INSTITUTE FOR DEFENSE ANALYSES

Public Safety and Emergency Management Communications Ontology

Serena Chan, *Project Leader*

Brian A. Haugh
Francisco L. Loaiza-Lemos
Steven P. Wartik

June 20, 2017

IDA Document
D-8583

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Task ET-5-4155, "DoD First Responder Communications Interoperability," for Director, C4 Resilience & Mission Assurance. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments

Reginald N. Meeson Jr., Stefania A. Brown-VanHoozer

For more information:

Serena Chan, Project Leader
schan@ida.org, 703-933-6563

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

INSTITUTE FOR DEFENSE ANALYSES

IDA Document D-8583

Public Safety and Emergency Management Communications Ontology

Serena Chan, *Project Leader*

Brian A. Haugh
Francisco L. Loaiza-Lemos
Steven P. Wartik

Executive Summary

This document reports on work done by the Institute for Defense Analyses (IDA) for the Office of the Program Manager, Information Sharing Environment (PM-ISE), Office of the Director of National Intelligence, and for the Office of the Deputy Chief Information Officer (DCIO) for Command, Control, Communications, and Computers and Information Infrastructure Capabilities (C4&IIC), Department of Defense (DoD) Chief Information Officer (CIO).

The objective of the IDA project is to assess the current state of communications interoperability between DoD public safety and emergency management (PS/EM) entities and U.S. civilian PS/EM entities and how that is likely to change as the next generation of public safety information systems is implemented across the nation. This document addresses one aspect of this project—the development of a formal semantic information model (ontology) for PS/EM information products.

The document begins by describing the general approach taken in building ontologies for specific PS/EM information-sharing standards based on a foundation of widely used upper and mid-level ontologies. The Basic Formal Ontology (BFO) is used as the top-level "upper ontology" to define the most abstract concepts. The Common Core Ontologies (CCO) are used as "mid-level ontologies" to defined common sense concepts, such as Person and Organization, which specialize the concepts of the upper ontology.

The PS/EM information-sharing standards used as the basis for a *PS/EM Communications Ontology* were identified in a related task that assessed the data requirements for information exchanges involving DoD and civilian PS/EM entities.[*] The set of standards used comprised the following documents from the Emergency Data Exchange Language (EDXL), as well as other sources listed:

- EDXL-DE (Distribution Element),
- EDXL-RM (Resource Messaging),
- EDXL-HAVE (Hospital Availability Exchange),
- EDXL-CAP (Common Alerting Protocol),

[*] S. Chan et al., *Department of Defense Public Safety and Emergency Management Communications: Interoperability Data Requirements*, IDA Document D-8416 (Alexandria, VA: Institute for Defense Analyses, March 2017).

- Emergency Incident Data Document (EIDD),
- Public Safety Communications Common Incident Types,
- Keystone / Unified Incident Command and Decision Support (UICDS) Schemas.

Ontologies for these PS/EM information standards were constructed by adding specializations of the BFO and CCO classes and properties to cover the standards' information requirements. Separate ontologies were developed for these standards so that they could stand alone. Then they were merged into a common *PS/EM Communications Ontology*[†] to facilitate comparative analysis of the information requirements in each standard. Subsequent analysis is planned to identify duplication and overlaps between concepts from different standards and to identify gaps in capabilities of the National Information Exchange Model (NIEM) to support all identified information requirements.

The majority of this document is devoted to describing how the conceptual models and schemas of each of the PS/EM information-sharing standards are transformed into formal ontologies. This document is intended to provide information-modeling professionals with an understanding of the approaches taken in capturing the semantics of the PS/EM information-sharing standards.

The document describes how representative classes that model PS/EM concepts are related to the classes of the upper and mid-level ontologies. Furthermore, it explains how the identified properties of the foundational ontologies are used to represent relationships among PS/EM entities and their attributes. Given the technical nature of these descriptions, this document is not intended for a general audience, although every effort is made to clearly define technical concepts as they are introduced to make it accessible to a broader audience.

This document does not describe every class and property used in the ontologies. Instead, it describes representative classes and properties, providing an overview of the ontologies and a guide to understanding related ontology elements. English language definitions, and formal relationships asserted in the ontologies, record the detailed intended semantics for the concepts. These details can be reviewed by viewing the ontologies using an ontology tool such as Protégé or TopBraid. Alternatively, the details can be reviewed in the comprehensive documentation automatically generated from the ontologies.

The ontologies described herein provide a foundation for semantic interoperability amongst diverse PS/EM communication systems using different types of information-sharing standards. Semantic interoperability requires the use of a common semantics (i.e.,

[†] The ontologies are implemented in the Web Ontology Language (OWL), and the merging is accomplished using OWL's "import" construct.

meaning) for the terminology used in information shared among interoperating systems. An ontology captures terminology in a formalism reducible to a logic that expresses logical relationships among the various concepts. Furthermore, ontologies enable a degree of machine “understanding” sufficient to standardize the derivation of implicit information from the explicit information of information exchanges. Utilizing a common ontology across interoperating systems helps ensure that all parties share the same extent of such derived information. That is, the ontology supports common understanding of shared information by humans and machines alike, and facilitates automated reasoning with that information. This document describes initial work addressing this issue of improving semantic interoperability across the PS/EM communications enterprise.

Contents

Figures

1. Introduction

A. Background

1. Issues Addressed

Department of Defense (DoD) public safety and emergency management (PS/EM) entities and U.S. civilian PS/EM entities have time-critical needs to communicate effectively when coordinating responses to public safety incidents. Certain DoD military bases in the United States depend on U.S. civilian firefighting and emergency medical services (EMS) for response to incidents on base. Public Safety Answering Points (PSAPs) serving DoD bases may need to dispatch requests to civilian public safety responders when they do not have the requisite services on base or when they are overwhelmed. On the other hand, civilian responders may need to request and coordinate with military emergency management entities, especially with the National Guard, when confronted with situations requiring humanitarian assistance and disaster relief (HADR). Many different lines of communication are available for such coordination, including computer-aided dispatch (CAD) from PSAPs, and shared websites, such as WebEOC and the All Partners Access Network (APAN). However, better understanding of these communications capabilities and requirements is needed, especially as we move into the next generation of public safety information systems, such as FirstNet[1] and Next-Generation 9-1-1 (NG9-1-1).[2]

We need to better understand the existing communication systems: how interoperable they are with respect to the Internet of Things, Internet of Networks, and human interchange/protocols/procedures, as well as what PS/EM information-sharing requirements they serve. Such an improved understanding provides a foundation for migrating to next-generation systems that exceed current capabilities and require more data information to meet future needs.

The Institute for Defense Analyses (IDA) previously issued a document[3] assessing the types of data required to support information exchanges between DoD and U.S. civilian PS/EM entities. This document identified a set of data standards that need to be considered for use in future DoD and U.S. civilian PS/EM communications systems, such as FirstNet. Building on these requirements, this document describes an effort to structure the syntactic data elements, which are

[1] First Responder Network Authority (FirstNet), 2017. http://www.firstnet.gov/.

[2] National Emergency Number Association (NENA), “NG9-1-1 Project,” 2017, http://www.nena.org/?NG911_Project.

[3] S. Chan et al., *Department of Defense Public Safety and Emergency Management Communications: Interoperability Data Requirements*, IDA Document D-8416 (Alexandria, VA: Institute for Defense Analyses, March 2017).

identified, into a formal semantic model of the information exchanges and information content most relevant to information exchanges between DoD and U.S. civilian PS/EM entities. Such a semantic model addresses the issue of improving semantic interoperability among diverse PS/EM communication systems using different types of information-sharing standards.

Semantic interoperability requires the use of a common semantics (i.e., meaning) for the terminology used in information shared among interoperating systems. A formal semantic model captures terminology in a formalism that is reducible to a logic that expresses logical relationships among the concepts that the terminology represents. Such a semantic model enables a degree of machine "understanding" of terminology sufficient to standardize the derivation of implicit information from the explicit information of information exchanges. Utilizing a common semantic model across interoperating systems can help ensure that only those inferences that follow logically from the shared information are derived and that all parties share the same extent of such derived information. That is, the semantics supports common understanding of shared information by humans and machines alike and facilitates automated reasoning with that information. This document describes initial work addressing this issue of improving semantic interoperability across the PS/EM communications enterprise.

2. Project

The work described here is part of a larger project whose objective is to assess the current state of communications interoperability between DoD's public safety and emergency management (PS/EM) entities and U.S. civilian PS/EM entities. The work further addresses how this current state will likely change as the next generation of public safety information systems is implemented across the nation.

Another part of this project surveyed civilian and DoD mass warning and notification systems to identify their commonalities and differences, including their use or neglect of national and international standards for information sharing. The results are reported in another document.[4]

This document reports on one aspect of this project: describing ontologies for representing the semantics of some of the most prominent information-sharing standards in the PS/EM communications domain.

[4] J. W. Bailey et al., *A Survey of Mass Warning and Notification Systems,* IDA Document D-8388 (Alexandria, VA: Institute for Defense Analyses, March 2017).

B. Approach

1. Foundations and Structure of the Ontologies

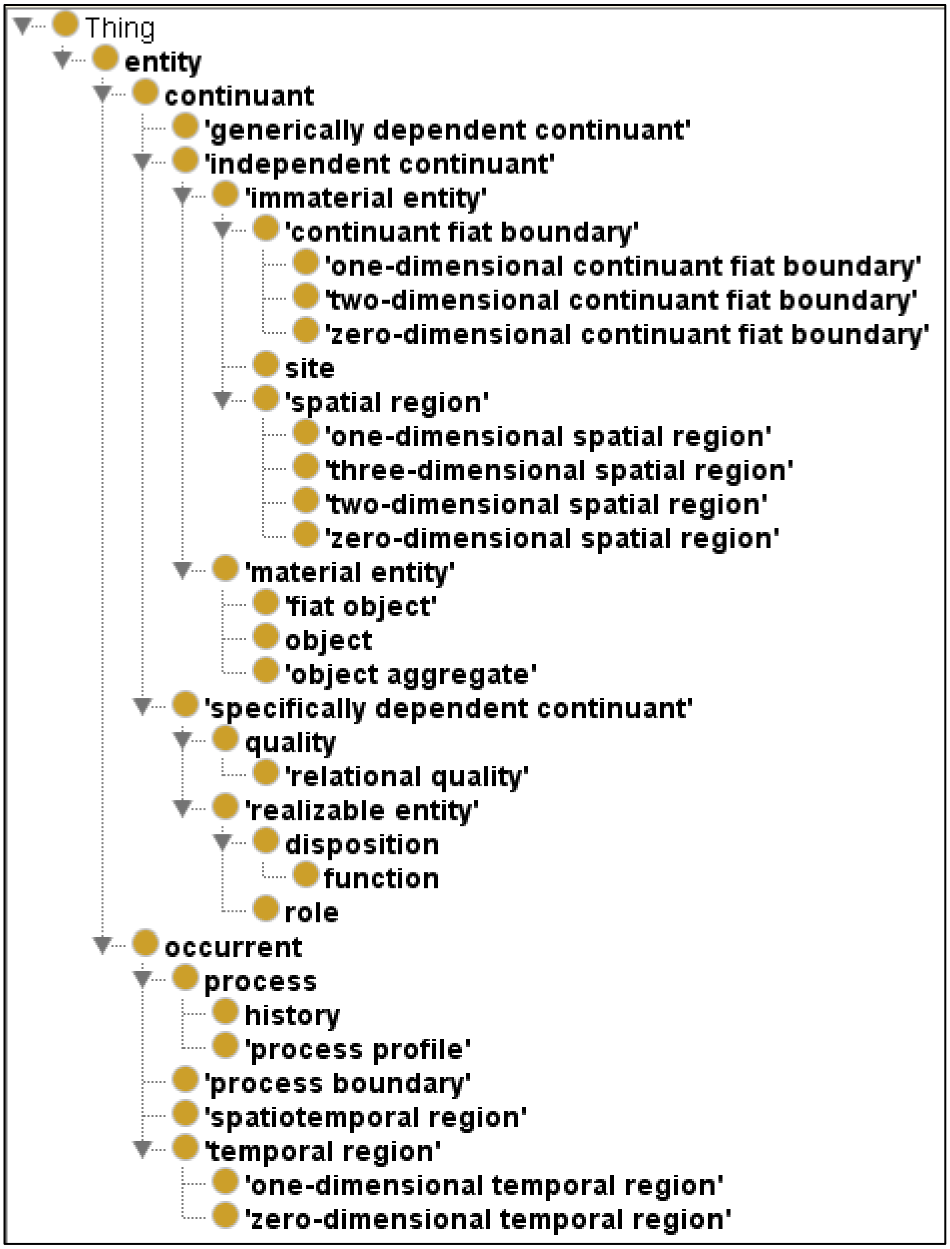
Our approach to ontology development in the PS/EM communications domain began with the selection of an upper level ontology, the Basic Formal Ontology (BFO),[5] as a foundation providing the most abstract upper level classes to structure the more specific information beneath them. Figure 1-1 shows the class hierarchy of this upper ontology. This figure uses the common convention of showing subclasses listed with an indent below their superclasses, connecting the subclasses to them with lines.

There are two main divisions of the entity class in this hierarchy: the continuant and the occurrent classes and their subclasses. These classes and their subclasses are described in some detail in the following sections. As an initial orientation, the continuant class can be understood to contain persisting objects in the world and their properties, while the occurrent class can be understood to contain processes, events, and related spatiotemporal entities that unfold in time, are boundaries of such entities, or are spatiotemporal regions that they occupy.

The BFO was then supplemented with a middle-level ontology, comprising the Common Core Ontologies (CCO).[6] These consist of an integrated set of ontologies for widely used common sense concepts with the import structure illustrated in Figure 1-2.

[5] R. Arp, B. Smith, and A. Spear, *Building Ontologies with Basic Formal Ontology* (Cambridge, MA: The MIT Press, 2015).

[6] See http://www.cubrc.org/index.php/data-science-and-information-fusion/ontology for an overview of the Common Core Ontologies. See the following documents for an exposition of their content: Ron Rudnicki, *An Overview of the Common Core Ontologies* (Buffalo, NY: CUBRC, Inc., 2016) and *Modeling Information with the Common Core Ontologies* (Buffalo, NY: CUBRC, Inc., October, 2016).



```
Thing
  entity
    continuant
      'generically dependent continuant'
      'independent continuant'
        'immaterial entity'
          'continuant fiat boundary'
            'one-dimensional continuant fiat boundary'
            'two-dimensional continuant fiat boundary'
            'zero-dimensional continuant fiat boundary'
          site
          'spatial region'
            'one-dimensional spatial region'
            'three-dimensional spatial region'
            'two-dimensional spatial region'
            'zero-dimensional spatial region'
        'material entity'
          'fiat object'
          object
          'object aggregate'
      'specifically dependent continuant'
        quality
          'relational quality'
        'realizable entity'
          disposition
            function
          role
    occurrent
      process
        history
        'process profile'
      'process boundary'
      'spatiotemporal region'
      'temporal region'
        'one-dimensional temporal region'
        'zero-dimensional temporal region'
```

Figure 1-1. BFO Class Hierarchy

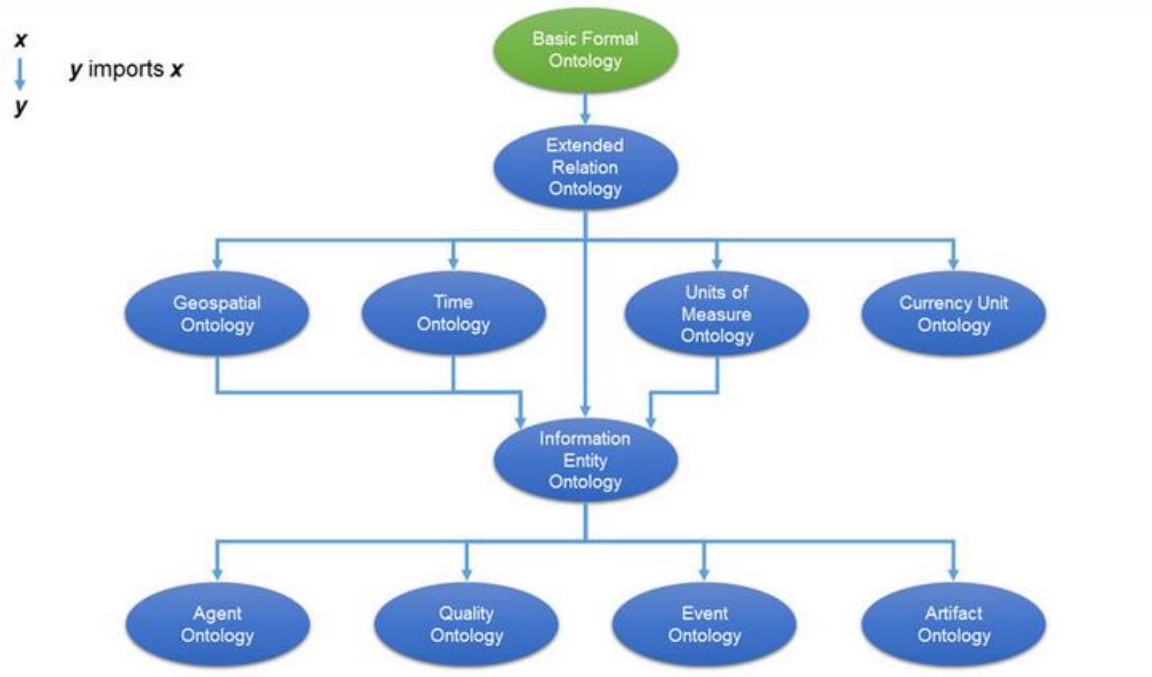


Figure 1-2. Common Core Ontologies Import Structure[7]

Ontologies for PS/EM information standards were constructed by adding specializations of the BFO and CCO classes and properties to cover the information requirements of PS/EM standards. The set of standards used for this initial *PS/EM Communications Ontology* comprises the following standards from the Emergency Data Exchange Language (EDXL) and the other sources listed:

- EDXL-DE (Distribution Element),
- EDXL-RM (Resource Messaging),
- EDXL-HAVE (Hospital Availability Exchange),
- EDXL-CAP (Common Alerting Protocol),
- Emergency Incident Data Document (EIDD),
- Public Safety Communications Common Incident Types,
- Keystone / Unified Incident Command and Decision Support (UICDS) Schemas.

Separate ontologies were developed for these standards so that they could stand alone. Then they were all imported into a common *PS/EM Communications Ontology* to facilitate their comparative analysis. Going forward, the next step is to perform an analysis of duplications and

[7] Source: *Common Core Ontologies for Data Integration*. CUBRC, Buffalo, NY. 2017. http://www.cubrc.org/index.php/data-science-and-information-fusion/ontology

overlaps among these ontologies and the Emergency Management (EM) Domain of the National Information Exchange Model (NIEM).

The information structures of the NEIM EM Domain will be compared with the other PS/EM information-sharing standards, and gaps in its capabilities to cover their information requirements will be identified. Results of these analyses and recommendations on addressing gaps will be included in a separate paper to be prepared for this project.

2. Document Scope and Audience

The bulk of this document is devoted to describing how the conceptual models and eXtensible Markup Language (XML) schemas of each of the PS/EM information-sharing standards are transformed into formal ontologies. It is intended to provide information-modeling professionals with an understanding of the approaches taken to capturing the semantics of the PS/EM information-sharing standards. The document describes how representative classes that model PS/EM concepts are related to the classes of the upper and mid-level ontologies. The document explains how the properties of those foundational ontologies are used to represent relationships among PS/EM entities and their attributes. Given the technical nature of these descriptions, this document is not intended for a general audience, although every effort has been made to clearly define technical concepts as they are introduced to make it accessible to a broader audience.

This document does not describe every class and property used in the ontology, but does describe representative classes and properties to provide an overview of the ontologies and a guide to understanding related ontology elements. English language definitions and formal relationships asserted in the ontologies record the detailed intended semantics for the concepts included therein. These details can be reviewed by viewing the ontologies using an ontology tool such as Protégé or TopBraid. Alternatively, they can be reviewed in the comprehensive documentation automatically generated from the ontologies.

C. Overview

Section 2 begins with an overview of ontologies developed to capture the information content and message structures of the EDXL standards from the Organization for the Advancement of Structured Information Standards (OASIS).[8] Separate ontologies are described for the four parts of the EDXL standards. These are subsequently imported into the overall *PS/EM Communications Ontology*. Furthermore, all these ontologies use the BFO as an upper level ontology and the CCO as mid-level ontologies.

Section 3 describes an ontology for the Emergency Incident Data Document (EIDD), which was developed jointly by the Association for Public-Safety Communications Officials (APCO)

[8] See the OASIS Emergency Management Technical Committee website for links to all the EDXL standards, https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency.

International and the National Emergency Number Association (NENA) and approved by the American National Standards Institute (ANSI). This international data standard provides industry-neutral specifications for exchanging emergency incident information with agencies and regions that implement NG9-1-1, as well as Internet Protocol (IP) based emergency communications systems.[9]

Section 4 describes an ontology developed for the APCO Public Safety Communications Common Incident Types for Data Exchange.[10] This includes a standardized set of 197 incident classes and corresponding codes for common types of PS/EM incidents. These codes are used in the EIDD standard to provide a standard means of categorizing incidents. The codes from this APCO standard have now been formally captured in an ontology, which is imported by the EIDD ontology described in Section 3.

Section 5 describes the ontology for the information-sharing requirements of Keystone, a standards-based middleware designed to support real-time information sharing among force protection and emergency management applications.[11] Keystone, developed by DoD, was based on the earlier Unified Incident Command and Decision Support System (UICDS)[12] system from the Department of Homeland Security (DHS). It incorporates a variety of enhancements of UICDS to better meet DoD requirements.

[9] APCO International, “Emergency Incident Data Document (EIDD),” APCO NENA 2.105.1-2017 NG9-1-1, p. 2, https://www.apcointl.org/doc/911-resources/apco-standards/694-apco-nena-2-105-1-2017-ng9-1-1-emergency-incident-data-document-eidd/file.html.

[10] APCO International, “Public Safety Communications Common Incident Types for Data Exchange,” APCO ANS 2.103.1-2012, https://www.apcointl.org/doc/911-resources/apco-standards/386-public-safety-communications-common-incident-types-for-data-exchange/file.html.

[11] SSC Pacific, *EUCOM Keystone Product Reference Guide* Revision 1.0, September 2015, p. 2.

[12] SAIC, *Unified Incident Command and Decision Support* (*UICDS*) *Getting Started Guide*, September 2010.

2. Emergency Data Exchange Language Ontologies

A. Introduction

The Emergency Data Exchange Language (EDXL) is a composite standard developed by the Organization for the Advancement of Structured Information Standards (OASIS), which is composed of a group of related standards for information-sharing messages based on the eXtensible Markup Language (XML). Other emergency management standards (e.g., NIEM EM) and systems use EDXL and its component standards, especially its Common Alerting Protocol (CAP), to define messages for information sharing.[13]

The IDA team developed ontologies based on the four EDXL standards:

1. EDXL-DE (Distribution Element). EDXL-DE serves as a kind of wrapper for other messages. According to OASIS, "the primary purpose of the Distribution Element is to facilitate the routing of any properly formatted XML emergency message to recipients."[14]
2. EDXL-RM (Resource Messaging).
3. EDXL-HAVE (Hospital Availability Exchange).
4. EDXL-CAP (Common Alerting Protocol).

Each of these ontologies is described in following sections, but first we introduce some EDXL concepts.

