Technical Guide: Incident Management Technology

Guidance on Incident Management Information Sharing Standards

November 2021

National Alliance for Public Safety GIS (NAPSG) Foundation
5335 Wisconsin Ave., NW | Suite 440 | Washington, DC 20015

Table of Contents

Table of Figures

I. Overview

A variety of technologies and products are available for use by the public safety community in supporting incident management and mutual aid. These tools, systems, and products – hereinafter referred to as incident management technology – can support any one or more of the following functions:

- Resource or Asset Inventorying
- Personnel Qualifications and Credentialing
- Deployment Management
- Incident or Crisis Management
- Mutual Aid Operations
- Situational Awareness and Decision Support

The public safety community continues to experience challenges carrying out the functions identified above, not because of a lack of technology, but due to the insufficient use of interoperability and information exchange standards between systems. This issue is often a principal reason why technology often fails to meet the needs of the public safety community. Information that can be shared directly between systems improves reliability, accountability, speed, and accuracy. Phone calls, radio calls, email, and other methods of communication that involve human intervention can slow the flow of information and introduce human errors, including mistranscription, misinterpretation, and delay. During an incident, speed is life. The speed by which accurate information is available to Leaders and Managers directly influences the outcomes of events.

Information shared between systems using common data standards are less prone to these errors and can speed up the flow of information, since modern technology enables near real-time information sharing. Accurate, reliable, and timely information is critical to the public safety community.

The goal of this technical guide is to equip technologists and vendors with the requisite knowledge to aid in the development of incident management technologies and to ensure that information sharing requirements and standards are included in the development and implementation.

II. Recommended Standards

The Standards Review and Assessment involved a comprehensive research activity on relevant standards for incident management and mutual aid requirements and was carried out by the National Alliance for Public Safety GIS (NAPSG) Foundation. This review identified a variety of standards from the Organization for the Advancement of Structured Information Standards (OASIS) Emergency Data Exchange Language (EDXL) suite of standards that are directly applicable to the core functions listed in section 1.0. These include:

Standard	Authoritative Information
Common Alerting Protocol (CAP) - OASIS	https://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.html
Hospital Availability Exchange (HAVE v2) - OASIS and HL7®	https://docs.oasis-open.org/emergency/edxl-have/v2.0/edxl-have-v2.0.html
Distribution Element (DE) - OASIS	https://docs.oasis-open.org/emergency/edxl-de/v2.0/edxl-de-v2.0.html
Resource Messaging (RM) - OASIS	https://docs.oasis-open.org/emergency/edxl-rm/v1.0/EDXL-RM-SPEC-V1.0.html
Situation Report (SitRep) - OASIS	https://docs.oasis-open.org/emergency/edxl-sitrep/v1.0/edxl-sitrep-v1.0.html
Tracking Emergency Patients (TEP) - OASIS	https://docs.oasis-open.org/emergency/edxl-tep/v1.1/edxl-tep-v1.1.html
Emergency Management Loose Coupler - National Information Exchange Model (NIEM)	NIEM EM - https://www.niem.gov/communities/emergency-management NIEM Releases - https://niem.github.io/niem-releases/

Figure 1 - Suite of Standards in document

The standards listed above are focused on information exchange for different types of emergency management systems that support incident management and mutual aid functions. It is recommended that most technology tools or products for this mission would need to implement multiple standards to cover the breadth of information to be shared.

This document serves as a simple guide to choosing the appropriate information sharing standard for a given need. The primary audience is public safety Leaders and Managers, to help them determine the best options for their needs and properly communicate those

requirements to technology vendors. The secondary audience is technologists and vendors, to help guide implementation and provide technical guidance.

Adoption and use of the standards listed above is typically on a voluntary basis, and most used when prompted or required by the customer – the public safety community. This is where a paradigm shift needs to occur by the technology providers and vendors, where they design solutions based on the inherent interoperability and information sharing needs of the public safety community first and foremost.

III. Use Case Scenario

This document has walked through various recommended standards. The next step is to progress through a "real life" emergency scenario to show how these implementations could improve and enhance the way data is shared in the field. The premise of this scenario is a large-scale traffic accident involving multiple injuries, fatalities, vehicle fires, hazardous material leakage, and multi-jurisdiction response. This scenario highlights how each of the identified standards could be used to improve situational awareness and response.

3.1 Set-Up

A large winter storm is impacting a small Midwest town with blizzard conditions and reported power outages. A regional Emergency Operations Center (EOC) has been activated to monitor and respond to the changing weather conditions. Emergency operations plans are in place to deal with the situation. Reports of a multi-vehicle pileup on the interstate are starting to trickle in. Response to the incident will be coordinated through the EOC.

3.2 Available Data

The EOC situational awareness system is already receiving Hospital AVailability Exchange Reports (HAVE reports) from the regions' hospitals. This information includes bed status, emergency services status, and EMS services status. Additionally, the EOC is receiving real-time local agency Computer-Assisted Dispatch (CAD) information about active incidents, unit status, and unit locations via the National Information Exchange Module Emergency Management Loose Coupler (NIEM EMLC) reports. Blizzard warnings and alerts (EDXL CAP) are being received from the Federal Emergency Management Agency (FEMA) Integrated Public Alert and Warning System (IPAWS) as the National Weather Service updates them.

3.3 Missing/Future Data

In this situation, and in addition to the HAVE reports, a new type of report dealing with the electric grid would be useful. This information would include facility ID, overall capacity, status, and expected issue correction estimates.

A new type of report dealing with Department of Transportation (DOT) road information would also be useful in the situation. This information should include things like road ID, road status, and expected future status.

3.4 Incident Field Data

During the incident, field reports, like Emergency Data Exchange Language Situation Reports (EDXL SitRep), can be generated from boots on the ground to indicate any immediate needs and initial observations from the scene. This information could also be generated by personnel in the EOC or dispatch centers from radio reports in the field.

Converting this information to Situation Reports (SitRep) allows the information to be shared more easily across systems.

3.5 Mutual Aid Requests

As the incident escalates, both automatic and longer-term mutual aid requests can be made to nearby jurisdictions using EDXL Resource Management (RM). The automatic request would include unit availability, unit capabilities, unit type, and estimated departure/arrival information. The long-term aid would most likely include costing information as well as the previously identified fields.

3.6 Context Diagram

Figure 2 illustrates what data could be provided by what system and in what format. It is intended to highlight what could be possible when the right standards are used. It illustrates how the various standards apply to different types and levels of incident management technology and workflows. These range from field-based applications to Emergency Communication Centers, mass notification systems, and EOCs.

The communication methods Hypertext Transfer Protocol (HTTP) or Message Queuing Telemetry Transport (MQTT) will be system dependent and are not displayed. Additional details about communication methods are provided in Section VI.

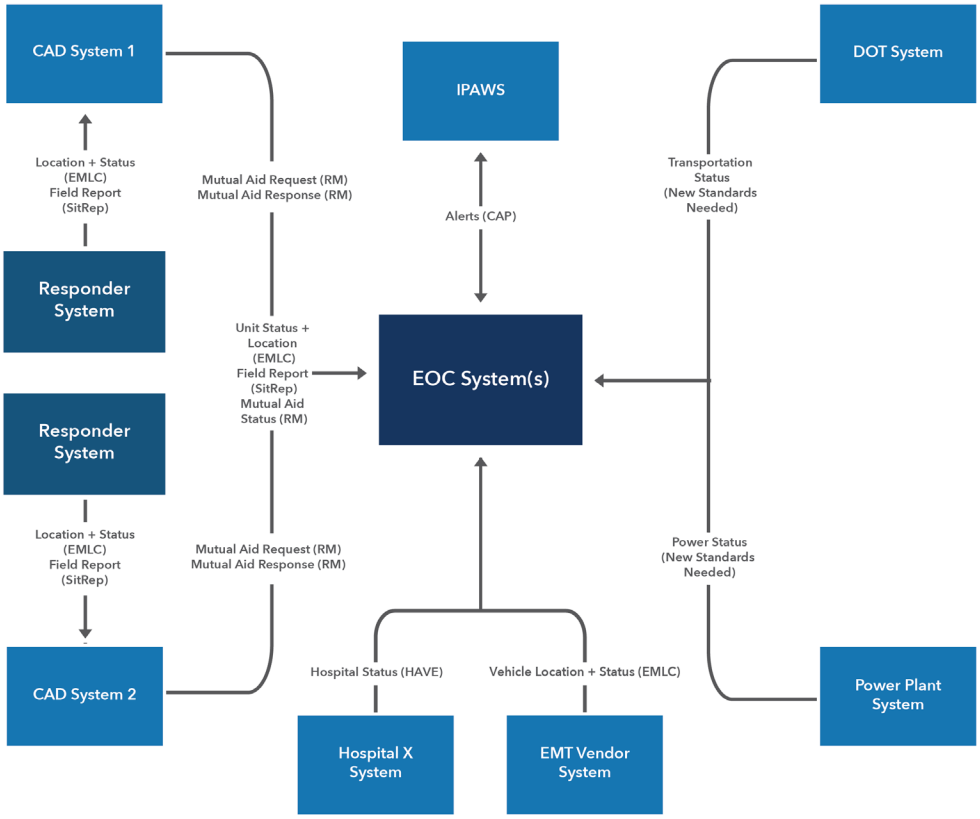


Figure 2 - Context Diagram for Use Case Scenario

IV. Implementing the Standards to Incident Management Technology

The standards described in this document will help public safety Leaders and Managers understand the basic information within relevant standards and how they can help in the product selection and adoption process. Figure 3 illustrates the sequence of decision and implementation processes.

