Software Engineering Institute

Wireless Emergency Alerts: Trust Model Simulations

Timothy B. Morrow
Robert W. Stoddard II
Joseph P. Elm

February 2014

SPECIAL REPORT
CMU/SEI-2013-SR-026

CERT® Division, Software Solutions Division

http://www.sei.cmu.edu

Carnegie Mellon University

DRAFT PENDING RRO APPROVAL

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.

DM-0000907

Table of Contents

List of Figures

List of Tables

Executive Summary

Trust is a key factor in the effectiveness of the Wireless Emergency Alerts (WEA) service, formerly known as the Commercial Mobile Alert Service (CMAS). Alert originators (AOs) working at emergency management agencies (EMAs) must trust WEA to deliver alerts to the public in an accurate and timely manner. Absent this trust, AOs will not use WEA. Members of the public must also trust the WEA service. They must understand and believe the messages that they receive before they will act on them. Clearly, the Federal Emergency Management Agency (FEMA), the EMAs, and the AOs must all strive to maximize and maintain trust in the WEA service if it is to be an effective alerting tool.

In 2012, the Department of Homeland Security Science and Technology Directorate (DHS S&T) tasked the Carnegie Mellon Software Engineering Institute (SEI) with developing a WEA trust model. The purpose of this model was to provide data that would enable FEMA to maximize the effectiveness of WEA and provide guidance for AOs that would support them in using WEA in a manner that maximized public safety. This effort resulted in two separate models: a public trust model to examine the degree of trust that the public will have in the WEA system and the resulting alerts and an AO trust model to examine the degree of trust that AOs will have in the WEA system. Section 1 overviews the models.

We used Bayesian belief networks (BBNs) to model trust in WEA. The BBN provides a way to describe complex probabilistic reasoning in a graphical format, and its main use is in situations that require statistical inference. A key feature of BBNs is that they enable modeling and reasoning about uncertainty. The BBN forces the assessor to expose all assumptions about the impact of different forms of evidence, so it provides a visible and auditable dependability or safety argument. We developed the two trust models using AgenaRisk, Version 6.0, a commercial software application suited for BBN modeling. Section 2 details the procedures used to run simulations on the trust models with this application.

For each trust model, we ran four types of simulations. Single-factor simulations focused on assessing the sensitivity of the 20 individual factors identified in the public trust model. Multifactor simulations investigated interactions between combinations of factors within and across groups of factors. Random-input simulations used stochastic samples of input variables. Special-case simulations addressed specific combinations of inputs variables determined to drive the model outputs to extreme values. Sections 3 and 4 include the simulations run on each factor and group of factors investigated.

The purpose of the trust model and the multitude of simulation runs is to identify factors and practices that enhance or degrade trust. The analysis process had two goals: to identify those simulations that predicted the highest levels of trust and those simulations that predicted the lowest levels of trust. Section 5 includes the steps of this analysis process and the results for each trust model.

The public and AO trust models are available for download at the following URLs:

- http://www.sei.cmu.edu/community/wea-project/public-bbn.cfm
- http://www.sei.cmu.edu/community/wea-project/ao-bbn.cfm

Those wishing to run their own simulations and study trust factors in their own contexts of emergency alerting may download them from there.

Abstract

Trust is a key factor in the effectiveness of the Wireless Emergency Alerts (WEA) service. Alert originators must trust WEA to deliver alerts to the public in an accurate and timely manner. Members of the public must also trust the WEA service before they will act on the alerts that they receive. This research aimed to develop a trust model to enable the Federal Emergency Management Agency to maximize the effectiveness of WEA and provide guidance for alert originators that would support them in using WEA in a manner that maximizes public safety. This report overviews the public trust model and the alert originator trust model. The research method included Bayesian belief networks (BBNs) to model trust in WEA because they enable reasoning about and modeling of uncertainty. The report details the procedures used to run simulations on the trust models. For each trust model, single-factor, multifactor, random-input, and special-case simulations were run on each factor and group of factors investigated. The analysis of the simulations had two goals: to identify those simulations that predicted the highest levels of trust and those simulations that predicted the lowest levels of trust. This report includes the results for each trust model.

1 Introduction

1.1 Overview of the Wireless Emergency Alerts

The Wireless Emergency Alerts (WEA) service, formerly known as the Commercial Mobile Alert Service (CMAS), enhances public safety by providing authorized emergency management agencies (EMAs) with the capability to issue alerts and warnings to mobile communication devices (e.g., cell phones) in a designated geographic area. WEA is a component of the Integrated Public Alert and Warning System (IPAWS) operated by the Federal Emergency Management Agency (FEMA) in cooperation with the Federal Communications Commission and supported by the Department of Homeland Security Science and Technology Directorate (DHS S&T).

WEA messages may be initiated by authorized national, state, local, tribal, and territorial EMAs. Three categories of WEA messages may be sent:

1. Presidential – Only the president of the United States may issue a Presidential Alert. This message enables the president to alert or warn a specific region or the nation as a whole of an event of critical importance.
2. Imminent Threat – EMAs may issue alerts to specific geographic areas affected by an immediate or expected threat of extreme or severe consequences. Threats may arise from a number of sources, including weather conditions (e.g., tornadoes, flash floods), law enforcement actions (e.g., riots, gunfire), fires, and environmental hazards (e.g., chemical spills, gas releases).
3. Americas Missing: Broadcast Emergency Response (AMBER) – EMAs may issue AMBER Alerts for missing or abducted children.

WEA messages are initiated by the EMAs and transmitted to the IPAWS Open Platform for Emergency Networks (IPAWS-OPEN) system using the Common Alerting Protocol (CAP) format. After authentication and verification, IPAWS-OPEN processes the WEA message and sends it to the commercial mobile service providers (CMSPs). The CMSPs broadcast the alert from cell towers in the designated geographic area to all compatible cellular devices. The cellular devices produce a distinctive ringtone, vibration pattern, or both and display the WEA message.

1.2 Trust Models for the Wireless Emergency Alerts

Trust is a key factor in the effectiveness of the WEA service. Alert originators (AOs) working at EMAs must trust WEA to deliver alerts to the public in an accurate and timely manner. Absent this trust, AOs will not use WEA. Members of the public must also trust the WEA service. They must understand and believe the messages that they receive before they will act on them. Clearly, FEMA, the EMAs, and the AOs must all strive to maximize and maintain trust in the WEA service if it is to be an effective alerting tool.

In 2012, DHS S&T tasked the Carnegie Mellon Software Engineering Institute (SEI) with developing a WEA trust model. The purpose of this model was to provide data that would enable FEMA to maximize the effectiveness of WEA and provide guidance for AOs that would support them in using WEA in a manner that maximized public safety. At a high level, our approach to this task was to build models that could predict the levels of AO trust and public trust in specific scenarios, validate these models using data collected from AOs and the public, and execute simulations on these models to identify recommendations to AOs and FEMA. We built two separate models:

1. a public trust model to examine the degree of trust that the public will have in the WEA system and the resulting alerts
2. an AO trust model to examine the degree of trust that AOs will have in the WEA system

We executed simulations on these models for numerous scenarios to identify both recommendations to AOs and FEMA for actions to take that increase trust and for actions to avoid that decrease trust.