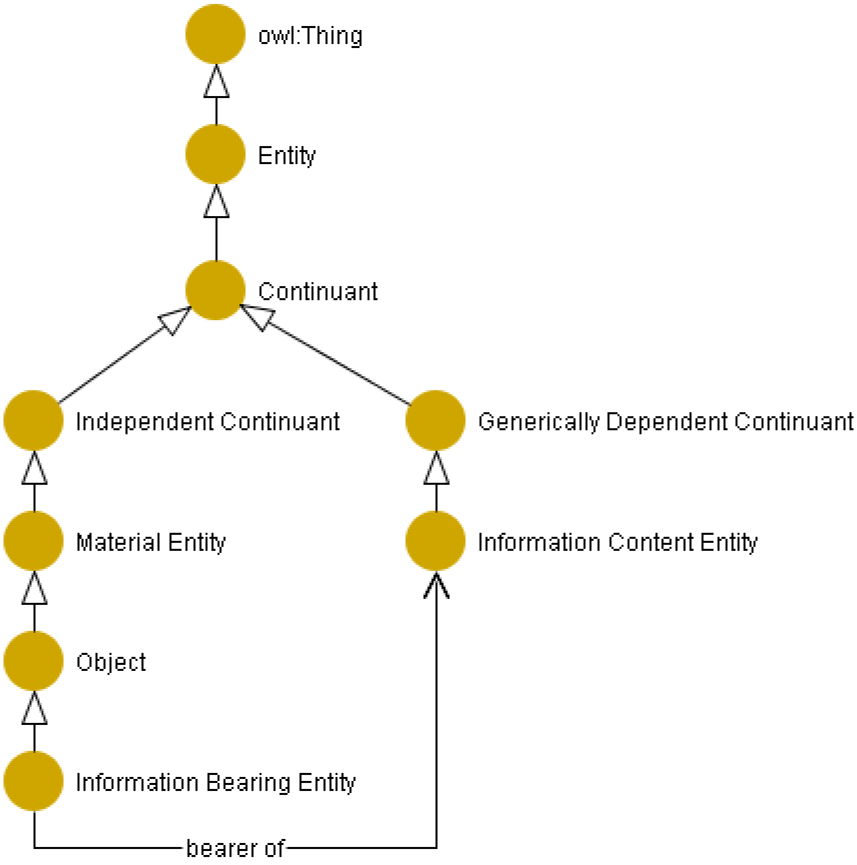
All four ontologies use the Common Core ontology suite as a middle-level ontology. The following paragraphs describe how EDXL concepts fit into the Common Core class hierarchy (which in turn extends the BFO).

The EDXL is used to exchange messages whose content concerns emergencies. This simple fact indicates that there are two domains of interest: *messages* and *emergencies*. In the Common Core, a message, whether on paper or electronic, is considered a kind of object, specifically an Information Bearing Entity. Figure 2-1 shows the Common Core ontology's class hierarchy for an Information Bearing Entity. As the name implies, an individual of this class bears information, which has two connotations. First, such an individual may have a value (or values). For example, a book has text; a newspaper has text and images. In the realm of computers and networks, a

[13] For links to the EDXL standards, see the OASIS Emergency Management Technical Committee website at: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency.

[14] https://www.oasis-open.org/committees/download.php/17227/EDXL-DE_Spec_v1.0.html, Section 1.1.

hyperlink has a Uniform Resource Locator (URL); an XML message has text consisting of tags, their attributes, and their content, which may be text or other elements. The Common Core provides datatype properties whose names have the form “has * value” (e.g., “has Boolean value”, “has decimal value”, “has text value”). These properties have primitive datatypes as their ranges.


owl:Thing
Entity
Continuant
Independent Continuant
Generically Dependent Continuant
Material Entity
Information Content Entity
Object
Information Bearing Entity
bearer of

Note: Subclass relationships are illustrated by an arrow from a subclass to its superclass. One class is a subclass of another if and only if all its members are members of the other class.

Figure 2-1. Common Core Class Hierarchy: Information-Related Entities

Second, an Information Content Entity (ICE) is said to be the bearer of information expressed in an Information Bearing Entity (IBE). To understand this, consider the following. Where an Information Bearing Entity expresses the representation of information transmitted, an Information Content Entity captures the meaning of that information. A CAD system might send a message to many recipients. Each of these messages is a distinct Information Bearing Entity. All messages express the same information—a single Information Content Entity. Figure 2-1 shows the “bearer of” object property, whose domain is Information Bearing Entity and whose range is Information Content Entity. In a knowledge base that captures a message sent from 1 sender to 20 recipients, there will be 20 Information Bearing Entity individuals (1 for each copy of the message), 1 Information Content Entity individual (for the full content of the message), and 20 object property assertions. Each object property assertion would have a distinct source individual (one of the messages). All would have the same target individual (the Information Content Entity individual).

An Information Content Entity describes content. In EDXL, this content is about some emergency-related concept. The concept might be an incident, or it might be an incident’s location, or a resource needed in response to an incident—it can be anything useful in understanding or responding to an incident. The Common Core ontology defines an object property named “is about”, the domain of which is Information Content Entity, and the range of which is, simply, “Entity”—that is, an Information Content Entity can be about anything that can be expressed in BFO. The EDXL ontologies, insofar as is possible, define what information content is about by using subclass restrictions. For example, the ontology derived EDXL-RM includes the concept of a message sender. The Information Content Entity derived from this concept “is about” an agent.

Class Information Content Entity has several subclasses that are useful in further categorizing EDXL-related content. Figure 2-2 shows some of them. An Information Content Entity may be descriptive, meaning its content is expressed in terms of attributes that allow content to be inferred via description. A measurement (class Measurement Information Content Entity) is perhaps the most familiar example. An Information Content Entity may be designative; in EDXL, such an entity is usually an identifier used to designate some other entity (e.g., a message identifier). An Information Content Entity may be directive, such as the content of a plan.

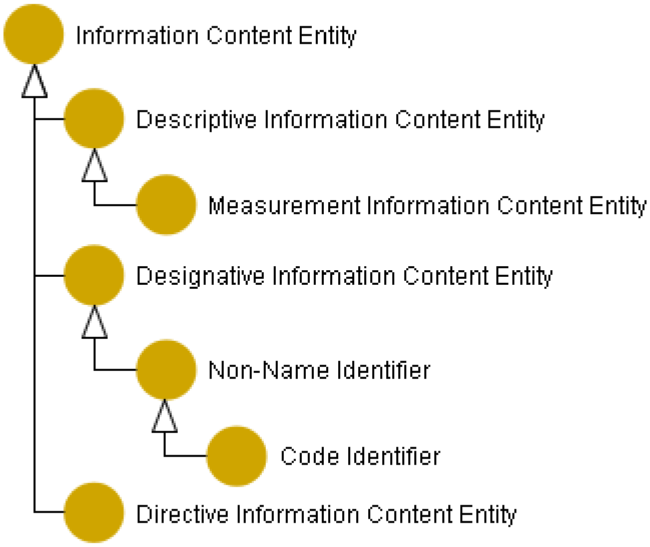

Information Content Entity
Descriptive Information Content Entity
Measurement Information Content Entity
Designative Information Content Entity
Non-Name Identifier
Code Identifier
Directive Information Content Entity

Figure 2-2. Information Content Entity Hierarchy (Partial)

Many elements in EDXL messages draw their values from a fixed set of strings. For example, if response information in EDXL-RM includes a response type, its value must be one of “Accept”, "Decline", or "Provisional".[15] The text value of a corresponding Information Bearing Element must be one of these values, a fact that can be expressed as a subclass restriction:

info:has_text_value **some** { "Accept", "Decline", "Provisional" }

The Information Content Entity borne by this Information Bearing Entity must reflect these three values. In a knowledge base, this is achieved by modeling each value as a Web Ontology Language (OWL) individual. More precisely, suppose *E* is an EDXL element whose values are limited to a fixed set of strings. Then:

- There is an Information Bearing Entity subclass *IBE*.
- *IBE* has a subclass restriction stating that the values of property info:has_text_value are limited to a fixed set of strings.
- There is an Information Content Entity subclass *ICE*.
- *IBE* has a subclass restriction stating that the range of property ero:bearer_of is limited to *ICE*.
- For each *s* that is a valid string value for the EDXL element, there exists an individual *sICE* of type *ICE* (types are asserted using property rdf:type).
- Individual *sICE* has an info:is_tokenized_by annotation, the value of which is *s*.

Figure 2-3 illustrates this modeling pattern.

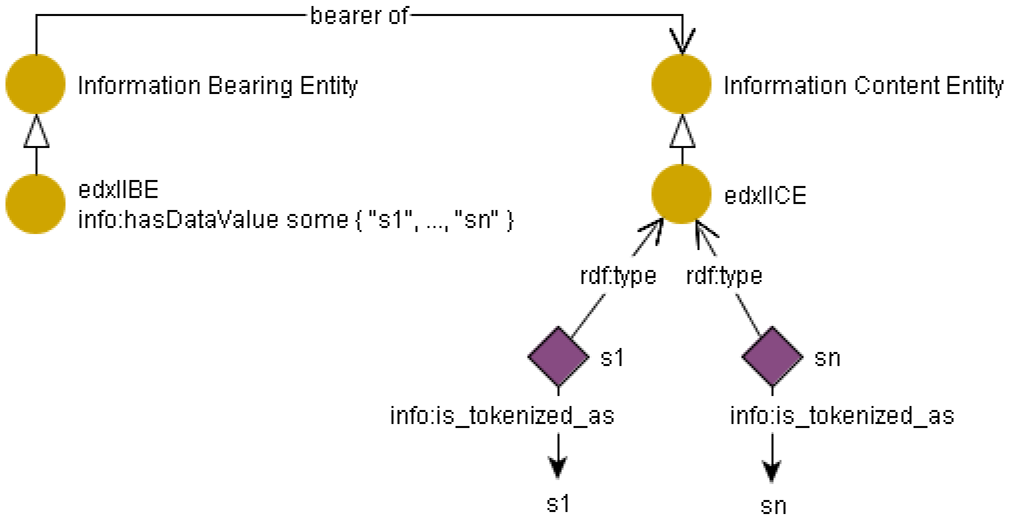

bearer of
Information Bearing Entity
Information Content Entity
edxlIBE
info:hasDataValue some { "s1", ..., "sn" }
edxlICE
rdf:type
rdf:type
s1
sn
info:is_tokenized_as
info:is_tokenized_as
s1
sn

Figure 2-3. Modeling Enumerated Values

[15] See http://docs.oasis-open.org/emergency/edxl-rm/v1.0/pr03/EDXL-RM-v1.0-PR03.html, Section 4.1.6, element ResponseType.

B. EDXL-DE Distribution Element

The EDXL-Distribution Element (EDXL-DE) provides a type of container for sending emergency-related messages, such as alerts or a resource message. The basic structure and content of an instance of an EDXL-DE is illustrated in Figure 2-4.[16]

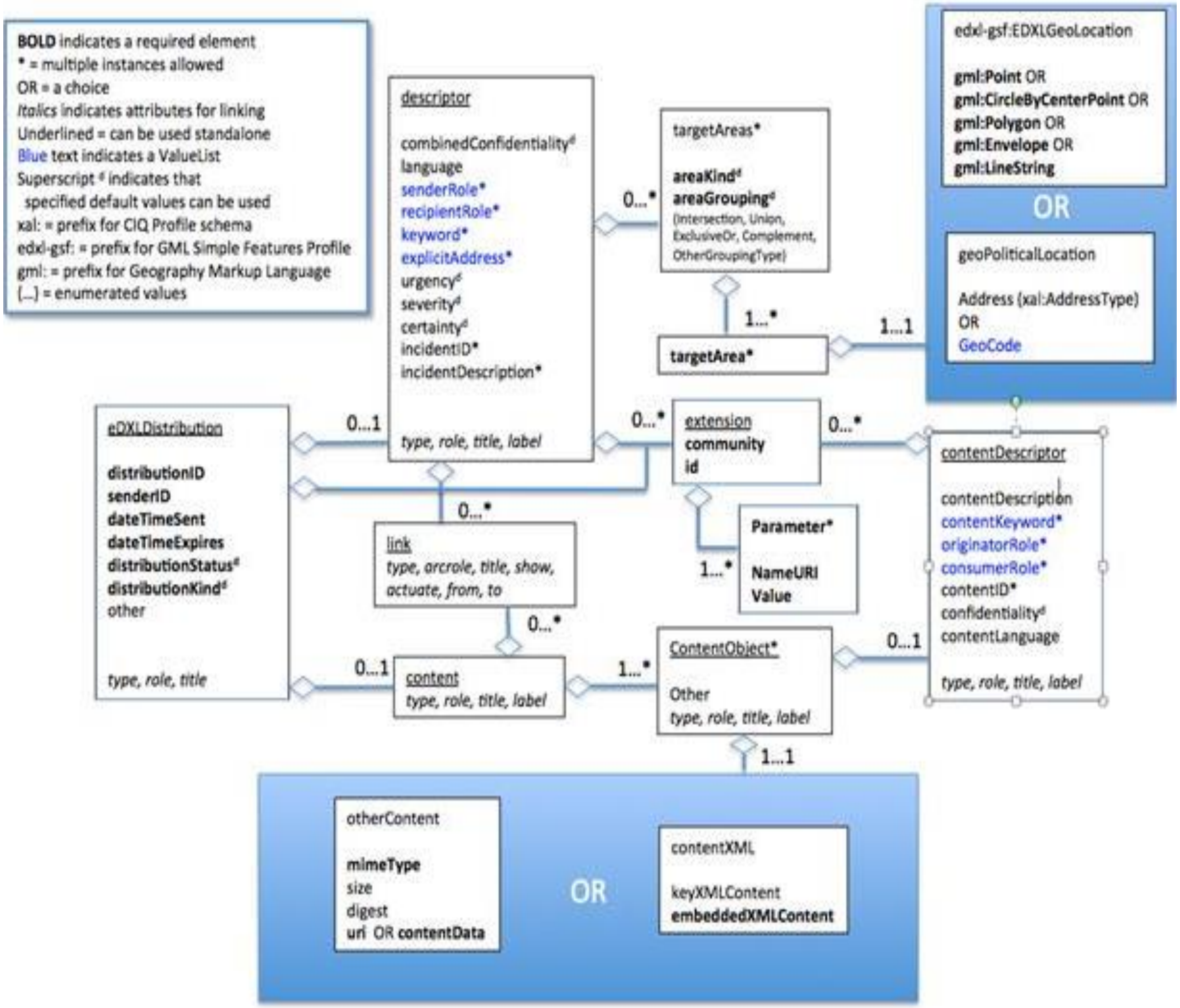


Figure 2-4. EDXL-DE Object Model

The EDXL-DE ontology conceptualizes the seven enumerated domains in Figure 2-4: *certainty*, *confidentiality*, *severity*, *distribution status*, *distribution kind*, *area kind*, and *area grouping*. Both the descriptor and contentDescriptor elements identically use confidentiality; hence,

[16] See http://docs.oasis-open.org/emergency/edxl-de/v2.0/edxl-de-v2.0.html, Section 3.1.

the ontology only needs one conceptualization of confidentiality. Each enumeration is expressed using the pattern illustrated in Figure 2-3.

The EDXL-DE ontology does not conceptualize any other elements in Figure 2-4. The ontology definition was driven by its role in Keystone exchanges (Section 5). These exchanges only use the enumerations.

C. EDXL-RM Resource Messaging

The EDXL-Resource Messaging (EDXL-RM) specification defines 16 separate and specific message types supporting the major communication requirements for allocation of resources across the emergency incident life cycle. This includes preparedness, pre-staging of resources, initial and ongoing response, recovery and demobilization/release of resources.[17]

The principal entities and their relationships in an EDXL-RM Resource Message are illustrated in the Resource Messaging Abstract Reference Model in Figure 2-5.[18] This model shows the three main types of resource message: *Request*, *Response*, and *Report*. It shows how each resource message contains resource data and identifies the parties that own the resource, the funding that is used to acquire or apply the resource, and assignments and schedules for managing the resource.

Resource messages draw on 47 enumerated domains. The EDXL-RM ontology conceptualizes them according to the pattern in Section 2 on p. 2-4.

In two cases, the Information Content Entity subclasses identified in the EDXL-RM ontology describe roles an agent may have in the context of a message. BFO includes the concept of a role; accordingly, the EDXL-RM ontology declares two subclasses of the Role class and adds subclass restrictions to the two InformationContentEntity classes, ContactRoleInformationContentEntity and PersonCategoryTypeListInformationContentEntity. These restrictions constrain the subclasses as about some agent with a role. Figure **2-6** shows this graphically for the former class. A Contact Role Information Content Entity "is about" an Agent, specifically one that has some Contact Role as a role.

[17] OASIS, *Emergency Data Exchange Language Resource Messaging* (*EDXL-RM*) 1.0, November 2008, http://docs.oasis-open.org/emergency/edxl-rm/v1.0/os/EDXL-RM-v1.0-OS.pdf.

[18] Ibid., 16.

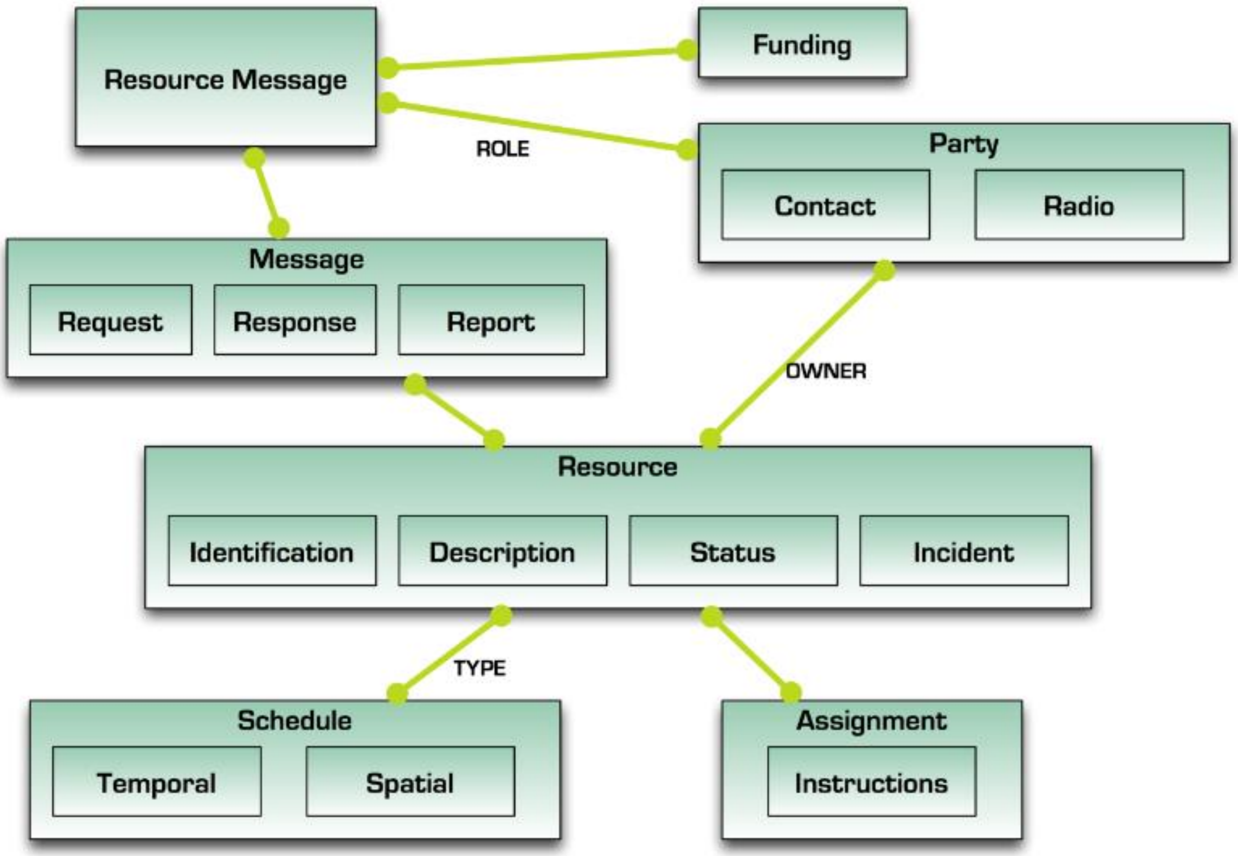
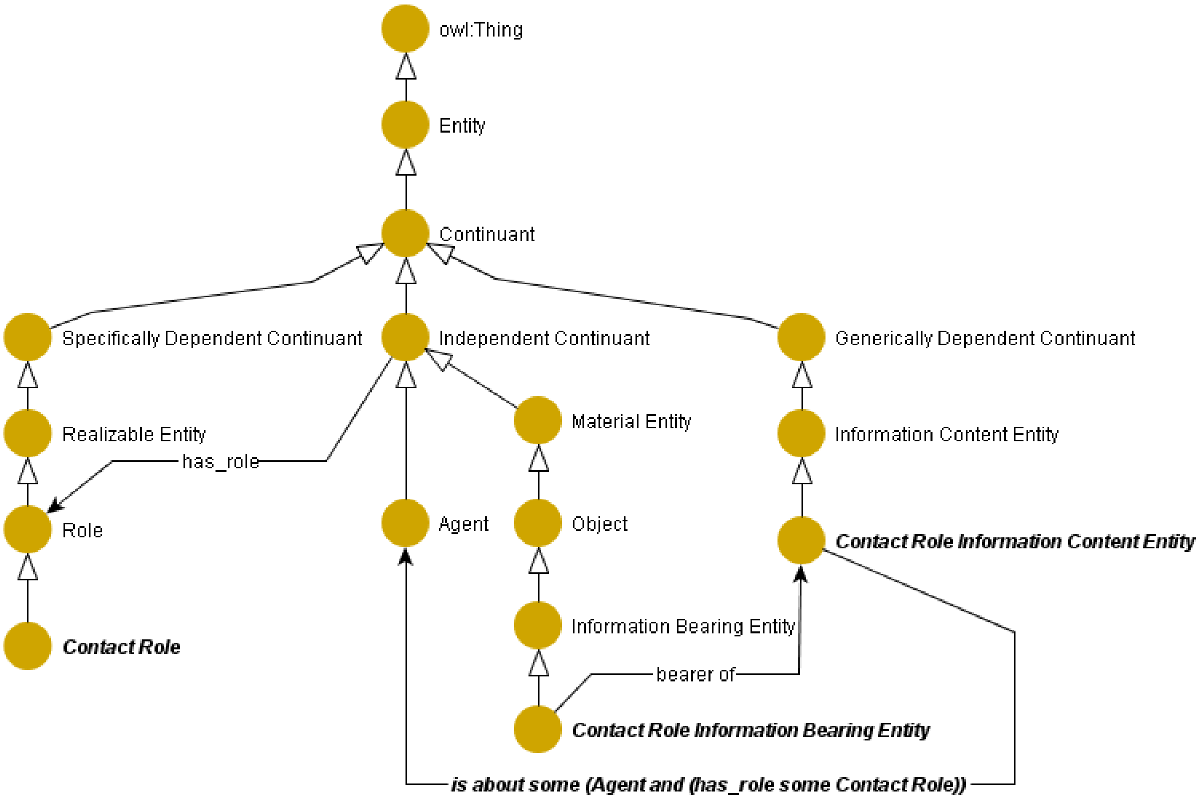


Figure 2-5. EDXL-RM – Abstract Reference Model


owl:Thing
Entity
Continuant
Specifically Dependent Continuant
Independent Continuant
Generically Dependent Continuant
Realizable Entity
Material Entity
Information Content Entity
has_role
Role
Agent
Object
Contact Role Information Content Entity
Contact Role
Information Bearing Entity
bearer of
Contact Role Information Bearing Entity
is about some (Agent and (has_role some Contact Role))

Note: Text in a plain face denotes an entity declared in BFO or the Common Core ontology; text in bold italics denotes an entity declared in the EDXL-RM ontology.

