Case Study for the Annual Computer Security Applications Conference

December 12, 2007 in Miami Beach, FL

Secure Network Integration of Military and Civilian Command & Control During The Trident Warrior Naval Exercise at Norfolk, VA in March, 2007

John A. Sturm

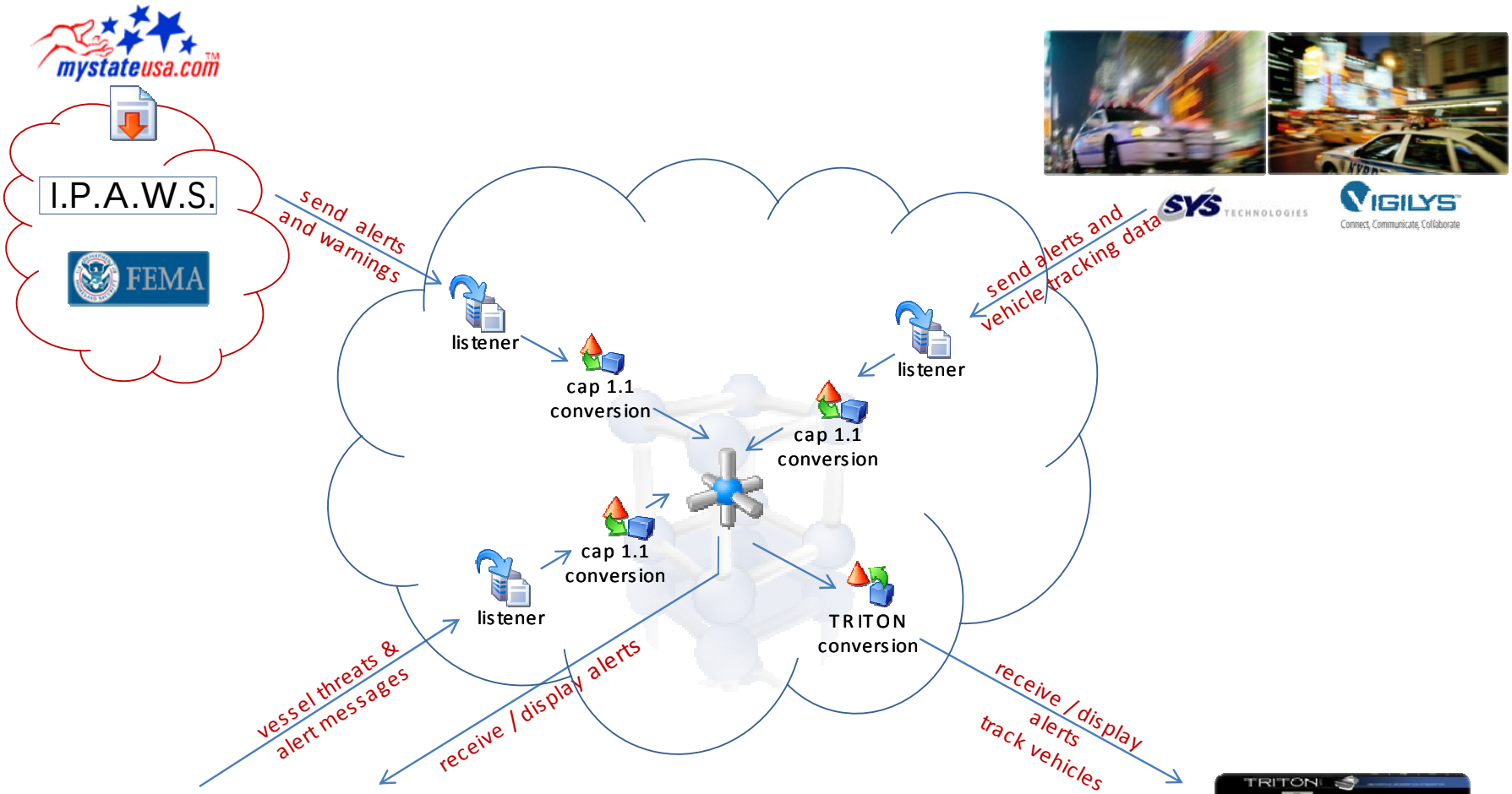
NuParadigm Government Systems

jsturm@nuparadigm.com

December 12, 2007

ABSTRACT

- NuParadigm recently received a Navy SPAWAR contract for "Secure Legacy Application Integration with NCES" (SLAIN).
- As a result, we are developing prototype system models to integrate civilian and military Command & Control (C2) across a Service Oriented Architecture (SOA) network using the internet protocol (IP).
- Web Services and standards provide the promise of reliable, secure interoperability among disparate applications and technologies. However, integration of Command across Civilian and Military structures is as much about creating interoperability among cultures.
