



# A National Effort on Emergency Data Distribution

David E. Ellis

Information Management Architect  
(505) 844-6697, [dellis@sandia.gov](mailto:dellis@sandia.gov)



# What is NAWWS

- A National Alerting and Warning System (NAWS) is an emerging Family of Service Oriented Architecture (SOA) Capabilities which would accomplish National Alerting and Warning needs by combining the capabilities of various Family/System of Systems.
- NAWWS is based on delivering information (Push) about:
  - Changes in the real world environment (Alerting).
  - Response guidance from appropriate decision authority (Warning).
- The OASIS Emergency Management Technical Committee is developing standards which provide the basis for NAWWS delivery (EDXL-DE) and content (CAP, EDXL-RM, etc.) for these SOA based communications.

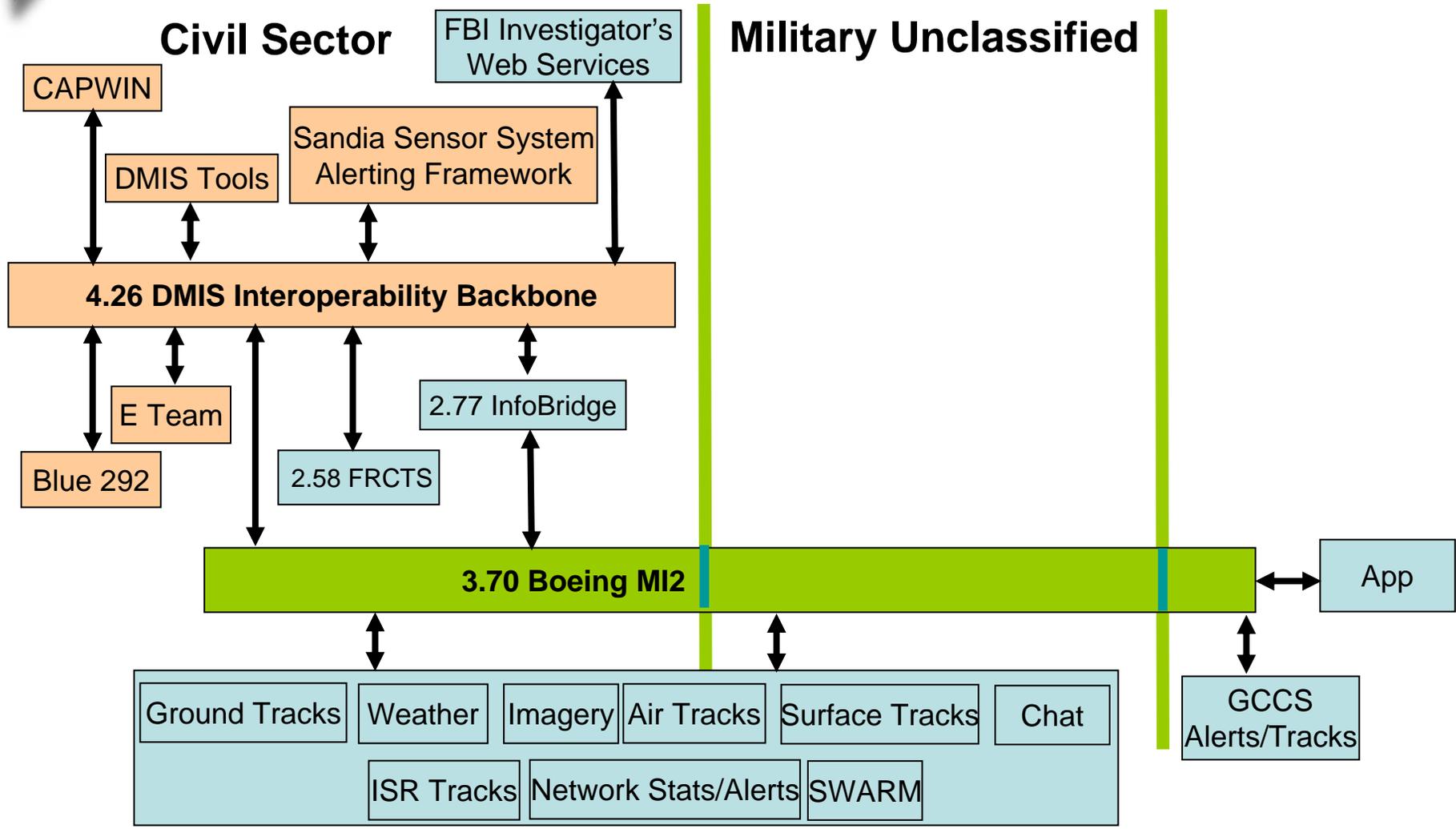


# Initial NAWS Evaluation

- Alerting and warning concepts were evaluated at Coalition Warrior Interoperability Demonstration (CWID) 2005.
- CAP 1.0 was the basis for all messaging interoperability
  - Only approved OASIS standard available.
  - Demonstrated CAP 1.0 was not suitable for delivery of sensor data.
  - Evaluation used the Nuparadigm Foundation software.
- Evaluation also exposed semantics engagement issues
  - Information model for various vendors was tailored to their application/functionality (e.g. parameter element tag usage).
- Sandia Sensor System used limited distribution filtering based on event location
  - No real attempt to use SOA capabilities-to-needs matching.
- CWID 2005 emphasized the need for creation of ad hoc sensor distribution capabilities based on real world incident dynamics.
- The following two slides represent chlorine incident scenarios
  - CWID 2005 depicts integration of various civil sector systems.
  - A Semantic Interoperability Architecture Pilot represents the flow of alerting/warning information.