Figure 2-6. An Information Content Entity Describing a Role

D. EDXL-HAVE (Hospital Availability Exchange)

The EDXL-Hospital AVailability Exchange (EDXL-HAVE) is designed to support the exchange of information about available hospital services and resources, such as available hospital beds and burn units. This type of information can be critical for effective routing of victims by EMS. Like many EDXL messages, those using EDXL-HAVE are more likely to go to Emergency Operations Centers (EOCs) or dispatching operations than directly to field responders. The emergency management infrastructure requires such information for effective dispatching and coordination of incident responders themselves. Figure 2-7 shows the document object model for EDXL-HAVE messages.[19]

[19] OASIS, “Emergency Data Exchange Language (EDXL) Hospital AVailability Exchange (HAVE) Version 1.0,” December 22, 2009, Section 3.1, http://docs.oasis-open.org/emergency/edxl-have/v1.0/errata/edxl-have-v1.0-os-errata-os.html.

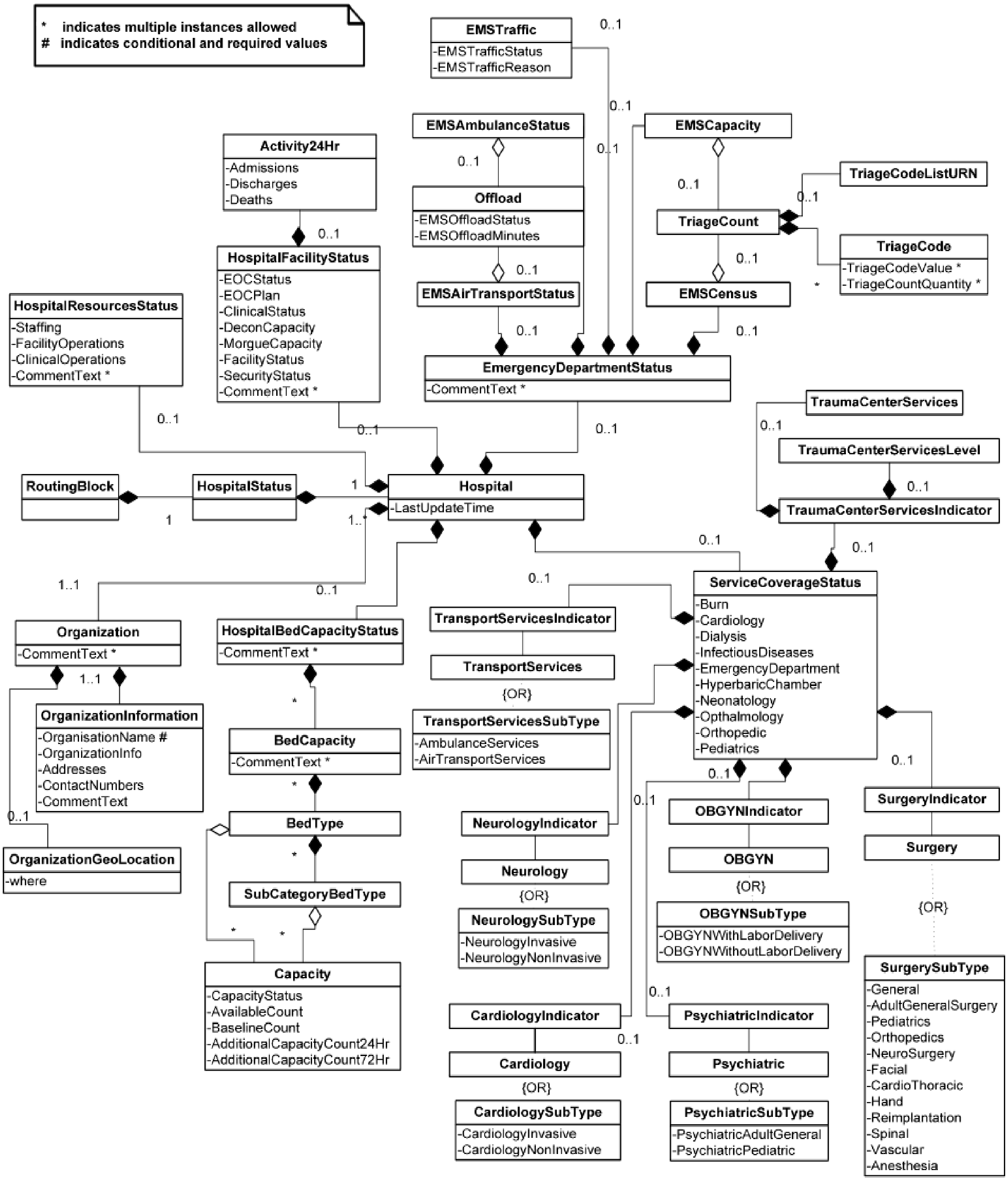


Figure 2-7. EDXL-HAVE Document Object Model

The EDXL-HAVE ontology, like the EDXL-DE and EDXL-RM ontologies, declares an Information Bearing Entity subclass for each EDXL-HAVE enumeration, declares corresponding Information Content Entity subclasses, and, insofar as is possible, asserts an “is about” subclass restriction on these subclasses. The EDXL-HAVE ontology goes further, completely defining the text that can be borne in an EDXL-HAVE message and the structure of valid messages. The structure as specified in the ontology derives from the XML Schema Definition (XSD) for EDXL-HAVE published by OASIS (Figure 2-7, while much easier to read than an XSD, is non-normative).[20]

This ontology structure is defined as follows. When an XSD declares an element, it defines the element as either simple or complex. A simple element has no structure and has textual content. A complex element consists of nested elements. Each nested element has a multiplicity. EDXL-HAVE uses four multiplicities: 1..1 (required), 0..1 (optional), 0..* (an unspecified number, including zero), and 1..* (at least one, but no fixed upper limit).

Suppose the XSD states that an element *E* has exactly one instance of a nested element *F* (1..1 multiplicity). In the EDXL-HAVE ontology, the Information Bearing Entity conceptualizing *E* includes the following subclass restriction:

ro:has_part **exactly** 1 F

where F is the Information Bearing Entity conceptualizing *F*. Object property ro:has_part is a primitive BFO property used to assert a part-whole relationship between two individuals. Figure 2-7 shows that a Hospital must have an Organization. Therefore, class HospitalInformationBearingEntity has the subclass restriction:

ro:has_part **exactly** 1 Organization

Furthermore, Figure 2-7 shows that class Hospital owns class Organization. Therefore, class Organization includes the subclass restriction:

ro:part_of **exactly** 1 Hospital

If an element is optional, the restriction uses max instead of exactly. Class Hospital has the restriction:

ro:has_part **max** 1 HospitalBedCapacityStatus

Again, HospitalBedCapacityStatus has a restriction making it part of exactly one Hospital.

An association requiring at least one element translates to a restriction that uses “some”.

For an association that is optional and without upper limit (0..* multiplicity), the corresponding containing ontology class has no restriction. The nested class is still restricted to be part of the containing class.

[20] The schema is available at http://docs.oasis-open.org/emergency/edxl-have/v1.0/edxl-have.xsd.

A few elements can be nested within more than one element (e.g., Capacity). The restriction on the corresponding nested class expresses this by using the union of all possible classes. For Capacity, the restriction is:

ro:part_of **exactly** 1 { BedType, SubCategoryBedType }

Using this structure, the ontology can express the complete content of an EDXL-HAVE message as a collection of Information Bearing Entity individuals related by part-of and has-part object property assertions. Because has-part restrictions cannot express 0..* multiplicities, the ontology cannot be used to deduce the complete structure of an EDXL-HAVE message from the top down (i.e., by starting at the topmost element, HospitalStatusInformationBearingEntity, and recursively following ro:has_part assertions). The structure can, however, be deduced bottom up: by starting from all leaf-level classes (those without ro:has_part restrictions) and following their ro:part_of restrictions.

Every leaf-level class in the EDXL-HAVE ontology has a restriction declaring it to be the bearer of some Information Content Entity subclass. This is the pattern used for enumerations in the other EDXL ontologies, but in EDXL-HAVE it also applies to non-enumerated entities. For example, an EDXL-HAVE message may include an AvailableCount element, referring to the number of available beds to which patients can be transported. The AvailableCount element is expressed as class AvailableCountInformationBearingEntity. That class has restriction:

ero:bearer_of **some** info:CountMeasurement

Class CountMeasurement, which is part of the Common Core ontology, is a Descriptive Information Content Entity that measures the number of members of some aggregate.

E. Common Alerting Protocol

The Common Alerting Protocol (CAP) was developed to provide a standard for sending and receiving alerts and notifications. In November 2000, the National Science and Technology Council issued a report with this recommendation: "a standard method should be developed to collect and relay instantaneously and automatically all types of hazard warnings and reports locally, regionally, and nationally for input into a wide variety of dissemination systems."[21] CAP version 1.0 was released in 2004. Changes based on user feedback were incorporated into version 1.1, which was released in 2005. The current version, 1.2, was released in 2008. CAP was then incorporated into the broader EDXL standard since CAP is appropriate for providing alerts in emergency situations.

[21] FEMA, "Effective Disaster Warnings Report Published," news release no. HQ-00-135, November 17, 2000, https://www.fema.gov/news-release/2000/11/17/effective-disaster-warnings-report-published.

The CAP is non-proprietary. It is platform-independent: it can be used to send messages from, route messages through, and deliver messages to any digital device. Its objective is to eliminate the need for custom software interfaces devoted to warning sources and dissemination systems.

A CAP message is an XML document. Figure 2-8 shows its structure. The document contains an *alert*. An *alert* contains elements to identify itself; to supply such metadata on the sender; the time the message was sent, the status (actual, exercise, etc.), the type (alert, update, etc.), and the scope (public, restricted, or private); and to provide the alert's information contents (*info*). The *info* content comprises information that includes:

- Textual descriptions, suitable for display on devices (these descriptions may be brief, suitable for receipt as text messages, or arbitrarily long);
- Dates and times when events related to the alert are slated to begin (or have begun) and end and when the alert is to expire;
- Parameters intended for use by automated systems processing the message.

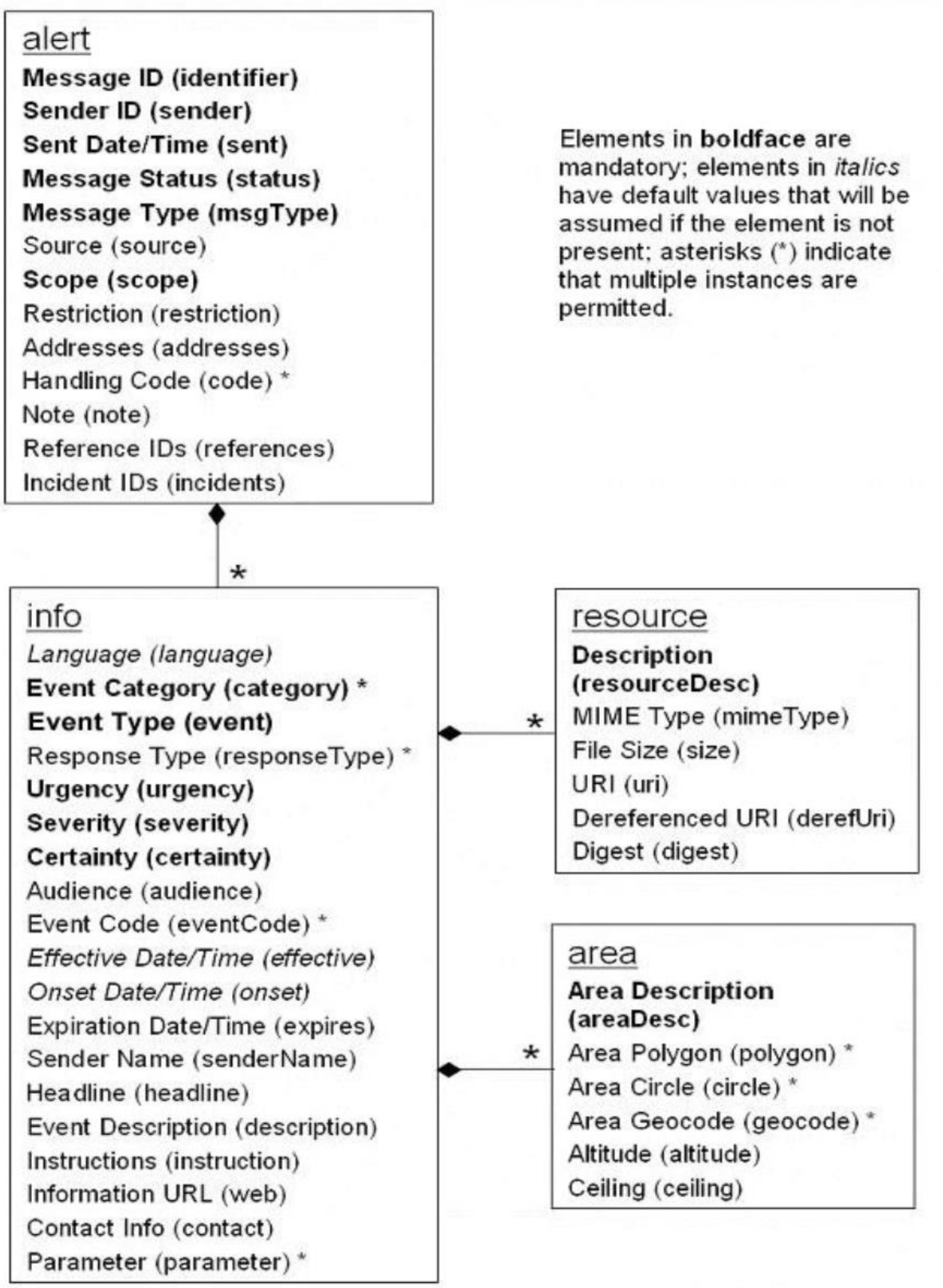
The information also contains any number of two categories of elements: *area* and *resource*. Area elements describe the geographical area in which an event occurs. An area can be given as a circle or polygon or by using an application-specific coding system. It may be two or three dimensional.

A *resource* is an entity of interest to describing an event. Typically, it is a file containing an image, audio, video, or some other content that cannot be represented as text. A *resource* can be a URL, if the receiving device is expected to have access to the Internet. Alternately, a *resource* can be embedded in the content of an alert message using base-64 encoding.

The CAP ontology models messages, but a CAP message is in response to an incident, so the CAP ontology goes into some detail to define what an incident is and how a CAP message expresses the incident. Furthermore, CAP allows for several types of messages. An actor may send an initial alert message; may update an alert message; and may send a message canceling an alert. A receiver may acknowledge or reject an alert.

With these points in mind, the CAP ontology can be understood as organized around the following concepts:

- Message—An Information Bearing Entity denoting a physical CAP message, that is, an electronically transmitted XML document.
- Incident—A Process (something with material effect, occurring at some location and during some time instant or interval), denoting a situation deemed to require the transmission of alerts and an emergency response.
- Incident Response Activity—An Intentional Act undertaken to investigate or ameliorate an Incident and initiated by a Message.



Elements in **boldface** are mandatory; elements in *italics* have default values that will be assumed if the element is not present; asterisks (*) indicate that multiple instances are permitted.

Figure 2-8. Alert Message Structure

Each of these concepts sits at the root of a class hierarchy in the CAP ontology. The hierarchy derives from CAP terminology and definitions. Figure 2-9 shows the CAP hierarchy for the Message categories.

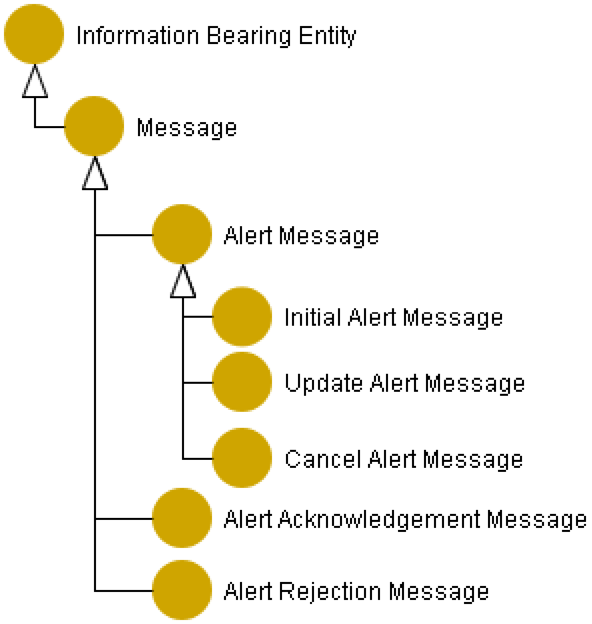


Figure 2-9. CAP Message Class Hierarchy

Similarly, the CAP ontology defines an incident hierarchy of 25 classes, including such categories as nuclear incidents, environmental incidents, and health incidents. It uses the CAP concept of incident response categories to define seven kinds of acts that might be undertaken in response to an incident (see Figure 2-10).

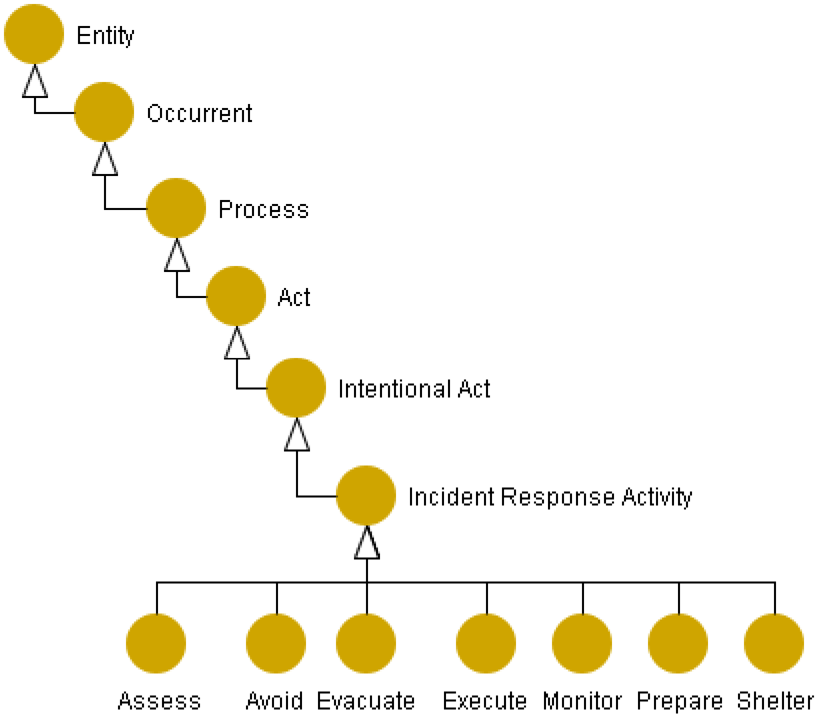


Figure 2-10. Incident Response Activity Class Hierarchy

Some CAP message elements and referents, such as scope (public, private, or restricted) and status (actual, exercise, etc.), can be perceived as what BFO terms a *quality*; that is, a CAP message has the quality of being public, private, or restricted. Figure 2-11 shows the two currently defined quality classes. The Common Core ontology declares an object property has_quality, which associates an independent continuant with a quality. The CAP ontology declares an object property that specializes has_quality: hasScope, the range of which is Message Distribution Scope. Distribution scope is a required quality of a CAP message. Accordingly, class CAPMessage has the following restriction:

cap:hasScope **some** cap:MessageDistributionScope

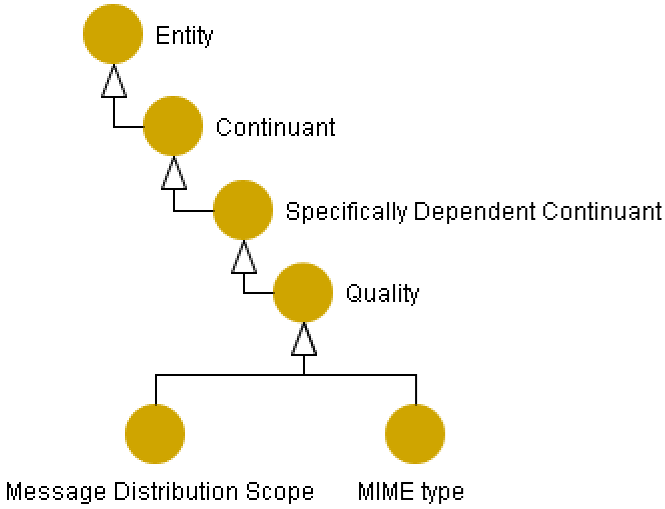


Figure 2-11. Quality Hierarchy

Figure 2-12 shows an example of modeling a message using the CAP ontology. The example, taken from a message in Appendix A, Section A.1 of the OASIS CAP specification, contains a Homeland Security Advisory System Alert. Figure 2-12 shows a few of the OWL individuals that would be used to model it. Individual homeland-security-advisory-system-alert-message denotes a physical message, a string of characters that form an XML message, shown in Figure 2-12 as the value of the info:has_text_value data property. This OWL individual is the "bearer of" four individuals. One, homeland-security-advisory-system-alert-message-content, is the Information Content Entity that denotes the entire message's content; every instance of the message sent would be a distinct Information Bearing Entity (more specifically, a distinct cap:InitialAlertMessage); all would be associated with this one Information Content Entity.

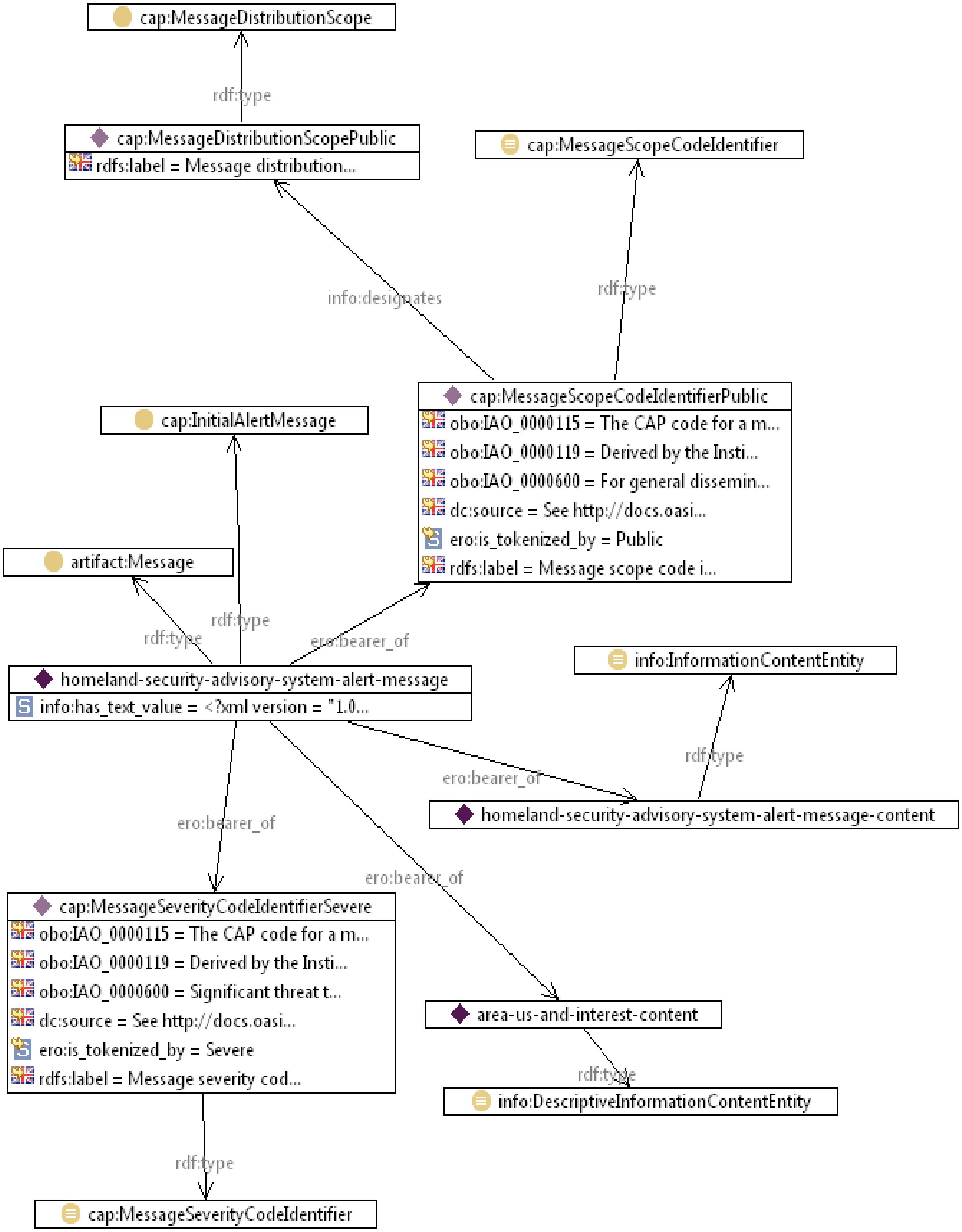

cap:MessageDistributionScope
rdf:type
cap:MessageDistributionScopePublic
rdfs:label = Message distribution...
cap:MessageScopeCodeIdentifier
info:designates
rdf:type
cap:MessageScopeCodeIdentifierPublic
obo:IAO_0000115 = The CAP code for a m...
obo:IAO_0000119 = Derived by the Insti...
obo:IAO_0000600 = For general dissemin...
dc:source = See http://docs.oasi...
ero:is_tokenized_by = Public
rdfs:label = Message scope code i...
cap:InitialAlertMessage
artifact:Message
rdf:type
rdf:type
ero:bearer_of
info:InformationContentEntity
homeland-security-advisory-system-alert-message
info:has_text_value = <?xml version = "1.0...
rdf:type
ero:bearer_of
homeland-security-advisory-system-alert-message-content
ero:bearer_of
ero:bearer_of
cap:MessageSeverityCodeIdentifierSevere
obo:IAO_0000115 = The CAP code for a m...
obo:IAO_0000119 = Derived by the Insti...
obo:IAO_0000600 = Significant threat t...
dc:source = See http://docs.oasi...
ero:is_tokenized_by = Severe
rdfs:label = Message severity cod...
area-us-and-interest-content
rdf:type
info:DescriptiveInformationContentEntity
rdf:type
cap:MessageSeverityCodeIdentifier

Figure 2-12. Example CAP Message Fragment

Other Information Content Entities shown in Figure 2-12 illustrate specific kinds of content borne by the message. For example, every CAP message must have a scope. Figure 2-12 shows that the message is the bearer of individual cap:MessageScopeCodeIdentifierPublic, which designates the quality of public scope (individual cap:MessageDistributionScopePublic). This paradigm, tying a physical message to a quality through its content, is how semantics are established using an ontology based on the Common Core.

