Network Centric Operations Industry Consortium

Emergency Services
Operational Net-Centric Pattern

Rex Brooks, Emergency Management Standards Consultant

V1.0
December 2013

Version History

Version Number	Description	Author
1.0	Initial Release	Rex Brooks

Abstract

The Emergency Services Operational Pattern describes the prescriptive operational pattern for a set of discrete but interrelated communications services based on the Emergency Data Exchange Language (EDXL) suite of standards. These data-interoperability standards have been developed by the Organization for the Advancement of Structured Information Standards (OASIS) Emergency Management Technical Committee (EMTC). This set of standards prescribes messages for the range of emergency communications, from initial alerts and warnings to decision-supporting situation reports, including detailed message exchange patterns for handling resource management.

The operational core is the EDXL Distribution Element (EDXL-DE) v1.0, which handles the distribution of emergency messages, providing for audit trails, updates, cancellations, requests, responses and reports, allowing an Incident Command System (ICS) to redistribute message traffic internally without the need for examining the payloads. This can save time and increase effectiveness for the agencies and jurisdictions that take advantage of these features. Version 2.0 is in progress.

We highlight EDXL-DE because it points to the combined benefit of the EDXL suite, namely effectiveness for the response community as well as the communities served and the general public. Thus, this Net-Centric Pattern is aimed at all of these emergency services stakeholders.

Table of Contents

List of Figures

1 Introduction and Problem Description

The ***complexity and difficulty of emergency communications*** among jurisdictions and between jurisdictions and the public require a balance between timeliness and completeness within the variety of messages (alerting, logistics, situational awareness, etc.) for rapid and accurate decision making.

1.1 Context

Whether necessitated by a large-scale disaster like Hurricane Katrina or a traffic accident involving hazardous materials, emergency services communications need to be flexible and scaled appropriately to the size of the incident. From simple and immediate to detailed and in-depth, getting the right information in the hands of those who need it, when they need it, is essential. For emergency management, the lifecycle of an incident often determines the kind of communications that can occur. The overall need for different kinds of communications makes a Service-Oriented Approach (SOA) to communications highly appropriate in most circumstances. Therefore, we undertake development of this Emergency Services Operational Pattern with the SOA ecosystem as the context in which these emergency services are discovered and engaged.

Emergency services taken as a whole is the mission domain and the operational entities are described below.

The Organization for the Advancement of Structured Information Standards (OASIS) Emergency Data Exchange Language (EDXL) suite of standards is or will be implemented by a set of emergency services -- each of which implements the specific highly-focused standard from the suite in accordance with its rules for conformance.

These standards are discussed more fully later in this pattern. They are mentioned here because they each focus on a distinct area of the emergency context, from alerting the public quickly, to gathering information about local hospital capacities, to finding, utilizing and distributing response resources more quickly and efficiently.

Emergency situations have often been described as chaotic, largely due to confusion and lack of cooperation among responders; this is due, in turn, to the lack of common terminologies for emergency information and communication systems. By bringing order to this chaos, these standards change the emergency context and make coordinated response faster and more efficient.

In practical terms, especially within small agencies, organizations and jurisdictions, these emergency services will need to be implemented through a unified, singular set of software components, even while remaining distinct emergency services to be combined as needed and for the purposes of accurate accounting and auditing operations.

Additionally, the standards have the ability to use the code lists from other standards and standards organizations, such as the former “Tactical Situation Object (TSO)” created by the European Committee for Standardisation and now being worked through the International Organization for Standardization ISO TC 223—Societal Security. When approved, it will be included, as well as the ability to use the message structure of that specification along with EDXL-Resource Messaging (EDXL-RM) v1.0 to build special-purpose, user-defined messages.

Figure 1 provides a picture of the scope of the EDXL suite of standards from OASIS; the specifications are described in greater detail in Section 2.8--Standards. Figure 2 shows one way that code lists can be modeled, showing the TSO CodeList Rules[1]. (A CodeList is a collection of name-value pairs.) It should be noted that this is but one way, among several, that code lists can be modeled.

In larger agencies, organizations and jurisdictions, the emergency services described will be delivered through a Service-Oriented Architecture. The design will give careful attention to critical infrastructure protection, especially emergency communications, and their re-establishment if the infrastructure is damaged. Another consideration is providing these emergency services in a way that minimally impacts daily operations where they are used. Additionally these emergency services should be measured for fitness of use, at least by the criterion of whether they offer service efficiencies compared to current capabilities,

Of course, not every emergency service is needed in every context. For example, a small jurisdiction with a small number of well-known hospitals may not need an emergency service to locate available bed space for treating certain types of injuries. However, if a small jurisdiction is part of a larger-scale emergency, there will be a need for outside assistance organizations to access such a service. So, some accommodation to provide that information may be necessary even if maintaining the emergency service is not needed.

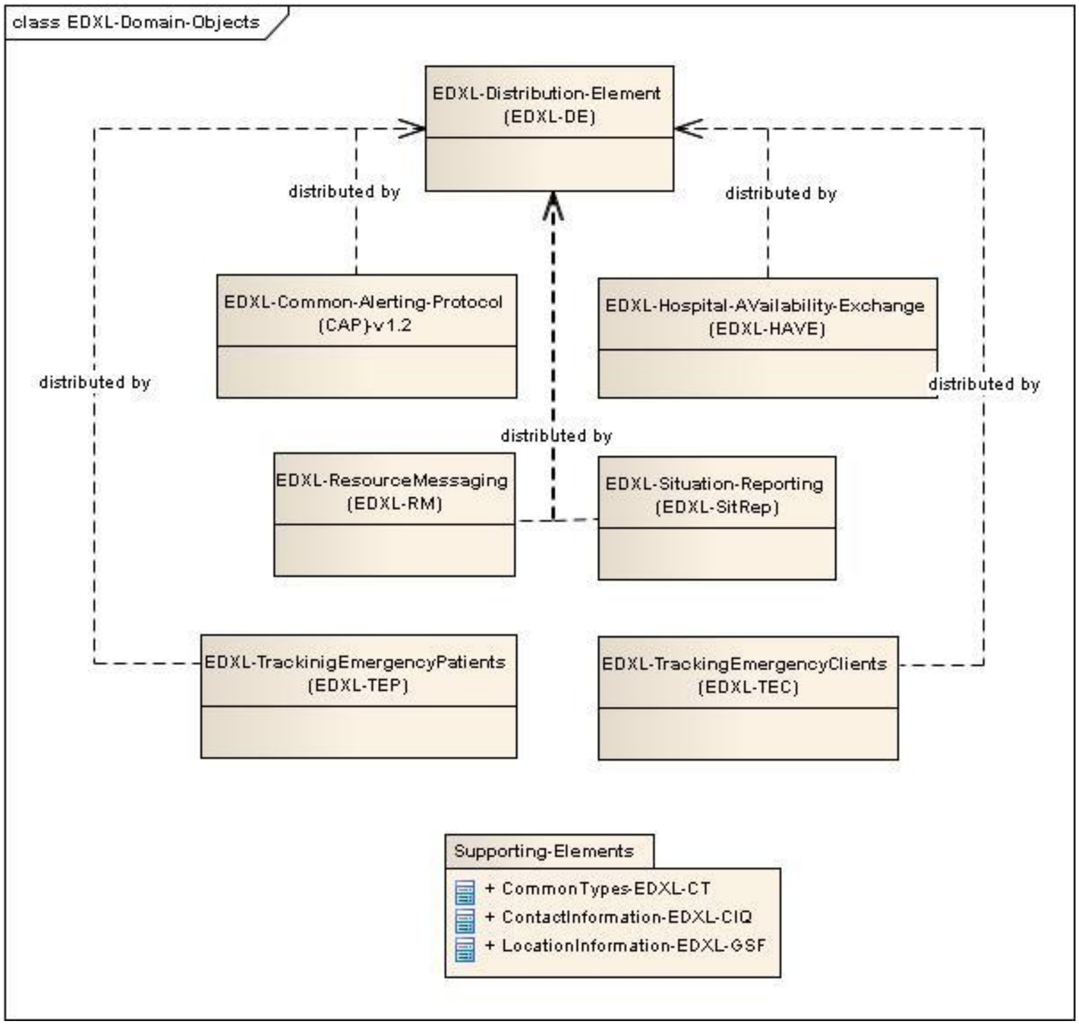
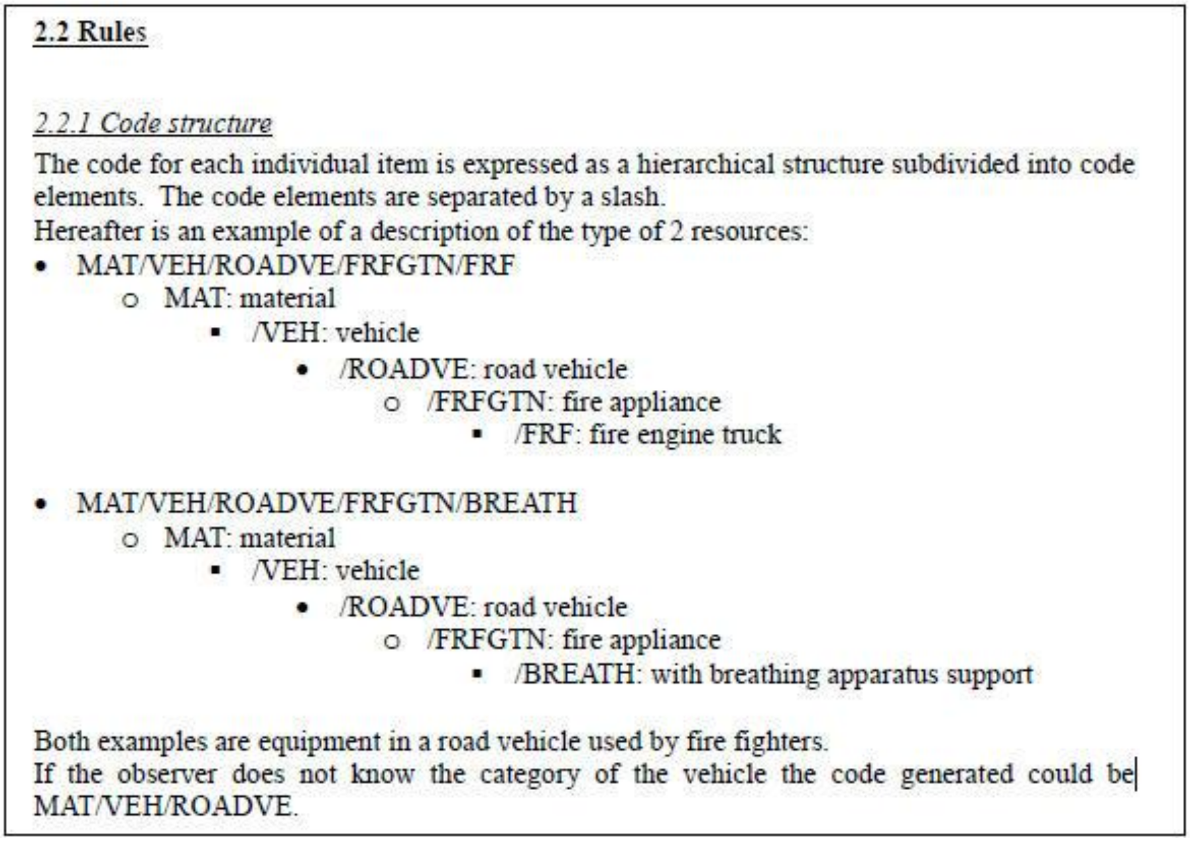

class EDXL-Domain-Objects
EDXL-Distribution-Element (EDXL-DE)
distributed by
distributed by
EDXL-Common-Alerting-Protocol (CAP)-v1.2
EDXL-Hospital-AVailability-Exchange (EDXL-HAVE)
distributed by
distributed by
distributed by
EDXL-ResourceMessaging (EDXL-RM)
EDXL-Situation-Reporting (EDXL-SitRep)
EDXL-TrackinigEmergencyPatients (EDXL-TEP)
EDXL-TrackingEmergencyClients (EDXL-TEC)
Supporting-Elements
+ CommonTypes-EDXL-CT
+ ContactInformation-EDXL-CIQ
+ LocationInformation-EDXL-GSF

Figure 1 EDXL Suite of Standards Approved and Pending

"Supporting Elements" shown in Figure 1 and Figure 10 refers to sets of information (indicated in the figure by the plus signs) that pertain to contact information, location information and general information types that are used by more than one of the EDXL standards. This was done to prevent repeating the specification of these information types each time they are used.

