Order Through KAoS: New Trends in Policy-Based Privilege and Responsibility Management

Jeffrey M. Bradshaw, Ph.D.

jbradshaw@ihmc.us

27 April 2009

ihmc

FLORIDA INSTITUTE FOR HUMAN & MACHINE COGNITION

A University Affiliated Research Institute

University of West Florida
FAU Florida Atlantic University
UCF
Florida Institute of Technology 1958

Florida University Affiliations

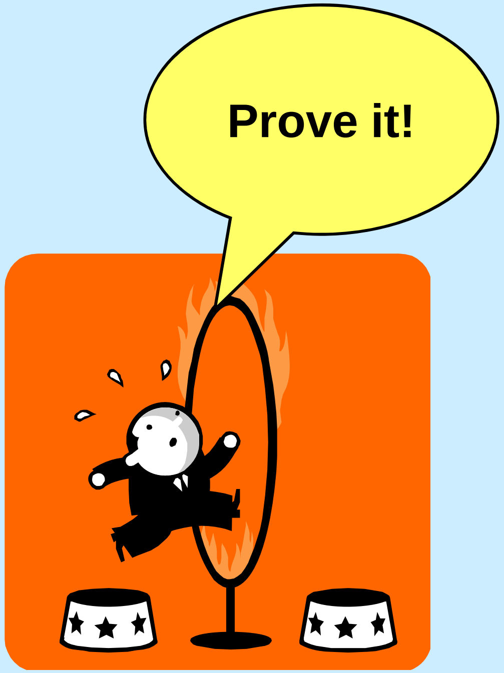
Some Current IHMC Focus Areas

- Next-Generation Interfaces
- Cognitive Work Analysis, Work Systems Design
- Intelligent Data Mining
- Semantically-Rich Policies for Distributed Systems and Human-Agent-Robot Teamwork
- Education, CmapTools
- Semantic Technologies, Cmap Ontology Editor
- MANET, Bio-Inspired Security, Learning
- Agile Computing Middleware
- Multi-Modal Dialogue
- Biologically-Inspired Robotics

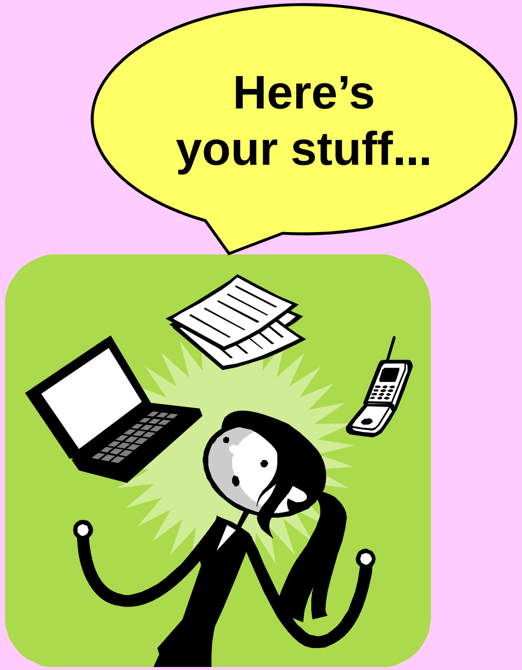
Privilege Management in Eight Words

Identification

Authentication



Authorization



The fine print (Open Group XDSF, ISO 10181-3)

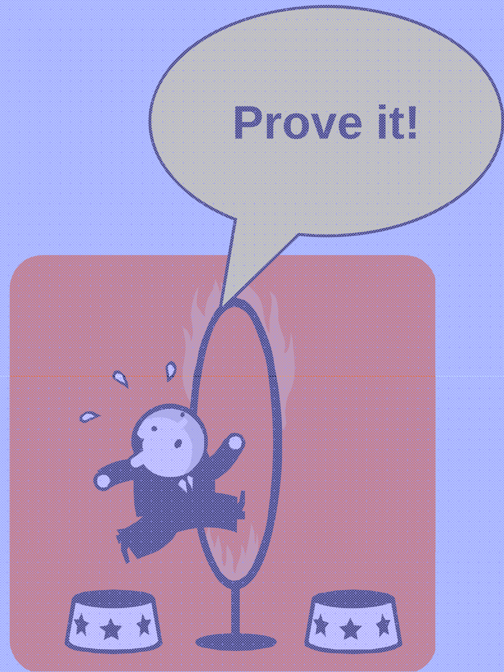
- Identification: The presentation of an identifier so that the system can recognize and distinguish the presenter from other principals
- Authentication: The exchange of information in order to verify the claimed identity of a principal
- **Authorization: The granting of rights, including access, to a principal, by the proper authority**

Principal: An entity (people, devices, applications, etc.) whose identity can be authenticated

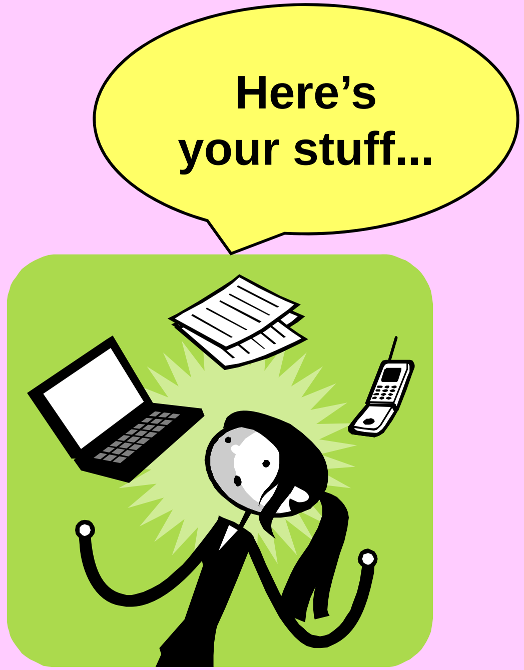
Privilege Management in Eight Words

Identification

Authentication



Authorization



The fine print (Open Group XDSF, ISO 10181-3)

- Identification: The presentation of an identifier so that the system can recognize and distinguish the presenter from other principals
- Authentication: The exchange of information in order to verify the claimed identity of a principal
- **Authorization: The granting of rights, including access, to a principal, by the proper authority**

Principal: An entity (people, devices, applications, etc.) whose identity can be authenticated

Additional Challenge

From Stovepiped Programs…

Courtesy US Army

…to One Roof

Responsibility Management

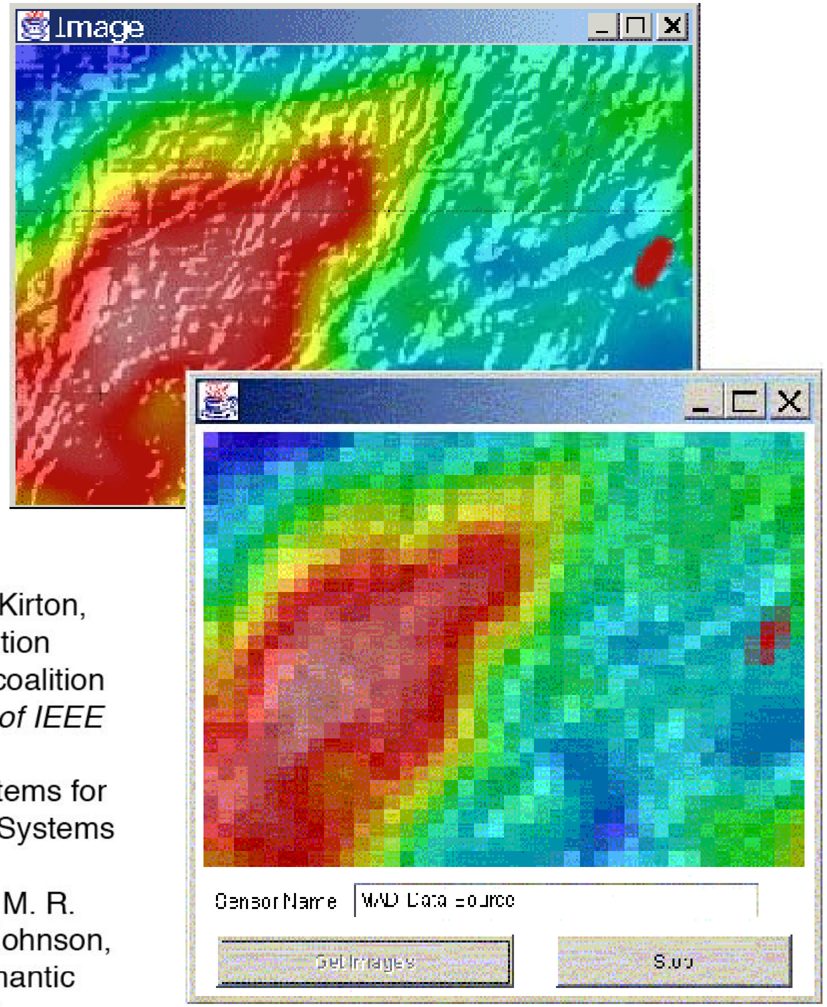
- From “need to know” to “responsibility to share”
- Examples
  - Share and notify
  - Obtain human approval
  - Transform
  - Redact
  - Delay
  - Log

In-Stream Data Processing/Filtering for Policy Enforcement

Example with Video Data

Policies can control

- Resolution
- Frame-rate
- Real-time delays



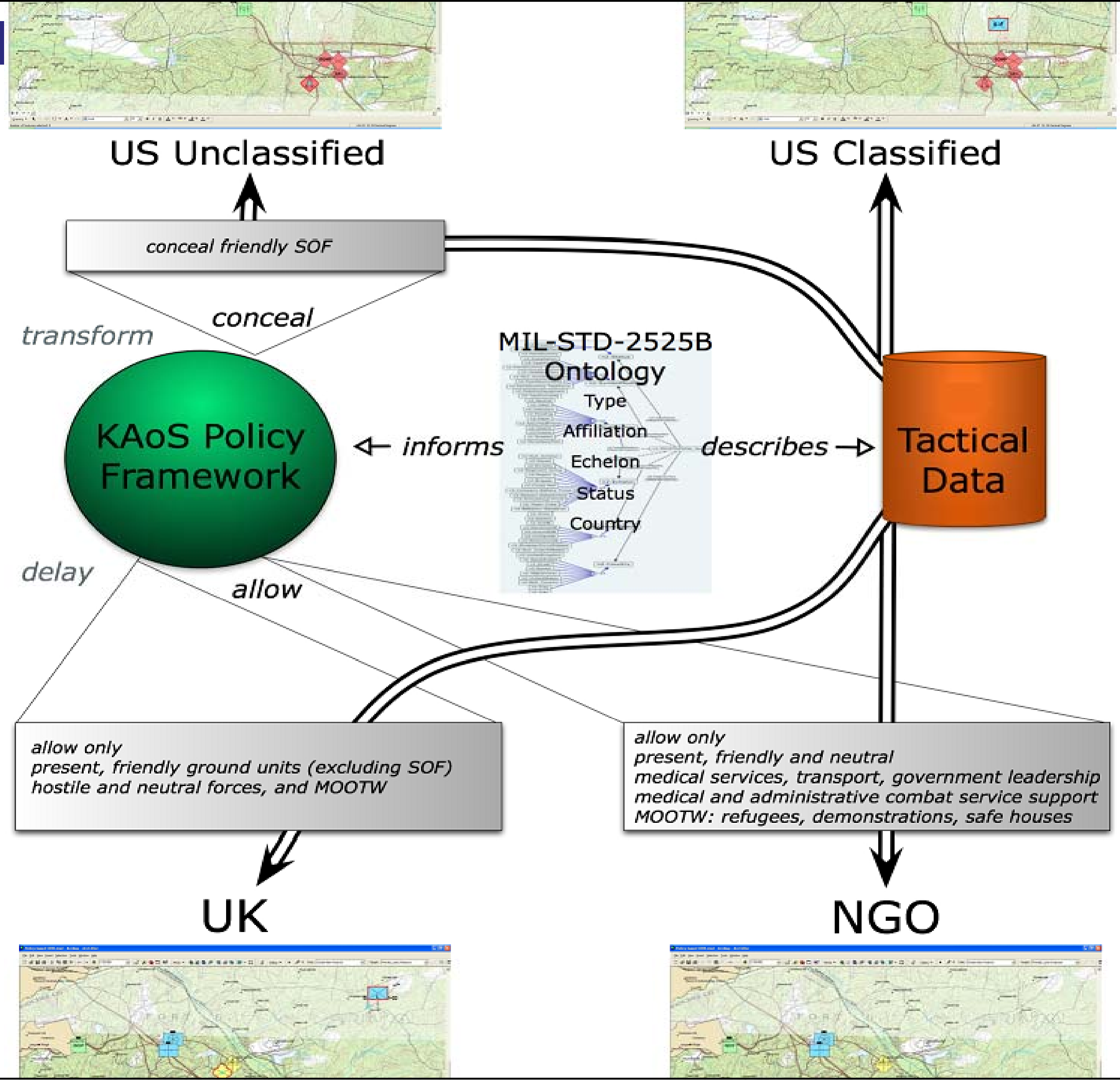
Allsopp, David, Patrick Beautement, Jeffrey M. Bradshaw, Ed Durfee, Michael Kirton, Craig Knoblock, Niranjan Suri, Austin Tate, and Craig Thompson. "Coalition Agents eXperiment (CoAX): Multi-agent cooperation in an international coalition setting." *A. Tate, J. Bradshaw, and M. Pechoucek (Eds.), Special issue of IEEE Intelligent Systems 17*, no. 3 (May/June 2002): 26-35.

