Common Object Interoperability Layer

Software Enforced Legislation and Policy

In today's interconnected and complex world, no single agency, service, or jurisdiction can protect citizens from the diversity of threats to national, regional and local safety and security. The Public Security Community comprises dozens of federal, provincial (state) and municipal agencies that need to share information:

- to assure a common understanding of events (shared situational awareness) and
- to assure the best allocation of scarce resources to planning, response and recovery activities.

It has been long known that decision makers require timely access to relevant and accurate information in order to exercise their responsibilities. In the real world of Public Security and Emergency Management, this implies the capability to rapidly establish communications across a diverse community, in response to planned and unplanned events, and adjust these communications to the changing conditions on the ground. As recent events (e.g., 9-11, Katrina, 1998 Ice Storm, tsunami and SARS) have illustrated, the lack of well established capability can have severe consequences to the general population, the responder community and the reputation of the governments and supporting agencies.

Improving the quality of information, and making that information "discoverable", "accessible", and "understandable" has long been the desire of stakeholders. However, this desire is often tempered by the need to protect and safeguard sensitive (private, confidential and classified) government information holdings. This competing set of stakeholder requirements is commonly referred to as "interoperability". But, as desirable interoperability is to stakeholders, the ability to achieve interoperability within an agency, let alone a diverse community of agencies, has been difficult to achieve.

Challenges

The community seeks the capacity to work seamlessly in the execution of their shared responsibility to help detect, prevent, and respond to threats (whether criminal, security, or health), and respond to incidents in an effective and timely manner. The environment should be one that enables decision makers to dynamically establish the capacity to combine critical intelligence, gleaned from seemingly unrelated sources and incidents, into a holistic situation assessment. And use this assessment to develop and affect a coordinated, multiagency course of action.

This requires the community to develop new strategies and information sharing capabilities that deliver shared situational awareness, collaboration and interoperability across the broadest cross section of participating agencies. In response to this need, the IT industry has been evolving an approach that allows respondents to identify rules, validate those rules, and apply them in a quasi real-time, dynamic, environment. This has been identified as a policy-driven approach.

Challenges

The operational, interoperability and communications challenges are well documented in a number of government and press reports and do not have to be rearticulated.

- **Legislation and Policy** are often written in general terms and do not provide the precision needed for individual agencies to deliver capability while assuring that they adhere to sometimes conflicting legislative mandates.
- **Governance** structures and practices are often agency specific and not focussed on the challenges of interoperability across a diverse community such as Public Security and Emergency Management. (e.g., There are no definitive certification processes for shared services delivery)
- **Architecture (Enterprise and System)** have not kept pace with stakeholder demands for enhanced interoperability and information protection within and between agencies
- **Engineering (Information, Systems and Applications)** have not kept pace with expanding information sharing requirements in the system of systems (SOS) and Organization of Organizations (agencies).
- **Technology** has been delivered in an over abundance of proprietary and evolving solutions; such that the Public Security and Emergency Management Agencies are challenged to select and deploy capability that will be interoperable.
- **Agency Capacity** to adapt to the rapid changes in requirements, practices and technologies are severely limited.

As illustrated, enhancements are required across a broad spectrum of activities and diciplines.