- Atkinson & Moffat (2005, pg 161) describe the nature of Command as “a function of trusts, fidelity and agility”, whereas, Control is a function of rules, time and bandwidth”.
- The figure on next slide illustrates a High Level view of the Maritime Domain Awareness (MDA) COI experiment in the Trident Warrior'07Experiment.


mystateusa.com
I.P.A.W.S.
FEMA
send alerts and warnings
listener
cap 1.1 conversion
listener
cap 1.1 conversion
send alerts and vehicle tracking data
SYS TECHNOLOGIES
VIGILYS
Connect, Communicate, Collaborate
cap 1.1 conversion
listener
TRITON conversion
vessel threats & alert messages
receive / display alerts
receive / display alerts track vehicles
TRITON
LOCKHEED MARTIN
We never forget who we're working for
MIDAS
The SLAIN Network
built on
NuParadigm's Foundation™
SPAWAR

- It is important to observe the role of communication networks and particularly the internet in supporting the creation, self-organization and maintenance of Command & Control structures.

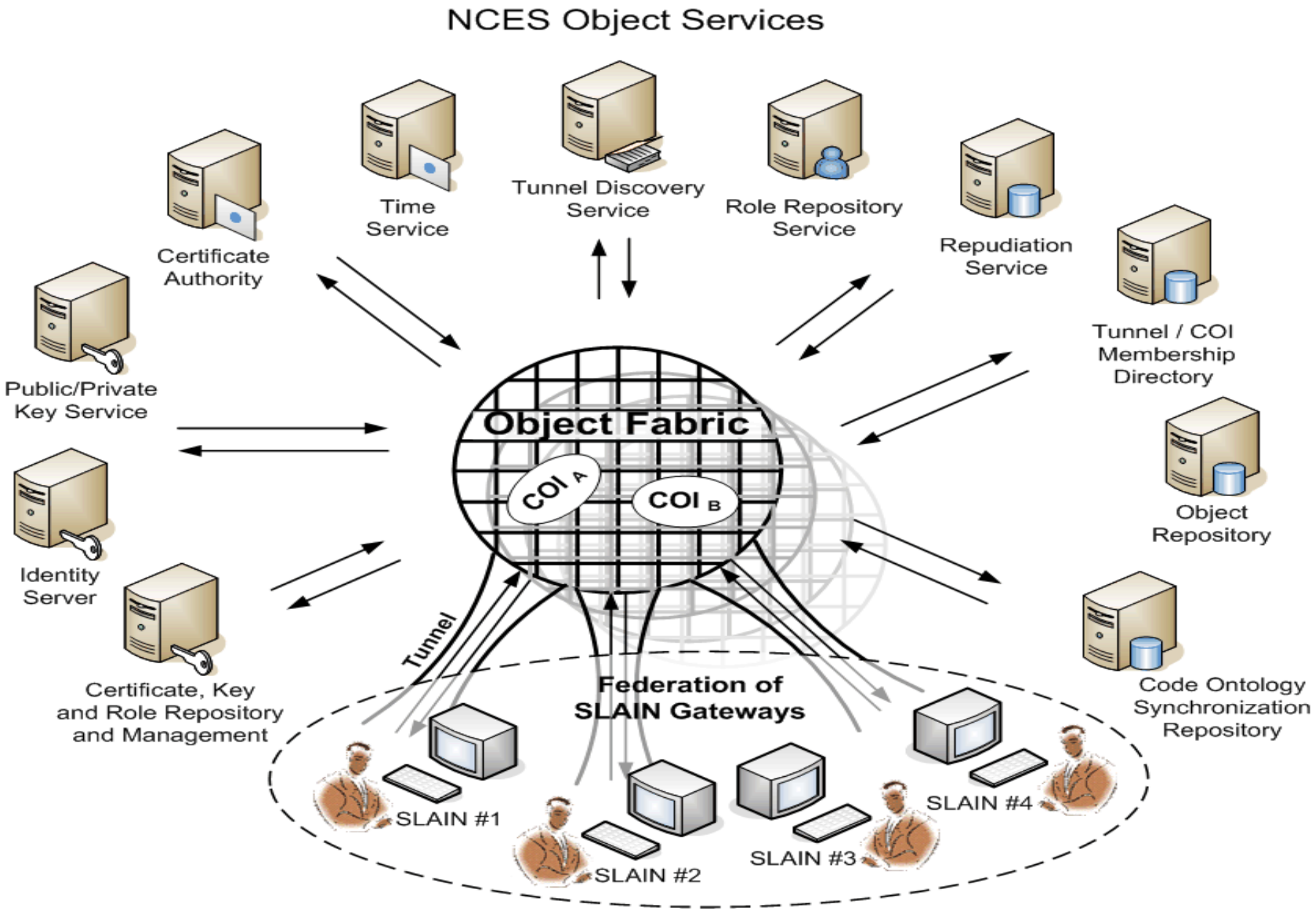
- Atkinson & Moffat (2005, pg 161) also stated, “Organizations have a choice:

    - if they wish to exert control over the battlespace, as opposed to command, they need to provide the rules and quantitative technological bandwidth necessary.

    - If they wish to command, as opposed to control the battlespace, they need to provide the more qualitative trusts of fidelity and agility in their people.

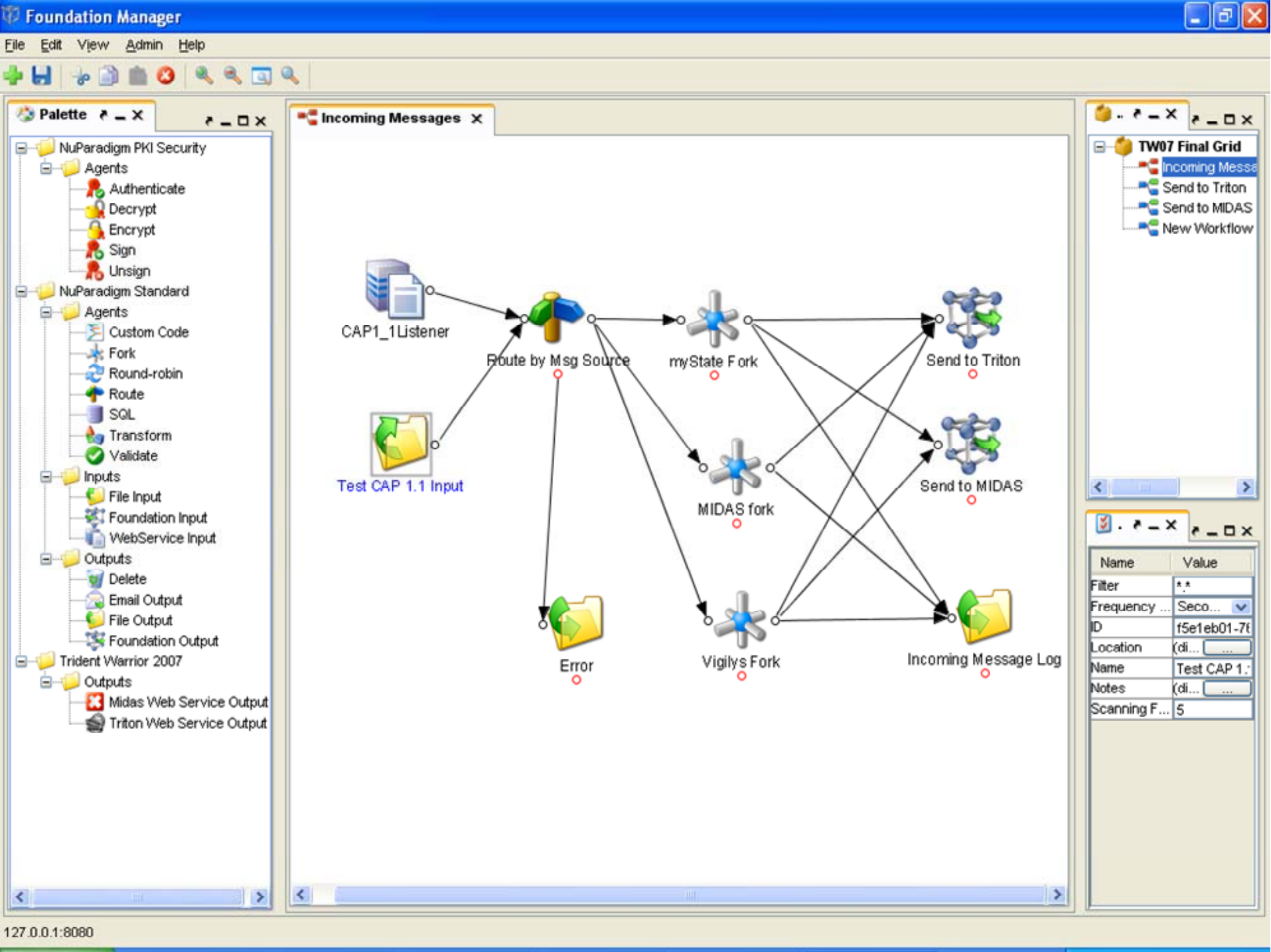
    - Taken one step further, command is more associated with culture, and control with technology; and it is the effect of one upon the other that is key.”