Tate, Austin, Jeff Dalton, Jeffrey M. Bradshaw, and Andrzej Uszok. "Agent systems for coalition search and rescue task support." Presented at the Knowledge Systems for Coalition Operations (KSCO 2004) 2004, 137-44.

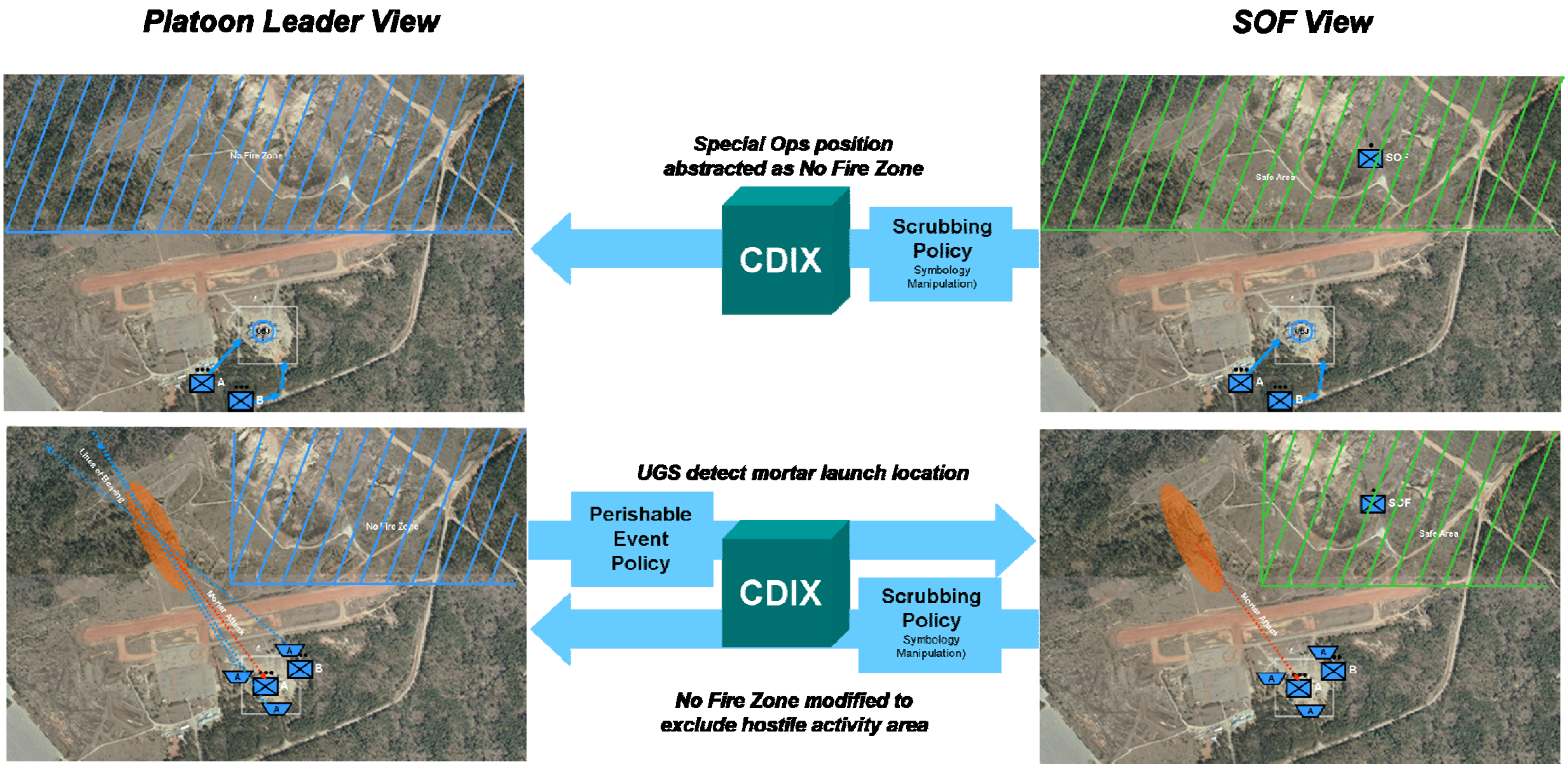
Suri, Niranjan, J. M. Bradshaw, Mark H. Burstein, Andrzej Uszok, Brett Benyo, M. R. Breedy, Marco Carvalho, David Diller, P. T. Groth, R. Jeffers, Matthew Johnson, Shri Kulkarni, and James Lott. "DAML-based policy enforcement for semantic data transformation and filtering in multi-agent systems." Presented at the Proceedings of the Autonomous Agents and Multi-Agent Systems Conference (AAMAS 2003), Melbourne, Australia, 14-18 July, 2003.

Blue Force Tracking Demonstration (ARLADA)

- Reduce the risk of “friendly-fire”
  - Context-sensitive release of “sensitive but perishable information”
    - Based on dynamics of time, location, situation, current mission status
  - Emphasis on “actionable intelligence”
    - “What is happening” vs. “what to do”
  - Transform or redact
    - Protect secret information
    - Obscure methods and sources

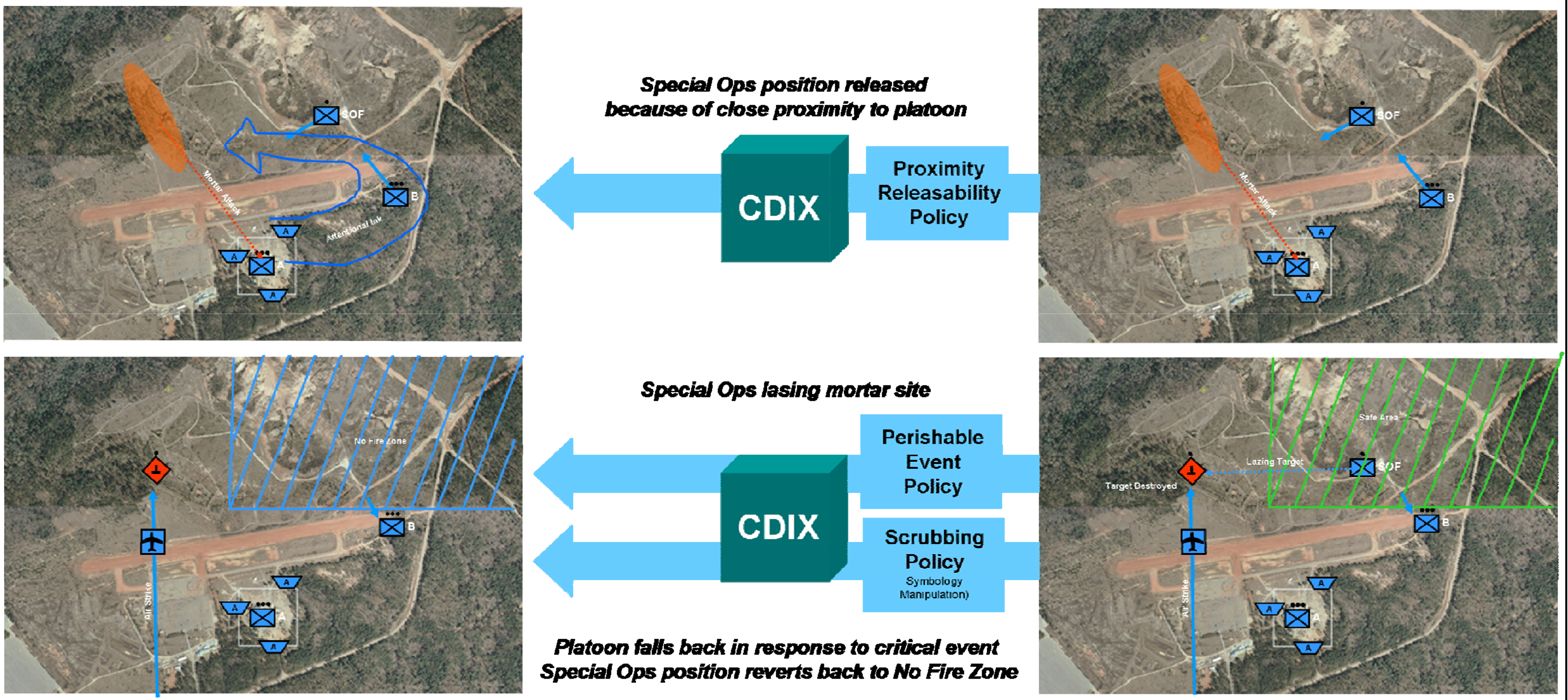

US Unclassified
US Classified
conceal friendly SOF
conceal
transform
MIL-STD-2525B
Ontology
Type
Affiliation
Echelon
Status
Country
KAoS Policy
Framework
informs
describes
Tactical
Data
delay
allow
allow only
present, friendly ground units (excluding SOF)
hostile and neutral forces, and MOOTW
allow only
present, friendly and neutral
medical services, transport, government leadership
medical and administrative combat service support
MOOTW: refugees, demonstrations, safe houses
UK
NGO

Blue Force Tracking: Abstraction



Blue Force Tracking: Proximity

Platoon Leader View ***SOF View***



Policy Representation in OWL

- Rich and meaningful
  - Describe contexts in human-accessible terms involving multiple attributes at multiple levels of abstraction
- Formal
  - Support automated reasoning and enforcement
- Flexible and Extensible
  - Quickly adapt to changing needs and contexts
  - IHMC extensions for ‘variables’ and enhanced reasoning

What is OWL?

- OWL stands for Web Ontology Language
- OWL is built on top of RDF and written in XML
- OWL was designed to be interpreted by computers, not people
- OWL has three sublanguages: OWL-Full, OWL-DL, and OWL-Lite
- OWL is a Web standard
- The use of OWL is not restricted to Web applications

Bradshaw, J. M. (2008). How to do with OWL what people say you can't. Invited keynote. 2008 IEEE Conference on Policy, Palisades, NY, 2-4 June

Policy Representation in OWL

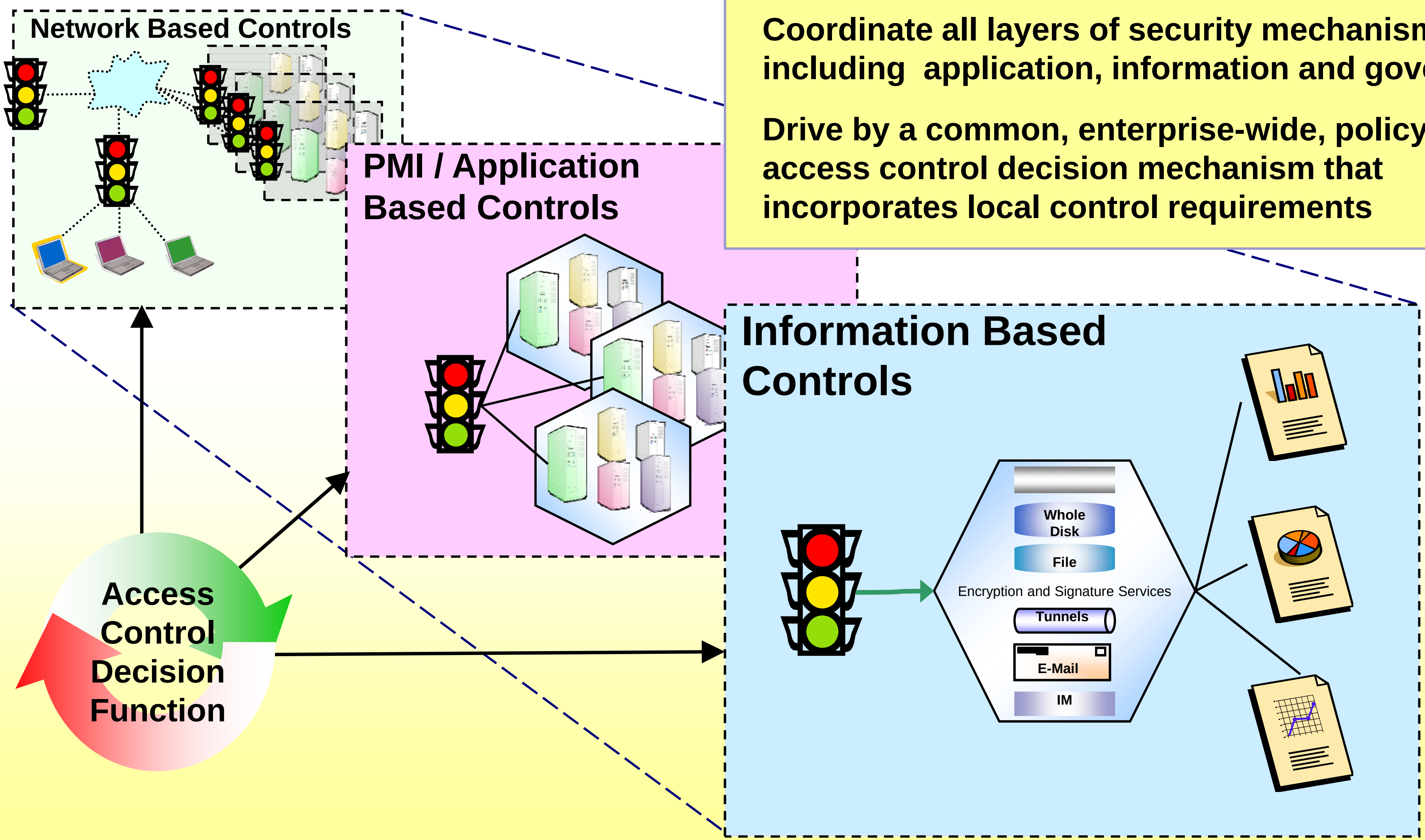
- Support for obligations as well as authorizations
- Support for standard attribute types
  - Principal/Role Attributes
  - Resource Attributes
  - Environmental Attributes
- Support for sophisticated context descriptions
  - Time and space
  - History and state
  - Situation and task context
- Support for reusable abstractions
  - Classification and subsumption
  - Extensible, composable vocabularies and relationships
- Support for online learning and modification

