Modeling Communities of Interest (CoI)/ Communities of Practice

CoI policies for automated system/service enforcement and Managing Interoperability Complexity

A **community of interest** or Community of Practice is a community of people, systems or organizations that share common interests, goals or objectives. Each member of the community needs the capacity to exchange or share information (situation, plans, ideas and thoughts) within the domain of interest; but often knows (or cares) little about other members of the community outside one specific area of discourse. Participation in a community can be for short or protracted periods depending on the area of discourse, the event or incident, or the business needs.

Communities are typically informal, self-forming, and self-organized networks of peers with a diverse set of skills and experience. The groups are initiated by the members' desire, objectives or goals to share information and advance their own knowledge by obtaining information from others.

In computer science a Community of Interest (**CoI)** is a means by which network assets and or network users are segregated by some technological means for some established purpose: business or operational requirement; level in an organization or community; sensitivity of information; or other operational consideration. CoI's are a strategy realm within computer security engineering. CoI's are also designed to protect their user community or information from the rest of the user population.

A CoI can be utilized to provide multiple levels of protection or access for members within a CoI and often consists of a logical/physical perimeter around the assets, IT infrastructure and information of the community or enclave. It allows for separate security management and system operation. The CoI *segregates* in order to achieve *security*.

The above description of CoI is typical of those found in the literature. However, this computer science description is network focussed and fails to address many of the issues facing the operations communities:

- How does one identify membership in a community, participation level and information needs?
- How does one establish the adhoc communities of interest/practice needed to address unforeseen operational requirements?
- How does one assign a community to a specific IT, communications and security infrastructure?
- How does one establish and then terminate a CoI when its business need is identified and then subsequently ended?
- How does one specify (establish policy for) the information elements or instances of information that can be shared within a CoI?
- How does one engineer an environment where members of an operation or business activity need to simultaneously participate in many CoI?
- How does one specify allowable data information aggregates moving within and between communities?
- How does one specify the information guards and filters

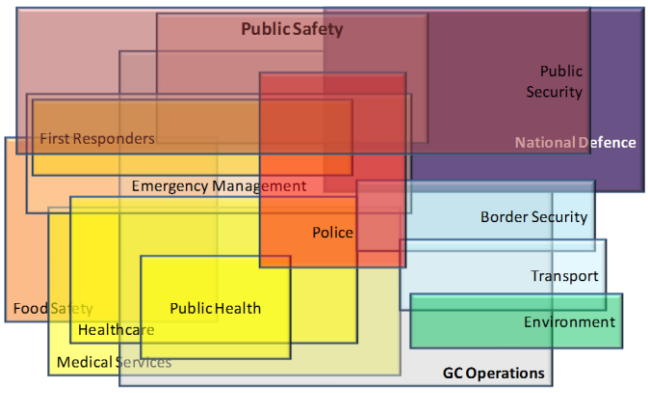

Figure 1: Multiple Overlapping Communities

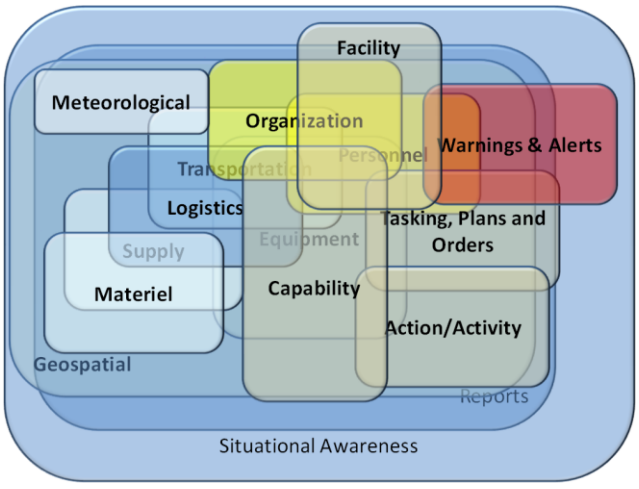

Figure 2: Multiple Overlapping information Domains

that govern the release-ability of sensitive (classified, confidential and private) information?