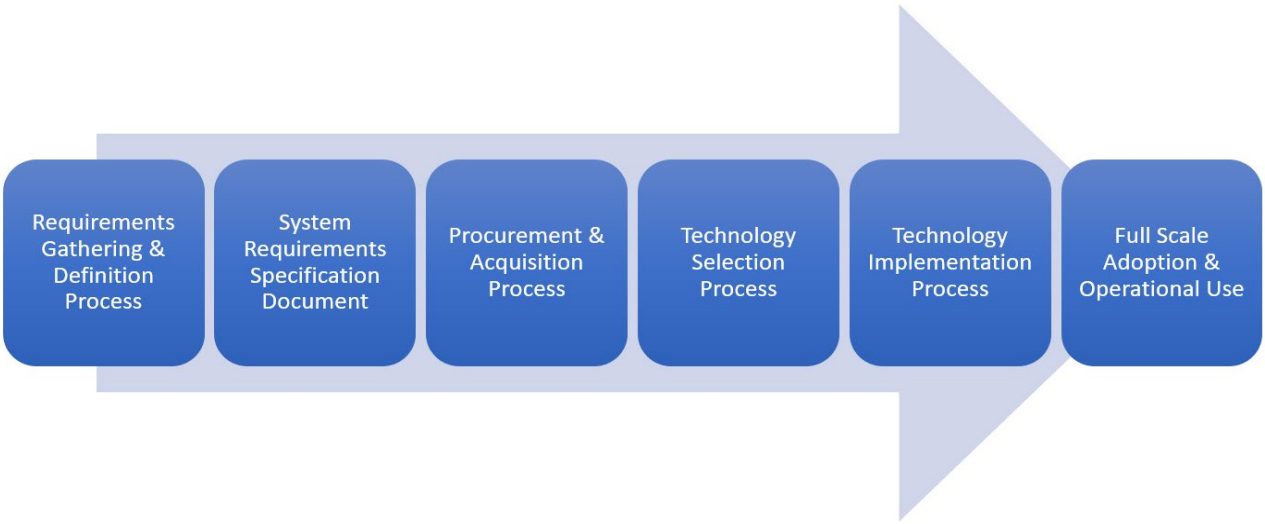


Figure 3 - Technology Decision and Implementation Process

To improve interoperability and information sharing across agencies and organizations for incident management, public safety Leaders and Managers need to require that their technology vendors and providers implement appropriate information sharing standards.

An appendix is provided with technical details and samples of what application programming interfaces (APIs) and architectures might look like to provide additional technical insight. Leaders and Managers can share this document, and the detailed appendices, with their Information Technology (IT) staff and technology vendors and providers.

4.1 Why Are Information Sharing Standards Important?

When looking to implement a new software for emergency management use, it is important for agencies to focus on the high-level requirement areas for a system so that the software purchased is of greater value for a longer period. For instance, the agency needs to ensure that the software, application, or product they are purchasing is built to the appropriate interoperability standard. Leaders and Managers cannot assume that interoperability is inherent in the products being promoted by technology providers and vendors.

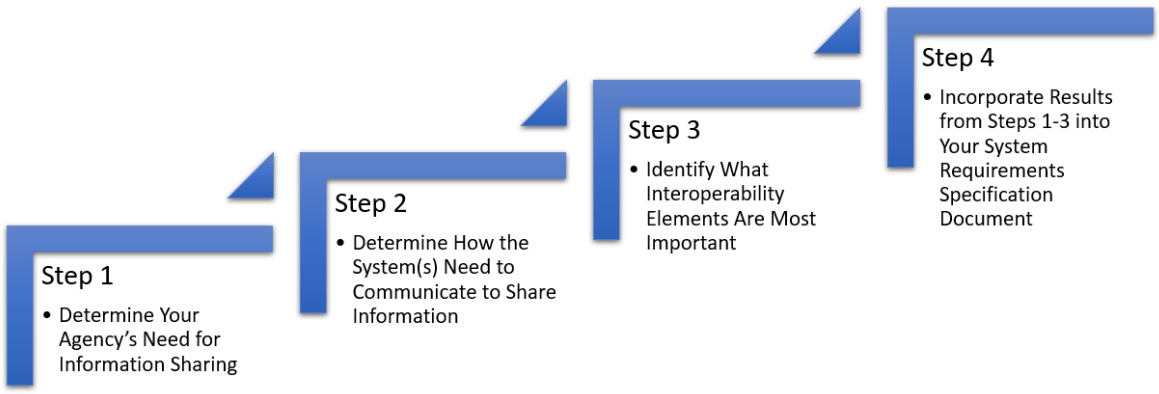
Ensuring interoperability increases the longevity of the technology investment and overall sustainability. Since standards do not change frequently, upgraded software and technology does not need to be purchased as often. While user interface and functionality requirements are important, the underlying data, how it is managed and shared, provide the true longevity of any system. Achieving effective incident management and mutual aid relies on the following:

- Use of standards within the technology system or product,
- Technical communication between systems, and
- Consistent use of the system and decision support products by the community.

Standards provide an agreed upon data format that knowledgeable groups have vetted through a series of community-involved reviews and can allow systems to speak easily to one another. By reducing the need for extensive customization, typically offered as an expensive add-on, the overall costs should be reduced, and interoperability should improve.

Further, it is important to consider the use of open standards that are widely available at no cost to the community. Open standards for technology and data exchange are more readily accessible and are therefore easier for the technology/vendor community to adopt. The standards referenced in this document are all open standards that are publicly available at no cost.

Illustrated below in Figure 4, are the four steps in assessing information sharing needs and requirements, which are critical in implementing incident management technology that is scalable, flexible, and interoperable.



STEP 1 – DETERMINE YOUR AGENCY'S NEED FOR INFORMATION SHARING

The decision maker should ask questions about their system needs, such as:

- What are we trying to share and why?
- With whom are we trying to share data?
- What are the major elements of the data that we need to share (e.g., incident info, resource info, patient info, etc.)?

Once these answers are identified, the decision maker can then run through the workflow provided in Figure 6 of this guide to identify the best standards to cover their needs. As noted, there is no one-stop-shop standard, so multiple standards likely apply. Leaders and Managers should also ensure they share information in compliance with their respective policies and legal parameters.

Example: Our agency is trying to share field observations and field reports with neighboring jurisdictions providing mutual aid to ensure situational awareness and prevent duplication of effort in response. Major data elements include incident information, resource information, incident stabilization efforts, and damage assessment reports.

STEP 2 – DETERMINE HOW THE SYSTEM(S) NEED TO COMMUNICATE TO SHARE INFORMATION

Once standards are identified, the decision maker can then turn their attention to the aspect of communication for their system. As noted above, communication, when identified as the way systems "speak" to one another, can also limit the amount of customization or cost associated with procuring a system. If the decision maker identifies a specific communication system that neighboring jurisdictions use, and that system utilizes Open Data Standards, it may be in their

best interest to shop for that same style of communication to ensure interoperability. The decision maker can also work with their technical staff to use the communications workflow included in the accompanying Technical Guide to determine the best communication choice for their software.

STEP 3 – IDENTIFY WHAT INTEROPERABILITY ELEMENTS ARE MOST IMPORTANT

After running through these activities, the decision maker should be able to identify the types of interoperable elements most important to their system and can request that of technology providers and vendors. If the proper system or tool does not currently exist, the demand by decision makers – as the purchasers - should eventually create a market for vendors to meet the demand. Gone will be the days where systems are stove piped by proprietary development and expensive support; a national (and global) ecosystem of strong software choices that increase interoperability will be created. Example interoperability elements include:

- Location format (latitude/longitude, USNG, etc.)
- File format or type
- Unique identifiers

STEP 4 – INCORPORATE RESULTS FROM STEPS 1-3 INTO YOUR SYSTEM REQUIREMENTS SPECIFICATION DOCUMENT

The findings and results from the requirements gathering and definition process will establish a strong foundation for the procurement and acquisition. Sound technology procurement and acquisition practices rely upon clear and comprehensive requirements and specifications that are developed and provided by the decision maker as the purchaser. This ensures that the decision maker clearly conveys to technology providers and vendors what their explicit needs are. By incorporating the inputs from Steps 1-3 in an agency's technology specifications or system requirements specification (SRS) document, the decision maker ensures that technology providers and vendors know up front what standards they must implement and comply with to ensure scalability, flexibility, and ultimately interoperability.

V. Standards Workflows

The following section describes the decision workflow for choosing the appropriate standard based on need. The intent is to aid in the selection of which standards should be used based on what information needs to be shared.

The workflow in Figure 5 is split into two branches based on the type of information needed to be shared.

- Situational Awareness
- Resource Management

The alignment of standards for each is based on the results from the standards review and assessment process that NAPSG Foundation carried out as part of the development of this document. The Situational Awareness branch of the workflow aligns itself to the Situational Awareness Requirements, while the Resource Management branch aligns itself to the Resource Management Requirements.