Observe that cap:MessageScopeCodeIdentifierPublic has annotation assertion ero:is_tokenized_by = Public. “Public” is one of the strings in a CAP message that can be used to state a message’s scope. This use of the annotation property is one of the ways an Information Content Individual can be related to the specific portion of the text that bears it.

3. Emergency Incident Data Document (EIDD) Ontology

A. Introduction

The Emergency Incident Data Document (EIDD) is an international data standard that provides industry-neutral National Information Exchange Model (NIEM) conformant (XML-based) specifications for exchanging emergency incident information among agencies and regions that implement NG9-1-1 and IP-based emergency communications systems.[22] It was developed by the Association for Public-Safety Communications Officials (APCO) International and the National Emergency Number Association (NENA), and approved by the American National Standards Institute (ANSI) on January 3, 2017.

The EIDD's recent pedigree and approval by multiple relevant standards bodies makes it an excellent basis for future emergency incident information exchanges. Hence, its information elements and structures are included in the *PS/EM Communications Ontology*. A distinct ontology has been developed for the EIDD, which is imported into the overall *PS/EM Communications Ontology*.

B. EIDD Structure

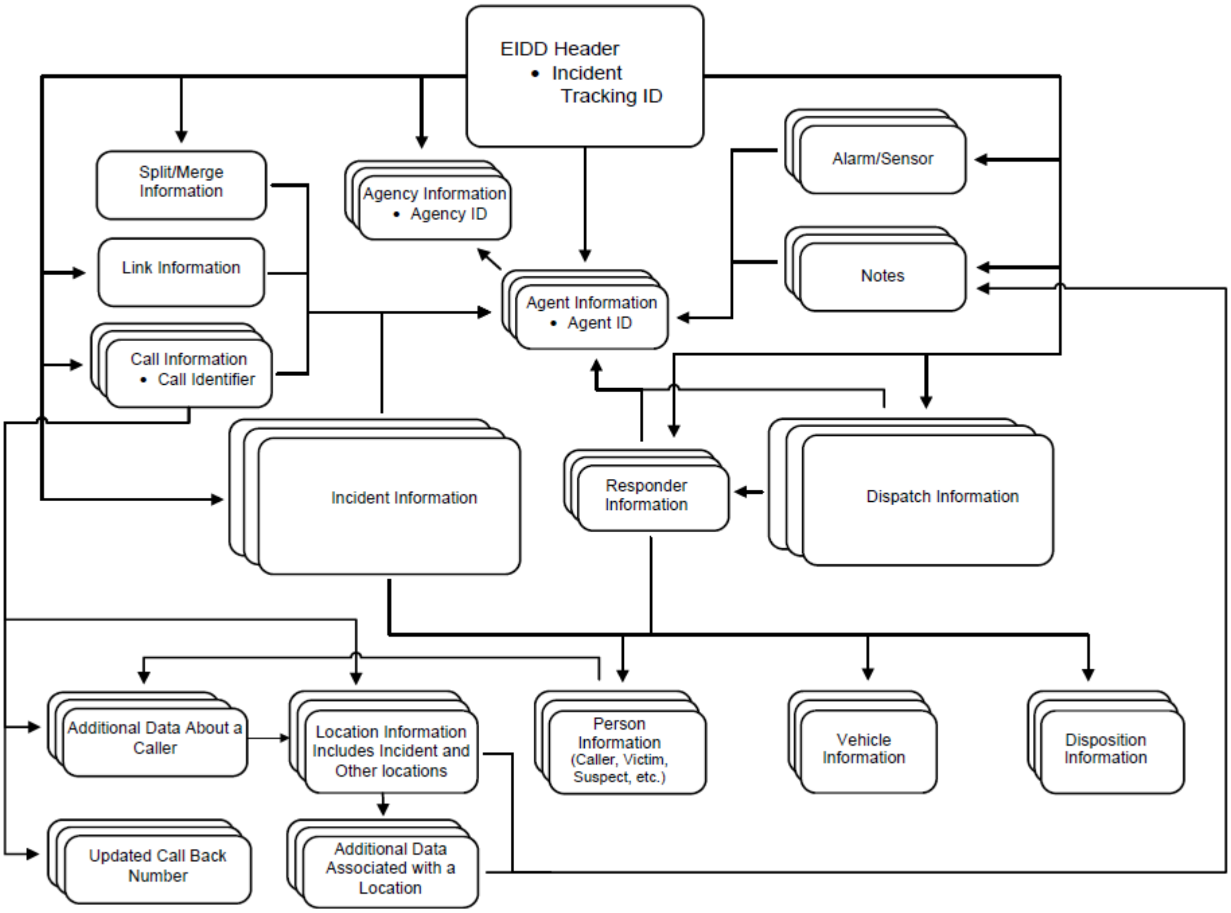
The EIDD standard specifies the format for EIDD messages, which are referred to as EIDDs. An EIDD is organized into related sets of EIDD information components, which comprise the EIDD, as illustrated by Figure 3-1.

This figure shows an EIDD as composed of an *EIDD Header*, which comprises numerous other EIDD data components, such as *Agent Information*, *Incident Information*, and *Dispatch Information*. Each of the links between components in this figure indicates that one component (with the arrowhead) is part of the other component. Some components are required and others are optional, although this status is not indicated by the diagram.

EIDDs are represented in the EIDD ontology as instances of the 'EIDD Message' class, highlighted in the screenshot from the Protégé ontology tool shown in Figure 3-2. The placement of 'EIDD Message' in the Class hierarchy windowpane of this Protégé view shows that the class is a subclass of the 'Message' class, which is a subclass of the 'Information Bearing Artifact' class, which is a subclass of 'object', which is a type of **'material entity'**. That is, all EIDD messages are modeled

[22] APCO International, *NG9-1-1 Emergency Incident Data Document* (*EIDD*), APCO/NENA 2.105.1-2017, p. 2, https://www.apcointl.org/doc/911-resources/apco-standards/694-apco-nena-2-105-1-2017-ng9-1-1-emergency-incident-data-document-eidd/file.html.

as types of information-bearing artifacts, which are specific physical encodings of the EIDD information content for a particular incident.

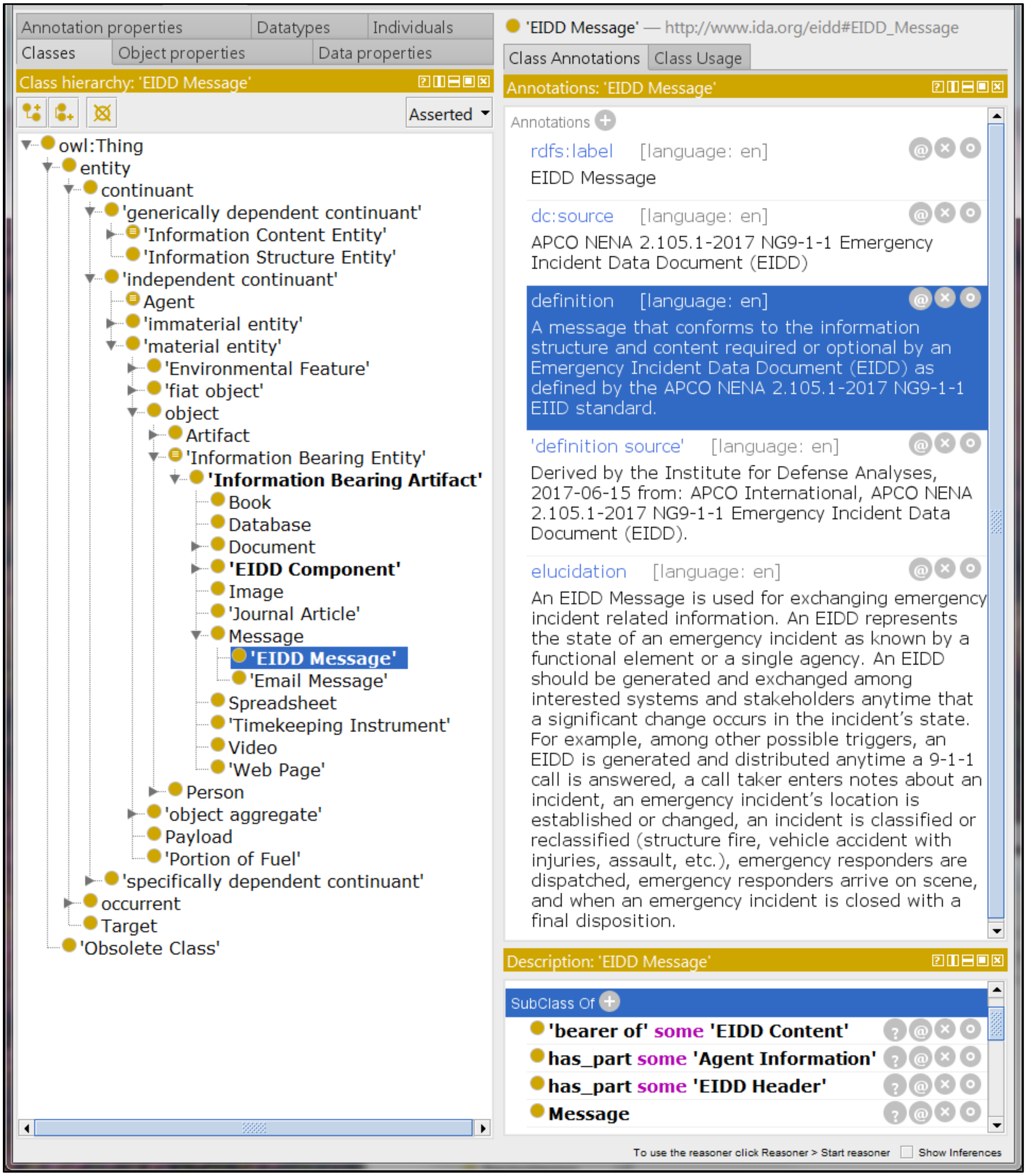


Source: APCO International, *NG9-1-1 Emergency Incident Data Document* (*EIDD*), 16.

Figure 3-1. EIDD Message Component Structure

The Protégé windowpane labeled *Description* in Figure 3-2 asserts that instances of the 'EIDD Message' class have a minimum of two parts: an 'Agent Information' component and an 'EIDD Header' component. These are the only required components in an EIDD message.

The Protégé *Annotations* windowpane in Figure 3-2 asserts metadata about the 'EIDD Message' class, including a label, source, definition, definition source, and elucidation of the definition. Note that the source of the definition identifies it as derived by IDA from the APCO/NENA EIDD documentation because that documentation does not provide an explicit definition for this concept. That source does include an extensive discussion of the concept, which is captured by the elucidation annotation.



'EIDD Message' — http://www.ida.org/eidd#EIDD_Message

rdfs:label [language: en]
EIDD Message

dc:source [language: en]
APCO NENA 2.105.1-2017 NG9-1-1 Emergency Incident Data Document (EIDD)

definition [language: en]
A message that conforms to the information structure and content required or optional by an Emergency Incident Data Document (EIDD) as defined by the APCO NENA 2.105.1-2017 NG9-1-1 EIID standard.

'definition source' [language: en]
Derived by the Institute for Defense Analyses, 2017-06-15 from: APCO International, APCO NENA 2.105.1-2017 NG9-1-1 Emergency Incident Data Document (EIDD).

elucidation [language: en]
An EIDD Message is used for exchanging emergency incident related information. An EIDD represents the state of an emergency incident as known by a functional element or a single agency. An EIDD should be generated and exchanged among interested systems and stakeholders anytime that a significant change occurs in the incident's state. For example, among other possible triggers, an EIDD is generated and distributed anytime a 9-1-1 call is answered, a call taker enters notes about an incident, an emergency incident's location is established or changed, an incident is classified or reclassified (structure fire, vehicle accident with injuries, assault, etc.), emergency responders are dispatched, emergency responders arrive on scene, and when an emergency incident is closed with a final disposition.

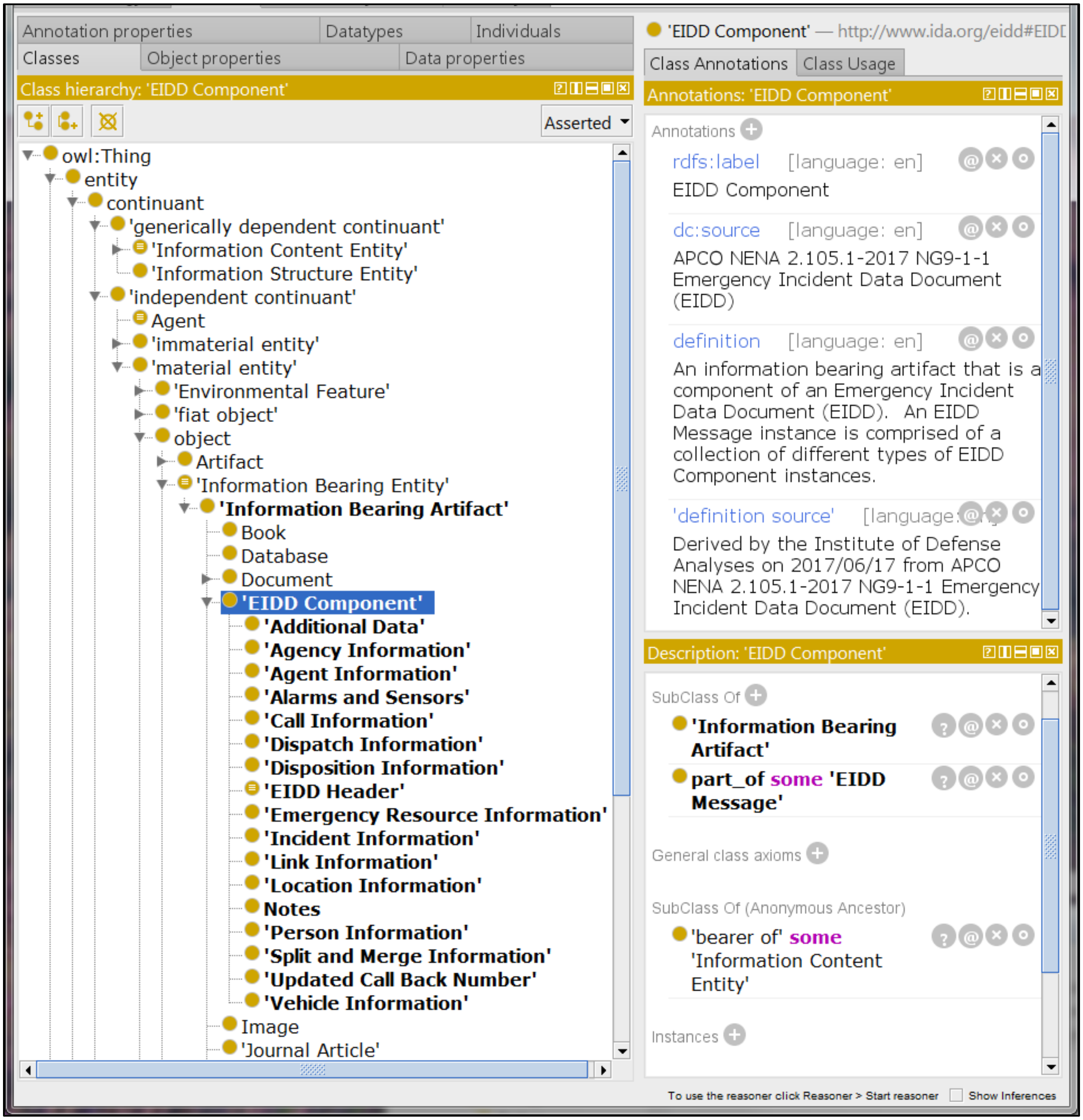
SubClass Of
'bearer of' some 'EIDD Content'
has_part some 'Agent Information'
has_part some 'EIDD Header'
Message

Figure 3-2. 'EIDD Message' Class Specification in the EIDD Ontology

Components of an EIDD are represented by the 'EIDD Component' class and its subclasses. This is illustrated in the Protégé class view of Figure 3-3, where the 'EIDD Component' class is expanded to show its subclasses. The EIDD structure is represented in the EIDD ontology by modeling the parts of EIDDs using the part_of relation from the BFO relations ontology (ro.owl).

The Description windowpane of Figure 3-3 includes the assertion that every instance of an ‘EIDD Component’ is part_of some ‘EIDD Message’. Note that this does not imply that every ‘EIDD Message’ has every EIDD component as a part since most of the EIDD components are optional. Those that are optional are individually asserted to be part of some instance of ‘EIDD Message’ since every component only exists as part of a whole EIDD, as it is defined in the ontology.

Each of the EIDD components is modeled as a separate class, which is a subclass of the ‘EIDD Component’ class, as shown in Figure 3-3.



rdfs:label [language: en]
EIDD Component

dc:source [language: en]
APCO NENA 2.105.1-2017 NG9-1-1 Emergency Incident Data Document (EIDD)

definition [language: en]
An information bearing artifact that is a component of an Emergency Incident Data Document (EIDD). An EIDD Message instance is comprised of a collection of different types of EIDD Component instances.

'definition source' [language:
Derived by the Institute of Defense Analyses on 2017/06/17 from APCO NENA 2.105.1-2017 NG9-1-1 Emergency Incident Data Document (EIDD).

SubClass Of
'Information Bearing Artifact'
part_of some 'EIDD Message'

SubClass Of (Anonymous Ancestor)
'bearer of' some 'Information Content Entity'

Figure 3-3. EIDD Component Subclasses

C. Agent Information Component

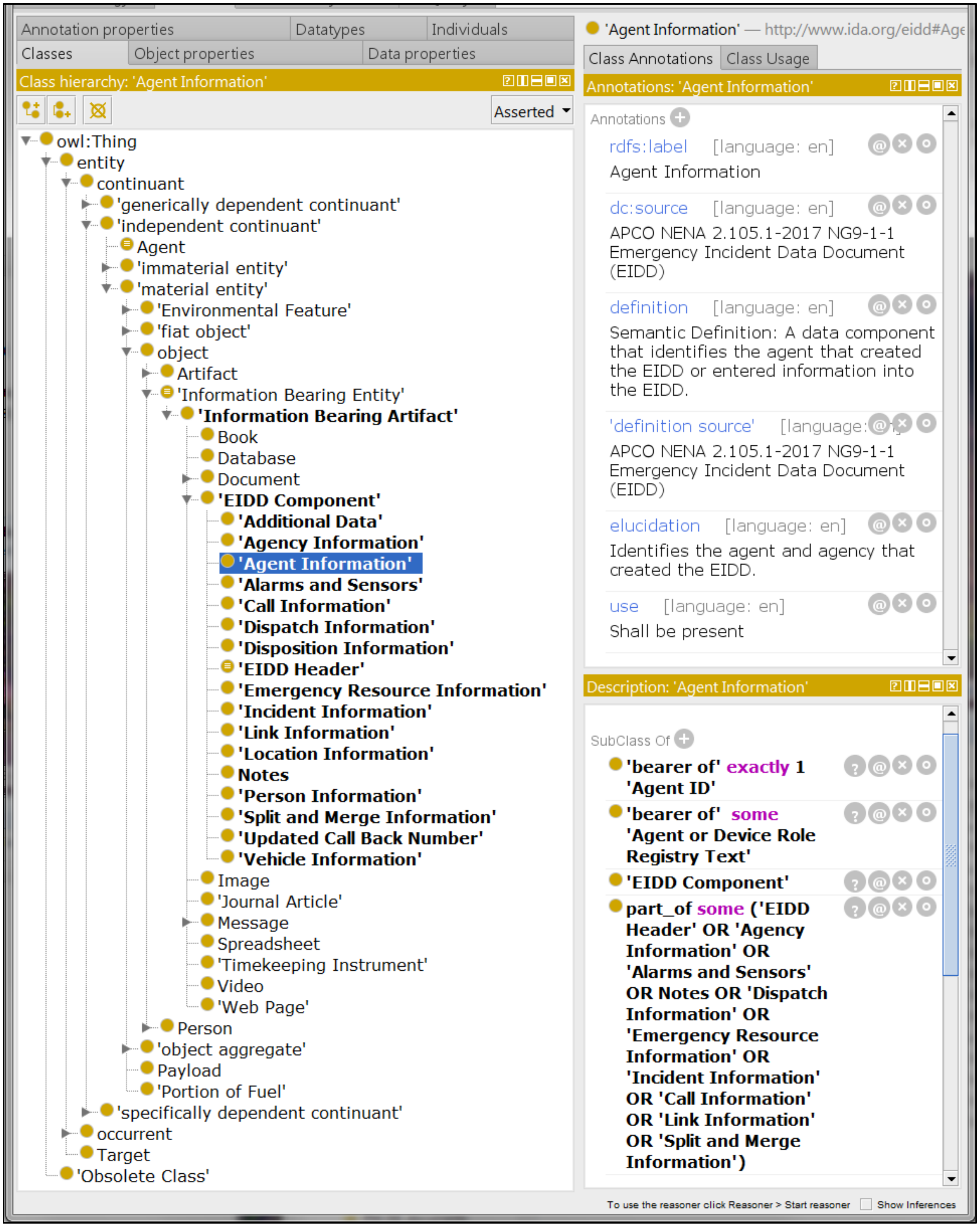
The Agent Information component of an 'EIDD Message' provides a good illustration of how an 'EIDD Component' and its information content are modeled in the EIDD ontology. Figure 3-4 shows the Protégé class view of the 'Agent Information' class. The Description windowpane in this screenshot identifies the essential information content elements that are required parts of the Agent Information component. In particular, every instance of 'Agent Information' is asserted to be the 'bearer of' exactly one 'Agent ID'. This reflects the use of Agent Information to represent the unique agent responsible for generating an EIDD or for contributing to a specific component of an EIDD.