- How does one specify the alignment of information, IT infrastructure elements, participants, and practices (policy, regulation, directives and procedures)?
- How does one specify the alignment between information, threats, risks and safeguards?
- How does one enforce, log and audit the interoperability and information protection specifications in the operational environment?
- How does one manage the trafficking of hundreds to millions of messages where some containing sensitive information and where aggregation of information often increases the sensitivity of the information?
- How does one manage change in this environment?
- How does validate, verify and certify this type of environment?

Similar challenges seem to arise with each strategy "du-jour": network rationalization, network virtualization, workstation rationalization, workstation virtualization, information virtualization, multi-level security (MLS), multi-independent levels of security, service oriented architectures (SOA), cloud computing and interoperability. In the interoperability domain we see the key issues to be:

- The lack of agreement on Common/shared vocabulary, lexicon, taxonomy or ontology in many of the domains.
- A growing challenge aligning the growing number of overlapping community developed vocabularies, lexicons, taxonomies or ontologies to internal information architectures and/or systems.
- A growing challenge aligning multiple communities (figures 1 and 2); each adopting their own application of standards, protocols and technology.
- Fixed interfaces and business rules, interfaces and systems make it difficult to adapt to the dynamics of real-world incidents and events.
- The growing number of privacy and security laws, policies and regulations makes it difficult to adhere and enforce the rules.
- The difficulty in certifying and accrediting information systems in environment where the rules governing sensitive information are routinely changing.
- Addressing a general growth in complexity.

The remainder of this paper will outline a strategy for specifying, designing and implementing communities of interest and practice that addresses these issues.

Why isn't technology delivering CoI interoperability?

In theory, the abundance of commercial capability and technology should enable interoperability in most domains. So why does the ability to align community enclaves (security, business, organization, agency, national, etc…) continue to evade most stakeholders and IT professional?

There are many standards, specifications, protocols and technologies on the market that claim to deliver broad based interoperability. Many work extremely well in self-contained integrated homogeneous environments. These technologies will allow closed (well defined) communities to interoperate and collaborate quite well. They also provide reasonable levels of information security while information is **in-use** (application on secure infrastructure in secure facilities), **at-rest** (physical or electronic vaults) and **in-transit** (secure encrypted virtual or physical networks). However, as the communities become more diverse legislatively, organizationally, culturally, procedurally, and technologically, many of these technologies are found wanting because they were never designed to be integrated.

Efforts to enable internal, coalition and interagency interoperability, shared situational awareness, collaboration, etc. have consumed substantial resources with fairly modest results. With all this technology at our fingertips – it is left to a handful of very gifted operators and low level decision makers to "MAKE-IT-WORK" – using well developed interpersonal relationships. Many exercises have illustrated that in an emergency, the technology is virtually useless and often ignored.

Interoperability: What is the problem?

Information and semantic interoperability is and always will be a business challenge with technology as a simple enabler. Interoperability requirements are driven from an operational need for shared operational awareness to ensure that decision makers have access to quality (Accurate, Relevant, Timely, Usable, Complete, Brief, Trusted and Secure) information. Specifications, design and implementation require a shared understanding of information requirements. Developing and maintaining these requirements within an agency or organization has proven to be a challenge, and is even more difficult in a community setting.