Results of this work consist of

- *Wireless Emergency Alerts: Trust Model Technical Report*, a detailed technical report describing the process employed in the development and validation of the trust models and the resulting structure and functionality of the models [Stoddard 2013]
- a technical report (this report) detailing the scenarios and simulations executed on the trust models
- *Maximizing Trust in the Wireless Emergency Alerts (WEA) Service*, a nontechnical report analyzing the results of the simulations and identifying trust-enhancing practices to be employed and trust-degrading processes to be avoided by both AOs and FEMA [Woody 2013]

Note that this report presents only the results of the trust model simulations. It does not attempt to interpret them. For interpretation, see the *Maximizing Trust in the Wireless Emergency Alerts (WEA) Service* report.

1.2.1 Bayesian Belief Models

A Bayesian belief network (BBN) is a way of describing complex probabilistic reasoning via a graphical format. The main use of BBNs is in situations that require statistical inference. A BBN is a directed graph, together with an associated set of probability tables [Fenton 2008]. The graph consists of nodes and arcs. The nodes represent variables, which can be discrete or continuous. The arcs represent causal or influential relationships between variables. Figure 1 shows a simple example.

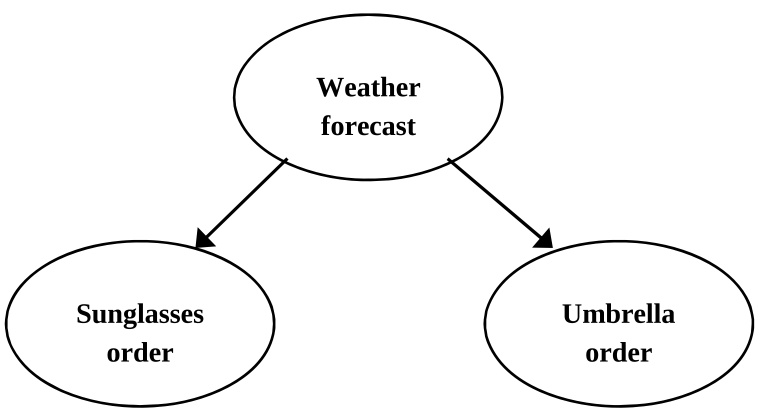


Figure 1: Example of a Directed Graph

This example examines the sales of two stores, Superior Sunglass Sales (SSS) and Rainy Day Umbrellas (RDU).

- Both SSS and RDU receive their supplies from Ajax Distributing Company.
- When the weather forecast is favorable, sales of sunglasses increase. On 70% of those sunny days, SSS places orders for sunglasses with Ajax. But on rainy days, sunglass sales decrease, and SSS places orders with Ajax on only 20% of those days.
- When the weather forecast is unfavorable, sales of umbrellas increase. On 90% of those rainy days, RDU places orders for umbrellas with Ajax. But on sunny days, umbrella sales decrease, and RDU places orders with Ajax on only 10% of those days.
- Sunny days outnumber rainy days 7 to 3.

We can summarize this information in several node probability tables, as shown in Table 1.

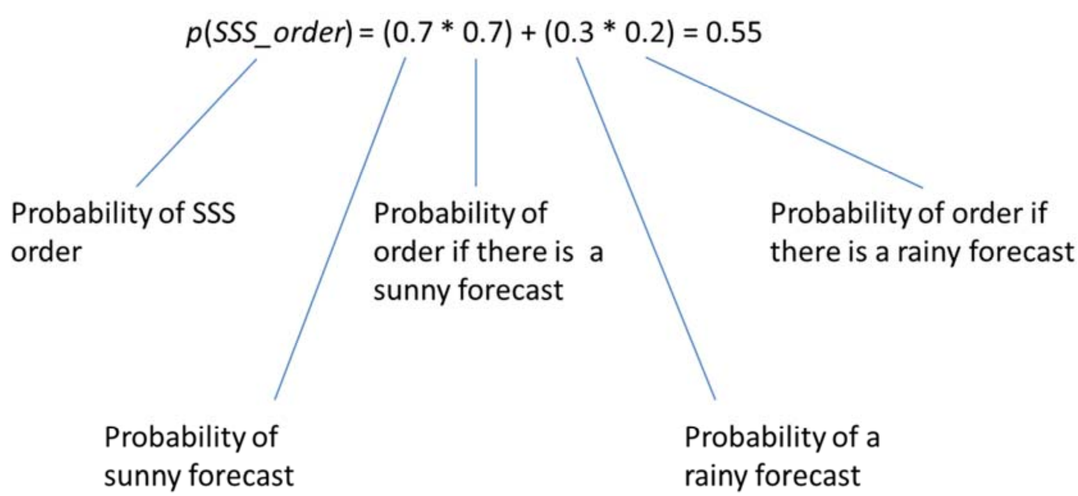
Table 1: Node Probability Tables

	Probability
Sunny forecast	70%
Rainy forecast	30%

	Probability	
	Sunny Forecast	**Rainy Forecast**
Order from SSS	70%	20%
No order from SSS	30%	80%

	Probability	
	Sunny Forecast	**Rainy Forecast**
Order from RDU	10%	90%
No order from RDU	80%	10%

Given this information, we can use Bayesian statistics to make some inferences and predictions. For example, the overall probability that Ajax will receive an order from SSS is the combination of probabilities for sunny and rainy days:



Likewise, the probability that RDU will place an order is

$$p(RDU\_order) = (0.7 * 0.1) + (0.3 * 0.9) = 0.34$$

We can now apply the Bayes theorem to examine some resulting relationships. The Bayes theorem states,

$$p(A|B) = \frac{p(B|A) * p(A)}{p(B)}$$

where:

p(A|B) = probability of event A, given that event B has occurred

$p(B|A)$ = probability of event B, given that event A has occurred

$p(A)$ = probability of occurrence of event A

$p(B)$ = probability of occurrence of event B

From Table 1, we know the probabilities of an SSS order and an RDU order in the event of a sunny forecast:

$$p(SSS\_order \mid sunny) = 0.7$$

$$p(RDU\_order \mid sunny) = 0.1$$

Using the Bayes theorem, we reverse this and calculate the probability that there is a sunny forecast if we know that SSS has placed an order:

$$p(sunny \mid SSS\_order) = \frac{p(SSS\_order \mid sunny) * p(sunny)}{p(SSS\_order)}$$

$$= \frac{0.7 * 0.7}{0.54} = 0.91$$

In this example, we initially believed that the probability of a sunny forecast was 70%. However, faced with the additional evidence that SSS has placed an order, we can update our belief to recognize that the probability of a sunny forecast is now 91%.

With this new knowledge, we can take this analysis further. We can calculate the probability that RDU will place an order, given the observation that SSS has placed an order.

$$\begin{aligned} p(RDU\_order \mid SSS\_order) &= [p(RDU\_order|sunny) * p(sunny)] + \\ &\quad [p(RDU\_order|rainy) * p(rainy)] \\ &= (0.1 * 0.91) + (0.9 * 0.09) = 0.17 \end{aligned}$$

Again, we initially believed that the probability of receiving an order from RDU was 34%. But given the evidence that Ajax has received an SSS order, we can update our belief to a 17% chance that Ajax will receive an RDU order.

The key feature of BBNs is that they enable us to model and reason about uncertainty. The BBN forces the assessor to expose all assumptions about the impact of different forms of evidence and hence provides a visible and auditable dependability or safety argument.

1.2.2 Public Trust Model

The public trust model examines the interaction of factors that influence the public's trust in the WEA service and the alerts issued through it. Through research of public alerting literature and discussions with experts in the field of public alerting, we identified the factors contributing to trust and their interactions. Figure 2 shows the results of these efforts in a directed graph, in which arrows show the relationships between factors.