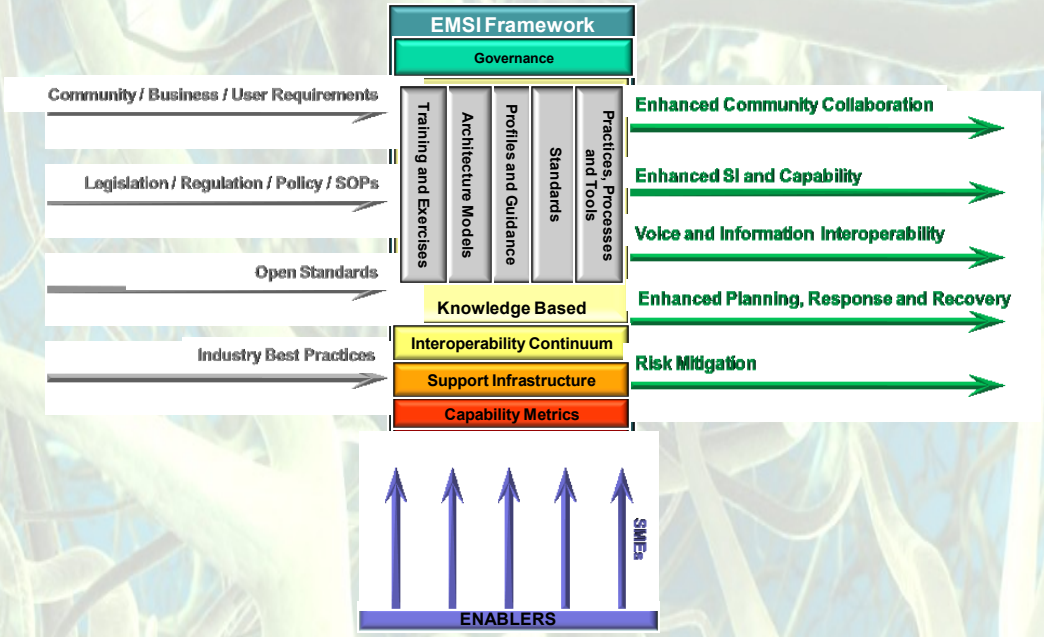

Figure 1 – EMSI Framework

EMSI Framework

In response to these challenges, Public Safety Canada, with support of the Centre for Security Sciences, undertook the definition of the Emergency Management System Interoperability (EMSI) Framework (Figure 1). This generic framework will provide a compendium of resources adopted and supported by Public Safety (PS) Canada to enable the specification, design, implementation and operation of interoperable capabilities in the areas of:

- ✓ Communications;
- ✓ Information Sharing;
- ✓ Situational Awareness;
- ✓ Joint or collaborative planning;
- ✓ Interagency coordination; and
- ✓ Decision support.

Additional information on the EMSIF can be obtained from Public Safety Canada and the Centre for Security Sciences, hosted on behalf of the Government of Canada by Defence Research and Development Canada (DRDC).

Required Capability

At the heart of the System Interoperability challenge is the specification of an interoperability lifecycle that clearly articulates how legislative mandates, community needs, practices and technologies are aligned to deliver real and sustainable capability to stakeholders. Figure 2 outlines the key elements of such a lifecycle.

The proposed lifecycle focuses on the translation of interoperability requirements (legislation, policy, operating procedures and other) into an executable form that can be enforced through technological solutions and controlled by each agency in several modes of operation (e.g., manual, automatic and semi-automatic). By separating the rules from the technology, the **Policy Driven** approach delivers the potential for:

- ✓ Increased governance and oversight by stakeholders;
- ✓ Increased flexibility, agility and sustainability;
- ✓ Increased collaboration; and
- ✓ Reduced risk.

In addition the policy driven approach enables many of the capabilities needed to advance across the Public Safety Interoperability Continuum elements: Governance, Operating Procedures, Information Management, Information Protection, Information Sharing, Technology (Platforms, Networks, Infrastructure, Security and Communications); Architecture, Training and Exercises and usage);

There are multiple community consortia and interest group seeking to address emergency and public security challenges. The EMSIF seeks to identify these efforts and provide guidance on their application to the best benefit of the communities.