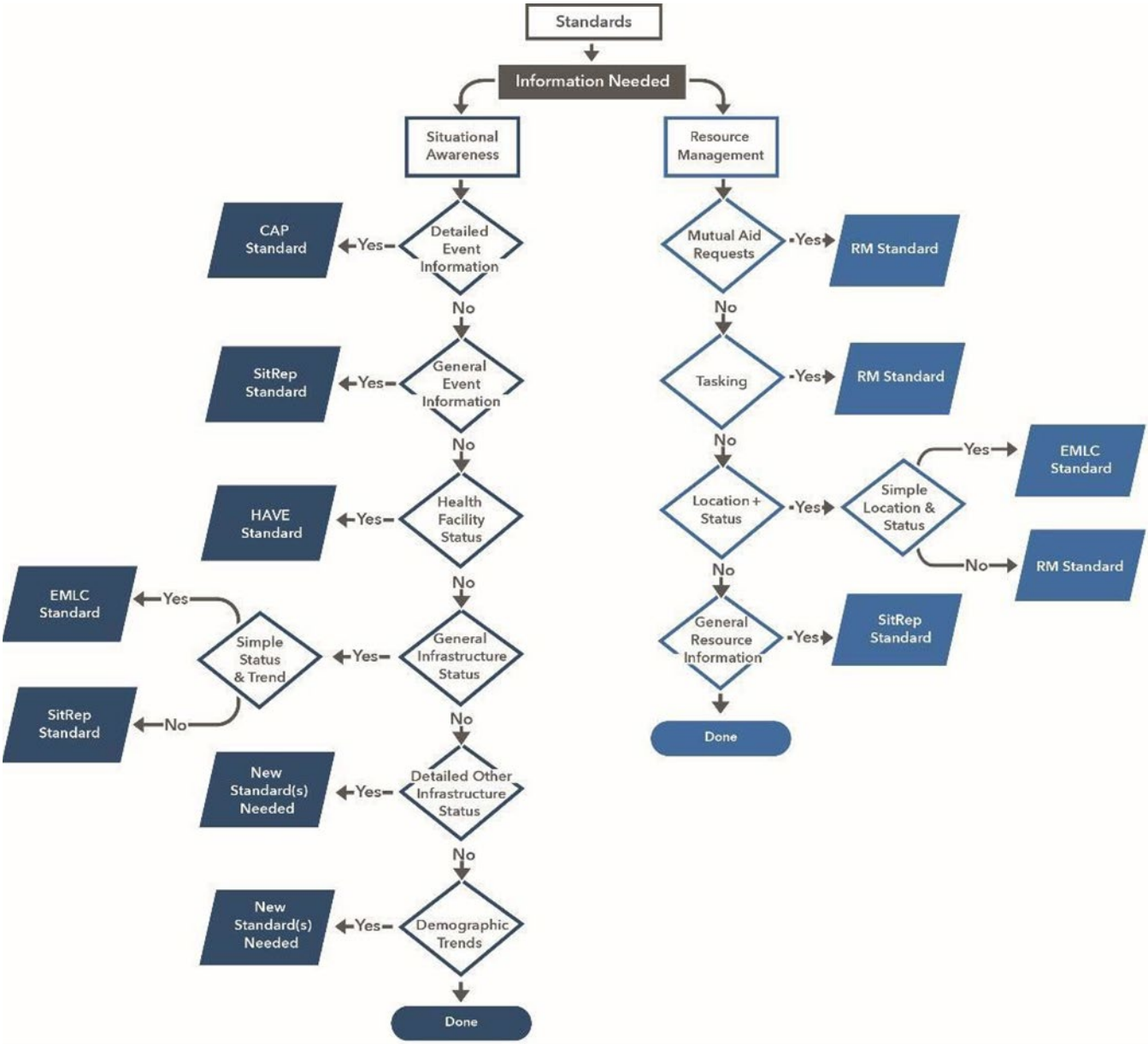


Figure 5 - Standards Selection Workflow and Decision Map

5.1 Situational Awareness Standards

The Situational Awareness workflow branch asks a series of questions about the kind of information needing to be shared. These are loosely based on the Situational Awareness requirements defined by public safety stakeholders over several years through coordination by NAPSG Foundation, and is documented in the Summary Report: Mutual Aid Information Requirements.

A "Yes" to the question points in the direction of a recommended standard, while a "No" simply moves you to the next question. The table in Figure 7 explains the intent of each workflow question.

Situational Awareness Workflow and Standards

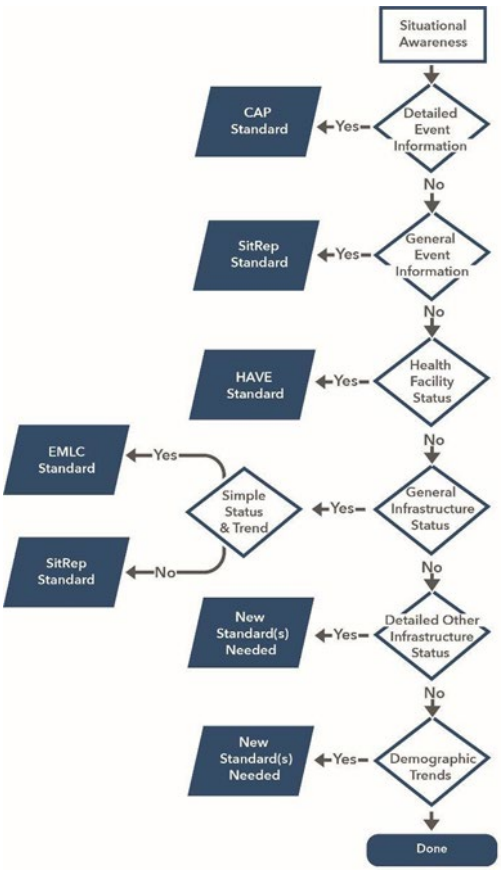


Figure 6 - Situational Awareness Workflow and Standards

The intent of the workflow is to match high-level information sharing needs to a recommended standard as simply as possible. In a few cases, there are no existing standards that meet an information need from the Situational Awareness requirements.

The standards that align with the Situational Awareness workflow include the following:

- CAP - https://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.html
- EDXL SitRep - https://docs.oasis-open.org/emergency/edxl-sitrep/v1.0/edxl-sitrep-v1.0.html
- HAVE - https://docs.oasis-open.org/emergency/edxl-have/v2.0/edxl-have-v2.0.html
- NIEM EMLC - https://niem.github.io/niem-releases/

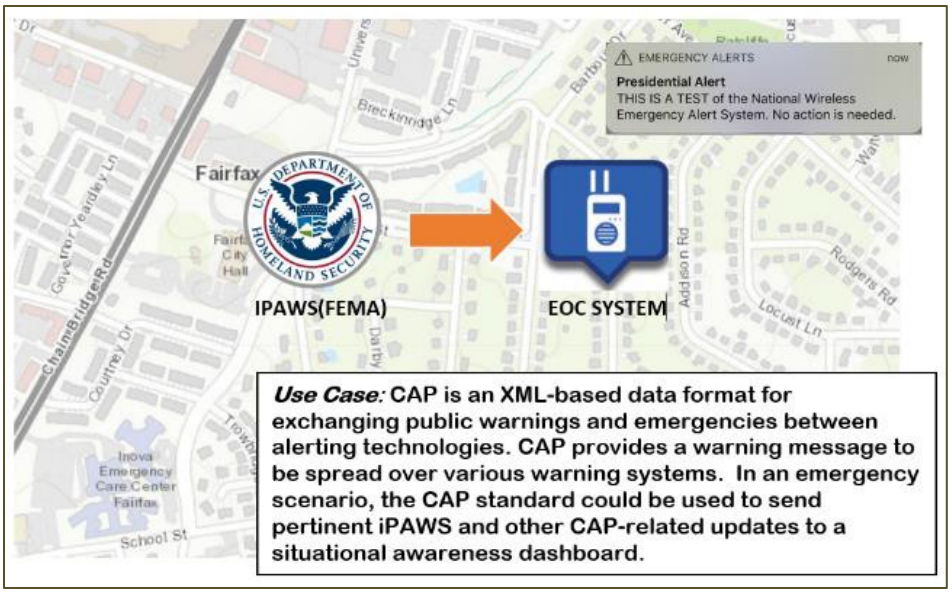
Workflow Considerations	Explanation
Detailed Event Information	Is detailed information needed about a specific event, including status and location, future predictions, impact area, and how to respond to a specific event?
General Event Information	Is more summary level, current information needed about an event?
Health Facility Status	Is detailed information needed about a specific health care facility, including bed status, Emergency Room (ER) capacity, Emergency Medical Services (EMS) response availability, etc.?
General Infrastructure Status	Is a general status needed for a specific infrastructure facility, such as Power Plant X, or for a general infrastructure category, such as communication?
Detailed Other Infrastructure Status	Is detailed information, like the type of information in health facility status, needed for a specific, non-health infrastructure facility?
Social Vulnerability and Demographic Trends	Is information needed about socially vulnerable, demographic trends, and/or demographic within the area of interest?

Figure 7 - Situational Awareness Workflow Considerations

5.1.1 Detail Event Information – EDXL CAP

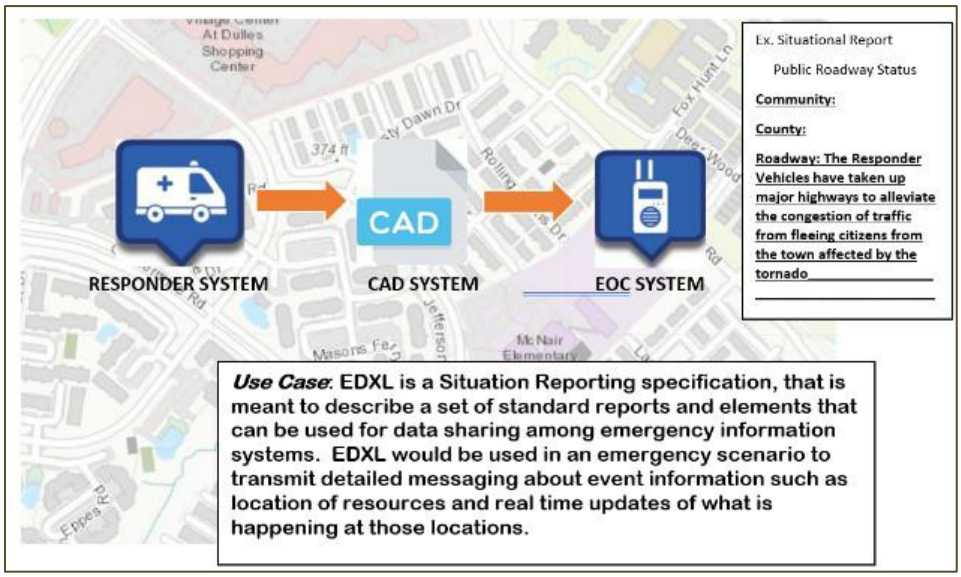
If detailed event information, such as severity, magnitude, consequences, directed action, location, etc., is required, then the OASIS EDXL CAP standard is recommended. CAP is the standard currently used by the Federal Emergency Management Agency (FEMA) Integrated Public Alert and Warning System (IPAWS) for issuing alerts and warnings around the country.

Seventy percent of the world's population lives in countries with a CAP based national alerting system. CAP is also published as Recommendation X.1303 by the International Telecom Union and recommended by the World Meteorological Organization.



5.1.2 General Event Information – EDXL SitRep

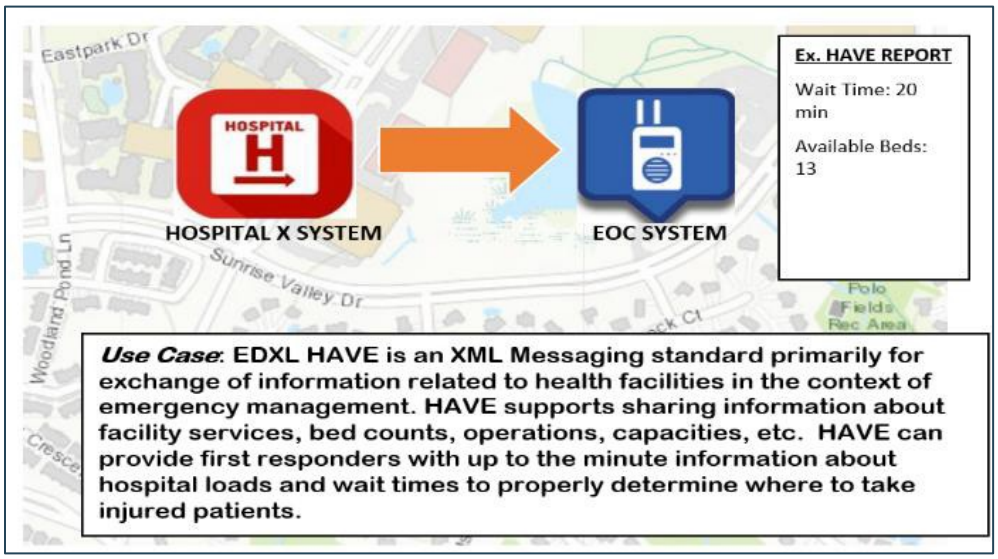
If more high-level, summary event information is required, then the OASIS EDXL SitRepstandard is recommended. There is a SitRep message for each of the standardized NIMS Incident Command System (ICS) reports.