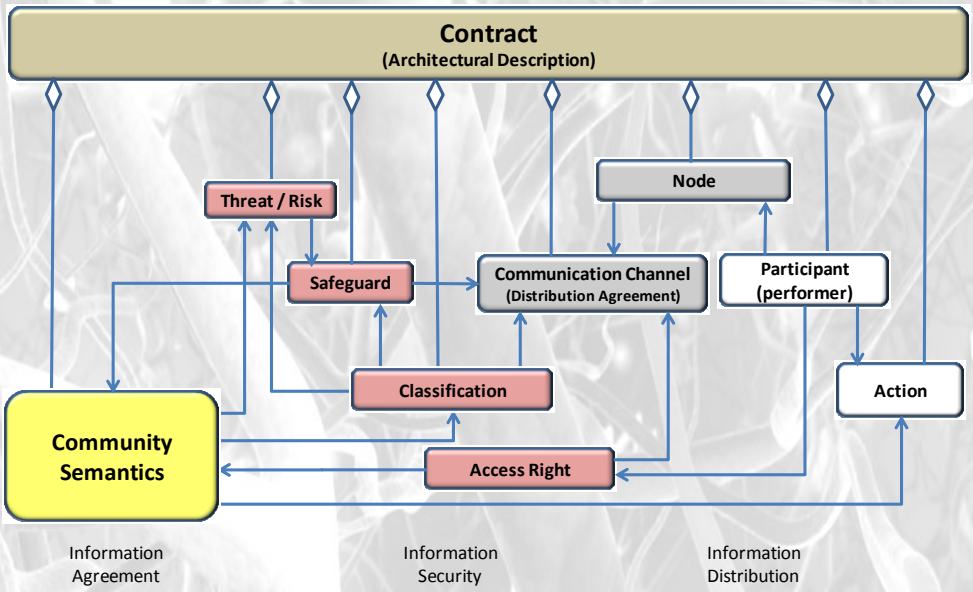

Figure 3: Architectural Description of a CoI (contract)

Many efforts are focussing on process based strategies, which do not address the fundamentals of the information sharing and protection realities. The Object Management Group (OMG) is focussing on a alternative approach – focussing on the specification of business (information) objects and Model Driven Architecture (MDA) approaches to rapidly develop and deploy capability, while maintain full audit-ability to business requirements. As illustrated in Figure 3, the approach focuses on the notion of a "**Contract**" or Information sharing agreement that incorporates specifications for:

1. An information Agreement,
2. Information Security requirements, and
3. Information Distribution Requirements.

The proposed architecture based approach is being developed under three OMG open-standards initiatives, which are based on lessons learned, and which generally apply to the business, government, public security and military application. The three OMG initiatives are:

1. Shared Operational Picture Exchange Services (SOPES),
2. Information Exchange Framework (IEF), and
3. UML Profile for DODAF and MODAF (UPDM).

What defines a CoI for Information Exchange

The requirements for a CoI derives from legislation, regulation, policy, strategic plans, memorandum of understanding (MOUs), Service Level Agreements (SLAs), Standard Operating Procedures (SOPs) or other governing document; and need to be traceable to those governance documents. The Information Exchange Framework seeks to exploit Enterprise Architecture (EA) and MDA to deliver this traceability.

A "Contract" represents an agreement to share information for an agreed purpose, e.g.:

- Collaboration (e.g., supply Chain)
- An emergency condition,
- An escalation in an emergency situation
- Testing,
- Training and exercise
- Business function, or
- Interagency / International Collaboration.

EA tools provide the ability to link architectural elements (e.g., contracts, operational nodes, semantics and safeguards) as illustrated in Figure 3.

Modeling a Contract

The SOPES and IEF initiatives are proposing two methods for defining Contracts and integrating them into the UPDM. The First is the realization of a **Contract** as a specialized "Operational Exchange" (Figure 4). This application of contracts is integrated

