

Emergency Services Enterprise Framework: A Service-Oriented Approach

Sukumar Dwarkanath
COMCARE
sdwarkanath@comcare.org

Michael Daconta
Oberon Associates
mdaconta@oberonassociates.com

ABSTRACT

The current *Emergency Services* landscape is characterized by a number of systems and networks that are isolated in nature, thus making information sharing impractical, if not impossible. Such an environment does not promote ease of information sharing, and each incident highlights the need for efficient collaboration and coordination, and the need for a holistic *internetwork* – a series of virtual interconnected networks - approach. In other words, it requires an overall framework that looks at *safety as an overall enterprise*, (albeit one with thousands of independent agency owners), with the strategic goal to facilitate greater collaboration and effectiveness of operations, and to ensure a streamlined and efficient prevention of, response to, and recovery from all-hazards.¹ Adopting a Service-Oriented enterprise approach is extremely useful and has number of advantages in such an environment. This paper defines a framework – in the context of an *enterprise* – an envisioned Emergency Services Enterprise Framework, and identifies the key elements of this framework.

Keywords

emergency services, emergency response, service-oriented enterprise, emergency services framework

EMERGENCY SERVICES: THE STAKEHOLDERS

The Emergency Services Enterprise consists of an inclusive and expansive list of emergency support functions and the organizations representative of each function as its stakeholders (see figure 1), including not only the traditional first responder agencies, but also public health, hospitals, transportation, emergency management, federal, state and local government agencies, private sector organizations, media, and others.² It includes all entities with primary and secondary responsibility for an Emergency Support Function (ESF).³ Given the diverse stakeholders in this enterprise, (the NRIC 1D report estimates there are more than 100,000 such independent organizations) it is obvious that policies and governance are essential to ensure a coordinated information sharing and management capability in this enterprise. It also ensures that entities - at their authorized levels – have access to the right information, at the right time, and at the right place.

Each emergency agency or stakeholder is a critical part of the enterprise, and it is vital to have its active involvement and participation in this process. This requires that there is a shared understanding, among the constituents, of the strategic objective. Applying the concept of a Community of Interest (COI), a collaborative group of users/stakeholders with a common business objective and mission, is useful here and the creation of an Emergency Services COI could serve as a channel for the definition of a shared goal for the enterprise.

Obtaining this shared context provides a foundation to define and identify elements of an envisioned framework. But it is clearly not an easy task. It needs to accommodate the diverse disciplines, needs and requirements of the

¹ This is closely aligned with the Federal Enterprise Architecture (FEA) and National Association of State CIO's (NASCIO) principles of a business-driven, collaborative, and Enterprise Architecture oriented approach to information-sharing.

² For our purposes, *Emergency Services* is a group of agencies that are involved in emergency preparedness, planning, response and recovery functions. This includes a diverse set of entities – from public safety to private industry. See the next section for a detailed explanation.

³ The Emergency Support Function or "ESF" is a mechanism that consolidates multiple agencies that perform similar or like functions into a single, cohesive unit to allow for the better management of emergency response functions. Rather than task a specific agency to perform a required task, an ESF Manager determines within the ESF group which agency or grouping of agencies would be in the best position to address the requirement based on the existing circumstances.

stakeholders, accommodate the dissimilar technologies and processes, operational characteristics, and other innumerable factors. A SOA pattern provides benefits in such a diverse environment, and allows the creation of a federated structure and a multilateral solution.