- The task of integrating Civilian and Military Commands is as much about respecting and communicating within the context of each participant’s culture as it is about having the bandwidth and network access to assign and manage the rules of a battle.


NCES Object Services
Time Service
Tunnel Discovery Service
Role Repository Service
Repudiation Service
Certificate Authority
Public/Private Key Service
Tunnel / COI Membership Directory
Object Fabric
COI A
COI B
Object Repository
Identity Server
Tunnel
Certificate, Key and Role Repository and Management
Federation of SLAIN Gateways
Code Ontology Synchronization Repository
SLAIN #1
SLAIN #2
SLAIN #3
SLAIN #4

Our approach is a generic "gateway/edge translation product" thru the Secure Legacy Application Integration with the NCES Enterprise Network structure (called “SLAIN”) that provides a modular implementation of the following:

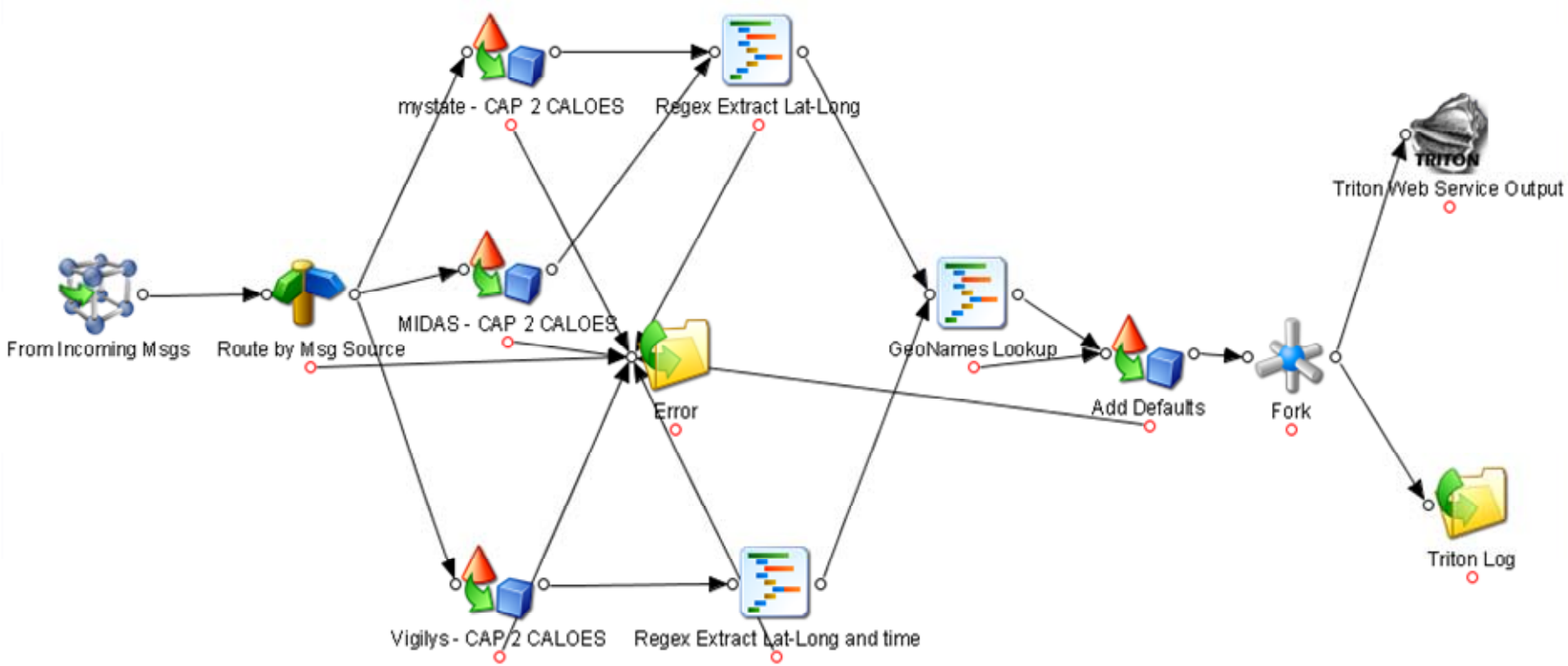
- IA Interoperability
- Cross-boundary policy enforcement
- User/role management,
- Protocol translation and transformation at the "Edge" as part of the NCES architecture/guidance and integration with all the proposed NCES Services,
- Distributed control and management,
