Software Engineering Institute

Commercial Mobile Alert Service (CMAS) Scenarios

The WEA Project Team

May 2012

SPECIAL REPORT
CMU/SEI-2012-SR-020

CERT® Division, Software Solutions Division

http://www.sei.cmu.edu

Carnegie Mellon University

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013 and 252.227-7013 Alternate I.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

DM-0000625

Table of Contents

List of Figures

List of Tables

Abstract

This report supports the Department of Homeland Security Research, Development, Testing, and Evaluation program in its collaboration with the Federal Communications Commission on the Commercial Mobile Alert Service (CMAS). CMAS plays a critical role in providing targeted alerts to a geographic area. As a system-of-systems implementation, CMAS crosses many organizations to accomplish its mission. Identifying the steps taken to respond to an incident across various system and organizational boundaries can help expose potential barriers and challenges to CMAS integration. This report organizes these steps into three types of scenarios. Operational mission threads illustrate the security and organizational aspects of the integration strategy, development mission threads illustrate technical and acquisition aspects of the integration strategy, and quality attribute scenarios illustrate nonfunctional aspects of the system such as latency, resilience, or scalability. The analysis of these scenarios will help CMAS stakeholders determine how to handle the challenges that they experience as part of this large-scale integration.

1 Introduction

The Software Engineering Institute (SEI) is supporting the Department of Homeland Security Research, Development, Testing, and Evaluation (DHS RDT&E) program in its collaboration with the Federal Communications Commission on the Commercial Mobile Alert Service (CMAS). CMAS is one of the major components of the Federal Emergency Management Agency (FEMA) Integrated Public Alert and Warning System (IPAWS), which enables federal, state, territorial, tribal, and local government officials to send targeted text alerts to the public via commercial mobile service providers (CMSPs). The SEI is developing integration strategies and associated artifacts to support the successful deployment, operations, and sustainment of the CMAS capability, with a special focus on the needs of alert originators [FEMA 2011b].

This report is the second product of the SEI effort. It describes a set of scenarios that the SEI has collected or developed for the CMAS RDT&E program. The first product of the SEI effort was a report on the CMAS Alerting Pipeline Taxonomy, a hierarchical classification that encompasses the following four elements of the alerting pipeline: alert originator, IPAWS aggregator, CMSP infrastructure, and recipients [SEI 2012].

The SEI has found scenario-based analysis to be highly effective. Stakeholders—including managers, operational users, and others—can better understand functional and nonfunctional attributes (also known as quality attributes) of systems when the attributes are presented in terms of scenarios. From techniques as simple as listening to stakeholders' stories to formal, in-depth development and vetting of mission thread scenarios, the method can help identify the issues, challenges, and barriers to CMAS integration. Iterative interchange between user needs and supply-side solutions, facilitated by stakeholders' scenarios that make the issues evident, reveals risk mitigations that inform the integration strategies. By documenting and sharing scenarios, the many research teams within the CMAS RDT&E effort will have a better understanding of the issues, challenges, and barriers to CMAS integration.

The goal of our analysis is to develop a set of integration strategies that will aid the national deployment of CMAS. The scenarios cover the context, externalities, and operational aspects of CMAS adoption and the internal workings of the architectures, systems, and system-of-systems aspects of CMAS. We continue to interact with key stakeholders to prioritize scenarios to ensure that we focus on the areas of highest value.

The scenarios presented in this document are the initial set that we have captured to date. Ongoing scenario analysis will serve as a tool to help us identify integration strategy barriers and challenges, and these scenarios will evolve as the CMAS integration strategy progresses. Similarly to the taxonomy, we expect the scenarios to evolve based on comments from external reviewers, information gleaned from our stakeholder interviews, input from the other tasks described in the SEI CMAS Project Management Plan, and the experiences of other performers involved in the CMAS RDT&E program.

2 Analysis Approach and Report Overview

2.1 Overview of Scenario Types Used for the Integration Strategy Analysis

We leveraged two primary types of scenarios to feed the scenario-based analysis techniques for our integration strategy analysis on the CMAS project: mission thread scenarios and quality attribute scenarios. In this section, we briefly describe each type of scenario and their relationship to each other. In subsequent sections, we provide detailed descriptions and mission thread scenarios.

Mission thread scenarios describe a set of steps taken to respond to an incident or execute a mission. They are useful for exploring operational interaction and relationships at the system-of-systems level. For example, if we create a mission thread describing an America's Missing: Broadcast Emergency Response (AMBER) alert, the mission thread may contain steps that span various systems and organizational entities. We might describe steps as follows: an event causes the user to generate an alert, the alert is sent, a message is disseminated by the carrier, and so on. The term *mission thread* has its origin in Department of Defense analysis in which operational scenarios may cross many organizations or military services to accomplish a mission. This technique is applicable to CMAS analysis because CMAS end-to-end scenarios may also span multiple systems and organizational entities.

Quality attribute (QA) scenarios are short descriptions of interactions in a system or subsystem that illustrate nonfunctional (quality) aspects of the system. We use these scenarios to augment mission thread steps to allow for deeper dives into systems-related concerns. Analysis of QA requirements is less concerned with the features that the systems must provide and more concerned with the qualities expected of the system. For example, a performance QA scenario may describe in detail how rapidly the system must respond when multiple concurrent alerts are sent. Typical QA requirements describe qualities such as performance, security, availability, extensibility, usability, testability, and modifiability. There is a critical relationship between QAs and a system's architecture; in fact, the architecture is the primary enabler of system qualities. QA scenario analysis is one of the SEI's signature analysis methods, and we have used it successfully on large-scale projects to identify architecture-related issues and risks [e.g., see Bergey 2000, 2002; Nord 2009].

Figure 1 shows the relationship between mission thread scenarios and QA scenarios. Mission thread scenarios contain steps that describe an end-to-end process, often across many systems or organizational entities, such as responding to an AMBER alert from initiation to message dissemination. We use QA scenarios to analyze the system's response to specific stimuli in a particular mission thread step. Continuing with the AMBER mission thread as our example, we can expand the first step in the thread to contain a QA scenario that describes how fast the system must authenticate a user trying to send an alert under peak load (this is a *performance* QA scenario). We use QA scenarios to identify risks or problems that we may need to address in the integration strategy. These scenarios are also useful for developing systems integration practices and standards for alert-generating originators or vendor tool providers.

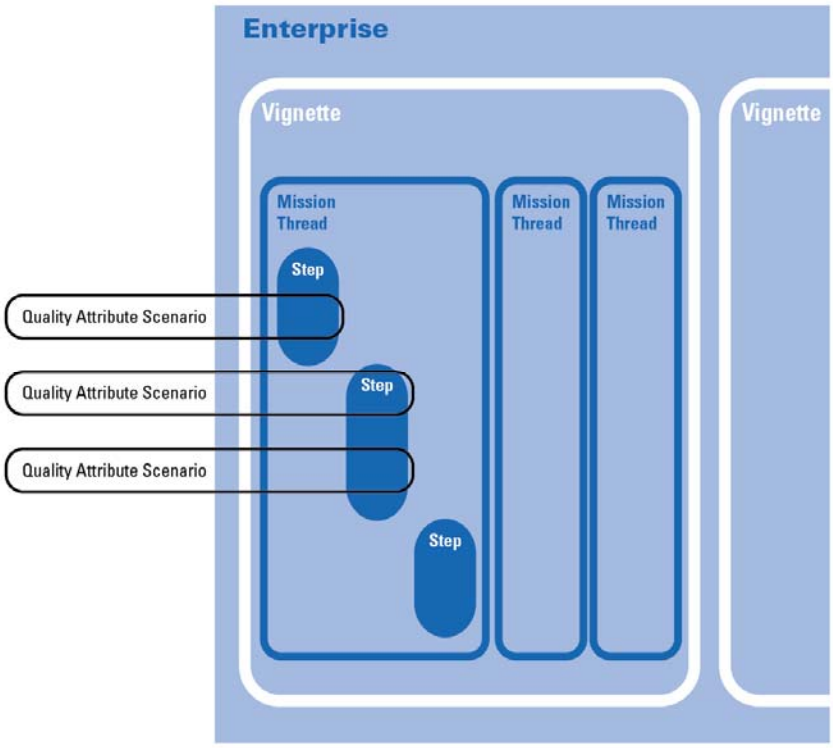


Figure 1: Relationships of Scenario Terms

Now that we have provided an overview of mission threads, QAs, and the relationship between them, in the remainder of this section we present more detailed information about mission thread scenarios, QA scenarios, and related terms.

As defined previously, mission thread scenarios (or simply mission threads) are high-level steps required to accomplish some significant process. We further classify mission threads as follows:

- **development mission threads**: what a development (or engineering) organization does to become CMAS capable, covering both green-field (no existing system) and brown-field (building on legacy systems) strategies
- **operational mission threads**: how users interact with CMAS to handle presidential, imminent threat, and AMBER alert scenarios
- **sustainment mission threads**: scenarios related to keeping the system in operating condition, including upgrades, emergency maintenance, return to service, security incident handling, and change management

Vignette scenarios (or simply vignettes) are a type of scenario used to support mission thread analysis. Vignettes describe the context for mission threads. They provide a view of the environment before the incident or stimulus of interest happens.

QA scenarios are short descriptions that illustrate nonfunctional aspects of the system such as latency, resilience, or scalability. From traditional SEI architectural analysis, we further classify QA scenarios as follows [Bass 2003]:

- **use-case QA scenarios**: scenarios that examine how the architecture handles under normal operating conditions
- **growth QA scenarios**: scenarios that push the architecture beyond normal operating conditions (e.g., increase to peak load)
- **exploratory QA scenarios**: scenarios that significantly stress the system, almost to the breaking point, to identify weaknesses

QA scenario types typically focus on a system or a component of a system. We use QA scenarios to isolate a QA of interest or help illuminate issues in a given step of a mission thread. These scenarios consist of the following parts [Bass 2003]:

- a stimulus: a condition that must be considered when it arrives at a system
- a source of the stimulus: the entity (e.g., a human or computer system) that generated the stimulus
- an environment: the conditions under which the stimulus occurs (e.g., when the system is in an overload condition)
- the artifact affected by the stimulus
- a response: the activity undertaken after the arrival of the stimulus
- a response measure: the attribute-specific constraint that the response must satisfy

There are many more scenario characteristics and relationships. Appendix C provides more detail on the subject.

2.2 Data Gathering Methods

Our scenario analysis methods are typically based on workshops. We facilitate the development of mission threads and QA scenarios in a workshop setting, and the scenarios are the output from the workshop. However, due to the distributed nature CMAS, we have tailored our approach to accommodate the stakeholders. Our approach to date for developing scenarios has leveraged methods such as

- published literature searches
- documentation provided by interviewees
- email exchanges
- telephone interviews
- personal interviews
- small-group workshop sessions

For this report, we primarily used telephone interviews with emergency response organizations. The process for the telephone interviews follows these steps:

- Prepare initial stakeholder descriptions and a template for technical exchanges.
- Conduct external stakeholder technical exchanges (we have included all the CMAS performers in order to use stakeholders' time efficiently).
- Share findings within the SEI team, refine as appropriate, and perform derivative investigations as necessary.

- Develop scenarios from data gathered, and populate the analysis templates that we will use for risk analysis.
- Improve the template for future technical exchanges.
- Expand and correct the taxonomy [see SEI 2012].

As part of integration analysis, we also gather contextual information that is helpful for categorizing the information that we collect. The five *W*s (who, what, where, when, and why) shown in Table 1 have been useful for this purpose.

Table 1: The Five Ws of CMAS Integration

The Five *W*s	**Relevance to CMAS Integration**
Who	Key stakeholders: alert originator organizations and vendors that supply these organizations
What	Types of alerts: presidential, imminent threat, and AMBER
Where	Jurisdictions that must be covered: federal, state, territorial, tribal, and local
When	Phases of adoption: integration/development, operation, and sustainment
Why	Value propositions: prepare and respond to threats to life and property

2.3 Overview of the Report Structure

In the remainder of this report, the key sections covered include

- high-level descriptions of four mission threads (Section 3)
- a sample set of QA scenarios that we collected to augment those mission threads (Section 4)

We provide the complete scenarios in Appendix A, formatted for ease of reuse in subsequent stakeholder engagements.

3 The Mission Thread Scenarios

We have identified four mission threads that we believe cover a sufficient variety of situations to stimulate our initial integration strategy research. These include three operational mission threads: (1) a terrorist threat, which is a presidential alert; (2) a weather threat, which is an imminent threat alert; and (3) an abduction, which is an AMBER alert. We also include a fourth mission thread about CMAS adoption, which addresses development and sustainment of CMAS. These four high-level mission threads will be the basis for developing more detailed mission threads that address threats specific to an organization's jurisdiction. Further interactions among stakeholders may reveal the need for additional threads or thread variants to account for different organizational characteristics.

We anticipate that vetting the operational mission threads will predominantly inform the security and organizational aspects of the integration strategy. The adoption mission thread will predominantly inform the technical and acquisition aspects of the integration strategy.