# CWID '05 "The Real McCoy's"

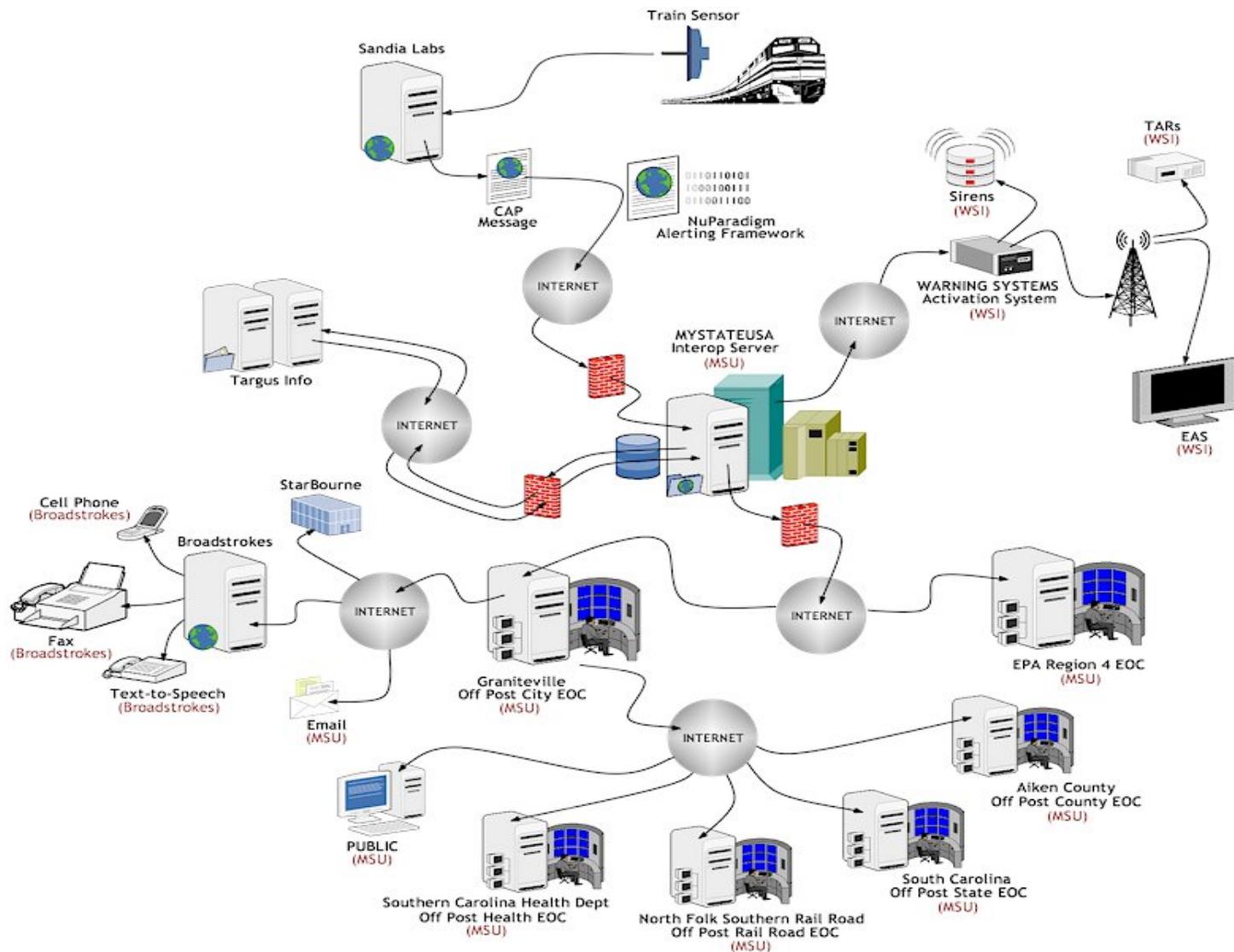
## Collaborating Trials



Exchange alerts containing links to situation awareness artifacts using the Common Alerting Protocol (CAP) Standard