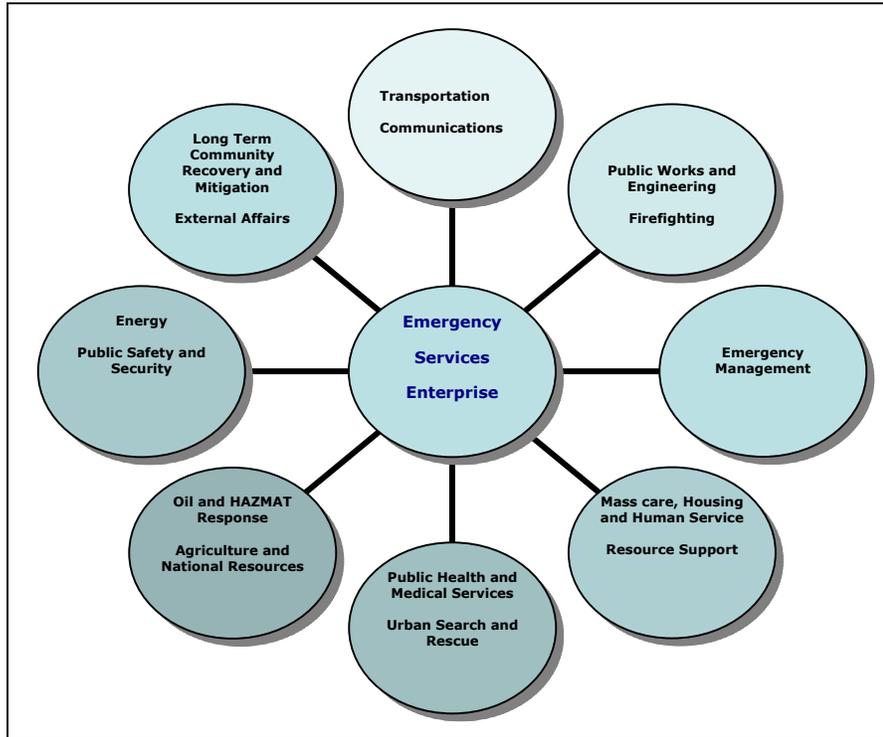


Figure 1: The Emergency Services Enterprise: ESFs and Stakeholders

SERVICE-ORIENTED ARCHITECTURE (SOA)

A SOA is an architectural approach and methodology that builds on the concept of *services*.⁴ These services are aligned with business requirements in an enterprise context and are *reusable* and *loosely coupled*. Furthermore, the *services* abstract the technical implementations and complexity, and enable ease of integration.

The following are the characteristic principles of a Service-Oriented approach:

- Open architecture and standards-based
- Modular and scalable
- Flexible
- Focus on security and privacy

The above principles, coupled with other advantages of SOA – both, in terms of technical and business areas – make it well suited to serve the unique characteristics and requirements of the Emergency Services community. It not only provides a mechanism to create a decentralized, federated structure, but also provides a logical approach to tie the heterogeneous components together. Recognizing its advantages and benefits, a number of organizations in this landscape have already adopted, and recommend an enterprise approach.

THE EMERGENCY SERVICES ENTERPRISE FRAMEWORK

The envisioned Emergency Services Enterprise Framework is described below in figure 2. While Governance dictates the business rules for the enterprise, enterprise services component is used to implement and enforce the

⁴ A Service is an implementation of a well-defined business functionality that operates independent of the state of any other Service defined within the system.

rules to enable and facilitate interoperability and information sharing in the enterprise. While some rules are enforced by the Line of Business Services, the shared agreements are enforced by Core Services. The Service Platform includes the methodologies and applications used to actually implement the services that are accessed using the Infrastructure component layer.

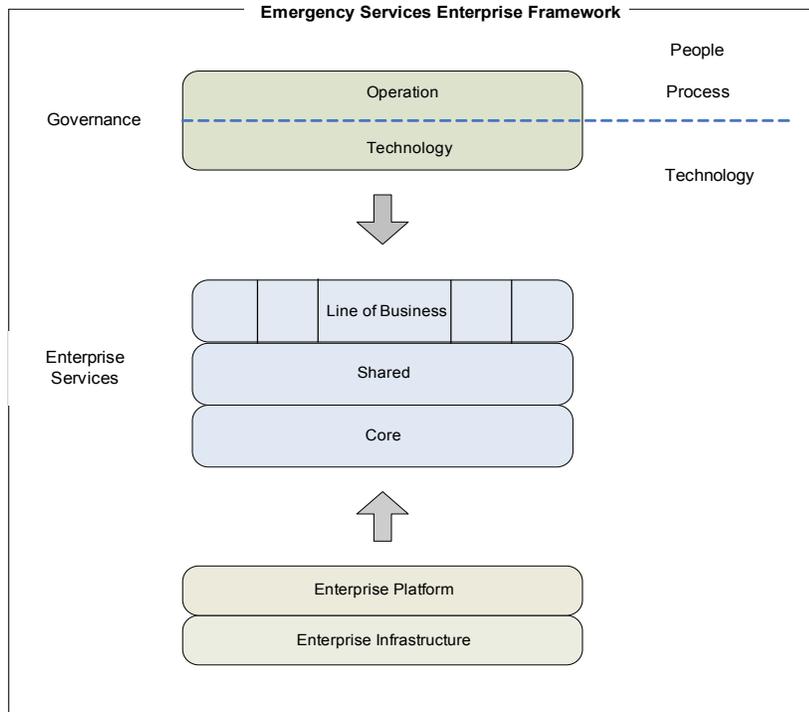


Figure 2: Emergency Services Enterprise Framework: Key Components

Governance

Governance includes the high-level set of policies and procedures that govern the *Emergency Services Enterprise*. It is composed of two fundamental components – Operational governance and Technology governance.

