SOPES Overview (final revised submission)

Presented: June 2009

Michael Abramson, President, ASMG Ltd.

Jean-Claude Lecomte, V-P, ASMG Ltd.

OBJECT MANAGEMENT GROUP

ASMG
ADVANCED SYSTEMS MANAGEMENT GROUP

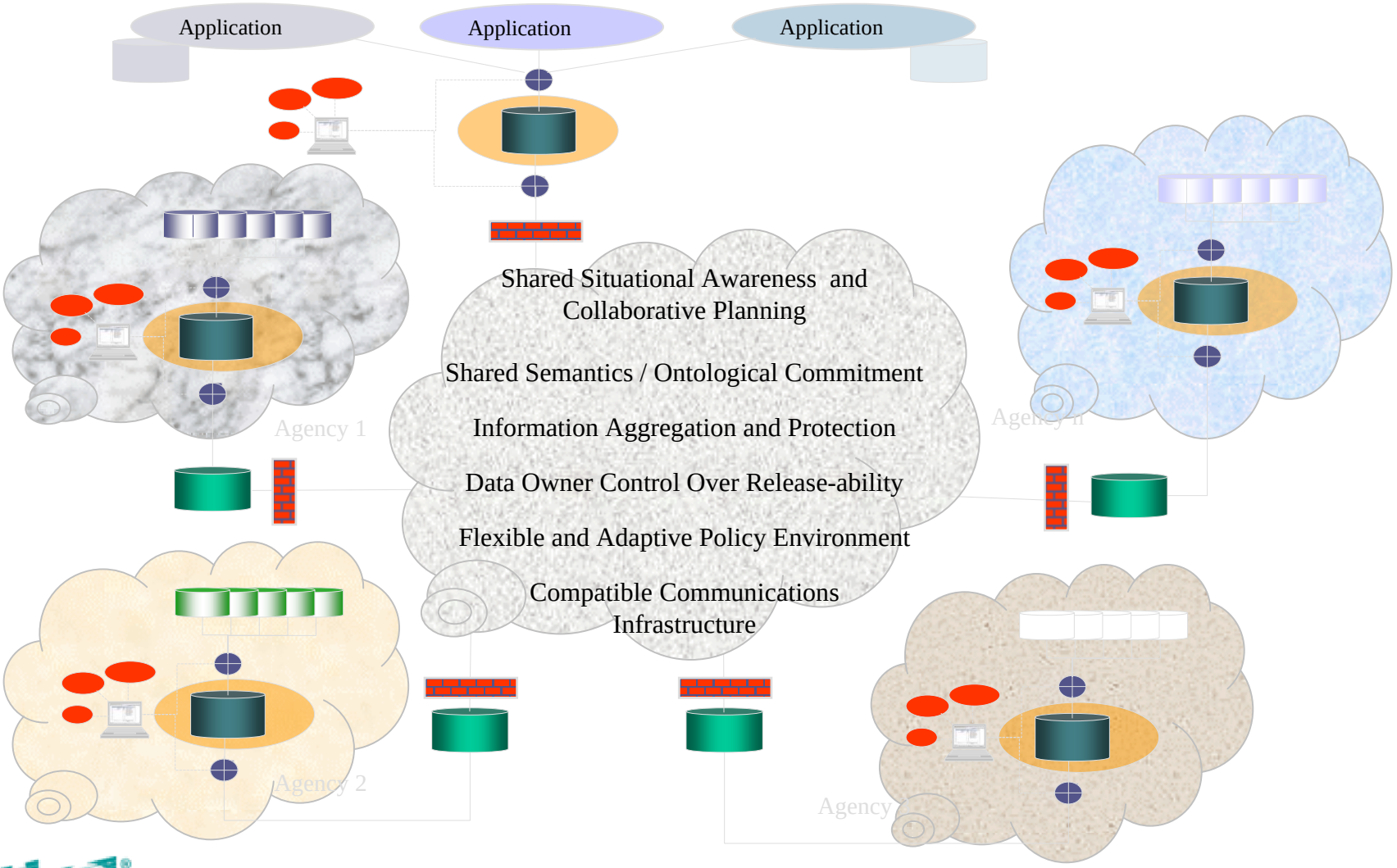
The Operational Challenge

- Rigid and brittle information systems; lacking information quality; and security
  - Growing requirement for dynamic and adaptive information systems
    - Adapt to the changing context of the operational environment with embedded security
    - Adapt to changing coalitions, interagency coalitions and Communities of Interest
    - Adapt to dynamic real-world events in near real-time
    - Provide event (new data) change global update
- Poor Information Quality and Availability
  - Growing requirement for significant improvements in information quality
    - Accurate: information that conveys the true situation.
    - Relevant: information tailored to specific requirements of the mission, role, task or situation at hand.
    - Timely: information is provided in time to make decisions.
    - Useable: information presented in a common, easily understood format.
    - Complete: information that provides all necessary (or available) information needed to make decisions.
    - Brief: information tailored to the level-of-detail required to make decisions and reduces data overload.
    - Trusted: information quality and content can be trusted by stakeholders, decision makers and users.
    - Secure: Information is protected from inadvertent or malicious release to unauthorized participants.
- Overly Complex IT environments
  - Collapse the number single domain networks into one virtual MLS domain

"We can't solve problems by using the same kind of thinking we used when we created them."

Albert Einstein

Interoperability Challenge



OBJECT MANAGEMENT GROUP

ASMG ADVANCED SYSTEMS MANAGEMENT GROUP

Objectives

- Improve shared situational awareness and collaborative planning capability in coalition and multi-agency operations;
- Increase interoperability within and between organizations, systems and applications;
- Facilitate the implementation and deployment of capability to meet the emerging requirements of stakeholders and users;
- Enable the exploitation of community information assets;
- Improve the quality of information Control the spiraling life-cycle costs of information systems and technology;
- Improve the management of private, confidential and sensitive information; and
- Increase flexibility, agility and adaptability in deployed information systems.

Information Quality

- **Accuracy**: semantics to accurately convey the perceived situation.
- **Relevance**: information tailored to specific requirements of the mission, role, task or situation at hand.
- **Timeliness**: information flow required to support key processes, including decision making.
- **Usability**: information presented in a common, easily understood format.
- **Completeness**: information that provides all necessary (or available) information needed to make decisions.
- **Brevity**: information tailored to the level-of-detail required to make decisions and reduces data overload.
- **Trustworthiness**: information quality and content can be trusted by stakeholders, decision makers and users.
- **Protected**: Information is protected from inadvertent or Malicious Release

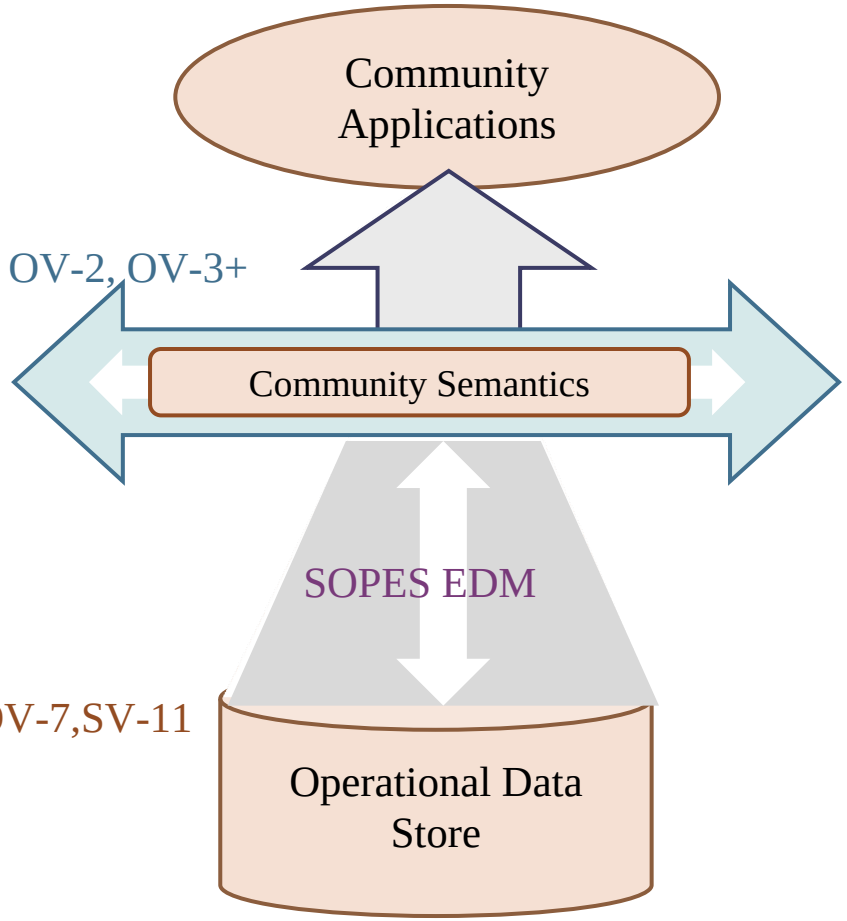
Architecture Driven Interoperability (SOPES Exemplar)