# Semantic Interoperability

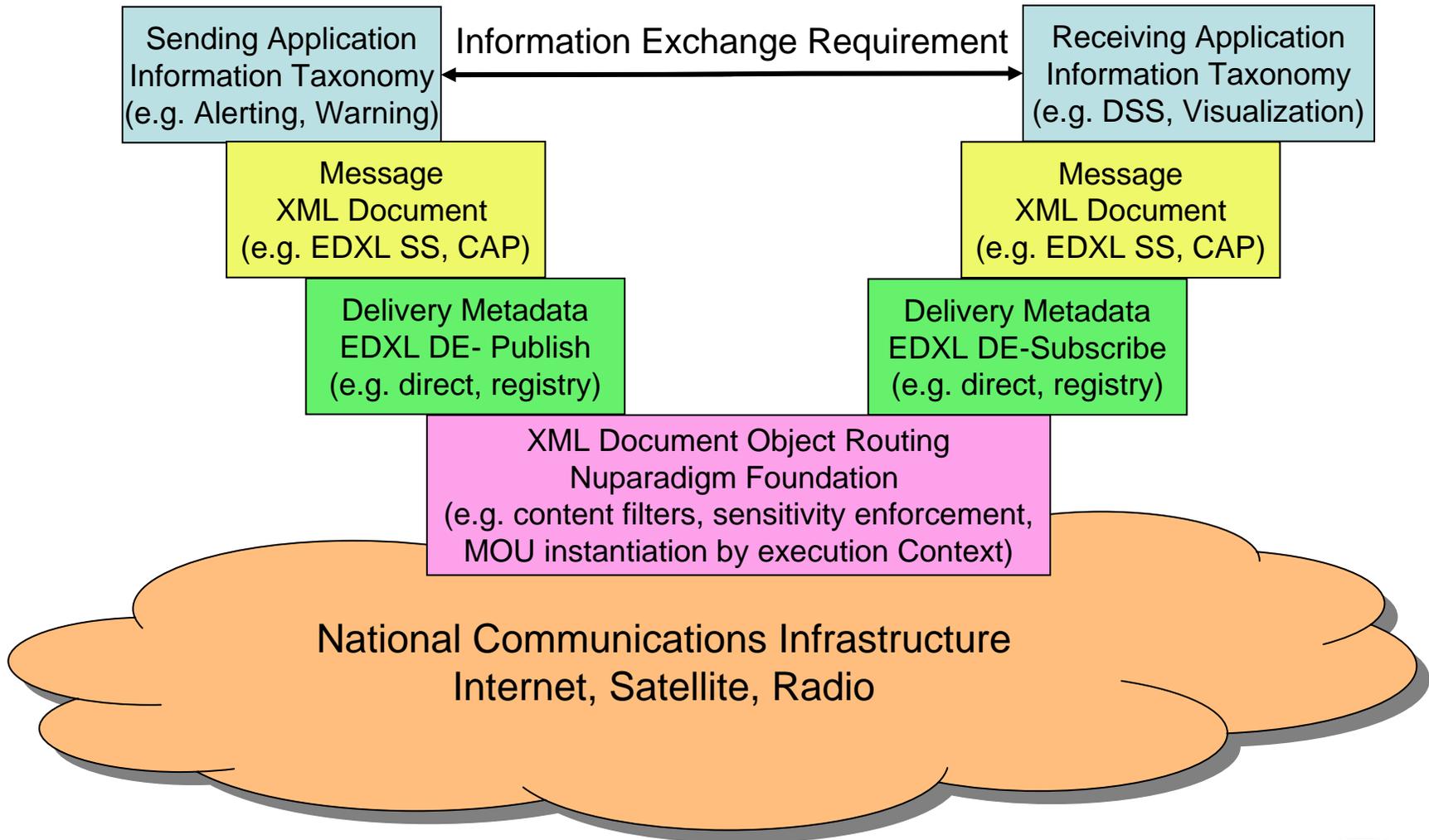




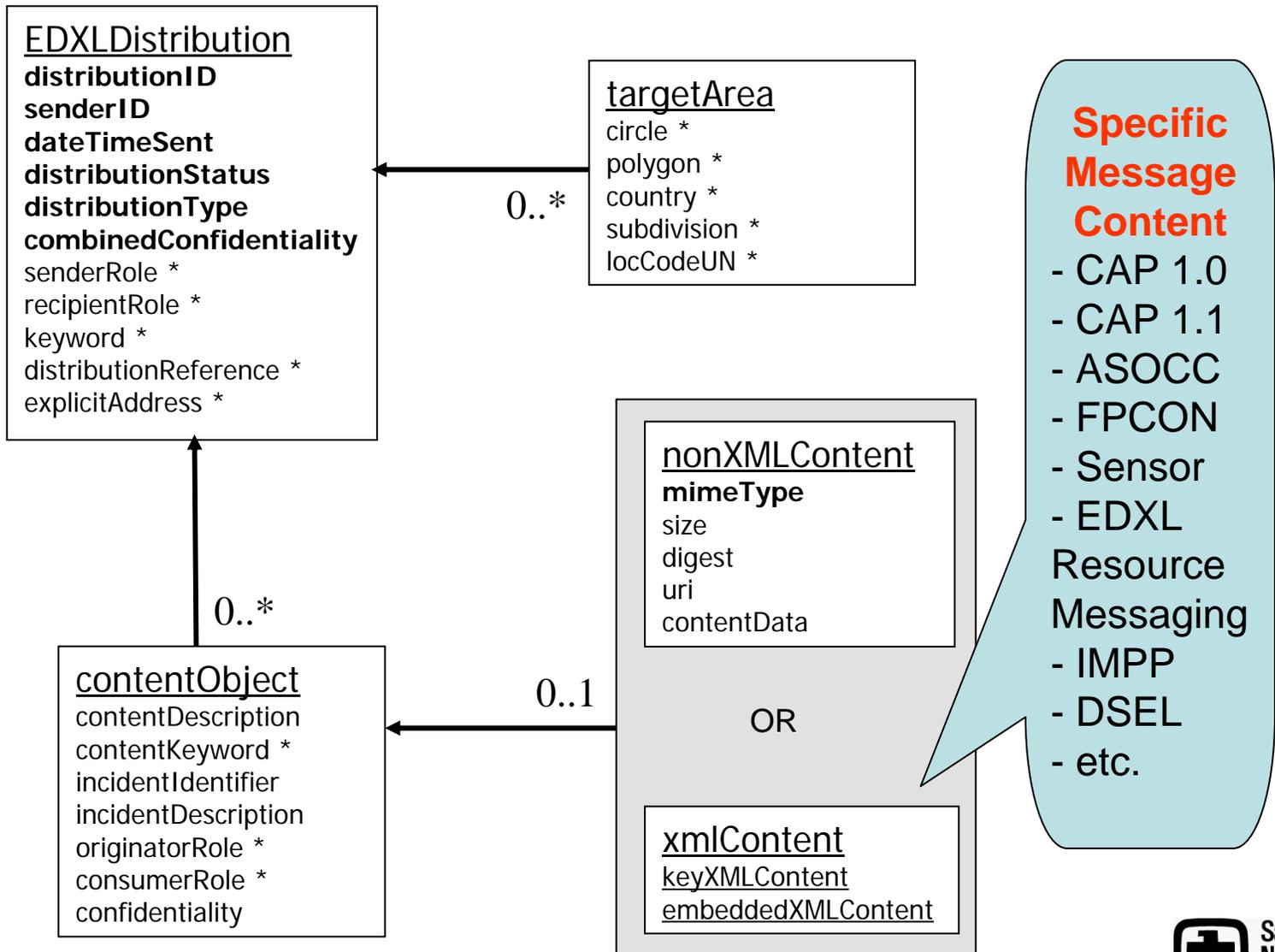
# NAWS Development

- OASIS CAP 1.1 standard approved and in use.
- EDXL-DE created to allow a true SOA approach to alerting and warning system integration.
- Semantic Interoperability Architecture pilot is continuing to work on CAP taxonomy and ontology issues.
- EDXL-DE is currently in ballot at OASIS and expects standard release in April 2006.
- Numerous OASIS EDXL/CAP capable systems will be available this calendar year for deployments.

# NAWS Exchange Architecture



# EDXL Distribution Element (DE)



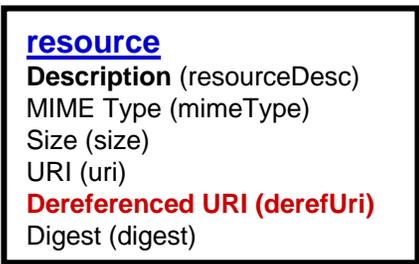
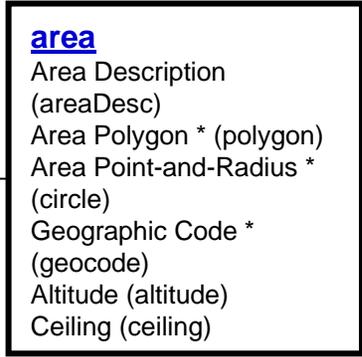
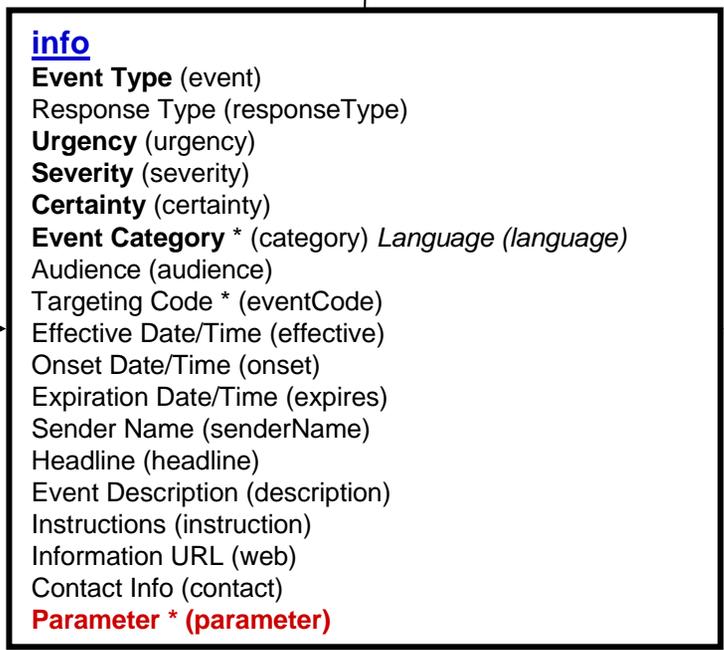
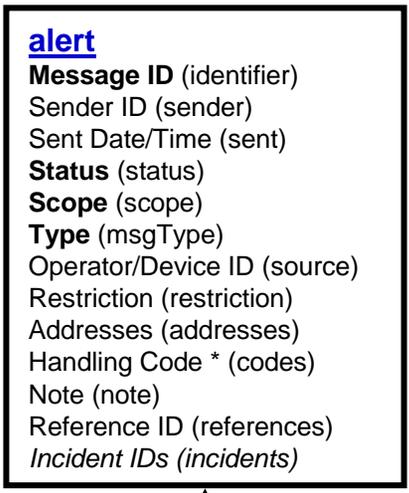
## Specific Message Content