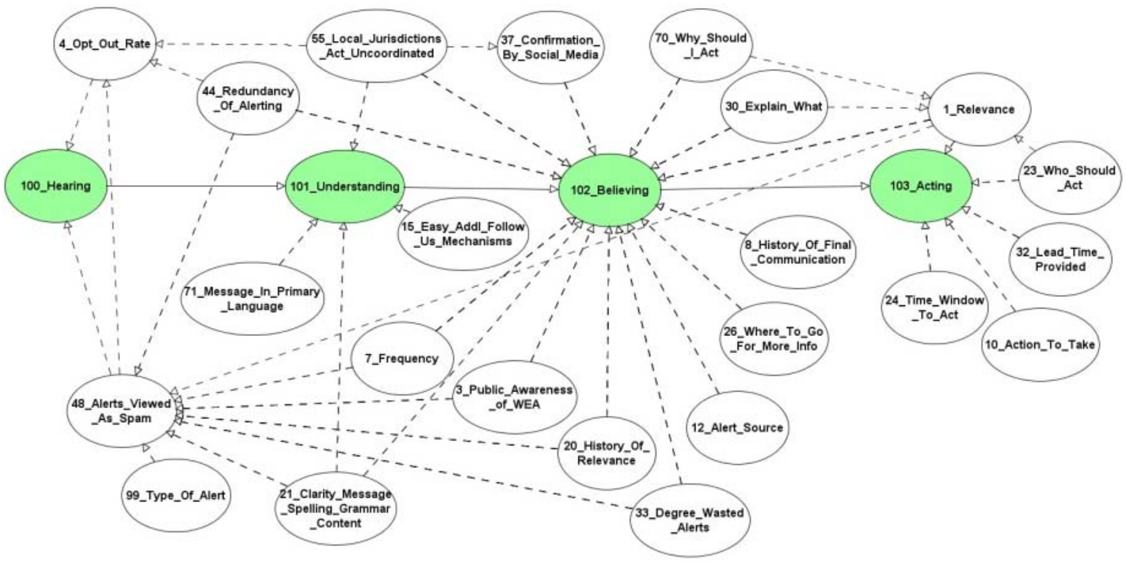


Figure 2: WEA Public BBN Expanded

We quantified the relationships between these factors through surveys and validated them with interviews of representatives of the public. We captured the results in a BBN implemented on AgenaRisk, a commercial platform suited for BBN modeling. For details about the creation of the model and the BBN, see the *Wireless Emergency Alerts: Trust Model Technical Report* [Stoddard 2013].

Table 2 and Table 3 show the model inputs and outputs, respectively.

Table 2: Factor Descriptions for Public Model Inputs

Factor	Description
1 Relevance	Applicability of the alert to the receiver. Does it affect the receiver's current location? Is it received at the appropriate time?
10 Action to take	A definitive statement of action to be taken
12 Alert source	The governmental tier of the sender (i.e., local, county, state, federal)
15 Easy additional follow-us mechanisms	Ease of obtaining additional information from the sender via other communications channels
20 History of relevance	The applicability of previously received alerts to the recipient
21 Clarity of message, spelling, grammar, and content	The degree of grammar and spelling errors in the alert
23 Who should act	A definitive statement of which recipients should take the actions specified in the alert
24 Time window to act	A definitive statement of when the recipient should take the actions specified in the alert
26 Where to go for more information	A definitive statement of places to seek additional information regarding the event precipitating the alert

Factor	Description
3 Public awareness of WEA	Public knowledge of WEA prior to issuance of an alert, developed through outreach via media channels (TV news reports, radio news reports, newspaper stories)
30 Explain what has happened	A definitive statement of the event that has precipitated the alert
32 Lead time provided	The amount of time between the issuance of the alert and the moment when action must be taken
33 Degree of wasted alerts	History of unneeded alerts
37 Confirmation via social media	Information contained in the alert is disseminated by others through social media networks such as Facebook and Twitter
4 Opt-out rate	The percentage of alert receivers who choose to disable the receipt of future alerts
44 Redundancy of alerting	Information contained in the alert is also available through other channels such as TV and radio news
48 Alerts viewed as spam	Alerts are prejudged as spam
55 Local jurisdictions activity uncoordinated	The level of cooperation between senders within a region, as evidenced by avoidance of redundant alerting, agreement between alerts, etc.
7 Frequency	The time rate at which alerts are received (e.g., alerts/month)
70 Explain why I should act	Provides a justification for the action specified in the alert
71 Message in primary language	Alert is provided in the primary language of the receiver
8 History of final communication	Issuance of a final communication (e.g., all-clear notice) at the end of the event
99 Type of alert	Presidential, Imminent Threat, or AMBER

Table 3: Public Model Outputs

Factor	Description
100 Hearing	Recipient receives and reads the alert
101 Understanding	Recipient comprehends the information provided in the alert
102 Believing	Recipient accepts the alert as true
103 Acting	Recipient takes action stated in the alert

1.2.3 Alert Originator Trust Model

The AO trust model examines the interaction of factors that influence the AO's trust in the WEA service. We identified the factors contributing to trust and their interactions through research of public alerting literature and discussions with AOs. Figure 3 shows the results of these efforts in a directed graph, in which arrows show the relationships between factors.