Semantically-Rich vs. Traditional Approaches

	Semantically-rich representations for policy management	Traditional approaches
Expressiveness	Capable of representing concepts and behavior of any complex environment	Capable of controlling specific sorts of behavior within object-oriented systems
	Multiple levels of abstraction	Low level of abstraction: object level
	Easy to extend policy ontology at runtime with new concepts	Extensibility supported by object-oriented inheritance at compile-time
Analyzability	Ontology representation simplifies and directly supports policy reasoning, conflict detection and harmonization	Conflict detection requires transforming policy specification into, e.g., an event calculus representation
	Simplified access to policy information by querying the ontology	Access to policy objects by API
Ease-of-use	Need of specialized GUIs to assist unskilled users with policy specification and interpretation	Language specifically designed for simple policy specification and direct readability
Enforceability	High-level specification requires skilled programmers or sophisticated policy automation mechanisms for enforcement	Detailed specifications can be directly mapped into policy enforcement mechanisms
	Policy sharing among heterogeneous systems requires an agreement on a common ontology	Policy sharing among heterogeneous systems requires agreement on interfaces

Tonti, G., Bradshaw, J. M., Jeffers, R., Montanari, R., Suri, N., & Uszok, A. (2003). Semantic Web languages for policy representation and reasoning: A comparison of KAoS, Rei, and Ponder. In D. Fensel, K. Sycara & J. Mylopoulos (Eds.), *The Semantic Web—ISWC 2003. Proceedings of the Second International Semantic Web Conference, Sanibel Island, Florida, USA, October 2003,* LNCS 2870. Berlin, Germany: Springer, pp. 419-437.

Coordinated Layer Controls

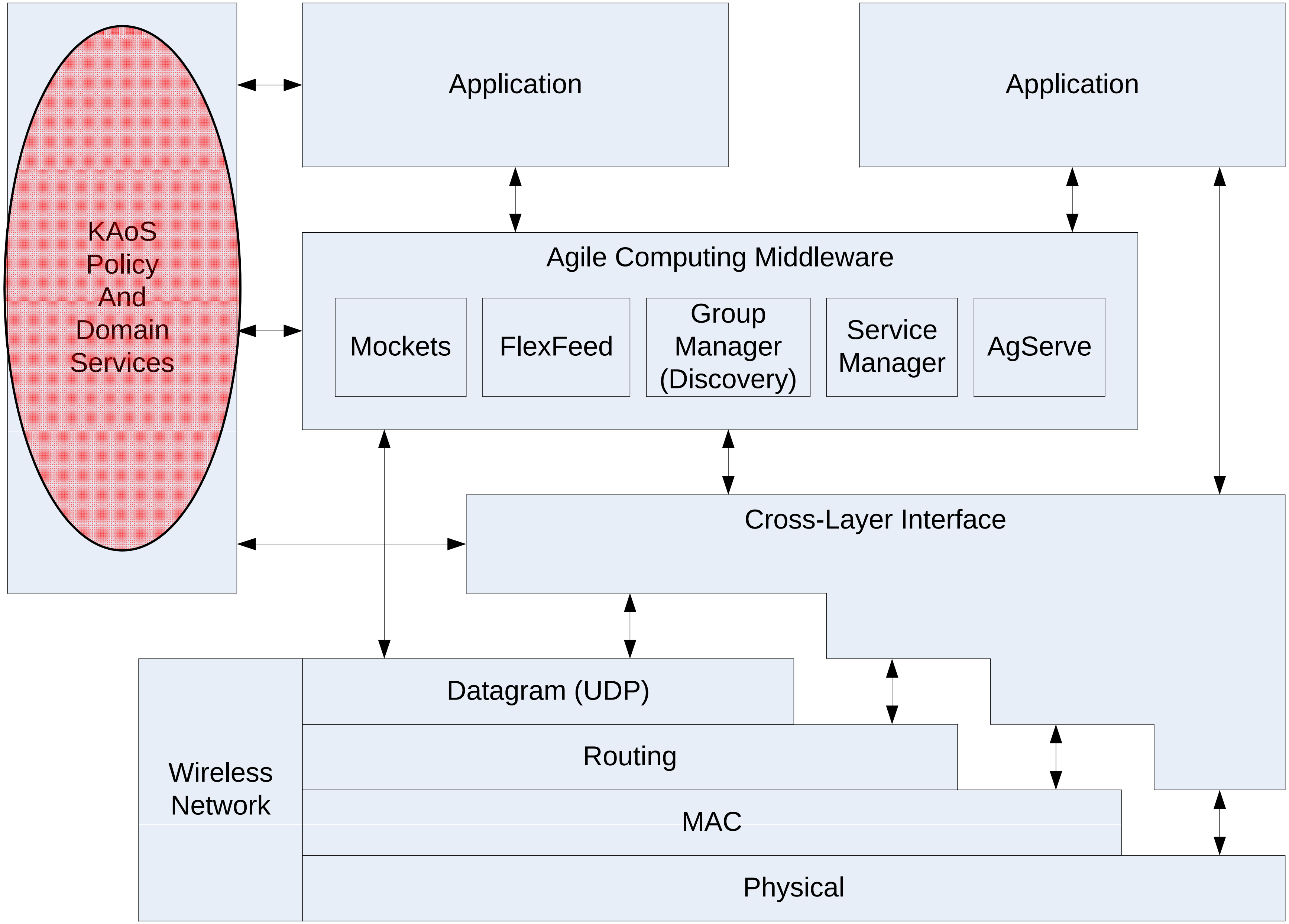


Coordinated Layered Controls

Coordinate all layers of security mechanisms, including application, information and governance

Drive by a common, enterprise-wide, policy-based access control decision mechanism that incorporates local control requirements

Multi-Layer Integration vs. Niche Policy Approaches




KAOS
JUGGLING...KITES...FUN
YELLOW PAGES
STOMP ROCKET
BROOKITE KITES
Chosen Cru

KAoS Overview

- IHMC framework for policy and domain services
- Easy integration through a Common Services Interface (CSI)
- Uses OWL to represent policy, application components, and the real world
  - No “proprietary” language
  - Optional use of “variables” (role-value maps)
  - Integrated reasoner
  - Extremely efficient
    - Fast description logic
    - Incremental (non-monotonic) reasoning
    - “Compiled” to efficient runtime format
- KPAT: rich tailorable GUI for administration
- Kaa: KAoS adjustable autonomy and policy learning
  - Probabilistic reasoning about trust and risk
  - Runtime adaptation based on context-sensitive learning

For more information, see http://ontology.ihmc.us

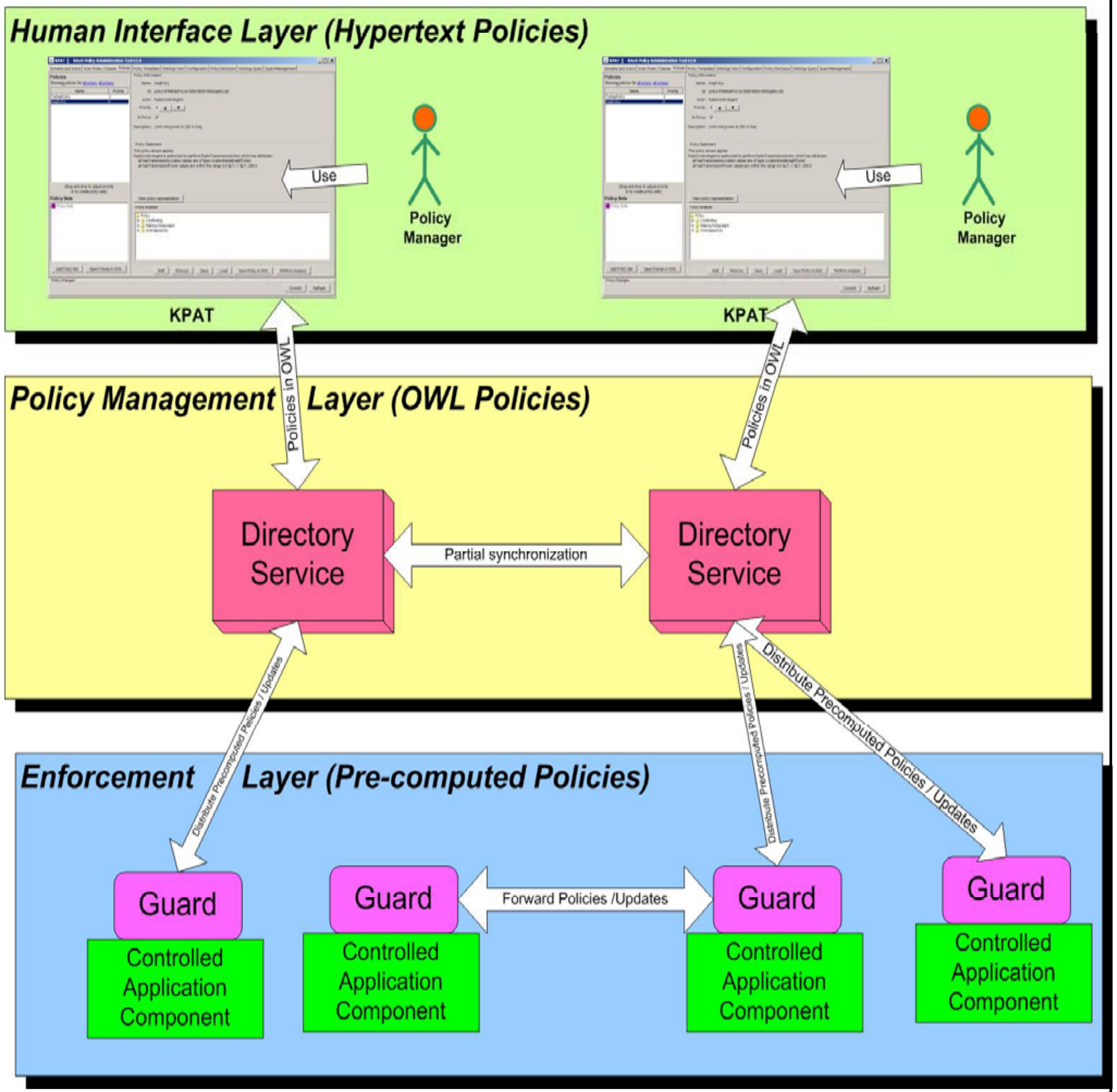
Policies and Domains

- Authorization Policies
  - *Positive Authorization Policy Example (A+)*
    - A is permitted to send a message of a given type to B
  - *Negative Authorization Policy Example (A-)*
    - A is forbidden from sending a message of a given type to B
- Obligation Policies
  - *Positive Obligation Policy Example (O+)*
    - When Event E occurs, A is required to send a message of a given type to B
  - *Negative Obligation Policy Example (O-)*
    - A is not required to send a message to B when Event E occurs
- Domains
  - Enable flexible and powerful definition of sets of individuals, roles, groups, organizational structures, communities of interest
  - Per domain configuration of default authorizations
    - **Laissez-faire mode**: Anything is permitted that is not explicitly forbidden
    - **Tyrannical mode**: Anything is forbidden that is not explicitly permitted

– *Policies and domains form the basis for coordinating joint activity in human-agent-robotic teamwork*
  - *Based on results of field experiments and a theory of joint activity (collaboration with P. Feltovich, G. Klein, D. Woods, and R. Hoffman)*
  - *HART Workshop co-located with HRI 2009, La Jolla, March 2009*

Conceptual Architecture

- *Human interface (KPAT):* a hypertext-like graphical interface for policy specification in the form of **natural English sentences**. The vocabulary is automatically provided from **ontology**.
- *Policy Management representation:* used to encode and manage policy-related information in **OWL**. Inside DS it is used for policy analysis and deconfliction.
- *Policy Decision and Enforcement representation:* KAoS automatically “compiles” OWL policies to an **efficient lookup format** that provides the grounding of abstract ontology terms, connecting them to the instances in the runtime environment and to other policy-related information. These polices are sent from DS to **Guards**, which serve as local **policy decision points.**



Uszok, A., Bradshaw, J. M., et al. (2008). New developments in ontology-based policy management: Increasing the practicality and comprehensiveness of KAoS. Proceedings of the 2008 IEEE Conference on Policy, Palisades, NY, 2-4 June

Policy Example:

Any communication outside the Arabello domain, which is not encrypted is forbidden.