A unique distinguishing feature of the Emergency Services Enterprise is that there is no single entity responsible for its entirety, and adopting a COI approach serves to be useful in such a setting. *Operational governance* helps to identify the strategic outcomes and objectives for the enterprise. It provides a channel to create, analyze, and streamline the shared business processes in the enterprise to achieve the shared objective. With the context of these goals, the stakeholder requirements drive the principles, guidelines and business rules that are enabled by technology. The Operational governance component is critical to the development and implementation of this enterprise perspective, and this inherently highlights the importance of stakeholders and the processes. It also needs to be agile and flexible to accommodate the diverse stakeholders and their interests, the different business processes, and in order to be successful, it must provide transparency in process and approach.

The Technology module governs the actual technical, information technology and communications issues, and seeks to ensure the application of policies and the re-use of services in the enterprise. It also provides a channel to create service level agreements, publish best practices, service contracts, and other related matters.

Enterprise Services

Enterprise Services are composed of Core Services, Shared Services, and Line of Business (LOB) Services. While Core Services are horizontal services that are shared and used across all domains, Shared Services are horizontal services shared across a subset of the enterprise COI and among two or more domains. A strong business case differentiates a Core Service from a Shared service and this is explained further in the following sections. These

services also include the reusable technical services that span across domains and are used to encapsulate technical functions. LOB services are vertical, intra-domain services offered within a single domain.⁵

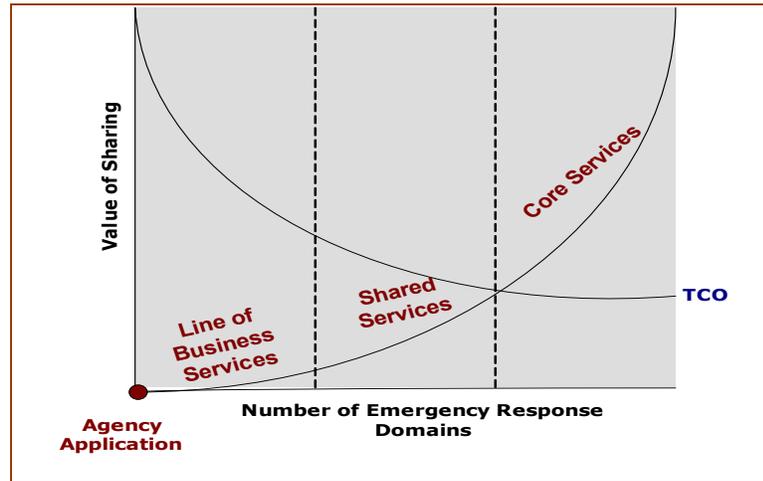


Figure 3: Enterprise Services TCO

Figure 3 illustrates how an application can be provided as different services in the enterprise. At one end of the spectrum is LOB services which are domain-specific services offered within a single domain. As the need for data sharing among domains increases, Shared services - horizontal services shared by a subset of the community - are provided. Shared Services are offered as Core Services when the business case is strong enough to justify the sharing of a service by the entire enterprise COI. Furthermore, the need and the increased value by sharing this common functionality are recognized by the entire stakeholder community. There is a clear correlation between the Total Cost of Ownership (TCO) and the number of domains that need to share information; the TCO decreases as we move from LOB to Shared to Core Services.

Line of Business Services

Line of Business services are the vertical, domain-specific business services that are provided by a single domain for use within the domain. For example:

- A Hazardous Materials (HAZMAT) identification service is a good example of a LOB service offered within the Emergency Management domain.
- A traffic advisory LOB services offered either by the Department of Transportation or another entity to other agencies in the regional domain.

Shared Services

Shared Services are the services that are shared among domains - usually two or more, and some services will be offered as competitive services in the marketplace. These services might also be specific to a region, city or any other subset of the larger COI and are governed by the specific region or subset COI.⁶ Some examples of Shared Services include:

- Intelligence and Information Analysis Service – This service provides means and mechanisms to enrich information, and resources to analyze the information. Consider a Hospital Bed Availability Service that can be shared between hospitals, EMS, and Emergency Management.