The class in turn has its own formal definition in terms of its place in the overall class hierarchy, as well as information on what it designates, as shown in Figure 3-5. In particular, 'Agent ID' is asserted to designate exactly one Agent.[23] The 'designates' property links an instance of a 'Designative Information Content Entity', such as an 'Agent ID', to a real-world object that it designates. This is one way of linking the information content of messages to real-world entities.

Every instance of 'Agent Information' must be a part of some EIDD component, such as the EIDD Header, as described by the part_of restriction in the Description windowpane of Figure 3-4. Every instance of 'Agent Information' must be part of one of the EIDD components listed in this restriction.

Each instance of 'Agent Information' is also identified as the 'bearer of' some instance of 'Agent or Device Role Registry Text', which is a 'Code Identifier' for the "*role of an agent or automaton that generated an EIDD or contributed information contained in an EIDD*," as defined by the APCO/NENA source document and captured in its definition annotation in the ontology. This is an example of how essential primitive information content (such as a code or ID) is modeled in the ontology. Nonessential, or optional, information content for an EIDD component may be asserted as inhering in that component when it exists, although it need not exist in every such component.

[23] NENA-STA-010 states that an Agent ID can be used to uniquely identify an agent, be it a human, automaton, or functional element. The syntax is an email address.


Annotation properties
Datatypes
Individuals
Classes
Object properties
Data properties
Class hierarchy: 'Agent Information'
Asserted
'Agent Information' — http://www.ida.org/eidd#Age
Class Annotations
Class Usage
Annotations: 'Agent Information'
Annotations
Description: 'Agent Information'
SubClass Of
To use the reasoner click Reasoner > Start reasoner
□ Show Inferences

- owl:Thing
  - entity
    - continuant
      - 'generically dependent continuant'
      - 'independent continuant'
        - Agent
        - 'immaterial entity'
        - 'material entity'
          - 'Environmental Feature'
          - 'fiat object'
          - object
            - Artifact
            - 'Information Bearing Entity'
              - **'Information Bearing Artifact'**
                - Book
                - Database
                - Document
                - **'EIDD Component'**
                  - **'Additional Data'**
                  - **'Agency Information'**
                  - **'Agent Information'**
                  - **'Alarms and Sensors'**
                  - **'Call Information'**
                  - **'Dispatch Information'**
                  - **'Disposition Information'**
                  - **'EIDD Header'**
                  - **'Emergency Resource Information'**
                  - **'Incident Information'**
                  - **'Link Information'**
                  - **'Location Information'**
                  - **Notes**
                  - **'Person Information'**
                  - **'Split and Merge Information'**
                  - **'Updated Call Back Number'**
                  - **'Vehicle Information'**
                - Image
                - 'Journal Article'
                - Message
                - Spreadsheet
                - 'Timekeeping Instrument'
                - Video
                - 'Web Page'
            - Person
          - 'object aggregate'
          - Payload
          - 'Portion of Fuel'
      - 'specifically dependent continuant'
    - occurrent
    - Target
  - 'Obsolete Class'

rdfs:label [language: en]
Agent Information

dc:source [language: en]
APCO NENA 2.105.1-2017 NG9-1-1 Emergency Incident Data Document (EIDD)

definition [language: en]
Semantic Definition: A data component that identifies the agent that created the EIDD or entered information into the EIDD.

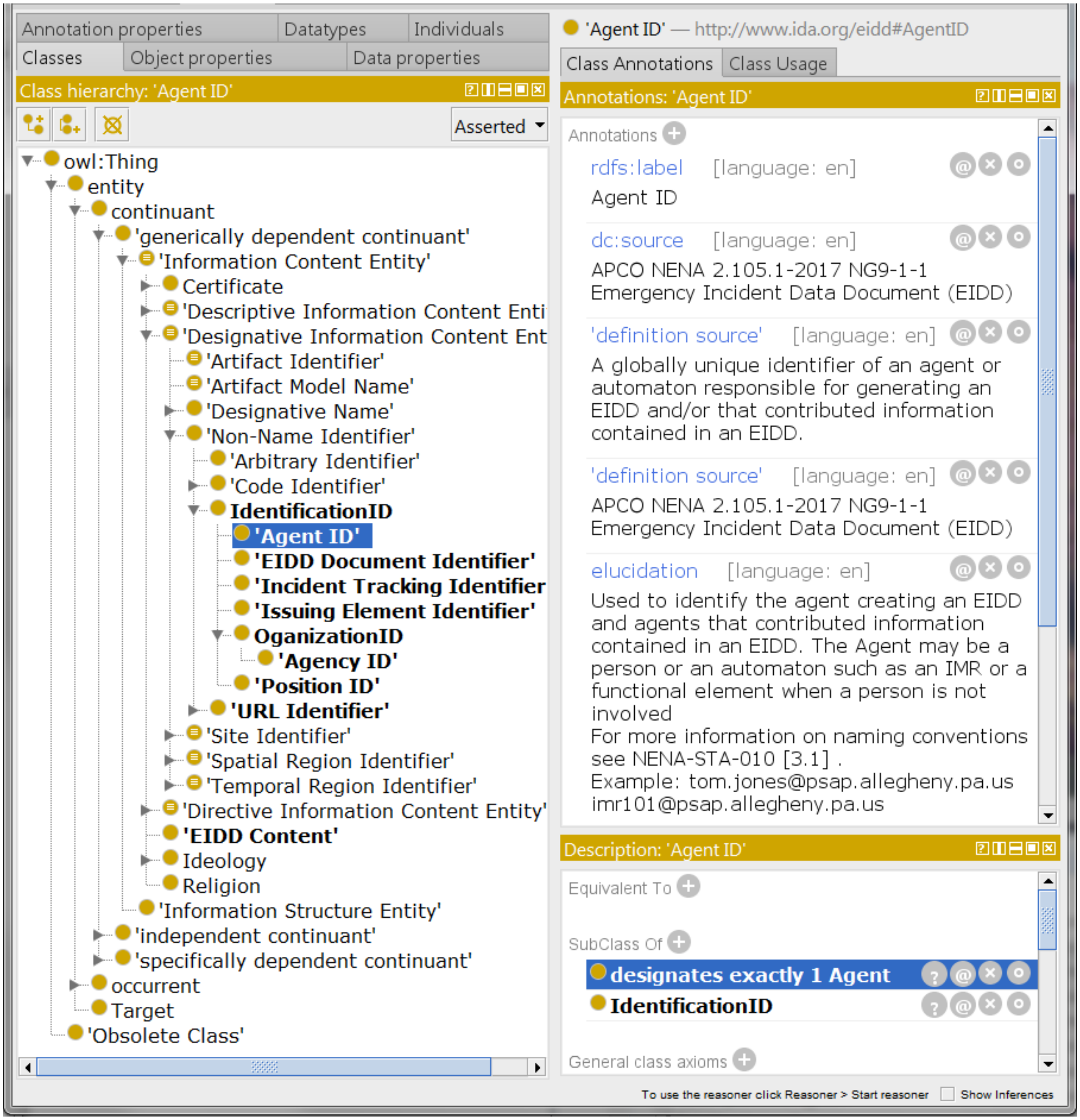
'definition source' [language:
APCO NENA 2.105.1-2017 NG9-1-1 Emergency Incident Data Document (EIDD)

elucidation [language: en]
Identifies the agent and agency that created the EIDD.

use [language: en]
Shall be present

- **'bearer of' exactly 1 'Agent ID'**
- **'bearer of' some 'Agent or Device Role Registry Text'**
- **'EIDD Component'**
- **part_of some ('EIDD Header' OR 'Agency Information' OR 'Alarms and Sensors' OR Notes OR 'Dispatch Information' OR 'Emergency Resource Information' OR 'Incident Information' OR 'Call Information' OR 'Link Information' OR 'Split and Merge Information')**

Figure 3-4. Agent Information EIDD Component Class Specification



- owl:Thing
  - entity
    - continuant
      - 'generically dependent continuant'
        - 'Information Content Entity'
          - Certificate
          - 'Descriptive Information Content Enti
          - 'Designative Information Content Ent
            - 'Artifact Identifier'
            - 'Artifact Model Name'
            - 'Designative Name'
            - 'Non-Name Identifier'
              - 'Arbitrary Identifier'
              - 'Code Identifier'
              - **IdentificationID**
                - **'Agent ID'**
                - **'EIDD Document Identifier'**
                - **'Incident Tracking Identifier**
                - **'Issuing Element Identifier'**
                - **OganizationID**
                  - **'Agency ID'**
                - **'Position ID'**
              - **'URL Identifier'**
            - 'Site Identifier'
            - 'Spatial Region Identifier'
            - 'Temporal Region Identifier'
          - 'Directive Information Content Entity'
          - **'EIDD Content'**
          - Ideology
          - Religion
        - 'Information Structure Entity'
      - 'independent continuant'
      - 'specifically dependent continuant'
    - occurrent
    - Target
  - 'Obsolete Class'

rdfs:label [language: en]
Agent ID

dc:source [language: en]
APCO NENA 2.105.1-2017 NG9-1-1
Emergency Incident Data Document (EIDD)

'definition source' [language: en]
A globally unique identifier of an agent or automaton responsible for generating an EIDD and/or that contributed information contained in an EIDD.

'definition source' [language: en]
APCO NENA 2.105.1-2017 NG9-1-1
Emergency Incident Data Document (EIDD)

elucidation [language: en]
Used to identify the agent creating an EIDD and agents that contributed information contained in an EIDD. The Agent may be a person or an automaton such as an IMR or a functional element when a person is not involved
For more information on naming conventions see NENA-STA-010 [3.1] .
Example: tom.jones@psap.allegheny.pa.us
imr101@psap.allegheny.pa.us

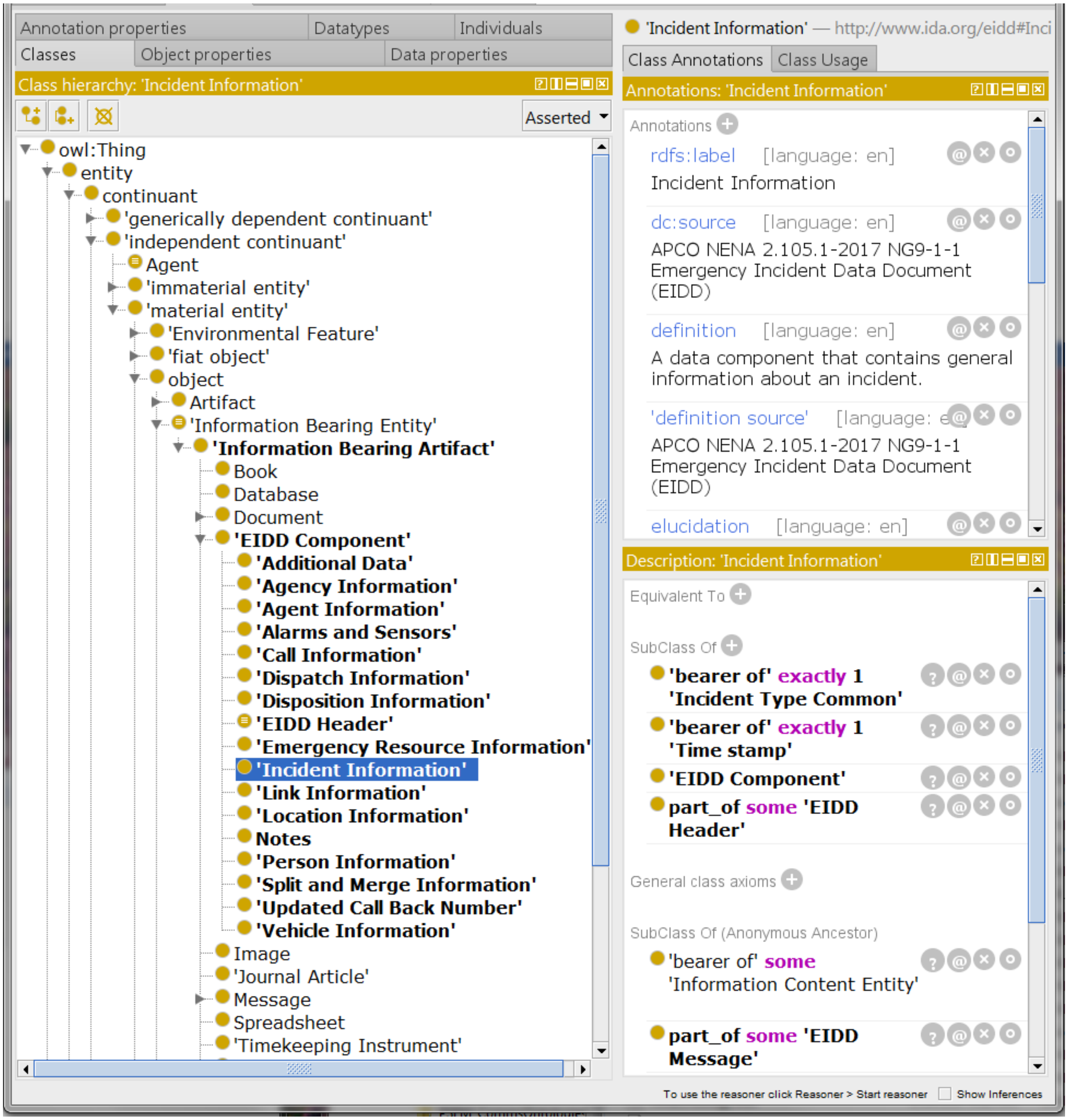
designates exactly 1 Agent
IdentificationID

Figure 3-5. Agent ID Class View in EIDD Ontology

D. Incident Information Component

The Incident Information component of an 'EIDD Message' is a key component of typical messages, although it is not required in every message. It is represented by the 'Incident Information' class in the EIDD ontology, as illustrated in the screenshot of Figure 3-6. This component has two required pieces of information content: exactly one 'Incident Type Common' and exactly one 'Time stamp'. The 'Time stamp' designates the date-time when the incident was created or updated. The

'Incident Type Common' element is designed to capture a common code for the type of the incident. The class definition for 'Incident Type Common' is captured in the screenshot of Figure 3-7.


Annotation properties
Datatypes
Individuals
Classes
Object properties
Data properties
Class hierarchy: 'Incident Information'
Asserted
'Incident Information' — http://www.ida.org/eidd#Inci
Class Annotations
Class Usage
Annotations: 'Incident Information'
Description: 'Incident Information'
To use the reasoner click Reasoner > Start reasoner
□ Show Inferences

- owl:Thing
  - entity
    - continuant
      - 'generically dependent continuant'
      - 'independent continuant'
        - Agent
        - 'immaterial entity'
        - 'material entity'
          - 'Environmental Feature'
          - 'fiat object'
          - object
            - Artifact
            - 'Information Bearing Entity'
              - **'Information Bearing Artifact'**
                - Book
                - Database
                - Document
                - **'EIDD Component'**
                  - **'Additional Data'**
                  - **'Agency Information'**
                  - **'Agent Information'**
                  - **'Alarms and Sensors'**
                  - **'Call Information'**
                  - **'Dispatch Information'**
                  - **'Disposition Information'**
                  - **'EIDD Header'**
                  - **'Emergency Resource Information'**
                  - **'Incident Information'**
                  - **'Link Information'**
                  - **'Location Information'**
                  - **Notes**
                  - **'Person Information'**
                  - **'Split and Merge Information'**
                  - **'Updated Call Back Number'**
                  - **'Vehicle Information'**
                - Image
                - 'Journal Article'
                - Message
                - Spreadsheet
                - 'Timekeeping Instrument'

Annotations

rdfs:label [language: en]
Incident Information

dc:source [language: en]
APCO NENA 2.105.1-2017 NG9-1-1 Emergency Incident Data Document (EIDD)

definition [language: en]
A data component that contains general information about an incident.

'definition source' [language: e
APCO NENA 2.105.1-2017 NG9-1-1 Emergency Incident Data Document (EIDD)

elucidation [language: en]

Equivalent To

SubClass Of

'bearer of' exactly 1 'Incident Type Common'

'bearer of' exactly 1 'Time stamp'

'EIDD Component'

part_of some 'EIDD Header'

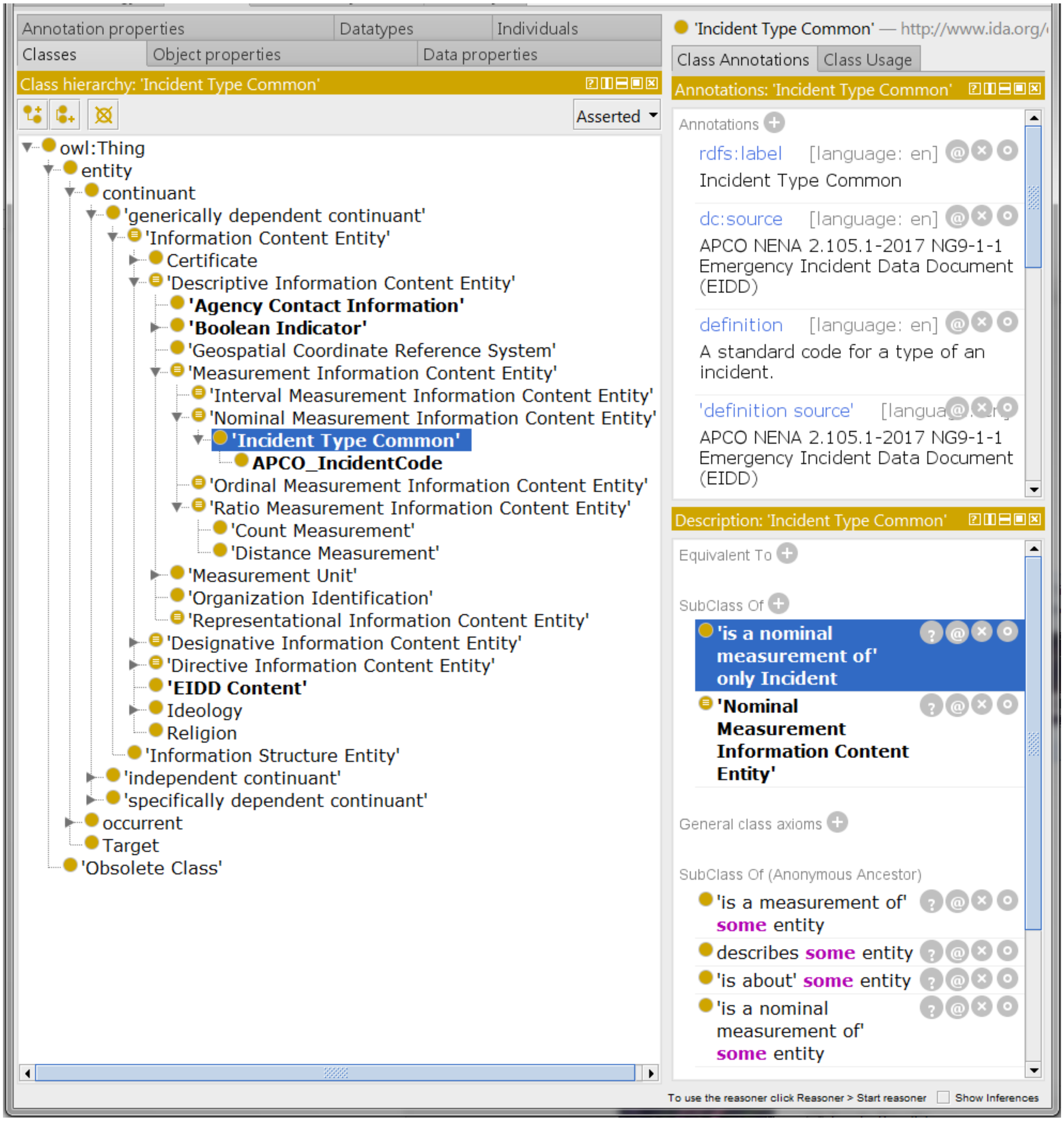
General class axioms

SubClass Of (Anonymous Ancestor)

'bearer of' **some** 'Information Content Entity'

part_of some 'EIDD Message'

Figure 3-6. Incident Information Component Class



Annotation properties | Datatypes | Individuals

Classes | Object properties | Data properties

Class hierarchy: 'Incident Type Common'

Asserted

- owl:Thing
  - entity
    - continuant
      - 'generically dependent continuant'
        - 'Information Content Entity'
          - Certificate
          - 'Descriptive Information Content Entity'
            - **'Agency Contact Information'**
            - **'Boolean Indicator'**
            - 'Geospatial Coordinate Reference System'
            - 'Measurement Information Content Entity'
              - 'Interval Measurement Information Content Entity'
              - 'Nominal Measurement Information Content Entity'
                - **'Incident Type Common'**
                  - **APCO_IncidentCode**
              - 'Ordinal Measurement Information Content Entity'
              - 'Ratio Measurement Information Content Entity'
                - 'Count Measurement'
                - 'Distance Measurement'
            - 'Measurement Unit'
            - 'Organization Identification'
            - 'Representational Information Content Entity'
          - 'Designative Information Content Entity'
          - 'Directive Information Content Entity'
          - **'EIDD Content'**
          - Ideology
          - Religion
        - 'Information Structure Entity'
      - 'independent continuant'
      - 'specifically dependent continuant'
    - occurrent
    - Target
  - 'Obsolete Class'

'Incident Type Common' — http://www.ida.org/

Class Annotations | Class Usage

Annotations: 'Incident Type Common'

Annotations

rdfs:label [language: en]
Incident Type Common

dc:source [language: en]
APCO NENA 2.105.1-2017 NG9-1-1 Emergency Incident Data Document (EIDD)

definition [language: en]
A standard code for a type of an incident.

'definition source' [langua
APCO NENA 2.105.1-2017 NG9-1-1 Emergency Incident Data Document (EIDD)

Description: 'Incident Type Common'

Equivalent To

SubClass Of

'is a nominal measurement of' only Incident

'Nominal Measurement Information Content Entity'

General class axioms

SubClass Of (Anonymous Ancestor)

'is a measurement of' **some** entity

describes **some** entity

'is about' **some** entity

'is a nominal measurement of' **some** entity

To use the reasoner click Reasoner > Start reasoner □ Show Inferences

Figure 3-7. Incident Type Common Class Definition

The 'Incident Type Common' class is a subclass of 'Nominal Measurement Information Content Entity', which is a class from the *Information Entity Ontology* of the *Common Core Ontologies*. The latter class is defined as *consisting of a symbol that classifies Entities according to some shared, possibly arbitrary, characteristic*. Thus, each 'Incident Type Common' instance is asserted to be a nominal measurement of an incident, identifying its type. These types are specified in a separate APCO standard for Public Safety Communications Common Incident Types, specified by the 'APCO Incident Code class, which is described in Section 4.

