School of Systems&Enterprises

Architecting Cognitive Seaports for Improved Security and Resilience

Presented at the 2011 DHS Science Conference
5th Annual DHS University Network Summit

Ali Mostashari, Ph.D
Associate Professor, School of Systems and Enterprises
Center for Secure and Resilient Maritime Commerce (CSR)

Cognitive Seaports: Efficiency, Security and Resilience

- The ability of a seaport to maximize its operational efficiency, security and resilience depends on the availability of the right information at the right time for the right stakeholder.
- The multiplicity of stakeholders in a seaport, including terminal operators, federal agencies, state agencies and local law enforcement authorities often results in fragmented information flows that do not allow for a systemic response to natural disasters, malicious attacks or accidents.

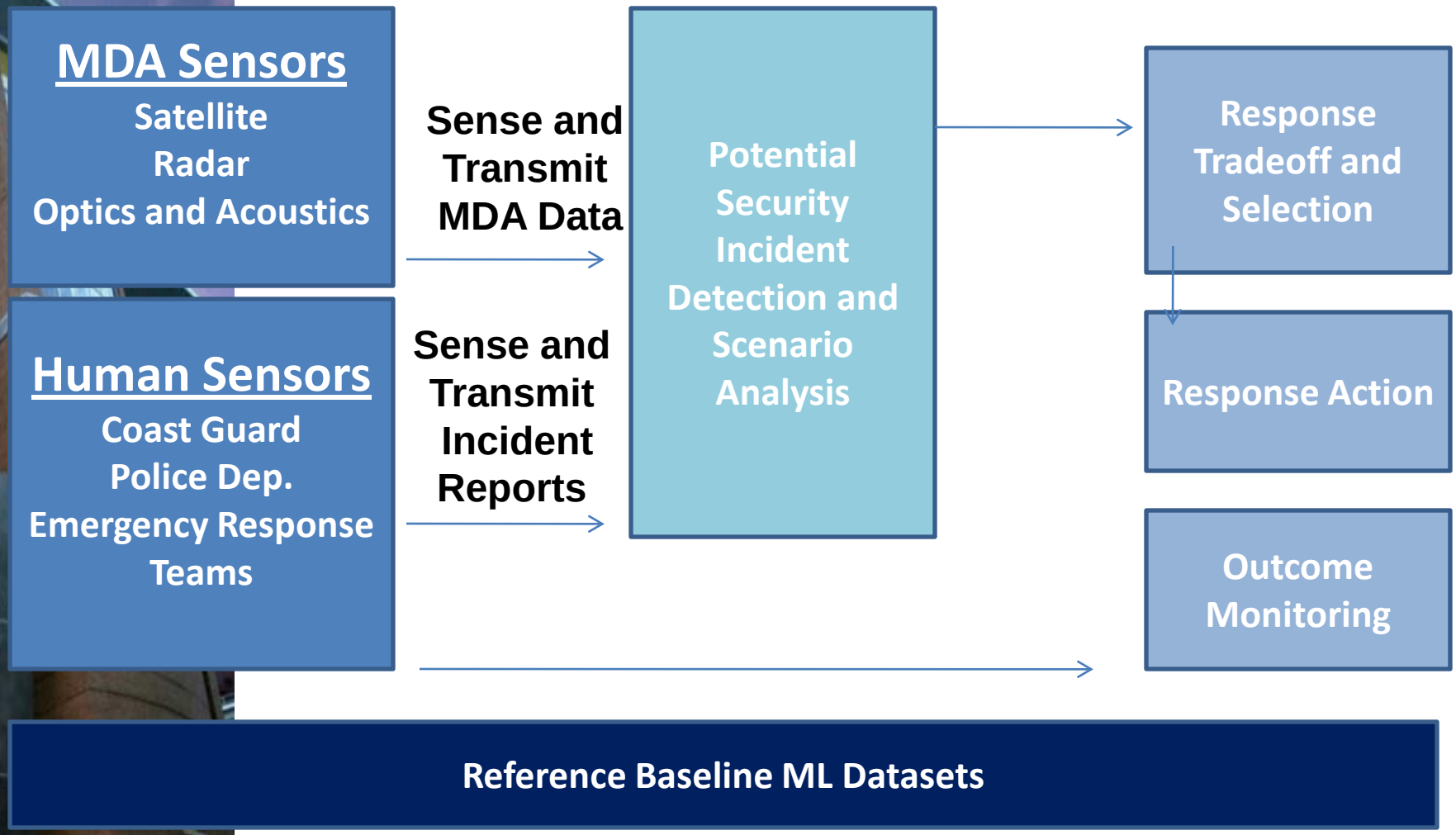
Cognitive Seaports: Efficiency, Security and Resilience

- This challenge can be mitigated by shifting more towards a cognitive seaport that adapts its behavior based on past experience and is able to sense, understand and respond to changes in its environment.
- In this research we propose the Cognitive Process Architecture Framework (CPAF) that allows seaport stakeholders to sense changes/events, perceive operational scenarios, choose response alternatives based on tradeoffs and monitor the implementation of the responses.