- CAP 1.0
- CAP 1.1
- ASOCC
- FPCON
- Sensor
- EDXL Resource Messaging
- IMPP
- DSEL
- etc.

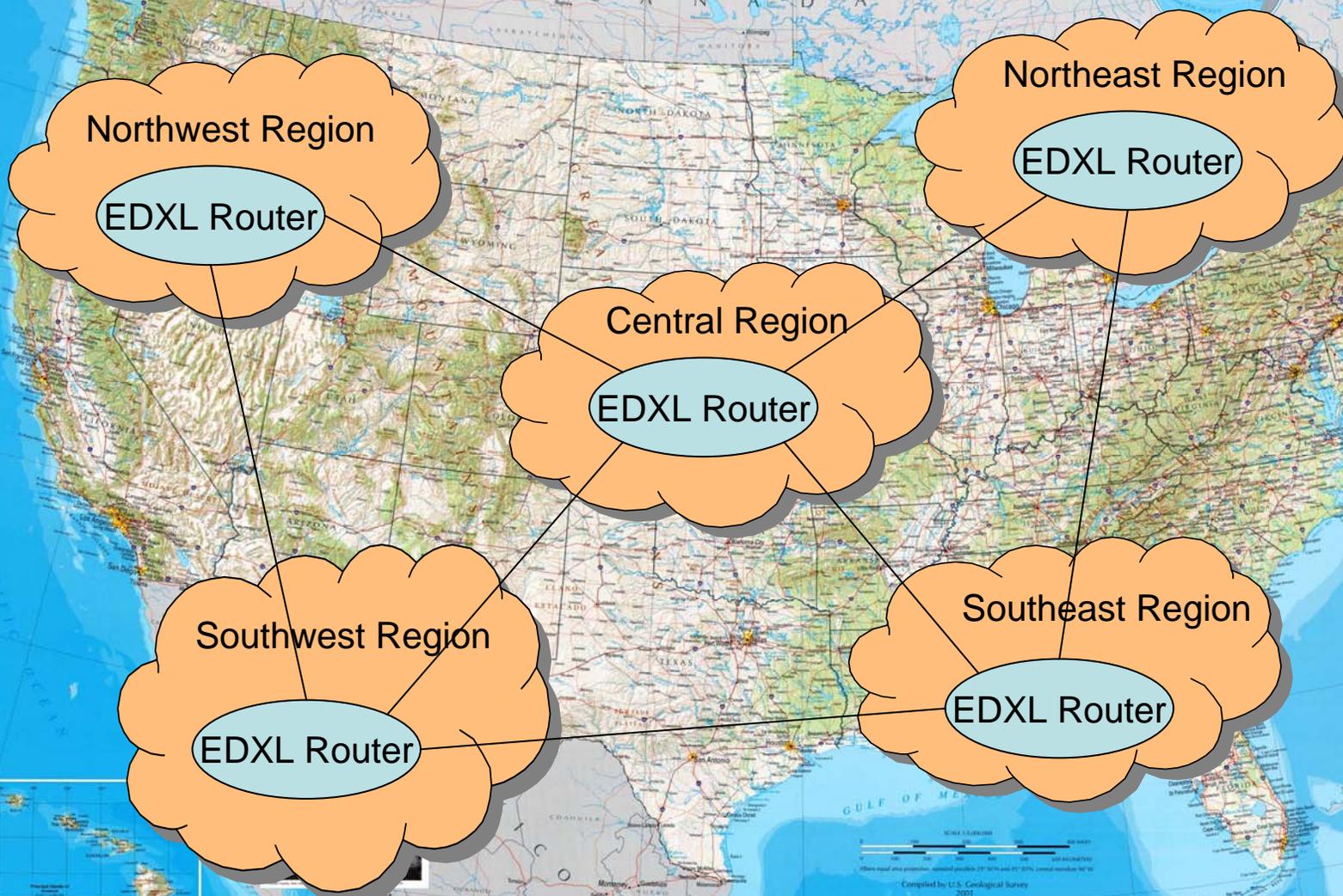


Elements in **bold** are mandatory; those in *italics* are optional; asterisk (\*) indicates multiple instances permitted

# EDXL Content CAP 1.1 Structure



# Notional EDXL Routing Grid



**POPULATED PLACES**

- 1,000,000 and over
- 500,000 - 999,999
- 250,000 - 499,999
- 100,000 - 249,999
- 50,000 and over
- National capital
- State or provincial capital
- Other cities
- Chicago
- Seattle
- St. Louis
- Portland
- San Francisco
- Washington
- Albany

**TRANSPORTATION**

- Interstate, Federal or state highway
- Other principal highway
- Other
- Railroad

**PHYSICAL FEATURES**

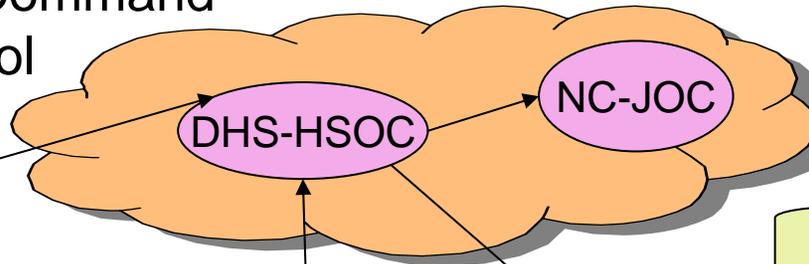
- Mountain, general or prominent
- Valley, general or prominent
- Barrenness indicator
- Higher elevation or steeper slope
- Other elevation data
- State coast