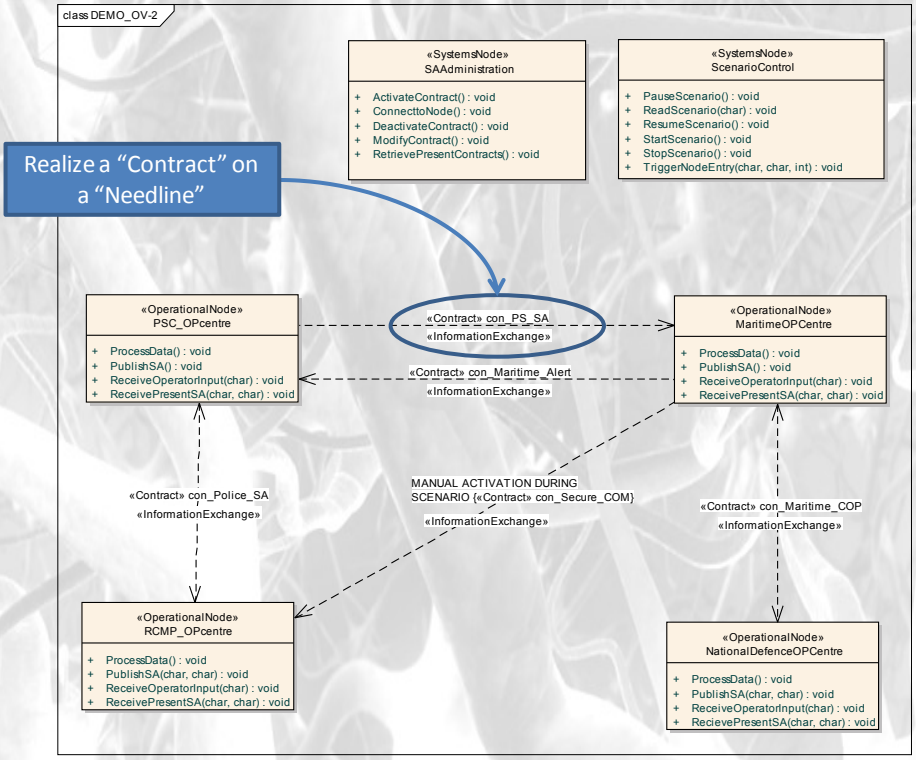

Figure 4: Integrating Contracts into an conventional Operational View (OV-2) – (based on a COIL demonstration)

into the UPDM Version 2 Domain Model (DM) and Profile. The SOPES Alignment to the UPDM is outlined in 201008 SOPES Profile Integrated into UPDM.pdf.

The SOPES profile currently aligned to UPDM was developed to increase the enterprise and system architecture fidelity when specifying information exchanges and the business rules governing the aggregations and protection of information assets.

The current Operational Views OV-2, OV-3 and OV-7 (which became Data and Information Views (DIV-2) in DODAF 2), cannot express the complexity of the information sharing and collaboration requirements introduced by legislation and regulation for the protection of information holdings. This is further complicated by the need to improve the quality (Accuracy, Relevance, Timeliness, Usability, Completeness, Brevity and Perception) of the information being shared. Simply looking at the issuance of Alerts and Warning (Figure 4) in the Canadian Public Security domain one can see the challenges. Many of the agency definitions and CoIs can be further subdivided to improve fidelity and information quality. The traditional OV-2, OV3 and OV-7 (DIV-2) do not support the complexity in a manner that would be relevant to stakeholders.

Realizing this limitation of many architectural frameworks and the information exchange semantic work (e.g., Common Alerting Protocol (CAP), CAP Canadian Profile (CAPCP), National Information Exchange Model (NIEM), EDXL and others), the SOPES and IEF initiatives are proposing a complementary or alternate architectural view to address CoIs and information exchange. This alternate approach aligns well with the evolution of architecture frameworks and the incremental evolution of community exchange semantics.

Modeling a Contract

The SOPES and IEF proposed view(s) can be referred to as the OV-2b or DIV 4 and will eventually be named by the DODAF, MODAF or NAF development teams. The "Contract" view is intended to address the complexity of a typical information environment.

Figure 5 illustrates possible distribution patterns for Alert Messages supported by the OASIS Standard CAPCP. As illustrated the CAPCP can be subdivided[1]

[1] This illustration is not based on an assessment of real stakeholder needs. It is simply provided as a