User Semantics
User Syntax and Structure

Community Exchange Agreement
Community Semantics
Community Exchange Syntax and Format
Community Exchange Protocol

Construction / Processing Plans / Info Patterns
Guard and Filtering Constraints
Construction Constraints

Information Store Taxonomy
Information Store Business Rules
Information Store Attributes / Data Elements
Meta Tags and Labels
Information Element relationships
GUIDs and DBKeys



Data in use

Data in Motion

Data at Rest

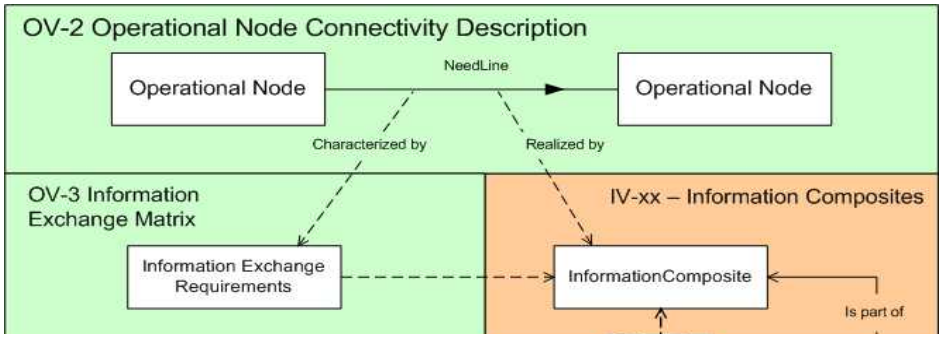
Exemplar
JC3IEDM

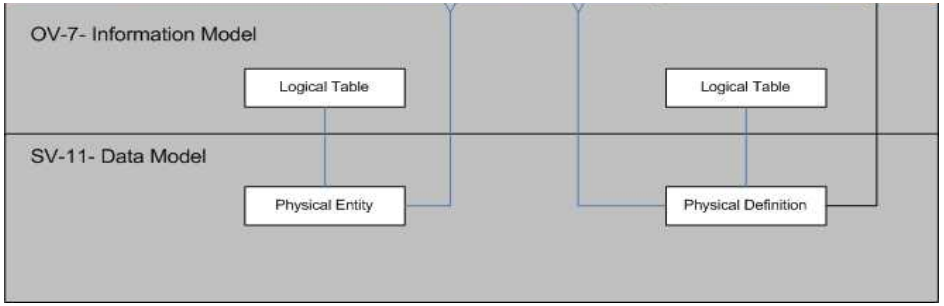
OBJECT MANAGEMENT GROUP

ASMG ADVANCED SYSTEMS MANAGEMENT GROUP

OV-37 Overview

- Aligned to UPDM and DODAF
- Glues existing views together
- Provides Information Focus
- Defines the policies and business rules for processing (constructing / marshalling) data
- Focussing on reusable data patterns for an underlying data store
- Targeting platform independence





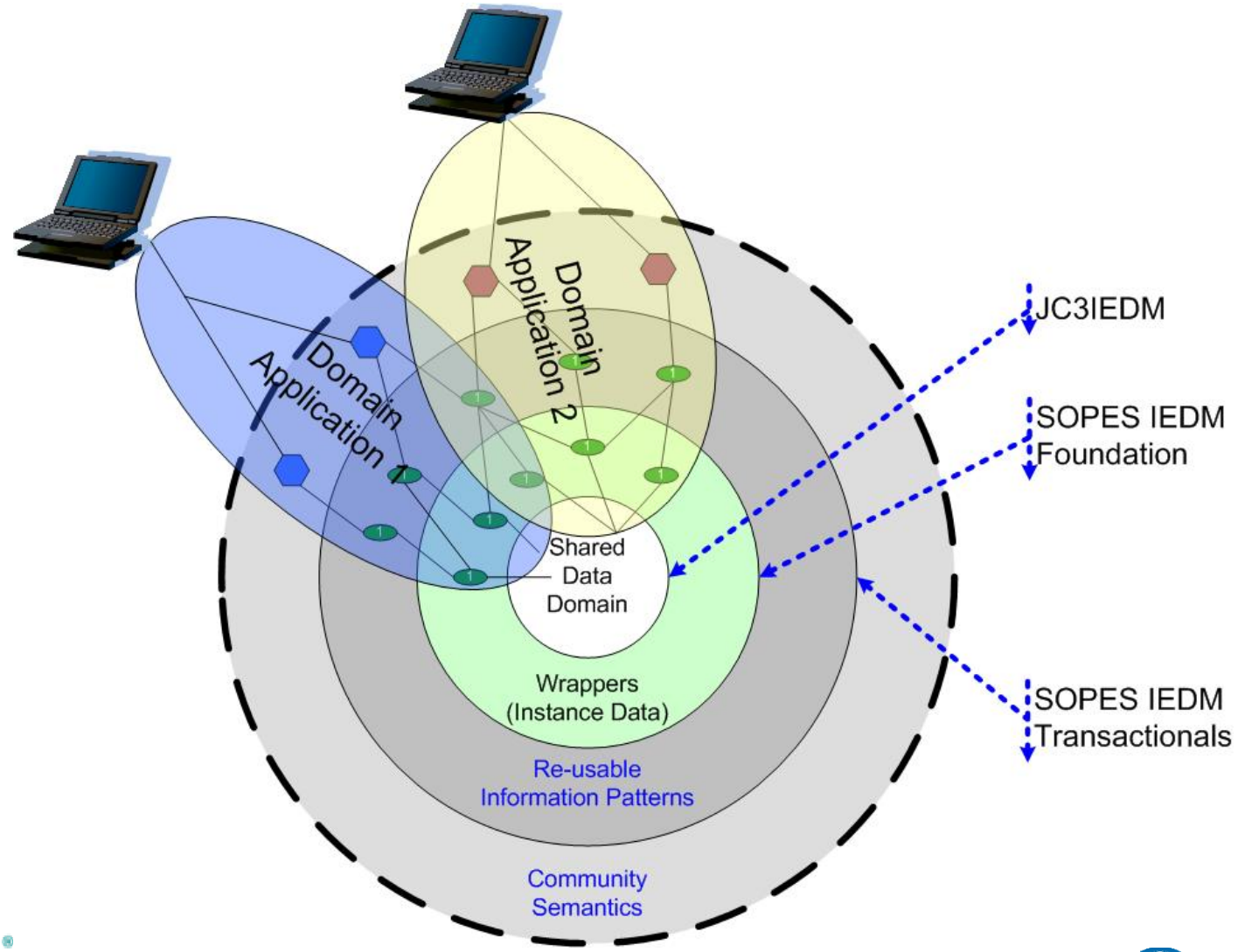
OBJECT MANAGEMENT GROUP

ASMG ADVANCED SYSTEMS MANAGEMENT GROUP

OV-37: Alignment to Architecture Views (UPDM 2.x)

OV-37	Reallocate Views	Description
OV-37a – Contact View	OV-3b	Aligns the OV-2/3 with the OV-7
OV-37b – Community Semantics View	IV-3a	Aligns the available data patterns of the OV
OV-37c – Transactional View	IV-3b	Defines a set of reusable information patterns based on the information elements and structures defined by the OV-7 or SV-11.
OV-37d – Wrapper View	IV-3c	Documents Information Element instance data from the OV-7 or SV-11
OV-37b1 & c1: Filtering View or View point	SecV-xx	Adds filters and constraints to the OV-37b and/or 37c
OV-37b1 & c1: Transformation View or View point	IVxx and/or SecV-xx	Adds methods and attribution to the to the OV-37b and/or 37c to document data transformation and/or security label processing
OV-37e: GuardSemantic	SecV-xx	Enabling the modeling of information guards from complex information patterns that carry sensitivity, security or confidentiality restrictions.