What are Cognitive Ports?

- A cognitive system is one that learns and adapts its behavior based on past experience and is able to sense, understand and respond to changes in its environment
- A Cognitive Maritime and Port Security Enterprise Architecture will allow leveraging information technology and human resources to couple **efficiency, security and resilience** in a cost-effective manner
- It will allow currently separate efforts in **maritime domain awareness, emergency response and resiliency** to be integrated and create significant synergies over time

Cognitive Maritime Security Architecture



Cognition-Centric systems Capabilities

Sensing internal and external (local) system conditions

Perceiving /Understanding the (local/global) system state

Associating the situation with past experiences

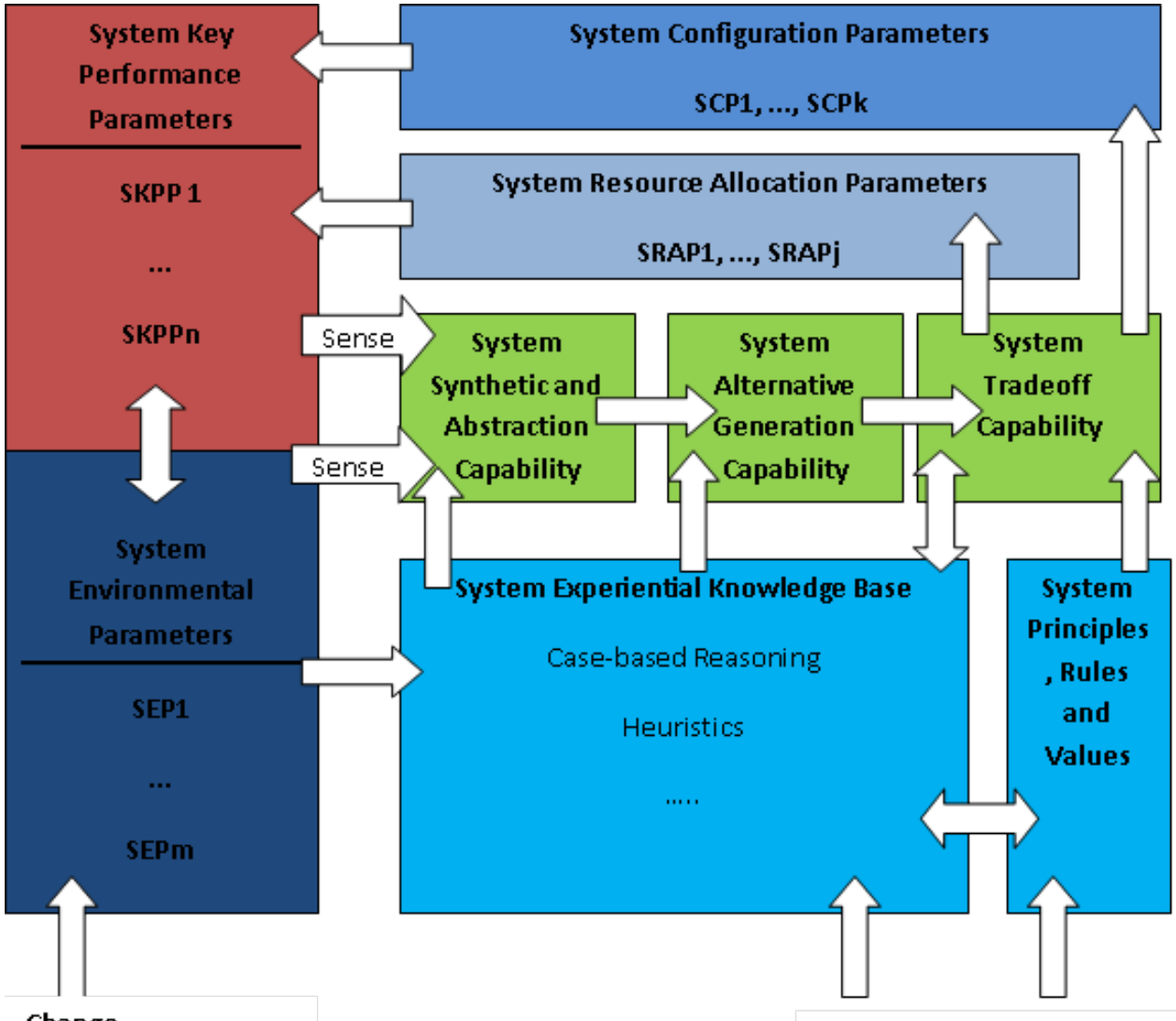
Trading-off various alternatives

Selecting course of action for response to situation

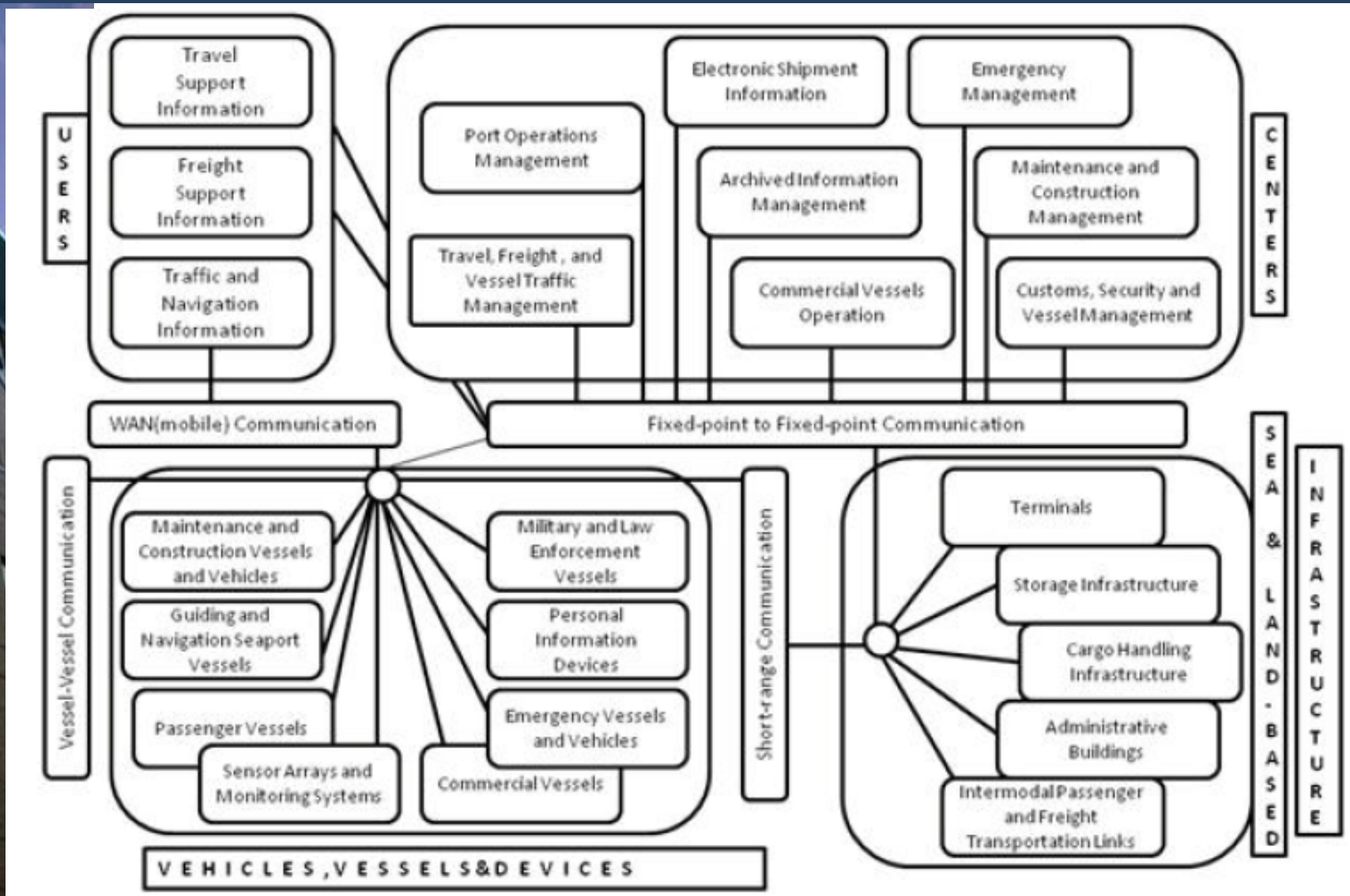
Implementing action by adjusting resources and configurations