It is important for all jurisdictions to carefully select the emergency services they need based on a number of criteria, from the size of the jurisdiction to the likely scale of emergencies. Figure 2 highlights some additional factors that may need to be taken into consideration. In particular, software applications need to understand code lists beyond those included in the EDXL suite.



2.2 Rules

2.2.1 Code structure

The code for each individual item is expressed as a hierarchical structure subdivided into code elements. The code elements are separated by a slash.
Hereafter is an example of a description of the type of 2 resources:

- MAT/VEH/ROADVE/FRFGTN/FRF
    - MAT: material
        - /VEH: vehicle
            - /ROADVE: road vehicle
                - /FRFGTN: fire appliance
                    - /FRF: fire engine truck
- MAT/VEH/ROADVE/FRFGTN/BREATH
    - MAT: material
        - /VEH: vehicle
            - /ROADVE: road vehicle
                - /FRFGTN: fire appliance
                    - /BREATH: with breathing apparatus support

Both examples are equipment in a road vehicle used by fire fighters.
If the observer does not know the category of the vehicle the code generated could be MAT/VEH/ROADVE.

Figure 2 CodeList Rules from TSO from European Committee for Standardization (CEN)
CEN Workshop Agreement: CWA 15931-2

Figure 2 shows the code list structure for the TSO, which will almost certainly be carried over into the ISO standard built upon the TSO work.

We will also face contextual challenges from proprietary software already in place, which makes the accomplishment of interoperability at the level of data difficult. However, there are answers to this problem available through the use of terminology and data-type translation capabilities. Indeed, given the aggregate size of this potential market, such solutions could represent opportunities for some Network Centric Operations Industry Consortium (NCOIC) member-companies once the market is understood, especially where civilian and military humanitarian services intersect. Crafting adaptable solutions that can be fitted to the needs of the market is the main challenge.

1.1.1 Net-Centric Principles

We look to net-centric principles to provide guidance for the net-centric patterns we develop in a domain and platform independent way. These principles are described in the NCOIC Interoperability Framework (NIF) and in particular the Net-Centric Information Framework[2] (NCIF) along with the Net-Centric Services Framework (NCSF) v2.0[3]. A matrix showing the currently referenced interrelationships among these principles can be found in Appendix A.4 of the NCIF.

Rather than recite how each principle comes into play, for this pattern we are mentioning only the most significant. These principles are summarized in the following subsections.

1.1.1.1 Explicitness and Ubiquity

Explicitness is particularly important in an emergency services context because the diverse and heterogeneous participants and jurisdictions may not all share the same vocabulary, resources, constraints and regulatory environment assumptions. Furthermore, in an emergency context, it may be difficult or impossible to access information and references concerning these information topics by those participants who are unfamiliar with the capabilities and conventions of the other participants in the emergency situation. At the same time, it is important to be terse and precise in emergency situations in the interest of timely action and so as not to tax whatever limited communication resources might be available to share. This pattern provides explicit vocabulary sets and code lists to support this objective of communication economy while applying the net-centric principle of explicitness. Likewise, the principle of ubiquity is important in an emergency services context because it is generally not possible to predict precisely where and when particular emergency response services and resources might be needed. Therefore, such services should be accessible as broadly as possible -- anywhere in the emergency geospatial area and by any participant (legal/regulatory constraints and economics permitting). This pattern fosters and facilitates ubiquity through enabling information sharing among a broader set of emergency response participants, including non-governmental organizations and the general public.

The senders and recipients of emergency messages SHALL be as explicit as possible to ensure the timeliness and completeness of emergency response.

1.1.1.2 Dynamism

The next most critical principle for this operational pattern is Dynamism. The ability to adapt to circumstances is practically the definition for effective emergency response. It is critical for sustained operations after initial circumstances have been assessed. As many disasters in the 2000s showed, it is often the public that proves to be the most dynamic and adaptable in using the tools of the Internet to find friends and family and to report rapidly evolving conditions, both in the most-affected areas and in the less-affected areas nearby or contiguous with the main incident area. The challenge to official jurisdictions is to step up their capabilities to match ongoing technological development and to implement policies that relax information-sharing constraints in emergency contexts. Of particular concern here are liability issues and privacy constraints that would otherwise constrain emergency responsiveness and information exchange.

1.1.1.3 Globalism, Relationship Management and Pragmatism

The principle of Globalism is important, but the approach of this pattern should not be seen as a one-size-fits-all model. This pattern and the standards it uses provide enough flexibility to cover the needs of most, if not all, emergency incidents. That flexibility provides the kind globalism found in the solution that the pattern is built upon. That solution is a ***playbook*** that also combines the features of a checklist and a script. Seeking wide (if not completely global) adoption, this pattern aims to achieve that kind of Globalism as well.

To provide the widest possible adoption, this pattern needs to be followed, especially with regard to implementing the standards that allow for data interoperability among different jurisdictions that need to share information. However, the standards as well as the incident command system SHOULD adapt global concepts and techniques to their own situation. And in some situations, there may be multi-national participants who may be using different standards or have already adopted global standards for particular services and data sources/exchanges.

In this regard, the principle of Relationship Management as it relates to managing relationships among the components of the emergency incident response is critically important. Whether this occurs within a given Incident Command Center (ICS) or between and across mutual aid partners, this practice SHALL be tempered with the net-centric principle of Pragmatism. What will work SHOULD be chosen over jurisdictional protocol, if that is known. For instance, if two jurisdictions use different frequencies and wavelengths for the radio communications for police, fire and/or Emergency Medical Technician (EMT) responders, they should be aware of that and use whichever set is likely to work best in any given situation.

1.1.1.4 Entity Primacy

In an emergency response context, participants and service providers need to recognize that no one jurisdiction or organizational perspective has a monopoly on how entities/objects are named or identified (e.g., vehicle identification/number, license plate number, Social Security Number, etc.). They need to respect that others may have different names or IDs for entities /objects concerning the emergency services. This, in essence, is the entity primacy principle. An effective technique for applying this principle is to rely on some ideally context-neutral and "innate" identifiers for these entities/objects. This pattern provides such mechanisms in the TSO CodeList Rules, the recognition that other code lists can be used or modeled, and in the use of Value Lists (see Section 3.1.1).

1.2 Problem Statement

The ability to communicate is at the heart of emergency response. In a serious emergency incident, communications are likely to be disrupted or fail. ***So, the establishment or re-establishment of communications is the first problem that SHALL be solved because all other command functions depend on these communications.***

1.3 Expected Benefits

We expect this pattern to produce tools for first responders that will provide improved response for all incident lifecycle phases, both in quality of service and speed of response.

One of the chief benefits of this pattern will be how well it can be adapted to Civilian-Military Cooperation and Collaboration (CIMIC as it is referred to in Europe and in NATO in particular, or Civilian-Military Operations (CMO as it is referred to in the U.S.).

2 Recommended Solution

This pattern prescribes a playbook approach to solve the complexity and difficulty of emergency communications, beginning from the most immediate local level following the onset of the emergency incident up to the scale of national and international involvement.

Initially, in almost all kinds of emergency incidents, the first communication comes from an individual on scene to the appropriate Public Service Answering Point (PSAP) or from an automated sensor on scene to its control system. This may be the 911 network or local emergency agency dispatch service. This is the point at which the playbook of emergency communications SHALL start.

Additionally, emergency services SHALL allow for appropriate response to all phases of emergency incidents:

- Preparation or Preparedness including training and exercises
- Operational Response, also known as Mitigation
- Demobilization and return of resources to owners
- After-Action Analysis leading to improvements in Preparation or Preparedness

Our recommendation is a playbook of processes/procedures that can be applied to any emergency incident response at any level of jurisdiction that needs to use it and among as many jurisdictions, agencies or military organizations that need to work together on a common incident. Each of the elements in the playbook will focus on one particular aspect of emergency communications and information sharing and will use one or several standards in the communications conducted within the response to the emergency incident.

2.1 Actors

Ideally, the actors that require this operational playbook and the technologies inherent in the various specifications start with the initial sensor report and extend to all emergency personnel and their IT tools in the Incident Command System (ICS).

We SHALL also include members of the public with whom appropriate, relatively secure and trusted communications also need to be established. To list and describe all roles that require actors involved in a given emergency incident response would be prohibitive, especially since job titles (or what we call role names) can vary from jurisdiction to jurisdiction; thus we will only provide general descriptions of the actor roles involved. This will include indirect actors that may provide or receive input as a result of Net-Centric Pattern (NCP) use, such as property owners and operators whose specific geopolitical address-based assets may be included within the data processed to respond accurately to the area of the incident.

Maps displaying meaningful icons or picture thumbnails are “worth a thousand words” if the intended viewers understand the visual methodology, and information accompanied by GPS coordinates can be placed on maps. The map context serves to locate the associated information accurately and immediately.

While our approach begins with the use of appropriate standards that allow for sharing information correctly with no loss of context across and within jurisdictional boundaries, we are also mindful that a Common Operational Picture (COP) is needed. This NCP will prescribe the elements of the COP and how the playbook allows for the information exchange to be represented on any conformant base-mapping system. A conformant base-mapping system may range from free Google Maps to proprietary products with greater capabilities, provided the Coordinate Reference System (CRS) is properly identified. Our recommendation, however, will be for the minimum low- or no-cost options that can be provided to jurisdictions and agencies with less funding than more affluent jurisdictions.

The following list identifies actors in the NCP context. The categories include their ICS support personnel.

2.1.1 Emergency Responders

These actors most often fall into three categories:

- Law Enforcement
- Firefighters
- Emergency Medical Technicians (EMTs)

2.1.2 Affected Public

These actors most often fall into two categories:

- Non-Injured or Slightly-Injured, who may or may not need to be transported to shelter
- Injured requiring emergency medical triage, treatment and transport to a field hospital or community hospital

2.1.3 IT Personnel

These actors provide support for the front-line responders and fall into three categories:

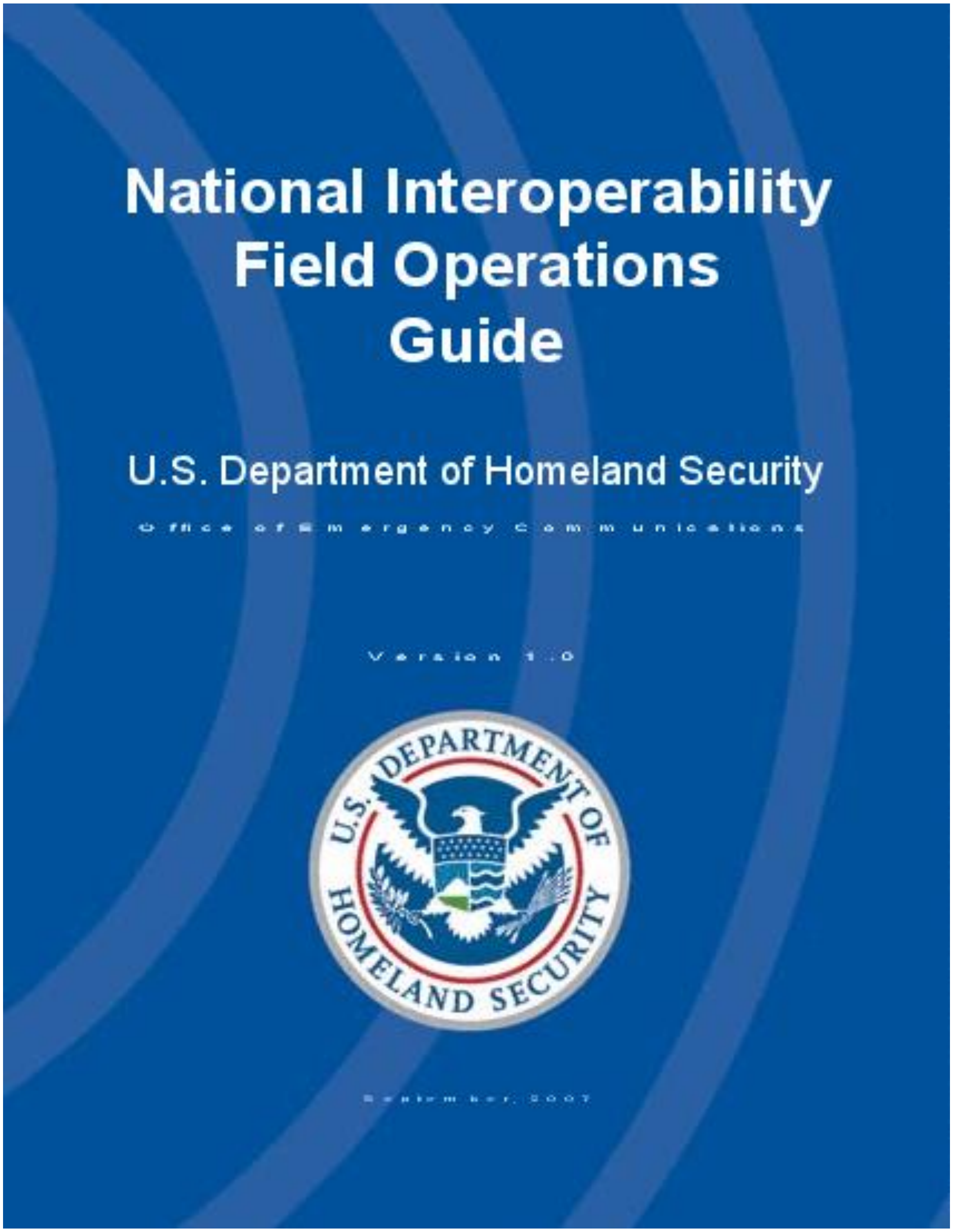
- Software Engineers or Providers who offer installation, configuration and maintenance contracts to community emergency agencies
- Data Center technicians whose support allows first responders and ICS personnel to do no more than minimal input into their handheld or suit-mounted smart-phone/mini-tablets or similar devices
- Emergency Management IT Standards Developers, such as the principal author of this pattern, who need to stay in a reciprocal relationship with the emergency-response community to improve existing standards and new standards such as the EDXL-Tracking Emergency Patients (EDXL-TEP) v1.0[4] specification that was ongoing during the development of this pattern; EDXL-TEP is being developed in close association with the Health Level Seven International organization[5]

2.2 Interfaces

The characteristics of interfaces between various emergency IT systems and actors, embodied in most cases through emergency services offered within the emergency services SOA ecosystem, are described in this section. As we stipulate, these emergency services will most often be implemented through communications applications that govern the visibility, description and governance of the services.

2.2.1 Key Guidance

In the United States, the Department of Homeland Security (DHS) has issued guidance on establishing communications in emergencies through The National Interoperability Field Operations Guide (NIFOG)[6]. NIFOG is a technical reference for emergency communications planning and for radio technicians responsible for radios that will be used in disaster response.



National Interoperability Field Operations Guide

U.S. Department of Homeland Security

Office of Emergency Communications

Version 1.0

September, 2007

Figure 3 National Interoperability Field Operations Guide

A great deal of this pattern will draw upon Version, 1.4 of this work, issued in 2011. The NIFOG provides a national framework that is published and maintained. It includes specific interoperability frequencies and will work with the OASIS Emergency Management Technical Committee's Emergency Data Exchange Language (EDXL) suite of standards. It is particularly important to the effort to establish interoperability as a working principle and to use guidance such as this Emergency Services Operational Pattern to pave the way forward as it provides a national framework that can be used as an example and as a starting point for moving forward on an international framework.

2.2.2 COP: Single Gateway

A tool that displays a Common Operating Picture of emergency information can be displayed across jurisdictional boundaries and can offer a single gateway into multiple specific interfaces that implement the EDXL suite. As an example, we refer to the VirtualUSA work done by many jurisdictions and supported by DHS Science and Technology, which also supports most of the other components we detail in this pattern.

This NCP also stipulates using the common symbology offered in the Federal Geographic Data Committee (FGDC) Homeland Security Working Group Emergency Symbology Reference.[7] This nationwide data-publishing effort is known as the National Spatial Data Infrastructure (NSDI).[8]

The specific interfaces enumerated in Section 2.2.3 SHOULD be offered as component emergency services, composed within a layer, or set of layers, in the COP.

Because all of these emergency services SHALL necessarily include and focus on the locations or areas of incidents, equipment, responders, at-risk public, etc., such emergency services are thought of as "location-based" services. We suggest, however, that these services should be thought of as simply "emergency" services.

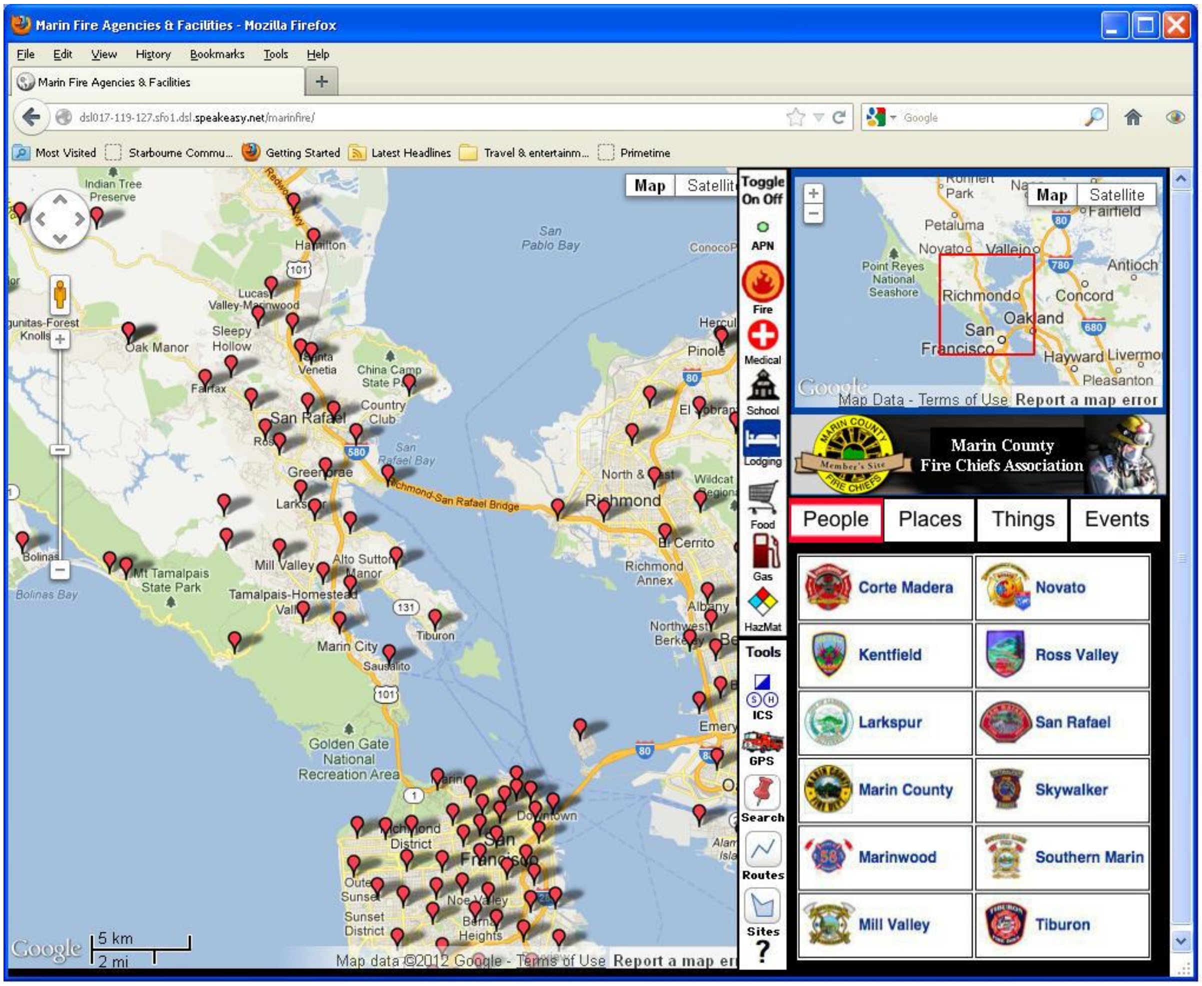


Figure 4 Common Operating Picture for Marin County, California highlighting fire stations

These interfaces can take many forms but the form preferred by this operational pattern is one that uses a Common Operational Picture (COP), independent of any software.

While the visual picture may be slightly different in different software, it SHOULD capable of being accurately displayed on the range of devices needed, from desktop Emergency Operations Center (EOC) systems to handheld devices on scene. The current information shared in the display of each emergency service layer (i.e. CAP Service layer, EDXL-RM Service layer, etc.) should be viewable and accurate.

This is best done with sets of layer-specific icons for information about locations or physical object resources available in that layer, from vehicles to fire hydrants. This SHOULD apply to all information categories, from critical protected infrastructure like utilities, schools and hospitals, to locations of hazardous materials like combustibles in a local gas station. The COP is the gateway to the information used in these specific interfaces, so it SHALL accommodate all data that needs to be represented. This is critical for interactions between actors from different jurisdictions and the system(s) or SOA software services associated with this pattern. A SOA software service might, for instance, automatically access or load current data available from members of a local mutual aid agreement.

The interfaces themselves need not be, and probably should not be, visible to the responder-user. For example, clicking on the icon for a fire station in an adjacent jurisdiction should indicate whether its equipment and crews are available to be requested, and the underlying application should make it possible for those resources to be requested, requisitioned and returned without requiring any action from a responder-user. Such actions as are necessary to conduct these exchanges would only need to be seen by an EOC user.

The COP will need to incorporate the various levels of information technology standards that apply. The following diagram shows the structure within which these standards provide data interoperability across jurisdictions.