Scale bar: 0 100 200 Kilometers / 0 100 200 Miles

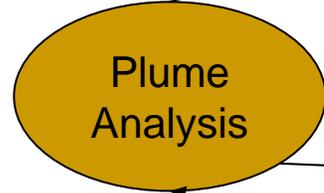
Compiled by U.S. Geological Survey 2001

# Capability Decomposition

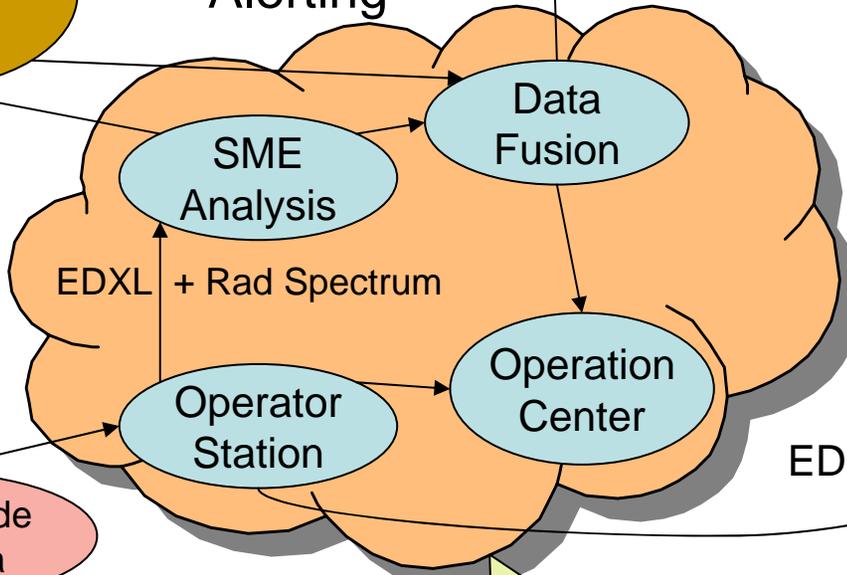
National Command  
and Control



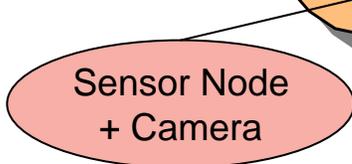
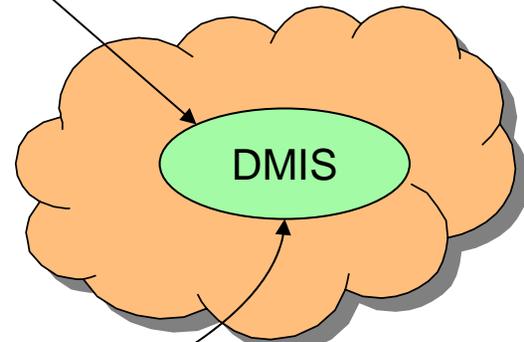
NC2 ValueListUrn