Our plan for initial use of these mission thread scenarios is through facilitated workshop-style engagements. We will give the participating organization the mission threads as read-ahead material. Before the workshop, the organization will critique and modify the mission threads to make them more focused on its own context. The workshop participants will then interactively drill down into the steps of the mission threads to identify issues, challenges, and barriers that inhibit CMAS adoption (e.g., a discovered security flaw increases a risk to an unacceptable level, or an inadequacy in standard operating procedures triggers rework to the procedures).

We will use the QA scenarios to augment discussion about mission thread steps to explore QA requirements in more detail (see Section 4). Such discussions also frequently expose operational risks. For example, "what if" discussions of a given step might reveal a need for alternative contact mechanisms to reach decision makers. Thus, participants identify redundancy as a needed QA that helps subsequent investigators quickly understand and address the issue. Subsequent analysis can determine whether this requires a technical solution, an operational solution, or both.

As the mission threads mature through these workshop engagements, they will become useful artifacts with which to build self-help practices or shared resources that the community can leverage to improve standard operating procedures.

3.1 Terrorist Threat Mission Thread

This section presents a summary description of an operational mission thread (elaborated in Appendix A.1) about a terrorist attack that we will use to conduct several mission thread analyses focused primarily on security and resilience. The terrorist mission thread description contains three parts: a vignette (describing the context in which the event takes place), a summary set of steps taken from the mission thread, and a picture illustrating the flow of the mission thread (Figure 2).

3.1.1 The Terrorist Threat Vignette

The Philadelphia subway system consists of both above- and below-ground stations. Multiple cell phone providers provide coverage for the city of Philadelphia. FEMA has set up IPAWS to support the East Coast of the United States with a FEMA operations center (FOC) and a regional emergency operations center. For this vignette, a Philadelphia emergency operations center is the Common Alerting Protocol (CAP) alert originator.

3.1.2 The Terrorist Threat Mission Thread Steps

Table 2 contains a set of steps taken from the mission thread scenario of a terrorist threat. The elaborated mission thread table appears in Appendix A.1.

Table 2: Terrorist Threat Mission Steps

Mission Steps	Time	Description
1	6:05 a.m.	The Main Street train has just left the Spring Garden Center Station.
2	6:07	Multiple bombs explode in the Spring Garden Center Station.
3	6:08	The Philadelphia Transportation Authority control center notices loss of video and data communications with the Spring Garden Station.
4	6:10	The Philadelphia Transportation Authority informs the Philadelphia Emergency Operations Center that a problem has occurred and the public should avoid the subway station.
5	6:12	The Philadelphia Emergency Operations Center's CAP console operator sends the message to IPAWS.
6	6:15	IPAWS verifies the message, and the message formatted in Commercial Mobile Alert Reference Point C (CMAC) is sent to the CMSP Gateway.
7	6:22	The cell phone providers receive the CMAS message and then broadcast the message to appropriate territory based on agreed to level of support.
8	6:24	Mobile device subscribers receive the message.
9	6:25	The message displays on mobile devices.
10	7:30	The president orders an alert for the entire nation.
11	7:31	The FOC receives the presidential alert.
12	7:33	The FOC's CAP console operator sends the message to IPAWS.
		(Repeat of Steps 6–9)
13	7:36	IPAWS verifies the message, and the CAP message is sent to the CMAS Alert Aggregator.
14	7:45	The cell phone providers receive the CMAS message and then broadcast the message to appropriate territory based on agreed to level of support.
15	7:47	Mobile device subscribers receive the message.
16	7:48	The message displays on mobile devices.

3.1.3 Illustration of the Terrorist Threat Mission Thread

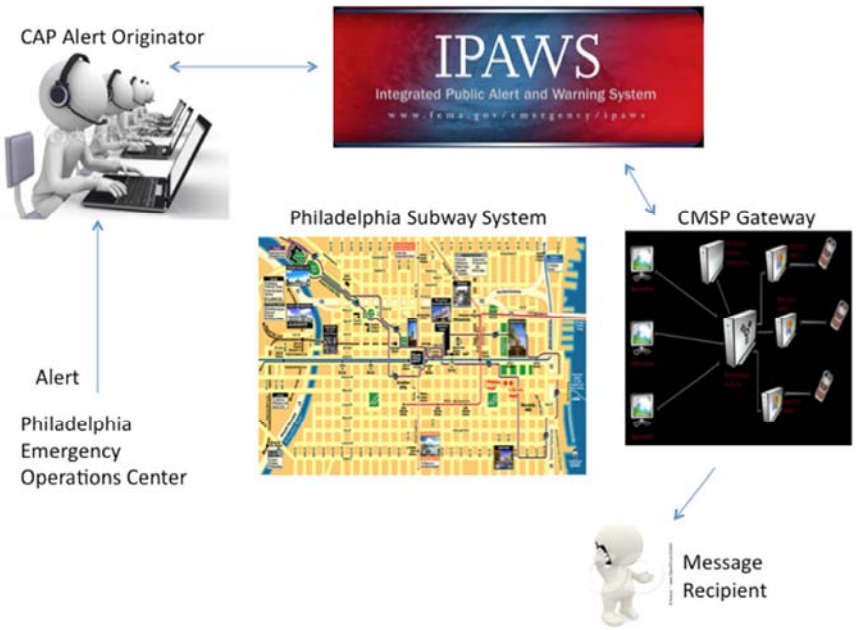


Figure 2: Context Diagram for Terrorist Mission Thread

3.2 Weather Mission Thread

We will use the CMAS operational weather mission thread to conduct several mission thread analyses with respect to two characteristics: cyber security and resilience (see Appendix A.2 for the complete scenario). This mission thread will be the basis for stakeholder exploration of CMAS utility in a weather scenario. We will validate it with stakeholder workshop activities.

The following sections summarize the weather mission thread in three parts: a vignette, a summary set of steps taken from the mission thread, and a diagram illustrating the context of the incident described in the mission thread (Figure 3).

3.2.1 The Weather Mission Thread Vignette

Rutherford County is located in central Tennessee. According to its website, “The Rutherford County Emergency Management Agency (RC EMA) is charged with the overall responsibility of coordinating the county's preparedness for and response to disasters. Geographically, its authority extends to the entire county as defined by state law TCA 58-2-110. . . . This agency combines the local resources of Rutherford County, the City of Murfreesboro, the Town of Smyrna, and the City of LaVergne; along with State and Federal resources” [Rutherford County 2008]. RC EMA uses Facebook, Twitter, and Nixle as well as IPAWS to distribute emergency information to residents [Rutherford County 2008]. Both Nixle and CMAS will send information via cell phones. Nixle is an “opt-in” service, requiring subscribers to take action to be included in the alert process. Multiple cell phone providers provide coverage for the county. FEMA has set up IPAWS to support the East Coast of the United States. FEMA also has an FOC and a regional emergency operations center that covers the East Coast. For this vignette, RC EMA is the CAP alert originator.

3.2.1 The Weather Mission Thread Steps

Table 3 contains a set of steps taken from the mission thread scenario for a weather threat. The elaborated mission thread table appears in Appendix A.2. The "Comments" contained in some steps provide example issues that we may need to explore with the stakeholders.

Table 3: Weather Threat Mission Steps

Mission Steps	Time	Description
1	12:05 a.m.	Severe Thunderstorm Warning is issued by the National Weather Service (NWS) for Rutherford County.
2	12:06	RC EMA receives the Severe Thunderstorm Warning. [Comments: How do staff receive the alert information? What procedures do they follow based on the warning/watch information?]
3	12:37	NWS upgrades warning to Tornado Watch for all of Rutherford County. [Comments: Do staff forward the watches, or do they wait for a Tornado Warning?]
4	12:38	RC EMA receives the Tornado Watch notification. [Comments: Does RC EMA receive alerts from NWS? If alerts go to Tennessee EMA (TEMA), who then alerts RC EMA? What procedures does RC EMA follow based on the warning/watch info staff receive? Do alerts for tornado watch go out to public?]
5	1:14	NWS upgrades to Tornado Warning for Rutherford County.
6	1:15	RC EMA receives the Tornado Warning. [Comments: How does RC EMA receive the alert information? What procedures do staff follow based on the warning/watch information?]
7	1:15	RC EMA Communications Coordinator begins to send out the information based on a developed procedure that prioritizes the information to IPAWS, Nixle, Facebook, and Twitter. [Comments: Are any distributions automated? What are the priorities?]
8	1:17	IPAWS verifies the message, and the CMAC-formatted message is sent to the CMSP Gateway.
9	1:17	Information is displayed on Facebook [Comments: Are recipients notified?] and received by mobile and other devices via Twitter and Nixle. [Comments: What is the timing of receiving the alerts?]
10	1:18	The cell phone providers receive the CMAS message and then broadcast the message to Rutherford County based on agreed to level of support.
11	1:19	Mobile device subscribers receive the message.
12	1:19	Message displays on mobile device.
13	1:25	NWS issues report of tornado on the ground in Rutherford County. [Comments: Does NWS do this, or does this usually come from news reports? Who initiates the local tornado sirens in different cities?]
14	1:26	RC EMA Communications Coordinator begins to send out the information based on a developed procedure that prioritizes the information to IPAWS, Nixle, Facebook, and Twitter. [Comments: Are any distributions automated? What are the priorities? Could CMAS be useful within this narrow time frame? Would NWS radio, TV/radio, etc. be better options?]
15–19	1:27–1:29	Repeat Steps 8–12
20	2:06	RC EMA director receives word from County Fire Chief of damaged areas that the public should avoid.
21	2:07	RC EMA Communications Coordinator begins to send out the information based on a developed procedure that prioritizes the information to IPAWS, Nixle, Facebook, and Twitter. [Comments: Are any distributions automated? What are the priorities?]
22–26	2:10–2:12	Repeat Steps 8–12
		[Comments: Would RC EMA send alert that Tornado Warning has ended?]

3.2.1 The Weather Mission Thread Illustration

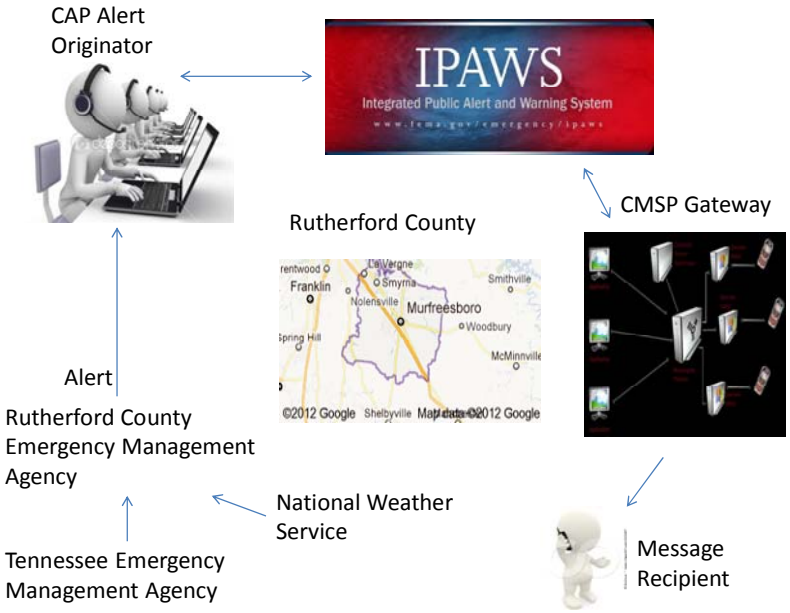


Figure 3: Context Diagram for Weather Mission Thread

3.3 Abduction Mission Thread

The following sections summarize the abduction mission thread in three parts: a vignette, a set of steps taken from the mission thread, and a picture illustrating the flow of the mission thread (Figure 4).

3.3.1 The Abduction Thread Vignette

A daycare on Arbor Road in Christiansburg, Virginia, has opened for child care and received 12 children, ages two to five, for the day. There are four staff members on duty, including the director. The staff and children are gathered in the playroom to start the daily program.

3.3.2 The Abduction Mission Thread Steps

Table 4 contains a set of steps taken from a mission thread scenario about an abduction. The elaborated mission thread table is included in Appendix A.3.

Table 4: Abduction Threat Mission Steps

Mission Steps	Time	Description
1	7:00 a.m.	Two people wearing black masks force their way into the daycare at gun point. One is carrying a photo and matching it to the children as the staff rush to collect and protect them. They push staff and children into the playroom across from the front entrance, which has one door and windows at the back.
2	7:05	The person with the photo grabs four-year-old Nancy and carries her out the door while she kicks and screams. He climbs into the back of a green SUV parked at the front door. Another person is in the driver seat.
3	7:07	At the same time, the second gunman pulls over the toy cabinets and kicks tables to block the daycare people in the back of the playroom, runs out the door, and jumps into the passenger side of the SUV as it moves out.