Monitoring and Learning from the consequences of the action

Cognition-Centric Systems Processes



Information Sharing Architecture in Cognitive Seaports



Architecting Cognitive Processes

- To design a cognitive seaport one can start with key processes within the seaport rather than making the entire seaport cognitive
- The Cognitive Process Architecting Framework (CPAF) (Mostashari, 2011) allows us to make a seaport enterprise more cognitive gradually
- It is important to note that some processes within the seaport enterprise might always remain non-cognitive. In fact a highly cognitive seaport may be one with less than 20% cognitive processes

The CPAF Framework

Cognitive Architecture

1. Identify Key Performance Metrics (KPP)
2. Identify Key Environmental Parameters (KEP)
3. Design Sensor Architecture for Measuring (KEP and KPP)
4. Develop Scenario Database and Baseline Behavior Benchmarks
5. Identify Scenario-based Response Alternatives and Actors

Cognitive Process

1. Measure KEP and KPPs
2. Identify closest scenario (baseline or change)
3. Select response alternatives from database based on tradeoff
4. Implement response alternative
5. Monitor impact of response alternative
6. Revise Cognitive architecture
7. Go back to Step 1 of Cognitive Process

Step 1>Examples of Key Performance Parameters for a Port

- **Capacity:**
  - # Vessels entering and exiting harbor per day
  - #Vessels processed at terminals per day
  - Tonnage processed per day
- **Safety**
  - # of minor water-side accidents and near accidents per year (or quarter or month)
  - # of major water-side accidents per year
  - # of accidents on port facility
- **Economy**
  - Value of goods processed per day
  - Total cargo handling costs at port

Step 1> Examples of Key Performance Parameters for a Port

– **Security and Resilience**

- # of security breaches at port facility per year
- # of suspicious incidence on port facilities per year
- Number of unidentified vessels entering harbor per day
- Number of investigated suspicious vessels per year
- Number of terrorist attempts per year
- Number of successful terrorist attacks per year
- Number of port closure hours per year
- Etc.

Step 2> Examples of Key Environmental Parameters

Vessel Security

- # and locations of vessels unidentified at this snapshot
- # and locations of vessels exhibiting suspicious behavior (e.g. outside usual routes, unusual maneuvering etc.)
- # and location of vessels close to critical port facilities
- # and location of unidentified divers in the harbor

Step 2> Examples of Key Environmental Parameters

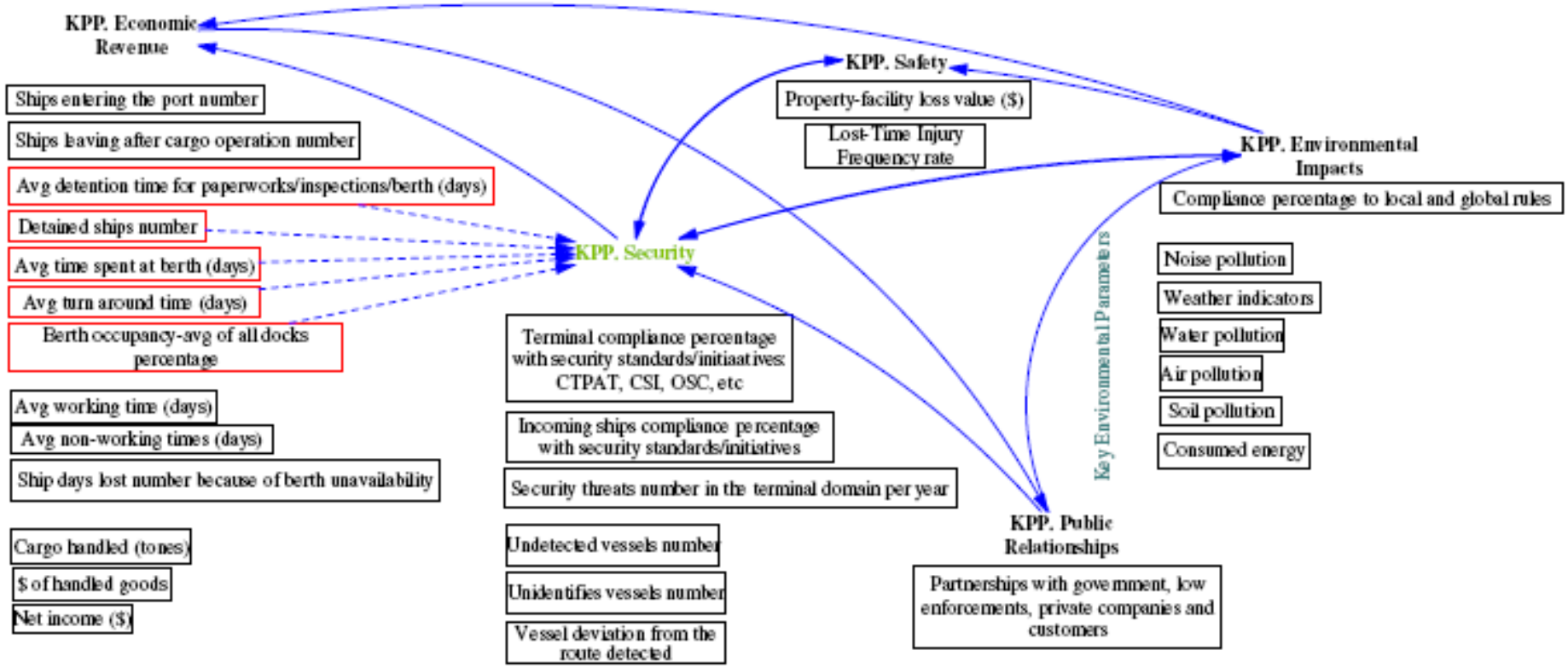
- Container Security
  - # of containers with suspicious RFID tagging
  - # of containers to be inspected with X-Ray etc.
  - # of containers to be inspected manually
  - Number, location and background information on suspicious containers
  - # containers to pass radiation screening