4. Public Safety Communications Common Incidents Ontology

A. Introduction

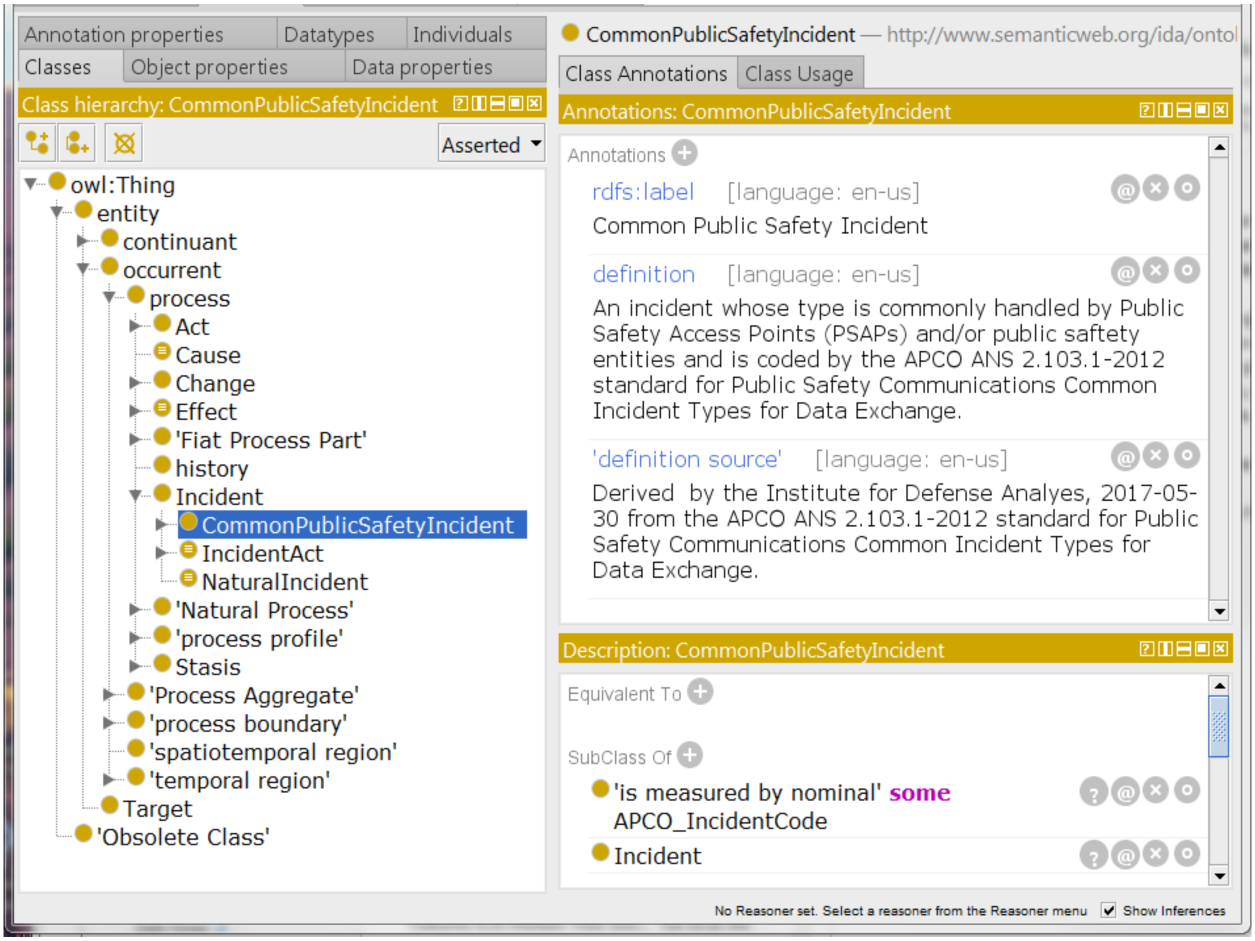
A vital information standard in the PS/EM domain is the one developed by APCO International for categorizing common incident types codified in "Public Safety Communications Common Incident Types for Data Exchange," published in 2012 (APCO ANS 2.103.1-2012). This standardized list of incident types comprises 197 codes intended for use by emergency communications and public safety stakeholders when sharing incident related information. The standard provides the alphanumeric codes for each of the incident types, together with a human-readable legend that the CAD system can display. The standard also provides additional notes and examples for most of the codes. These additions are intended to facilitate the understanding of the meaning and correct use of the codes.

The analysis presented here describes the approach taken when modeling these APCO incident types as OWL classes that form part of the comprehensive PS/EM Communications Ontology.

B. The CommonPublicSafetyIncident Class

Figure 4-1 shows the context of the new CommonPublicSafetyIncident class in the subclass hierarchy of the *PS/EM Communications Ontology*. This class is defined as: *An incident whose type is commonly handled by Public Safety Answering Points* (*PSAPs*) *and/or public safety entities and is coded by the APCO ANS 2.103.1-2012 standard for Public Safety Communications Common Incident Types for Data Exchange*.

As shown in Figure 4-1, the class is modeled as a subclass of Incident, which is defined as: *An occurrence*, [a.k.a. process] *caused by either human action or natural phenomena, that may cause harm and that may require action*. The class Incident is embedded in the standard class hierarchy of the BFO developed by Barry Smith and his associates. That hierarchy starts with the class entity, defined as: *Anything that exists or has existed or will exist*, and specializes into the subclasses continuant and occurrent. The latter is defined as: *An entity that unfolds itself in time or it is the instantaneous boundary of such an entity* (*for example a beginning or an ending*) *or it is a temporal or spatiotemporal region which such an entity occupies temporal-region or occupies spatiotemporal region*. An occurrent that has temporal proper parts and for some time *t* depends on some material entity at *t* is called a process.



rdfs:label [language: en-us]
Common Public Safety Incident

definition [language: en-us]
An incident whose type is commonly handled by Public Safety Access Points (PSAPs) and/or public saftety entities and is coded by the APCO ANS 2.103.1-2012 standard for Public Safety Communications Common Incident Types for Data Exchange.

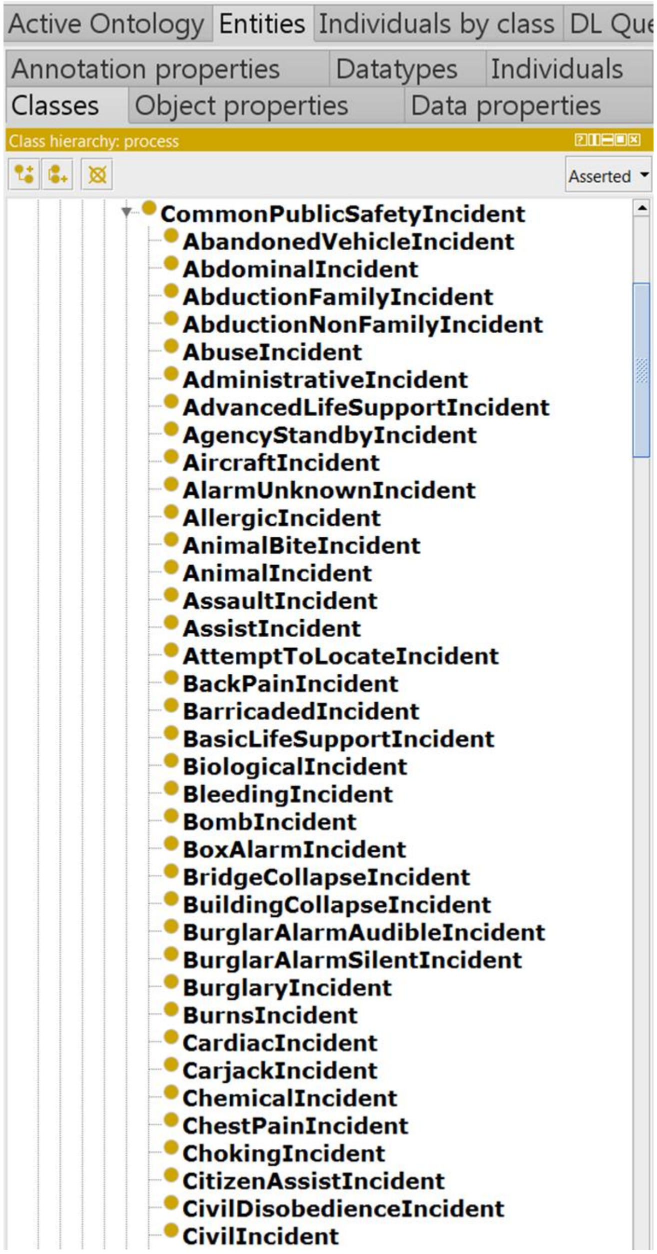
'definition source' [language: en-us]
Derived by the Institute for Defense Analyes, 2017-05-30 from the APCO ANS 2.103.1-2012 standard for Public Safety Communications Common Incident Types for Data Exchange.

SubClass Of
'is measured by nominal' **some** APCO_IncidentCode
Incident

Figure 4-1. Context of CommonPublicSafetyIncident Class in the Ontology

C. The APCO Incident Classes

The 197 incident types contained in the APCO ANS 2.103.1-2012 specification are modeled as subclasses of the proposed new CommonPublicSafetyIncident class. Figure 4-2 shows the first 37 classes that are derived from the APCO codes.



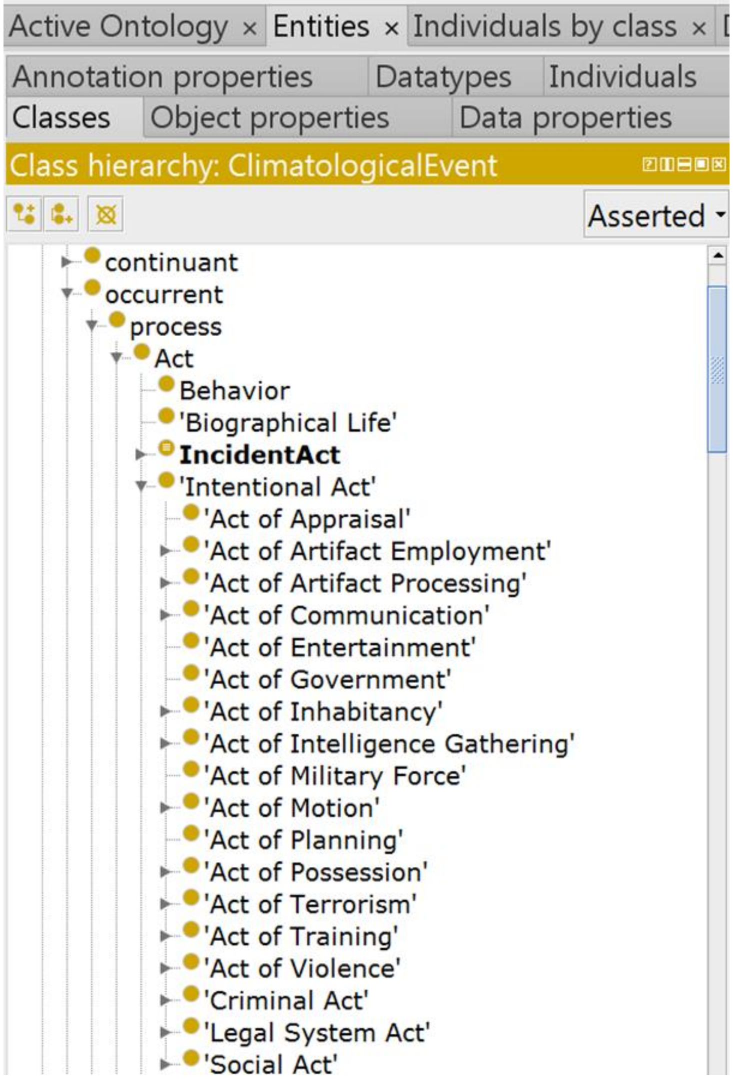
CommonPublicSafetyIncident
- AbandonedVehicleIncident
- AbdominalIncident
- AbductionFamilyIncident
- AbductionNonFamilyIncident
- AbuseIncident
- AdministrativeIncident
- AdvancedLifeSupportIncident
- AgencyStandbyIncident
- AircraftIncident
- AlarmUnknownIncident
- AllergicIncident
- AnimalBiteIncident
- AnimalIncident
- AssaultIncident
- AssistIncident
- AttemptToLocateIncident
- BackPainIncident
- BarricadedIncident
- BasicLifeSupportIncident
- BiologicalIncident
- BleedingIncident
- BombIncident
- BoxAlarmIncident
- BridgeCollapseIncident
- BuildingCollapseIncident
- BurglarAlarmAudibleIncident
- BurglarAlarmSilentIncident
- BurglaryIncident
- BurnsIncident
- CardiacIncident
- CarjackIncident
- ChemicalIncident
- ChestPainIncident
- ChokingIncident
- CitizenAssistIncident
- CivilDisobedienceIncident
- CivilIncident

Figure 4-2. Snippet of the Class Hierarchy under CommonPublicSafetyIncident

Each of these classes is defined as a type of incident that conforms to the APCO standard and deals with a specific set of cases. So, for example, the BarricadeIncident class is defined as: *The APCO incident class pertaining to cases of barricaded individuals, including gunmen*, and the ChokingIncident is defined as: *The APCO incident class pertaining to cases of conditions characterized by severe difficulty in breathing, often caused by the presence of toxic fumes or the lack of oxygen*.

D. The BFO IntentionalAct Classes

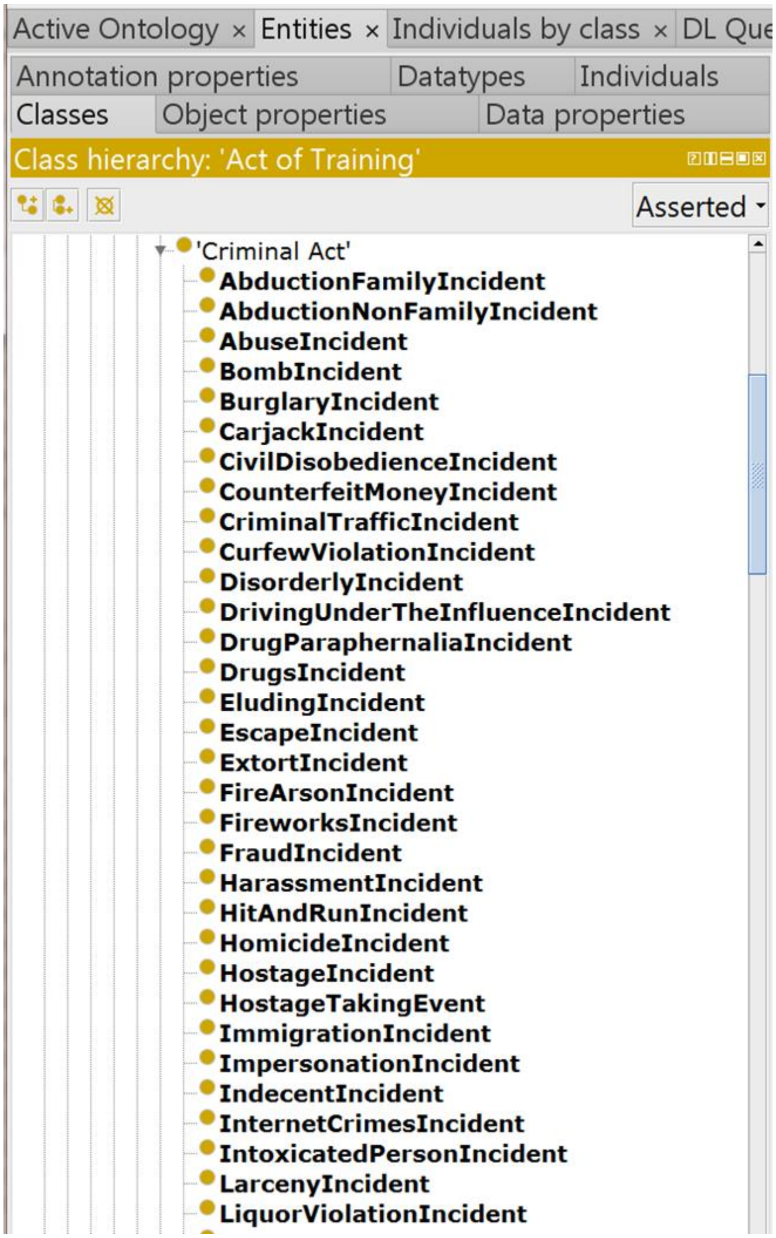
The BFO provides a rich characterization of types of process that specialize as some kind of Act, which in turn can be viewed as an IntentionalAct, defined as: *An Act in which at least one Agent plays a causative role and which is prescribed by some Directive Information Content Entity held by at least one of the Agents.* See Figure 4-3.



- continuant
- occurrent
  - process
    - Act
      - Behavior
      - 'Biographical Life'
      - **IncidentAct**
      - 'Intentional Act'
        - 'Act of Appraisal'
        - 'Act of Artifact Employment'
        - 'Act of Artifact Processing'
        - 'Act of Communication'
        - 'Act of Entertainment'
        - 'Act of Government'
        - 'Act of Inhabitancy'
        - 'Act of Intelligence Gathering'
        - 'Act of Military Force'
        - 'Act of Motion'
        - 'Act of Planning'
        - 'Act of Possession'
        - 'Act of Terrorism'
        - 'Act of Training'
        - 'Act of Violence'
        - 'Criminal Act'
        - 'Legal System Act'
        - 'Social Act'

Figure 4-3. The BFO Hierarchy for the Intentional Act Class

Many of the APCO incident classes deal with cases that are either criminal in nature or involve violence, as well as cases where individuals or equipment send messages indicating the presence of fire or some other hazardous condition. We therefore link the subclasses representing such intentional acts classified under the CommonPublicSafetyIncident class (see Figure 4-2) as subclasses of the IntentionalAct class (see Figure 4-3). Representative subclasses of one substantial category of such intentional acts are shown for Criminal Act in Figure 4-4. These acts are both intentional, in the sense that an actor deliberately commits a crime, and incidents, in that they may cause harm or require human action, which is the Public Safety Emergency Management Ontology's definition of an Incident. These two facts explain why the classes are subclasses of CriminalAct and have names suffixed with "Incident".

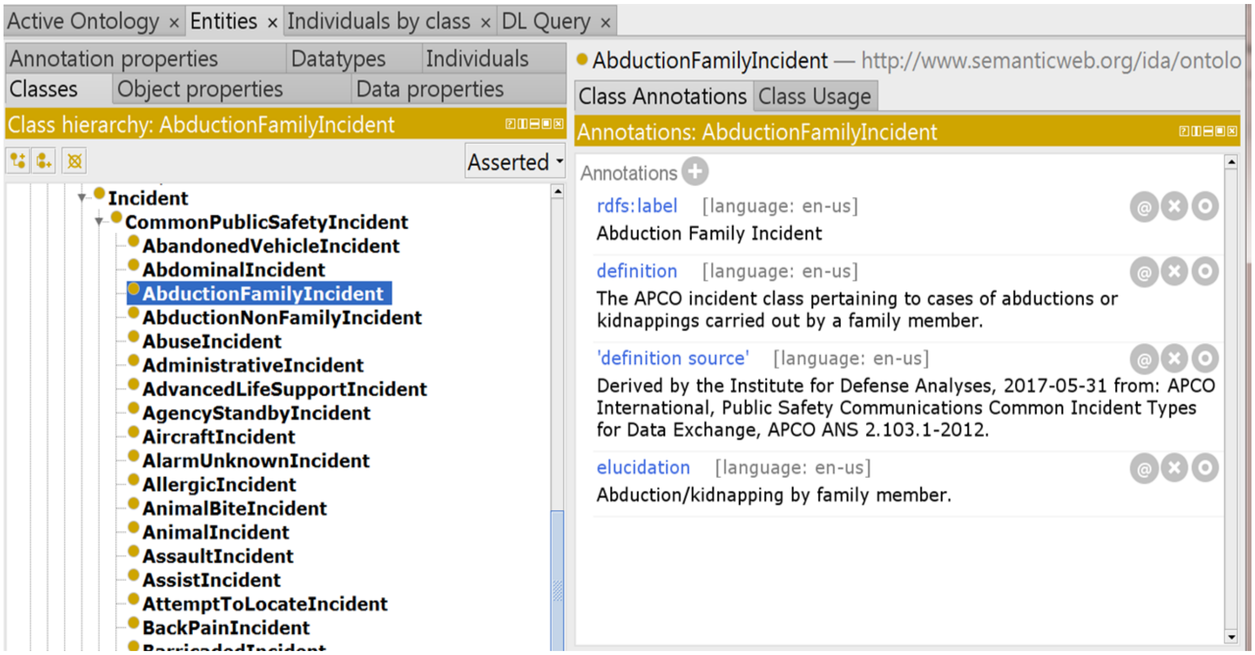


'Criminal Act'
AbductionFamilyIncident
AbductionNonFamilyIncident
AbuseIncident
BombIncident
BurglaryIncident
CarjackIncident
CivilDisobedienceIncident
CounterfeitMoneyIncident
CriminalTrafficIncident
CurfewViolationIncident
DisorderlyIncident
DrivingUnderTheInfluenceIncident
DrugParaphernaliaIncident
DrugsIncident
EludingIncident
EscapeIncident
ExtortIncident
FireArsonIncident
FireworksIncident
FraudIncident
HarassmentIncident
HitAndRunIncident
HomicideIncident
HostageIncident
HostageTakingEvent
ImmigrationIncident
ImpersonationIncident
IndecentIncident
InternetCrimesIncident
IntoxicatedPersonIncident
LarcenyIncident
LiquorViolationIncident

Figure 4-4. Modeling of APCO Incident Classes as Subclasses of Criminal Act

E. The Class Annotations

To retain the maximum degree of traceability of the new APCO incident classes with its source, each class contains four annotations: rdfs:label, definition, 'definition source', and elucidation (see Figure 4-5). The rdfs:label is used to capture a human-readable form of the class name. The definition indicates the subset of incidents that the class encompasses. The source of the definition is in most cases the APCO standard itself. Finally, the elucidation is the place where the original additional notes and examples are entered.



- Incident
  - CommonPublicSafetyIncident
    - AbandonedVehicleIncident
    - AbdominalIncident
    - AbductionFamilyIncident
    - AbductionNonFamilyIncident
    - AbuseIncident
    - AdministrativeIncident
    - AdvancedLifeSupportIncident
    - AgencyStandbyIncident
    - AircraftIncident
    - AlarmUnknownIncident
    - AllergicIncident
    - AnimalBiteIncident
    - AnimalIncident
    - AssaultIncident
    - AssistIncident
    - AttemptToLocateIncident
    - BackPainIncident
    - BarricadedIncident

rdfs:label [language: en-us]
Abduction Family Incident

definition [language: en-us]
The APCO incident class pertaining to cases of abductions or kidnappings carried out by a family member.

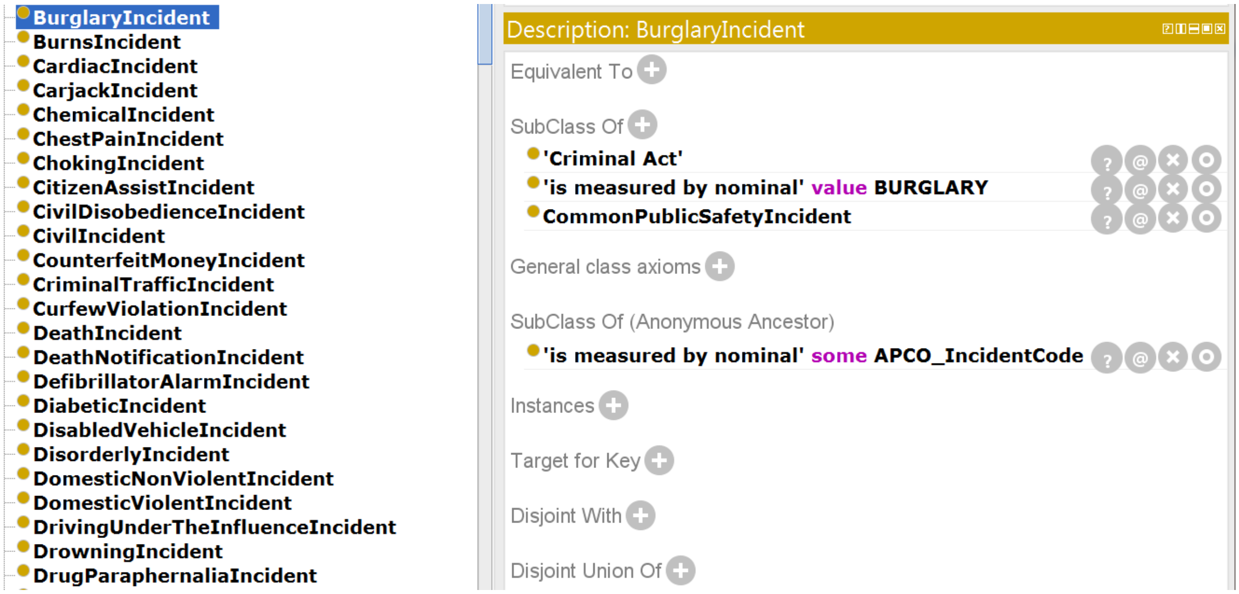
'definition source' [language: en-us]
Derived by the Institute for Defense Analyses, 2017-05-31 from: APCO International, Public Safety Communications Common Incident Types for Data Exchange, APCO ANS 2.103.1-2012.

elucidation [language: en-us]
Abduction/kidnapping by family member.