OWL Policy Syntax Example

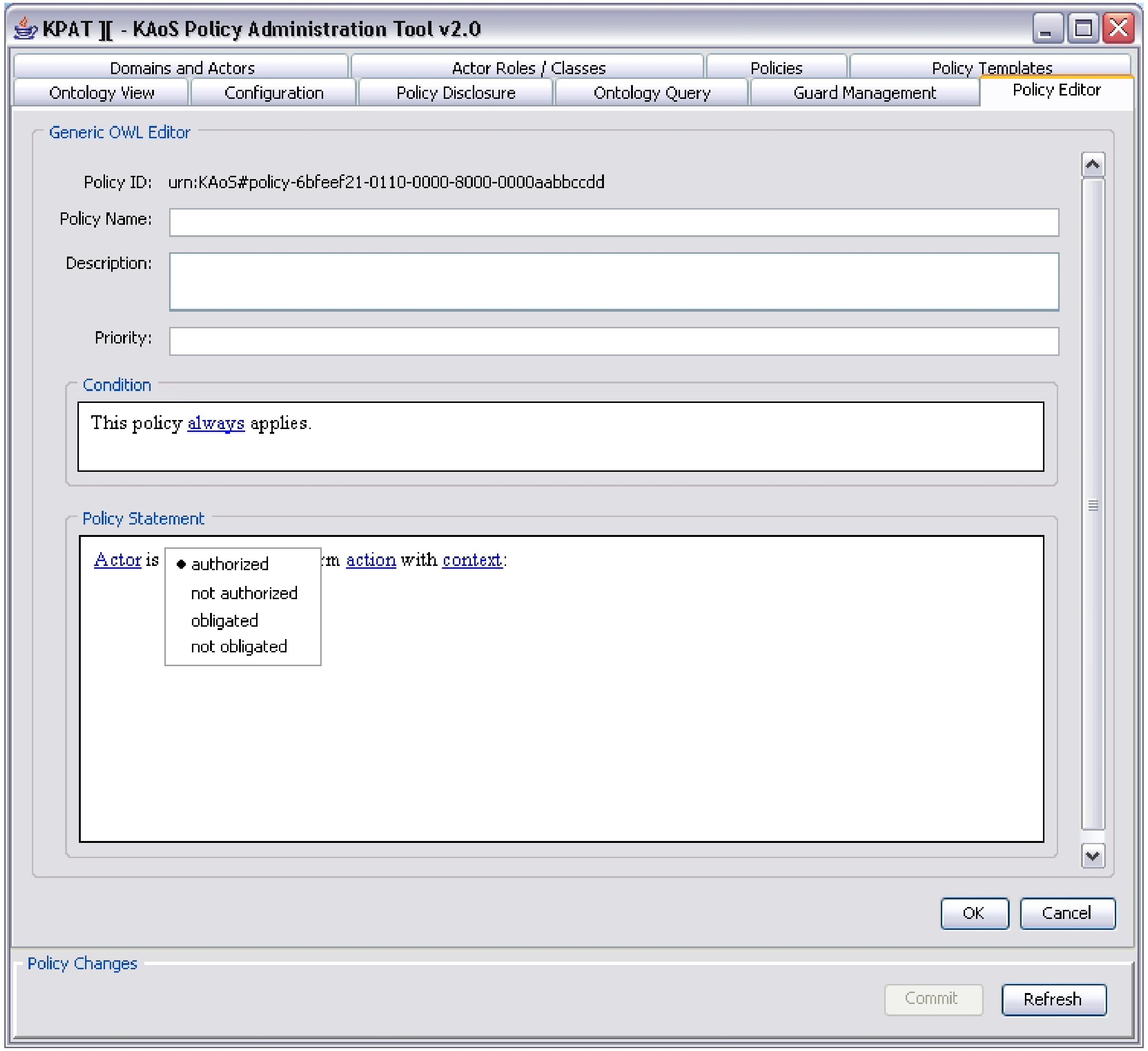
```
<?xml version="1.0" ?>
<!DOCTYPE P1 [
      <!ENTITY policy  "http://ontology.ihmc.us/Policy.owl#" >
      <!ENTITY action  "http://ontology.ihmc.us/Action.owl#" >
      <!ENTITY domains  "http://ontology.ihmc.us/ExamplePolicy/Domains.owl#" >
]>

<rdf:RDF
       xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
       xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
       xmlns:owl="http://www.owl.org/2001/03/owl+oil#"
       xmlns:policy="http://ontology.ihmc.us/Policy.owl#"
>
<owl:Ontology rdf:about="">
       <owl:versionInfo>$ http://ontology.ihmc.us/ExamplePolicy/ACP1.owl $</owl:versionInfo>
</owl:Ontology>

<owl:Class rdf:ID="OutsiteArabelloCommunicationAction">
      <owl:intersectionOf rdf:parseType="owl:collection">
           <owl:Class rdf:about="&action;NonEncryptedCommunicationAction" />
           <owl:Restriction>
                  <owl:onProperty rdf:resource="&action;#performedBy" />
                  <owl:toClass rdf:resource="&domains;MembersOfDomainArabello-HQ" />
           </owl:Restriction>
           <owl:Restriction>
                 <owl:onProperty rdf:resource="&action;#hasDestination" />
                 <owl:toClass rdf:resource="&domains;notMembersOfDomainArabello-HQ" />
           </owl:Restriction>
      </owl:intersectionOf>
</owl:Class>

<policy:NegAuthorizationPolicy rdf:ID="ArabelloCommunicationPolicy1">
      <policy:controls rdf:resource="#OutsiteArabelloCommunicationAction " />
      <policy:hasEnforcementSite rdf:resource="&policy;ActorSite" />
      <policy:hasPriority>10</policy:hasPriority>
      <policy:hasUpdateTimeStamp>446744445544</policy:hasUpdateTimeStamp>
</policy:NegAuthorizationPolicy>
```

KPAT: KAoS Policy Administration Tool — Hides Complexity of OWL

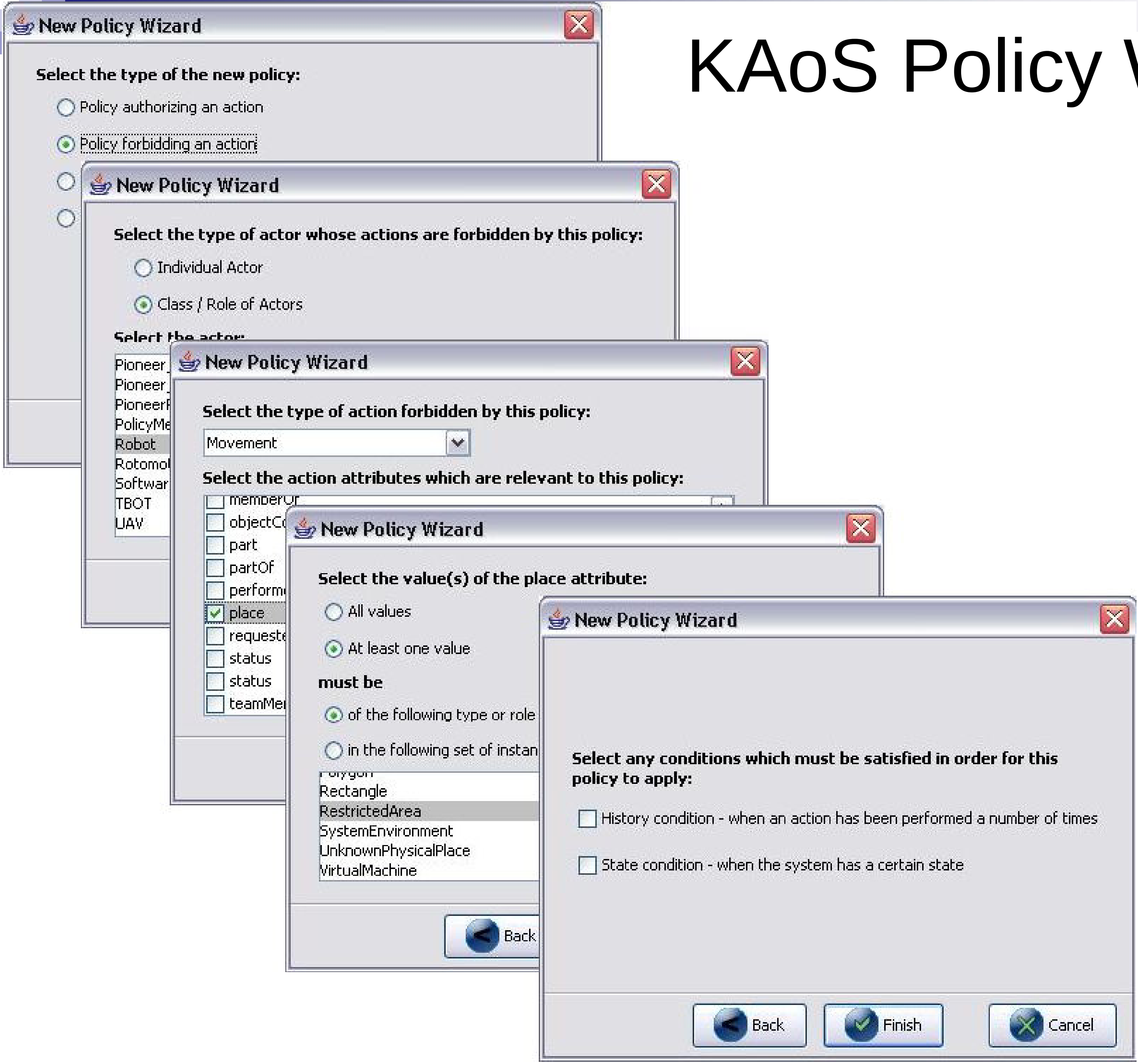


Dynamically obtains list of selections from the ontology repository based on the current context.

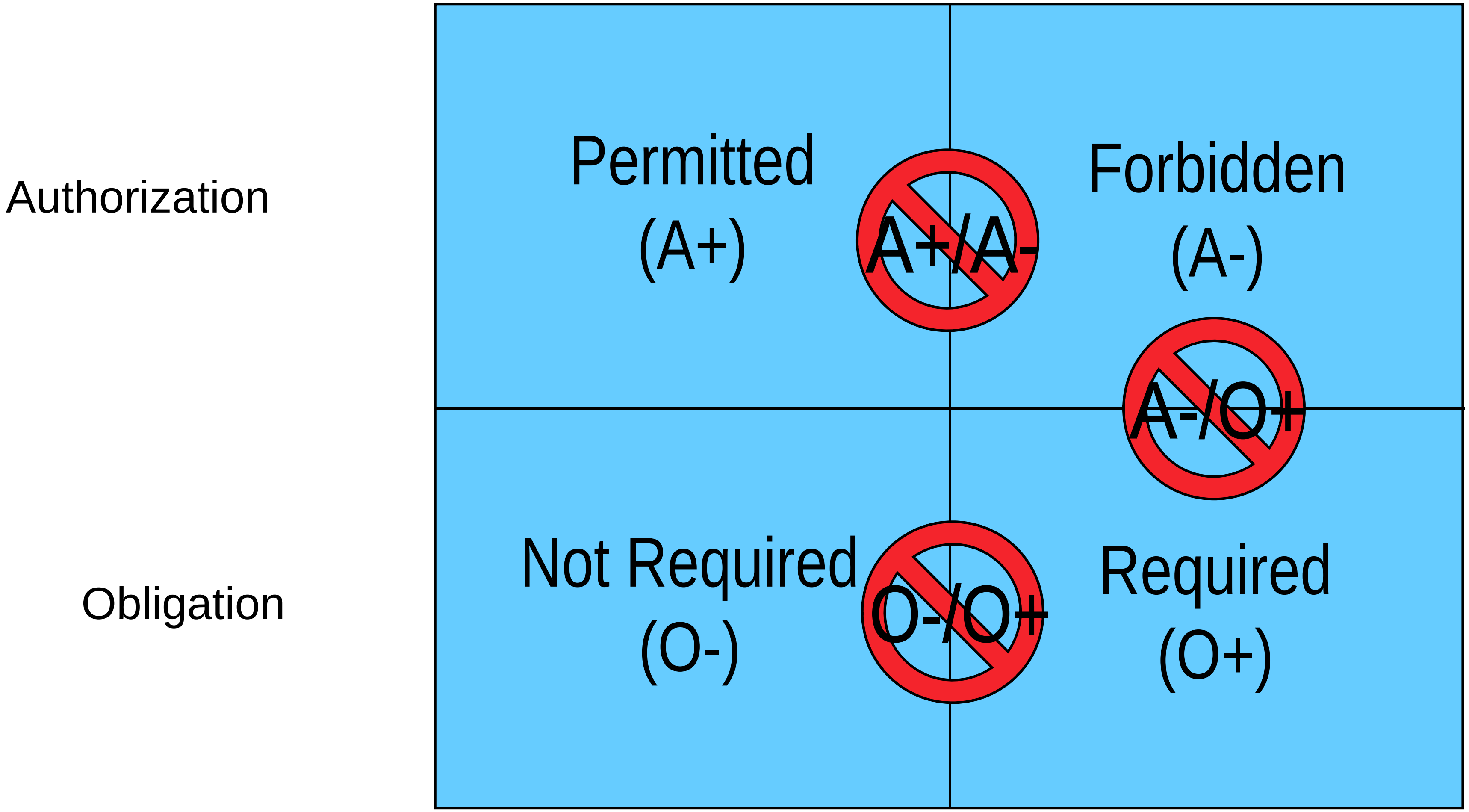
Graphical template editor allows creation of simplified GUIs