Mission Steps	Time	Description
4	7:09	Staff looking out the back window see the SUV turn right out of the parking lot, head down Arbor Road, and turn left in the direction of U.S. 460. They think the SUV turns west on U.S. 460, but trees obscure a clear view.
5	7:09	Director pushes tables out of her way, heads into the office, and calls the police via 911.
6	7:12	Director collects available information for the police (photo, description). Nancy's parents are undergoing a highly contentious divorce. The courts had previously notified the daycare not to release the child to the father because of the risk of abuse.
7	7:18	Christiansburg Police Department deputy officer picks up the call and rushes to the daycare. He was at a bank just down the road from the daycare.
8	7:22	Deputy officer takes the child's information from the director and calls the report into the police chief that this case meets the criteria for issuing an AMBER alert.
9	7:27	Police chief agrees and authorizes deputy officer to submit an AMBER alert for Montgomery and Giles counties to cover the towns connected by U.S. 460.
10	7:32	Deputy officer uses his car's workstation to send the data required for the AMBER alert to the command center at the police station.
11	7:35	The command center officer on duty faxes the information to the National Center for Missing & Exploited Children to have the missing child added to the National Crime Information Center database, logs on to the alert aggregator system, and copies the data sent by the deputy director into the appropriate data fields to submit the CAP message to IPAWS.
12	7:40	IPAWS verifies the message, and the CAP message is sent to the CMAS Alert Aggregator, which sends it to the Federal Alert Gateway, which in turn sends a CMAC-formatted message to the CMSP Gateway.
13	7:50	The cell phone providers receive the CMAS message and then broadcast the message to cell phones in the selected counties.
14	8:00	A message recipient seated at a Burger King near U.S. 460 sees a vehicle that fits the description of the SUV headed west on U.S. 460 and calls the police to report the vehicle location.
15	8:30	Police set up a roadblock at the Montgomery County line. As the SUV approaches, it does a U-turn and heads in the opposite direction. The police give chase and apprehend the vehicle, arresting the three men (the child's father is driving) and recovering the child, who is scared but uninjured.

3.3.3 The Abduction Mission Thread Illustration

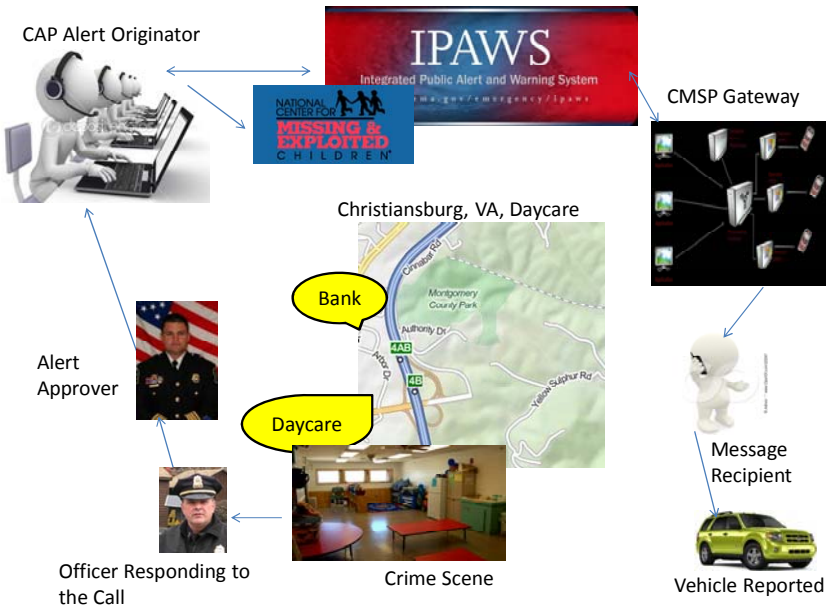


Figure 4: Context Diagram for AMBER Alert Mission Thread

3.4 CMAS Adoption Mission Thread

Appendix A.4 presents a development mission thread concerning CMAS adoption that we will use to conduct several mission thread analyses with respect to two technical characteristics (cyber security and resilience) and four program management characteristics (budget, schedule, resource allocation, and organizational relationships). This mission thread will be the basis for stakeholder exploration of CMAS adoption issues and barriers. We will validate it with stakeholder workshop activities.

The following sections summarize the adoption mission thread in three parts: a vignette, a set of steps taken from the mission thread, and an illustrating concept of the incident described in the mission thread (Figure 5).

3.4.1 The Adoption Thread Vignette

The County Emergency Management Agency (EMA) is responsible for ongoing 24-hour operations servicing

- one federal EMA
- one state EMA
- one city Transportation Authority control center (bus and light rail)
- one city EMA (fire, police, HazMat, emergency medical services [EMS], and river rescue)
- one university campus with its own police force
- three boroughs with fire and police forces
- local utilities (water, gas, and electric)

- local industries with hazardous materials

One of the County EMA's objectives is to issue imminent threat and AMBER alerts for dissemination to recipients in affected areas. The alerts must be accurate, timely, and usable, informing recipients of recommended actions to take. FEMA has set up IPAWS to support aggregation and dissemination of such alerts. One capability is CMAS, by which EMAs send approved alerts to CMSPs in the appropriate area, which then broadcast them to mobile devices within a specified geographic area. The County EMA has acquisition and integration processes in place that it will use to evaluate and implement the CMAS capability.

3.4.1 The Adoption Mission Thread Steps

Table 5 contains a set of steps taken from a mission thread scenario for adoption. The elaborated mission thread table appears in Appendix A.4.

Table 5: Adoption Mission Steps

Mission Steps	Start Time	Description
1	Day 1	County EMA management initiates study of CMAS usefulness to organization.
2	Day 8	Based on the initial CMAS study, County EMA management initiates feasibility assessment of CMAS adoption. *This is a high-level assessment, done before determining eligibility and requirements.*
3	Day 23	County EMA management reviews the initial approach developed by the CMAS feasibility team and provides concurrence to proceed.
4	Day 24	CMAS feasibility team initiates technical and acquisition efforts based on plan.
5	Day 38	County EMA management receives update from CMAS feasibility team and provides guidance.
6	Day 52	CMAS feasibility team provides assessment to County EMA management.
7	Day 55	County EMA management completes agreement paperwork with FEMA (e.g., memorandum of agreement).
8	Day 66	County EMA management accepts the plan to incorporate CMAS into their operations and authorizes the commitment of funding and staff to proceed.
9	Day 68	County EMA issues a request for quotation (RFQ) for integrating CMAS into its operations.
10	Day 89	County EMA receives bids and begins evaluation process.
11	Day 110	County EMA selects proposal and executes a contract.
12	Day 111	County EMA staff begin developing the CMAS rollout plan.
13	Day 111	County EMA staff define and plan the integration activities needed for the CMAS capability.
14	Day 111	County EMA staff begin developing a risk management plan for the integration effort using risks identified in the feasibility analysis and the vendor evaluation process.
15	Day 131	County EMA staff begin executing integration plan.
16	Day 140	County EMA staff perform technical acceptance activities with their vendor and complete any changes and corrections.
17	Day 147	County EMA begin executing the CMAS rollout plan.
18	Day 154	Deploy and monitor CMAS integration (preconditions: (a) CMAS capability has been communicated and training has occurred, and (b) CMAS is deployed and has fully checked out in operating environment).
19	Day 168	County EMA CMAS capability goes live.

3.4.1 The Adoption Mission Thread Illustration

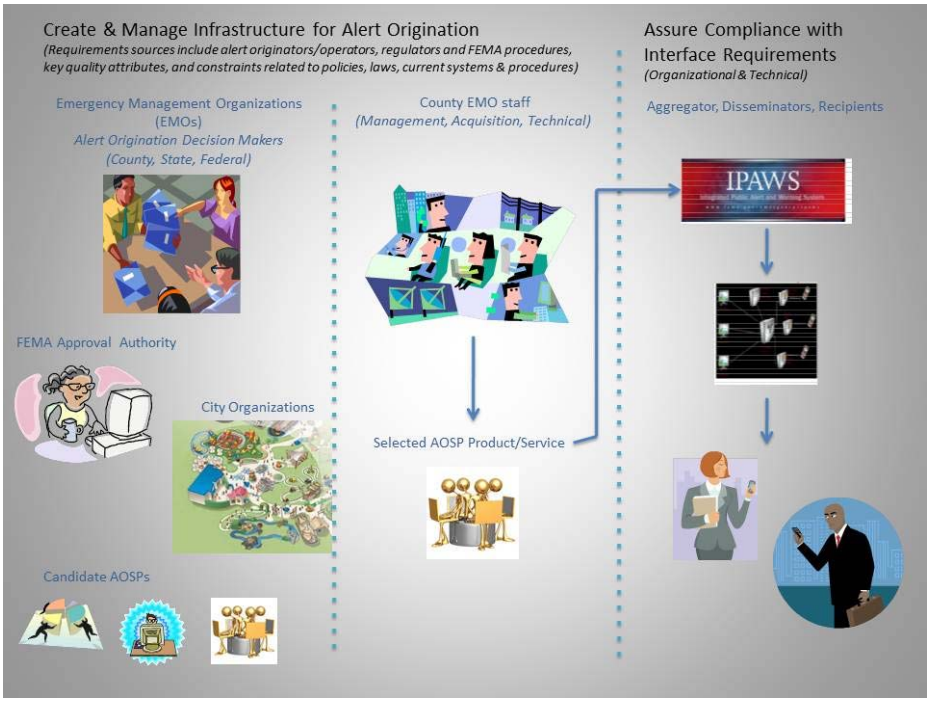


Figure 5: Context Diagram for CMAS Adoption Mission Thread

3.5 Collaborator-Provided Scenarios

The County of San Diego Office of Emergency Services (OES) generously contributed scenarios that they have developed to exercise and maintain their preparedness. Appendix B provides a CMAS Users Trial After-Action Report and a list of alert types classified by handling, status, response type, category, severity, urgency, and certainty.

4 The Quality Attribute Scenarios

In contrast with the top-down approach to mission thread scenarios, we took two different bottom-up approaches for deriving the QA scenarios. First, we analyzed eight RFQs for alert-origination support systems and extracted implicit or explicit QA requirements in these RFQs. Second, we reverse engineered QA scenarios from stakeholder interviews with members of the County of San Diego OES, interviews with other participating organizations, and the first CMAS Forum Workshop. Many of the issues and challenges that participants expressed during interviews are related to feature shortfalls that alert originators perceived in the CMAS design. While these inform CMAS enhancement research, they do not bear directly on the challenges of integrating the present set of CMAS capabilities. However, some of the issues provide concrete examples of matters that must be addressed for successful CMAS integration.

The intersection of these two investigation paths produced QA-linked cross-references to allow further probing for CMAS integration challenges. For example, QAs that appear in both sources are likely to be hard challenges in the marketplace because RFQs are asking for the QA while stakeholders see that same QA as a challenge. On the other hand, QAs that are unique to the interview path may represent challenges that have not found their way back to the RFQ mechanism[1] (the mitigation path that brings the vendor community's resources to bear on the challenge).

The systematic development of QA scenarios supports the analysis of many aspects of the software product and feeds into the higher level analysis associated with mission threads. The steps in a mission thread provide the context for discussing individual qualities and their effects on the overall quality of the system. The QA scenarios presented in this section provide a basis to probe issues and challenges that others have seen or anticipate.

As mentioned earlier, functional requirements specify which functions a system must provide to meet stated and implied user needs. For example, "The system shall allow users to send alert messages." Functionality specification is relatively easy to control and in our experience does not present a high risk for the integration strategy. On the other hand, the QA requirements indicate the degrees to which a system must exhibit various quality properties and often are associated with integration challenges. For example, a sample list of nonfunctional requirements that specify levels of QAs for a system might include the following:

- Availability: The system shall recover from a processor crash within one second.
- Portability: The system shall allow the user interface to be ported to a new platform within six months.
- Performance: The system shall process sensor input within one second.
- Security: The system shall deny access to unauthorized users 100% of the time.
- Testability: The system shall allow a user to test connectivity with a communication link within five minutes.

[1] The RFQs are a mixture of CMAS-specific solicitations and more general alert-originator supporting systems. We conducted the interviews before the activation of CMAS, so interviewees can only speculate about anticipated issues. Nevertheless, improvement of QAs requested in RFQs will facilitate CMAS integration.

- Usability: The system shall allow users to cancel an operation within one second.
- Capacity: The system shall have a maximum of 50% utilization of the central processing unit.

4.1 Sample Quality Attribute Scenarios for CMAS

QA scenarios provide a mechanism to further define and illustrate the requirements for specific QA levels, thus enabling better control of these elusive properties. To date, our bottom-up derivation has produced a set of QA scenarios applicable to CMAS originator systems. The QA scenarios presented here illustrate the pattern for illumination of issues that could be associated with particular mission thread steps.

The tables containing the scenarios are structured as follows:

- Scenario: A brief statement of an interaction with a system under given conditions and the response of the system. This is similar to a "user story" specifying functionality, but with inclusion of at least one QA.
- Stimulus, stimulus source, environment, artifact, response, and response measure: As we described in Section 2.1, these entries decompose important elements of the scenario.
- Business goals: Business- or mission-oriented rationale for satisfying this scenario.
- Quality attributes: A high-level classification of a quality that this scenario might represent.
- Notes: Optional comments on the scenario.