Figure 4-5. Annotations Defined for All APCO Incident Classes

F. The Modeling of the APCO Incident Codes Proper

Figure 4-6 and Figure 4-7 show the way in which the APCO codes themselves are modeled in the DoD First Responders Communications Ontology. Each of the 197 classes is made a subclass of the anonymous class defined by the object property ‘is measured by nominal’, which points to some APCO_IncidentCode individual (i.e., to the codes themselves). The class APCO_IncidentCode class is modeled as a subclass of Nominal Measurement Information Content Entity, under the Information Content Entity hierarchy in the BFO.



BurglaryIncident
BurnsIncident
CardiacIncident
CarjackIncident
ChemicalIncident
ChestPainIncident
ChokingIncident
CitizenAssistIncident
CivilDisobedienceIncident
CivilIncident
CounterfeitMoneyIncident
CriminalTrafficIncident
CurfewViolationIncident
DeathIncident
DeathNotificationIncident
DefibrillatorAlarmIncident
DiabeticIncident
DisabledVehicleIncident
DisorderlyIncident
DomesticNonViolentIncident
DomesticViolentIncident
DrivingUnderTheInfluenceIncident
DrowningIncident
DrugParaphernaliaIncident

Description: BurglaryIncident

Equivalent To

SubClass Of
- 'Criminal Act'
- 'is measured by nominal' value BURGLARY
- CommonPublicSafetyIncident

General class axioms

SubClass Of (Anonymous Ancestor)
- 'is measured by nominal' some APCO_IncidentCode

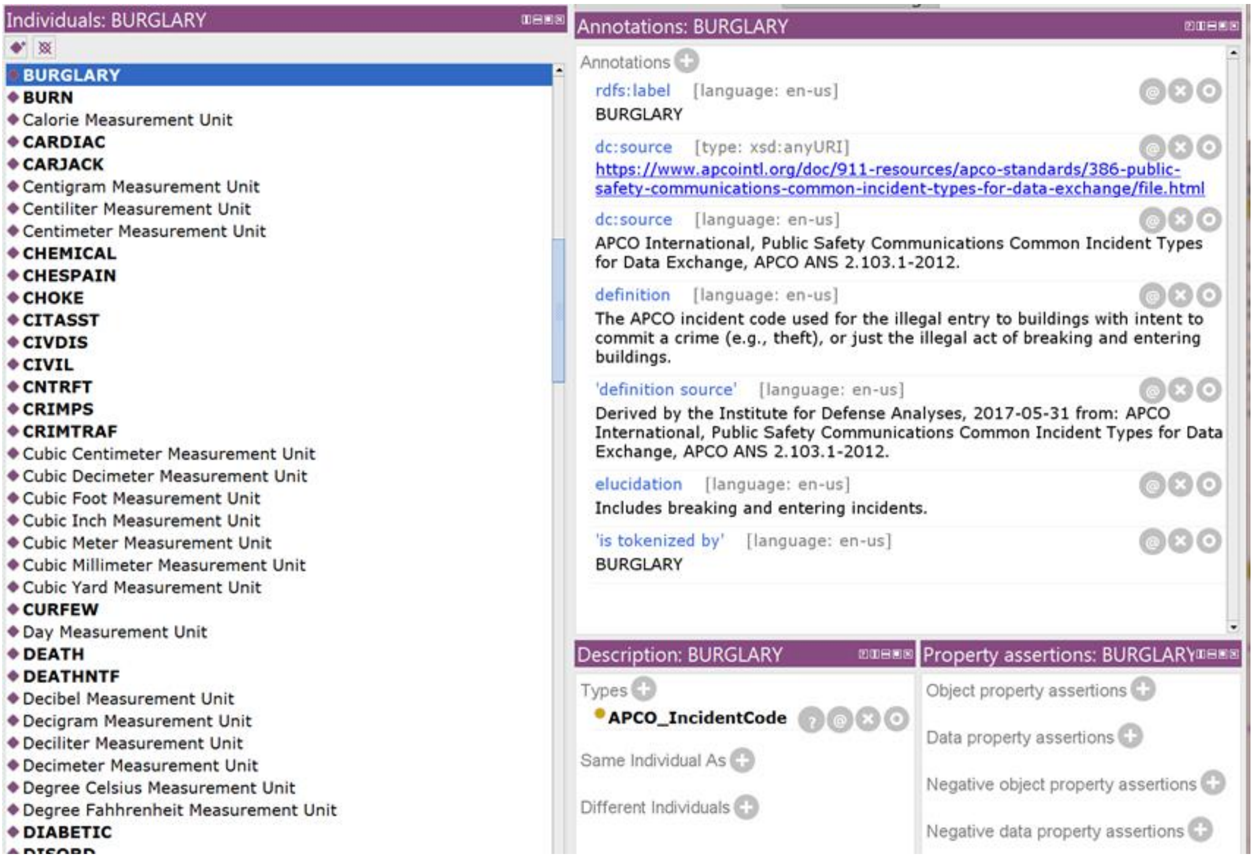
Instances

Target for Key

Disjoint With

Disjoint Union Of

Figure 4-6. Modeling of the APCO Codes Via Is Measured By Nominal



Individuals: BURGLARY

BURGLARY
BURN
Calorie Measurement Unit
CARDIAC
CARJACK
Centigram Measurement Unit
Centiliter Measurement Unit
Centimeter Measurement Unit
CHEMICAL
CHESPAIN
CHOKE
CITASST
CIVDIS
CIVIL
CNTRFT
CRIMPS
CRIMTRAF
Cubic Centimeter Measurement Unit
Cubic Decimeter Measurement Unit
Cubic Foot Measurement Unit
Cubic Inch Measurement Unit
Cubic Meter Measurement Unit
Cubic Millimeter Measurement Unit
Cubic Yard Measurement Unit
CURFEW
Day Measurement Unit
DEATH
DEATHNTF
Decibel Measurement Unit
Decigram Measurement Unit
Deciliter Measurement Unit
Decimeter Measurement Unit
Degree Celsius Measurement Unit
Degree Fahhrenheit Measurement Unit
DIABETIC

Annotations: BURGLARY

Annotations

rdfs:label [language: en-us]
BURGLARY

dc:source [type: xsd:anyURI]
https://www.apcointl.org/doc/911-resources/apco-standards/386-public-safety-communications-common-incident-types-for-data-exchange/file.html

dc:source [language: en-us]
APCO International, Public Safety Communications Common Incident Types for Data Exchange, APCO ANS 2.103.1-2012.

definition [language: en-us]
The APCO incident code used for the illegal entry to buildings with intent to commit a crime (e.g., theft), or just the illegal act of breaking and entering buildings.

'definition source' [language: en-us]
Derived by the Institute for Defense Analyses, 2017-05-31 from: APCO International, Public Safety Communications Common Incident Types for Data Exchange, APCO ANS 2.103.1-2012.

elucidation [language: en-us]
Includes breaking and entering incidents.

'is tokenized by' [language: en-us]
BURGLARY

Description: BURGLARY

Types
- APCO_IncidentCode

Same Individual As

Different Individuals

Property assertions: BURGLARY

Object property assertions

Data property assertions

Negative object property assertions

Negative data property assertions

Figure 4-7. Specification of the APCO Codes as Instances of APCO_IncidentCode

5. Keystone / UICDS Ontologies

Keystone is "a standards-based middleware that receives, translates, and transmits incident-related data between linked disparate systems to allow a common view between them."[24] Its purpose is to promote automated, near-real-time information sharing among force protection and emergency management applications. Keystone middleware intends to allow the integration of existing systems, requiring users to acquire neither new hardware nor software. Keystone aims to address the many stovepipe solutions that have been developed for transmitting emergency-related information and to overcome the consequent information-sharing problems.

Keystone is based on an older system, the Unified Incident Command and Decision Support System (UICDS).[25] UICDS is a network, each node of which is managed by a system known as a UICDS Core. A UICDS Core provides the infrastructure for communication with other Cores and application programming interfaces (APIs) that clients may use. These APIs are organized into 18 service categories, of which 8 address infrastructure—that is, they offer network- and system-related functions. The remaining 10 focus on emergency management services, including incident management, alerts, mapping, and resource management.

The IDA team conceptualized certain services and used the results as the basis for eight ontologies. The team emphasized the emergency management services, opting to view them as more in the project's scope, and studied the infrastructure services only insofar as was necessary to create well-defined models of emergency management services.

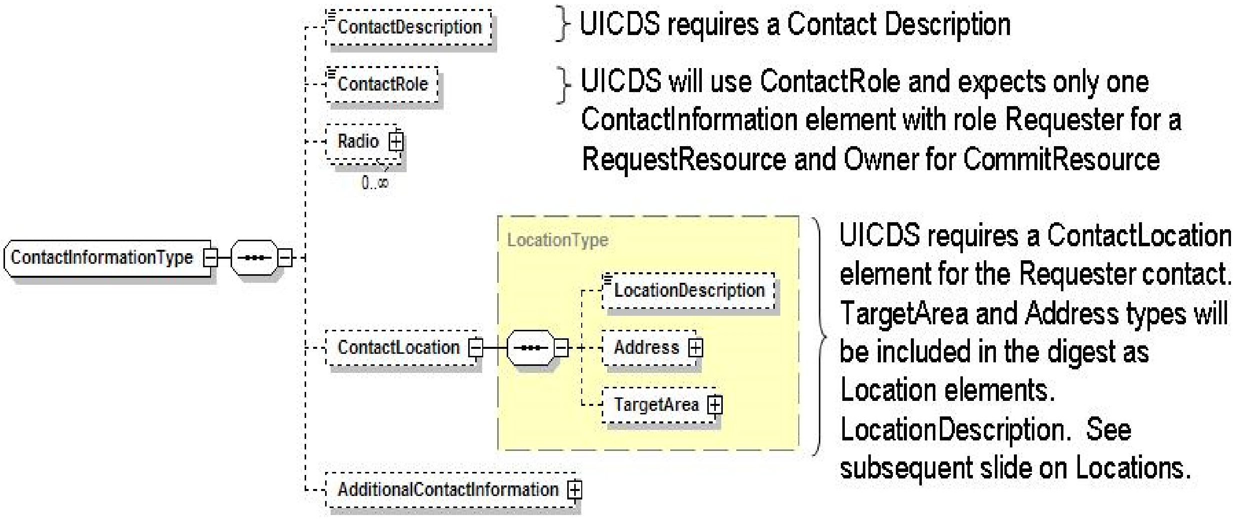
The IDA team received a package of the XML schemas used in Keystone exchanges. This package included XML schema graphical representations. These representations, which present top-level views of important data concepts, were used as the starting point for developing ontologies. The package's documentation included images of UML sequence diagrams; these diagrams describe events, their order, the actors involved, and the data transmitted. Information extracted from the sequence diagrams also was used in ontology development.

A. Contact Information

Contacts, which are used through UICDS, are defined in a schema that is part of the EDXL Resource Management specification. It has the structure shown in Figure 5-1:

[24] SSC Pacific, *EUCOM Keystone Product Reference Guide* Revision 1.0, September 2015, p. 2.

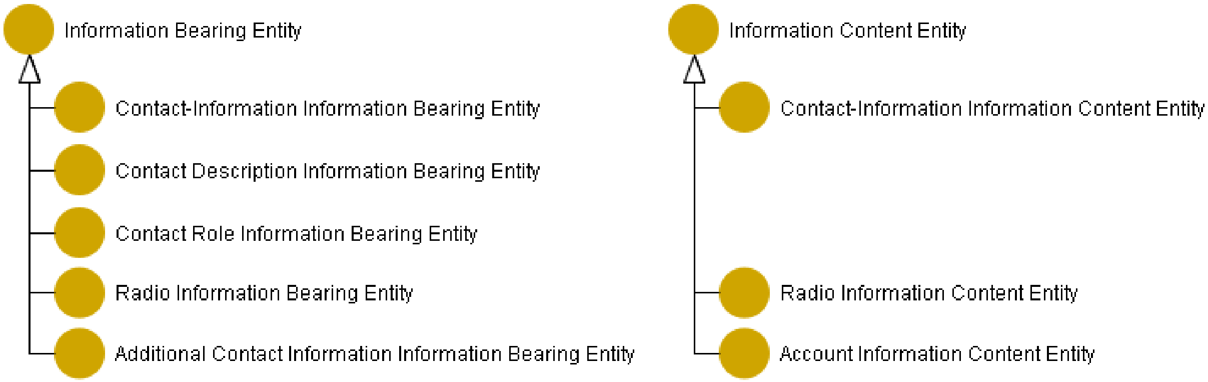
[25] SAIC, *Unified Incident Command and Decision Support* (*UICDS*) *Getting Started Guide*, September 2010.



ContactInformationType
ContactDescription
ContactRole
Radio
0..∞
LocationType
ContactLocation
LocationDescription
Address
TargetArea
AdditionalContactInformation
UICDS requires a Contact Description
UICDS will use ContactRole and expects only one ContactInformation element with role Requester for a RequestResource and Owner for CommitResource
UICDS requires a ContactLocation element for the Requester contact. TargetArea and Address types will be included in the digest as Location elements. LocationDescription. See subsequent slide on Locations.

Figure 5-1. UICDS Contact Information Schema

The Contact Concepts ontology derives five Information Bearing Entities and three Information Content Entities from this structure, shown in Figure 5-2. The ontology also conceptualizes location using the Location ontology, which is described below.



Information Bearing Entity
Contact-Information Information Bearing Entity
Contact Description Information Bearing Entity
Contact Role Information Bearing Entity
Radio Information Bearing Entity
Additional Contact Information Information Bearing Entity
Information Content Entity
Contact-Information Information Content Entity
Radio Information Content Entity
Account Information Content Entity

Figure 5-2. Contact Concepts: Information Bearing and Content Hierarchies

A ContactInformationInformationBearingEntity derives from ContactInformationType and comprises a full description of a contact. Other Information Bearing Entities form parts of information about a contact.

Horizontally aligned classes in Figure 5-2 indicate correspondences between Information Bearing Entities and Information Content Entities. A contact description, being simply text, has no corresponding information content; the text is expressed as a data property assertion on a

ContactDescriptionInformationBearingEntity individual using the has_text_value data property.[26] A role is expressed not as an Information Content Entity but as a role; an individual of class ContactInformationInformationBearingEntity may have an object property assertion with an individual of class ContactRole using property has_role.

Schema element AdditionalContactInformation has a complex datatype that includes many kinds of information. The Contact Concepts ontology currently models only account information.

B. Incident Management

Keystone provides services for creating, updating, querying, and deleting incidents. The Keystone XML schemas define a type, UICDSIncidentType, which is the basis of incident-management-related messages. It has the structure shown in Figure 5-3. The type mainly builds on NIEM's IncidentType, which in turn extends NIEM's ActivityType; UICDSIncidentType also adds three elements, SharedCoreName, IncidentActionPlan, and OwningCore.

The Incident Concepts ontology is derived from this structure. Message content describing an incident is expressed as an IncidentBearingEntity individual, which is a subclass of the Common Core ontology's InformationBearingEntity class. The Incident Concepts ontology defines an InformationBearingEntity subclass for each of the elements shown in Figure 5-3 that can be included in a UICDSIncidentType. The ontology asserts subclass restrictions for each of these Information Bearing Entity classes that ensure they are part of an IncidentBearingEntity. None of the elements are required (that Figure 5-3 shows otherwise contradicts the schema), so class InformationBearingEntity has no has_part restrictions.

The Incident Concepts ontology specifies that an IncidentBearingEntity is the bearer of an IncidentInformationContentEntity. The ontology defines InformationContentEntity subclasses corresponding to the other InformationBearingEntity subclasses it defines.

The Incident Concepts ontology conceptualizes an incident as a subclass of the BFO process class. An individual of class Incident is required to specify when it occurs and to specify the location at which it occurs. These two requirements derive from the inclusion of elements ActivityDate and IncidentLocation in UICDSIncidentType. Note that a specific incident-management message does not have to specify a date and location. In the real world, however, an incident always has a time and place.

[26] In this release of the ontologies, no attempt is made to glean semantics from text.

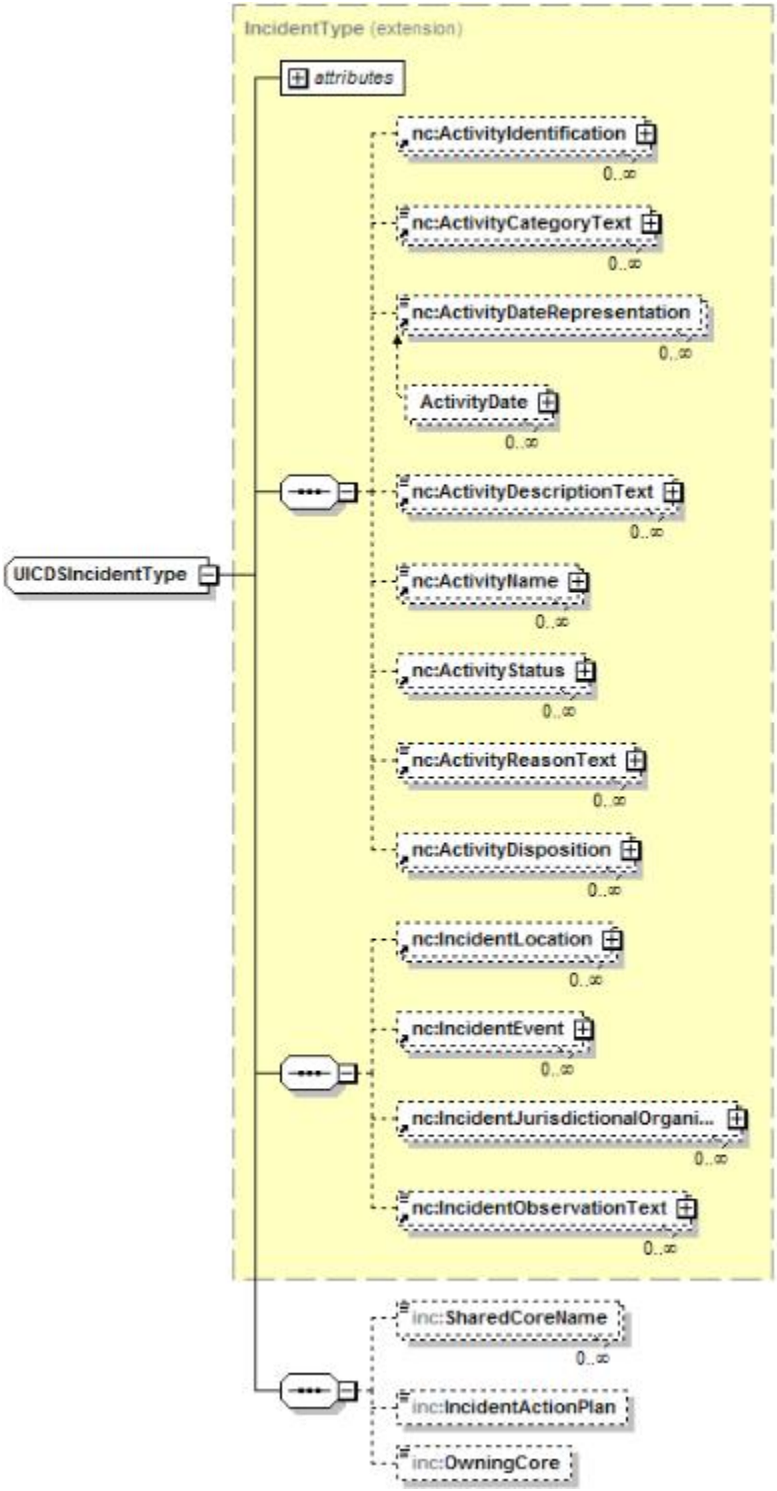


Figure 5-3. Incident Type Structure

C. Message Concepts

The Keystone documentation includes a high-level overview of how CAD applications create, update, close, and transmit incidents. This overview, shown in Figure 5-4, is not specific to any kind of incident or application. It just provides a view of information flows between resource consumers and suppliers. The overview divides messages into three categories, and shows the information flows and sequences pertinent to each category.

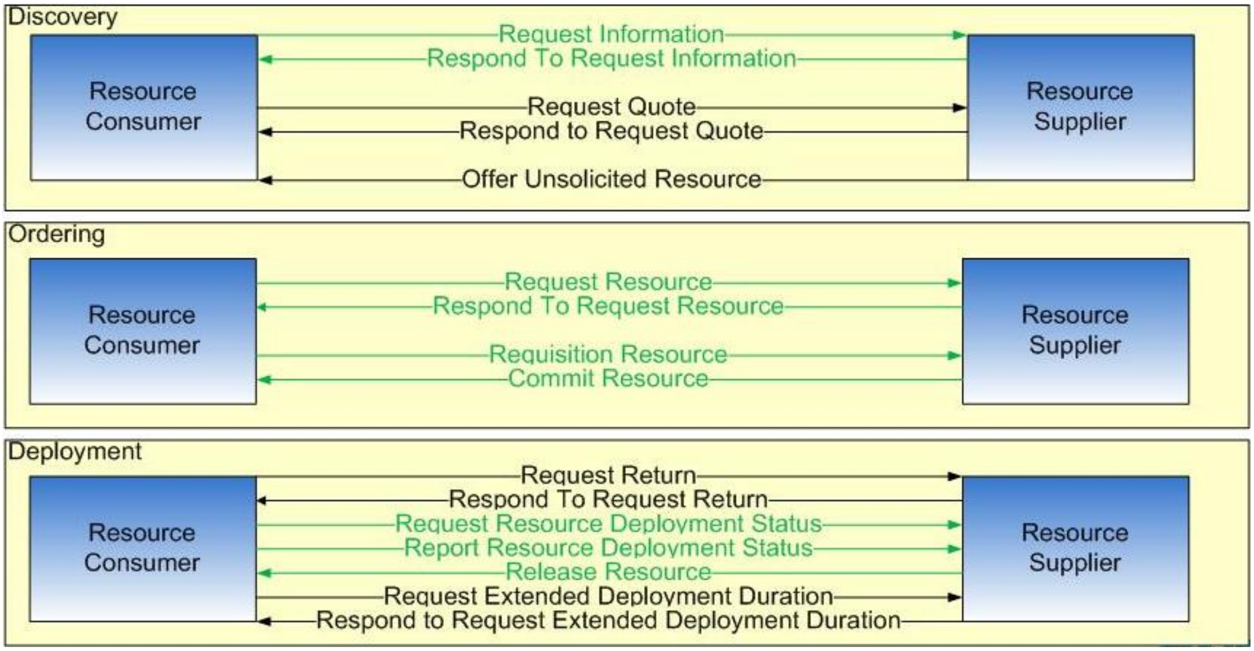


Figure 5-4. Resource Consumer/Supplier Message Exchanges

IDA developed the Message Concepts ontology to express these concepts. Unlike the other ontologies, the Message Concepts ontology places little emphasis on Information Bearing entities. It defines only one InformationBearingEntity subclass, MessageInformationBearingEntity, and three InformationContentEntity subclasses, DeploymentStatus, Quote, and ResourceIdentifier. The ontology instead emphasizes process-oriented classes, in particular, acts of communication. It extends the Common Core class hierarchy with class hierarchies for requesting resources and responding to requests. Figure 5-5 shows selected acts drawn from Figure 5-4 and expressed in the ontology. The ontology also defines classes for consumers and suppliers (subclasses of Agent) and for Resource (an independent continuant).

Classes Act of Requesting and Response are not at the same hierarchical level. An Act of Directive Communication expects the receiver to take some action; a response may be nothing more than an acknowledgment.