Cmap interface (COE) available for ontology definition

KAoS Policy Wizard



Example of KAoS Reasoning: Resolving Three Types of Policy Conflicts



- *Positive vs. negative authorization*: being simultaneously permitted and forbidden from performing action
- *Positive vs. negative obligation*: being both required and not required to perform some action
- *Positive obligation vs. negative authorization*: being required to perform a forbidden action

Policy Analysis (continued)

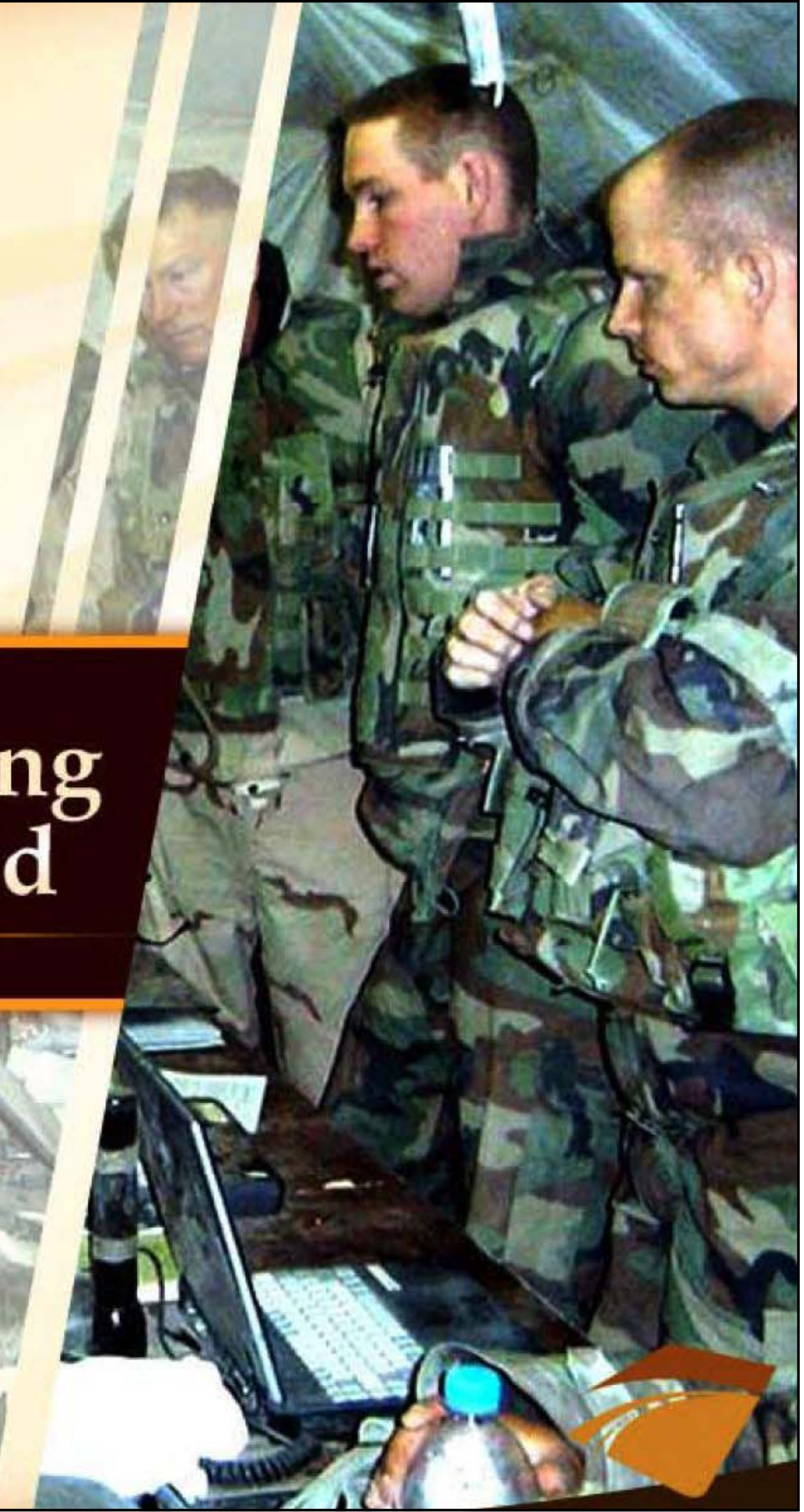
- Evaluate how policies affect actions:
  - ***Test Permission*** – verifies authorization to perform a given action
  - ***Get Obligations*** – gets a list of required actions in a given situation
  - ***Learn Options*** – gets all possible options for a given situation, in the form of properties that will allow the action to be authorized
  - ***Make Compliant*** – transforms a forbidden action into one that can be permitted (in progress)
- Available through KPAT, as a Java API or through remote network calls

INNOVATION AND POLICY ANALYSIS

AT CALIFORNIA STATE UNIVERSITY SAN BERNARDINO

Saving Lives by Delivering Information Soldiers Need

Policy Working Group



One Public Policy Barrier:
Difficulties in Releasing Classified Information that is Sensitive but Perishable

National security policy dictates that certain documents are **classified** and accessible only to the highest levels of command. However, **sensitive but perishable information** could be transformed into **actionable intelligence** and sent into the field to enable the Soldier to "see around corners."

B3AN Demonstration

Technical Objectives

- Show that emerging technologies are capable of representing and reasoning about the complex policies that govern information sharing
- Augment and complement human abilities to share information within policy constraints

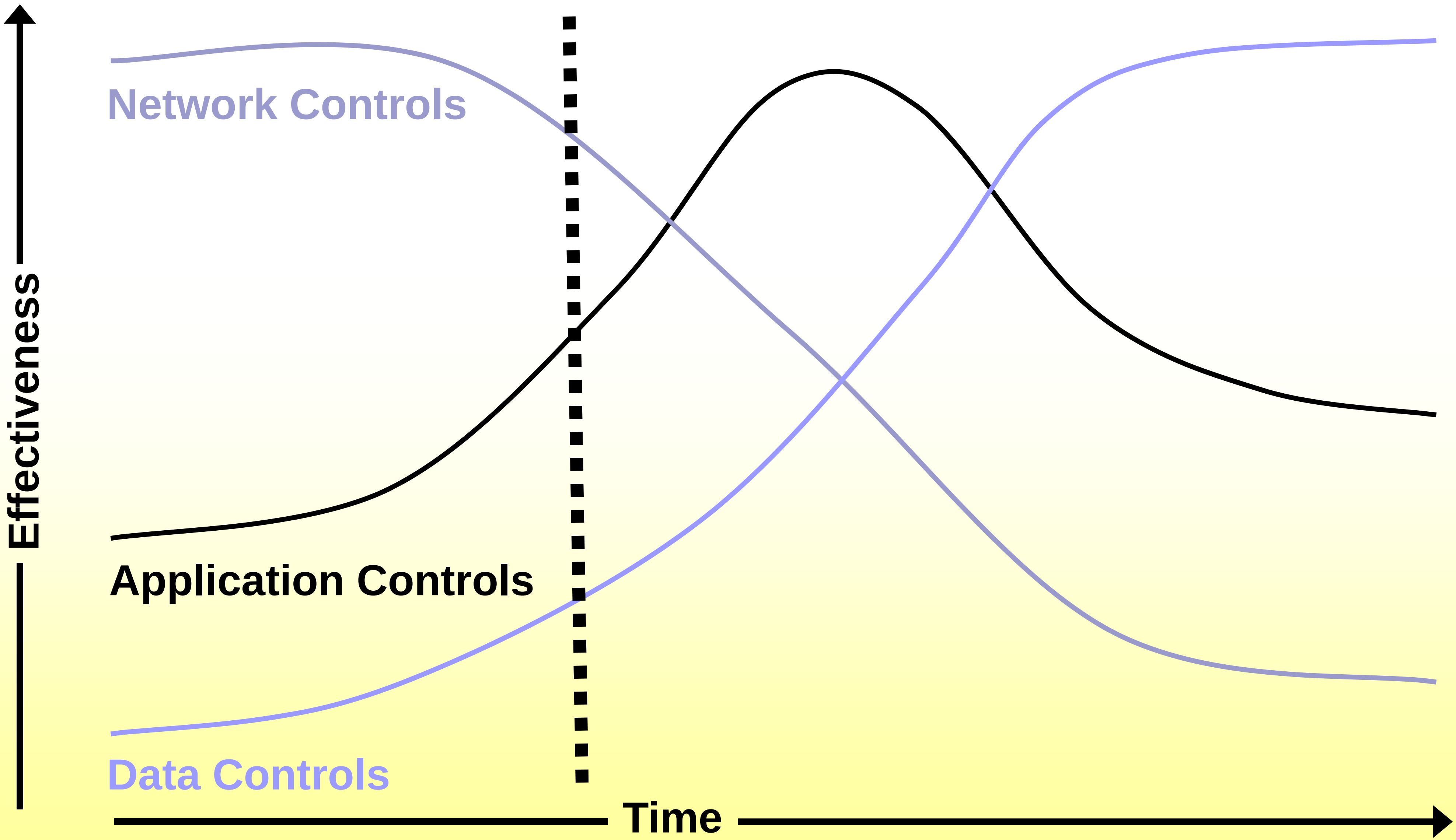
- Operational Objectives
  - Help Soldiers identify the best available information for their mission context
  - Reduce the burden required of Soldiers to understand and comply with information sharing policies
  - Help Soldiers recognize information sharing requirements and opportunities

L. Bunch, *et al.*, Regulating the Cross-Domain Exchange of Tactical Information through Automated Policy Decisions and Enforcement, ARLADA Book Chapter, in press.

B3AN Policy Themes

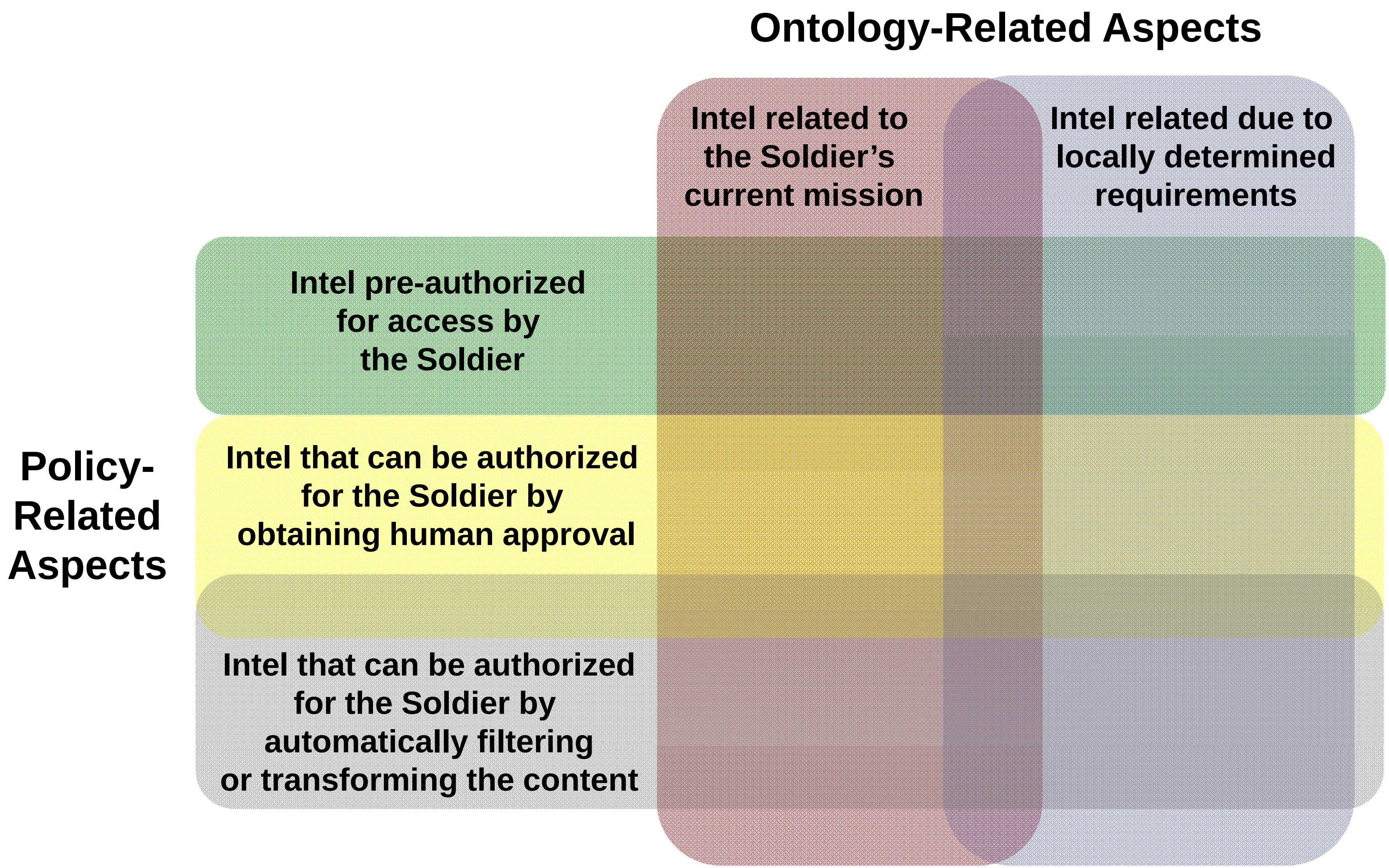
- Policy-governed release of authorized intelligence
- Policy-defined levels of human oversight and approval
  - Can be easily adjusted for greater or lesser degrees of human oversight
- Policy-mandated information sharing
- Policy dynamics in light of new fragmentary orders
  - Semantically-rich policy approach enables responsiveness to changing contexts