Shared Data Patterns



OBJECT MANAGEMENT GROUP

ASMG ADVANCED SYSTEMS MANAGEMENT GROUP

Changes Since Last Release

- Integrated of MDA generated OCL into the UML Model
- Navigation constraints for Generalizations
- Editorial Clean-up based on:
  - DND
  - DoD
  - MIP

Document Structure

- **Section 1**: presents the introduction to the specification.
- **Section 2**: provides an introduction to the consultation, command and control information domain and the JC3IEDM.
- **Section 3**: provides a description of the Conformance and Compliance requirements for those organizations developing information applications based on this specification
- **Section 4**: lists the reference documents which form an integral part of this standard
- **Section 5**: provides the design rationale for the SOPES IEDM PIM and PSMs
- **Section 6**: illustrate several of the problem domains in which the SOPES IEDM is applicable
- **Section 7**: overviews the organization of the SOPES IEDM
- **Section 8:** SOPES Transactional Model
- **Section 9:** Exemplar Semantics

SOPES IEDM Annexes

- **Annex A**: UML modeling profile used in this Specification
- **Annex B**: Wrapper Class Descriptions
- **Annex C:** SOPES Transactional Model Details
- **Annex D**: SOPES IEDM XSD PSM – provides the XML PSM for the SOPES IEDM
- D1: Verbose XSD
- D2: Optimized XSD
- **Annex E:** JAVA Platform Specific Model
- **Annex F:** Compliance Matrix
- **Annex G**: Glossary
- **UML Model**: Enterprise Architect Project file: 20090525_SOPES_IEDM_Revision(Final Revised).EAP

SOPES Data Patterns

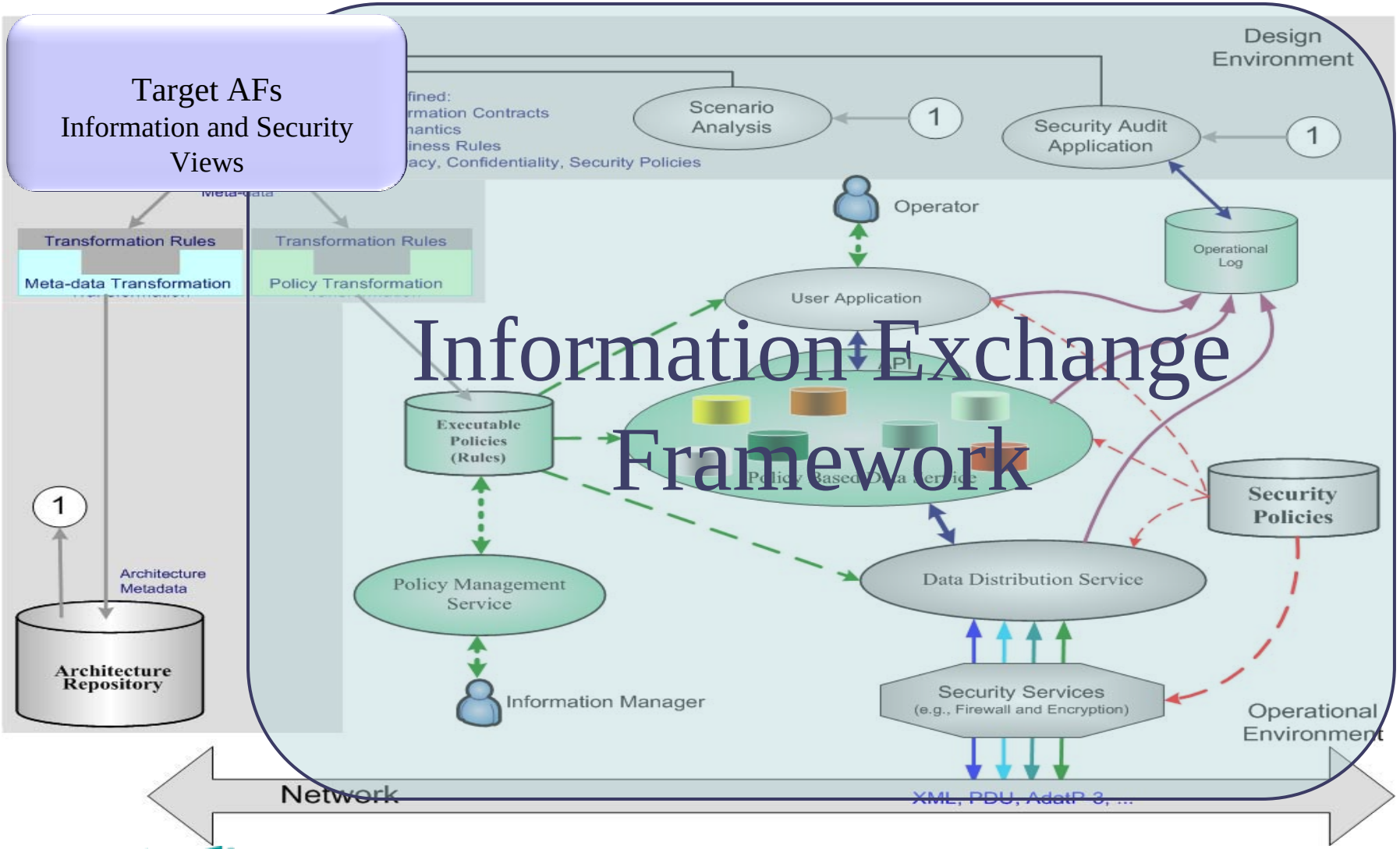
- 190 Shared Data patterns based on the JC3IEDM Business Rules
- These patterns cover the following 16 subject areas:
  - Actions (45);
  - Capabilities (6);
  - Context (12);
  - Control Features (6);
  - Facilities (22);
  - Geographical Features (5);
  - Holdings (2);
  - Locations (22);
  - Materiel (9);
  - Meteorological Features (2);
  - Object Item (11);
  - Object Type (6);
  - Organization (20);
  - Personnel (7);
  - Plans & Orders (13); and
  - Reporting (2).
- Providing 100% coverage of the JC3IEDM Tables

JAVA PSM

The skeleton does not contain:

- Integration code for the community application interfaces;
- Integration code for the selected distribution mechanisms;
- Integration with a selected data management system;
- Exception handling.

Positioning The SOPES IEDM



OBJECT MANAGEMENT GROUP

ASMG ADVANCED SYSTEMS MANAGEMENT GROUP

Q & A

Michael Abramson
Advanced Systems Management Group Ltd
265 Carling Ave, Suite 630, Ottawa
613-567-7097 x222

Jean-Claude Lecomte
Advanced Systems Management Group Ltd
265 Carling Ave, Suite 630, Ottawa
613-567-7097 x222

Operational Prototype

- Enterprise Information Security Environment Project
- Department of National Defence
- Demonstration December 2009

Operational Prototype Objectives

Develop a prototype for an operational environment that demonstrates the following elements of the EISE mandate:

- The use of security architecture to directly support operations;
- The use of ontology in the development of information protection services;
- The use of architecture to enhance the security profile of operational systems;
- The use of architecture to enable policy based information sharing and protection;
- The demonstration of architecture-driven, policy-based information aggregation, filtering and transformation;
- The demonstration of architecture-driven, policy-based information sharing;
- The integration of ontology into security architecture; and
- The use of architecture to increase the flexibility, adaptability, agility and cost-effectiveness (lower life-cycle costs) of information sharing and protection solutions.
- Risk Mitigate