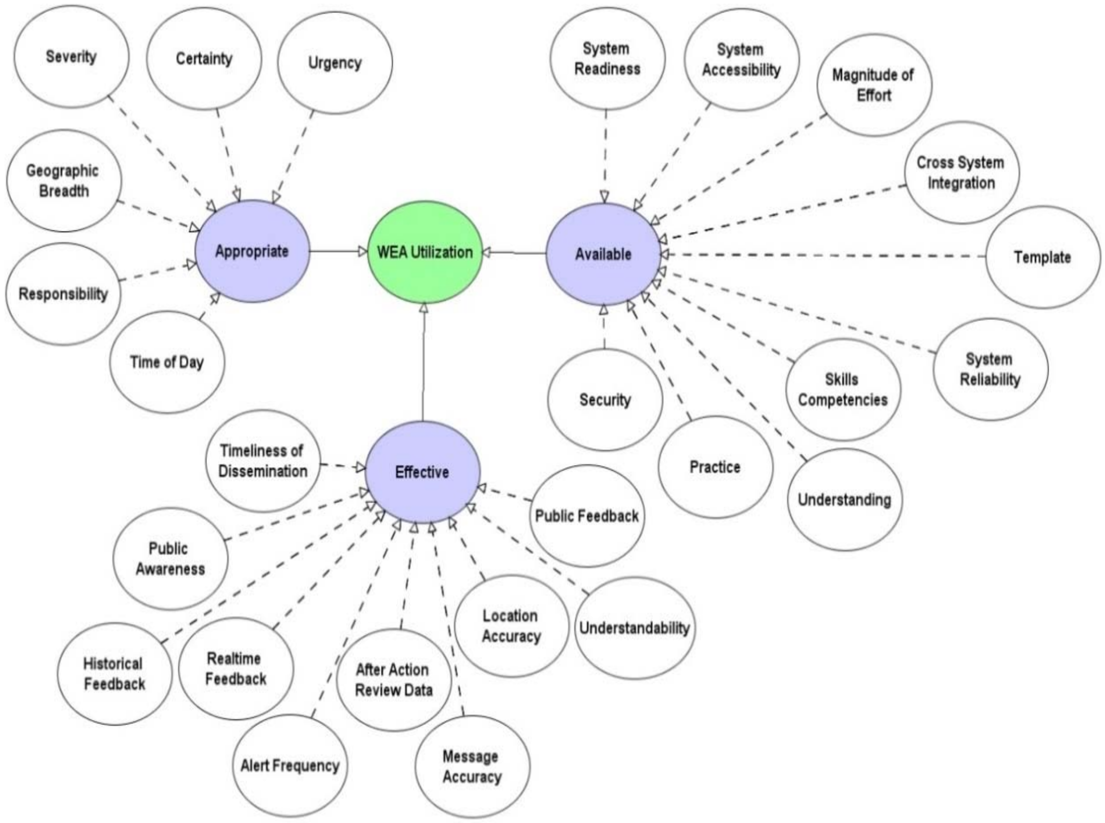


Figure 3: WEA Alert Originator BBN

Similarly to the public trust model, we quantified the relationships between these factors through surveys and validated them with interviews of AOs. We captured the results in a BBN implemented on AgenaRisk. For details about the creation of the model and the BBN, see the *Wireless Emergency Alerts: Trust Model Technical Report* [Stoddard 2013].

Table 4 and Table 5 show the model inputs and outputs, respectively.

Table 4: Factor Descriptions for Alert Originator Model Inputs

Factor	Definition
Appropriateness	The degree to which WEA provides an alerting solution that is appropriate to the event
• Urgency	The degree of immediacy associated with an event is consistent with WEA usage
• Severity	The degree of impact associated with an event is consistent with WEA usage
• Certainty	The verifiability of the associated event is sufficient to justify a WEA message
• Geographic breadth	The size and location of the geographic region impacted by the emergency event is consistent with WEA capabilities
• Time of day	The time of day (e.g., waking hours, middle of the night) when the alert is to be issued
• Responsibility	The AO's obligation and authority to issue the alert (i.e., is it clear that the responsibility and authority to issue the alert resides with the AO, or could some other organizations be responsible for issuing the alert?)

Table 4: Factor Descriptions for Alert Originator Model Inputs

Factor	Definition
Availability	The degree to which the WEA system is capable of being used when needed to issue an alert
• System readiness	The degree to which the WEA service is operable and ready for use when needed
• System accessibility	The ability of AOs to gain access and admittance to the WEA service when and where desired
– Remote/portable access	The ability of AOs to generate WEA messages from remote locations
• System reliability	The degree to which AOs may depend on the WEA system to operate correctly when needed
• System ease of use	The facility (or difficulty) with which AOs may use the WEA service to issue alerts
– Magnitude of effort	The amount of time and work needed to issue the alert
– Cross-system integration	The ability of the WEA service to work in conjunction with other emergency management systems
– Templates	The availability of predefined formats and information to accelerate and ease the process of alert issuance
• Training	Creation of skills, competencies, and knowledge for AOs
– Skills/competencies	The aptitude and capability to operate the WEA service effectively
– Understanding	The knowledge of the operational characteristics of the WEA service
– Practice	The exercising of skills needed to operate the WEA service effectively
• Security	The degree of confidence that the WEA service is robust against attempt-ed cyber attacks (e.g., spoofing, tampering, and denial-of-service attacks)
Effectiveness	The degree to which the WEA service accomplishes its intended purpose
• System feedback	The quality and value of information describing system function that is provided by the WEA service to the AO
– Real-time system feedback	Information from the WEA service reporting the status of the current WEA message dissemination process (e.g., message delivered, message re-jected)
– Historical system feedback	Information from the WEA service regarding prior performance (e.g., dis-semination time, alert geolocation data)
• Public feedback history	Information received from the public regarding prior WEA messages (e.g., "thanks for warning me," “don't wake me at night")
• After-action review data	Knowledge resulting from in-house review and analysis of prior WEA mes-sage disseminations
• Timeliness	The ability of the WEA service to disseminate a WEA message within a suitable time frame
• Message understandability	The ability to convey necessary information within the constraints of the WEA message
• Accuracy	The ability of the WEA system to disseminate correct alert information to intended recipients
– Message accuracy	The ability of the WEA service to disseminate alerts with the message content intended by the AO
– Location accuracy	The ability of the WEA service to disseminate alerts to the defined loca-tions
• Public awareness/outreach	The establishment of prior awareness and public education regarding WEA services
• Alert frequency	The number of WEA messages issued within an area in the immediate past

Table 5: Alert Originator Model Outputs

Factor	Definition
Appropriateness	The degree to which WEA provides an alerting solution that is appropriate to the event
Availability	The degree to which the WEA service is capable of being used when needed to issue an alert
Effectiveness	The degree to which the WEA service accomplishes its intended purpose
WEA utilization	The degree to which the AO is willing to use the WEA service

2 Using the Trust Models

We developed the two trust models using the application AgenaRisk, Version 6.0. To eliminate the need for future users to purchase or subscribe to this software, we configured the models to run on a free version of the software application—AgenaRisk Free. This version of the application has some limitations not found in the commercial version, as shown in Table 6. However, for purposes of running these models, these limitations do not apply.

Table 6: Differences Between Versions of AgenaRisk

Feature	AgenaRisk Free	AgenaRisk Pro
Save model containing ranked nodes	Limited to maximum of 5	Unlimited
Save model containing ranked nodes	Limited to maximum of 5	Unlimited
Save model containing multiple Bayesian network objects	Limited to maximum of 2	Unlimited
Maintenance support	None	Unlimited for duration of subscription
Upgrades	None	Unlimited for duration of subscription
Cost	Free	Subscription

The models can be run on AgenaRisk Free using the following procedure:

1. Access http://www.agenarisk.com/products/free_download.shtml
2. Select the Windows version for download: AgenaRisk_6_0_Free_Release_1312_win32bit.exe
3. Download and review the **README** file for AgenaRisk, which is also on the same web page.
4. Install the application following the instructions in the README file.
5. Start the AgenaRisk application.
6. Load either of the two models by clicking **File** and then clicking **Open Model**.
    a. The public trust model is WEA Public BBN-v030.
    b. The alert originator trust model is WEA AO BBN-v090.
7. After the model is loaded, the application displays the model's risk map. Use the mouse to click the **Risk Table**.
8. For ease in configuring the inputs, order the risk objects in the same order as they appear in the simulation spreadsheet.
    a. The public trust model simulations file is 130304 JPE Public BBN structure.
    b. The alert originator model simulations file is 130425 JPE AO BBN structure.
9. To minimize time invested in configuring the model, enter up to four scenario inputs prior to running the simulation.
    a. The application starts with one scenario open, so click **Scenarios**, and **Add a New Scenario** three times.
    b. Click the **Active** boxes for Scenarios 2–4 to make them active and visible in the application. The boxes associated with the **Display on Risk Graphs** are selected by default for all the scenarios.

10. Verify that the **Auto Calculate** button is not selected.
11. Enter the simulation inputs for the scenarios based on the definitions contained in the simulation files. Note that no answer or a blank in a cell will cause the simulation to use a uniformly distributed probability for the risk object.
12. Because the simulations were run with inputs set at known values—or either 0%, 100%, or uniformly distributed between these values—input and output risk graphs are not of interest, so click **Risk Graphs**, and then click **Close All Graphs**.
13. Run the simulation by clicking the **Run Calculation** button.
14. When the simulation has completed, select the appropriate output risk objects to view their risk graphs and obtain the median value.