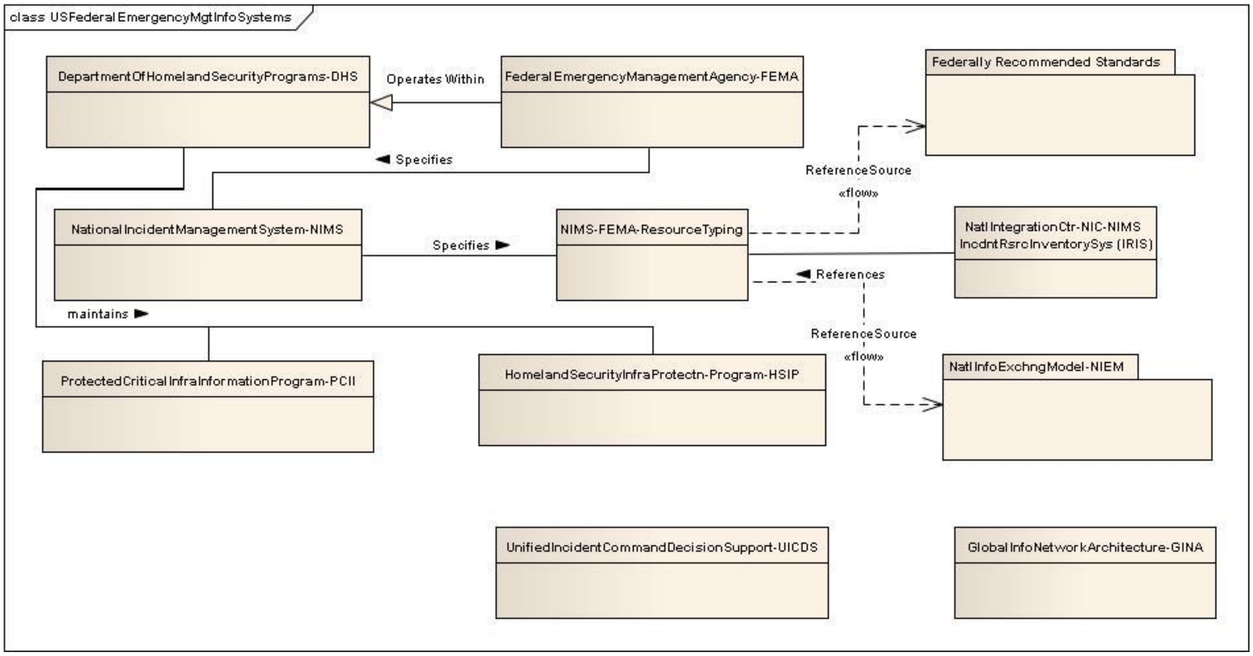

class USFederal EmergencyMgtInfoSystems
DepartmentOfHomelandSecurityPrograms-DHS
Operates Within
Federal EmergencyManagementAgency-FEMA
Federally Recommended Standards
◄ Specifies
ReferenceSource
«flow»
National IncidentManagementSystem-NIMS
Specifies ►
NIMS-FEMA-ResourceTyping
Natl IntegrationCtr-NIC-NIMS IncdntRsrcInventorySys (IRIS)
◄ References
maintains ►
ReferenceSource
«flow»
ProtectedCriticalInfraInformationProgram-PCII
HomelandSecurityInfraProtectn-Program-HSIP
Natl InfoExchngModel-NIEM
UnifiedIncidentCommandDecisionSupport-UICDS
Global InfoNetworkArchitecture-GINA

Figure 5 US Federal Emergency Management Information Systems -- High-Level View

2.2.3 OASIS EDXL Standards: Basis for Emergency Services

For the most part, each emergency service in this pattern is based on one or more of the EDXL suite of IT standards developed by the EMTC. Interfaces to all of the OASIS Emergency Data Exchange Language standards should be available through the COP.

Briefly, these interfaces should implement the latest available versions of

- An **EDXL Common Alerting Protocol** (CAP) Interface represented in the NCOIC All-Hazards Alerts and Warnings Capability Pattern[9]
- An **EDXL-Distribution Element** (DE) or its equivalent as the wrapper/header and as the interface to all emergency messaging-based communications[10]
- An **EDXL Hospital AVailability Exchange** (EDXL-HAVE) Interface for sending and receiving timely, up-to-the-instant snapshots of a hospital's capabilities, usually expressed in terms of available bed types[11]
- An **EDXL Resource Messaging** (EDXL-RM) Interface to handle all aspects of logistics management in an incident[12]

- An **EDXL Situation Reporting** (EDXL-SitRep) Interface, when this specification is approved, for providing timely decision support to ICS
- An **EDXL Tracking Emergency Patients** (EDXL-TEP) Interface for handling electronic health-encounter records prior to handoff to a hospital system, to also be used when it is approved

These standards and specifications are discussed in more detail in Sections 2.7 - 2.7.5.6. Regardless of the software deployed, this NCP needs and expects

- Neighboring jurisdictions to agree to similar icons per layer for deployable resources
- Emergency communications among cooperating jurisdictions to communicate directly
- Databases of deployable resources among cooperating jurisdictions to exchange data
- Availability of resources like firefighting equipment and personnel to be shared

However, to a fairly great extent, law enforcement policy may require that information sharing over the Internet be more closely monitored and restricted. Similarly, if the military is involved, its communications within its own ICS would likely be restricted. Thus these interfaces wouldn't ordinarily be available to EMTs through the COP, for instance. This shows the need for the principles of pragmatism and dynamism.

Static interfaces, such as EDXL-Hospital AVailability Exchange (EDXL_HAVE) snapshots of a hospital's current capabilities, and more dynamic interfaces, defined in Section 2.5, for EDXL-Resource Messaging (EDXL-RM) SHALL both be accommodated by COP-based display systems. The following diagram shows the overall EDXL distribution element, the header/wrapper element used to route emergency messages.

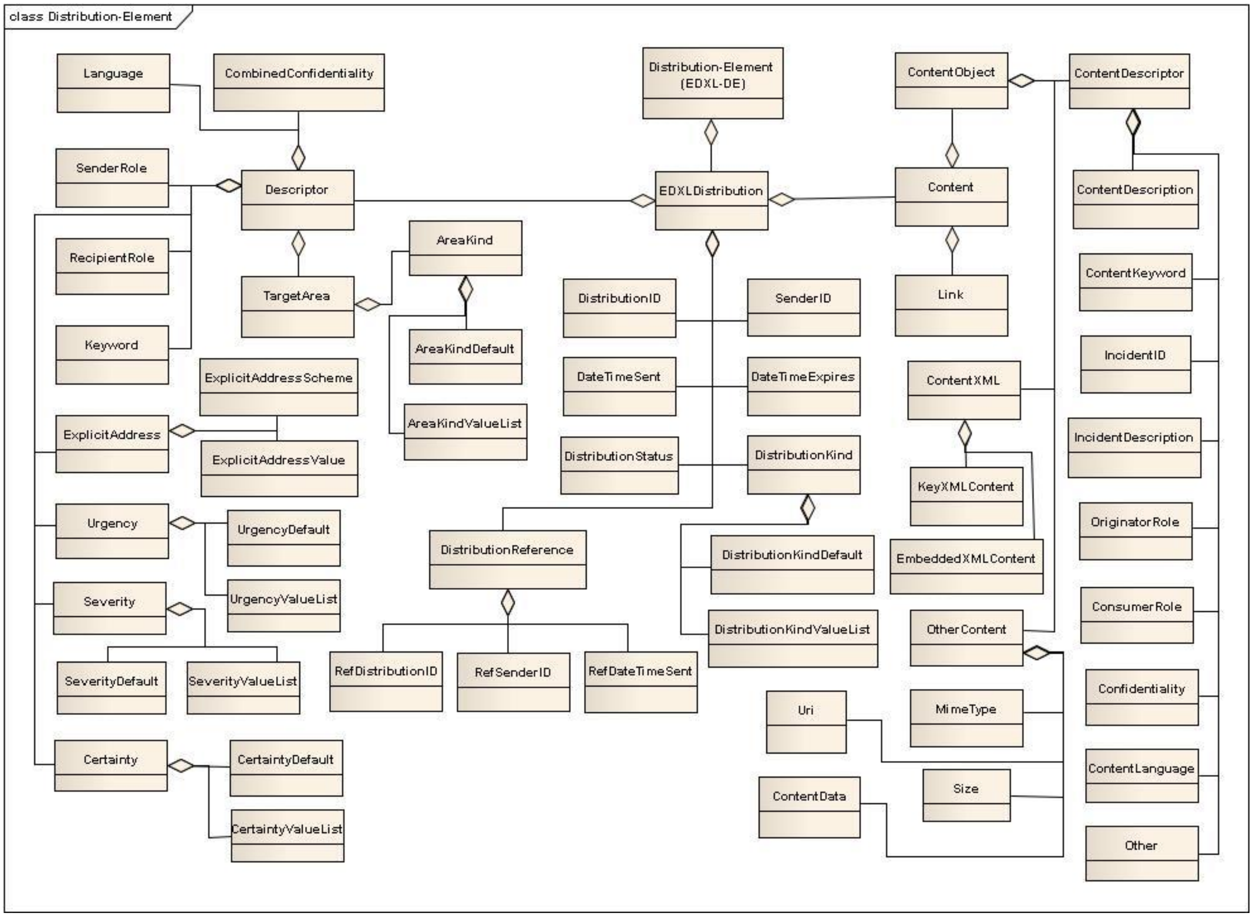


Figure 6 The Emergency Data Exchange Language Distribution Element v1.0

The actual software interactions between systems SHOULD be opaque to all necessary users during operations. This is of the utmost importance since we SHALL make emergency services a part of ordinary everyday operations and not something only used in emergencies. This is critical to accomplishing the widespread uptake necessary to make net-centric interoperability work correctly.

2.3 Pre-Conditions

When used solely ***within*** a jurisdiction, there are few pre-conditions for employing this pattern, other than the use of emergency communications software that implements the standards that allow data interoperability. However, it is important to understand that the tools used in this pattern SHALL be the same as those in ordinary daily operations.

In other words, zoning, permits and planning agencies need to use the same or similar vocabularies that allow clear information sharing. Data systems for emergency operations among cooperating jurisdictions SHOULD be capable of sharing data. More stringent pre-conditions apply for data interoperability ***across*** boundaries between cooperating jurisdictions.

For boundary-crossing data interoperability, certain operational states SHALL exist before the NCP can be applied, specifically a network of networks similar to the U.S. DHS-Federal Emergency Management Agency (FEMA) Open Platform for Emergency Networks (OPEN)

.This ensures that all cooperating jurisdictions apply the standards in a way that is conformant with the stated requirements in the standards.

If the stated pre-conditions are not met, the pattern cannot be successfully implemented. This does place a requirement on jurisdictions that could be difficult, and for this reason, all measures should be taken that can allow smaller, less-affluent jurisdictions to implement standards in conformance with the requirements.

Note: an emergency declaration should not be needed for cooperating jurisdictions to share data and information.

2.4 Structure

The infrastructure discussed in this NCP is based on systems similar to the U.S. DHS-FEMA OPEN. The technical approach for enabling interoperability of emergency services available to jurisdictions worldwide is Service-Oriented Architecture (SOA).

The scope for this operational pattern is global, even though some of the components are based on U.S. Government-developed models. Because it needs to support civilian-military collaboration and cooperation, special effort is made to include contingencies for humanitarian aid during large-scale incidents from the military domain.

2.4.1 SOA Ecosystem

One of the chief characteristics of the U.S. DHS-FEMA-OPEN network-of-networks model is that it is decentralized. This means that there is no single point of failure that can cripple the incident-response effort. Combining this with SOA means that response efforts can take advantage of the SOA ecosystem supporting the network-of-networks approach. This kind of SOA ecosystem is described in the OASIS Reference Architecture Foundation[13] for SOA (SOA-RAF).

2.4.1.1 Visibility and Reachability

Emergency services offered in this pattern SHALL be visible and reachable, manifestations of the ubiquity principle.

One of the key requirements for jurisdictions interacting with each other in the context of a SOA ecosystem is achieving ***visibility*** before SOA/software services can share information and interoperate. The participants have to be visible to each other using whatever means are appropriate. This may be achieved through third-party registry/repository services or members of a local mutual-aid group may set up their cooperating systems in a regional peer-to-peer agreement.

Service ***reachability*** allows participants to locate and interact with one another. To support service reachability, the service description of which jurisdictions need to exchange with each other should indicate the ***endpoints*** to which the jurisdiction acting in the role of service consumer can direct messages to invoke actions. The service description for these emergency services should include the protocol to be used for message exchange using their endpoints.

For instance, a jurisdiction X, in which a residence fire incident is occurring, may need to request the use of a certain kind of fire engine and crew. So, it needs to be able to send a request for that type of engine and crew to the jurisdiction Y provider service. Likewise, the responding jurisdiction Y SHALL be able to send confirmation to jurisdiction X.

In SOA terms, the endpoint is the conceptual location where one applies an action; with respect to service description, it is the actual address where a message is sent.

This is a simplification, but the point remains that there needs to be this kind of interaction as well as others that allow the requested resource to be deployed where needed and its use to be properly accounted.