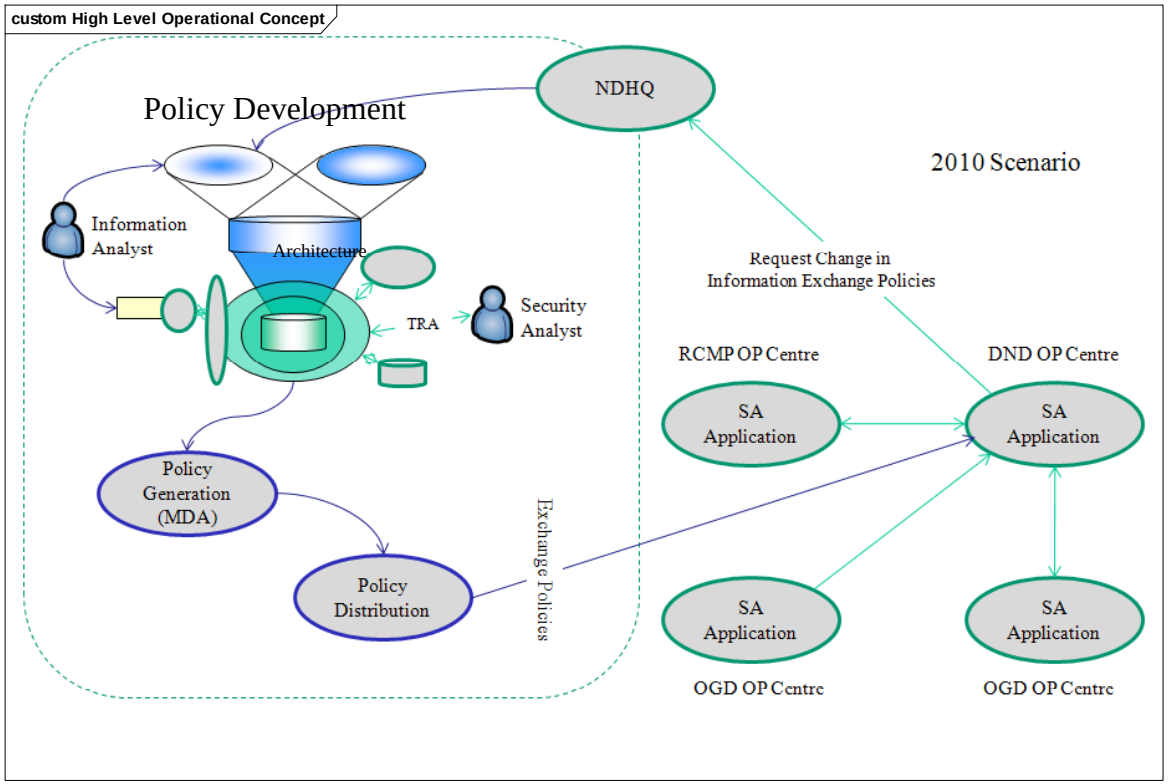
Directly from the CV-1 description of the Operational Prototype

Rules, Criteria, and Conventions

- EISE seeks to employ open architecture, standards and software wherever possible.
- EISE seeks to demonstrate the benefits of policy based systems and applications.
- EISE seeks to demonstrate the benefits of architecture driven solutions.

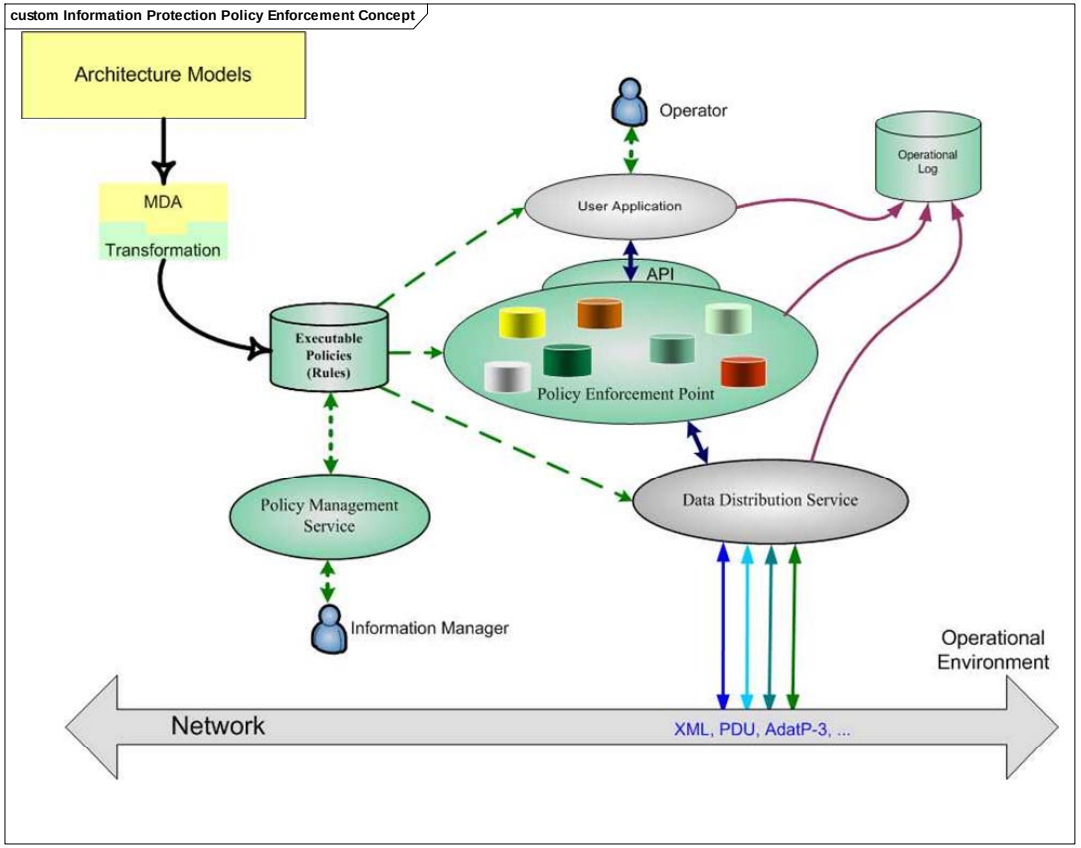
OV: 1 Operational Concept

- Progressive increase in the need to share information between GC agencies as the scenario evolves
- Several of the changes to information requirements will fall within SOPs and the changes made at the nodes
  - Demonstrate local control
  - Demonstrate remote or central control
  - Requirement to share information not supported by SOPs
  - Modify Architecture Models
  - Initiate Situational Risk Assessment
  - Reject Initial Policy Change
  - Add filters to policy to restrict data release and reduce potential sensitivity of release-able Data
  - Approval given to the new information sharing policy
  - Executable rules are generate and issues to the Policy management station in the MOC
  - Policies are received and instantiated on the MOC Operational Node
  - Additional information shared with the RCMP Operational Node



OV1: Policy Driven Information Sharing and Protection

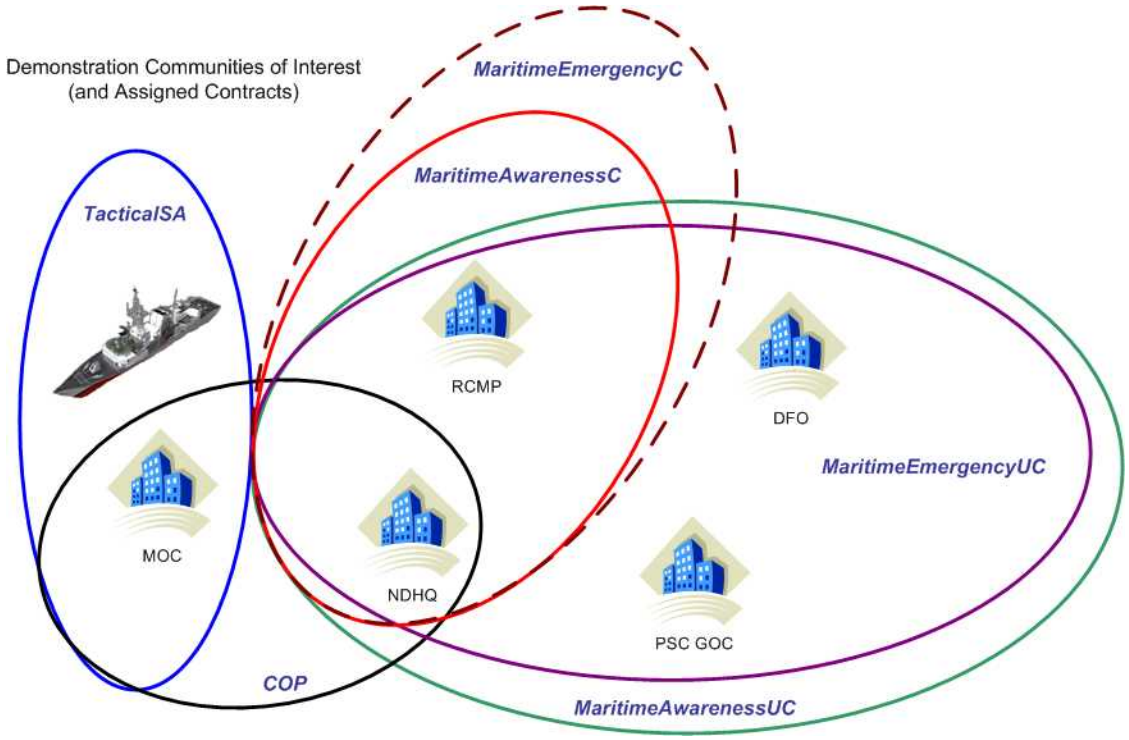
- Architecture Models are converted to Executable Rules based on an MDA transformation (Serialized Meta Objects for this demonstration). Architecture Views Include:
  - OV-3b – Exchange Contracts
  - IV-3a – Agreed Semantics
  - IV-3b – Data Store Transactionals
  - IV-3c – Wrappers for Data Store Tables
  - IV-3b&c models adopted from the SOPES IEDM Specification
- Policies are instantiated on an operational in a policy enforcement point (Adaptive Data Service) the executes and enforces the policies specified in the architecture models
- The Policies can be activated, deactivate, modified within the limits of the architectural model and the delivered policy management interface.
  - Provides local control
  - Provides remote (central) control
  - Distribution provided by a standards based exchange service