4.1.1 Availability

Table 6: Availability Through Natural Disaster

Scenario	**An earthquake has rendered the Office of Emergency Services unsafe to enter, and the primary CMAS server has become inactive. CMAS capabilities are seamlessly transferred to an alternative physical location and alternative command authority within 30 minutes.**
Stimulus	Site-monitor-component listener determines that primary site is no longer active.
Stimulus source	Site-monitor component
Environment	CMAS primary site shuts down unexpectedly.
Artifact	Site-monitor component
Response	The site-monitor component sends a message to notify the administrator that the primary site is down. The administrator takes steps to ensure that capabilities are operational within 30 minutes.
Response measure	Full operational capabilities within 30 minutes of incident
Business goals	Continuous operations
Quality attributes	Availability (passive redundancy and failover)

4.1.2 Reliability

Table 7: Reliability During Nominal Operations

Scenario	**Most of the time there is no emergency, and the center is either idle or handling routine maintenance. The center should be operational during these times. An incident occurs, requires an alert, and is processed within *x* minutes.**
Stimulus	New alert comes into an idle emergency center.
Stimulus source	An emergency responder in the jurisdiction
Environment	The center has been operational for several months and had its last exercise a month ago.
Artifact	The text of the alert
Response	The message is entered into the originating software, successfully validated, and issued.
Response measure	How quickly the message was ready to send after being received during an idle period
Business goals	99.99% uptime, ability to initiate messages 24/7
Quality attributes	Reliability, availability

Table 8: Reliability Under Emergency Conditions

Scenario	**A chemical spill has occurred and is causing a toxic cloud to spread. An alert is issued for citizens in the path of the cloud. A shift in wind endangers a different locale. A new alert is issued for the new location, and a cancelation is issued for the original alert. The alerting system allows the operator to reuse the original message in the new alert and tracks all alerts that are active.**
Stimulus	The emergency operations center receives situation reports from the field.
Stimulus source	Incident commander in the field
Environment	The center is in operational mode.
Artifact	Multiple alerts
Response	Correct messages are sent in the correct order.
Response measure	The appropriate audience receives messages in the correct sequence and in the appropriate time frames.
Business goals	Reliable management of sets of alerts
Quality attributes	Reliability

4.1.3 Access Control

Table 9: Information Security

Scenario	**An EMAs territory includes a nuclear power plant. Hackers attempt to represent themselves as an alert originator to corrupt an emergency notification about the power plant.**
Stimulus	A hacker attempts to log in to the emergency alert system using an injection technique.
Stimulus source	A hacker
Environment	The emergency management center has a high-speed internet connection through a local provider. The software requires a new password every 10 days.
Artifact	The hacker uses a fake web page that attracts one of the operators during an idle period. The web page collects login and password information from the EMA for later use.

Response	The originator software detects that the login attempt uses a 14-day-old password.
Response measure	The login is denied without providing access to any sensitive data.
Business goals	Unauthorized users cannot access the emergency alert system.
Quality attributes	Reliability, access control

4.1.4 Throughput

Table 10: Throughput During Emergency Notifications

Scenario	**An emergency message is sent out. Somewhere along the communication path, a performance bottleneck occurs. The CMAS system discovers the bottleneck, informs the originator, and provides information on alternative sending routes (if possible). At all times, the originators have a clear picture about the progress of sending the message.**
Stimulus	AMBER alert comes into the emergency center from the field.
Stimulus source	Local sheriff's office
Environment	CMAS originating software is in a nominal state.
Artifact	Information needed for the message
Response	Full set of messages is sent.
Response measure	The time required to send all applicable copies of the message
Business goals	CMAS must initiate 10,000 text messages per hour.
Quality attributes	Reliability, throughput

4.1.5 Testability

Table 11: Testability During an Exercise

Scenario	**A training exercise is executed using the CMAS system. The system allows the trainer to control the software system and the state of the system to ensure that the exercise covers as many aspects of system operation as the time allows.**
Stimulus	A series of actions defined in advance are requested using the menus of the system.
Stimulus source	Emergency manager
Environment	Realistic operating conditions are established.
Artifact	A deployed, operational CMAS origination system
Response	The system accepts and carries out the requested commands.
Response measure	The commands are carried out in a manner that satisfies the quality requirements.
Business goals	To ensure that the system is capable of all required actions under operational conditions
Quality attributes	Testability
Notes	Most exercises will not provide time to attempt actions in different sequences and with different timings.

4.1.6 Performance/Concurrent Processing

Table 12: Performance/Concurrent Processing of Multiple Alerts

Scenario	**A funnel cloud is spotted in the eastern part of the geographic area, and a CMAS warning is authorized and issued. A second funnel cloud is reported 3 minutes later in the same geographic area, and authorities determine that a second active CMAS message should be sent.**
Stimulus	Alert requests are generated by authorized users within 3 minutes of each other.
Stimulus source	Authorized user
Environment	Normal operating conditions (processing first request)
Artifact	IPAWS
Response	IPAWS processes a second active alert during the broadcast period of the first alert.
Response measure	IPAWS responds to the second alert within 5 seconds of receiving the request.
Business goals	Reliable operations and performance in times of system stress
Quality attributes	Performance/concurrent processing
Notes	[FCC 2007]

4.1.7 Usability

Table 13: Usability (Ability for User to Cancel a Request)

Scenario	**Parents reported that their child is missing. An AMBER alert was issued through CMAS. The child has now been found and is safe, so there is no imminent danger. The originator issues a cancelation of the alert that appears on all appropriately equipped cell phones in the geographic area.**
Stimulus	Cancelation request
Stimulus source	Originator selects cancelation button to generate cancelation event.
Environment	Normal operating conditions
Artifact	User interface event processor
Response	The AMBER alert cancelation appears on all appropriately equipped cell phones in the area.
Response measure	Recipients are notified within 2 seconds of cancelation request.
Business goals	Quick reaction to canceling event
Quality attributes	Usability (ability for user to cancel a request)
Note	[FCC 2007]

4.1.8 Sustainability

Table 14: Sustainability Through Integration

Scenario	**An incident occurs on a university campus that requires immediate notification of the campus community. Alerts are distributed through existing alert capabilities (telephone, short message service, email, website) and CMAS. Existing alert capabilities are used to support additional communications requirements, including special-needs communication, two-way communication, conferencing among key stakeholders, and language translation.**
Stimulus	A request to alert via a new media
Stimulus source	An alert recipient
Environment	The alert system is an aggregation of alerting software systems, each of which communicates via a specific medium.
Artifact	A new alerting system
Response	The new alerting system is integrated via a scripting environment that fires each system separately.
Response measure	A new alerting system is integrated in less than a person-month.
Business goals	Provide as many channels and modes for propagating alerts as possible.
Quality attributes	Sustainability

5 Summary and Future Directions

5.1 Summary to Date

As a major component of FEMA's IPAWS, CMAS plays a critical role in providing targeted alerts to a geographic area. As a system-of-systems implementation, CMAS crosses many organizations to accomplish its mission. Identifying the steps taken to respond to an incident across various system and organizational boundaries can help expose potential barriers and challenges to CMAS integration. We have organized these steps into an initial set of mission thread scenarios and QA scenarios. Operational mission threads predominantly inform security and organizational aspects of the integration strategy; development mission threads predominantly inform technical and acquisition aspects of the integration strategy; and QA scenarios illustrate nonfunctional aspects of the system such as latency, resilience, or scalability. QA scenarios also help illuminate issues in a given step of a mission thread. The ongoing analysis of these scenarios will help determine what challenges CMAS stakeholders may experience as part of this large-scale integration.

5.2 Future Directions

Our plan for initial elaboration of the mission thread scenarios is through workshop-style engagements. We will give the participating organization the mission threads as read-ahead material. Before the workshop, the organization will critique and modify the mission threads to make them more concrete to its own context. The workshop participants will then interactively drill down into the steps of the mission threads to identify issues, challenges, and barriers that inhibit CMAS adoption. As the mission threads mature through these workshop engagements, they will become useful artifacts with which to build self-help practices or shared resources that the community can leverage to improve standard operating procedures.

We will use the QA scenarios both to explore system-related issues in greater detail and to augment discussion about mission thread steps. Such discussions also frequently expose operational risks. Subsequent analysis can determine whether those risks will require a technical solution, an operational solution, or both.

The output derived from such scenario analysis will appear in the integration strategy, which will cover a variety of integration topics, including originator, aggregator, and disseminator issues; messaging standards; and security challenges, with a primary focus on originators. Figure 6 summarizes how we can use these scenarios to reveal issues and challenges across organizations and at the system level. The lessons, risks, and mitigations identified will inform the end product—the CMAS integration strategy.

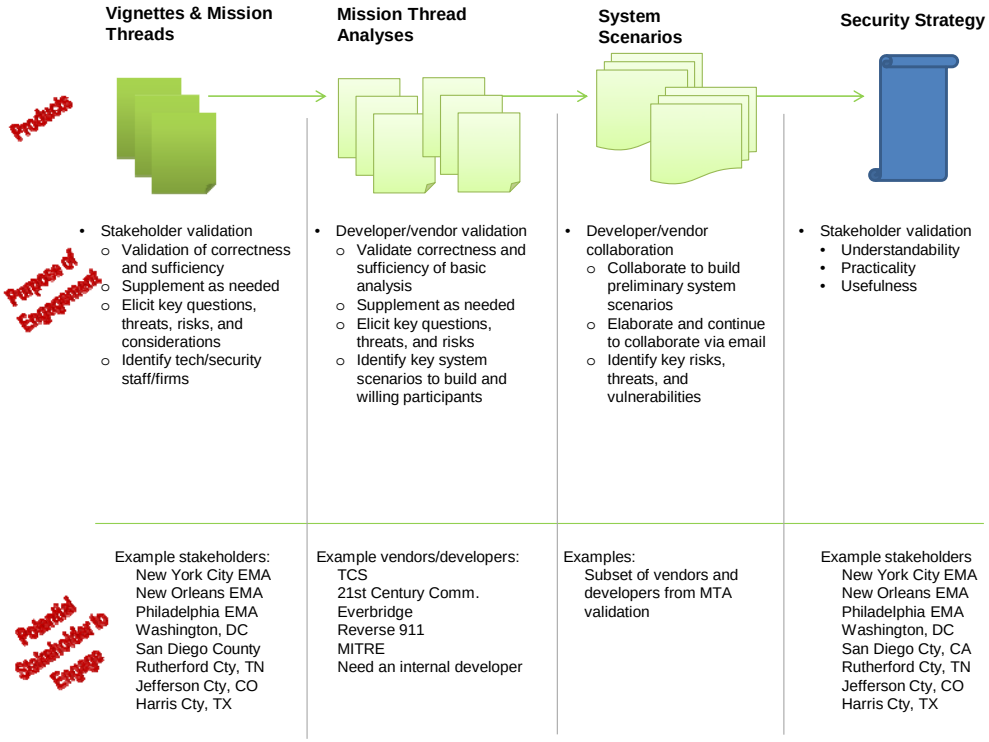


Figure 6: Summary of the Scenario Approach

Appendix A The Mission Thread Scenarios

A.1 Terrorist Threat Mission Thread

A.1.1 Introduction

This section describes an operational mission thread for CMAS that we will use to conduct several mission thread analyses with respect to two characteristics: cybersecurity and resilience. We will validate this mission thread with stakeholders through workshop activities.