Information-Centric Future of Access Controls



See: Dan Hitchcock, Evolution of Information Security Technologies, 2005 at http://movetheworld.wordpress.com

Policy- and Ontology-Related Aspects of Information Sharing Decisions

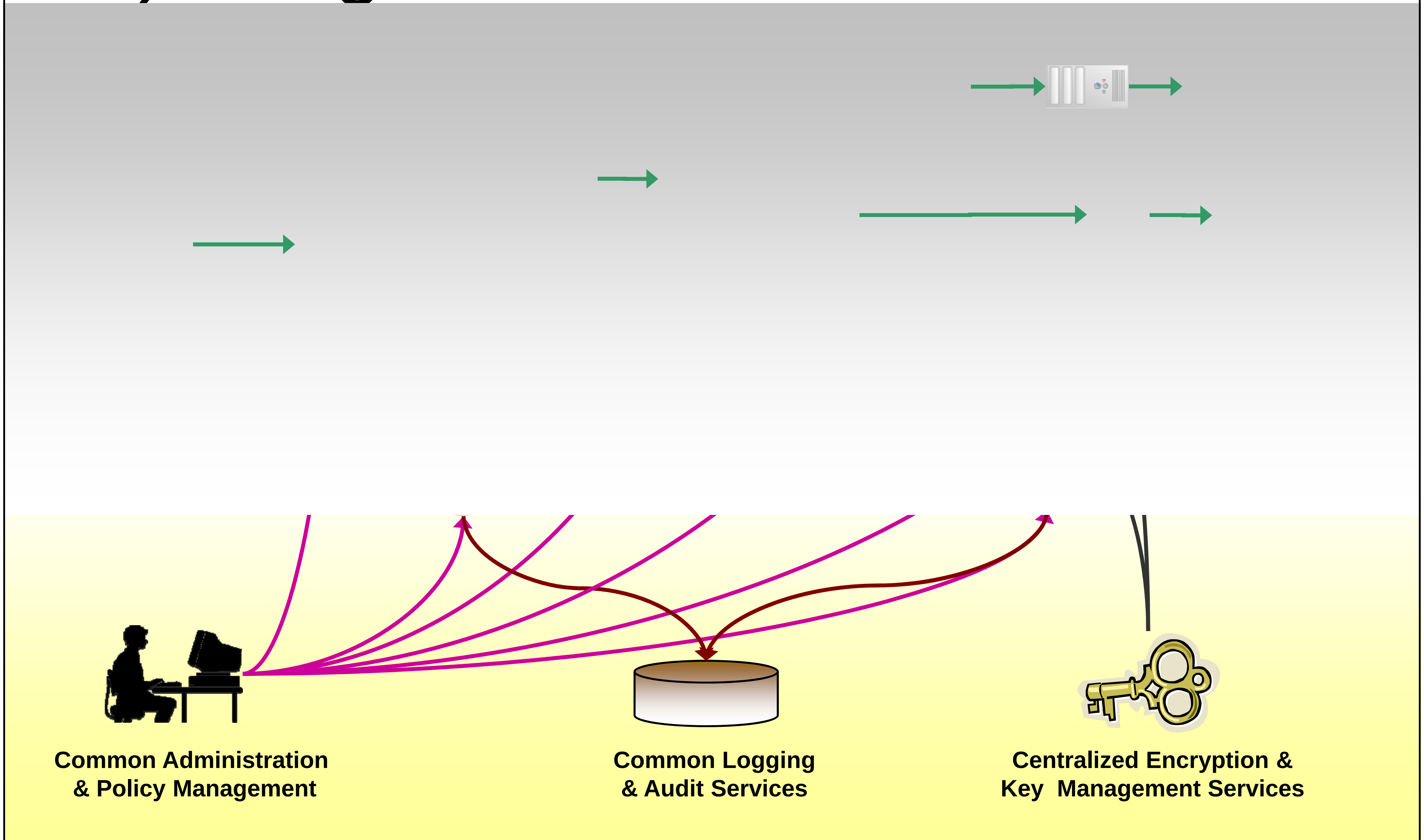


Intelligence products shared with a Soldier in the field must be:
- either pre-authorized, or authorized later through human approval and/or automated filtering
- mission-related and/or related due to locally determined requirements.

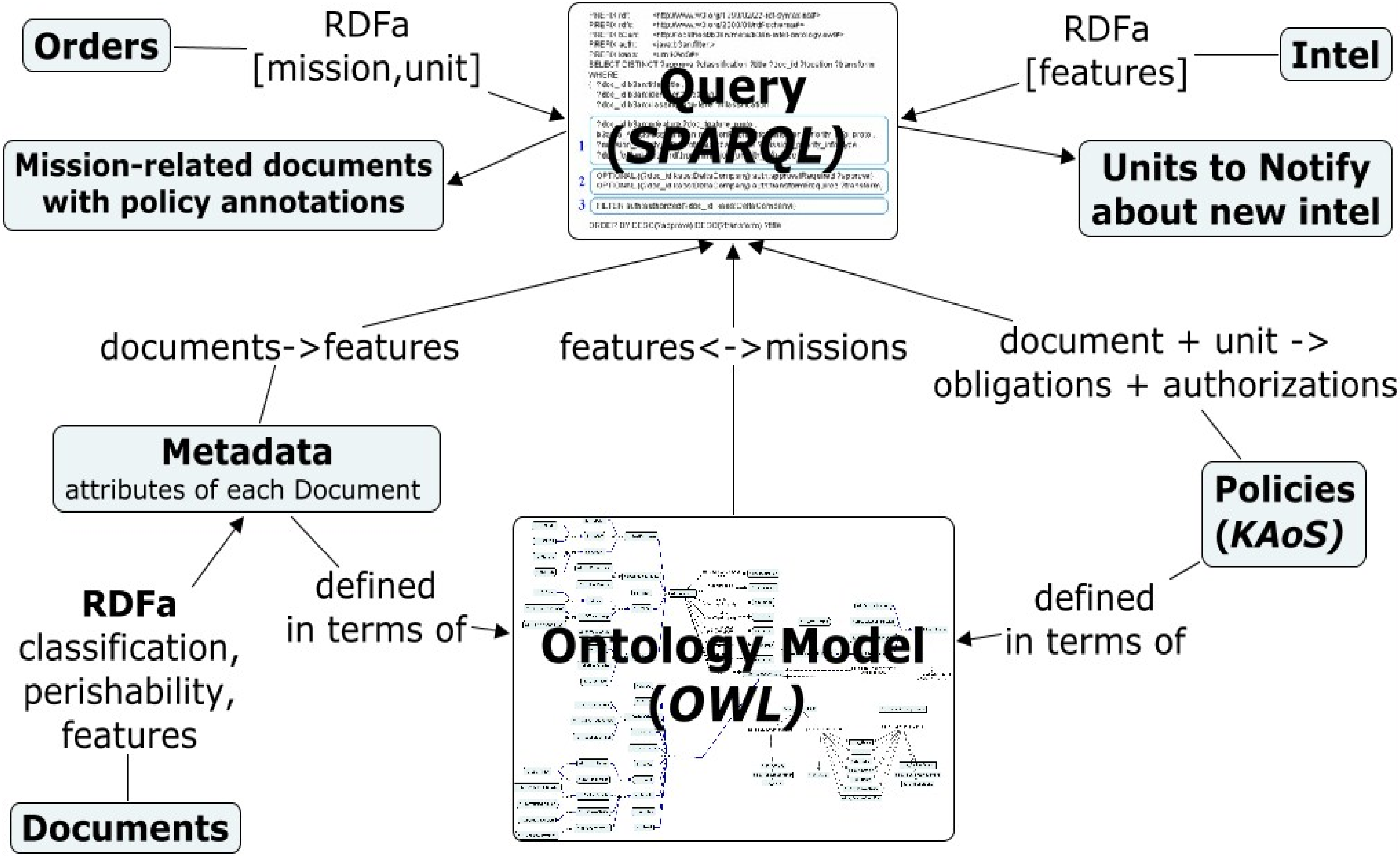
Technical Approach

- Use *RDF* and *RDFa* to make the document attributes extensible and machine-accessible
- Use *OWL* to model relationships between document features and military mission requirements
- Use *KAoS* Policy Services to represent and reason about policies and their contexts
- Use the *SPARQL* query language to search for documents based on the modeled relationships
- Extend SPARQL to
  - enforce KAoS authorization policies during query execution
  - include KAoS obligation policies in query results