5.1.3 Health Facility Infrastructure Status and Health Services Information – EDXL HAVE V2

If the status and state of health facilities are required, as part of infrastructure status or not, then the OASIS EDXL HAVE standard is recommended.

For events or incidents involving extensive health services support, the EDXL-HAVE v2 standard would be used on health information that supports clinical practice and the management, delivery, and evaluation of health services. This enables Emergency Managers and First Responders using the HL7 Implementation Guide within HAVE to communicate with HL7-based medical service providers such as emergency departments and hospitals. It directly supports communicating medical service types, quantity, and availability (e.g., number emergency beds available, dialysis service open/closed).



5.1.4 Patient Tracking – EDXL TEP

When an emergency patient is involved, the EDXL Tracking of Emergency Patients (TEP) Standard is recommended. It provides a standardized data format to collect patient information from first encounter through triage, field hospital(s), and the emergency medical services to the final care facility or hospital. There are also specifications available for transforming and sharing that data with the hospital's internal messaging system.

5.1.5 General Infrastructure Status – NIEM EMLC / EDXL SitRep

Currently, the only other standards that support infrastructure status are the NIEM Emergency Management Loose Coupler (EMLC) and SitRep standards. These standards only support general infrastructure status.

5.1.6 NIEM EMLC

The EMLC standard supports infrastructure status and trending for individual infrastructure entities, such as a power plant, highway, etc. Each entity is uniquely identified and located in addition to their status.

5.1.7 EDXL SITREP

The SitRep standard supports infrastructure status in a general category or capability, such as waterways, telecommunication, sewage, etc. Individual entities are not identified, and trending is not included. The EDXL Situation Reporting standard defines five (5) separate and specific report types to support incident command decision-making across the emergency incident life cycle. This includes preparedness, pre-staging of resources, initial, ongoing response, recovery and demobilization/release of resources, and after-action analysis to identify needed improvements in ongoing preparedness.

Use Case: Both standards can be used to transmit up to the minute information about various infrastructure entities that are or could be affected by an emergency. This information could then be added to a common dashboard for all parties to act upon.

5.1.8 OTHER INFRASTRUCTURE DETAILS – NEW STANDARD NEEDED

There are no other standards like EDXL-HAVE v2 that are currently available for the other infrastructure types. It should be noted that EDXL-HAVE v2 can be applied to health services information beyond common infrastructure details to include information on the availability of health and medical supplies within the facility itself.

5.2 Resource Management Standards

The Resource Management workflow branch asks a series of questions about the kind of information needing to be shared. These are loosely based on the Resource Management requirements defined by NAPSG Foundation in the Summary Report: Mutual Aid Information Requirements. They are broken down in Figure 8.

Resource Management Workflow and Standards

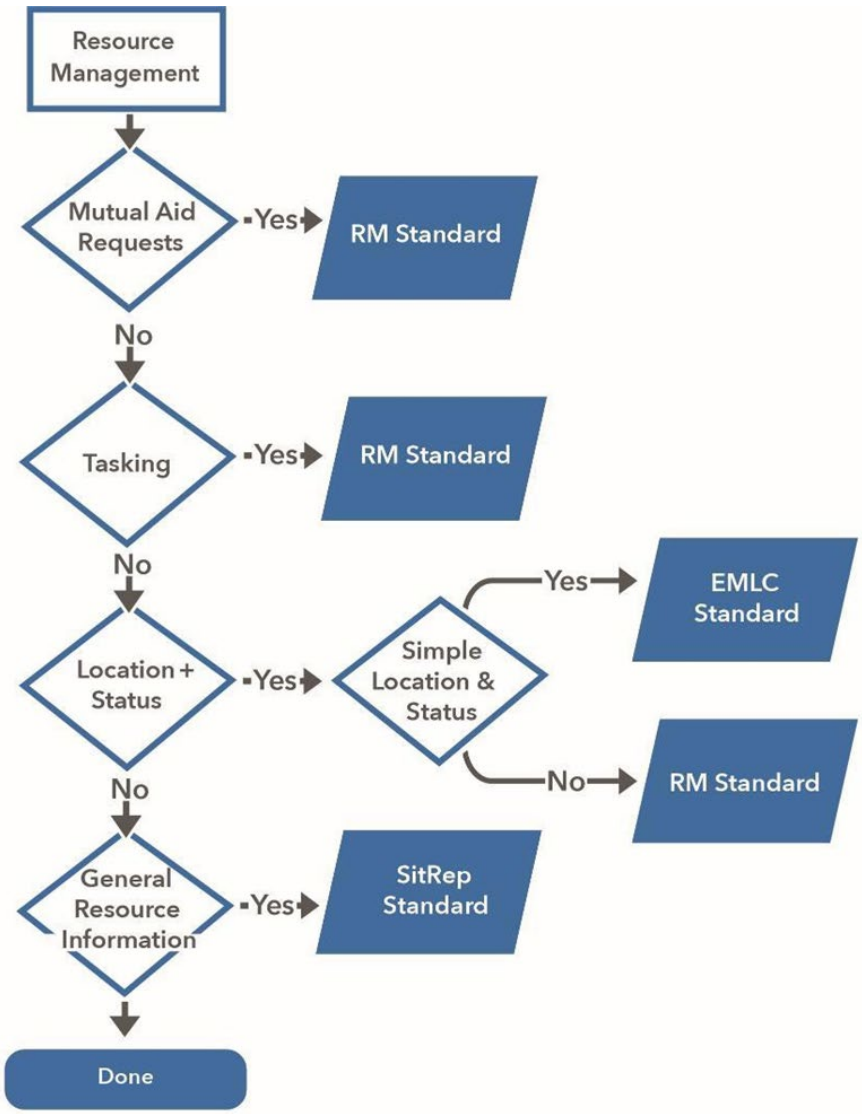


Figure 8 - Resource Management Workflow and Standards

General Category	SA Requirements	Workflow Considerations	Explanation
Mutual Aid	Resource Kind, Resource Response Availability, Resource Readiness, Deployment Time, Resource Cost	**Mutual Aid Request**	Is a request and response for aid needed, including costing?
Tasking	Status of taskings during the response	**Tasking**	Is the ability to task a responding resource needed?
Current Status	Resource Kind, Resource Response Availability, Resource Readiness	**Location + Status**	Is the status and location of a specific resource needed?
General Status	Resource Kind, Resource Response Availability, Resource Readiness	**General Resource Information**	Is a general status about a specific responding resource and/or all responding resources needed?

Figure 9 - Resource Management Workflow Considerations

The intent of the workflow is to match high-level information sharing needs to a recommended standard as simply as possible. In a few cases, there is no existing standard that meets an information need from the Situational Awareness requirements.

The standards that align with the resource management workflow include the following:

- EDXL RM - https://docs.oasis-open.org/emergency/edxl-rm/v1.0/EDXL-RM-SPEC-V1.0.html
- EDXL SitRep - https://docs.oasis-open.org/emergency/edxl-sitrep/v1.0/edxl-sitrep-v1.0.html
- NIEM EMLC - https://niem.github.io/niem-releases/

5.2.1 Mutual Aid Requests – EDXL RM / NIEM EMLC

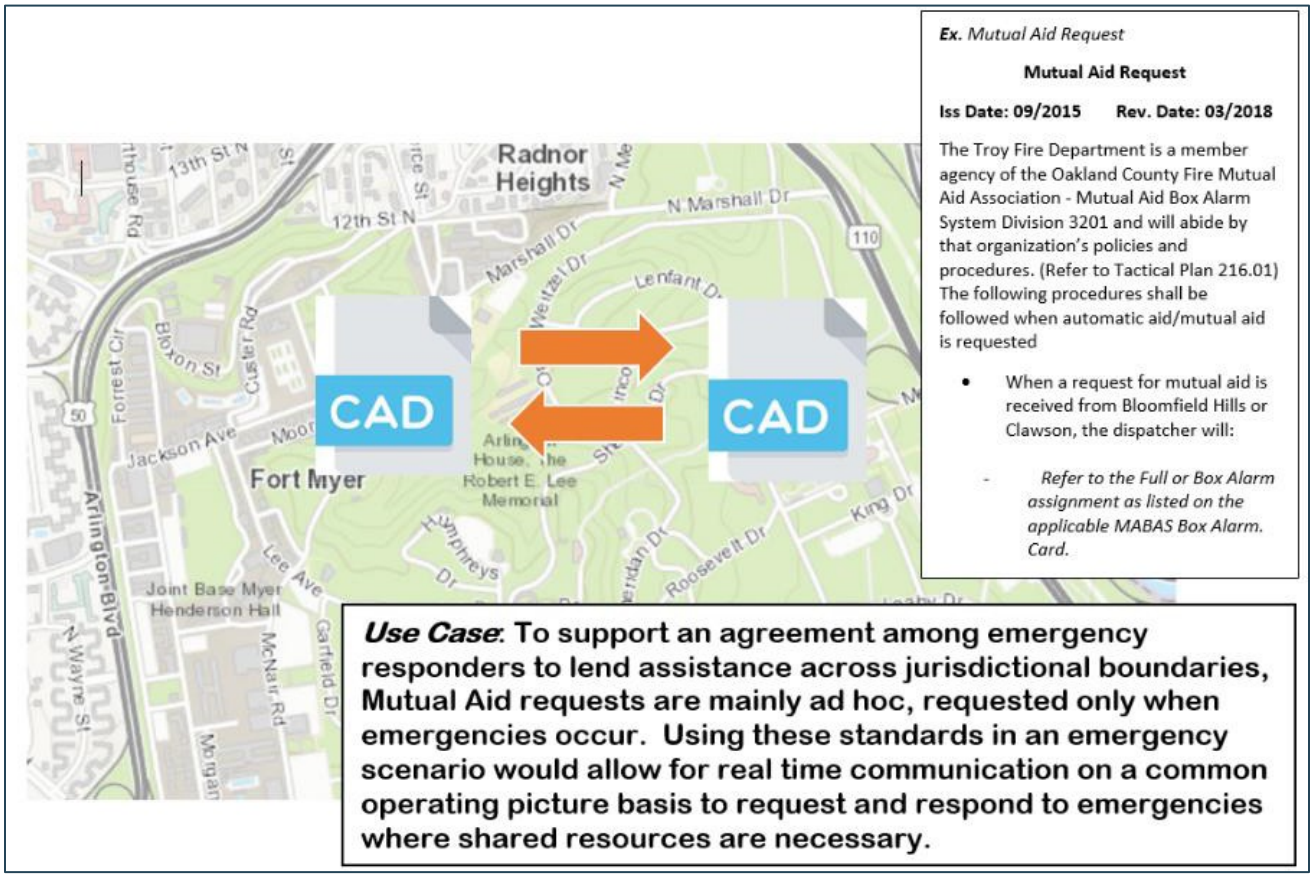
If making mutual aid requests and responses are required, then depending on the duration of the required aid and formality of the aid request either the OASIS EDXL RM standard or NIEMEMLC standard is recommended. EDXL RM has 16 pre-defined messages and the ability for custom user defined messages, and all RM messages include a location element.