⁵ This builds on the Department of Defense's Net-centric Enterprise Services (NCES) Program concept that serves to provide enterprise services for its domain users. See <http://www.disa.mil/pao/fs/ncs3.html>

⁶ In some instances, the market place might decide otherwise and shared services may eventually be offered as Core Services.

- Network Management and Analysis Service – The typical network management and quality of service capabilities are provided through this service.

Core Services

Core Services are provisioned as a common shared utility by the emergency enterprise. These *facilitation capabilities* allow stakeholders to leverage common processes and functions across the enterprise or across domains, and are governed by the entire emergency services COI. These services allow entities to discover and access information, and are enabled with the help of registries. Some examples of Core Services include:

- Identity and Access Management – This includes Authentication and Authorization Service
- Data Rights Management – It provides data rights management, and allows agencies to tag access privileges to data
- Entity Locator Service – It provides a mechanism to identify the agencies and their endpoints in the enterprise, and their incident interest profiles
- Information Discovery Service – The Information Discovery Service helps to look up and discover the services in the enterprise, including references to data sources

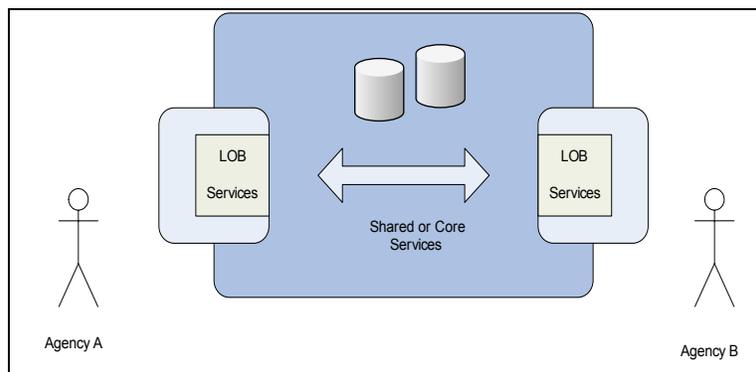


Figure 4: The Emergency Services Enterprise: Interactions

The above diagram (figure 4) illustrates interactions among agencies in this enterprise. The policies and procedures are created through the governance structure and are enforced by Enterprise Services that facilitate collaboration across agencies. The services in this component may be discovered and accessed by entities in the enterprise by using service registries and metadata repositories.

Enterprise Platform

The Enterprise Platform includes the methods and tools that enable the enterprise services. This includes the various sets of integration technologies, systems and standards that are used by the entities in the enterprise. Specifically, these are:

- Service Level Data Models – include information exchange models, interface definitions, reusable data components, metadata management and exchange packages⁷
- Data and Messaging Standards, including the set of Web Services standards, and extended specifications
- Integration services - like Messaging Brokers and Enterprise Service Bus (ESB), EAI, and others.

⁷ The National Information Exchange (NIEM) initiative is working to facilitate enterprise-wide information sharing through standards development, training and implementation support. See <http://www.niem.gov>

Enterprise Infrastructure

The Enterprise Infrastructure is composed of the Network and Transport modules - the access and delivery channels and the various transport modes like terrestrial and satellite communications, including wired and wireless communications. Internet Protocol (IP) is the underlying transport protocol, and serves as a key enabler of interoperability. Critical factors in the Network and Transport component are redundancy and reliability of communications links. Hurricane Katrina recently demonstrated the need to ensure these critical factors be accounted for, in the planning and preparedness stages.

Having defined and described the key elements of an envisioned framework, it is important to understand how such an enterprise approach is useful to the Emergency Services community. The following section addresses this aspect, and outlines a future state after a brief description of the current environment.

APPLYING THE FRAMEWORK

Voice and Data communications are complementary and mutually beneficial services, when properly integrated and used collaboratively, enhance the performance of the Emergency Services Enterprise. The current environment is marked with a number of limitations as voice communications remains the primary source of information exchange. In places where there is some inter-jurisdictional data sharing, it is often customized and access to relevant information and other data sources do not exist, thereby forcing emergency agencies to respond with limited resources and information. It is becoming increasingly evident that more emphasis needs to be placed on data communication since it provides a number of advantages in the broader context - better collaboration and sharing, reduction in customized and point-to-point solutions, improved scalability and information quality, and many others.