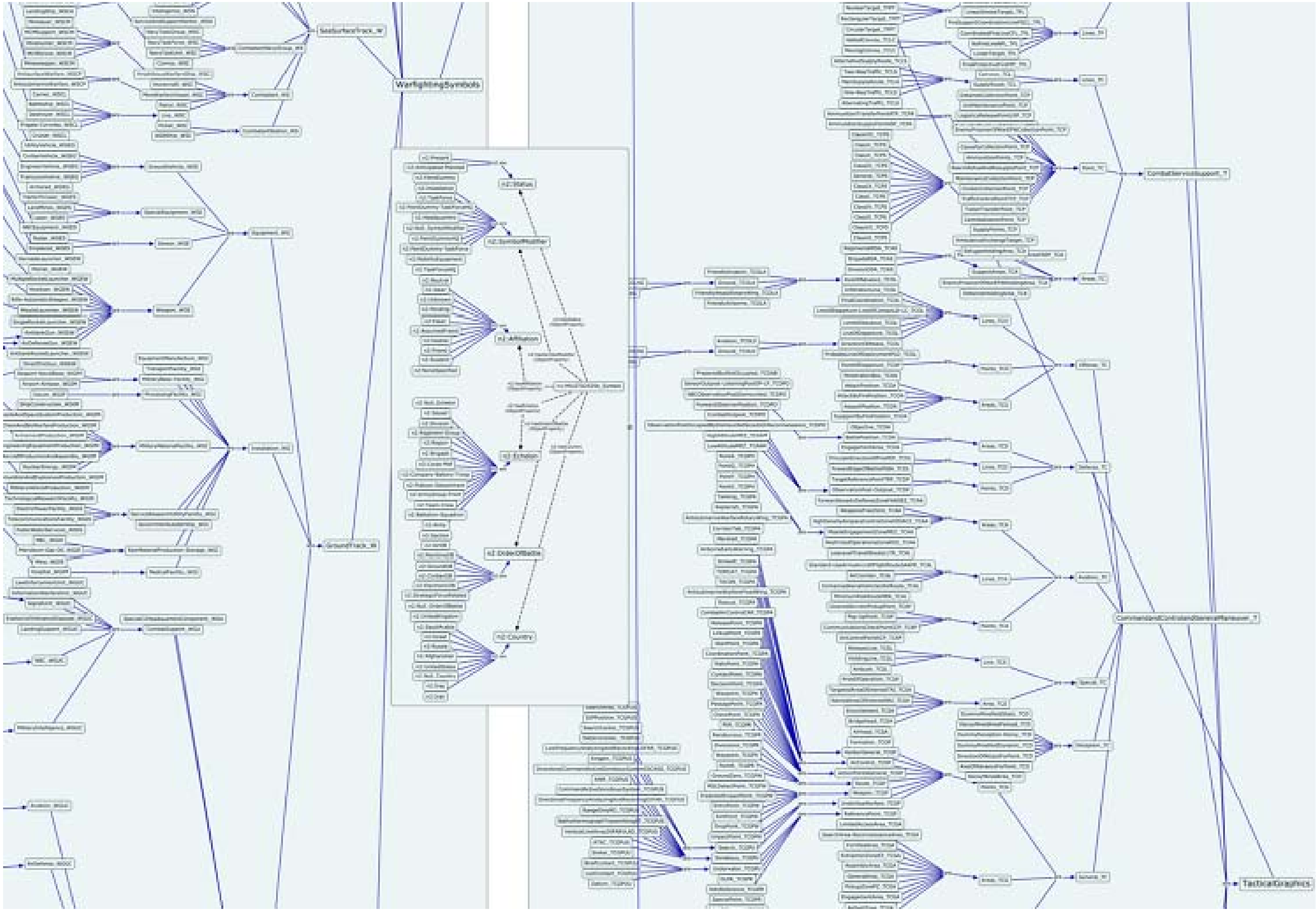
5) Integration



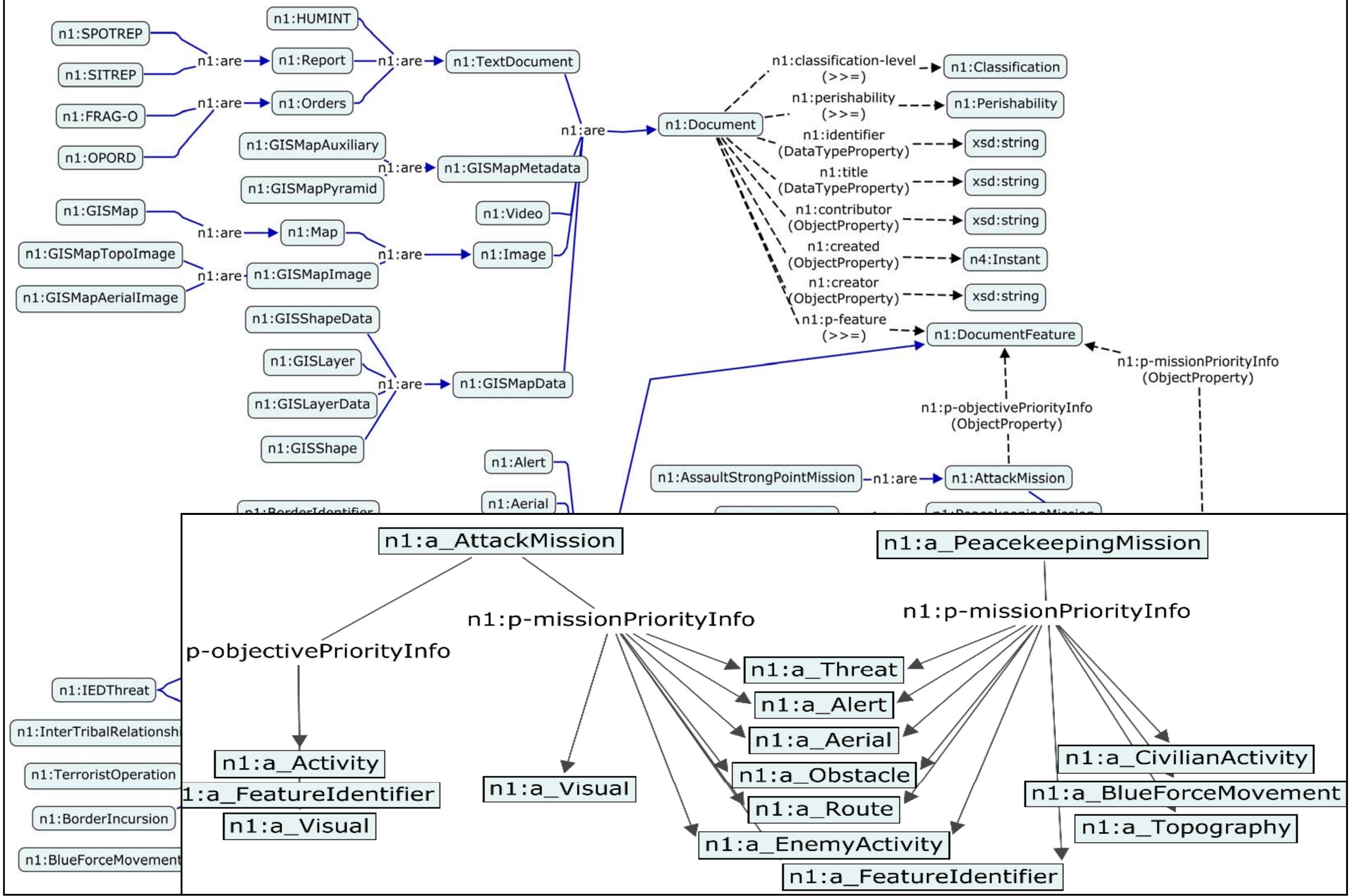
Component Relationships

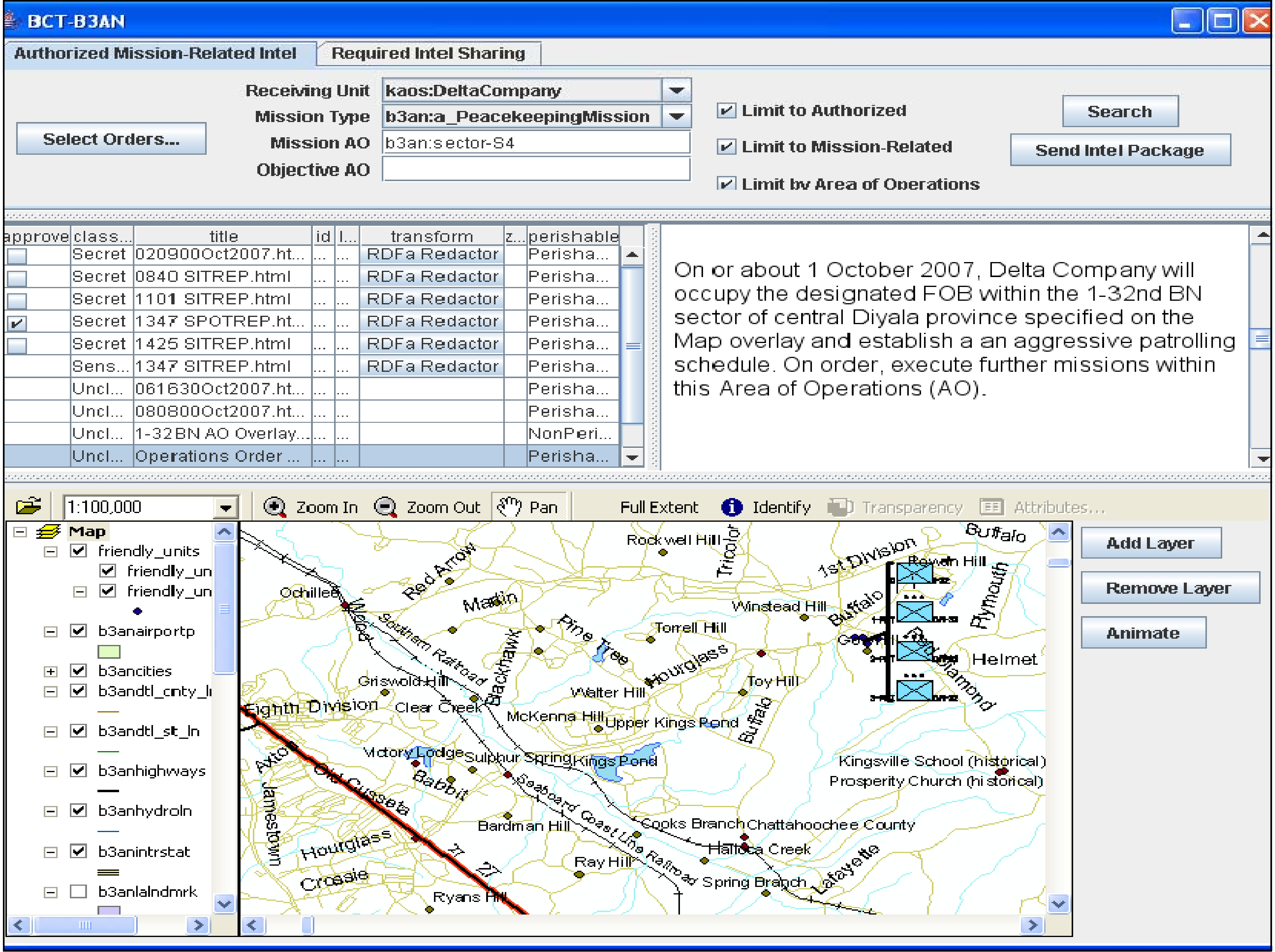


MIL-STD-2525b in OWL



OWL Ontology Relating Missions to Document Features




BCT-B3AN
Authorized Mission-Related Intel
Required Intel Sharing
Receiving Unit
kaos:DeltaCompany
Mission Type
b3an:a_PeacekeepingMission
Mission AO
b3an:sector-S4
Objective AO
Select Orders...
Limit to Authorized
Limit to Mission-Related
Limit by Area of Operations
Search
Send Intel Package
approve
class...
title
id
l...
transform
z...
perishable
Secret
020900Oct2007.ht...
0840 SITREP.html
1101 SITREP.html
1347 SPOTREP.ht...
1425 SITREP.html
Sens...
1347 SITREP.html
Uncl...
061630Oct2007.ht...
080800Oct2007.ht...
1-32BN AO Overlay...
Operations Order ...
RDFa Redactor
Perisha...
NonPeri...
On or about 1 October 2007, Delta Company will occupy the designated FOB within the 1-32nd BN sector of central Diyala province specified on the Map overlay and establish a an aggressive patrolling schedule. On order, execute further missions within this Area of Operations (AO).
1:100,000
Zoom In
Zoom Out
Pan
Full Extent
Identify
Transparency
Attributes...
Map
friendly_units
friendly_un
friendly_un
b3anairportp
b3ancities
b3andtl_cnty_l
b3andtl_st_ln
b3anhighways
b3anhydroln
b3anintrstat
b3anlalndmrk
Add Layer
Remove Layer
Animate
Rockwell Hill
Tricolor
Buffalo
1st Division
Rowan Hill
Red Arrow
Odhillee
Martin
Winstead Hill
Plymouth
Torrell Hill
Pine Tree
Hourglass
Helmet
Southern Railroad
Blackhawk
Toy Hill
Griswold Hill
Walter Hill
Eighth Division
Clear Creek
McKenna Hill
Upper Kings Pond
Victory Lodge
Sulphur Spring
Kings Pond
Kingsville School (historical)
Prosperity Church (historical)
Babbit
Old Cusseta
Jamestown
Bardman Hill
Seaboard Coast Line Railroad
Cooks Branch
Chattahoochee County
Hourglass
Hallaca Creek
Ray Hill
Lafayette
Crossie
Spring Branch
Ryans Hill

Key Benefits

- Policy-governed information sharing
  - Rapid context-driven access to authorized mission-related intelligence
  - Assured policy compliance
  - Assured information sharing
  - Appropriate levels of human oversight and approval

- Potential Operational Benefits
  - Faster information package preparation
  - More complete information (drawing upon a broader base)
  - More mission-focused information (semantically filtered)

- Fulfilling the need to share
  - More information sharing
  - More focused information sharing

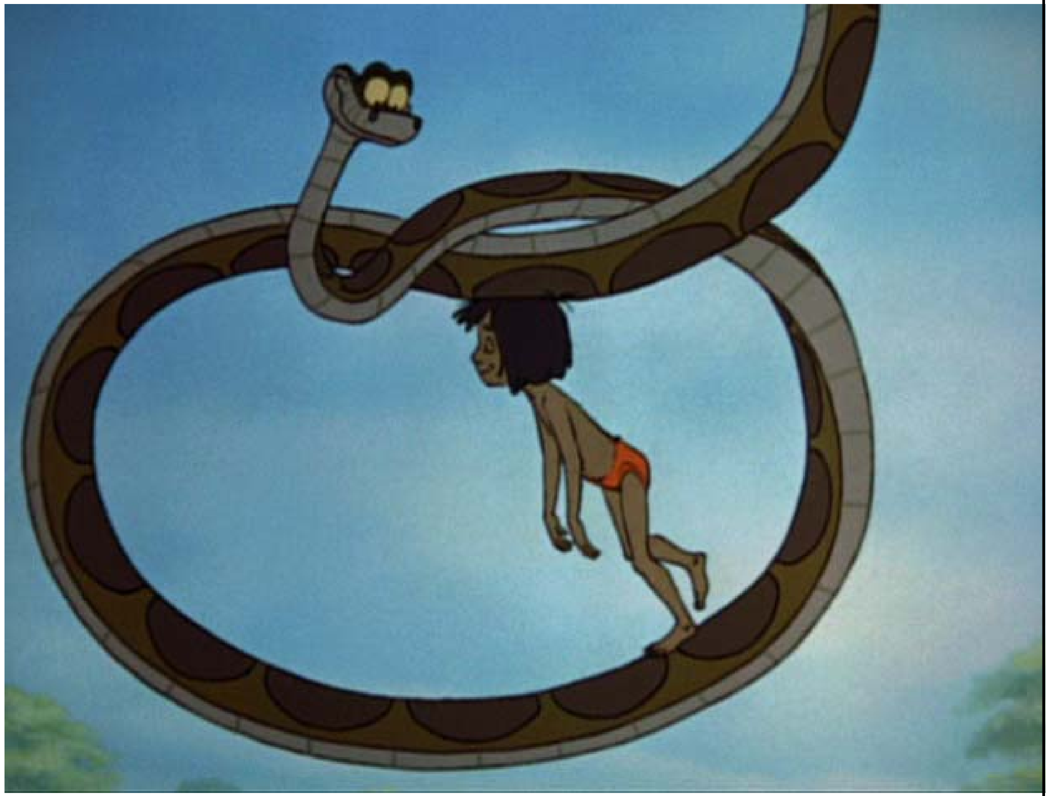
Current Areas of R&D

- Adjustable autonomy
- Policy precedence
- Policy refinement
- Collective obligations
- Policy learning