However, neither the incident commander from jurisdiction X on scene, nor the ICS operator in jurisdiction Y needs to actually see or be aware of these messaging interactions. In fact, this would cause unnecessarily delay in real-world actions; in fact, such actions should not be concerned with the exchange of messages between systems and networks. Both consumer and provider should be able achieve their purposes through the mutual use of a Common Operating Picture, while the tracking and accounting functions are accomplished without human supervision or intervention unless an error occurs. In that case, only the ICS operator should be aware of it and should be capable of taking whatever remedial action is necessary to achieve the desired outcome.

The following diagram shows how a SOA Service Description SHOULD set the stage for such automatic actions, if the service description is accurate and the network is available.

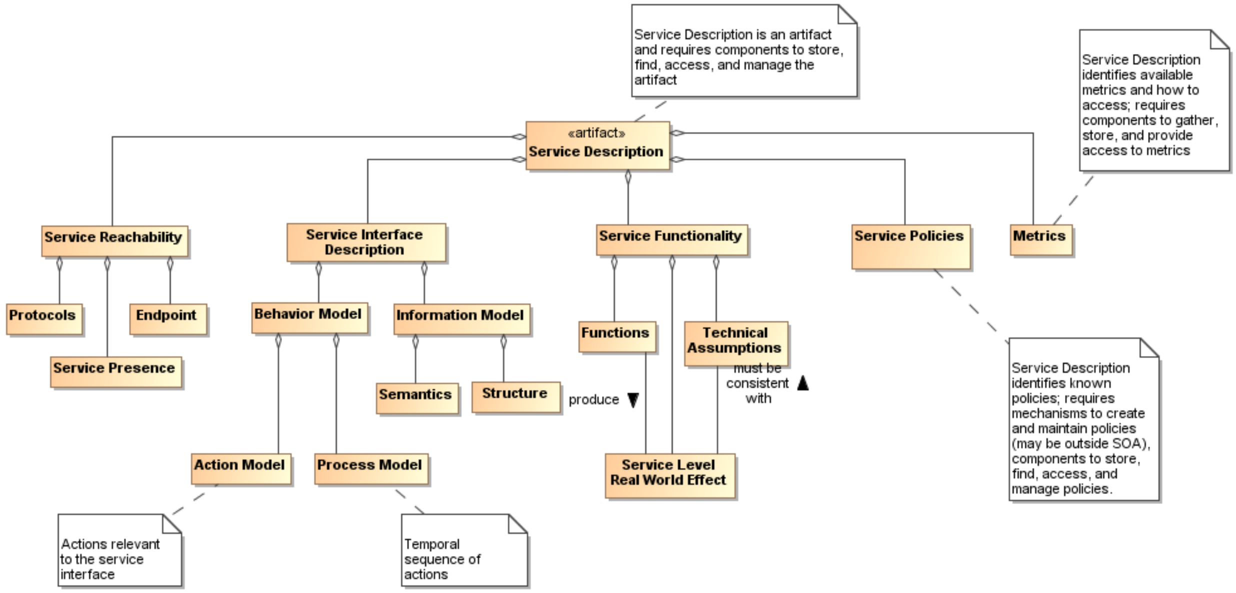

Service Description is an artifact and requires components to store, find, access, and manage the artifact
Service Description identifies available metrics and how to access; requires components to gather, store, and provide access to metrics
«artifact»
Service Description
Service Reachability
Service Interface Description
Service Functionality
Service Policies
Metrics
Protocols
Endpoint
Service Presence
Behavior Model
Information Model
Semantics
Structure
Functions
Technical Assumptions
produce
must be consistent with
Service Level Real World Effect
Action Model
Process Model
Service Description identifies known policies; requires mechanisms to create and maintain policies (may be outside SOA), components to store, find, access, and manage policies.
Actions relevant to the service interface
Temporal sequence of actions

Figure 7 Service Description from the
OASIS Reference Architecture Foundation for Service Oriented Architecture[13]

2.5 Behavior

At the outset of an incident, the playbook should be consulted. The purpose for outlining a series of actions in a sequence is to ensure that necessary steps are taken so that important information is not neglected because there may be confusion during the actual emergency. In addition, the playbook is intended to be used on an ordinary, daily basis. The result is less temptation to abandon normal procedure in the face of an emergency. This should also improve performance and reinforce the confidence of the public and responders alike.

2.5.1 Initial Sensor Report

An initial sensor report triggers incident response. This can be accomplished by an automated sensor within a given jurisdiction, or a report originating from a citizen's 911 phone call. This initial sensor report triggers the first action that the jurisdictional authority will take.

2.5.2 Establish Communications

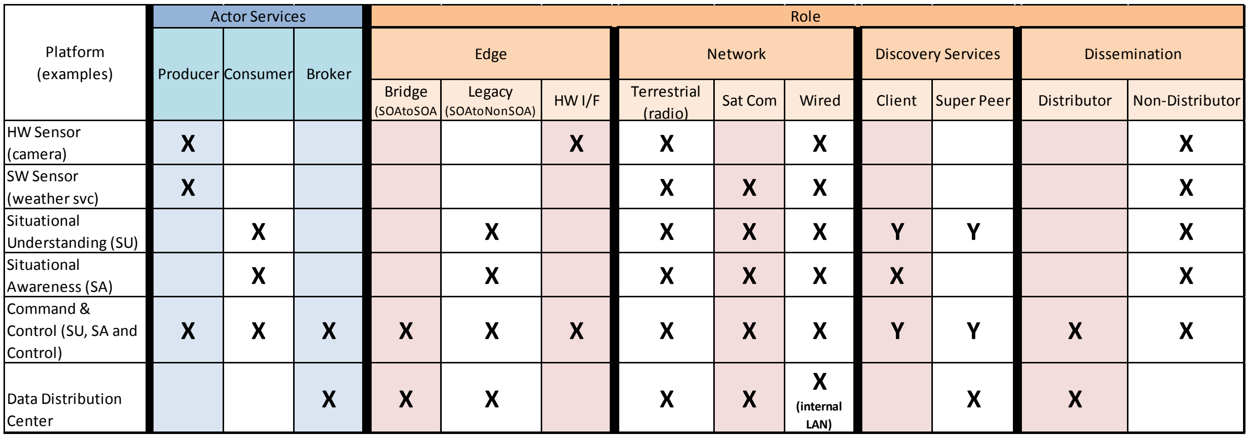
The rapid establishment of which communications channels are available and which will be used by which agencies will be the first action in the playbook. This is of the utmost importance. This will be followed by the most rapid dissemination of information through the communications channels available. It may be necessary to use the step-by-step discovery of usable communications detailed in the NCOIC Discontinuous, Intermittent and Limited (DIL) Communications Management Technical Pattern.

In Section 1.1 Context of the DIL pattern this is described

> *"A major interoperability problem in the deployment of heterogeneous networks is the coordination of the capacity allocation algorithms associated with, or embedded in, the control of each type of network device. Capacity allocation is an essential underpinning for the proper operation of network-centric services."*

This is the only set of actions that does not directly use any of the OASIS EDXL Standards, but it does use the standards detailed within the DIL Pattern. Additionally, the appropriate actions described in the NCOIC Multi-level Distributed Discovery and Dissemination Capability Pattern (MD3).

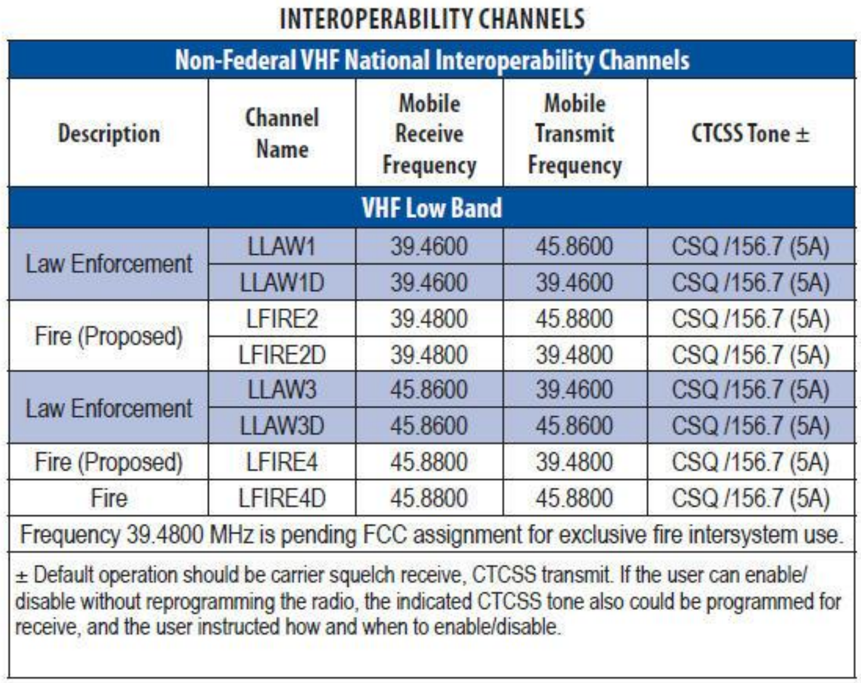
The MD3 Pattern specifies how to discover, provision, and maintain a mobile ad-hoc network (MANET) of the type we expect to need in the earliest stages of a fairly major emergency incident. This is contained in sections that specify network entity components and the table copied below.



Platform (examples)	Actor Services			Role									
				Edge			Network			Discovery Services		Dissemination	
	Producer	Consumer	Broker	Bridge (SOAtoSOA	Legacy (SOAtoNonSOA)	HW I/F	Terrestrial (radio)	Sat Com	Wired	Client	Super Peer	Distributor	Non-Distributor
HW Sensor (camera)	X					X	X		X				X
SW Sensor (weather svc)	X						X	X	X				X
Situational Understanding (SU)		X			X		X	X	X	Y	Y		X
Situational Awareness (SA)		X			X		X	X	X	X			X
Command & Control (SU, SA and Control)	X	X	X	X	X	X	X	X	X	Y	Y	X	X
Data Distribution Center			X	X	X		X	X	X (internal LAN)		X	X	

Figure 8 Potential MANET Components

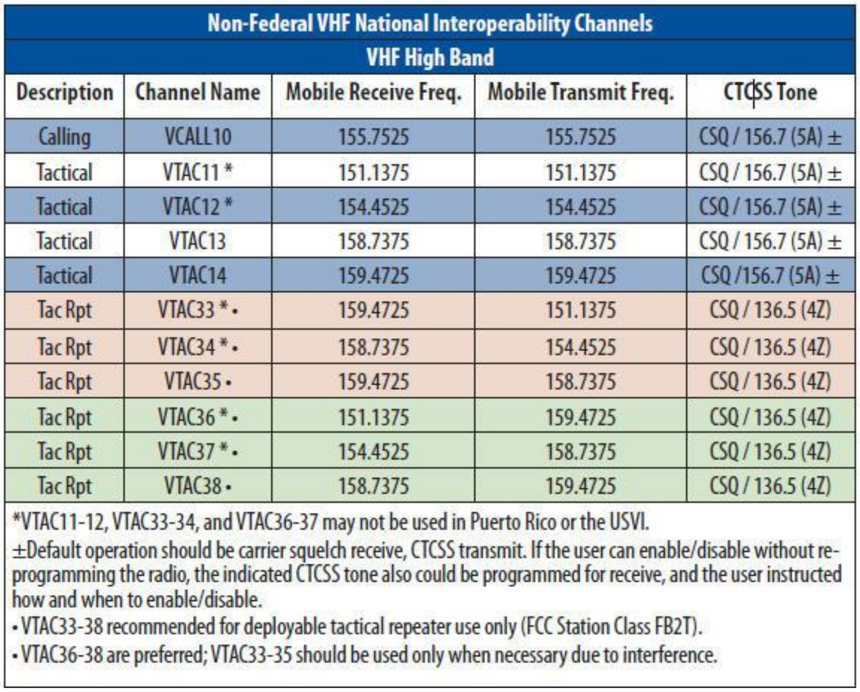
In its simplest terms, we SHALL create a working mesh network from the incident to the local emergency-management agencies within the jurisdictions in which they operate, and work from there to increase communications capabilities as the incident response proceeds. As noted in Section 2.2.1, the NIFOG provides vital information for interoperability shown in the following figures for interoperability channels.