Alerting



Response/Warning

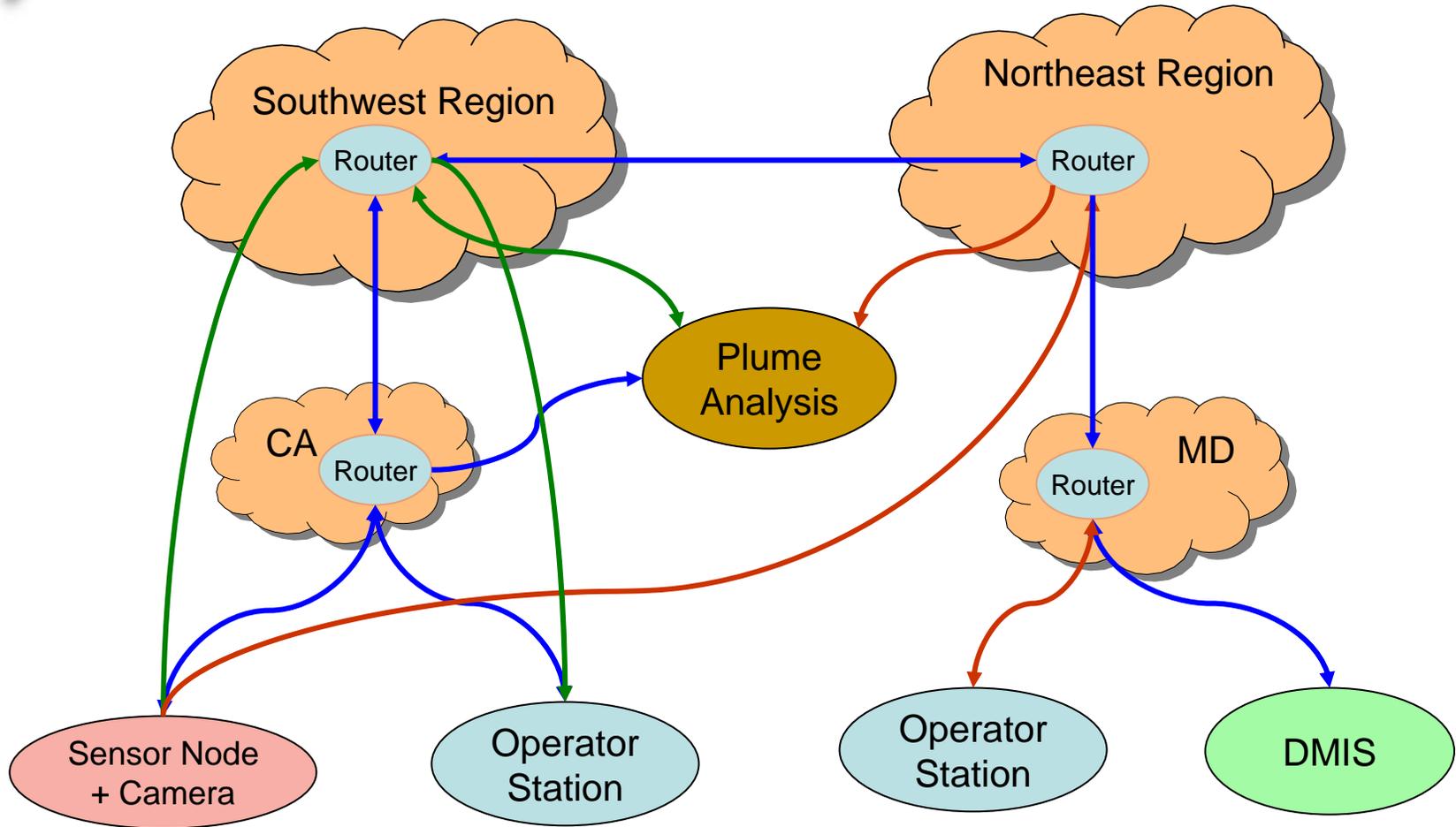


EDXL Proxy

Warning ValueListUrn

Alerting ValueListUrn

# WSDL Distribution Path



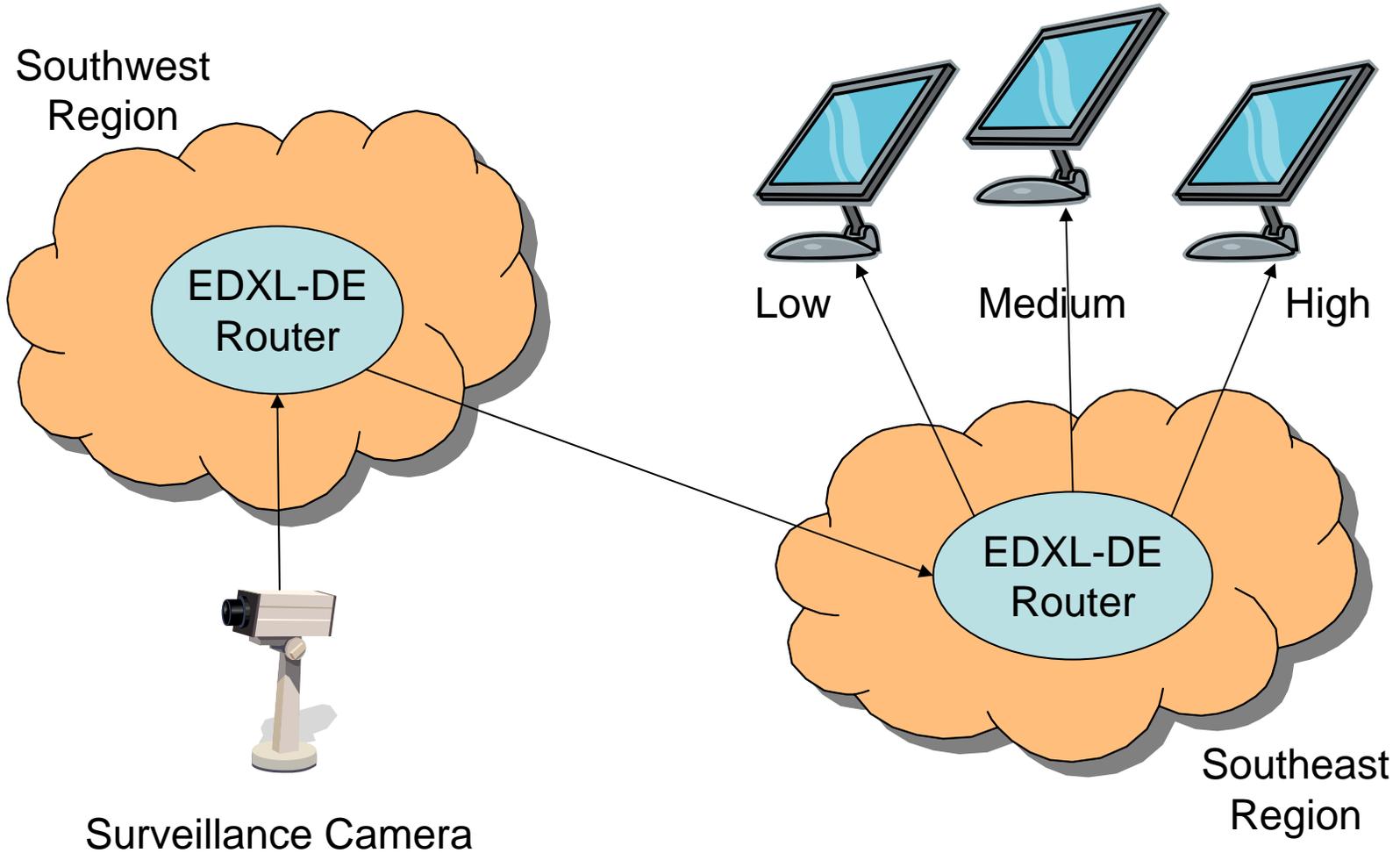
Default WSDL, Secondary WSDL, WSDLs of Last Resort in routing Configuration File