Kaa: KAoS adjustable autonomy

- **Adjustable autonomy**
  - Ability to impose and modify constraints that affect the range of actions available (authorizations) and required (obligations)
  - Intent of adjustment is to lead to measurably better overall performance of the system in a given context

- **Kaa**
  - Support for adjustable autonomy
    - Considers costs and benefits of various alternatives for adjustment
    - Adjusts constraints accordingly
    - Example: Risk-adaptive access control for the GIG



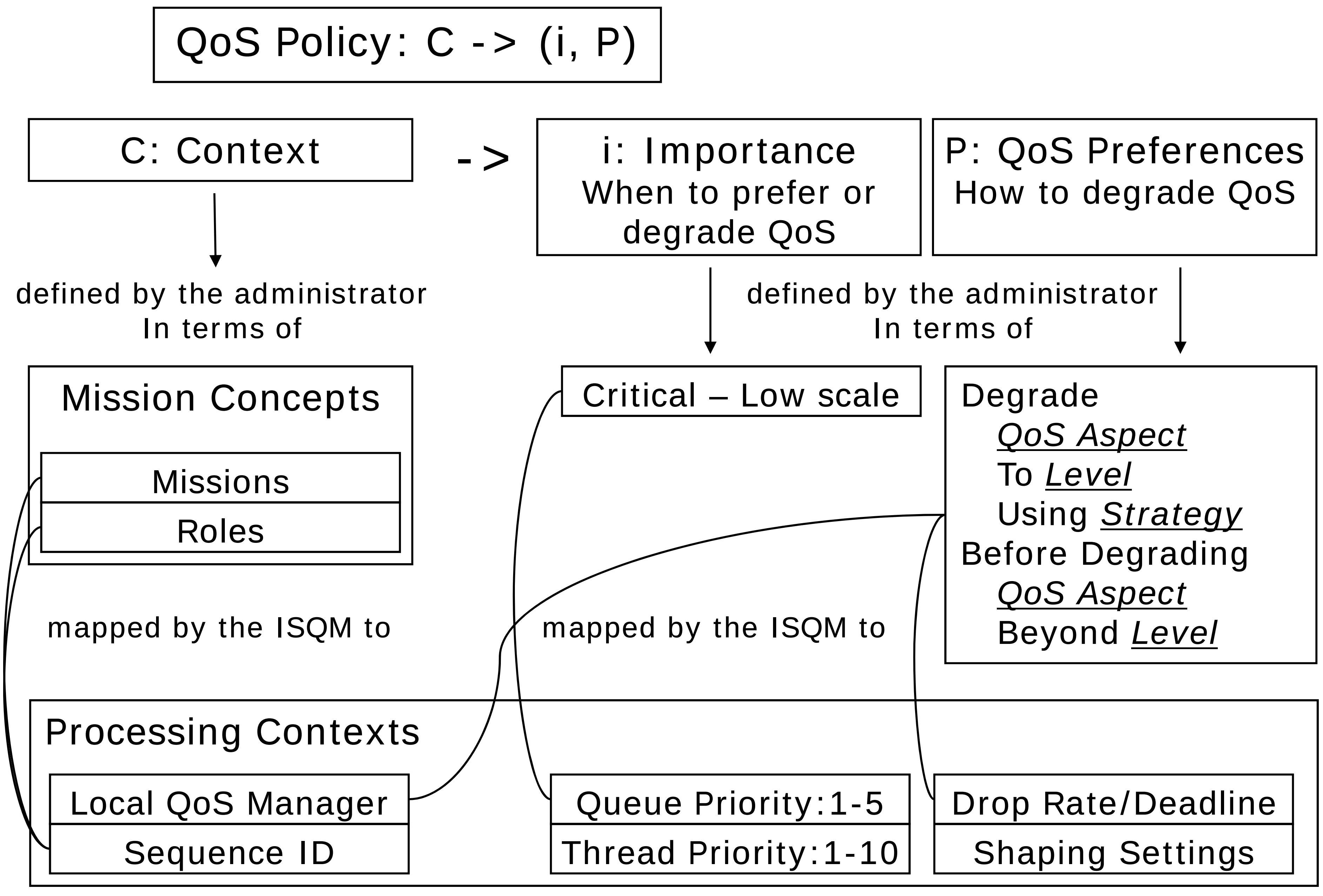
Bradshaw, J. M., Jung, H., Kulkarni, S., Johnson, M., Feltovich, P., Allen, J., Bunch, L., Chambers, N., Galescu, L., Jeffers, R., Suri, N., Taysom, W., & Uszok, A. (2005). Toward trustworthy adjustable autonomy in KAoS. In R. Falcone *et al.* (Eds.), *Trusting Agents for Trustworthy Electronic Societies.* LNAI. Berlin: Springer

Policy Precedence Specification

- New policy mechanism will allow flexible runtime specification of which policies or sets of policies take precedence. Examples:
  - Name or role
    - Policies defined by Victor take precedence over anyone else’s policies
    - Policies of the domain administrator take precedence over user policies
  - Time when the policy was created
    - More recent policies take precedence over older policies
  - Relative scope of class of the policy subject
    - Superdomain policies take precedence over subdomain policies
    - Policies for Device X take precedence over policies for the device class
  - Relative scope of the class of policy action
    - Policies about writing to a specific directory take precedence over policies about writing to the volume
    - Policies about Mobility (in general) take precedence over policies about Forward Movement
  - Modality of the policy
    - Negative authorizations take precedence over positive authorizations
  - Priority level of the policy (e.g., numeric, high-medium-low)

KAoS Policy Refinement

- Goal oriented requirements engineering
  - Ensure that operation of the system matches high-level objectives
    - Capture administrator intent
  - Generate lower-level policies from higher-level ones
    - Decompose policies relevant to a composite system into a set of policies that are executed in its constituent parts to implement the behavior intended by the overall system level policy
    - The resultant more specific policies are better suited for use in different execution environments.
- Example: AFRL QoS Enabled Dissemination (QED)


QoS Policy: C -> (i, P)
C: Context
->
i: Importance
When to prefer or degrade QoS
P: QoS Preferences
How to degrade QoS
defined by the administrator
In terms of
defined by the administrator
In terms of
Mission Concepts
Missions
Roles
Critical – Low scale
Degrade
QoS Aspect
To Level
Using Strategy
Before Degrading
QoS Aspect
Beyond Level
mapped by the ISQM to
mapped by the ISQM to
Processing Contexts
Local QoS Manager
Sequence ID
Queue Priority:1-5
Thread Priority:1-10
Drop Rate/Deadline
Shaping Settings

Collective Obligations in KAoS

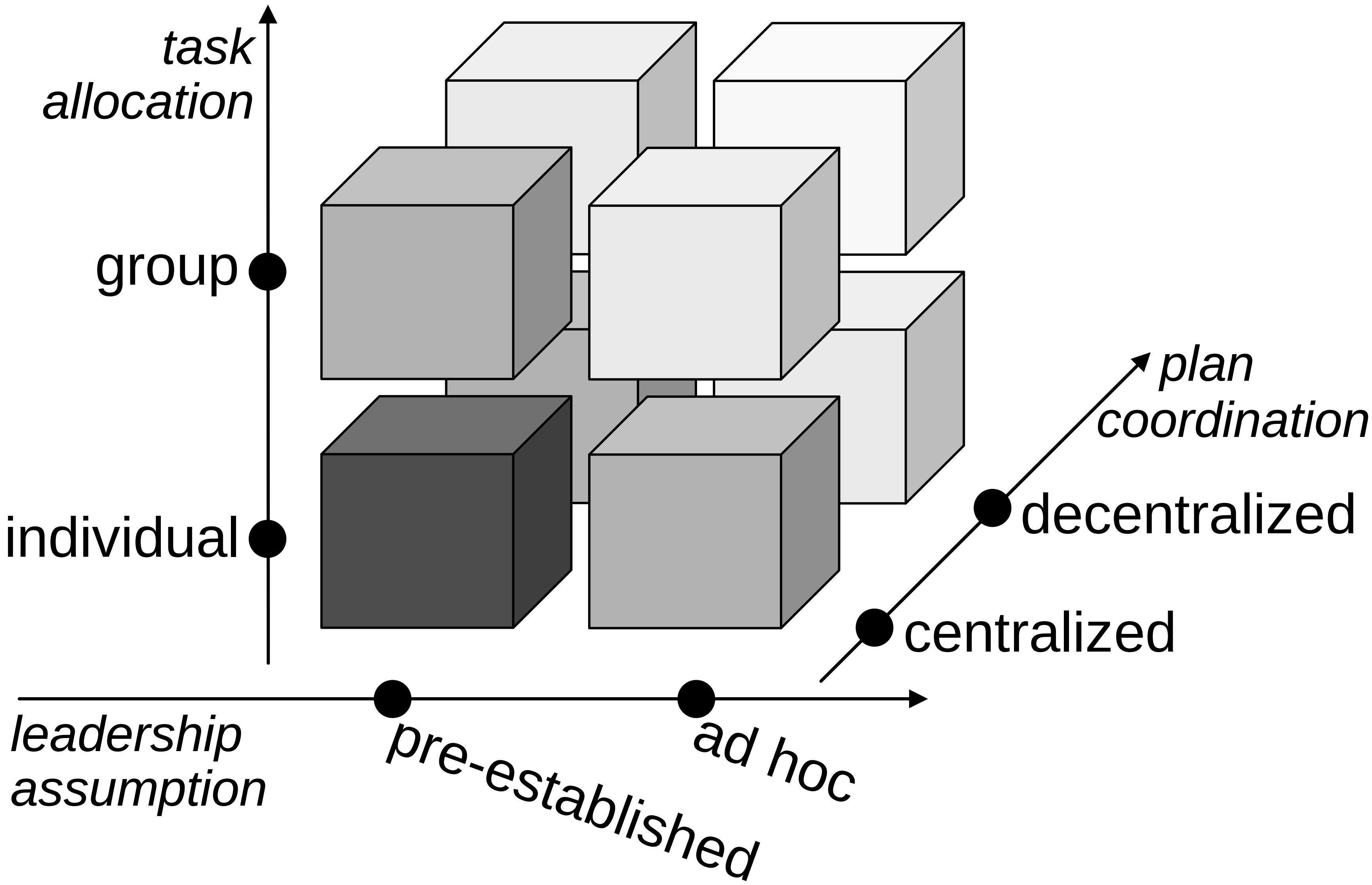
- An *individual obligation* describes what must be done by a particular individual
- A *collective obligation* (CO) describes what must be done by a team of agents, without specifying who must do what

Example

the *MECA-team* must *ensure-safety* of its members after a *safety-critical-event* has occurred

van Diggelen, J., Bradshaw, J.M., Johnson, M. & Feltovich, P. 2008. Fulfilling collective obligations in human-agent teams using KAoS policies, in press.

Dimensions of Team Design



Policy Learning

- Domain Independent Learning Methods
- Domain Dependent Learning Methods
- Population-based Evaluation/Sharing

- Building capabilities into core KAoS framework

Policy Learning Applications

- First Prototype
  - Logistics domain
    - Learn policies to choose shippers to use for each supply type
    - Based on Rehak, M., M. Gregor, et al. (2006). Representing Context for Multiagent Trust Modeling. Proceedings of the IEEE/WIC/ACM international conference on Intelligent Agent Technology, IEEE Computer Society.
- New Industry-Funded Tasks
  - Cognitive Radios
    - Learn policies to choose spectrum, configuration given environment and regulatory guidelines

Summary

- Collaboration requires support for “responsibility to share” in addition to “need to know”
- New trends require richer policy semantics that go beyond XML-based approaches
  - Need for greater expressiveness, flexibility, and extensibility
  - Multi-layer integration vs. niche policy representations
  - Runtime reasoning, adaptation, and learning
  - Deperimeterization and the information-centric future of access control
- OWL provides a mature standards-based migration pathway for the future

Implications for Cloud Computing

- The long term business driver for cloud computing is collaboration
  - Variety of cloud computing services
  - Complexity of information protection issues
  - New Collaboration-Oriented Architectures
- Need for rich semantics to dynamically describe and manage resources, information, people, situations, and policies in a common, secure, formally-described yet human-accessible manner

More Information

- http://ontology.ihmc.us
- jbradshaw@ihmc.us