INTEROPERABILITY CHANNELS

Non-Federal VHF National Interoperability Channels				
Description	Channel Name	Mobile Receive Frequency	Mobile Transmit Frequency	CTCSS Tone ±
VHF Low Band				
Law Enforcement	LLAW1	39.4600	45.8600	CSQ /156.7 (5A)
	LLAW1D	39.4600	39.4600	CSQ /156.7 (5A)
Fire (Proposed)	LFIRE2	39.4800	45.8800	CSQ /156.7 (5A)
	LFIRE2D	39.4800	39.4800	CSQ /156.7 (5A)
Law Enforcement	LLAW3	45.8600	39.4600	CSQ /156.7 (5A)
	LLAW3D	45.8600	45.8600	CSQ /156.7 (5A)
Fire (Proposed)	LFIRE4	45.8800	39.4800	CSQ /156.7 (5A)
Fire	LFIRE4D	45.8800	45.8800	CSQ /156.7 (5A)
Frequency 39.4800 MHz is pending FCC assignment for exclusive fire intersystem use.				
± Default operation should be carrier squelch receive, CTCSS transmit. If the user can enable/disable without reprogramming the radio, the indicated CTCSS tone also could be programmed for receive, and the user instructed how and when to enable/disable.				

Figure 8 Interoperability Channels from NIFOG



Non-Federal VHF National Interoperability Channels				
VHF High Band				
Description	Channel Name	Mobile Receive Freq.	Mobile Transmit Freq.	CTCSS Tone
Calling	VCALL10	155.7525	155.7525	CSQ / 156.7 (5A) ±
Tactical	VTAC11 *	151.1375	151.1375	CSQ / 156.7 (5A) ±
Tactical	VTAC12 *	154.4525	154.4525	CSQ / 156.7 (5A) ±
Tactical	VTAC13	158.7375	158.7375	CSQ / 156.7 (5A) ±
Tactical	VTAC14	159.4725	159.4725	CSQ /156.7 (5A) ±
Tac Rpt	VTAC33 * •	159.4725	151.1375	CSQ / 136.5 (4Z)
Tac Rpt	VTAC34 * •	158.7375	154.4525	CSQ / 136.5 (4Z)
Tac Rpt	VTAC35 •	159.4725	158.7375	CSQ / 136.5 (4Z)
Tac Rpt	VTAC36 * •	151.1375	159.4725	CSQ / 136.5 (4Z)
Tac Rpt	VTAC37 * •	154.4525	158.7375	CSQ / 136.5 (4Z)
Tac Rpt	VTAC38 •	158.7375	159.4725	CSQ / 136.5 (4Z)
*VTAC11-12, VTAC33-34, and VTAC36-37 may not be used in Puerto Rico or the USVI. ±Default operation should be carrier squelch receive, CTCSS transmit. If the user can enable/disable without re-programming the radio, the indicated CTCSS tone also could be programmed for receive, and the user instructed how and when to enable/disable. • VTAC33-38 recommended for deployable tactical repeater use only (FCC Station Class FB2T). • VTAC36-38 are preferred; VTAC33-35 should be used only when necessary due to interference.				

Figure 9 Interoperability Channels High Band

2.5.3 Connect Best Case Mesh Network through the Common Operating Picture

The COP gateway incorporates individual interfaces for discrete emergency services, so it uses the combined databases used in those emergency services for the local or regional agencies involved in the incident response. Orienting all activities to a base map as the single key interface for all operations is essential and SHALL also be accomplished using the ordinary, daily tools of responders. This will undoubtedly create a period of adjustment, as this kind of implementation is established widely, but it will repay our efforts by greatly increasing our ability to respond to emergency incidents quickly and appropriately.

2.5.4 The DHS-FEMA-IPAWS OPEN Network of Networks Model using EDXL-DE

If the situation warrants it, this federal network of networks can be used, especially if the scale of the incident is such that a combined response is likely to rise to the national level.

The Department of Homeland Security (DHS), through the Federal Emergency Management Agency's (FEMA's) Integrated Public Alert and Warning System (IPAWS), provides a network of networks based largely on the EDXL-CAP and, more recently, the EDXL-DE, which allows all of the EDXL message payload types available for emergency communications.

If used, this network model serves as the basis for the dynamic interaction of the structural elements embodied in the individual message standards and the specific interfaces used by the actors described in the prior sections. This architecture is made available to properly authorized Common Operating Groups (COGs)

IPAWS provides two sets of Simple Object Access Protocol (SOAP) web services:

1. Its CAP aggregator service accepts and validates CAP messages for the following functions:
   - Organization-to-organization (cog-to-cog) direct exchange
   - Emergency Alerting System (EAS) broadcast
   - Cellular Mobile Alerting Service (CMAS) distribution via Wireless Emergency Alerts (WEA)
   - Non-weather emergency messages for broadcast over National Oceanic and Atmospheric Administration (NOAA) radio
   - A pin-restricted feed of all public IPAWS profiles conforming CAP messages for use by re-distributors (e.g. Google Alerts)
2. Its distribution element service accepts valid DE messages for cog-to-cog exchange only. It does no validation of internal DE content. It does not use the DE metadata for routing except for <explicitAddress>, which is used to identify intended cogs in the cog-to-cog exchange.

2.5.5 Reuse of Data Types and Models

During the development of the OASIS Emergency Management IT Standards, it was discovered that certain kinds of information are used in most of the specifications in the EDXL family. This information was put into the set of such reused information in the Supporting Elements Model shown in Figure 1. This is discussed further in Section 2.9.

CAP is the standard most used at the time this pattern is being written. This standard is used between government agencies, from the public to government in some cases, and from the government to the public in most cases, since that is the prime purpose of CAP. As the groundbreaking effort, CAP has also moved through several v1.x versions. Much of what was learned came through the work on CAP. We have learned to reuse data types and to continue working on the overall data model of the EDXL suite.

2.5.6 Secondary Major Steps

- Establish or revise ICS (most likely local at inception, then changing to county, state or national as warranted)
- Use latest available version of EDXL-DE to route and track (automatic date-time stamped) emergency messages (EDXL-DE 1.0 or 2.0 -- bear in mind that availability also refers to an ICS's currently installed version, not only the version approved by OASIS)
- Send and/or relay EDXL-CAP v1.2 (or latest version) alerts to affected public and any Integrated Public Alert and Warning System (FEMA-IPAWS) or Emergency Alert System (EAS) messages
    - Affected public is defined by geospatial extent of incident – combination of geographical and geopolitical areas
- Compile initial EDXL SitRep Reports for ICS decision making
- Issue response orders
- Monitor alert updates, network system status
- Assess resource availability (EDXL-RM, EDXL-HAVE) and monitor actively
- Schedule shift and ICS updates
- Repeat appropriate actions until incident is declared over

2.6 Developing Emergency Services

It ought to be noted that any individual action step above can be a separate emergency service or aggregated together with others in any combination. Development of emergency applications and emergency services for this domain ought to be done in close association with front-line responders as well as incident commanders and tested as much as possible during development. It is necessary, as noted in Section 2.3, to make certain that these emergency services are included in ordinary, daily responder activities, not reserved for major emergencies when they would not be used for lack of practice and familiarity.

The following diagram illustrates how this pattern fits into the current existing set of NCOIC patterns and OASIS EDXL standards. Taken together, these patterns and standards set the stage for a vigorous and wide-ranging SOA ecosystem in which the emergency services implement this pattern and the standards cited.

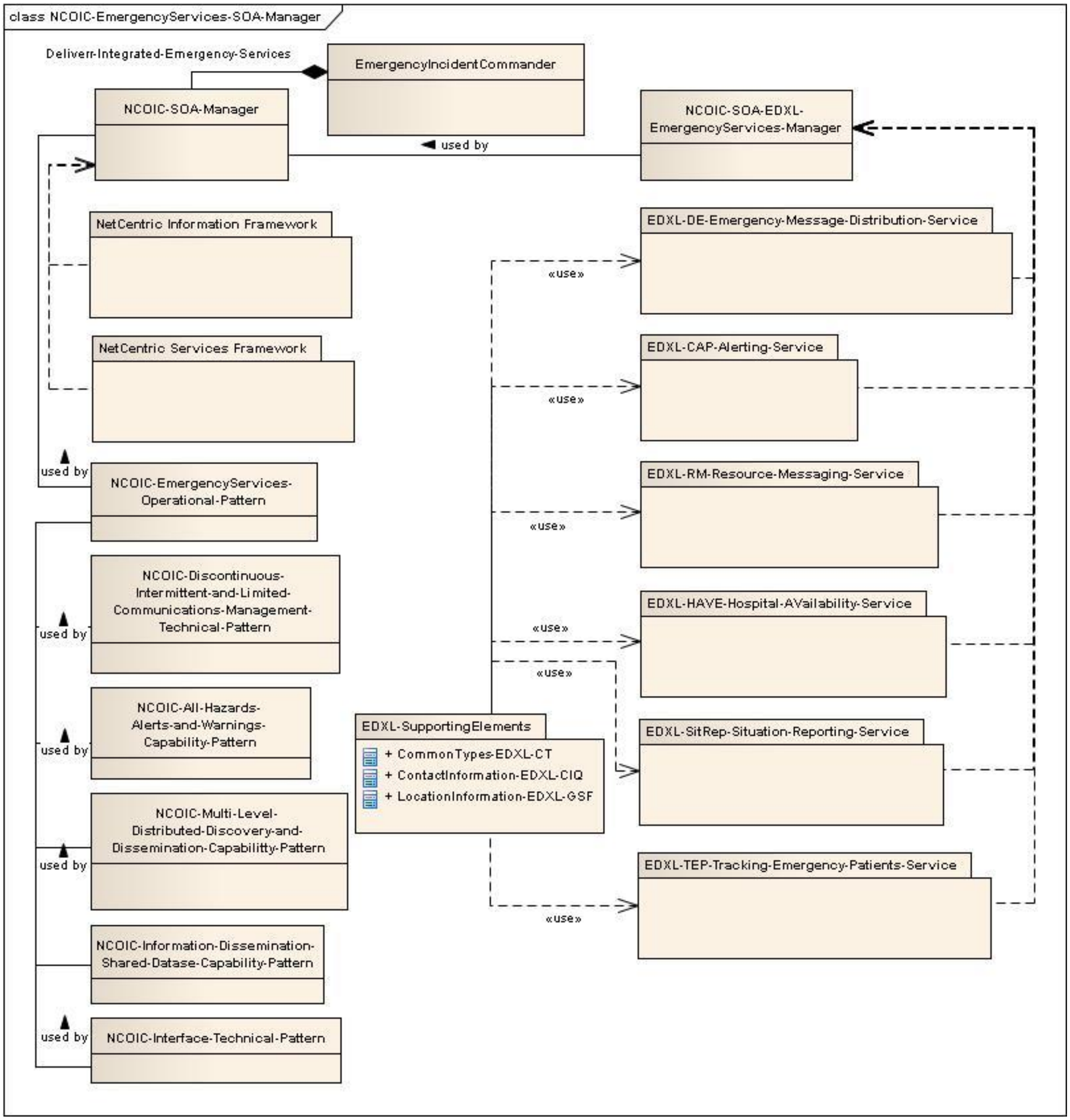

class NCOIC-EmergencyServices-SOA-Manager
Deliverr-Integrated-Emergency-Services
EmergencyIncidentCommander
NCOIC-SOA-Manager
used by
NCOIC-SOA-EDXL-EmergencyServices-Manager
NetCentric Information Framework
NetCentric Services Framework
EDXL-DE-Emergency-Message-Distribution-Service
EDXL-CAP-Alerting-Service
EDXL-RM-Resource-Messaging-Service
EDXL-HAVE-Hospital-AVailability-Service
EDXL-SitRep-Situation-Reporting-Service
EDXL-TEP-Tracking-Emergency-Patients-Service
«use»
«use»
«use»
«use»
«use»
«use»
used by
NCOIC-EmergencyServices-Operational-Pattern
used by
NCOIC-Discontinuous-Intermittent-and-Limited-Communications-Management-Technical-Pattern
used by
NCOIC-All-Hazards-Alerts-and-Warnings-Capability-Pattern
EDXL-SupportingElements
+ CommonTypes-EDXL-CT
+ ContactInformation-EDXL-CIQ
+ LocationInformation-EDXL-GSF
used by
NCOIC-Multi-Level-Distributed-Discovery-and-Dissemination-Capabilitty-Pattern
NCOIC-Information-Dissemination-Shared-Datase-Capability-Pattern
used by
NCOIC-Interface-Technical-Pattern

Figure 10 Relationships of Patterns and Standards for the NCOIC Emergency Services Operational Pattern

2.7 Post-Conditions

This Emergency Services Operational Pattern differs from more narrowly focused patterns due to the fact that it models a range of services for incident command, including the time period that might otherwise be thought of as the time when post-conditions apply. Specifically, this is the period after mitigation, when the incident is declared over. There are no plans to create an

EDXL specification for this period in the lifecycle of emergency incidents. However, there are obvious functions that have been addressed within the existing specification

2.7.1 Resource Return

All resources that have been requested, ordered, requisitioned, deployed and used/consumed will be returned to the owning agency or jurisdictional partner in mutual-aid situations. This is covered in the EDXL-Resource Messaging Standard. Whether vehicles are returned with full fuel tanks, or other resources are returned in a replenished condition, is subject to agreement of the parties involved.