Communities of Interest

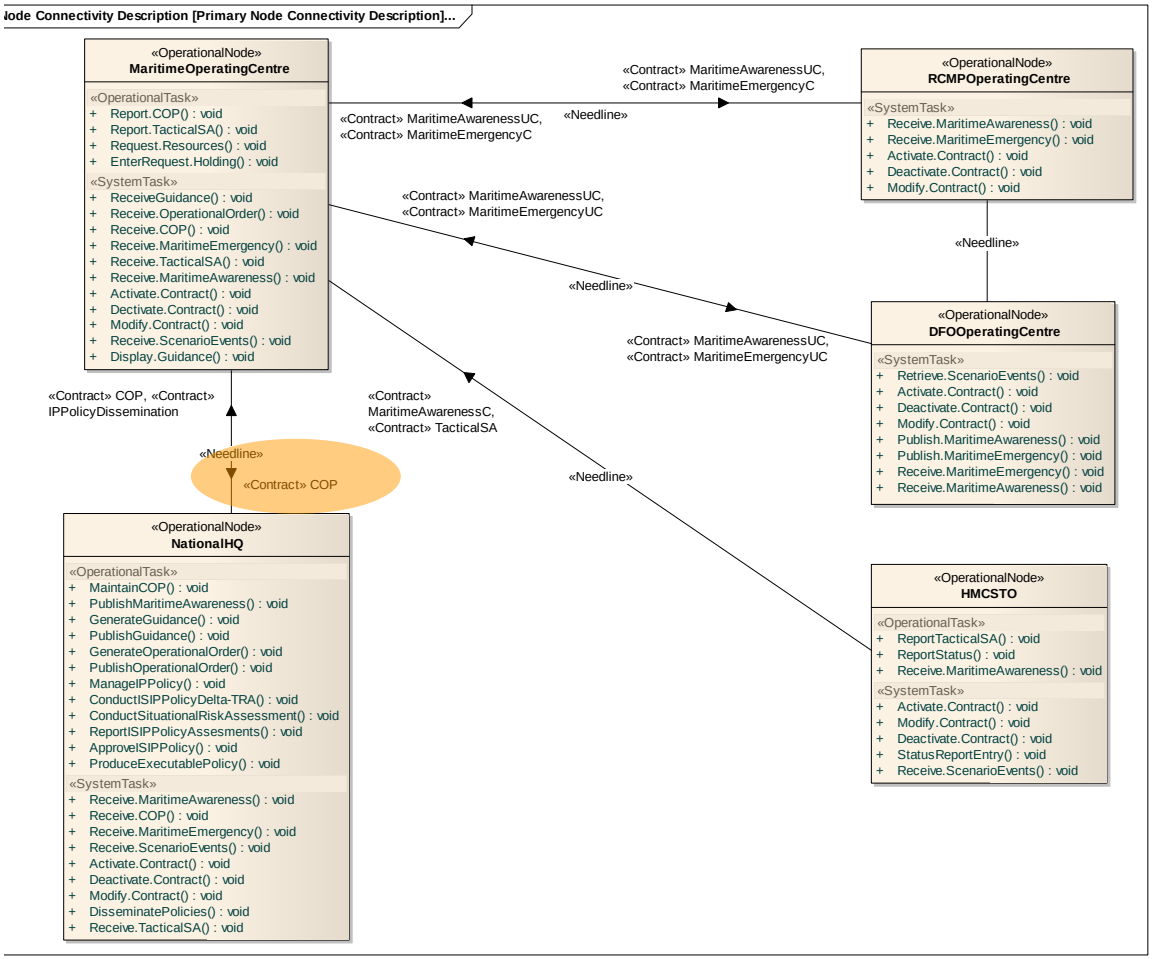
- Model illustrates the grouping of operational nodes that share information on a specific contract

- Identifies
  - Peer-to-Peer Interfaces
  - Multi-cast patterns



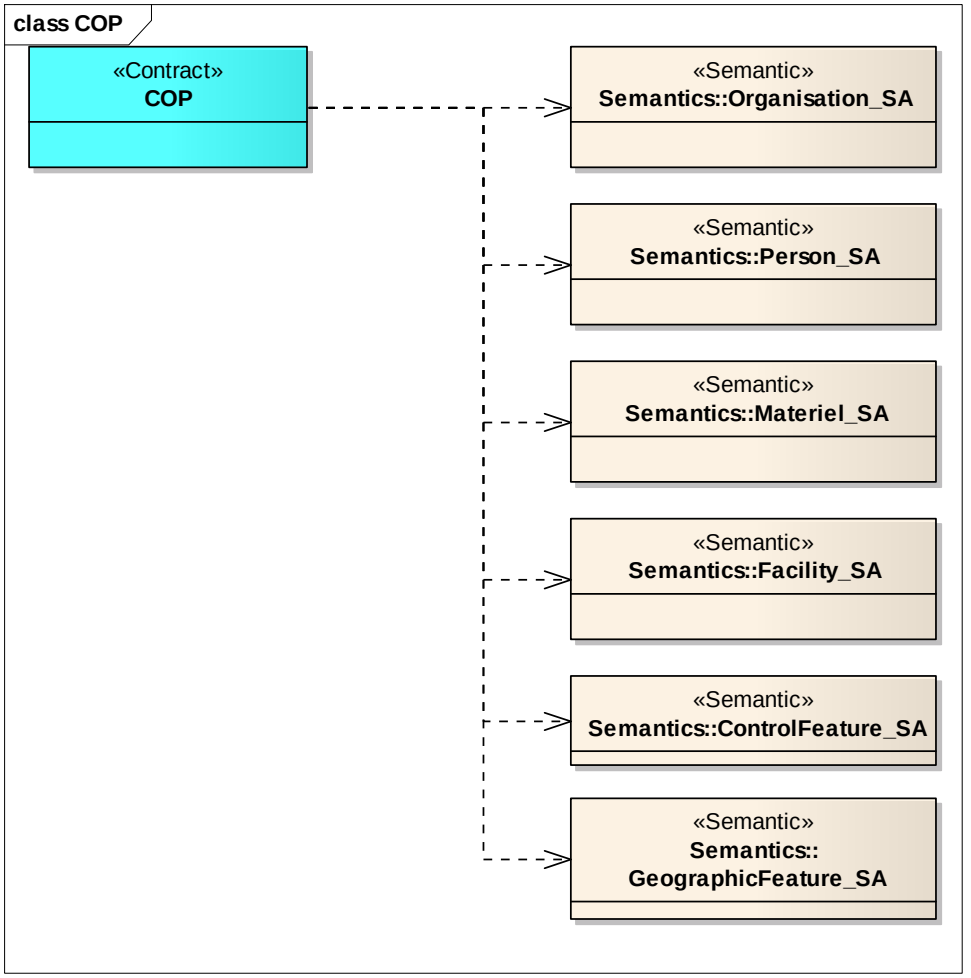
OV-2 – Operational Nodes

- Identifies 7 Nodes (one on Secondary Diagram)
- Contracts shared between Operational Nodes
- Nodes can share multiple contracts representing multiple virtual networks (Security Levels)
- Operational Tasks Supported by Each Operational Node
  - Requires UIs for each Operational Task
  - Operational Task required to operate manually and Automatically to support varying lengths of Demonstrations
- System Task which are Supported by core Applications:
  - User Interfaces (UIs)
  - Policy Enforcement Points
  - APIs
  - PEP
  - DDS