The following section, with the help of a scenario and examples, illustrates and applies the concepts discussed in earlier sections and presents a practical perspective.

Scenario Description

A major terrorist attack has occurred in a downtown area, and a mass disaster has been declared, given the scope and nature of the attack. The local emergency management agency (EMA) needs resources, and needs to collaborate with other agencies and share information.

- *Through the established governance structure, agencies in the region have agreed on a uniform policy and procedure on regional collaboration, and are willing to provide access to authorized agencies during emergencies.*
- *The local EMA queries the entity locator service to look up authorized emergency responder agencies in the area, alerts these agencies of the disaster.*
- *Response units are dispatched, and on the way to the scene, they use a number of enterprise services that provide them with additional information to respond efficiently. Some examples include:*
 - *The Department of Transportation's Traffic Advisory Service provides the best and alternate route information*
 - *The Weather Information and Discovery Service allows the response units to get the current and predicted weather information*
 - *The Intelligence and Information Analysis Service provides a detailed analysis of nearby schools, critical infrastructure etc., which enables decision support applications to provide simulations*
 - *The Regional Resources Information and Discovery Service provides an updated status on the available resources in the region, and its neighboring areas*
 - *The Hospital Availability Information and Discovery Service provides an updated status of availability of nearby hospitals*
 - *The Identity and Management Services monitors and regulates access to the above services, and allows authorized response units from neighboring jurisdictions, the required access to the above information.*

- *The Network and Management Service ensures that messages and information can be exchanged among the agencies in a seamless fashion.*
- *The agencies use established data standards and exchange packages to disseminate information, and some information requests and data transformations are provided by Enterprise Service Brokers (ESB)*
- *The service delivery and access channels have redundant wired, wireless, and satellite communications links to ensure available links.*

Thus, adopting a service-oriented enterprise approach provides a number of key benefits – it enables a collaborative platform through inter-agency agreements and protocols. It provides ease of information-sharing; allows agencies to re-use services and to discover and access the various sources of data and information. In addition, it provides a scalable and flexible multilateral solution, and offers ease of integration and implementation. During an incident, this allows emergency response agencies - a common operating picture and situational awareness for better coordination and collaboration. In summary, the envisioned architecture improves efficiency, streamlines effectiveness, and enhances enterprise-wide operations.

CONCLUSION

To ensure efficiencies and to promote collaborative information-sharing in the complex Emergency Services enterprise, there needs to be a logical framework that provides an integrated process and technology methodology in the context of an overall enterprise. A service-oriented enterprise approach is the most appropriate mechanism, and the envisioned Emergency Services Framework builds on this methodology to provide a high-level logical and conceptual architecture to bind together the process and the technology elements. But the benefits and advantages can only be leveraged if the stakeholder community adopts this *enterprise* approach to work towards a common and shared strategic outcome.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the contributions of a number of people (including COMCARE staff) who reviewed and provided suggestions. In particular, we would like to thank David Aylward and Judith Woodhall for their input and feedback.

REFERENCES

1. Department of Homeland Security. (December 2004). National Response Plan. Retrieved January 2005, from http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml
2. Federal Communications Commission. Network Reliability and Interoperability Council (NRIC) Focus Group 1D. (December, 2005). *Properties, network architectures and transition issues for communications between emergency services organizations, including Public Safety Answering Points (PSAPs)*, Final Report.
3. Lomow, G. and Newcomer, E. (2004). *Understanding SOA with Web Services*. Addison-Wesley, Upper Saddle River.
4. Mahmoud, Q. H. (April 2005). *Service Oriented Architecture and Web Services: The Road to Enterprise Application Integration (EAI)*. Retrieved January 21 2005, from <http://java.sun.com/developer/technicalArticles/WebServices/soa/>
5. Office of Management and Budget (May 2005). *FY07 Budget Formulation: Federal Enterprise Architecture (FEA) Consolidated Reference Model Document*. Retrieved January 21 2005, from <http://www.whitehouse.gov/omb/egov/documents/CRM.PDF>
6. Schekkerman, J. *Services Orientation: Hype or Hope? Structuring the Enterprise around Services*. Retrieved January 21 2005, from http://www.enterprise-architecture.info/Images/Services%20Oriented%20Enterprise/EA_Services-Oriented-Enterprise1.htm