A.1.2 Contents

- Vignette description, nodes/actors, assumptions, and context: Environment before the event
- Top-level mission thread (nominal conditions): Sequence of steps describing the event and the CMAS response
- List of extension steps: Mission thread steps representing off-nominal conditions
- Overarching QA considerations: Considerations and issues not captured in steps

Table 15: Terrorist Threat Mission Thread

Name	Philadelphia Subway Bombing
Vignette (summary description)	The Philadelphia subway system consists of both above- and below-ground stations. Multiple cell phone providers provide coverage for the city of Philadelphia. FEMA has set up IPAWS to support the East Coast of the United States. FEMA has an operations center (FOC) and a regional emergency operations center that covers the East Coast. For this vignette, a Philadelphia emergency operations center is the CAP alert originator.
Nodes/actors	Philadelphia Transportation Authority control center (alert identifier), Philadelphia Emergency Operations Center (CAP alert originator), IPAWS, cell phone service providers, cell phone subscribers, and the FOC
Assumptions	• No power disruptions besides where the bomb exploded • Normal weather conditions • Normal civil alert level • Required monthly test is handled in another mission thread. (Note: These messages may take as long as 24 hours to be sent over CMSP infrastructure.) • All CMAS system functions are available and operational. • IPAWS consists of the IPAWS Open Platform for Emergency Networks (OPEN) Gateway, CMAS Alert Aggregator, and Federal Alert Gateway. *Note: These are just example assumptions; there would likely be more.*

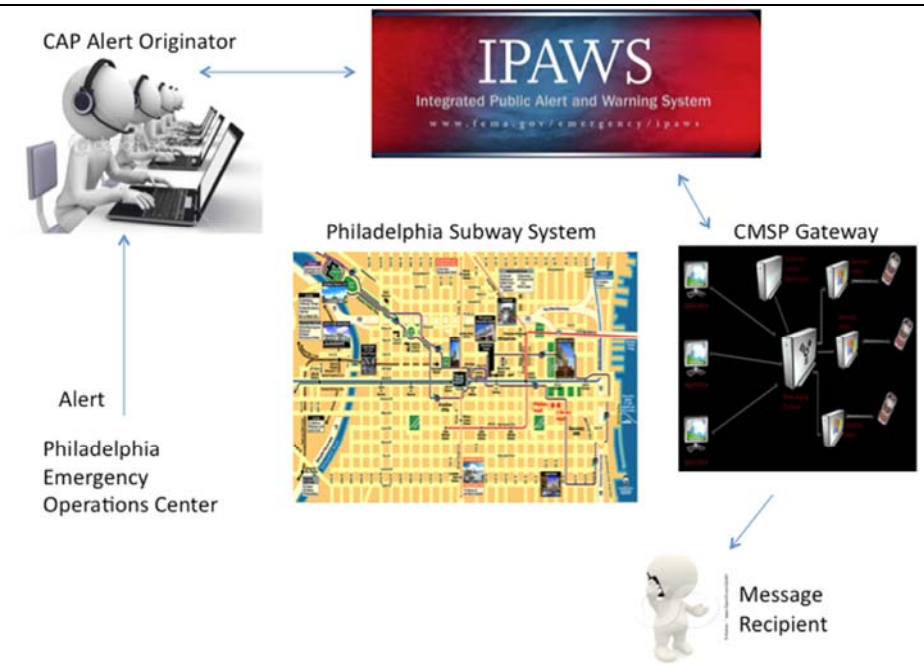
Environmental context diagram	

Table 16: Terrorist Thread Mission Steps

Mission Steps	Time	Description	Engineering Considerations, Issues, and Challenges
1	6:05 a.m.	The Main Street train has just left the Spring Garden Center Station.	Resilience: Performance: Cybersecurity:
2	6:07	Multiple bombs explode in the Spring Garden Center Station.	Resilience: Performance: Cybersecurity:
3	6:08	The Philadelphia Transportation Authority control center notices loss of video and data communications with the Spring Garden Station.	Resilience: Performance: Cybersecurity:
4	6:10	The Philadelphia Transportation Authority informs the Philadelphia Emergency Operations Center that a problem has occurred and the public should avoid the subway station.	Resilience: Performance: Cybersecurity:
5	6:12	The Philadelphia Emergency Operations Center's CAP console operator sends the message to IPAWS.	Resilience: Performance: Cybersecurity:

Mission Steps	Time	Description	Engineering Considerations, Issues, and Challenges
6	6:15	IPAWS verifies the message, and a CMAC-formatted message is sent to the CMSP Gateway.	Resilience: Performance: Cybersecurity:
7	6:22	The cell phone providers receive the CMAS message and then broadcast the message to appropriate territory based on agreed to level of support.	Resilience: Performance: Cybersecurity:
8	6:24	Mobile device subscribers receive the message.	Resilience: Performance: Cybersecurity:
9	6:25	The message displays on mobile devices.	Resilience: Performance: Cybersecurity:
10	7:30	The president orders an alert for the entire nation.	Resilience: Performance: Cybersecurity:
11	7:31	The FOC receives the presidential alert.	Resilience: Performance: Cybersecurity:
12	7:33	The FOC's CAP console operator sends the message to IPAWS.	Resilience: Performance: Cybersecurity:
		(Repeat of Steps 6–9)	
13	7:36	IPAWS verifies the message, and the CAP message is sent to the CMAS Alert Aggregator.	Resilience: Performance: Cybersecurity:
14	7:45	The cell phone providers receive the CMAS message and then broadcast the message to appropriate territory based on agreed to level of support.	Resilience: Performance: Cybersecurity:

Mission Steps	Time	Description	Engineering Considerations, Issues, and Challenges
15	7:47	Mobile device subscribers receive the message.	Resilience: Performance: Cybersecurity:
16	7:48	The message displays on mobile devices.	Resilience: Performance: Cybersecurity:
N			

Table 17: Terrorist Thread Extension Steps

Extension Steps	Time	Description of Extension Step (Off-nominal Condition for Mission Step)	Failure Expectations/Behavior for Extension Step
Step 5A		The Philadelphia Emergency Operations Center is unable to successfully send the CAP message to the IPAWS-OPEN Gateway.	
Step 6A		The IPAWS-OPEN Gateway is not operational (off-line).	
Step 6B		The IPAWS-OPEN Gateway determines that the CAP message is invalid.	
Step 6C		The IPAWS-OPEN Gateway is unable to successfully send the CAP message to the CMAS Alert Aggregator.	
Step 6D		A subset of the CMAS Alert Aggregators is not operational (off-line).	
Step 6E		A CMAS Alert Aggregator determines that the CAP message is invalid.	
Step 6F		A CMAS Alert Aggregator is unable to successfully send the CAP message to the Federal Alert Gateway.	
Step 6G		A subset of the Federal Alert Gateway is not operational (off-line).	
Step 6H		A Federal Alert Gateway determines that the CAP message is invalid.	
Step 6I		A Federal Alert Gateway is unable to successfully send a translated CAP-formatted message (now in CMAC protocol) to the CMSP Gateways.	
Step 7A		A subset of a provider's CMSP Gateway is not operational (off-line).	
Step 7B		All of a provider's CMSP Gateways are not operational (off-line), but other providers' CMSP Gateways are operational.	
Step 7C		A provider's CMSP Gateway determines that the CMAC-formatted message is invalid.	
Step 7D		A provider's CMSP Gateway is unable to successfully send the message to the mobile device subscribers.	
Step 8A		Mobile device determines that the CMAS message is invalid.	
N			

Table 18: Quality Attributes for Terrorist Threat Mission Thread

Quality Attribute	Overarching (End-to-End) Considerations, Issues, and Challenges*
Resilience	
Performance	
Security	
N	

* Items include constraints, requirements, and concerns raised through workshop activities that affect the end-to-end mission thread.

A.2 Weather Mission Thread

A.2.1 Introduction

This section describes an operational mission thread for CMAS that we will use to conduct several mission thread analyses with respect to two characteristics: cybersecurity and resilience. We will validate this mission thread with stakeholders through workshop activities.

A.2.2 Contents

- Vignette description, nodes/actors, assumptions, and context: Environment before the event
- Top-level mission thread (nominal conditions): Sequence of steps describing the event and the CMAS response
- List of extension steps: Mission thread steps representing off-nominal conditions
- Overarching QA considerations: Considerations and issues not captured in steps

Table 19: Weather Mission Thread

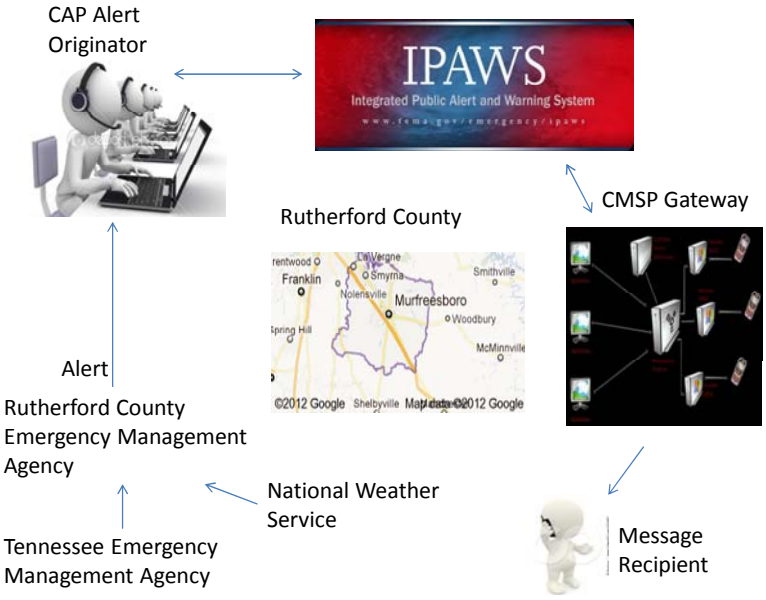
Name	Rutherford County Tornado
Vignette (summary description)	Rutherford County is located in central Tennessee. **"**The Rutherford County Emergency Management Agency [RC EMA] is charged with the overall responsibility of coordinating the county's preparedness for and response to disasters. Geographically, its authority extends to the entire county as defined by state law TCA 58-2-110. . . . This agency combines the local resources of Rutherford County, the City of Murfreesboro, the Town of Smyrna, and the City of LaVergne; along with State and Federal resources" [Rutherford County 2008]. RC EMA uses Facebook, Twitter, and Nixle as well as IPAWS to distribute emergency information to residents. Both Nixle and CMAS will send information via cell phones. Nixle is an opt-in service. Multiple cell phone providers provide coverage for the county. FEMA has set up IPAWS to support the East Coast of the United States, with a FOC and a regional emergency operations center that covers the East Coast. For this vignette, RC EMA is the CAP alert originator.
Nodes/actors	NWS (alert identifier), RC EMA (CAP alert originator), IPAWS, cell phone service providers, cell phone subscribers, Tennessee Emergency Management Agency (TEMA), County Fire Chief, and other emergency personnel
Assumptions	• NWS issues original warning. • RC EMA relies on NWS for alerts and does not issue alerts based on local news channels. [Comment: What role does TEMA play, if any?] • Connectivity to internet by RC EMA • All systems used by RC EMA are available and operational. • All CMAS system functions are available and operational. • IPAWS consists of the IPAWS-OPEN Gateway, CMAS Alert Aggregator, and Federal Alert Gateway. • Ready TN is available (TEMA's mobile, smartphone application, which provides location-based information on severe weather, road conditions, open shelters, and local government contacts; available for Android market, with iPhone application in development). • RC EMA is registered with NWS and/or TEMA to receive the information in a secure process. *Note: These are just example assumptions; there would likely be more.*
Environmental context diagram	

Table 20: Weather Thread Mission Steps

Mission Steps	Time	Description	Engineering Considerations, Issues, and Challenges
1	12:05 a.m.	Severe Thunderstorm Warning is issued by the NWS for Rutherford County.	Resilience: Performance: Security:
2	12:06	RC EMA receives the Severe Thunderstorm Warning. [Comments: How do staff receive the alert information? What procedures do they follow based on the warning/watch information?]	Resilience: Performance: Security:
3	12:37	NWS upgrades warning to Tornado Watch for all of Rutherford County. [Comments: Do staff forward the watches, or do they wait for a Tornado Warning?]	Resilience: Performance: Security:
4	12:38	RC EMA receives the Tornado Watch notification. [Comments: Does RC EMA receive alerts from NWS? If alerts go to TEMA, who then alerts RC EMA? What procedures does RC EMA follow based on the warning/watch info received? Do alerts for tornado watch go out to public?]	Resilience: Performance: Security:
5	1:14	NWS upgrades to Tornado Warning for Rutherford County.	Resilience: Performance: Security:
6	1:15	RC EMA receives the Tornado Warning. [Comments: How does RC EMA receive the alert information? What procedures do staff follow based on the warning/watch information?]	Resilience: Performance: Security:
7	1:15	RC EMA Communications Coordinator begins to send out the information based on a developed procedure that prioritizes the information to IPAWS, Nixle, Facebook, and Twitter. [Comments: Are any distributions automated? What are the priorities?]	Resilience: Performance: Security:
8	1:17	IPAWS verifies the message, and a CMAC-formatted message is sent to the CMSP Gateway.	Resilience: Performance: Security:
9	1:17	Information is displayed on Facebook [Comments: Are recipients notified?] and received by mobile and other devices via Twitter and Nixle. [Comments: What is the timing of receiving the alerts?]	Resilience: Performance: Security:

Mission Steps	Time	Description	Engineering Considerations, Issues, and Challenges
10	1:18	The cell phone providers receive the CMAS message and then broadcast the message to Rutherford County based on agreed to level of support.	Resilience: Performance: Security:
11	1:19	Mobile device subscribers receive the message.	Resilience: Performance: Security:
12	1:19	Message displays on mobile device.	Resilience: Performance: Security:
13	1:25	NWS issues report of tornado on the ground in Rutherford County. [Comments: Does NWS do this, or does this usually come from news reports? Who initiates the local tornado sirens in different cities?]	Resilience: Performance: Security:
14	1:26	RC EMA Communications Coordinator begins to send out the information based on a developed procedure that prioritizes the information to IPAWS, Nixle, Facebook, and Twitter. [Comments: Are any distributions automated? What are the priorities? Could CMAS be useful within this narrow time frame? Would NWS radio, TV/radio, etc. be better options?]	Resilience: Performance: Security:
15–19	1:27–1:29	Repeat Steps 8–12	Resilience: Performance: Security:
20	2:06	RC EMA director receives word from County Fire Chief of damaged areas to avoid.	Resilience: Performance: Security:
21	2:07	RC EMA Communications Coordinator begins to send out the information based on a developed procedure that prioritizes the information to IPAWS, Nixle, Facebook, and Twitter. [Comments: Are any distributions automated? What are the priorities?]	Resilience: Performance: Security:
22–26	2:10–2:12	Repeat Steps 8–12	
…		[Comments: Would RC EMA send alert that Tornado Warning has ended?]	
N			