3 Public Trust Model Simulations

3.1 Defining Simulation Scenarios

The public trust model includes 20 input factors. For the simulations, we evaluated these factors in three states:

1. 0% probability – The factor is absent for the simulation.
2. 100% probability – The factor is present for the simulation.
3. Uniformly distributed probability between 0% and 100% – We assert no knowledge of the absence or presence of the factor for the simulation.

Evaluating all combinations of all factors in all states would require 3^{20} (>3 billion) simulation runs—clearly an unreasonable amount. To circumvent this combinatorial explosion, we chose to group the factors in five categories, as shown in Table 7:

1. message characteristics
2. history
3. confirmation
4. preparation
5. alert process

Table 7: Factor Groupings for Public Trust Model

Category	Factor
Message characteristics	010_Action to take
	021_Clarity of message spelling and grammar
	023_Who should act
	024_Time window to act
	026_Where to go for more information
	030_Explain what has happened
	070_Explain why I should act
	071_Message in primary language
History	008_History of final communication
	033_Degree of wasted alerts
	007_Frequency
	020_History of relevance
Confirmation	037_Confirmation via social media
	015_Easy additional follow-us mechanisms
	044_Redundancy of alerting
Preparation	003_Public awareness of WEA
Alert process	012_Alert source
	032_Lead time provided
	055_Local jurisdictions act uncoordinated
	099_Type of alert

We could now simplify our investigations to examine the interactions between these five groups and the interactions within each group. To bring these interactions into focus, we ran three types of simulations: single factor simulations, multifactor simulations, and random simulations.

3.1.1 Single-Factor Simulations

The single-factor simulation efforts focused on assessing the sensitivity of the 20 individual factors identified in the public trust model. For each factor in each category, we configured a simulation run in which we set the factor under analysis to 0% probability and set all the other factors to uniform probability distribution. Next, we repeated this process with each factor set to 100% probability rather than 0%.

These single-factor simulations supported the assessment of the individual impact of each factor.

3.1.2 Multifactor Simulations

Multifactor simulations investigated interactions between combinations of factors within and across the groups noted in Table 7. For example, the Confirmation category has three factors (037_Confirmation via social media, 015_Easy additional follow-us mechanisms, and 044_Redundancy of alerting). Using a factorial design approach, we treated each factor as an independent variable. Since there are three factors and two levels (0% and 100%), the design would have 2^3 or eight different experimental conditions or runs. Using the factorial design to consider the Message Characteristics category with its eight factors would require 2^8 or 256 runs to account for the all variations.

To address the exponential growth when the number of factors increases, statisticians have developed the fractional factorial design, which involves a simple fraction (e.g., ½ or ¼) of the experimental conditions in a corresponding factorial design [Penn State 2012]. The fractional factorial design takes advantage of redundancies observed in the factorial design to reduce the number of runs needed. Through the use of a balance property, in which every level of a factor appears the same number of times at every level of each of the other factors, fractional factorial design very closely approximates the results of a factorial design in an efficient manner because the lower order effects in the factorial design are estimated [Wu 2009]. A 2^{k-p} design is a fractional factorial design with k factors, each at two levels, consisting of 2^{k-p} runs. This means that it is a (2^{-p})th fraction of the 2^k full factorial design in which the fraction is determined by p defining words, and a “word” consists of letters that are the names of the factors denoted by 1, 2, … , k. A side effect of using fractional factorial designs is the consequence of aliasing of factorial effects. See Wu and Hamada’s work for further details [Wu 2009].

Since the Preparation category has only one factor, the single-factor simulations covered all of its experimental conditions. For the other four categories in the public trust model, Table 8 through Table 11 show the multifactor simulation runs. Each table represents one factor grouping from 7, with the factors internal to the grouping established using Plackett-Burman fractional factorial designs [Giesbrecht 2004]. We used a commercial statistical software application to select the fractional factorial designs that would ensure coverage of the factor space and provide results containing the greatest possible amount of information. In Table 8 through Table 11, the table titles identify the fractional factorial design selected, where resolution indicates the interactions among the main factors and the lower level factors. For each category, we executed one run for each experimental condition identified in its associated table. In that run, we set the factors from other categories to uniform probability distribution.

Table 8: Message Characteristics Category (8 factors @ 2 levels each Resolution III)

Simulation Run	**Factors**								
	010_Action to Take	**021_Clarity of Message Spelling and Grammar**	**023_Who Should Act**	**024_Time Window to Act**	**026_Where to Go for More Information**	**030_Explain What Has Happened**	**070_Explain Why I Should Act**	**071_Message in Primary Language**	**All Other Factors**
41	1	1	1	1	1	1	1	1	U
42	1	1	1	0	0	0	1	0	U
43	1	1	0	0	0	1	0	0	U
44	1	0	1	1	1	0	0	0	U
45	1	0	0	1	0	1	1	1	U
46	1	0	0	0	1	0	0	1	U
47	0	1	1	1	0	0	0	1	U
48	0	1	0	1	1	1	0	0	U
49	0	1	0	0	1	0	1	1	U
50	0	0	1	0	1	1	1	0	U
51	0	0	1	0	0	1	0	1	U
52	0	0	0	1	0	0	1	0	U

Note: 0 = 0% probability, 1 = 100% probability, U = uniform probability distribution.

Table 9: History Category (4 factors @ 2 levels each Resolution IV)

Simulation Run	**Factors**				
	008_History of Final Communication	**033_Degree of Wasted Alerts**	**007_ Frequency**	**020_History of Relevance**	**All Other Factors**
53	1	1	1	1	U
54	1	1	0	0	U
55	1	0	1	0	U
56	1	0	0	1	U
57	0	1	1	0	U
58	0	1	0	1	U
59	0	0	1	1	U
60	0	0	0	0	U

Note: 0 = 0% probability, 1 = 100% probability, U = uniform probability distribution.

Table 10: Confirmation Category (3 factors @ 2 levels each Resolution III)

Simulation Run	Factors			
	037_Confirmation via Social Media	015_Easy Additional Follow -Us Mecha-nisms	044_Redundancy of Alerting	All Other Factors
61	1	1	0	U
62	1	0	1	U
63	0	1	1	U
64	0	0	0	U

Note: 0 = % probability, 1 = 100% probability, U = uniform probability distribution.

Table 11: Alert Process Category (4 factors @ 2 levels each Resolution IV)

Simulation Run	Factors				
	012_Alert Source	032_Lead Time Provided	055_Local Jurisdic-tions Act Uncoor-dinated	099_Type of Alert	All Other Factors
65	1	1	1	1	U
66	1	1	0	0	U
67	1	0	1	0	U
68	1	0	0	1	U
69	0	1	1	0	U
70	0	1	0	1	U
71	0	0	1	1	U
72	0	0	0	0	U

Note: 0 = 0% probability, 1 = 100% probability, U = uniform probability distribution.

3.1.3 Random-Input Simulations

For the public trust model, we ran 27 simulations with inputs randomly set to either 0%, 100%, or a uniform probability distribution between these values (Runs 73–100), as shown in Table 12. We used stochastic, or probabilistic, simulations, in which one or more input variables are random. A stochastic simulation produces output that is itself random and therefore gives only one data point indicating how the system might behave.