NIEM EMLC

The NIEM EMLC supports simple mutual aid requests and responses without costing information. This standard is intended for short-term aid requests for an escalating incidentmost likely from neighboring jurisdictions.

EDXL RM

The EDXL RM supports both long-term and short-term aid requests, including costing information.



5.2.2 Resource Tasking – EDXL RM

If simple resource tasking is required, then the OASIS EDXL RM standard is recommended. RM supports simple text strings to indicate mode of transportation, navigation instructions, and reporting instructions as part of the assignment instructions.

5.2.3 Location + Status – EDXL RM / NIEM EMLC

If resource location and status are required, then depending on the need for real-time accuracy or not, either the EDXL RM standard or NIEM EMLC standard is recommended.

NIEM EMLC

The NIEM EMLC standard is designed to provide lightweight, real-time updates for responderlocation and status.

EDXL RM

The EDXL RM standard is designed for more periodic or transition updates for responder location and status, such as changes in availability or changes to estimated departure andarrival times.

5.2.4 General Resource Information – EDXL SitRep

If an overview of the resources currently assigned to an incident is required, then the EDXL SitRep standard is recommended. SitRep supports a "Response Resources Totals" report which provides an overview of the current resources, what agencies they work for, what they are assigned to, their status, etc. The SitRep does not provide resource location, unlike the EMLC and RM.

VI. Technical Communication

The following section describes the decision workflow for choosing the appropriate technical communication methodology between systems based on need. The intent is to aid in the vendor selection process when comparing different systems. The aim is to avoid the stove-piped nature of many of the existing systems in the Emergency Management Enterprise. There is a workflow provided which is split into two branches based on the information needs to be shared. See Appendix B for the entire workflow. For purposes of discussion, each workflow tree will be provided and elaborated upon in this section. The communication workflow focuseson the two most popular methods of sharing information between enterprise-level systems over the Transmission Control Protocol and the Internet Protocol (TCP/IP): Hypertext Transfer Protocol (HTTP) or Message Queuing Telemetry Transport (MQTT).

5.3 General Questions

The communication guidance workflow starts with a couple of questions to help determine which of the two most popular communication methods is recommended. However, the main question to ask is whether the system in question supports the recommended MACM standard(s) as determined in the standards workflow above. If the system in question does not, that defeats the intent of these documents and guidance, and it should be avoided. Which method to use is largely dependent on how the information needs to be shared between two systems or multiple systems and whether a response to a message is required. In some instances, because of business, operational, policy, or technological requirements, a positive response is required for some piece of information being shared, but this is not always the case.

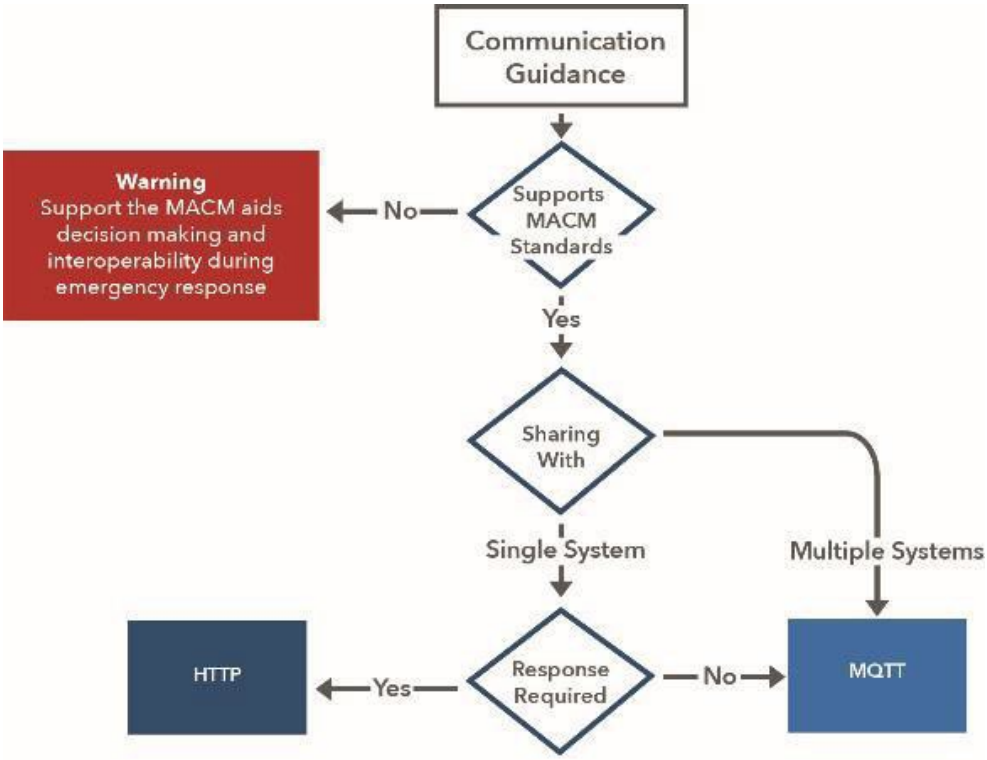


Figure 10 - Communication Main Questions

5.4 HTTP Branch Workflow

The HTTP workflow branch asks a series of questions about how the information will be shared. They are broken down in Figure 11 below.

Workflow Considerations	Explanation
Uses TLS	TLS stands for Transport Layer Security and is the current cryptographic protocol for securing network traffic while in transit.
Has an API Defined	API stands for Application Programming Interface. It defines the methods and information needed to interface to a system.
Is Accessible	How accessible is the system? Can it be accessed from the internet?
Uses XML or JSON	XML (Extensible Markup Language) and JSON (JavaScript ObjectNotation) are two of the most widely used data formats. This is how the information is structured in a message or file.
Uses DE to Wrap Other Standards	Does the system use the OASIS EDXL DE standard to wrap and route information?

Figure 11 - HTTP Workflow Questions

The intent of the workflow is to ensure the HTTP system supports security and enables information sharing.

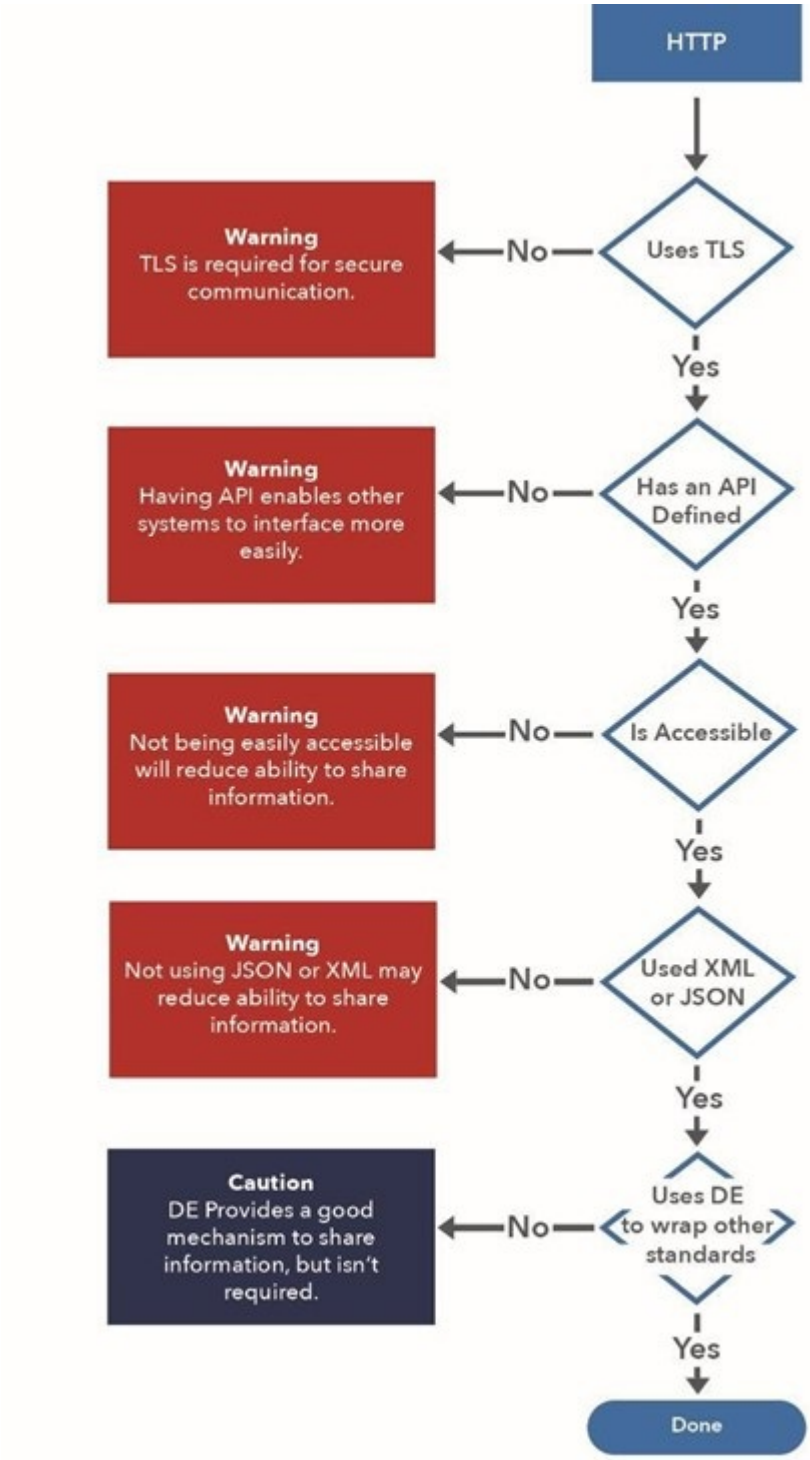


Figure 12 - HTTP Branch Workflow

5.4.1 Uses TLS

TLS ensures messaging over the network is secure. This is a requirement for sharing information between systems.