Table 21: Weather Thread Extension Steps

Extension Steps	Time	Description of Extension Step (Off-nominal Condition for Mission Step)	Failure Expectations/Behavior for Extension Step
Step 7A		The RC EMA is unable to successfully send the CAP message to the IPAWS-OPEN Gateway.	
Step 8A		The IPAWS-OPEN Gateway is not operational (off-line).	
Step 8B		The IPAWS-OPEN Gateway determines that the CAP message is invalid.	
Step 8C		The IPAWS-OPEN Gateway is unable to successfully send the CAP message to the CMAS Alert Aggregator.	
Step 8D		A subset of the CMAS Alert Aggregators is not operational (off-line).	
Step 8E		A CMAS Alert Aggregator determines that the CAP message is invalid.	
Step 8F		A CMAS Alert Aggregator is unable to successfully send the CAP message to the Federal Alert Gateway.	
Step 8G		A subset of the Federal Alert Gateway is not operational (off-line).	
Step 8H		A Federal Alert Gateway determines that the CAP message is invalid.	
Step 8I		A Federal Alert Gateway is unable to successfully send a translated CAP-formatted message (now in CMAC protocol) to the CMSP Gateways.	
Step 10A		A subset of a provider's CMSP Gateways is not operational (off-line).	
Step 10B		All of a provider's CMSP Gateways are not operational (off-line), but other providers' CMSP Gateways are operational.	
Step 10C		A provider's CMSP Gateway determines that the CMAC-formatted message is invalid.	
Step 10D		A provider's CMSP Gateway is unable to successfully send the message to the mobile device subscribers (for any reason, including cell towers are down).	
Step 11A		Mobile device determines that the CMAS message is invalid.	
N			

Table 22: Quality Attributes for Weather Threat Mission Thread

Quality Attribute	Overarching (End-to-End) Considerations, Issues, and Challenges*
Resilience	
Performance	
Security	
N	

* Items include constraints, requirements, and concerns raised through workshop activities that affect the end-to-end mission thread.

A.3 Abduction Mission Thread

A.3.1 Introduction

This section describes an operational abduction mission thread for CMAS that we will use to conduct several mission thread analyses with respect to two characteristics: cybersecurity and resilience. We will validate this mission thread with stakeholders through workshop activities.

A.3.2 Contents

- Vignette description, nodes/actors, assumptions, and context: Environment before the event
- Top-level mission thread (nominal conditions): Sequence of steps describing the event and the CMAS response
- List of extension steps: Mission thread steps representing off-nominal conditions
- Overarching QA considerations: Considerations and issues not captured in steps

Table 23: Abduction Mission Thread

Name	Christiansburg Daycare Kidnapping
Vignette (summary description)	A daycare on Arbor Road in Christiansburg, VA, has opened for child care and received 12 children ages 2–5 for the day. There are four staff on duty, including the director. The staff and children are gathered in the playroom to start the daily program.
Nodes/actors	Police Deputy (alert identifier), Police Chief (alert approver), Christiansburg Police Department (CAP alert originator), IPAWS, cell phone service providers, cell phone subscribers
Assumptions	• The daycare has the ability to enter missing child information into the National Crime Information Center (NCIC) system. All systems used by the National Center for Missing & Exploited Children (NCMEC) are available and operational. • Once law enforcement has determined that the abducted child's case meets their local, regional, or statewide/territorial program's criteria, an AMBER alert is issued via IPAWS to EAS, radio, television, and CMAS. • There is reasonable belief by law enforcement that an abduction has occurred. • The abduction is of a child age 17 or younger. • The law-enforcement agency believes that the child is in imminent danger of serious bodily injury or death. • There is enough descriptive information about the victim and abduction for law enforcement to issue an AMBER alert to assist in the recovery of the child. • The child's name and other critical data elements, including the Child Abduction flag, have been entered into the NCIC database available via the internet by NCMEC. • Law enforcement notifies NCMEC when an AMBER alert is released for a specific geographic area. Once NCMEC validates the AMBER alert, it is entered into a secure system and transmitted to authorized secondary distributors for dissemination to customers within the specified geographic areas. All systems used by NCMEC are available and operational. • The Christiansburg police have a central IPAWS entry capability at the police station. • All CMAS system functions are available and operational. • IPAWS consists of the IPAWS-OPEN Gateway, CMAS Alert Aggregator, and Federal Alert Gateway. *Note: These are just example assumptions; there would likely be more.*

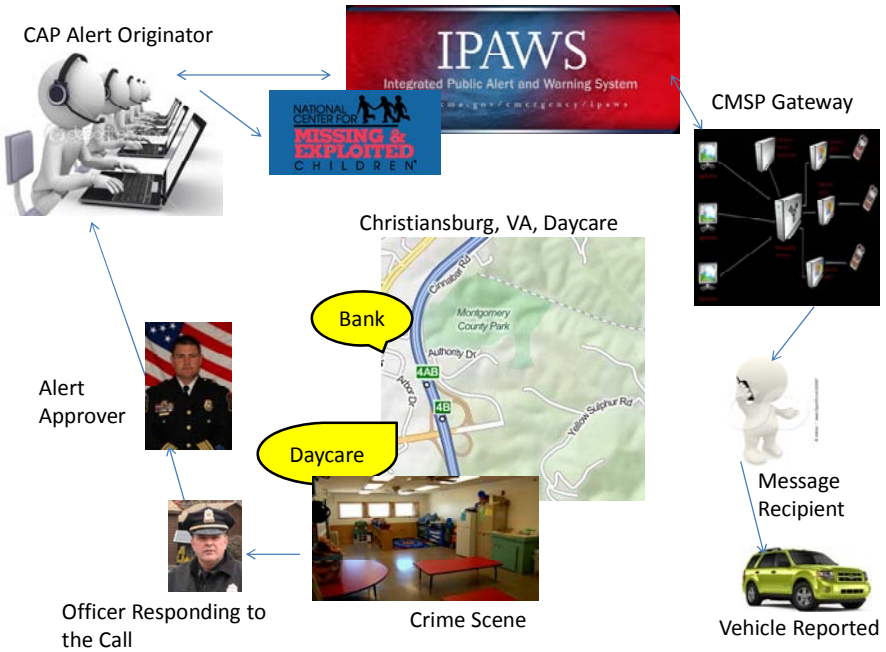
Environmental context diagram	

Table 24: Abduction Thread Mission Steps

Mission Steps	Time	Description	Engineering Considerations, Issues, and Challenges
1	7:00 a.m.	Two people wearing black masks force their way into the daycare at gun point. One is carrying a photo and matching it to the children as the staff rush to collect and protect them. They push staff and children into the playroom across from the front entrance, which has one door and windows at the back.	Resilience: Performance: Security:
2	7:05	The person with the photo grabs four-year-old Nancy and carries her out the door while she kicks and screams. He climbs into the back of a green SUV parked at the front door. Another person is in the driver seat.	Resilience: Performance: Security:
3	7:07	At the same time, the second gunman pulls over the toy cabinets and kicks tables to block the daycare people in the back of the playroom, runs out the door, and jumps into the passenger side of the SUV as it moves out.	Resilience: Performance: Security:
4	7:09	Staff looking out the back window see the SUV turn right out of the parking lot, head down Arbor Road, and turn left in the direction of U.S. 460. They think the SUV turns west on U.S. 460, but trees obscure a clear view.	Resilience: Performance: Security:

Mission Steps	Time	Description	Engineering Considerations, Issues, and Challenges
5	7:09	Director pushes tables out of her way, heads into the office, and calls the police via 911.	Resilience: Performance: Security:
6	7:12	Director collects available information for the police (photo, description). Nancy's parents are undergoing a highly contentious divorce. The courts had previously notified the daycare not to release the child to the father because of the risk of abuse.	Resilience: Performance: Security:
7	7:18	Christiansburg Police Department deputy officer picks up the call and rushes to the daycare. He was at a bank just down the road from the daycare.	Resilience: Performance: Security:
8	7:22	Deputy officer takes the child's information from the director and calls the report into the police chief that this case meets the criteria for issuing an AMBER alert.	Resilience: Performance: Security:
9	7:27	Police chief agrees and authorizes deputy officer to submit an AMBER alert for Montgomery and Giles counties to cover the towns connected by U.S. 460.	Resilience: Performance: Security:
10	7:32	Deputy officer uses his car's workstation to send the data required for the AMBER alert to the command center at the police station.	Resilience: Performance: Security:
11	7:35	The command center officer on duty faxes the information to NCMEC to have the missing child added to the NCIC database, logs on to the alert aggregator system, and copies the data sent by the deputy director into the appropriate data fields to submit the CAP message to IPAWS.	Resilience: Performance: Security:
12	7:40	IPAWS verifies the message, and the CAP message is sent to the CMAS Alert Aggregator, which sends it to the Federal Alert Gateway, which in turn sends the CMAC-formatted message to the CMSP Gateway.	Resilience: Performance: Security:
13	7:50	The cell phone providers receive the CMAS message and then broadcast the message to cell phones in the selected counties.	Resilience: Performance: Security:

Mission Steps	Time	Description	Engineering Considerations, Issues, and Challenges
14	8:00	A message recipient seated at a Burger King near U.S. 460 sees a vehicle that fits the description of the SUV headed west on U.S. 460 and calls the police to report the vehicle location.	Resilience: Performance: Security:
15	8:30	Police set up a roadblock at the Montgomery County line. As the SUV approaches, it does a U-turn and heads in the opposite direction. The police give chase and apprehend the vehicle, arresting the three men (the child's father is driving) and recovering the child, who is scared but uninjured.	Resilience: Performance: Security:

Table 25: Abduction Thread Extension Steps

Extension Steps	Time	Description of Extension Step (Off-nominal Condition for Mission Step)	Failure Expectations/Behavior for Extension Step
Step 10A		Police car system does not connect to receiving station in the central office.	
Step 12A		The IPAWS-OPEN Gateway is not operational (off-line).	
Step 12B		The IPAWS-OPEN Gateway determines that the CAP message is invalid.	
Step 12C		The IPAWS-OPEN Gateway is unable to successfully send the CAP message to the CMAS Alert Aggregator.	
Step 12D		A subset of the CMAS Alert Aggregators is not operational (off-line).	
Step 12E		A CMAS Alert Aggregator determines that the CAP message is invalid.	
Step 12F		A CMAS Alert Aggregator is unable to successfully send the CAP message to the Federal Alert Gateway.	
Step 12G		A subset of the Federal Alert Gateway is not operational (off-line).	
Step 12H		A Federal Alert Gateway determines that the CAP message is invalid.	
Step 12I		A Federal Alert Gateway is unable to successfully send a translated CAP-formatted message (now in CMAC protocol) to the CMSP Gateways.	
Step 13A		A subset of a provider's CMSP Gateways is not operational (off-line).	
Step 13B		All of a provider's CMSP Gateways are not operational (off-line), but other providers' CMSP Gateways are operational.	
Step 13C		A provider's CMSP Gateway determines that the CMAC-formatted message is invalid.	
Step 13D		A provider's CMSP Gateway is unable to successfully send the message to the mobile device subscribers.	
Step 13A		Mobile device determines that the CMAS message is invalid.	
N			

A.4 CMAS Adoption Mission Thread

A.4.1 Introduction

This section describes a development mission thread for CMAS adoption that we will use to conduct several mission thread analyses with respect to two technical characteristics (cybersecurity and resilience) and several program management characteristics (budget, schedule, resource allocation, and organizational relationships). We will validate this mission thread with stakeholders through workshop activity.