Step 2> Examples of Key Environmental Parameters

- **Vessel Traffic**
  - Smoothness of traffic compared to baseline
  - Traffic volume in harbor, terminal etc. compared to baseline
  - Etc.

- **Environmental and Climate-Related**
  - Weather forecast
  - Actual weather conditions
  - Chemical concentration levels in water
  - Chemical concentration levels in air
  - Chemical Spills location and extent

Linking KEPs and KPPs to Security Metrics



Step 3> Designing Sensor Network

- Based on the KPPs and KEPs identified, what kinds of sensors do we need to measure each?
  - Technological: HF Radar, Satellite, Optics and Acoustics, Infrared, radiation, binoculars etc.
  - Human: Port-side operators, law enforcement officers, coast guard personnel on CG vessels and in command centers, TSA officers etc.

Step 4> Develop Scenario Database

Sensor Grid 1 (Satellite-based)	Sensor Grid 2 (Radar)	Sensor Grid 3 (Acoustics and Optics)	Sensor Grid 4 (other)	Scenario
Data Profile 1.1	Data Profile 2.1	Data Profile 3.1	Data Profile 4.1	S1. Baseline (NO THREAT)
Data Profile 1.2	Data Profile 2.2	Data Profile 3.1	Data Profile 4.1	S1. Baseline (NO THREAT)
Data Profile 1.3	Data Profile 2.2	Data Profile 3.2	Data Profile 4.1	S2. Unidentified Vessel at location (x,y) headed to (x',y') + Threat level
Data Profile 1.1	Data Profile 2.3	Data Profile 3.3	Data Profile 4.1	S3. Unidentified vessel with explosives on board
Data Profile 1.2	Data Profile 2.3	Data Profile 3.3	Data Profile 4.2	S4. Identified Vessel in Distress

Develop Response Alternatives

Scenario	Response Strategy	Actors Involved
S1	Continue monitoring	CG, COTP, CBP, Law Enforcement, TSA, etc.
S2	• Use databases to identify vessel • Communicate to vessel for identification • Send Coast Guard Vessel to investigate • Continue monitoring •Etc.	CG, CBP, COTP and Law Enforcement
S3	• Intercept vessel and disarm	CG, other DHS, U.S. Air Force etc.
S4	• Search and Rescue	CG, etc.

Cognitive Process

1. Measure KEP and KPPs
2. Identify closest scenario (baseline or change)
3. Select response alternatives from database based on tradeoff
4. Implement response alternative
5. Monitor impact of response alternative
6. Revise Cognitive architecture (modify scenario and response database)
7. Go back to Step 1 of Cognitive Process

- When new scenarios (those not anticipated) happen, we add them to the database.
- We also record response effectiveness for future response preparation and tradeoffs

Summary

- The Cognitive Process Architecture Framework (CPAF) allows port authorities to take individual seaport processes and leverage information technology in an integrated fashion to improve safety, security, resilience and efficiency.
- It can serve as a common information-sharing and decision-making platform for various port stakeholders to work together in identifying, preempting or responding to potential threats in a more consorted manner