- Information Dissemination Management,
- Data synchronization support and data persistence management,
- A highly flexible, easily configured, and easily deployed solution,
- A modular structure that accommodates new protocols and upgrades of existing GCCS-M, FORCEnet or other systems to work together and support any COP
- Support for C2 Integration and Information sharing through a federation of SLAIN Gateways.


Foundation Manager
File
Edit
View
Admin
Help
Palette
NuParadigm PKI Security
Agents
Authenticate
Decrypt
Encrypt
Sign
Unsign
NuParadigm Standard
Agents
Custom Code
Fork
Round-robin
Route
SQL
Transform
Validate
Inputs
File Input
Foundation Input
WebService Input
Outputs
Delete
Email Output
File Output
Foundation Output
Trident Warrior 2007
Outputs
Midas Web Service Output
Triton Web Service Output
Incoming Messages
CAP1_1Listener
Route by Msg Source
myState Fork
Send to Triton
Test CAP 1.1 Input
MIDAS fork
Send to MIDAS
Error
Vigilys Fork
Incoming Message Log
TW07 Final Grid
Incoming Messa
Send to Triton
Send to MIDAS
New Workflow
Name
Value
Filter
Frequency ...
Seco...
ID
f5e1eb01-7
Location
Name
Test CAP 1.
Notes
Scanning F...
5
127.0.0.1:8080

