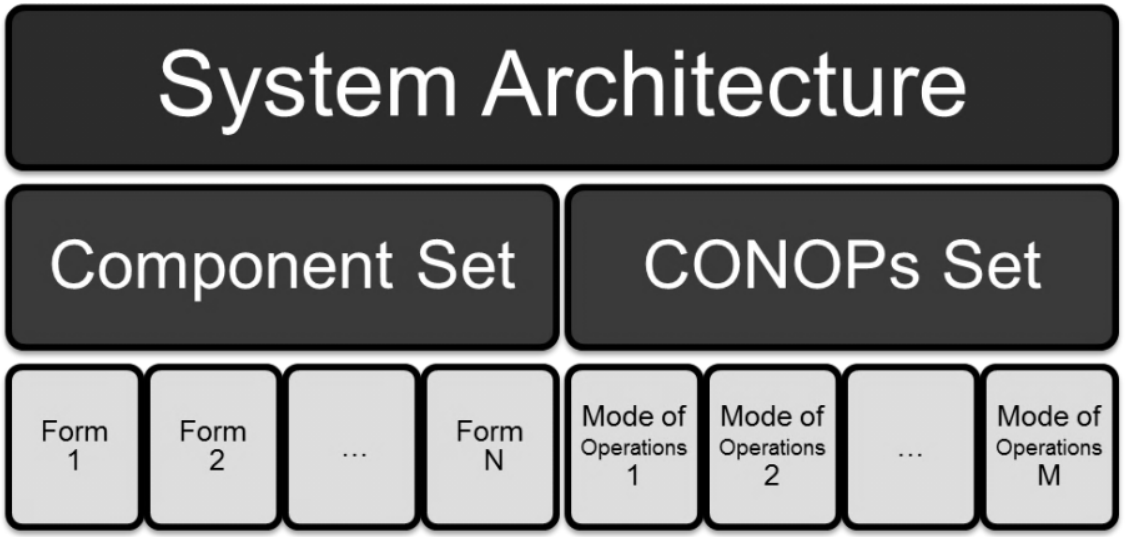
- Queuing
  - Tasks take a finite amount of time and resources.
- Task Sharing
  - Not all tasks can be done by a single component
- Travel
  - Large-scale AOI, time-criticality and limited sphere of influence make travel necessary and problematic
- Vigilance
  - Terrorists may appear to be civilians at first, but change their behavior closer to their target.

© 2012 Massachusetts Institute of Technology

Identifying Choices in System Architecture

System architecture:

The specification of components, their capabilities, organization of components, and concept of operations that determine allowed form, function, and behavior of a system. It describes the mapping of function to form that allows for design variables to be specified. The architecture description includes a set of allowable design instances.



© 2012 Massachusetts Institute of Technology

Identifying Choices in System Architecture

© 2012 Massachusetts Institute of Technology

Example CONOPs Variable 1: Authority

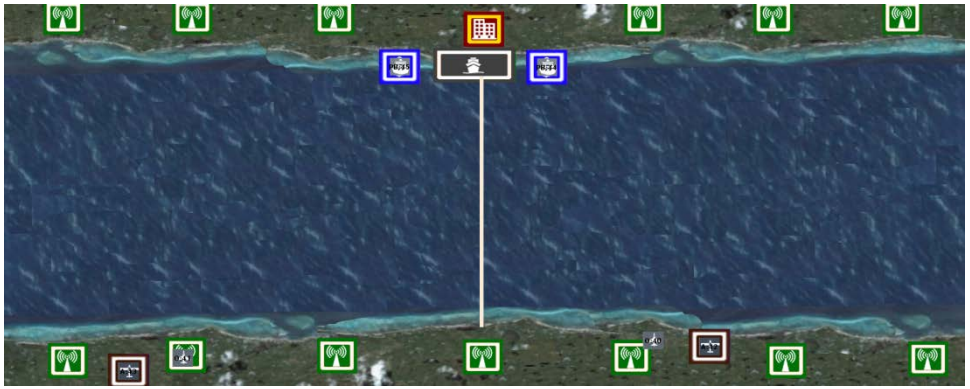
- Common problem with large-scale, geospatial systems of systems is whether to have a central, top-down authority, or a distributed, flat organization.
- Authority issues were one of the major obstacles in the effectiveness of the emergency response to Hurricane Katrina[1]

Pros to central authority

- Reduces maximum number of simultaneous connections
- Simplified operations for constituent systems
  - Less chance of operator / automation error
- Location of central authority fixed
  - Reduces the maximum distance required for communications
- Reduces social loafing

Cons to central authority

- Delays due to queuing
- Constituent systems may not share all information, leading to task allocation errors
- Single point of failure
- Additional constituent systems added at a later date may not recognize central authority



[1]Linda Singer, James Howell, et al. (2005). "A Continuing Storm:The ongoing struggles of Hurricane Katrina evacuees

© 2012 Massachusetts Institute of Technology

Example CONOPs Variable 2: Vigilance

.