For the purpose of simplicity, trained personnel and equipment are not separated from all other resources, so all management of resources, from scheduling to funds accounting, is handled within the EDXL-RM Standard. This applies to consumables such as gasoline or aviation fuel as well as vehicles like airplanes or construction equipment like bulldozers.

There is no use of the term “asset” to avoid confusion. If encountered in other standards to be used in conjunction with the EDXL suite, accommodations will need to be made unless a prior agreement is in place. Making such accommodations ahead of time is encouraged.

2.7.2 Audit Trail Accounting

The cost accounting needed for emergency services received and emergency-related resources consumed are readily handled if EDXL-Resource Messaging has been used as intended. This is recommend for most standards cited below as they are designed to be used in applications that automatically handle and record transactions without requiring operators to enter information, except by selecting icons and indicating choices from drop-down lists or radio-buttons. This applies to most telephonic or radio communication with resource suppliers. A record of messages pertaining to the incident are automatically kept for later retrieval. It is important to note that this requires that the standard be employed at least by the agency or jurisdiction that receives the emergency services and emergency-related resources, since cost accounting is included in EDXL-RM and can be implemented to be used automatically. However, the standard does not specify how such automation should work. If all parties to the incident response use EDXL-RM within their ICT applications, this should be a much more easily accomplished post-condition. Regardless, the date-time stamped messages will be ready for assembling when needed.

2.7.3 After-Action Analysis

Once the accounting has been done and the reports concerning those issues are compiled, analysis is needed and should be more easily enabled with the combined use of EDXL-RM and EDXL-SitRep, which uses information from EDXL-RM and EDXL-DE as well.

In the following paragraph, italicized text refers to elements within the report types.

EDXL-SitRep includes information such as that contained within the Casualty and Illness Summary for categories like *Fatalities*, *Hospitalized*, *Evacuated*, *Missing*, *Shelter In Place*, *In Temporary Shelter*, etc. that happen over the course of the incident. EDXL-SitRep also includes Response Resources Total for information such as *Resource Personnel Count*, *Unassigned*

Resource Personnel, Resource Detail and *Special Equipment and Supplies*. The Management Reporting Summary Report includes *Damage Assessment Information, Primary Hazards, HazMat Incident Report, Extent of Contamination* and *Infrastructure Affected*.

All of these EDXL-SitRep reports contain many more information elements and the information needed to use them correctly.

2.7.4 Lessons Learned Adjust Preparedness

Based on the after-action analysis, there should be some lessons-learned type reports that should be taken into consideration in making recommendations for how to address those lessons as they apply to improving overall response to the types of incidents documented. These lessons should then be implemented in adjusting normal preparedness to include those recommendations.

Unintended problems and side-effects should be noted and recommendations made to ameliorate these conditions. It is expected that there will be some mismatches in ICS reporting systems for various jurisdictions, and agencies that do not use software that either implements the standards noted below or can either ingest or output information compatible or interoperable with such standards-based software.

2.8 Standards

There are a number of emergency-specific standards that are required or strongly recommended. All of these are open in the sense that the work that has gone into them is available to be viewed and their use is unencumbered by any necessity of membership in any particular group or association. Most of them, particularly the OASIS EDXL Standards, are also free-of-charge for anyone to use. Additionally, all of the OASIS EDXL standards are specifically formulated to be international standards, not U.S.-centric standards. While the submission process uses a DHS-sponsored practitioner steering group, it also passes the requirements and/or candidate specification through the Emergency Interoperability Consortium (EIC) for approval and modification before making the submission to the OASIS EM TC.

Because this operational pattern focuses on the lifecycle of emergency incidents, we focus on those standards; however this should be assumed to use the standards cited in EDXL standards and the SOA-RAF[13].

2.8.1 Emergency Data Exchange Language (EDXL) Suite of Standards

Note: Full Name in table below refers only to the part of the name that follows the acronym EDXL which is not repeated.

Acronym & Version	Full Name	OASIS-Approved Date	Approval Pending
EDXL-CAP v1.2	Common Alerting Protocol	July 2010	
EDXL-DE v1.0	Distribution Element	May 2006	
EDXL-HAVE v1.0 Errata	Hospital AVailability Exchange	November 2008	
EDXL-RM v1.0 Errata	Resource Messaging	November 2008	
EDXL-SitRep v1.0	Situation Reporting		Pending 2013
EDXL-TEP v1.0	Tracking Emergency Patients		Pending Year –N/A

2.8.2 EDXL-CAP v1.2

The Common Alerting Protocol is widely accepted around the world and is cross-adopted by the International Telecommunications Union (ITU). EDXL-CAP is the basis for emergency alerting services.

2.8.3 EDXL-DE v1.0-2.0

EDXL-Distribution Element is the header for emergency messages using the EDXL suite of standards.

2.8.4 EDXL-HAVE v1.0

The Hospital AVailability Exchange standard provides an up-to-the-moment snapshot of a hospital system’s capabilities. It was severely tested in the Haiti earthquake of 2010 and the lessons learned are being incorporated in v2.x currently in work as of the time of the writing of this pattern. EDXL-HAVE is the basis for emergency hospital status reporting services.

2.8.5 EDXL-RM v1.0

The Resource Messaging standard handles all logistical information for an emergency incident in exactly the same way that it handles that same type of information on a daily basis.

EDXL-RM specifies 16 predefined messages with ability for user-defined messages. EDXL-RM is the basis for emergency resources messaging services.

2.8.6 EDXL-SitRep v1.0

The Situation Reporting standard provides the kind of categorically summarized information (data with agreed/understood semantics) needed for accurate and timely decision making during an incident, as well as provides key information about the uses for which the requisitioned resources can be used.

EDXL-SitRep provides for five message types: a basic Field Observation report, a Situation Information report, a Response Resources Totals report, a Casualty and Illness Summary report, and a Management Reporting Summary report. When accessed via a COP, this information can be rapidly assembled and made available to the ICS.

EDXL-SitRep will be the basis for emergency-situation reporting services.

2.8.7 EDXL-TEP v1.0

The Tracking Emergency Patients standard provides the means for creating an electronic health record for individuals harmed by an emergency incident and the kind of care that has been rendered to them up to the point at which the patient is handed off to a hospital system. It is being developed in cooperation with the Health Level Seven standards organization.

EDXL-TEP will be the basis for emergency patient-tracking services.

2.9 The EDXL Domain and Supporting Elements Models

As noted previously, the OASIS EM TC discovered that certain types of information were used repeatedly in the individual specifications; it was decided to set these aside in their own specifications, which the individual standards could then use as needed without defining these elements in each new EDXL specification or version of existing specifications. It is important to include some of the lessons learned in the development of the EDXL suite or domain model here in context with the defining specifications, so that the reader need not shift from one section to another to connect lessons learned with the application of those lessons. This will be noted again in the pattern-specific lessons learned in Section 3.1.

2.9.1 Value Lists in EDXL-DE

As the first specification undertaken after CAP in the EM TC, and the first specification in the EDXL family per se, the emergency message header/wrapper for reliable distribution of emergency messages, EDXL-DE v1.0, developed a mechanism to avoid probable difficulties with communications that cross jurisdictional boundaries where terminologies for identical or similar elements and data types can be different, thus impeding or preventing interoperability in the midst of emergency incidents. This mechanism is designated as Value List Uniform Resource Identifiers (URIs). These Value List URIs include specific kinds of Value Lists such as Value Keys, Value Key String Pairs, Value Key Integer Pairs, etc.

Provided a given jurisdiction publishes its managed lists, or points to an external managed list it uses, so that they can be found and used by its emergency incident response partners, any particularized list of keyword-indexed name-value pairs can be used interoperably across any jurisdictional boundary.

2.9.2 Common Types

Common types was the first set of repeatable data name and type pairs that were identified. value lists were among the first set of common types.

The use of common types within a specification was first used in the EDXL-RM to reduce the amount of work needed to change an element that appears in several of the 16 pre-defined EDXL-RM message types. Changing the element in that specification's Common Types XML Schema automatically makes the change everywhere the element is referenced by its <ct:…> Common Type abbreviation.

Supporting information model specifications use a lightweight process making it easier and quicker to make changes as needed. Thus, when changes are made, they will be automatically applied to any and all EDXL specifications that use those changed elements. The EDXL Common Types Committee Specification (EDXL-CT) can be found at http://docs.oasis-open.org/emergency/edxl-ct/v1.0/edxl-ct-v1.0.pdf

This mechanism has been adapted for the entire EDXL suite as part of the supporting information model. This eliminates a great deal of unnecessary effort usually involved in versioning related specifications.

2.9.3 Location Information

Location information elements are perhaps the most often re-used set of elements in the EDXL suite. From its earliest work on CAPv1.0, the OASIS EM TC has taken advice from and used standards from the Open Geospatial Consortium (OGC). As we learned more, and as OGC also developed according to its experience, we ultimately decided to define our own EDXL Profile of the OGC Simple Features Profile in order to simplify this complex set of elements to the few required by our specifications.

Of course, when specifying organizational locations and locations defined by political jurisdictions, more particular kinds of information than simple geographical locations were needed and the OASIS EM TC divided location information into geographical and geopolitical domains.

The EDXL Profile of the Open Geospatial Consortium Simple Features Profile of the Geographic Markup Language Committee Specification (EDXL-GSF) can be found at http://docs.oasis-open.org/emergency/edxl-gsf/v1.0/edxl-gsf-v1.0.pdf

2.9.4 Contact Information

Contact Information spans personal, organizational and political information types.

The OASIS EM TC decided to use a profile of the OASIS Customer Information Quality (CIQ), which is comprised of several specific profiles of the specifications which comprise CIQ:.

- EDXL-Extensible Party Information Language (EDXL-xPIL)
- EDXL-Extensible Name Language (EDXL-xNL)
- EDXL-Extensible Address Language (EDXL-xAL)
- Subsidiary information carried in this supporting model include:
    - Addresses
    - Contact Numbers
    - Electronic Address Identifiers
    - Other Identifiers

3 Additional Information

While it should be clear by this point that the standards cited above are intended to provide for a comprehensive domain data model, it should be noted that a great deal of work remains to be done and there may be changes we do not yet anticipate. The greatest need at this point is to support adoption of these standards so that a proprietary collection of data models is not allowed to become a de facto rule of the road.