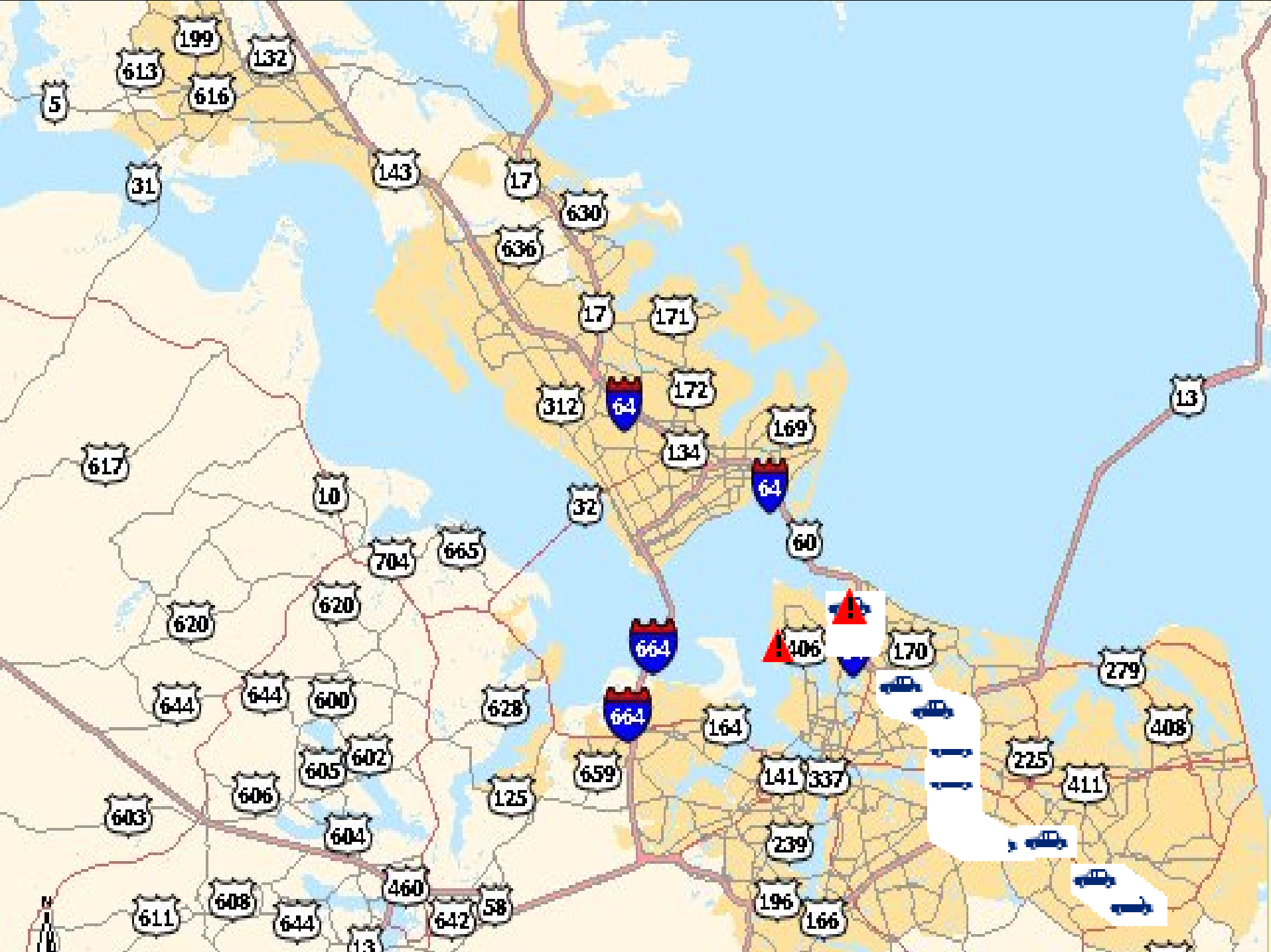
Foundation Manager

File Edit View Admin Help

Send to Triton | Incoming Messages



127.0.0.1:8080


199
132
613
616
5
31
143
17
630
636
17
171
312
64
172
169
134
64
13
617
10
32
60
704
665
620
620
664
406
170
279
644
644
600
628
664
164
408
605
602
659
141
337
225
411
606
125
603
604
239
460
608
58
196
611
644
642
166
13

Summary

- The SOA network environment can act as a strong catalyst for development of effective and agile C2 structures.
- The vision of an effective C2 system becomes a network of formally defined, locally clustered cells with longer range links (shortcuts over the internet) between them: a Small World network.
- In summary, “both Informal Networks and the Formal Organizational Structure are required to work well together in order to deliver the Agile Organization” for effective C2. The secure object routing framework described earlier promises to provide the “shortcuts” essential to C2 network evolution.
- However, significant challenges remain to develop the SOA networks required. The overhead associated with maintaining the message stream and the higher levels of abstraction required in web service communication make this promise difficult in systems of even moderate complexity.
- The challenge is maintaining security, performance, and reliability across disparate systems while minimizing the impact on service levels and the need for significant additional infrastructure investment.
- As a result of our Navy work, we will be addressing several fundamental issues that need to be solved for full deployment of C2 Systems over the GIG with complete situational (and cultural) awareness to support integrated Military & Civilian Ops.