Table 12: Random-Input Simulations

Simulation Run	Factors																			
	010_Action to Take	021_Clarity of Message Spelling and Grammar	023_Who Should Act	024_Time Window to Act	026_Where to Go for More Information	030_Explain What Has Happened	070_Explain Why I Should Act	071_Message in Primary Language	008_History of Final Communication	033_Degree of Wasted Alerts	007_Frequency	020_History of Relevance	037_Confirmation via Social Media	015_Easy Additional Follow-Us Mechanisms	044_Redundancy of Alerting	003_Public Awareness of WEA	012_Alert Source	032_Lead Time Provided	055_Local Jurisdictions Act Uncoordinated	099_Type of Alert
73	U	1	0	0	1	0	1	0	U	U	U	1	0	U	0	1	1	1	U	1
74	1	U	1	1	0	0	U	0	U	0	U	U	U	1	U	U	U	U	U	U
75	0	0	1	0	U	U	U	U	1	1	0	0	1	U	0	0	1	0	1	1
76	U	1	U	0	0	U	0	U	0	1	U	U	U	U	0	U	U	1	U	U
77	1	U	1	1	0	1	0	0	0	0	1	0	U	U	1	0	U	1	U	U
78	1	1	U	U	0	1	0	1	0	U	U	0	1	1	U	1	U	0	0	1
79	1	1	1	U	0	U	1	U	U	0	1	0	0	0	U	U	U	U	U	U
80	0	0	U	1	U	1	0	1	0	U	0	1	U	1	1	1	1	0	U	1
81	1	U	U	U	1	1	U	0	0	0	0	1	1	U	1	1	U	U	0	1
82	1	1	1	U	1	0	1	0	0	0	U	U	0	U	1	1	U	1	U	U
83	1	0	0	U	1	U	1	0	1	U	1	0	0	U	0	1	1	U	0	0
84	U	U	U	0	1	U	0	0	U	1	0	0	U	1	0	U	0	0	1	1
85	0	U	0	U	U	0	U	1	0	1	0	0	1	1	U	U	1	1	U	U
86	U	U	0	1	1	U	0	1	0	0	U	1	U	1	U	1	1	U	1	1
87	1	1	0	1	U	0	U	0	0	U	0	U	U	1	U	1	0	U	0	1
88	U	U	0	1	0	U	0	0	1	1	0	U	0	1	1	0	U	1	1	0
89	U	U	1	U	U	U	1	U	1	1	0	1	U	0	1	1	0	U	1	1
90	0	U	U	1	1	U	1	0	1	1	0	0	U	0	1	1	1	0	1	1
91	U	0	1	U	1	0	U	U	1	U	0	U	1	U	1	0	0	U	0	U
92	U	1	0	U	1	0	0	1	0	1	1	U	U	1	0	0	0	1	1	1
93	U	0	0	U	0	1	U	0	1	U	U	1	0	0	1	U	U	U	U	U
94	0	U	U	1	U	1	0	1	0	U	0	1	0	U	1	U	U	U	0	U
95	1	0	1	0	U	U	1	0	U	U	0	1	U	1	1	U	U	1	0	1
96	0	1	1	U	0	U	1	U	1	U	U	1	U	1	1	U	U	U	1	U
97	0	1	0	0	0	0	0	0	0	1	1	1	U	U	U	0	1	0	U	1
98	U	1	1	1	U	U	U	0	1	U	0	1	U	0	0	1	1	U	0	1
99	1	U	1	1	U	0	U	0	1	0	1	U	1	U	0	U	1	U	0	0
100	0	0	0	1	0	0	U	0	U	1	1	U	0	U	1	U	1	0	U	0

Note: 0 = 0% probability, 1 = 100% probability, U = uniform probability distribution.

3.1.4 Special-Case Input Simulations

In the last set of simulations with the public trust model, we ran seven special cases involving the inputs shown in Table 13. These simulations were defined to drive the model outputs to extreme values.

Table 13: Special-Case Input Simulations

Simulation Run	Factors																			
	010_Action to Take	021_Clarity of Message Spelling and Grammar	023_Who Should Act	024_Time Window to Act	026_Where to Go for More Information	030_Explain What Has Happened	070_Explain Why I Should Act	071_Message in Primary Language	008_History of Final Communication	033_Degree of Wasted Alerts	007_Frequency	020_History of Relevance	037_Confirmation via Social Media	015_Easy Additional Follow-Us Mechanisms	044_Redundancy of Alerting	003_Public Awareness of WEA	012_Alert Source	032_Lead Time Provided	055_Local Jurisdictions Act Uncoordinated	099_Type of Alert
101	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	0	1
102	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U
103	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	1	0
104	0	0	0	0	1	0	1	0	0	1	0	0	0	1	0	0	0	0	1	1
105	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1
106	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	1
107	0	0	0	0	1	0	0	0	0	1	0	0	0	1	0	0	0	0	1	1

Note: 0 = 0% probability, 1 = 100% probability, U = uniform probability distribution.

3.2 Simulation Results

Table 14 shows the results of the previously defined 107 simulation runs. The primary outputs of the model are the following nodes:

- 100_Hearing
- 101_Understanding
- 102_Believing
- 103_Acting
- 004_Opt-out rate
- 048_Alerts viewed as spam
- 001_Relevance

The values in Table 14 represent the likelihood of the truth of the output. So a value of 48 for 100_Hearing represents a 48% likelihood that a member of the public in the area receiving the alert will hear it.

Table 14: Simulation Results

Simulation Run	Outputs						
	100_Hearing	101_Understanding	102_Believing	103_Acting	004_Opt-Out Rate	048_Alerts Viewed as Spam	001_Relevance
1	48	27	14	8	52	37	67
2	48	27	15	9	52	37	67
3	48	27	15	9	52	37	67
4	48	27	15	8	52	37	67
5	48	27	15	8	52	37	67
6	48	27	15	8	52	37	67
7	48	27	15	9	52	35	73
8	48	28	15	9	52	37	67
9	48	27	15	9	52	37	67
10	49	27	15	9	52	39	67
11	49	27	15	9	52	40	67
12	48	27	15	9	52	37	67
13	48	27	15	8	52	37	67
14	48	27	15	9	52	37	67
15	47	26	14	8	49	35	67
16	48	27	15	9	52	37	67
17	48	27	15	8	52	37	67
18	48	27	15	9	52	37	67
19	49	26	14	8	55	37	67
20	48	27	15	8	52	37	67
21	48	27	15	8	52	37	67
22	48	27	14	8	52	37	67
23	48	27	15	8	52	37	67
24	48	27	15	8	52	37	67
25	48	27	15	8	52	37	67
26	48	27	15	8	52	37	67
27	49	27	15	8	52	40	56
28	48	27	14	8	52	37	67
29	48	27	15	8	52	37	67
30	48	27	15	8	52	36	67
31	48	27	15	8	52	35	67
32	48	27	14	8	52	38	67