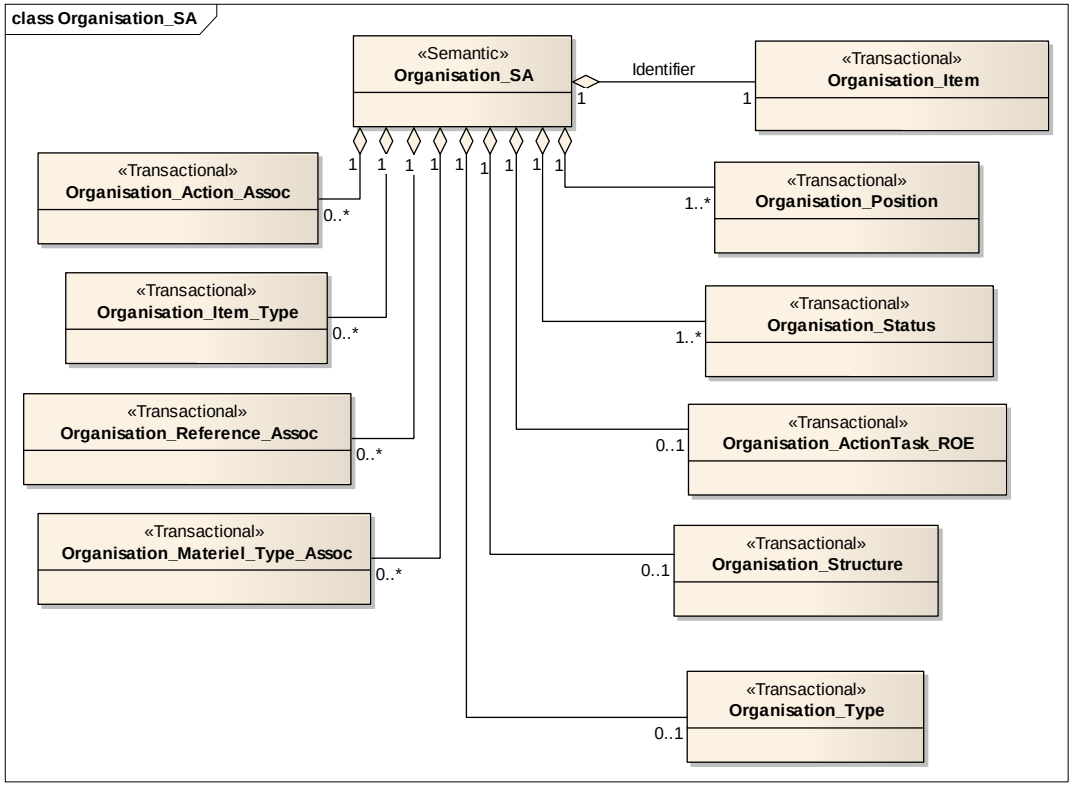
Contract Exemplar

- Contracts group community semantics (Messages) to be shared between members of a community
- Semantic specify the data aggregations for information shared by the community



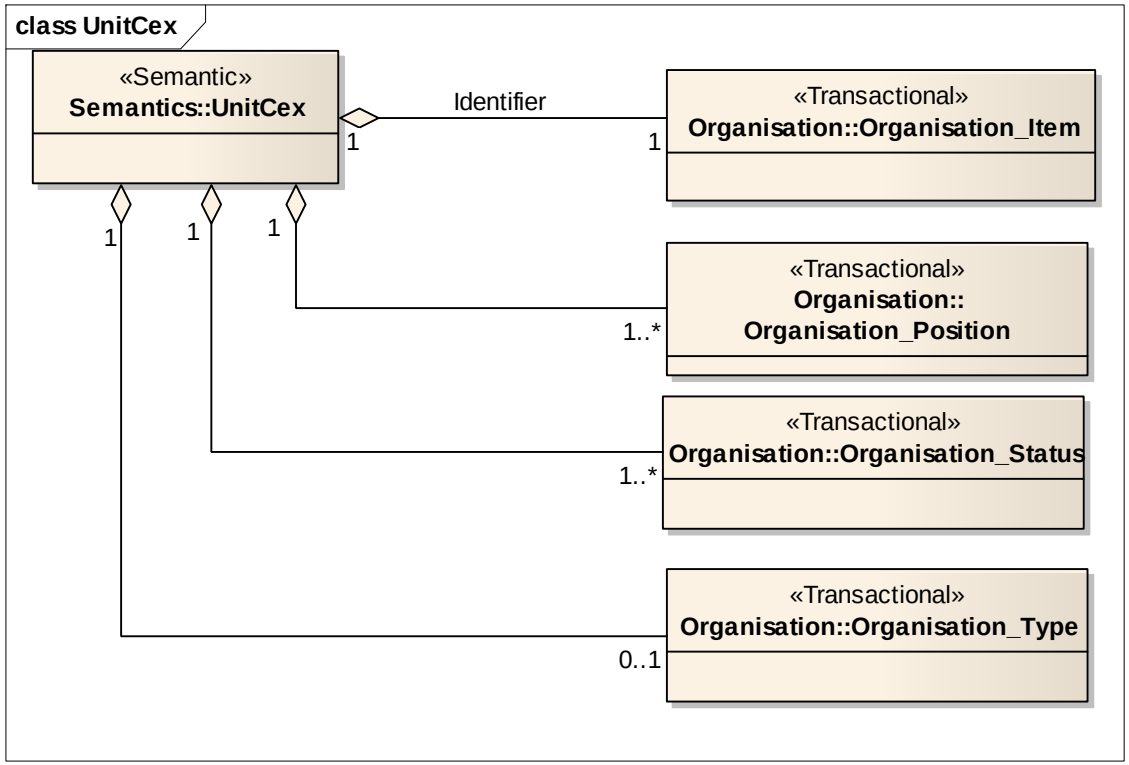
Semantic Exemplar

- Semantics specify the Transactions needed to aggregate information messages deemed complete by the members of a community
- Semantics Identify both mandatory and optional transactions in an information build
- Includes all Data Elements in subtended transactional



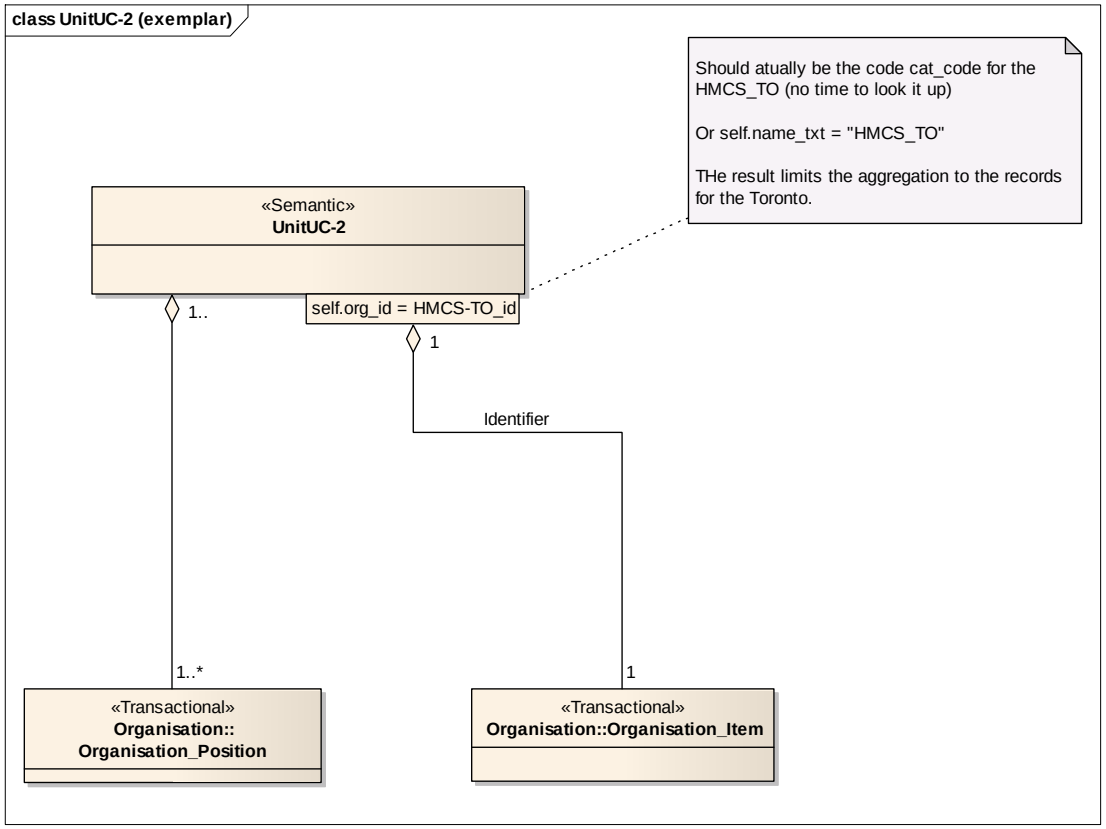
Re-using Architectural Models

- Unit Classified External is based on OrganizationSA (subset)
- Reduces Release-able Data and this Sensitivity
- UNITCex Aggregates a number of data patterns derived from more than 20 JC3IEDM Tables
- Can represent 1000s of aggregates with varying levels of sensitivity