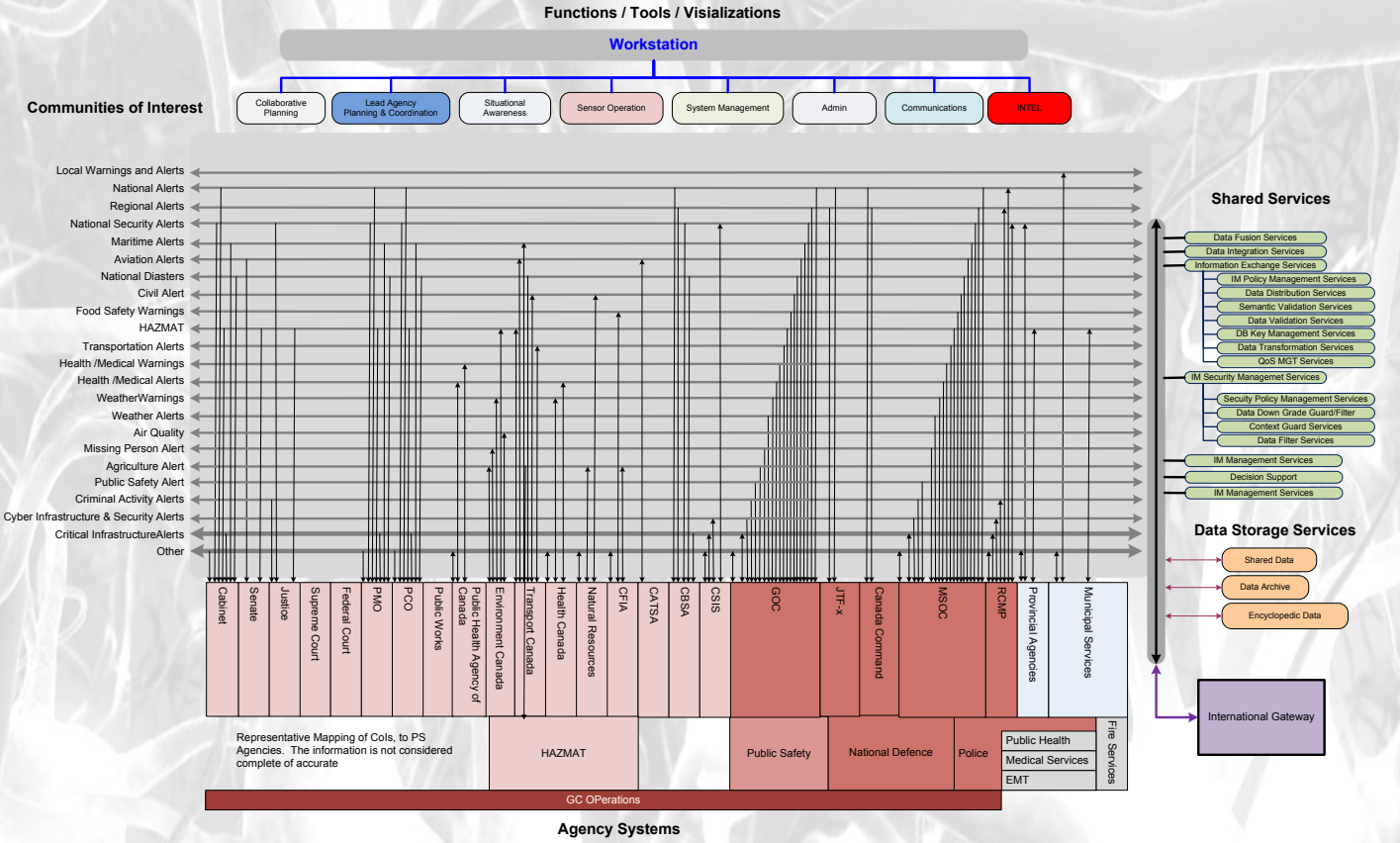

Figure 5: Representative Publication and Subscription Mapping for Warnings and Alerts

into specific alerting areas to address the needs of specific stakeholder communities and enhance the fidelity and quality of the information provided within the domain. The direction of the arrows on the vertical lines indicated an organization's responsibility to provide (publish), receive (subscribe) specific types of warnings and alerts.

The proposed SOPES and IEF view(s) enable a community to specify its needs, by specifying semantics (described in a separate whitepaper) to the individual participants (parties, publishers, subscribers) comprising the community. As illustrated in Figure 5, the CAP-CP message has been grouped into several categories based on filters to various domain values (an actual data instance value) in the XML schema and associated domain values. Messages based containing these domain values can then be assigned to participating agencies at run-time.