5.4.2 Has an API Defined

Having a defined API allows other system vendors to share information to and from this system more easily. Without it, other systems may not be able to share information to this system. Certainly, they will not be able to share information easily, as they may not understand what methods are available for them to use and what information is expected. APIs also need to define the security aspects of the system so other vendors know what methods to use. For example, does the system use username and password authentication or certification authentication or some other mechanism? Does it support single sign on? This information is important to other vendors as they determine how to share information to and from this system.

5.4.3 Is Accessible

How accessible is the system? Can other systems access it from the internet? If a system is behind paywalls, on a private network, or some other hinderance, this will reduce the ability of other systems to share information with it. While a system does not have to be on the open internet, it should be accessible from it. For example, a system could be running in a private cloud environment, but still be accessible through the internet. The problem arises if that system requires others to be in the same private cloud environment to access it.

5.4.4 Uses XML Or JSON

Does the system support either XML or JSON, or both, for messaging? Other formats may reduce the ability to easily share information. Most modern systems use either XML or JSON.

5.4.5 Uses DE To Wrap Other Standards

Does the system use the OASIS EDXL DE to transport other information? While this is not a hard requirement, the EDXL DE provides an excellent mechanism to share a wide variety of information that can be either structured or unstructured data. It acts as a wrapper for other information standards, much like an envelope wraps a letter. A DE-based system would be able to send and receive all the recommended MACM standards without the need for different endpoints or topics necessarily. This simplifies the overall system-to-system architecture and would aid in the ability to share a wide array of information. New standards could be added as EDXL DE payloads, supporting new and unexpected CONOPS, without the need to update the interfaces between systems. It is highly recommended that the EDXL DE be used as the primary transportation mechanism.

5.5 MQTT Branch Workflow

The MQTT workflow branch asks a series of questions about how the information will be shared. They are broken down in Figure 13.

Workflow Considerations	Explanation
Uses TLS	TLS stands for Transport Layer Security and is the current cryptographic protocol for securing network traffic while in transit.
Has a Defined Topic Structure	Is the topic structure defined? Does it have an easy to use template pattern?
Is Accessible	How accessible is the system? Can it be accessed from the internet?
Uses XML or JSON	XML and JSON are two of the most widely used data formats. This is how the information is structured in a message or file.
Has a Defined Payload	Have the payloads been defined, including whether XML or JSON is expected?
Uses DE to Wrap Other Standards	Does the system use the OASIS EDXL DE standard to wrap and route information?

Figure 13 - MQTT Workflow Questions

The intent of the workflow is to ensure the MQTT system supports security and enables information sharing.

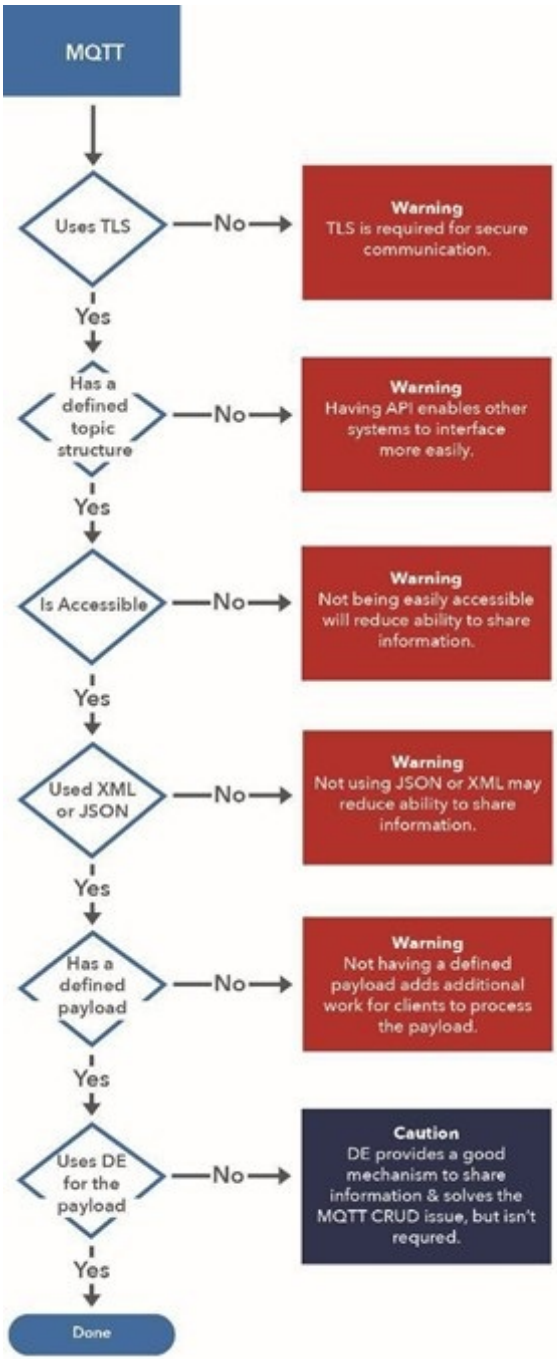


Figure 14 - MQTT Branch Workflow

5.5.1 Uses TLS

TLS ensures messaging over the network is secure. This is often a requirement for sharing information between systems.

5.5.2 Has a Defined Topic Structure

Topics in MQTT are a way to filter and categorize information. MQTT clients publish information and receive information through these topics. For example, a client might publish resource location on a topic like /<agency>/<unit id>/location, which might display as/lafd/ra52/location. Other clients would subscribe to the /lafd/ra52/location topic to receive updates for the Los Angeles Fire Department rescue ambulance 52's location.

The difficulty with using MQTT topics is they can be organized in a variety of ways and by the client. There is no discoverability mechanism that allows other clients to know what topics are available that they can subscribe to. This makes information sharing more difficult. By defining the topic structure ahead of time as part of an API for the system, other vendors will understand what the expectations of the system are, which improves the information sharing situation.

5.5.3 Is Accessible

How accessible is the system? Can other systems access it from the internet? If a system is behind paywalls, on a private network, or some other hinderance, this will reduce the ability of other systems to share information with it. While a system does not have to be on the open internet, it should be accessible from it. For example, a system could be running in a private cloud environment, but still be accessible through the internet. The problem arises if that system requires others to be in the same private cloud environment to access it.

5.5.4 Uses XML or JSON

Does the system support either XML or JSON, or both, for messaging? Other formats may reduce the ability to easily share information. Most modern systems use either XML or JSON.

5.5.5 Has a Defined Payload

Payloads in MQTT are typically text-based and can be any type of text information. This can make it very difficult for receiving systems (i.e., clients that have subscribed to a topic) to parse and understand the incoming information. To improve information sharing, the system's payload format (XML or JSON) and content format (i.e., what data standard) should be defined as part of the system's API. This will aid other vendors in understanding what to expect and how to parse the information coming from the MQTT server on a given topic. A map should be made for each topic in terms of format and content so it is clear what is expected to be sent and received for each given topic.

5.5.6 USES DE TO WRAP OTHER STANDARDS

Does the system use the OASIS EDXL DE to transport other information? While this is not a hard requirement, the EDXL DE provides an excellent mechanism to share a wide variety of information. It is well suited as an MQTT payload as it provides a mechanism internally to indict the usual CRUD (Create, Read, Update, Delete), as well as tasking and requests and responses, which are mechanisms that many systems employ today. It is highly recommended that the EDXL DE be used as the primary transportation mechanism.

VII. Security

Security is an extremely important aspect of information sharing between systems and involves multiple levels. Information should be secured in transit at a minimum and should ideally be secured while at rest. Transport Layer Security (TLS) is a cryptographic protocol to secure messages in transit over a network. It is a staple of secure web-communication. Both HTTP and MQTT support TLS communication in the form of HTTPS and MQTTs and was previously used for communication between systems. Further, EDXL DE allows for denoting classified/unclassified content and an encryption scheme that is used in the payload. As an additional layer of security, the message itself can be encrypted on top of TLS. If message encryption is required, the information and methodologies required to encrypt and decrypt the message must be a part of a system's API so clients can behave appropriately.

In addition to TLS and message encryption, system authentication and authorization requirements need to be considered. Authentication may be as simple as a username and password, or more complicated using client-server certificates. A username and password should never be exchanged in plain text and should be obscured/encrypted to secure them. Authorization is granted after authentication has been established and enables role- based permissions. System-to-system communication offers some unique challenges to authentication and authorization. Requiring users to enter multiple usernames and passwords to access information can hamper a mission. However, federated authentication and single sign on are not always possible. The goal of authentication should be to reduce user impact while still maintaining secure systems and communication. Client-server certificate maintenance and distribution can be challenging. Revoking and issuing new certificates can be time consuming and difficult.

While these challenges can be difficult to manage, security needs to be the priority of system-to-system communication and access. Message integrity is critical to emergency managers, so they do not question the information being provided. Message provenance is also critical to emergency managers, so they understand that the information being provided is from a reliable source. Communication and system security help ensure these things.

VIII. Data Integration and Feature Manipulation Engines

The second scenario on data integration using feature manipulation engine (FME) is based on a real-world pilot implementation by the National Police Foundation, the National Sheriffs' Association, and NAPSG Foundation to help track the impact of the COVID-19 virus on law enforcement personnel and PPE supplies across the US. This scenario highlights the use of the data integration and merging capabilities with FME to continuously merge two separate

feature layers into a single feature layer that can be used in GIS-based resource management platforms such as, but not limited to, ArcGIS Online Web Apps and Operations Dashboard.

5.6 Setup

Two geo-enabled live feature services were generated (in this example, the data source was ArcGIS Survey123) from two different organizations. These feature services reflected data collected on a daily and weekly basis from local, county, and state level law enforcement agencies to track the impact of COVID-19 on law enforcement personnel and PPE supplies. To obtain a comprehensive view of COVID-19 impact of law enforcement personnel and PPE supply needs nationwide, this data had to be combined into one dataset and still be flexible enough to receive updates as agencies provide new information. This data also had to be aggregated to the state level to protect agency-specific information being exposed on a public facing application.