Additionally, work is proceeding in ISO to make a standard of an exhaustive language independent code list of named resources, incident-types and message-types, based on work done previously on a Tactical Situation Object (TSO). This work is being followed as closely as possible by the OASIS EM TC to ensure that we maintain interoperability between such a code list and the standards cited previously. The supporting elements information models and value list mechanisms should provide this assurance.

3.1 Lessons Learned

Over the ten years that the OASIS EM TC has been working in this emergency management domain, a number of lessons have been learned. The effort has been to produce low- to no-cost standards that can ensure data and terminology interoperability at a minimum.

3.1.1 Value Lists

Very early on, we learned that no single list of approved terms and data types was likely to emerge in time to be useful. So we developed the managed-list system we call the value list. This simply means that literally anyone can publish their own list of name-value pairs for a given category of data such as event types, equipment names, job titles, etc.

3.1.2 Supporting Elements Information Models

The OASIS EM TC learned over the course of developing the EDXL suite of standards that certain information categories arose time after time and could be better managed in specifications of their own. This provides two benefits.

3.1.2.1 Avoiding Repetition of Definitions and Approval Campaigns

Whether it is the set of categories needed to define a street address, personal name or geographical information, by having these in separate specifications, they can be invoked by citation rather than requiring repetition within each new major specification.

In addition, by taking these supporting models only to the level of an OASIS committee specification, the requirement for mounting a major approval campaign is avoided.

3.1.2.2 Change Once, Change All Instances

Lastly, the use of supporting models allows for a change to a particular kind of named data type to be made once only, rather than needing to add a new version of each specification that uses the named data type. So the work of maintenance of OASIS EM TC standards is greatly reduced.

3.1.3 Documentation and Support

While it has been difficult to attract volunteer time at the NCOIC member-company and individual level, the need for best practices documentation and support to aid in encouraging adoption was acknowledged fairly early on. However the OASIS EM TC decided to spin off the EM Adoption Technical Committee dedicated to promoting adoption of the EDXL suite. This goal is supported by the following subcommittees;

- **Events and Demonstrations**
- **Outreach and Education** to the academic and public domains
- **Collateral and Documents** dedicated to providing support material like advertising, brochures, educational videos and panel discussions as well as other documents in support of adoption

3.2 Constraints and Opportunities

Constraints: The largest constraint that is likely to occur while using this standards-based pattern will be by jurisdictions whose use of non-standard, proprietary solutions will make it difficult for their partner agencies to provide interoperability. This will greatly hamper mutual aid and, when the local agency where the emergency incident occurs is using one of the non-standard, proprietary solutions on the market, it will require agencies bound by mutual-aid agreements to either provide information in the formats and data types of the jurisdiction of the incident, or it will require the larger jurisdiction that contains the local jurisdiction of the incident to take over the ICS for the incident.

The fact is that there are marketing strategies in which proprietary software is literally given away for free, at least in the short term, to jurisdictions that cannot afford custom software, which is, unfortunately, much too large a percentage of the potential market.

Opportunities: This same situation provides a remarkable opportunity for companies that are willing to court a large market comprised of small jurisdictions and that produce standards-based implementation that can be easily customized to fit the wide range of jurisdictions in the market. Clearly this is not applicable to large, affluent jurisdictions, but those are relatively few.

Granted it takes a different approach from that of the large companies in NCOIC, but the long-term profit is there for those that can leverage the recommendation of DHS in support of voluntary consensus standards such as the OASIS EDXL suite.

3.3 Known Uses

EDXL-HAVE was used extensively in the Haiti crisis of 2010. CAP is used world wide and currently has profiles in place for Canada and Australia. There are many examples of CAP and the FEMA-IPAWS CAP v1.2 Profile used in abducted children alerts is in daily use across the U.S.

3.4 Potential Capability

The chief potential capability of the NCOIC Emergency Services Operational Net-Centric Pattern is in the 4G mobile communications arena. Since the very first operation needed in any emergency according to the playbook of the pattern is to connect and implement communications with whatever kind of mesh network can be quickly and reliably put together, this immediately shows the potential of integrating these capabilities.

This pattern is intended to be used on a daily basis in normal communications on the ICS level for the EDXL suite. CAP is an exception and should be implemented as an always-on service that should be polling local, state and national sources, such as the weather service.

3.5 Related Patterns

As has been mentioned, there are several related patterns:

- Discontinuous, Intermittent and Limited (DIL) Communications Management Technical Pattern
- Multi-Level Distributed Discovery and Dissemination (MD3) Capability Pattern
- Information Dissemination Shared Database Capability Pattern
- All-Hazards Alerts and Warnings (AHAW) Capability Pattern

DIL provides the mechanism for capacity allocation of scarce communications resources in an emergency services or tactical network.

MD3 provides network assurance for reliable data discovery and dissemination for a system, or systems of systems, working within the challenging and dynamic environment of a mobile ad-hoc network (MANET). This pattern uses a distributed registry to enable SOA features such as loosely coupled emergency services. This especially suits the basis of this pattern for emergency services.

AHAW sets the stage for selective use of the capabilities described in the DIL and MD3 patterns by establishing the initial use of EDXL-DE to handle the messaging transactions of this pattern.

3.5.1 Extra Potential

The calculated use of the best set of capabilities in the AHAW, DIL and MD3 patterns is what will set those companies that can do this apart from any others in this still largely underestimated and vital field. This will play especially well as it becomes increasingly clear that spanning the levels of government jurisdictions involved in responding to emergency incidents is critical to timely success.

4 Verification

While a self-test suite for verifying conformance with the standards cited in this pattern is possible, it needs a separately funded project. However, for most of the EDXL Standards cited above, the U.S. Department of Homeland Security provides a third-party evaluation facility which is included here.

The Federal Emergency Management Agency (FEMA) National Preparedness Directorate (NPD) offers a project to assist the response community with interoperability test and evaluation (T&E). The Preparedness-Technology, Analysis and Coordination (P-TAC) Center manages the Supporting Technology Evaluation Project (STEP), which conducts T&E of technologies relating to incident management and response. T&E activities verify interoperability of commercial and government software and hardware products and provide the response community with reports to support purchasing decisions.

STEP uses an accredited testing laboratory located in Somerset, KY, (Incident Management Test and Evaluation Laboratory – IMTEL) for conducting T&E activities. IMTEL leverages the P-TAC Center infrastructure to evaluate the following:

- Incorporation of National Incident Management System (NIMS) concepts and principles
- Organization for the Advancement of Structured Information Standards (OASIS) Common Alerting Protocol (CAP) version 1.1 and 1.2 standards
- OASIS CAP version 1.2 USA Integrated Public Alert and Warning System (IPAWS) Profile version 1.0
- OASIS Emergency Data Exchange Language – Distribution Element (EDXL-DE) 1.0 standard
- OASIS EDXL – Hospital Availability Exchange (EDXL-HAVE) 1.0 standard
- OASIS EDXL – Resource Messaging (EDXL-RM) 1.0 standard

A Verification Cross-Reference Index (VCRI) is shown in the table below. The purpose of the matrix is to highlight prescriptive language cited throughout this document in a “playbook” format convenient for use in tabulating verification of requirements.

The following terminology is used throughout this Net-Centric Operational Pattern as taken from RFC 2119:

- “SHALL” and “SHALL NOT” with all letters set in uppercase expresses a requirement
- “SHOULD” and “SHOULD NOT” with all letters set in uppercase expresses a recommendation
- “MAY” and “MAY NOT” with all letters set in uppercase expresses allowable behavior, but is not required

In general, verification methods include examination, analysis, demonstration and test. For an operational pattern, demonstration is possible, but could be considered in analysis and, in general, and that can be sufficient. While the incorporation of the OASIS EDXL Standards allows the use of those standards to be tested in the P-TAC STEP program, it is not sufficient because the use of these standards takes place within services in a SOA ecosystem that SHALL also then be tested to be sufficient. However, demonstration with analysis is sufficient without the testing that would be necessary for a technical pattern.

No.	Requirement	Reference Section	Description	Verification Method
1	Various	Throughout	All statements herein that contain the words “SHALL” or “SHALL NOT” are considered requirements to be implemented as specified in the containing statement.	
2	Various	Throughout	The requirements cited in OASIS Standards or candidate standards and/or profiles and extensions of said standards or candidate standards documents are considered requirements. Said documents contain specific requirements language in keeping with that contained herein.	Demonstration

5 Appendices

5.1 Acronym List

AHAW	All-Hazards Alerts and Warnings
CAP	Common Alerting Protocol
CIMIC	Civilian-Military Cooperation and Collaboration
COP	Common Operational Picture
CONOPS	Concept of Operations
CRS	Coordinate Reference System
DIL	Discontinuous, Intermittent and Limited
EDXL	Emergency Data Exchange Language
EMT	Emergency Medical Technician
EM TC	Emergency Management Technical Committee
ICS	Incident Command System
IETF	Internet Engineering Task Force
IMTEL	Incident Management Test and Evaluation Laboratory
IPAWS	Integrated Public Alert and Warning System
ISO	International Organization for Standardization
ITU	International Telecommunication Union
NATO	North Atlantic Treaty Organization
NCOIC	Network-Centric Operations Industry Consortium
NCP	Network-Centric Pattern
NIF	NCOIC Interoperability Framework
NIMS	National Incident Management System
OASIS	Organization for the Advancement of Structured Information Standards
P-TAC	Preparedness-Technology, Analysis and Coordination
SCOPE	Systems, Capabilities, Operations, Programs, and Enterprises
SOA	Service Orientate Architecture
SOAP	Simple Object Access Protocol
STEP	Supporting Technology Evaluation Project
TSO	Tactical Situation Object
US	United States
VCRI	Verification Cross-Reference Index

5.2 Endnotes

[1] **CWA_15931-2**.pdf Disaster and emergency management - Shared situation awareness - Part 2: Codes for the message structure http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CD8QFjAA&url=ftp%3A%2F%2Fftp.cenorm.be%2Fpublic%2FCWAs%2FWS_ISDEM%2FCWA_15931-2.pdf&ei=kzcoUJm_CMTAiwL2vYHwAg&usg=AFQjCNFQdLIpaIhJVwqcixVK9Vbf-yMsOg

[2] Net-Centric Information Framework https://www.ncoic.org/apps/group_public/document.php?document_id=19574

[3] Net-Centric Services Framework v2 https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CDIQFjAA&url=https%3A%2F%2Fwww.ncoic.org%2Fapps%2Fgroup_public%2Fdownload.php%2F14326%2FNet_Centric_Services_Framework_V2.1(final).pdf&ei=4KsiUcejM4iCjALTnIHoDw&usg=AFQjCNH0zd2GHy5-7Q4J6ZLxWUYciwrSSQ&bvm=bv.42661473,d.cGE

[4] EDXL Tracking Emergency Patients v1.0 wd03 (Note: wd03 refers to "working draft 03" – there is no committee specification as of the time of this document -- https://www.oasis-open.org/apps/org/workgroup/emergency/download.php/47882/edxl-tep-v1.0-wd03.zip

[5] Health Level Seven International http://www.hl7.org/

[6] National Interoperability Field Operations Guides v1.4 http://www.dhs.gov/national-interoperability-field-operations-guide

[7] The Federal Geographic Data Committee Emergency Symbology Working Group Reference http://www.fgdc.gov/HSWG/index.html

[8] National Spatial Data Infrastructure, http://www.fgdc.gov/nsdi/nsdi.html

[9] Common Alerting Protocol v1.2 https://www.oasis-open.org/standards#capv1.2

[10] EDXL Distribution Element v1.0 https://www.oasis-open.org/standards#edxlde-v1.0

[11] EDXL Hospital AVailability Exchange https://www.oasis-open.org/standards#edxlhave-v1.0

[12] EDXL-Resource Messaging v1.0 https://www.oasis-open.org/standards#edxlrm-v1.0

[13] OASIS Reference Architecture Foundation for Service Oriented Architecture , https://www.oasis-open.org/apps/org/workgroup/soa-rm-ra/download.php/47144/soa-ra-v1.0-csprd03.pdf