A.4.2 Contents

- Vignette description, nodes/actors, assumptions, and context: Environment before the event
- Top-level mission thread (nominal conditions): Sequence of steps describing the event and the CMAS response
- List of extension steps: Mission thread steps representing off-nominal conditions
- Overarching QA considerations: Considerations and issues not captured in steps

Table 26: CMAS Adoption Mission Thread

Name	County EMA Adoption of CMAS Capability
Vignette (summary description)	County EMA is responsible for ongoing 24/7 operations servicing • one federal EMA • one state EMA • one city Transportation Authority control center (bus and light rail) • one city EMA (fire, police, HazMat, EMS, and river rescue) • one university campus with its own police force • three boroughs with fire and police forces • local utilities (water, gas, electric) • local industries with hazardous materials One of the County EMA's objectives is to issue imminent threat and AMBER alerts and transmit them for dissemination to recipients in affected areas. The alerts must be accurate, timely, and usable, informing recipients of recommended actions to take. FEMA has set up IPAWS to support aggregation and dissemination of such alerts. One capability is CMAS, with which FEMA sends approved alerts to CMSPs in the appropriate area, who then broadcast them to mobile devices. The County EMA has acquisition and integration processes in place, which it uses to evaluate and implement the CMAS capability.
Nodes/actors	County EMA State EMA Federal EMA Prospective vendors FEMA approval entities CMSPs Cell phone subscribers FOC
Assumptions	• County EMA has acquired products and services for alerting in the past. • County EMA has management, IT, information security, operators, training, and public relations staff. • County EMA has justification for using IPAWS and meets alert originator criteria. • County EMA would like to reach initial CMAS operational readiness with 6 months. • State and federal EMAs provide guidance, requirements, and constraints on the County EMA. *Note: These are just example assumptions; there would likely be more.*

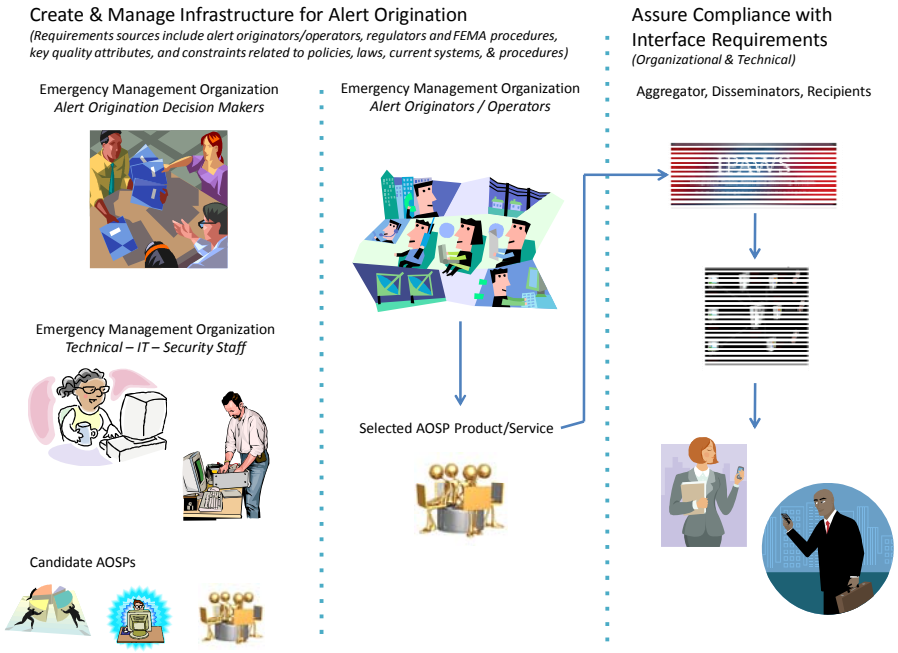
Environmental context diagram	 Note: AOSP = alert origination service provider.

Table 27: CMAS Adoption Mission Thread Steps

Mission Steps	Start Time	Description	Organizational and Technical Considerations, Issues, and Challenges
1	Day 1	County EMA management initiates study of CMAS usefulness to organization.	Program management: Acquisition: Technical:
2	Day 8	Based on the initial CMAS study, County EMA management initiates feasibility assessment of CMAS adoption. *This is a high-level assessment, done before determining eligibility and requirements.*	Program management: Acquisition: • Start development of cost estimate. Technical: • Assess current capabilities of system and survey prospective CMAS vendors.
3	Day 23	County EMA management reviews the initial approach developed by the CMAS feasibility team and provides concurrence to proceed.	Program management: • Identify acquisition strategy to be used. Acquisition: Technical:

Mission Steps	Start Time	Description	Organizational and Technical Considerations, Issues, and Challenges
4	Day 24	CMAS feasibility team initiates technical and acquisition efforts based on plan.	Program management: • Begin agreement paperwork with FEMA (e.g., MOA). Acquisition: • Begin development of acquisition plan and the criteria for evaluation. Technical: • Begin determining and specifying requirements and constraints (capability and QA).
5	Day 38	County EMA management receives update from CMAS feasibility team and provides guidance.	Program management: Acquisition: • Select acquisition path for alert authoring capability supplier (i.e., AOSP), employing one or more of the following: • Commercial off-the-shelf/government off-the-shelf product procurement • Service procurement • In-house/reuse-based development Technical: • View several CMAS vendors' demonstrations of their products.
6	Day 52	CMAS feasibility team provides assessment to County EMA management.	Program management: Acquisition: Technical:
7	Day 55	County EMA management completes agreement paperwork with FEMA (e.g., MOA).	Program management: Acquisition: Technical:
8	Day 66	County EMA management accepts the plan to incorporate CMAS into their operations and authorizes the commitment of funding and staff to proceed.	Program management: Acquisition: Technical:
9	Day 68	County EMA issues an RFQ for integrating CMAS into its operations.	Program management: Acquisition: Technical:
10	Day 89	County EMA receives bids and begins evaluation process.	Program management: Acquisition: Technical:

Mission Steps	Start Time	Description	Organizational and Technical Considerations, Issues, and Challenges
11	Day 110	County EMA selects proposal and executes a contract.	Program management: Acquisition: Technical:
12	Day 111	County EMA staff begin developing the CMAS rollout plan.	Program management: • Develop communications/PR plan that addresses both external and internal communications. • Complete initial IPAWS training. • Prepare for any specialized training needed. • Begin development of CMAS sustainment plan. Acquisition: Technical: • Identify technical tasks. • Identify staff needs. • Create checkout/monitoring plans. • Create contingency plans.
13	Day 111	County EMA staff define and plan the integration activities needed for the CMAS capability.	Program management: Acquisition: Technical: • Key element of the CMAS rollout plan
14	Day 111	County EMA staff begin developing a risk management plan for the integration effort using risks identified in the feasibility analysis and the vendor evaluation process.	Program management: Acquisition: Technical:
15	Day 131	County EMA staff begin executing integration plan.	Program management: • Manage risks. • Continue to identify potential new risks. Acquisition: • Consider whether new risks need to be identified. Technical: • Consider whether new risks need to be identified.
16	Day 140	County EMA staff perform technical acceptance activities with their vendor and complete any changes and corrections.	Program management: • Complete update of procedures (operational and sustainment) that involve the CMAS integration. Acquisition: Technical: • Support update of the procedures. • Perform checkout of interface with CMAS.

Mission Steps	Start Time	Description	Organizational and Technical Considerations, Issues, and Challenges
17	Day 147	County EMA begins executing the CMAS rollout plan.	Program management: Acquisition: Technical:
18	Day 154	Deploy and monitor CMAS integration (preconditions: (a) CMAS capability has been communicated and training has occurred, and (b) CMAS is deployed and has fully checked out in operating environment).	Program management: • Begin CMAS metric collection activities. Acquisition: Technical:
19	Day 168	County EMA CMAS capability goes live.	Program management: Acquisition: Technical: • Continue to monitor the system for potential risks.
N			

Table 28: CMAS Adoption Thread Extension Steps

Extension Steps	Time	Description of Extension Step (Off-nominal Condition for Mission Step)	Failure Expectations/Behavior for Extension Step
Step 6A		Technical risks are identified in integrating with existing alert capabilities.	
Step 7A		FEMA paperwork hits snag.	
Step 10A		Requirement conflict/cannot be met by candidate vendors.	
Step 11A		Funding is delayed or only partially available.	
Step 14A		Technical acceptance tests fail in sustainment tests.	
N			

Table 29: Quality Attributes for CMAS Adoption Mission Thread

Quality Attribute	Overarching (End-to-End) Considerations, Issues, and Challenges*
Resilience	
Performance	
Security	
N	

* Items include constraints, requirements, and concerns raised through workshop activities that affect the end-to-end mission thread.

Appendix B Collaborator-Provided Scenarios

B.1 CMAS Users Trial After-Action Report

The County of San Diego OES provided a CMAS Users Trial After-Action Report from the perspective of emergency managers (Figure 7). It covers their experiences testing the Personalized Local Alerting Network (PLAN) and discusses using the 90-character format, targeting a specific area, and developing scenarios of specific types of emergencies.

CMAS Users Trial After-Action Report: Emergency Management Perspective

As part of a coordinated effort with Sprint and the California Emergency Management Agency (CalEMA), the County of San Diego Office of Emergency Services (OES) had a unique opportunity to become the first in the nation to test the Personalized Local Alerting Network (PLAN) on a large scale. During the October 2010 trial, over 50 imminent threat and AMBER alerts were generated. These alerts were received by 120 mobile phones preloaded with Commercial Mobile Alert System (CMAS) software. Our intent was to put PLAN through its paces by simulating large and small disasters ranging from earthquakes and tsunamis to hazardous materials spills.

While our technical partners, Sprint and Alcatel Lucent, were able to gain some knowledge about the mechanics and technical specifications of the implementation, the Office of Emergency Services concentrated on the message. We were able to experience, in part, what it was like to be a local alerting agency working with the PLAN network.

90 Characters

One of the first standards we tested was the text message broadcast limit of 90 characters. There had been discussions on whether this was enough space to develop an informative message. Our objective was to develop messages that would quickly describe the type of disaster, area affected, recommended action, and advice to monitor media for more information, all the while avoiding the inclusion of a web link. While it was a challenge to script a 90-character alert, we were able to meet the minimum requirements. Some examples of our trial alerts were “Wild Fire in the Julian and Santa Ysabel area. Evacuate now. Monitor media for more info.” and “Toxic air quality near Mission Bay. Remain indoors. Turn off AC. Monitor local news.” Overall, this was a success.

However, when experimenting with AMBER alerts, we quickly realized that we didn’t have enough space to provide sufficient descriptive information as recommended by the Department of Justice’s AMBER Alert Guidelines. A description of the physical characteristics of the child and suspect, along with the make and model of the vehicle being used, followed by a contact number for the investigating jurisdiction's law enforcement department was not realistic using 90 characters.

The good news is that through our conversation with FEMA, we have learned that PLAN messages for AMBER alerts will be created by the National Center for Missing and Exploited Children (NCMEC). Because of their experience with AMBER alerts, they report that they will not have much of an issue with the 90-character limitation.

If the goal of PLAN is to alert and motivate people to seek further information, the trial proved that the 90-character limitation works fine, but it is not well suited as the sole information source for disaster notification messages. These messages would require more thorough descriptions of a disaster.

Target Area

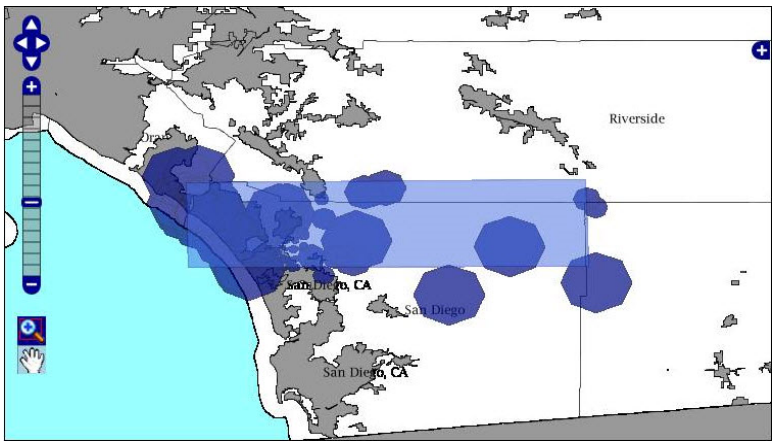
The FCC rules for carriers specify that they must "transmit any Alert Message that is specified by a geocode, circle, or polygon to an area no larger than [a county]." As San Diego County is roughly the same size as Connecticut, our tests attempted to target a more granular level.

Not surprisingly, we found that the best area for targeting was in our less populated East County; cell towers were spread out and overlapping coverage was not as frequent. Notifying an isolated community worked fairly well. Broadcasting to the heavily populated coastal cities was a greater challenge. Due to the large concentration of overlapping cell towers and wide coverage areas, targeting a small coastal community wasn't realistic.

For example, one of our tests attempted to target Petco Park, San Diego's premiere baseball stadium. The tiny four-block polygon mapped out around the park touched a large number of cell tower coverage areas. This resulted in cell towers activating from the Mexican border, north to La Jolla and east to Chula Vista, over 200 square miles of notification area. With the challenge of describing the area affected in 90 characters, this type of notification was not practical.

We learned that CMAS targeting lies between an EAS broadcast (county wide) and AlertSanDiego, our reverse 911 system (neighborhood wide) for geographic accuracy.

The map below provides a view of San Diego's North County. This example shows the target area in light blue and cell tower activation in dark blue.



Other Observations

The first part of the process of creating a PLAN alert involves choosing from predesignated lists for "response type" and "category." Response type choices include Shelter, Evacuate, Prepare, Execute, Monitor, and Assess. Category choices were Geo, Met, Safety, Security, Rescue, Fire, Health, Env, Transport, Infra, and CBRNE.

To come up with our 50 trial scenarios, we held a brainstorming session to try to match up natural and human-made disasters with the predefined lists. For most choices we had no problem imagining disasters that fit into these categories, but we did run into one category type that gave us problems. We could not find a good use for the predefined FEMA category of "Rescue." We thought about trapped miners or earthquake victims but couldn't come up with a good scenario. Under what circumstances would we notify residents of a rescue, what would we communicate to them, and would this qualify as an emergency?

One of our attempted scenarios during the trial was to create a geofence. This would be the process of setting up a geographic barrier using the map in the PLAN software. This would send an alert when a user entered a quarantined area; for example, if we were to identify an area around a damaged nuclear power plant, we could use a PLAN message to warn people to stay away before they entered a dangerous area.