5.7 Available Data

Both web-based forms include similar information, with some variation based on the unique needs of each organization. While the feature services being generated by the two agencies have some common fields, they are not identical. Further, when aggregating the data, it is critical that responses are only coming from law enforcement agencies and that there are no double or triple entries for the same agency. To address this, both forms required the respondent to enter their unique law enforcement agency number known as the ORI. This ORI number is a unique identifier (ID) that every law enforcement agency is assigned and required to submit the survey. The ORI points and survey feature layers can be joined to create a joint feature layer view that will automatically populate with the newest record for a given agency. This joint feature layer requires a level of quality control since all agencies may not input their ORI number correctly, which would result in their information not appearing in the joined data.

5.8 FME Integration

FME is a data translation software that uses a diagram interface to transform data. It works by using a series of technical readers, writers, and transformers to allow for manipulation of data to fit a new schema or export to a different format. In this scenario, using FME allowed for seamless and easy data merging and updating without going through the complex data mergingprocess. FME is like writing a script for running a tool (or series of tools) in ArcGIS - once it is written, the whole process can be run with a press of a button.

5.9 Example Implementation Options

FME Desktop is a locally hosted version of the software that has the workflow built in. Alternatively, a user can publish a workspace to FME Server or Cloud, which have the same basic interface and hold the same functionality. FME Server is hosted at your local computer and runs workflows locally, while FME Cloud is hosted in a cloud environment and workspaces can be triggered remotely. For users that have the ArcGIS Pro Data Interoperability extension, they have access to a similar set of capabilities seen in a separate FME Desktop solution. This workbench has the same capabilities as FME Desktop but does not allow you to publish workflows to FME Server or Cloud. If FME Desktop is used, a workspace can be published to FME Server/Cloud and automations can be set. Both suites allow for the use of automations to run a workspace automatically on a schedule or after a trigger. For example, automation can be set to run a workspace once a day at a user-defined time, or run every time a record is added to a dataset. In this scenario, updates are constantly coming in, so running this workspace once a day can eliminate a potential single point of failure and run in the background. More information can be found in Section 7.1 of this guidance document.

6.0 Context Diagram

Figure 15 below illustrates what the workflow would look like and how data from the example surveys was translated into one feature layer.

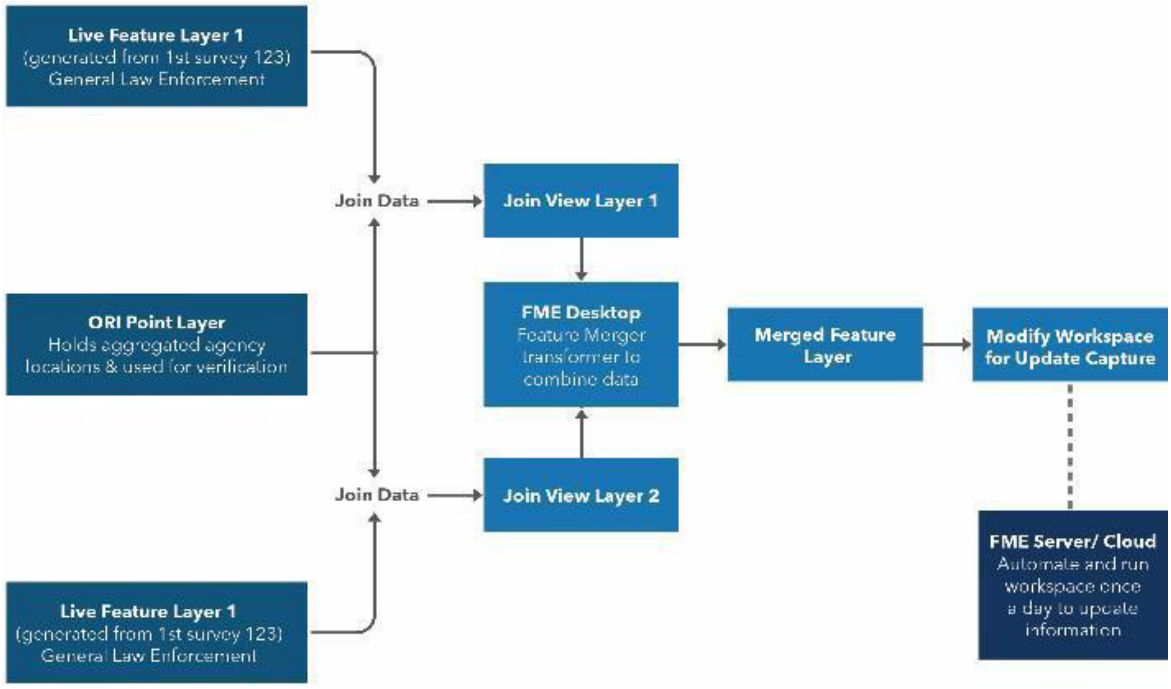


Figure 15 - FME Context Diagram

IX. Appendix

This section contains more detailed information on FME, HTTP, and MQTT as well as some insights to some of the common issues with both.

6.1 Data Interoperability Workflow with FME

FME works off a series of readers, writers, and transformers. The readers are the components that pull the data from a local computer or online connection (such as, but not limited to ArcGIS Online) into the FME workspace. There are hundreds of file formats that FME can read, including the following: AGOL feature layer, file geodatabase, excel, CSV, and AutoCAD. Writers are where data is "written out" or exported to. FME can write to all the same file formats that it can read in. FME can write into either existing dataset or create a new dataset using the information in the readers. Transformers are where data is changed and manipulated. There are hundreds of transformers in FME that include merging data together, splitting data, managing attributes, and creating reports. For Section 6 details above, the most effective transformers to use are the attribute manager for matching the attributes and feature merger for both merging the data into one dataset and looking for updates.

In Section 6, data was pulled from two feature layer joins. Both feature layers are readers, and both go through an attribute manager transformer to match one another. Using an existing feature layer as a writer helps with matching the attributes in the attribute manager. Once the two readers' attributes match the writer, a third reader is added. This reader is the same dataset as the writer (the merged dataset) and will be used to check the current dataset against the join feature layers to systematically look for any changes.

Once the readers and writers are added into the workspace, a feature merger transformer should be added to look for differences between the original layer and the join layers. Connect the two feature layers containing the survey points to the "Supplier" section and the third reader that is the same dataset as the writer to the "Requester" section. Double click the feature merger to open its parameters and make sure they join on the ORI number. This will ensure that the transformer is comparing the datasets based on the ORI number and will search for any changes in the records. See Figure 9 below for what the workspace should look like when finished.

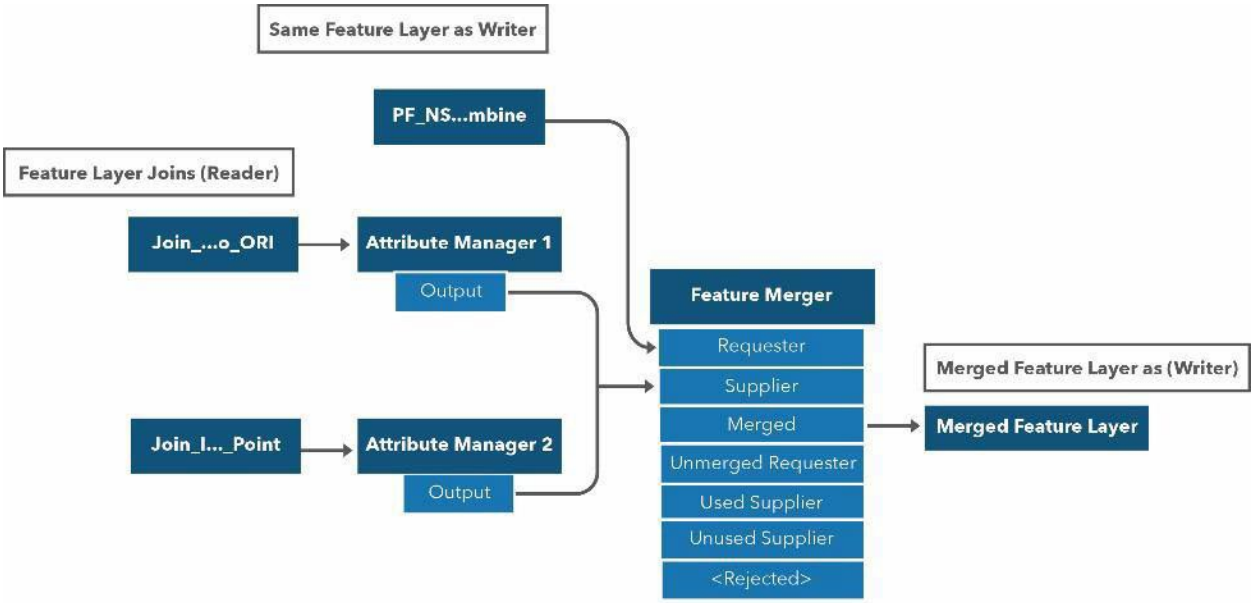


Figure 16 - Data Interoperability Workflow with FME

6.2 MQTT

One of the challenges of using MQTT to send and receive information is its topic structure and lack of verbs, like how HTTP has to describe what to do with the new information.

Depending on the type of information being shared, a delete or cancel operation might be necessary. If this type of information is not embedded in the standard, either a new topic will need to be used or the message payload will need to account for this operation. MQTT is a completely different technology, and architecture from HTTP is not a 1:1 alternative. It is designed for light-weight messaging and rapid distribution to multiple clients.

6.2.1 Topics

Topics in MQTT are freeform but follow a hierarchical structure, meaning a topic can be created about anything but typically follow a logical pattern. For example, if you had a home security system using MQTT where each security sensor reported its information to the MQTT message broker, you might have a topic structure that format like this: /home, home/<room>/, home/<room>/<sensor type>. <Room> and <sensor type> are template placeholders for actual data from a house. A real topic example for a house might look like this:

/home
/home/living room/
/home/living room/motion detector
/home/living room/smoke detector
/home/living room/window alarm

/home/mud room/
/home/mud room/door alarm
/home/kitchen/
/home/kitchen/smoke detector
/home/kitchen/flammable gas detector
Etc.…

An alternative topic structure might be by sensor instead of room: /home/<sensor type>/<room>

/home
/home/motion detector/
/home/motion detector/living room
/home/smoke detector/
/home/smoke detector/living room
/home/smoke detector/kitchen
/home/window alarm/
/home/window alarm/living room
/home/door alarm/
/home/door alarm/mud room
/home/flammable gas detector/
/home/flammable gas detector/kitchen
Etc.…

Either template is functional. This flexibility is great for using MQTT internally for a single system with multiple clients. However, this flexibility is very challenging when trying to use MQTT to connect external systems together. Part of an MQTT API must detail the what the topic structure is and how it is expected to be used. Without this, it will be very difficult for an external system to know what it can subscribe to for topics and what it can publish to for topics.