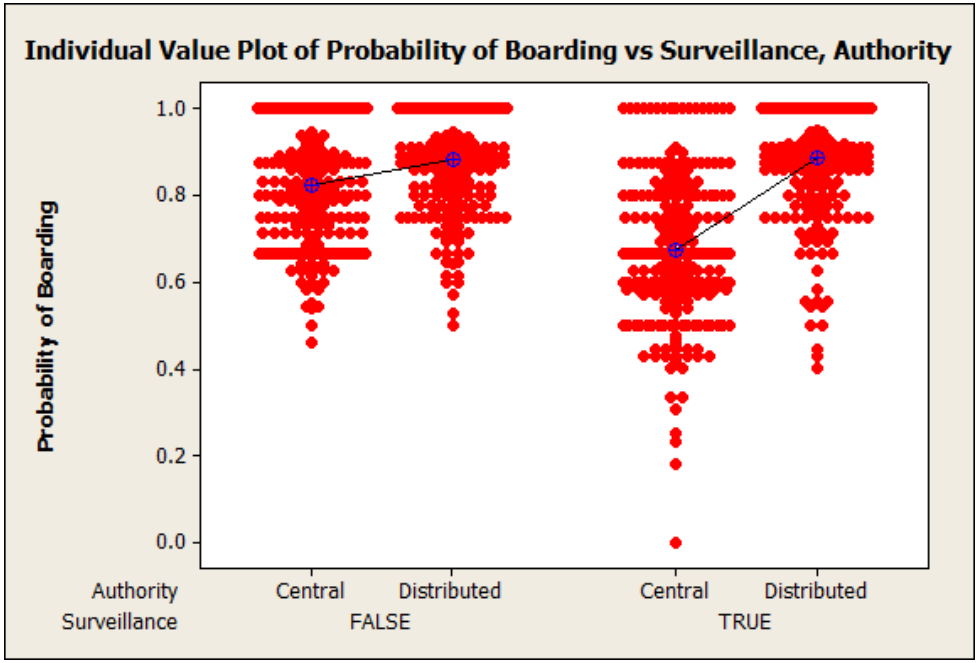
- Pirates/terrorists are indistinguishable from regular fishing vessels until you board them and find weapons, [2] or until they get close to their target.
- Terrorist Modus Operandi:
  - Appear as civilian ship, following maritime rules and regulations
  - Once close to port, increase speed to maximum, ignore all maritime rules, and detonate bomb once in port. (Based on terrorist scenario modeled by NPS study (2005)).

Keeping surveillance on ships that are heading to port, even after they have been identified as “friendly”, is an example of being *vigilant* against sudden changes in context, and may improve survivability by enabling a quicker response.

[2] (http://www.wired.com/dangerroom/2011/08/pirate-fighters-inc/all/1)

© 2012 Massachusetts Institute of Technology

Effects of CONOPs Change



Operational variables do have a significant impact on performance & survivability, but not necessarily how we would expect

Factor	Level	Probability of Boarding
Vigilance	**False**	**85.2%**
	True	77.9%
Authority	Central	74.8%
	Distributed	**88.3%**

Factor	Probability of Bomb Detonation	Difference in Probability of Bomb Detonation	P Value
Vigilance	False – 27.7% True – 24.4%	3.33%	0.270
Authority	Central – 93.3% **Distributed – 10.8%**	**87.5%**	**0.000**

Source	DF	SS	MS	F	P
Vigilance	1	1.2838	1.2837	67.75	0.000
Authority	1	4.3899	4.3899	231.69	0.000
Interaction	1	1.4669	1.4668	77.42	0.000
Error	956	18.1141	0.0189		
Total	959	25.35			

© 2012 Massachusetts Institute of Technology

Discussion

- Vigilance had a significant impact on performance (decreasing it) but no significant improvement in survivability.
  - Terrorist changes activity in high traffic area (port)
    - Behavioral change likely to be detected quickly even without dedicated observer.
    - Limiting factor was resources
      - Add more vehicles (form change)
- Distributed authority was better in both performance and survivability
  - Central authority suffers due to queuing
  - Central authority does not always know exactly what each constituent system is doing

Maritime SoS is a complex system with significant emergent behavior. CONOPS changes are important, but the effects need to be verified before they are approved.

© 2012 Massachusetts Institute of Technology