Table 14: Simulation Results

Simulation Run	Outputs						
	100_Hearing	101_Understanding	102_Believing	103_Acting	004_Opt-Out Rate	048_Alerts Viewed as Spam	001_Relevance
33	48	27	15	8	52	37	67
34	48	27	15	8	52	37	67
35	50	28	15	9	55	40	67
36	49	27	15	8	52	38	67
37	48	27	15	8	52	37	67
38	48	27	15	8	52	37	67
39	47	28	15	9	49	37	67
40	48	27	15	8	52	37	67
41	48	28	15	9	52	35	73
42	49	26	15	9	52	35	73
43	49	27	15	8	52	40	56
44	49	26	14	8	52	40	56
45	48	27	15	9	52	35	73
46	49	28	15	8	52	40	56
47	49	28	16	9	52	40	56
48	49	27	15	8	52	40	56
49	48	28	15	9	52	35	73
50	48	26	14	8	52	35	73
51	49	28	15	8	52	40	56
52	48	26	14	8	52	35	73
53	49	27	15	9	53	42	67
54	48	27	15	8	52	36	67
55	49	27	15	8	52	39	67
56	48	27	15	8	52	33	67
57	49	27	15	8	53	43	67
58	48	27	15	9	52	36	67
59	49	27	15	9	52	38	67
60	48	27	14	8	52	34	67
61	50	28	15	9	55	40	67
62	47	26	14	8	49	35	67
63	47	27	15	8	49	35	67
64	50	27	15	9	55	40	67

Table 14: Simulation Results

Simulation Run	Outputs						
	100_Hearing	101_Understanding	102_Believing	103_Acting	004_Opt-Out Rate	048_Alerts Viewed as Spam	001_Relevance
65	49	26	14	8	55	37	67
66	47	28	15	9	49	37	67
67	49	26	14	8	55	37	67
68	47	28	15	9	49	37	67
69	49	26	14	8	55	37	67
70	47	28	15	9	49	37	67
71	49	26	14	8	55	37	67
72	47	28	15	9	49	37	67
73	49	27	15	9	54	37	73
74	48	26	14	8	52	36	67
75	51	27	14	8	57	40	67
76	51	28	16	9	55	46	56
77	48	26	14	8	50	39	56
78	48	29	16	9	49	39	56
79	48	27	15	9	52	36	73
80	47	27	15	8	49	34	56
81	45	26	14	8	46	31	67
82	46	25	14	9	48	31	73
83	49	27	15	9	52	40	73
84	51	27	15	8	57	42	56
85	48	28	15	9	52	36	67
86	49	27	15	8	55	37	56
87	47	27	15	9	49	34	67

Table 14: Simulation Results

Simulation Run	Outputs						
	100_Hearing	101_Understanding	102_Believing	103_Acting	004_Opt-Out Rate	048_Alerts Viewed as Spam	001_Relevance
88	48	26	14	8	52	36	56
89	47	25	14	9	51	31	73
90	47	24	14	8	51	32	73
91	46	26	14	8	46	33	67
92	52	29	16	9	58	53	56
93	47	25	14	8	49	35	67
94	46	27	15	9	46	34	56
95	45	26	14	9	46	31	73
96	47	26	15	9	52	33	73
97	50	27	15	8	53	47	56
98	48	27	16	9	52	36	67
99	49	28	15	9	52	42	67
100	48	26	14	8	49	39	67
101	45	28	16	10	45	30	73
102	48	27	15	8	52	37	67
103	52	27	14	8	58	53	56
104	50	26	14	8	57	37	73
105	51	26	14	8	57	43	56
106	46	25	14	8	46	34	56
107	50	26	14	8	55	40	56

4 Alert Originator Trust Model Simulations

4.1 Defining Simulation Scenarios

The AO trust model includes 26 input factors. For the simulations, we evaluated these factors in three states:

1. 0% probability – The factor is absent for the simulation.
2. 100% probability – The factor is present for the simulation.
3. Uniformly distributed probability between 0% and 100% – We have no knowledge of the absence or presence of the factor for the simulation.

Evaluating all combinations of all factors in all states would require 3^{26} (>2.5 trillion simulation runs—clearly an unreasonable amount. To circumvent this combinatorial explosion, we chose to group the factors in nine categories, as shown in Table 15:

1. event characteristics
2. system characteristics
3. ease of use
4. system performance
5. training
6. governance
7. history
8. understandability
9. public awareness

Table 15: Factor Groupings for AO Trust Model

Category	Factor
Event characteristics	Urgency
	Severity
	Certainty
	Geographic breadth
	Time of day
System characteristics	System readiness
	System accessibility
	System reliability
Ease of use	Magnitude of effort
	Cross-system integration
	Templates
System performance	Timeliness
	Message accuracy
	Location accuracy
	Real-time system feedback
Training	Skills/competencies
	Understanding
	Practice
	Security
Governance	Responsibility

Category	Factor
History	Historical system feedback
	Public feedback history
	After-action review data
	Alert frequency
Understandability	Message understandability
Public awareness	Public awareness/outreach

We could now simplify our investigations to examine the interactions between these nine groups and the interactions within each group. To bring these interactions into focus, we ran four types of simulations: single-factor simulations, multifactor simulations, random simulations, and special-case simulations.

4.1.1 Single-Factor Simulations

The initial simulation efforts focused on assessing the sensitivity of the 26 individual factors identified in the AO trust model. For each factor in each category, we configured a simulation run in which we set the factor under analysis to 0% probability and set all the other factors to uniform probability distribution. Next, we repeated this process with each factor set to 100% probability rather than 0%.

4.1.2 Multifactor Simulations

Multifactor simulations investigated interactions between combinations of factors within and across the groups noted in Table 15. For the AO trust model, we used the fractional factorial design, as shown in Table 16 through Table 21.

Table 16: Event Characteristics Category (5 factors @ 2 levels each Resolution III)

Simulation Run	Factors					
	Urgency	Severity	Certainty	Geographic Breadth	Time of Day	All Other Factors
53	1	1	1	1	0	U
54	1	1	0	0	1	U
55	1	0	1	0	1	U
56	1	0	0	1	0	U
57	0	1	1	0	0	U
58	0	1	0	1	1	U
59	0	0	1	1	1	U
60	0	0	0	0	0	U

Note: 0 = 0% probability, 1 = 100% probability, U = uniform probability distribution.

Table 17: System Characteristics Category (3 factors @ 2 levels each Resolution III)

Simulation Run	Factors			
	System Readiness	System Accessibility	System Reliability	All Other Factors
61	1	1	0	U
62	1	0	1	U
63	0	1	1	U
64	0	0	0	U

Note: 0 = 0% probability, 1 = 100% probability, U = uniform probability distribution.

Table 18: Ease of Use Category (3 factors @ 2 levels each Resolution III)

Simulation Run	Factors			
	Magnitude of Effort	**Cross-System Integration**	**Templates**	**All Other Factors**
65	1	1	0	U
66	1	0	1	U
67	0	1	1	U
68	0	0	0	U

Note: 0 = 0% probability, 1 = 100% probability, U = uniform probability distribution.

Table 19: System Performance Category (4 factors @ 2 levels each Resolution IV)

Simulation Run	Factors				
	Timeliness	**Message Accuracy**	**Location Accuracy**	**Real-Time System Feedback**	**All Other Factors**
69	1	1	1	1	U
70	1	1	0	0	U
71	1	0	1	0	U
72	1	0	0	1	U
73	0	1	1	0	U
74	0	1	0	1	U
75	0	0	1	1	U
76	0	0	0	0	U

Note: 0 = 0% probability, 1 = 100% probability, U = uniform probability distribution.