6.2.2 Topic Discoverability

An additional challenge for MQTT is that topics are not necessarily discoverable. It is completely API dependent. There is no native way to discover all the topics in use on a given MQTT message broker. This is a significant challenge for the MACM domain where new topics could be easily added on the fly, and downstream (listening) clients would not know there is a new topic to listen to. If the system does not allow new topics to be added on the fly, this is not an issue. However, in a large-scale event, there may be a need to add new topics to organization information in new ways. One potential solution around this issue is support a well-known topic, that would be used by every MQTT MACM system, a topic like "/topics". An MQTT client to an MACM system would know it could subscribe to this topic and receive the information about the current topics. The MQTT broker would need to be setup so any client

subscribing to this topic would receive the full history on this topic. When the MQTT broker is started, a "master" client of the system would connect and publish the list of available/default topics to this topic. Once a new client subscribed to this topic, the existing topic information would be pushed to it. This information needs to be more than just a list of topic strings; it should also include the payload format and payload content for each topic. The payload for the "/topics" topic would be a simple JSON object that contains the remaining topic information. It might look something like this:

```
{
        topics: [
                {
                        topic:"/content/have",
                        format:"application/json",
                        content:"urn:oasis:names:tc:emergency:EDXL:DE:1.0"
                        description:"Hospital Status Updates"
                },
                {
                        topic:"/content/rm/request",
                        format:"text/xml",
                        content:"urn:oasis:names:tc:emergency:EDXL:DE:1.0"
                        description:"Resource Management Requests"
                },
                {
                        topic:"/content/rm/response",
                        format:"text/xml",
                        content:"urn:oasis:names:tc:emergency:EDXL:DE:1.0"
                        description:"Resource Management Responses"
                }


        ]
}
```

A structure like this would provide a human readable description of the topic, enable a client to understand what topics are available, what the format of the payload is, and what standard the payload is using. In theory, a client could publish information about a new topic before publishing information to the new topic. This would update all other clients that a new topic is available and allow them to subscribe to it to receive new information.

The "topic" field would be a simple string containing the topic. The format field should be limited to the media type for XML and JSON: text/xml and application/json respectively. The content field should either be a publish code list representing the different MACM standards or could simply be the namespace associated to the top-level element in the standard. The advantage to the second option is an external list would not need to be created.

6.2.3 PAYLOADS

As with topics, MQTT payloads are designed to be flexible in nature. The MQTT payload represents the dynamic part of an MQTT message and can be information that can be encoded into bytes, up to 256MB in size total. This is typically in the form of text, and is often JSON, but could be XML, CVS, ASCII, etc. There is control field to indicate what the format of the payload is. This means there needs to be an agreement between the publishers and subscribers on the format of the payload, so a subscriber can digest and understand the payload. For example, if a publisher publishes a payload in XML but the subscriber was expecting JSON, the subscriber will not be able to digest and understand the payload. Additionally, if the publisher publishes Resource Management information, but the subscriber was expecting Situational Awareness information instead, then the subscriber will not be able to digest and understand. It is important that these details are spelled out in the MQTT API.

6.2.3 PAYLOAD OPERATIONS

Additionally, there may be times where some information needs to be deleted or cancelled, such as an alert, like a shelter in place warning. Unless this information is embedded in the content of the payload, MQTT does not natively provide a mechanism to support this type of operation. Either the topic structure will need to account for this type of operation, or the payload itself will need to contain the operation. Fortunately, some standards such as CAP and DE already support this type of operation within their data structures. Depending on the standards transmitted in the payload, it may be necessary to define a new payload structure to account for these operations (if needed) or adopt a topic structure that will support these operations.

6.3 HTTP

Most modern web-based systems have adopted REST as their architecture. Consequently, the API guidance here will focus on a REST implementation. HTTP messages have two parts: the header and the body. The HEADER contains the HTTP operation, authentication information, media-type, etc., which helps the server determine what do with the client's request. The BODY (if present) contains the shared information. Unlike MQTT, HTTP has a well-known, well-defined set of operations for handle HTTP requests. These operations are generally defined as follows:

- GET – retrieves information from the system
- POST – adds new information to the system
- PUT – wholesale updates (replaces) existing information in the system
- DELETE – removes information from the system

- PATCH – partially updates (updates portions of) existing information in the system

These operations allow for a variety of actions to be taken. A HTTP API should attempt to practice high cohesion, so these operations perform as expected. It is not uncommon for a POST operation to be overloaded so both additions and updates are performed. This should be avoided, as it can add confusion on the intent of the operations.

6.3.1 REST

REST focuses on resources that are available in the system. An example for a mutual aid domain might be alerts. A REST-based API would describe the URL endpoints of that system that would allow for alerts to be created, updated, deleted, retrieved, and patched. These might look something like this, with the HTTP operation in the HEADER.

GET - https://some.server.com/alerts - retrieves all available alerts

POST - https://some.server.com/alerts - creates a new alert

DELETE - https://some.server.com/alerts - deletes all available alerts

GET - https://some.server.com/alerts/<some alert id> - retrieves a specific alert

PUT - https://some.server.com/alerts/<some alert id> - updates a specific alert

PATCH - https://some.server.com/alerts/<some alert id> - patches a specific alert

DELETE - https://some.server.com/alerts/<some alert id> - deletes a specific alert

Like MQTT's topic structure, REST endpoints can be very flexible, and it can be difficult to organize an API in a meaningful way. There have been several attempts in the past to describe a RESTful API in a machine-readable way, but there has been no consensus on a single approach. Consequently, this makes discovering RESTful endpoints very difficult if not impossible. Unlike MQTT, HTTP clients cannot create new endpoints, so the need to allow for discoverability is reduced. Proper API documentation should suffice.

6.3.2 DE DISTRIBUTION TYPE AND HTTP VERBS

The three DE distribution types provide an opportunity to set up a HTTP server in one of two ways. A simplified endpoint structure can be provided that simply supports two HTTP verbs, GET and POST. In this instance, the POST endpoint takes a DE and relies on the Distribution Type to determine how the DE message and content is handled. The alternative is a more RESTful HTTP server that supports GET, POST, PUT, and DELETE, where the POST, PUT, and DELETE endpoints are expected to receive a DE with the corresponding Distribution Type (Report, Update, Cancel).

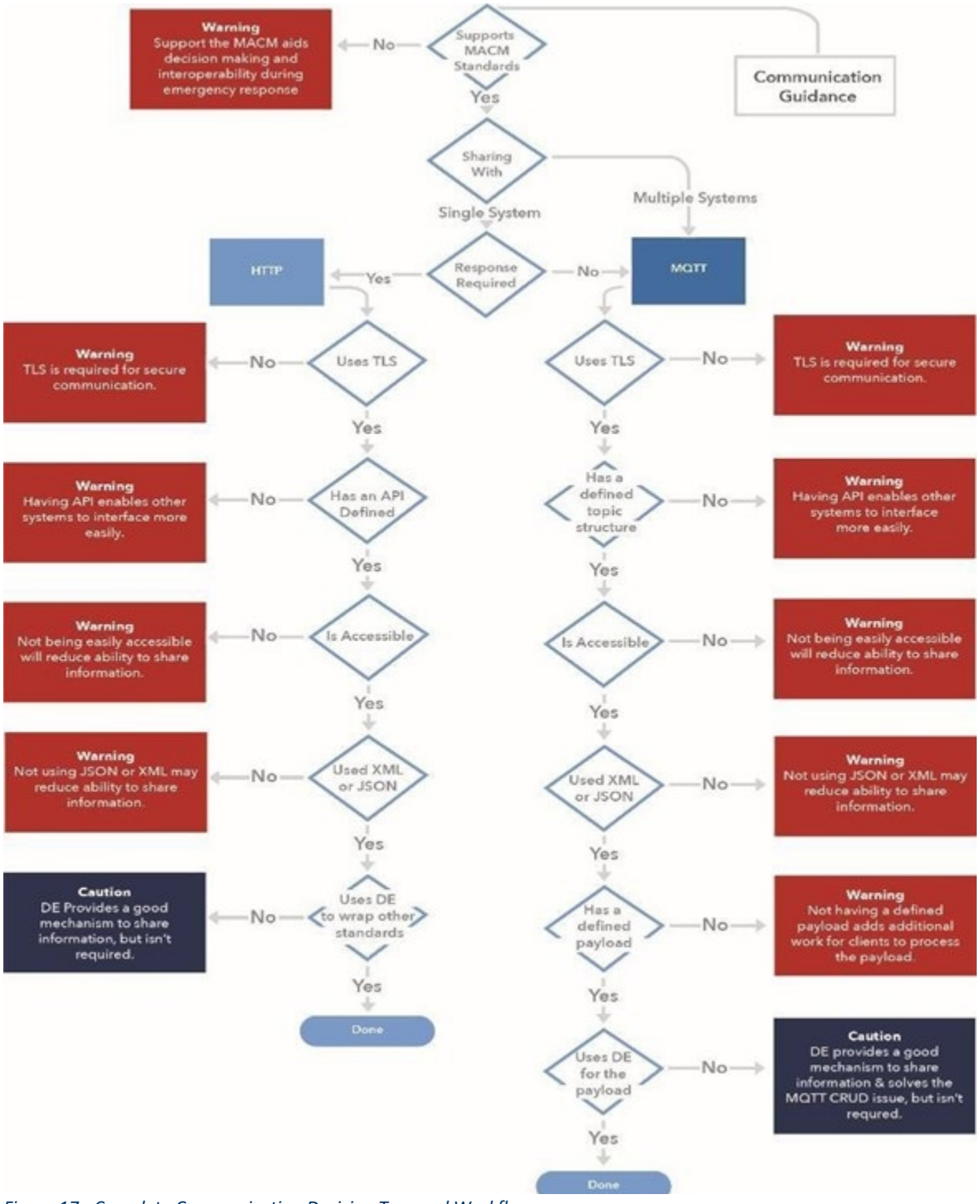


Figure 17 - Complete Communication Decision Tree and Workflow