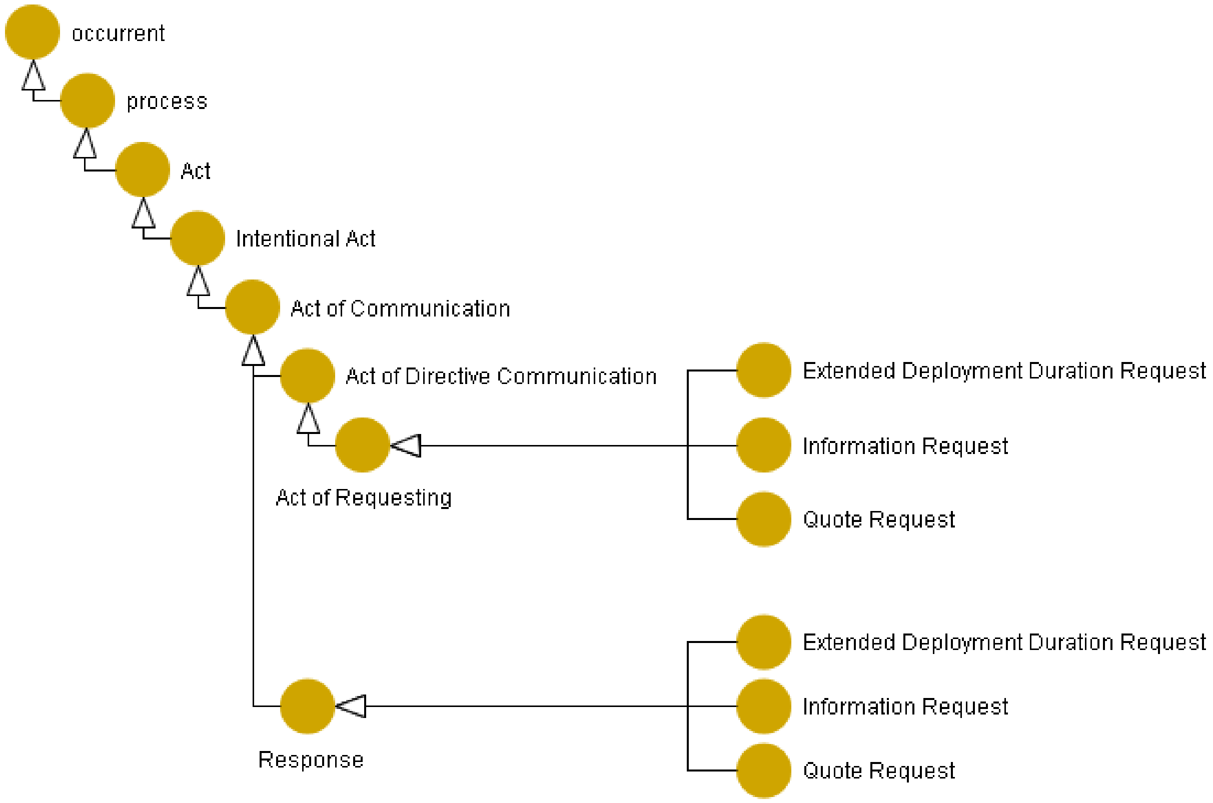


Figure 5-5. Request and Response Acts in Message Concepts Ontology (Partial)

D. Resources

Many Keystone messages are concerned with resource allocation: searching for resources, determining their availability, scheduling their use, and committing and releasing them. The Keystone XML schemas lay out the structure of resource-related information in detail. Figure 5-6 shows the top-level structure.

The Resource Concepts ontology expresses resource information in a message as an individual of class ResourceInformationInformationBearingEntity. In the XML schema, element ResourceInformation is information about a resource, including that resource as well as an identifier (of the resource information, not the resource), information on the assignment of the resource, and scheduling information. The Resource Concepts ontology has an analogous structure. An individual of type ResourceInformationInformationBearingEntity has an individual of type ResourceInformationBearing-Entity as a part, as well as individuals of type AssignmentInformation-InformationBearingEntity, ScheduleInformationInformationBearingEntity, and ResourceElementIdentifier-InformationBearingEntity.

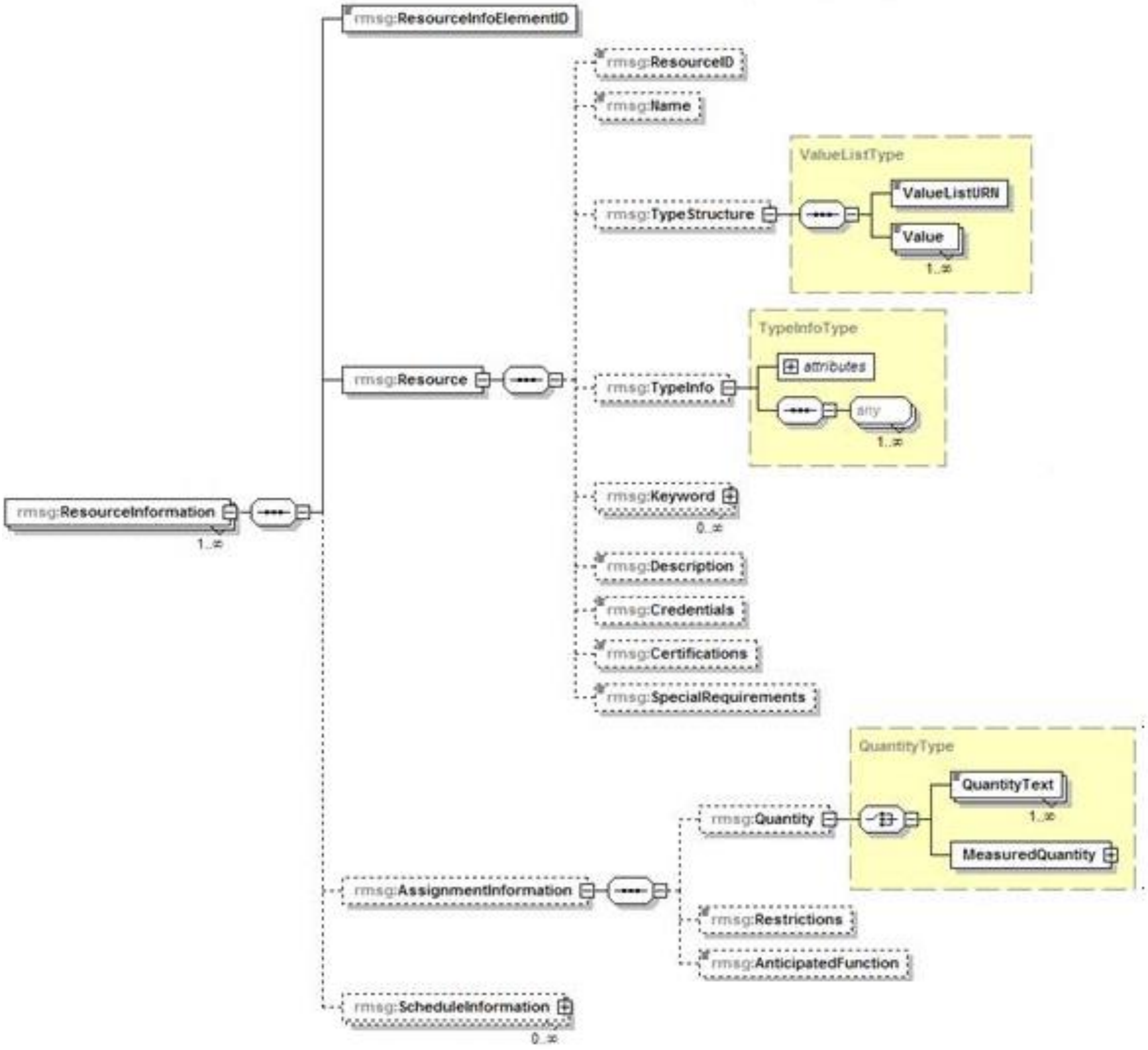


Figure 5-6. Resources

The Resource Concepts ontology declares corresponding Information Content Entity classes for the Information Bearing Entity classes. The ontology is able to use some specialized Information Content Entity subclasses, namely OrdinalMeasurementInformationContentEntity, which deals with ordinal measurements. Figure 5-6 shows that a quantity includes quantity text, which is a string representation of a number stating an ordinal quantity. In the ontology, this is expressed by stating that an individual of class QuantityTextInformationBearingEntity is the bearer of an individual of class QuantityICE. Class QuantityICE is a subclass of Common Core ontology class OrdinalMeasurementInformationContentEntity, which in turn, according to an assertion in the Common Core ontology, is an ordinal measurement of some entity.

E. Sensor Concepts

The Keystone software allows sensors to contribute information to incident messages. Figure 5-7 shows the structure of sensor-related components in a message. The information consists of the sensor identifier (a Uniform Resource Name [URN]), data from the sensor, and other information. The nature of other information is completely unspecified (as indicated by "##other") and cannot be further conceptualized. Sensor data themselves comprise a name, a description, and the sensor's geolocation. A SensorObservationInfo element must include all three of these components. Although the Keystone documentation does not say so, the name presumably identifies a type of data and the description presumably provides the reading.

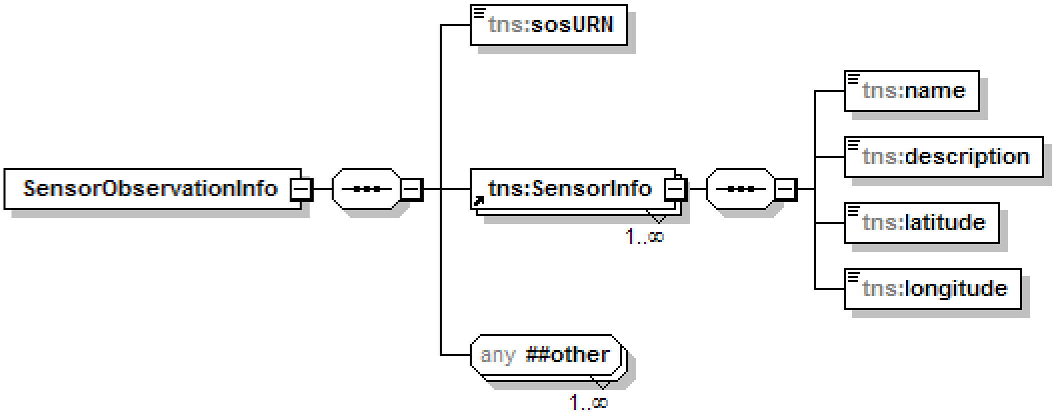


Figure 5-7. Sensor-Related Information

The Sensor Concepts ontology conceptualizes these items using class SensorInformationBearingEntity, a subclass of InformationBearingEntity, as the bearer of sensor-related information. Figure 5-8 shows these classes and the part-of relationships among them. Some further restrictions are imposed on these classes with respect to Information Content Entity classes:

- Sensor Information Bearer is the bearer of a Sensor Observation System Identifier, which is an Artifact Identifier.
- Sensor Name Bearer is the bearer of a designative name.
- Sensor Location Bearer is the bearer of a Spatial Region Identifier.
- Sensor Description Bearer is the bearer of some information content. The nature of this content is not further specified.

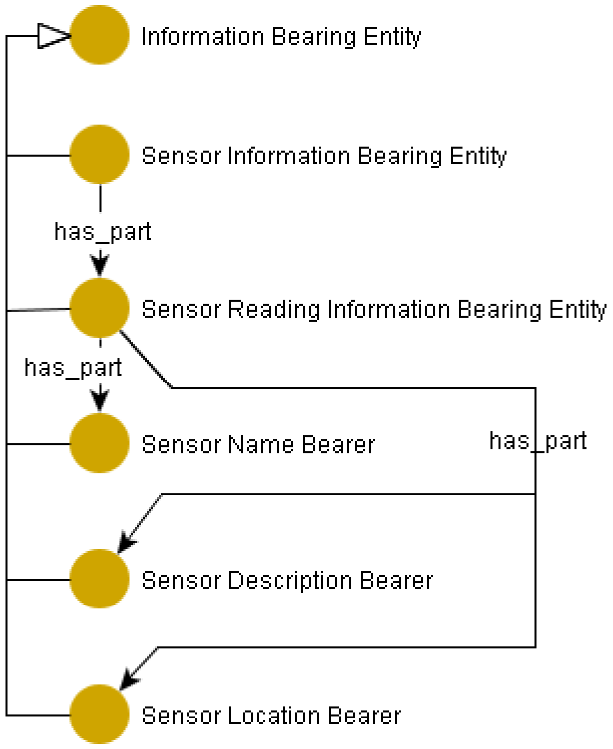

Information Bearing Entity
Sensor Information Bearing Entity
has_part
Sensor Reading Information Bearing Entity
has_part
Sensor Name Bearer
has_part
Sensor Description Bearer
Sensor Location Bearer

Figure 5-8. Sensor Information Bearing Entities

F. Tasks

The Keystone package includes tasking services. These services let a client create, query, update, and delete tasks related to a resource. Figure 5-9 shows task-related information. A task has an identifier, a textual description, a priority, a due date, and information on who it is assigned to, who assigned it, and its status.

The Task Concepts ontology has a collection of Information Bearing Entity subclasses linked by part_of subclass restrictions. These restrictions form a structure mirroring Figure 5-9. Most of the leaf-level classes (those not the target of a part_of subclass restriction) include a has_text_value restriction. The classes expressing priority and due date (TaskPriorityBearer and TaskDueDateBearer, respectively) instead assert has_decimal_value and has_dateTime_value.

The Information Content Entity subclasses borne by these classes generally have subclass restrictions specializing the general restriction that an Information Content Entity is about some Entity. For example:

- Class Task Bearing Entity is the bearer of class Task, which prescribes some Intentional Act.
- Class Task Priority Bearer is the bearer of some Information Content Entity that has a Priority as a quality.

- Classes Assignee Identity Bearer and Assignment Identity Bearer both are bearers of an Agent Identifier, which designates some Agent.

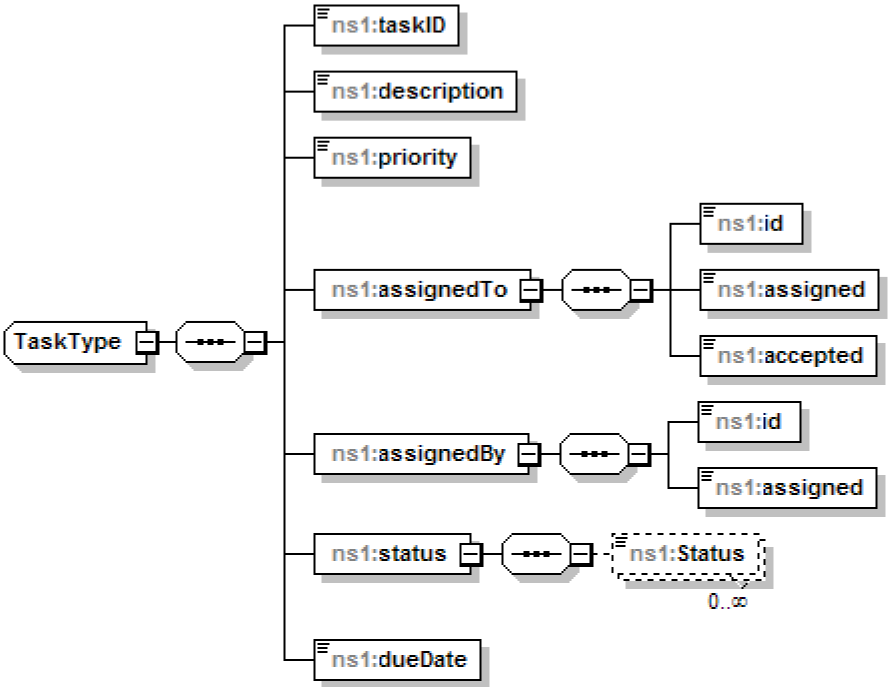


Figure 5-9. Tasks in Keystone

G. Sequence Diagram Concepts

The Keystone package includes four sequence diagrams that describe information flows involving CAD systems and UICDS middleware. Figure 5-10 shows an example. These diagrams do not describe data in detail; information in these diagrams, such as incidents and resources, has been described elsewhere. The sequence diagrams do, however, identify material entities that participate in message exchanges. The diagrams present a system-level view, rather than an operational-level view, as they depict CAD systems but not the users of those systems. They are particularly useful for tying together other ontologies.

The Sequence Diagram Concepts (SDC) ontology does not focus on Information Bearing Entity classes. The SDC ontology conceptualizes things that make use of information-bearing entities. It does define a Message as an InformationBearingEntity subclass: every arrow in a sequence diagram represents a message. The SDC ontology also conceptualizes a Map, which appears in several sequence diagrams, as an Information Bearing Entity.

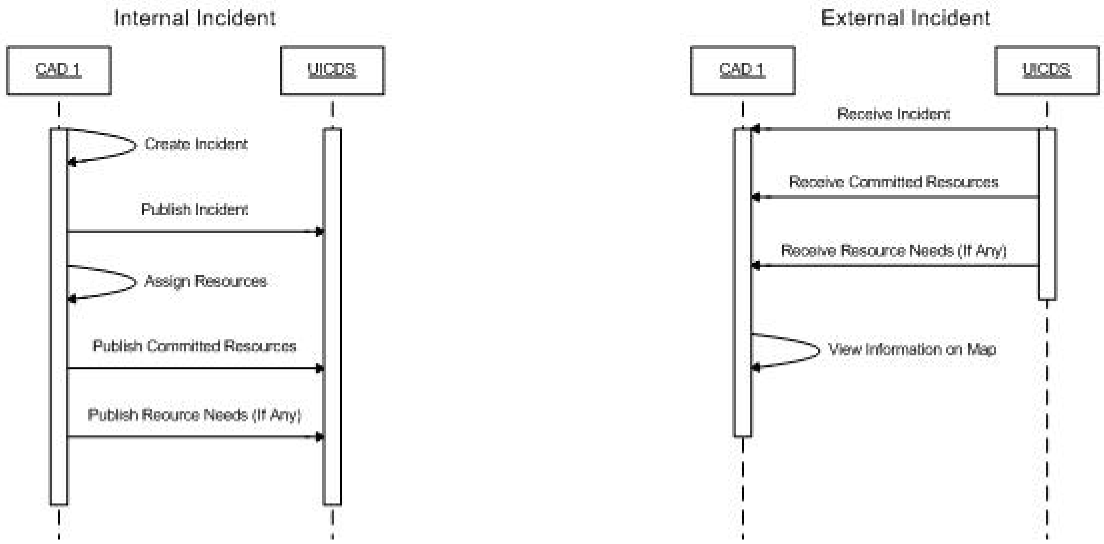


Figure 5-10. Example Sequence Diagram

The Sequence Diagram Concepts ontology conceptualizes:

- Artifacts, namely CAD systems and UICDS middleware systems.
- Events, where an event derives from an arrow in a sequence diagram and is associated in some way with the concept derived from the arrow's label.
- Incidents and Resources

It would be useful to specify temporal constraints among events—to state, for example, that creating an incident must occur before publishing an incident. Unfortunately, expressing such constraints as OWL subclass restrictions is not practical. The relationship between individuals of classes CreateIncident and PublishIncident might be expressed as the following restriction on PublishIncident:

ero:occurs_on **some** (time:interval_is_after **some** (ero:is_temporal_region_of **some** CreateIncident))

This restriction states that publishing an incident occurs during a time span (a temporal region) that is after some other time span corresponding to creating an incident. OWL, however, cannot require that the two events refer to the same incident.

Still, many useful subclass restrictions can be applied to events from the sequence diagrams. Class PublishIncident has the following restrictions:

- An individual must have a sender and a recipient.
- A CAD system and a UICDS system participate in publishing an incident.
- The CAD system is located at the place where the publication act occurs.
- Publishing an incident requires as input a message that is about an incident ("Incident" being a class conceptualized in the Sequence Diagram Concepts ontology).

6. Summary

The ontologies described herein provide a foundation for semantic interoperability amongst diverse PS/EM communication systems using different types of information-sharing standards. Semantic interoperability requires the use of a common semantics (i.e., meaning) for the terminology used in information shared among interoperating systems. An ontology captures terminology in a formalism reducible to a logic that expresses logical relationships among the various concepts. Furthermore, ontologies enable a degree of machine "understanding" sufficient to standardize the derivation of implicit information from the explicit information of information exchanges. Utilizing a common ontology across interoperating systems helps ensure that all parties share the same extent of such derived information. That is, the ontology supports common understanding of shared information by humans and machines alike and facilitates automated reasoning with that information. This document describes initial work addressing this issue of improving semantic interoperability across the PS/EM communications enterprise.

Acronyms and Abbreviations

ANSI	American National Standards Institute
APAN	All Partners Access Network
APCO	Association for Public-Safety Communications Officials
BFO	Basic Formal Ontology
C4&IIC	Command, Control, Communications, and Computers and Information Infrastructure Capabilities
CAD	Computer Aided Dispatch
CAP	Common Alerting Protocol
CCO	Common Core Ontologies
CIO	Chief Information Officer
DCIO	Deputy Chief Information Officer
DHS	Department of Homeland Security
DoD	Department of Defense
EDXL	Emergency Data Exchange Language
EDXL-CAP	Emergency Data Exchange Language-Common Alerting Protocol
EDXL-DE	Emergency Data Exchange Language-Distribution Element
EDXL-HAVE	Emergency Data Exchange Language-Hospital AVailability Exchange
EDXL-RM	Emergency Data Exchange Language-Resource Messaging
EIDD	Emergency Incident Data Document
EM	Emergency Management
EMS	Emergency Medical Services
EOC	Emergency Operations Center
HADR	Humanitarian Assistance and Disaster relief
IBE	Information Bearing Entity
ICE	Information Concept Entity
IDA	Institute for Defense Analyses
IP	Internet Protocol
NENA	National Emergency Number Association
NG9-1-1	Next Generation 9-1-1
NIEM	National Information Exchange Model
OASIS	Organization for the Advancement of Structured Information Standards
OWL	Web Ontology Language
PM-ISE	Program Manager – Information Sharing Environment
PS/EM	Public Safety and Emergency Management
PSAP	Public Safety Answering Point
SDC	Sequence Diagram Concepts
UICDS	Unified Incident Command and Decision Support System
URL	Uniform Resource Locator

URN	Uniform Resource Name
US	United States
XML	eXtensible Markup Language
XSD	XML Schema Definition

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number**. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YY)
20-06-17

2. REPORT TYPE
Final

3. DATES COVERED (From – To)

4. TITLE AND SUBTITLE
Public Safety and Emergency Management Communications Ontology

5a. CONTRACT NUMBER
HQ0034-14-D-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)
Serena Chan, Brian A. Haugh, Francisco L. Loaiza-Lemos, Steven P. Wartik

5d. PROJECT NUMBER
ET-5-4155

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES
Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311-1882

8. PERFORMING ORGANIZATION REPORT NUMBER
D-8583

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Joseph M. Wassel
Director, C4 Resilience & Mission Assurance
DoD CIO 6000 Defense Pentagon, Arlington, VA 20301

10. SPONSOR'S / MONITOR'S ACRONYM
DoD CIO

11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
Project Leader: Serena Chan

14. ABSTRACT

This document reports on work done by the Institute for Defense Analyses (IDA) for the Office of the Program Manager, Information Sharing Environment (PM-ISE), Office of the Director of National Intelligence and Deputy Chief Information Officer (DCIO) for Command, Control, Communications, and Computers and Information Infrastructure Capabilities (C4&IIC), Department of Defense (DoD) Chief Information Officer (CIO). The objective of this project is to assess the current state of communications interoperability between DoD public safety and emergency management (PS/EM) entities and U.S. civilian PS/EM entities and how that is likely to change as the next generation of public safety information systems is implemented across the nation. This white paper address the development of a formal semantic information model (ontology) for PS/EM information products.

15. SUBJECT TERMS
Public safety and emergency management communications; ontology; semantic information model

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Joseph M. Wassel
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified	Unlimited	68	19b. TELEPHONE NUMBER (Include Area Code) 703-901-7360