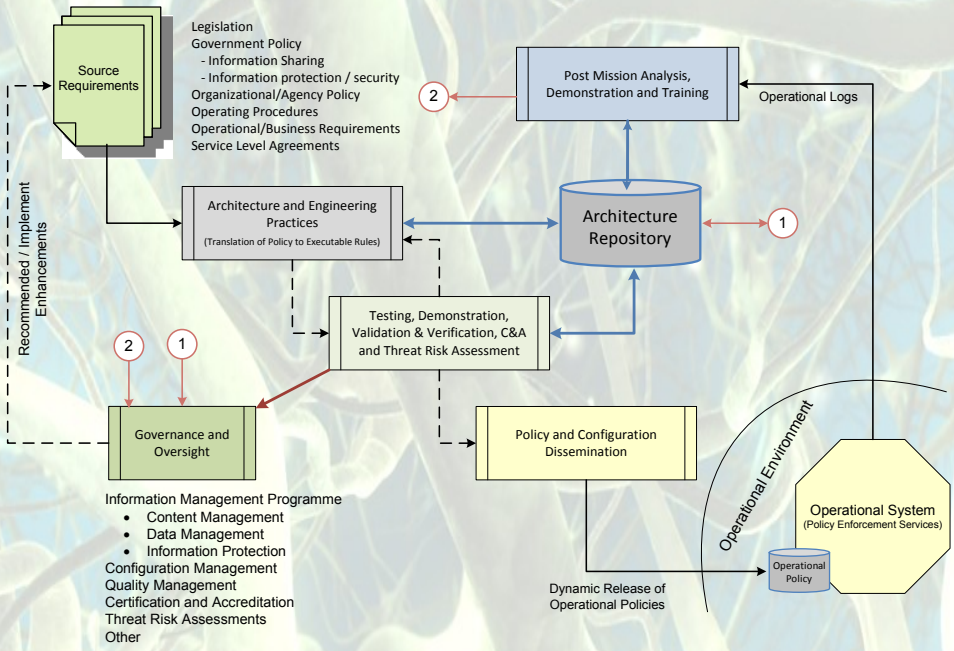

Figure 2 – Interoperability Lifecycle

Standards Community Responds

In the last few years the Open Standards Community has taken on the interoperability challenge with the participation of the Emergency and Public Security Communities, these include:

- **Organization for the Advancement of Structured Information *Standards (OASIS)***, *which focuses on the development, adoption, application, and implementation of emergency interoperability and communications standards for information sharing semantics (e.g., Common Alerting Protocol (CAP) and Emergency Document eXchange Language (EDXL)).*
- ***The Open Group and their Architecture Framework (TOGAF),*** which focuses on architecture best practices for the implementation and delivery of enhanced information systems. Other standards of interest are Semantic Interoperability and Unified Document Exchange Format (UDEF).
- **Object Management Group** (OMG), which focuses on the development of architecture and engineering practices and technologies, and interoperability solutions for multiple business domains including Emergency Management and C4I (Collaboration, Consultation, Command, Control, and Intelligence). Standards of interest include modelling standards such as the Unified Modelling Language (UML), and the Business Process Modelling Notation (BPMN). In addition, OMG has established a UML Profile for DODAF and MODAF architecture frameworks to foster toolset support, and a profile to address how to document shared information exchange messages and map them into the operational or situation awareness systems of the organization.

Shared Operational Picture Exchange Services (SOPES)

The SOPES Architecture Profile describes a standardised UML profile for describing

- **Contracts**, models of agreements to share information (Semantic) amongst two or more community members.
- **Semantics**, models of data patterns that govern the aggregation of data elements into meaningful information elements as defined by two or more community members. Semantics represent exchange messages such as those defined by CAP, EDXL, NIEM and others.
- **Filters**, which constrain the inclusion or exclusion of data during the preparation of a information elements – providing the ability to govern the release of information based in security and information protection legislation and policy.
- **Transformations**, which alter the structure of data elements to conform information sharing agreements.