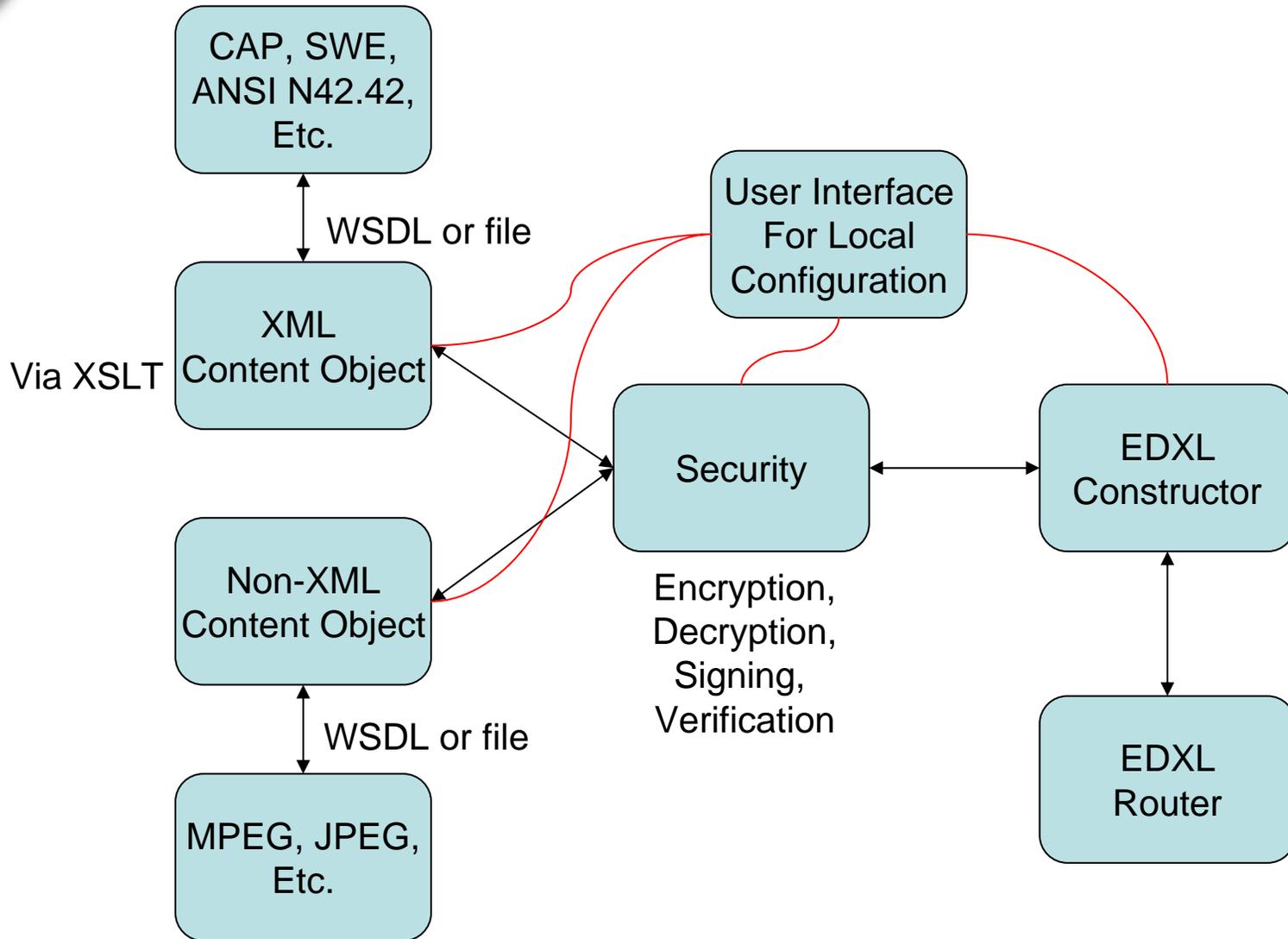
# valueListUrn Strategy

- Prefix for Encoding Schema of valueListUrn
  - NIEM-L-DoDAF
  - Others
- Possible use of Geographical Location Distribution Mask
  - US:SE:CA:
  - locCodeUN
- Topic or Functional Area grouping of Activities (OV1, FEA, others)
  - Alerting
  - Warning
- Potential valueListUrn schema combinations for XPath evaluation
  - NIEM-L-DoDAF:US:SE:CA:OV1:Alerting
  - Example
    - <senderRole>
      - <valueListUrn> NIEM-L-DoDAF:US:SE:CA:OV1:Alerting </valueListUrn>
      - <value>Operator Station</value>
    - </senderRole>
    - <recipientRole>
      - <valueListUrn>Alerting </valueListUrn>
      - <value>SME Analysis</value>
      - <value>Operation Center</value>
    - <recipientRole>