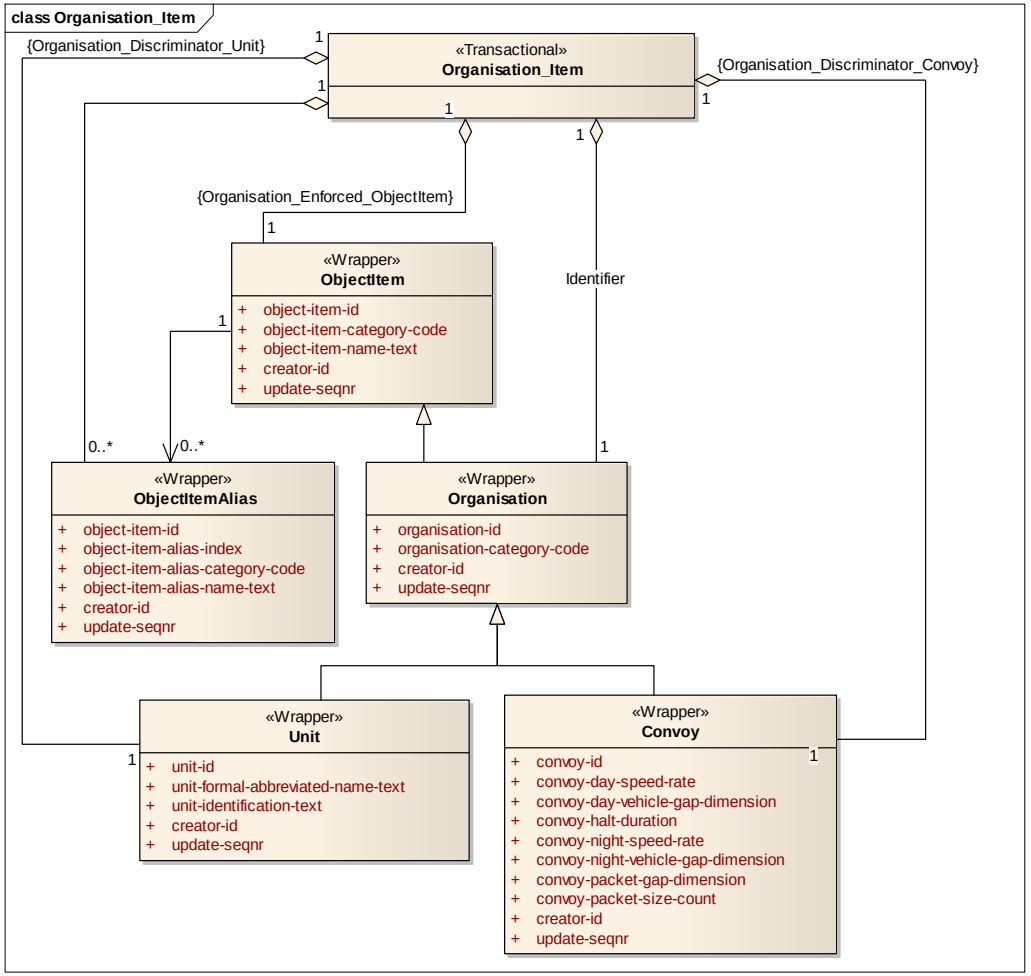
Re-using Architectural Models

- Another variant of the Organization Semantic
- Filters the aggregation to records concerning the HMCS-TO
- Any attribute of set of attributes can be filtered in this manner



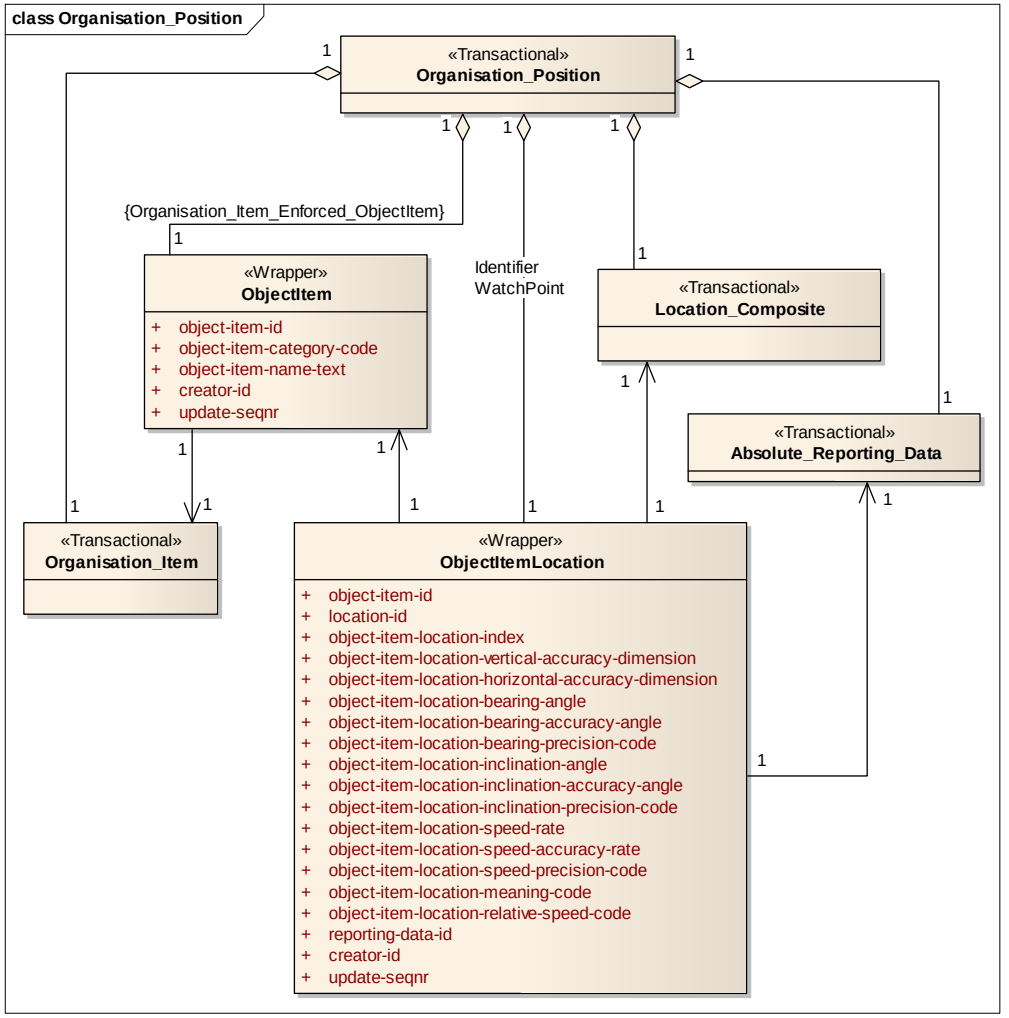
Transactional – Organization Item

- Aggregates Information (/data) Elements
- Includes all data elements in subtended transactions and wrappers