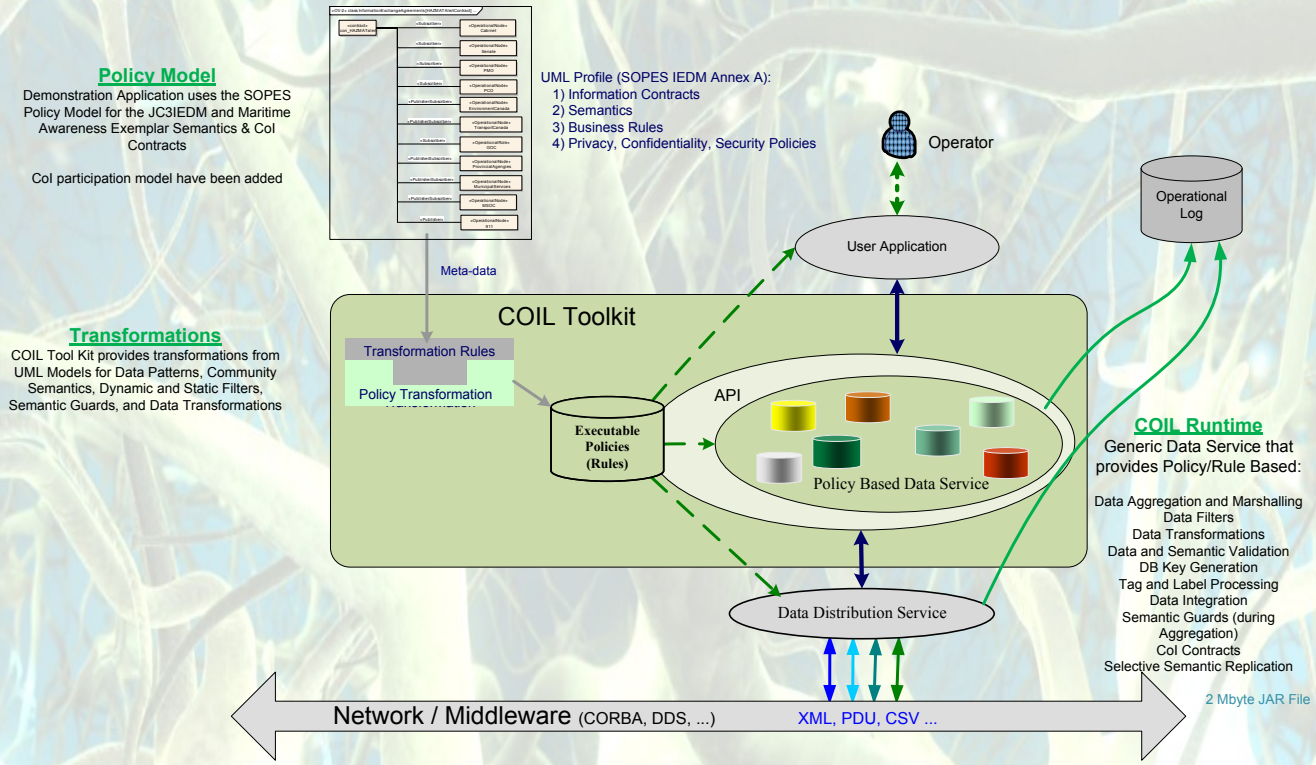

Figure 2 – SOPES Implementation (Policy Driven)

This notation will allow stakeholders to accurately specify information sharing requirements and provide the traceability necessary to the validation, verification and certification of systems developed for the community.

SOPES provides several capabilities for the emergency and public safety communities. These include:

1. An **Architecture Profile** that provides business (operational) analysts with a standardized notation for describing information sharing and protection within an architecture description.
2. A set of **Standardized Data Patterns** for the Joint Consultation, Command and Control Information Exchange Data Model, which has taken twenty years to develop for the exchange of collaborative planning and operational coordination information among partner nations; and SOPES will enable commercially available middleware solutions supporting that model out of the box.
3. Several **Implementation Patterns** for the SOPES models, including JAVA and XML, to allow for rapid adoption by middleware vendors and the Emergency Management Community.
4. An **Architecture Model** for reuse by communities seeking to exploit the patterns. These models are provided as XMI and Enterprise Architect (EAP) files.

Within a policy driven environment, the SOPES Specification would be implemented in a manner similar to that depicted in Figure 3. The data service is separated from the user application and the middleware; providing increased flexibility and agility within and between agencies. ASMG's Common Object Interoperability Layer (COIL) provides this capability.

For additional information on these or other interoperability topics, please contact:

Mr. Jean-Claude Lecomte, VP Business Development,

Or 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
Or visit our WEB SITE: www.asmg-ltd.com