As illustrated in Figure 6, the contract models in this proposed view allows stakeholders to rapidly identify the publishers and subscribers to information shared within a specific CoI or information exchange

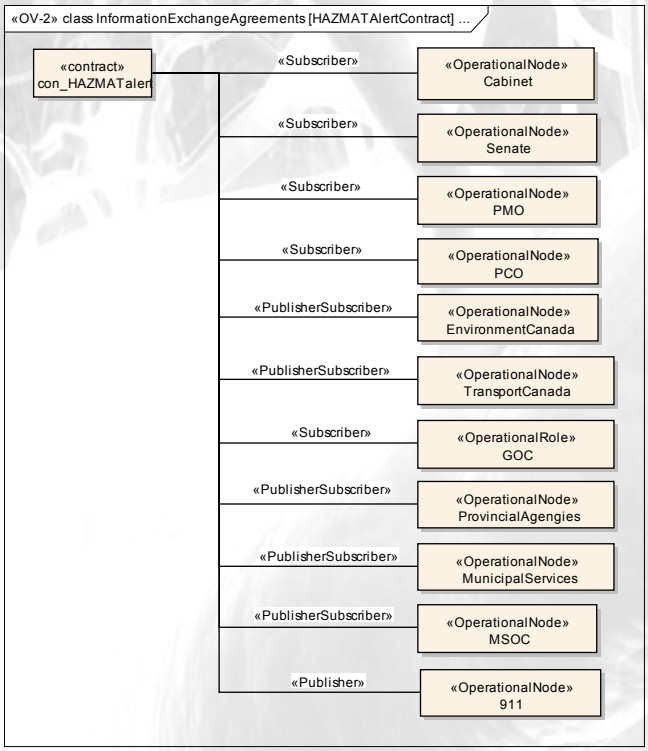

Figure 6: Contract (CoI) participants

agreement. The model format dramatically reduces the complexity of the environment and focuses stakeholders to the specification of their information need. In the case of Figure 5, information exchange agreements are aligned to operational nodes; tying them to the broader operational viewpoint in DODAF.

Figure 7, illustrates how the contacts are directly aligned to the information side of the agreement. In this cased, the community is seeking to share warnings and alerts related to Hazardous Materials (HAZMAT) incidents. The contract semantic ties the contract to the use of the CAPCP semantics for exchange. More on the alignment of semantics, filters, guards and business rules will be provided in a separate paper.

Figure 8 illustrates that the models can be combined into a single diagram. This is simply the preference of the architect or analysts and the capabilities of the UPDM tools applied.

The number of contract agreements and the participation of the nodes, organizations, systems, services is defined by stakeholder agreements. As with the semantics models, ASMG has demonstrated that these contract models can be used to automatically,

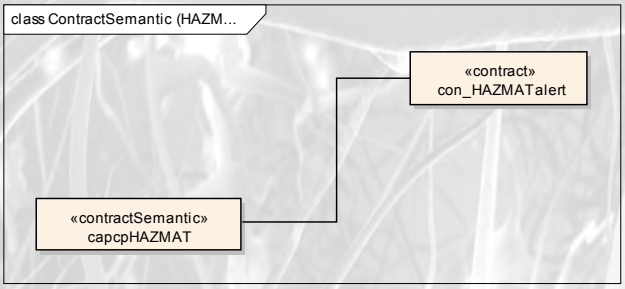

Figure 7: Contract Semantics (HAZMAT)

through an MDA process, develop and deploy the baseline configuration objects (files) for the middleware environment used by the community; providing traceability between the architecture models (views and viewpoints) and the deployment of operational systems.