While this was technically possible using the software, there was no predesignated PLAN response type for "Avoid the Area." The nearest categories were "Evacuate" or "Assess." Neither one was a perfect fit. Another discovery involved the message duration. The system limited the maximum duration of an alert to 24 hours. If an emergency manager needed a longer duration, another message was required.

We are sure many of these issues that we have identified will be solved with training or with the next generations of the PLAN system. We look forward to these advances and were honored to have a small part in the development of this important system.

Figure 7: San Diego OES CMAS Users Trial After-Action Report

B.2 List of Alert Types

San Diego OES provided a list of alert types, classified by handling, status, response type, category, severity, urgency, and certainty (Table 30).

Table 30: San Diego OES Classification of Alert Types

	Handling	Status	Resptype	Category	Severity	Urgency	Certainty
Child Abduction	"Child Abduction"	Actual	Monitor	Safety	Severe	Immediate	Likely
Wild Fire	"No Special Handling"	Actual	Prepare	Fire	Severe	Expected	Likely
Wild Fire Evacuation	"No Special Handling"	Actual	Evacuate	Fire	Extreme	Immediate	Observed
Earthquake	"No Special Handling"	Actual	Assess	Geological	Extreme	Immediate	Observed
Earthquake	"No Special Handling"	Actual	Assess	Geological	Severe	Immediate	Observed

Do Not Drink	"No Special Handling"	Actual	Execute	Health	Severe	Immediate	Observed
Flash Flood	"No Special Handling"	Actual	Assess	Meteorological	Severe	Expected	Likely
Tsunami	"No Special Handling"	Actual	Evacuate	Geological	Extreme	Immediate	Likely
Active Shooter	"No Special Handling"	Actual	Monitor	Security	Extreme	Immediate	Observed
Oil Spill	"No Special Handling"	Actual	Monitor	Environmental	Severe	Immediate	Observed
Unplanned Road Closure	"No Special Handling"	Actual	None	Transport	Severe	Immediate	Observed
Imminent Dam Failure	"No Special Handling"	Actual	Evacuate	Infra	Extreme	Immediate	Likely
Bomb	"No Special Handling"	Actual	None	CBRNE	Extreme	Immediate	Observed
				Other			

Appendix C More on Scenario Relationships

Scenario-based techniques have been developed for many analysis purposes. This appendix gives further details on how we unified some of the independently derived approaches for our CMAS integration analysis.

While we can apply any of the scenario types to point-situation analysis, when we want to examine large socio-technical systems or a system of systems such as the CMAS domain, a rough hierarchy of types is useful to show how multiple components interact. Figure 8 illustrates this hierarchy. At the highest level, vignettes establish context and describe the environment that bounds the investigation. Under a given vignette, mission threads describe what the organizations and systems do to accomplish a reaction to events or threats within the environment. For example, what steps does an emergency response center take to respond to a forest fire? The mission threads decompose into steps. For example, a decision step may need information from a system within a time window. This establishes latency as an important QA.

The steps are adjusted (decomposed or aggregated) to a granularity that illuminates an expectation of an issue or challenge. For instance, in a mission thread for CMAS adoption, a step that calls out "qualify vendors" may be sufficient in an organization that has a list of prequalified vendors but may require many additional steps for an organization that has experienced problems with poor vendor performance. The goal is to find the QAs that are important to the success of the mission. To investigate these important QAs, workshop participants use QA scenarios to localize an issue and provide a short, directed example of how an event will stress the QA, that is, how the system is expected to respond to a specific stimulus at the step level.

Figure 8 illustrates some of the key relationships between the scenario types and calls out various features and attributes associated with the scenario types. Typing is expressed explicitly or implicitly, or it is generated contextually through some organizational mechanism such as a table hierarchy or tree structure.

In practice, particularly for the purposes of our integration strategy analysis, the typing itself is not important. Stimulating dialog about issues, challenges, and barriers to CMAS adoption is important. Moreover, the emergency management community is familiar with scenario-based inquiry because it is a common organizational mechanism for emergency preparedness.

Scenario-based analysis may also develop contextual or domain specificity through various aspect specifications such as properties, attributes, or elements (the white boxes in Figure 8). There are no ontological standards for these aspects, but in practice they become relatively easy to appreciate (one person's attribute can be another person's property). Figure 8 also illustrates that in the CMAS domain it may be convenient to catalog "elements" of a given scenario such as originator, disseminator, or alert message. This hierarchy is not comprehensive, particularly in this aspect specification area, but it gives an overview of how our various types of scenarios (shown in green) relate to each other, the systems they illuminate, and some of the aspects (uncolored) that the various scenario types exhibit.

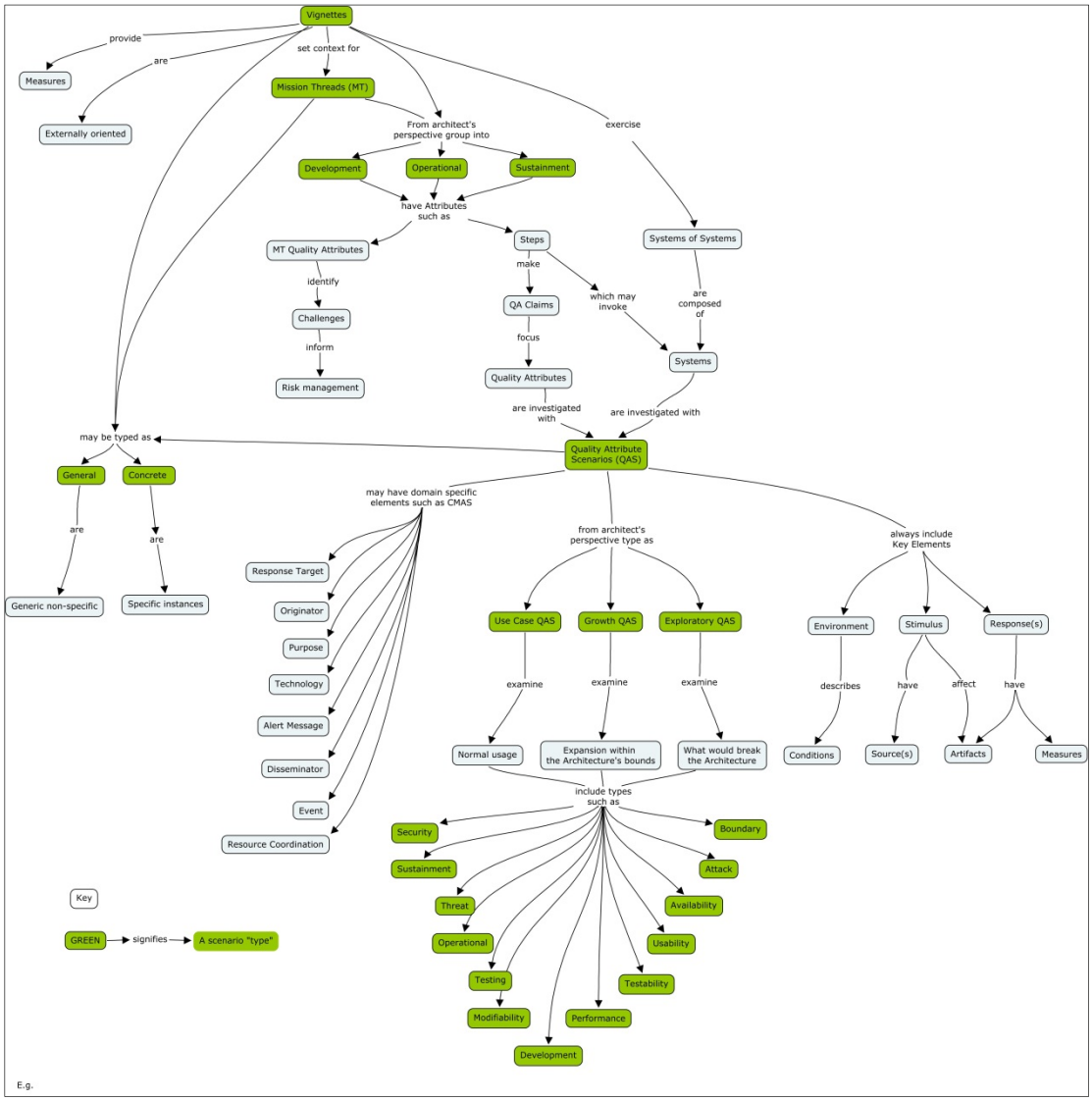


Figure 8: Scenario Entity Relationship Diagram

Appendix D Acronyms

AMBER	America's Missing: Broadcast Emergency Response
AOSP	alert origination service provider
CAP	Common Alerting Protocol
CMAC	Commercial Mobile Alert Reference Point C
CMAS	Commercial Mobile Alert Service
CMSP	commercial mobile service provider
DHS	Department of Homeland Security Science and Technology Directorate
EMA	emergency management agency
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FOC	FEMA operations center
IPAWS	Integrated Public Alert and Warning System
NWS	National Weather Service
OES	office of emergency services
OPEN	Open Platform for Emergency Networks
QA	quality attribute
RDT&E	Research, Development, Testing, and Evaluation

References

URLs are valid as of the publication date of this document.

[Adams 2011]
Adams, Stacy. "The Five W's (and one H) of Designing Cost Systems." *3CSoftware*. http://www.3csoftware.com/blog/the-five-ws-and-one-h-of-designing-systems (2011).

[Bass 2003]
Bass, L.; Clements, P. C.; & Kazman, R. *Software Architecture in Practice*, 2nd ed. InformIT, 2003.

[Bergey 2000]
Bergey, John K.; Barbacci, Mario R.; & Wood, William G. *Using Quality Attribute Workshops to Evaluate Architectural Design Approaches in a Major System Acquisition: A Case Study* (CMU/SEI-2000-TN-010). Software Engineering Institute, Carnegie Mellon University, 2000. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=5123

[Bergey 2002]
Bergey, John K. & Wood, William G. *Use of Quality Attribute Workshops (QAWs) in Source Selection for a DoD System Acquisition: A Case Study* (CMU/SEI-2002-TN-013). Software Engineering Institute, Carnegie Mellon University, 2002. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=5933

[Cook 2007]
Cook, Denise. "Architecture Evaluation and Review Practices." *Skyscrapr*. http://msdn.microsoft.com/en-us/library/bb896741.aspx (2007).

[Ellison 2004]
Ellison, R. J.; Moore, A. P.; Bass, L.; Klein, M. H.; & Bachmann, F. *Security and Survivability Reasoning Frameworks and Architectural Design Tactics* (CMU/SEI-2004-TN-022). Software Engineering Institute, Carnegie Mellon University, 2004. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=6949

[FCC 2007]
FCC Commercial Mobile Service Alert Advisory Committee. *Commercial Mobile Alert Service Architecture and Requirements* (PMG-0035, Version 0.6) [draft]. FCC, 2007.

[FEMA 2011a]
Federal Emergency Management Agency. *IPAWS Architecture Diagram*. http://www.fema.gov/pdf/emergency/ipaws/architecture_diagram.pdf (2011).

[FEMA 2011b]
Federal Emergency Management Agency. *IPAWS Projects: Commercial Mobile Alert System*. http://www.fema.gov/emergency/ipaws/projects.shtm#6 (2011).

[Nord 2009]
Nord, R.; Bergey, J.; Blanchette, S.; & Klein, M. “The Impact of Conducting ATAM Evaluations on Army Programs.” Presented at SATURN 2009. Pittsburgh, PA, May 2009. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=18984

[Rutherford County 2008]
Rutherford County Emergency Management Agency. “Mission Statement.” *Rutherford County, Tennessee.* http://www.rutherfordcountytn.gov/ema (2008).

[SEI 2012]
Software Engineering Institute. *CMAS Alerting Pipeline Taxonomy* (CMU/SEI-2012-SR-018). Software Engineering Institute, Carnegie Mellon University, 2012. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=70067

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	May 2012	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Commercial Mobile Alert Service (CMAS) Scenarios	FA8721-05-C-0003

6. AUTHOR(S)

The WEA Project Team

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2012-SR-020

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

This report supports the Department of Homeland Security Research, Development, Testing, and Evaluation program in its collaboration with the Federal Communications Commission on the Commercial Mobile Alert Service (CMAS). CMAS plays a critical role in providing targeted alerts to a geographic area. As a system-of-systems implementation, CMAS crosses many organizations to accomplish its mission. Identifying the steps taken to respond to an incident across various system and organizational boundaries can help expose potential barriers and challenges to CMAS integration. This report organizes these steps into three types of scenarios. Operational mission threads illustrate the security and organizational aspects of the integration strategy, development mission threads illustrate technical and acquisition aspects of the integration strategy, and quality attribute scenarios illustrate nonfunctional aspects of the system such as latency, resilience, or scalability. The analysis of these scenarios will help CMAS stakeholders determine how to handle the challenges that they experience as part of this large-scale integration.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Commercial Mobile Alert Service, CMAS, IPAWS, mission thread, quality attributes, scenarios, software acquisition, software architecture, software integration, systems of systems	60

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18
298-102