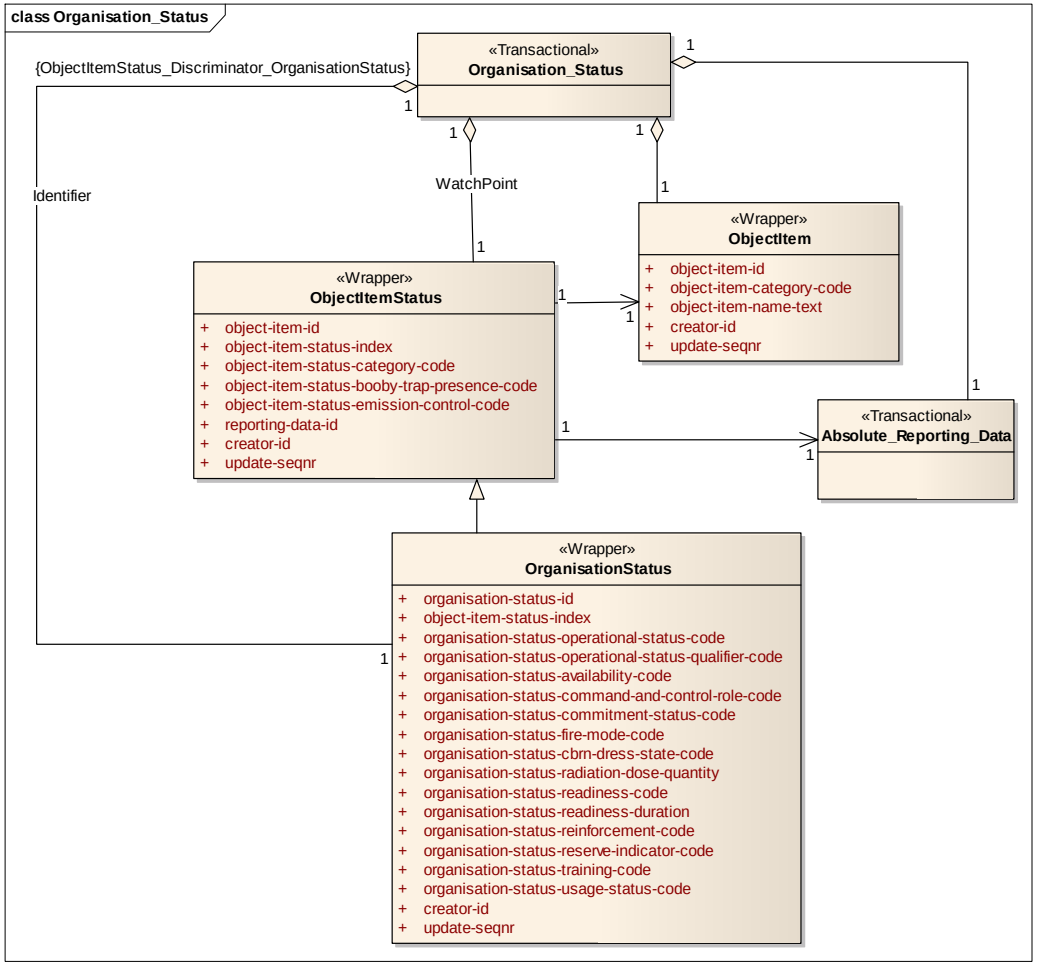


Transactional – Organization Position

- Can aggregate wrappers or other subtended transactionals
- Provides for a hierarchical build and reusable patterns
- Identified relationships (e.g., Key Relationships) between transactionals and/or wrappers

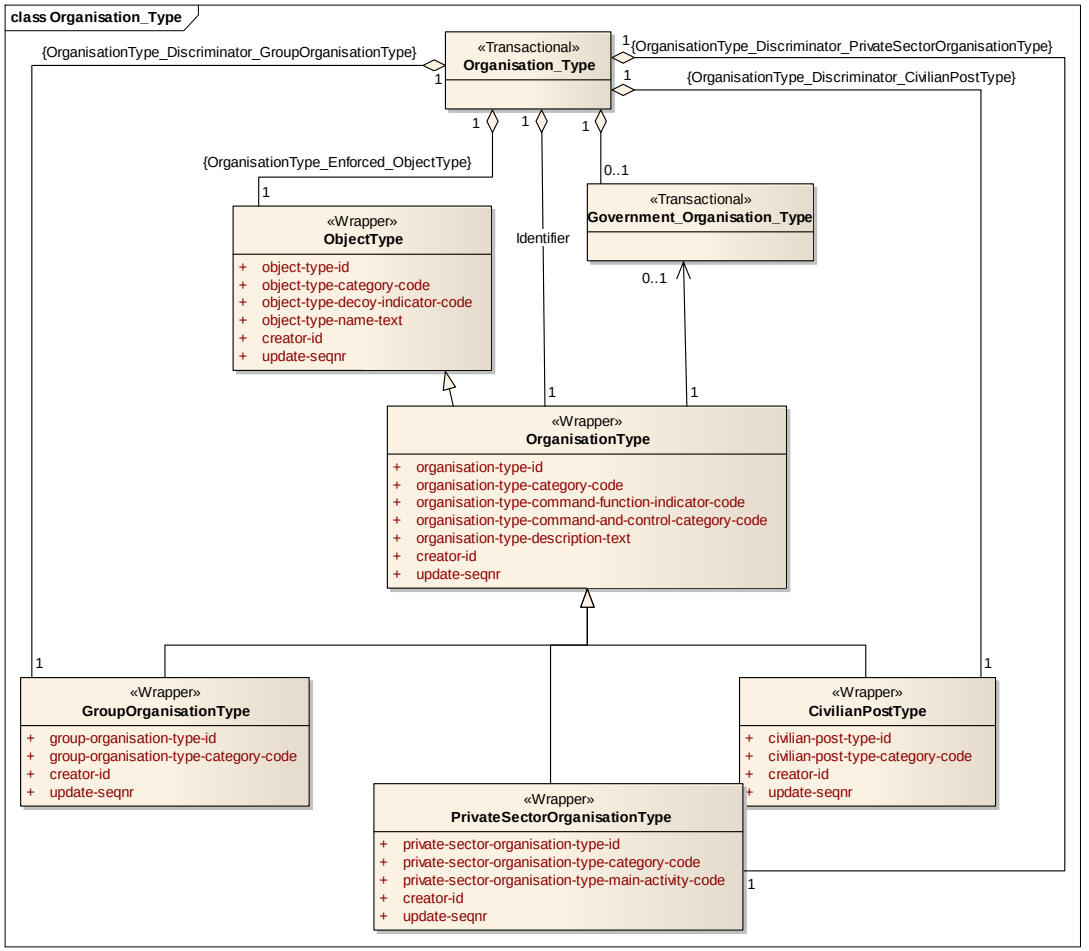


Transactional – Organization Status

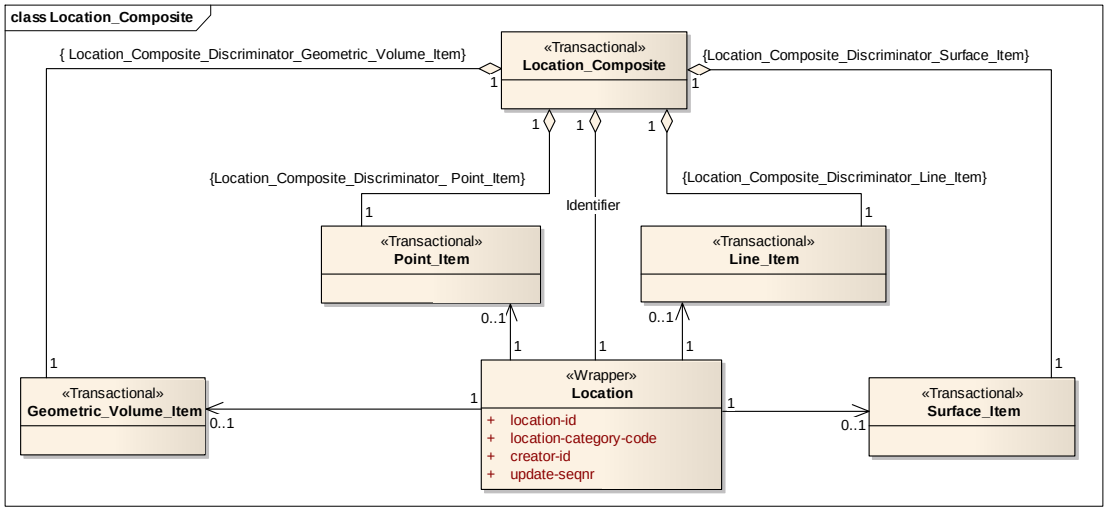


Transactional – Organization Type

- Allows for optional Selection and build



Transactional – Location Composite



Transactional – Absolute Reporting Data