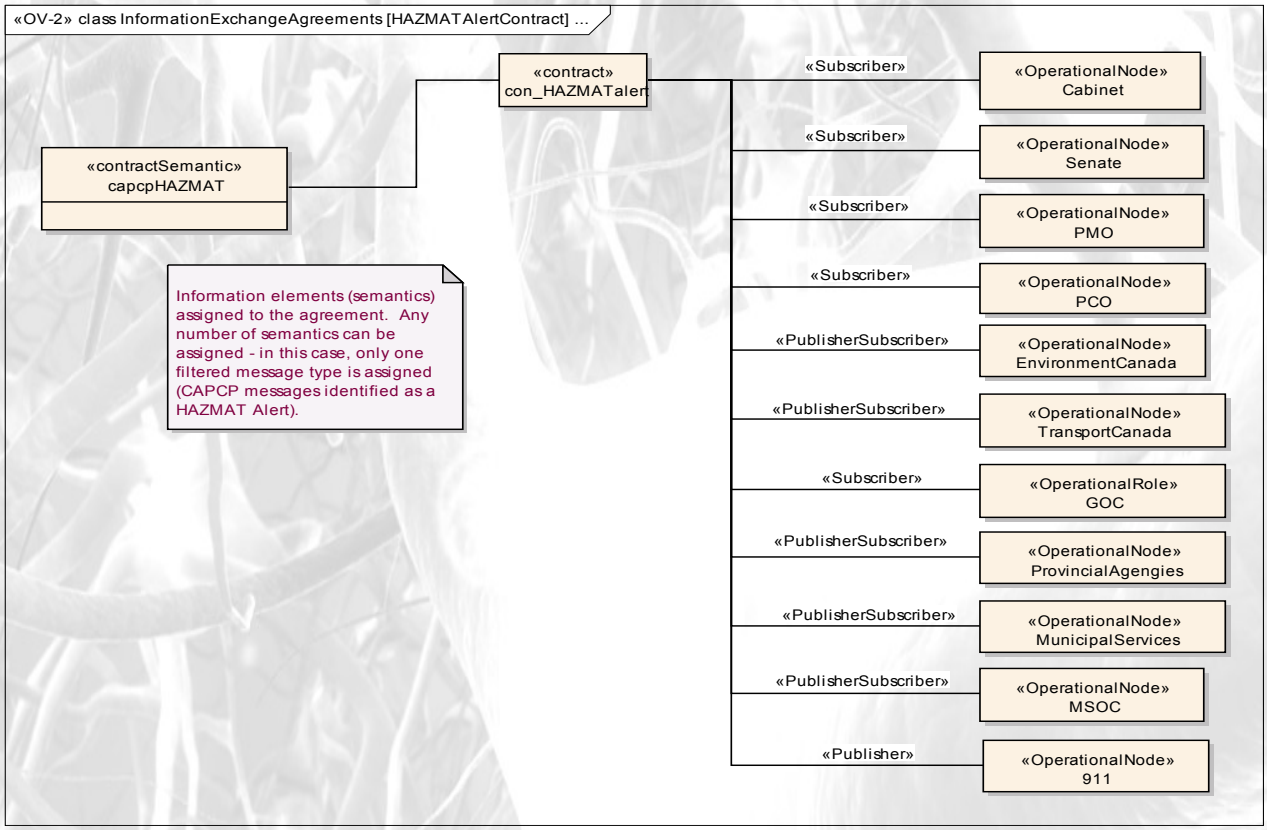

Figure 8: Combined Modeling Approach

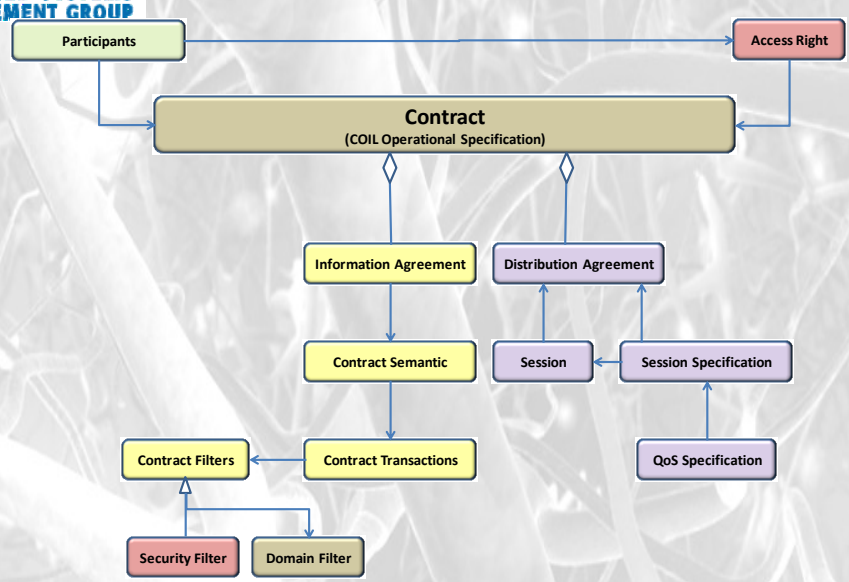

Figure 9: ASMG Implementation for COIL

Common Object Interoperability Layer (COIL)