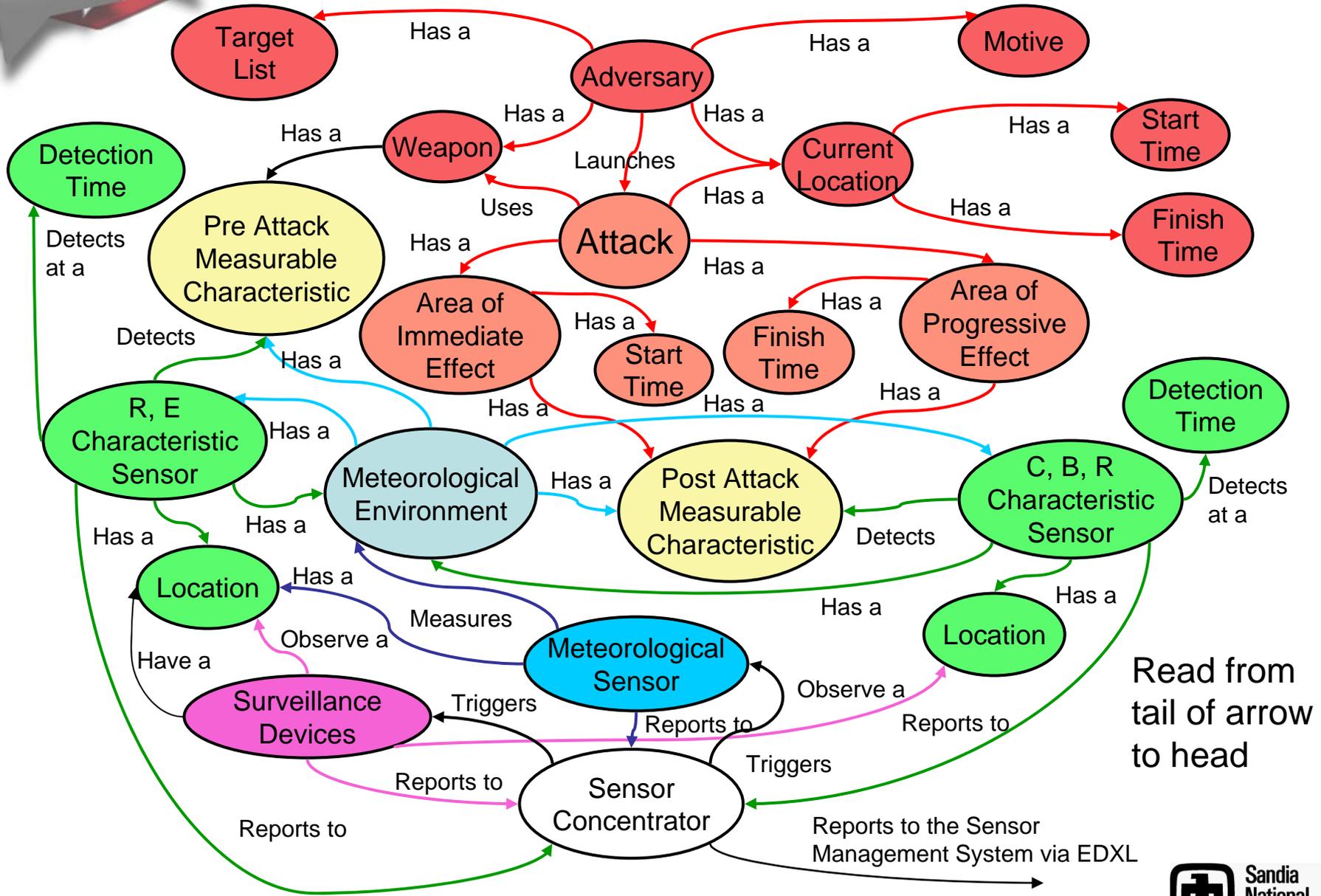
# Edge Message Replication



# Edge EDXL Proxy Service

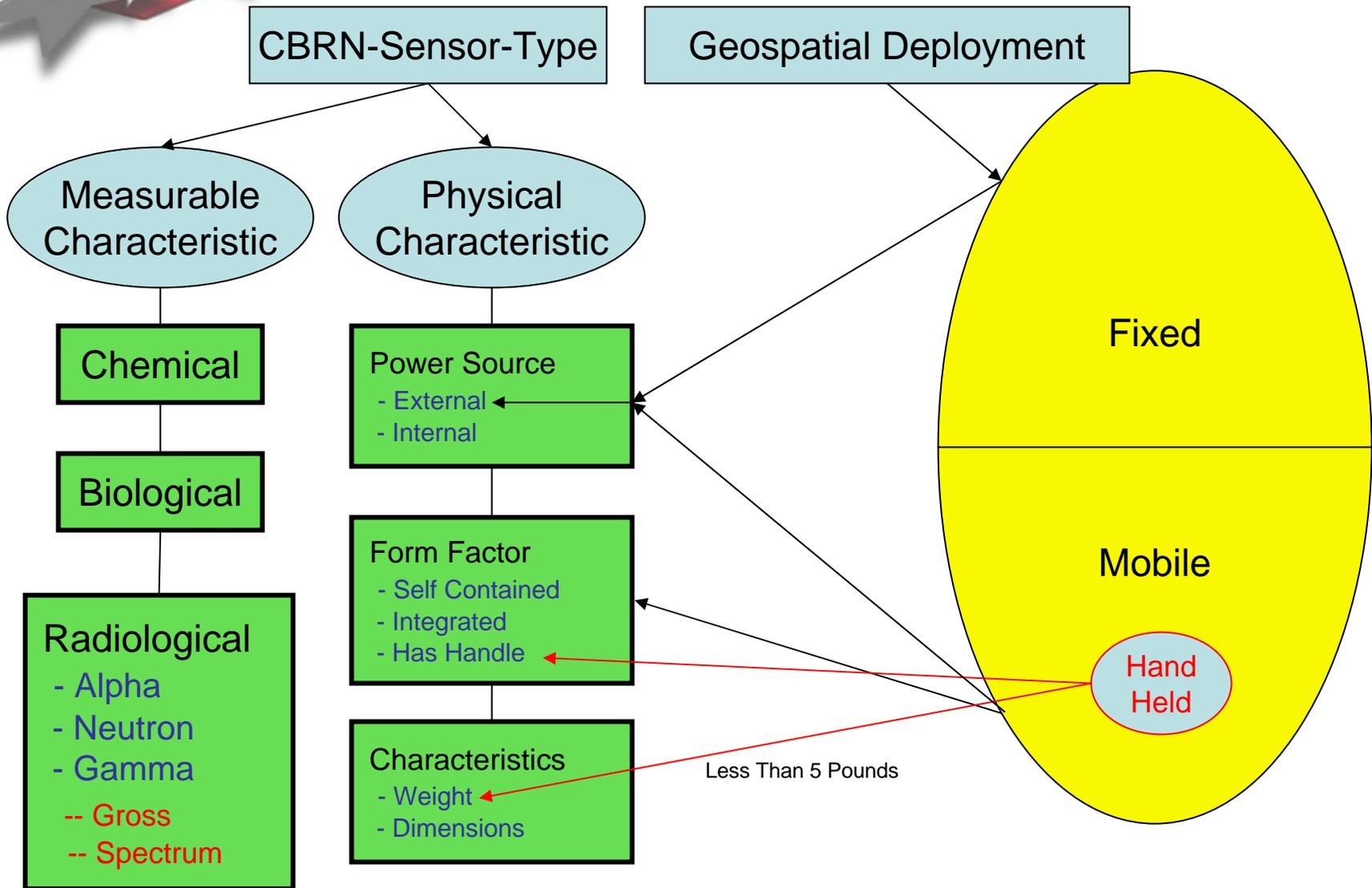


# CBRNE Sensor Detection Ontology



Read from tail of arrow to head

# Sensor Characteristic Decomposition





# Publish Subscribe Registration

<b>Publish</b> <ul style="list-style-type: none"><li>• Type of contentObject being sent<ul style="list-style-type: none"><li>◦ Specific schemas</li><li>◦ Specific mime types</li></ul></li><li>• Restrict usage of content keyword tables</li><li>• Register keyword tables for originator roles</li><li>• Ability to add new schemas, keyword tables, originator roles, and mime types</li></ul>	<b>Subscribe</b> <ul style="list-style-type: none"><li>• Type of contentObject to receive<ul style="list-style-type: none"><li>◦ Specific schemas</li><li>◦ Specific mime types</li></ul></li><li>• Restrict the consumer role tables and the values within the consumer role table</li><li>• Restrict the keyword tables and the values within the keyword table</li><li>• Evaluate all explicit addresses from all explicit address schemas<ul style="list-style-type: none"><li>◦ DMIS Cog/#215</li><li>◦ <a href="mailto:jon@me.org">Email/jon@me.org</a></li></ul></li></ul>
<ul style="list-style-type: none"><li>• Type of distribution element<ul style="list-style-type: none"><li>◦ Specific keyword table and values</li><li>◦ Specific sender role tables and values</li></ul></li></ul>	<ul style="list-style-type: none"><li>• Type of distribution element<ul style="list-style-type: none"><li>◦ Specific keyword tables and values</li><li>◦ Specific consumer role tables and values</li></ul></li></ul>

Certificates will be issued to any system which registers with the distribution system. Certificates will be used to create encrypted Tunnels and to Encrypt and Sign contentObjects.



# Conclusion

- EDXL-DE delivers arbitrary information:
  - Other sensor standards can be distributed (based on roles)
  - System capabilities are tailored to consumer needs by using appropriate standards (Management versus Alerting)
  - Ability to protect content is included
  - Provides for Post before processing (Tactical storage)
  - Architecture allows SOA document distribution
  - Allows for architectural level replication strategies
  - Model is shaped by DoD AF methodologies (can use DRM)
  - Improves on messaging and presence strategies
  - Allows for multiple sensitivity security message exchanges
- Now is the time for joint standard interoperability pilots
  - Obtain representative National use cases for CBRN
  - Access to sensors and sensor networks for pilots
  - Forum for joint experimentation needs to be funded