COIL represents the ASMG implementation of an information exchange policy enforcement service that demonstrates the viability of the modeling techniques used for architecture driven interoperability standards like SOPES and IEF. Figure 8 presents the COIL contracting model. The COIL implementation extends the IEF contract model by integrating the use of filters to specify releasable data under semantic definitions tied to a Contract. This approach integrates information protection safeguards, while retaining the benefits of reusable data patterns.

COIL demonstrates the ability to use architecture to specify deployable capability in the areas of information (semantic) interoperability; and information protection. COIL also includes the ability to define semantic guards that will be described in a separate paper.

The Architecture (Figure 10) based approach provides the traceability needed by many Information Assurance governance functions (e.g., Certification and Accreditation and Threat Risk Assessments); thereby addressing a growing number of security, privacy and regulatory requirements.

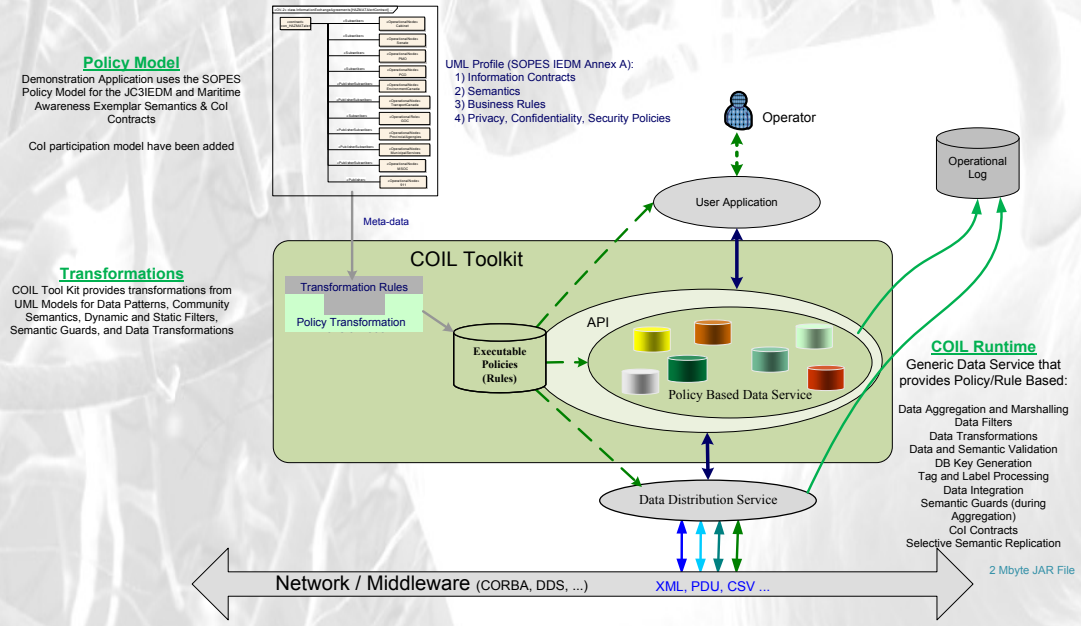

Figure 10: Architecture to Operations

Additional Information on SOPES, the modeling profile (including implemented extensions) and the first SOPES IEDM Implementation (COIL for SOPES IEDM) can be found on the ASMG website (http://www.asmg-ltd.com). Or by contacting:

Mr. Michael (Mike) Abramson, President

Advanced System Management Group Ltd.
265 Carling Avenue, Suite 630
Ottawa, Ontario K1S 2E1
Tel: 613-567-7097 ext 222
Cell: 613-797-8167
Fax: 613-231-2556