Table 20: Training Category (4 factors @ 2 levels each Resolution IV)

Simulation Run	Factors				
	Skills / Competencies	**Understanding**	**Practice**	**Security**	**All Other Factors**
77	1	1	1	1	U
78	1	1	0	0	U
79	1	0	1	0	U
80	1	0	0	1	U
81	0	1	1	0	U
82	0	1	0	1	U
83	0	0	1	1	U
84	0	0	0	0	U

Note: 0 = 0% probability, 1 = 100% probability, U = uniform probability distribution.

Table 21: History Category (4 factors @ 2 levels each Resolution IV)

Simulation Run	Factors				
	Historical System Feedback	**Public Feedback History**	**After-Action Review Data**	**Alert Frequency**	**All Other Factors**
85	1	1	1	1	U
86	1	1	0	0	U
87	1	0	1	0	U
88	1	0	0	1	U
89	0	1	1	0	U
90	0	1	0	1	U
91	0	0	1	1	U
92	0	0	0	0	U

Note: 0 = 0% probability, 1 = 100% probability, U = uniform probability distribution.

4.1.3 Random-Input Simulations

For the AO trust model, we ran 68 simulations with inputs randomly set to either 0%, 100%, or a uniform probability distribution between these values (Runs 93–160), as shown in Table 22. We used stochastic, or probabilistic, simulations, in which one or more input variables are random. A stochastic simulation produces output that is itself random and therefore gives only one data point indicating how the system might behave.

Table 22: Random-Input Simulations (0 = 0% probability, 1 = 100% probability, U = uniform probability distribution)

	Factors																									
Simulation Run	**Urgency**	**Severity**	**Certainty**	**Geographic Breadth**	**Time of Day**	**System Readiness**	**System Accessibility**	**System Reliability**	**Magnitude of Effort**	**Cross-System Integration**	**Templates**	**Timeliness**	**Message Accuracy**	**Location Accuracy**	**Real-Time System Feedback**	**Skills/Competencies**	**Understanding**	**Practice**	**Security**	**Responsibility**	**Historical System Feedback**	**Public Feedback History**	**After-Action Review Data**	**Alert Frequency**	**Message Understandability**	**Public Awareness/Outreach**
93	0	1	0	1	0	U	0	U	U	1	1	0	U	U	0	0	U	U	0	0	U	0	1	0	U	U
94	U	0	U	U	U	U	U	1	0	1	1	1	1	1	0	1	1	0	1	1	0	U	1	1	U	0
95	0	1	0	0	U	0	1	U	1	1	U	1	U	1	0	U	0	U	0	0	0	U	1	1	U	1
96	0	0	U	1	0	1	U	U	1	0	1	1	U	0	U	1	1	0	0	1	1	U	0	0	U	0
97	1	0	1	1	1	U	U	1	U	0	0	0	U	U	1	1	0	0	0	1	U	0	1	1	0	0
98	1	1	1	U	U	0	U	U	0	0	U	U	U	U	1	1	U	1	U	0	U	U	U	1	1	1
99	0	1	1	1	U	U	U	1	1	0	0	0	0	1	U	1	U	1	0	1	1	1	1	1	0	1
100	U	1	1	0	U	U	0	1	1	0	U	0	U	U	U	1	U	0	U	1	1	0	1	1	U	U
101	U	0	U	0	1	0	U	1	1	U	0	U	U	1	1	U	U	1	1	0	1	0	0	0	1	U
102	1	U	0	1	1	1	U	0	0	1	0	1	U	0	U	0	U	1	U	0	0	1	0	U	1	1
103	0	0	U	1	U	U	1	1	0	1	1	1	1	0	U	1	0	U	1	1	U	0	1	0	U	0
104	1	0	U	1	U	0	U	U	0	0	U	U	U	0	0	U	1	U	U	1	1	0	U	0	U	U
105	1	1	0	1	U	U	1	0	0	U	U	1	0	U	0	1	0	U	0	U	U	1	1	0	U	U
106	1	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	1	U	1	1	1	U	U
107	U	0	U	0	1	U	0	0	U	U	1	1	U	1	0	0	U	1	0	1	0	0	U	0	U	1
108	0	1	0	0	1	0	1	1	U	U	U	1	U	0	0	U	U	1	0	1	0	U	1	1	U	0
109	U	0	1	U	U	1	1	0	1	U	1	U	U	U	U	0	0	U	U	1	U	0	U	1	0	0

Table 22: Random-Input Simulations (0 = 0% probability, 1 = 100% probability, U = uniform probability distribution)

Simulation Run	**Factors**																									
	Urgency	**Severity**	**Certainty**	**Geographic Breadth**	**Time of Day**	**System Readiness**	**System Accessibility**	**System Reliability**	**Magnitude of Effort**	**Cross-System Integration**	**Templates**	**Timeliness**	**Message Accuracy**	**Location Accuracy**	**Real-Time System Feedback**	**Skills/Competencies**	**Understanding**	**Practice**	**Security**	**Responsibility**	**Historical System Feedback**	**Public Feedback History**	**After-Action Review Data**	**Alert Frequency**	**Message Understandability**	**Public Awareness/Outreach**
110	1	0	U	0	U	1	1	1	U	0	1	0	0	1	0	U	1	U	1	U	1	0	1	U	1	0
111	0	0	U	1	0	0	1	1	U	U	0	0	1	U	U	U	0	U	U	1	1	1	U	U	0	U
112	1	0	U	U	0	1	1	U	0	U	1	0	U	0	U	U	1	1	1	0	0	1	0	0	1	0
113	0	U	1	U	U	1	1	1	U	U	U	1	U	1	U	U	U	U	U	0	0	1	U	0	0	0
114	U	0	U	1	1	1	U	1	0	1	1	1	0	0	0	0	U	U	U	1	0	1	1	0	0	U
115	1	U	1	1	1	U	0	1	0	U	0	1	U	1	U	0	U	0	1	U	U	1	U	0	U	U
116	U	U	0	U	1	U	1	U	0	0	1	U	1	1	0	0	1	U	1	0	U	0	1	1	0	0
117	1	1	0	0	1	1	0	U	1	0	U	1	U	0	1	1	1	0	0	U	U	1	1	1	U	U
118	1	U	U	0	0	1	U	U	0	0	U	U	1	1	0	0	U	0	1	U	1	0	0	1	U	U
119	1	U	U	0	U	1	1	1	0	U	1	0	U	U	1	U	U	0	U	U	0	1	U	1	1	U
120	U	0	0	1	1	U	1	1	U	0	0	1	1	1	1	0	U	0	1	0	U	U	U	1	0	U
121	1	U	U	0	1	0	U	U	0	U	0	U	1	0	0	0	1	1	0	0	1	U	1	0	1	1
122	U	U	0	U	1	1	1	1	U	0	1	0	U	0	1	0	1	U	0	U	1	1	1	0	1	U
123	1	1	0	1	0	0	U	0	1	1	1	U	0	1	1	1	U	1	0	1	0	U	U	U	U	1
124	U	1	0	U	0	0	1	U	U	U	U	U	U	U	1	1	0	1	U	U	0	1	0	U	1	1
125	0	0	1	0	0	0	U	1	U	0	1	0	1	1	1	0	U	0	0	0	0	U	1	U	U	0
126	1	U	U	0	U	U	1	0	1	0	0	1	U	0	U	0	0	U	1	0	0	1	U	0	U	1

Table 22: Random-Input Simulations (0 = 0% probability, 1 = 100% probability, U = uniform probability distribution)

Simulation Run	Factors																									
	Urgency	**Severity**	**Certainty**	**Geographic Breadth**	**Time of Day**	**System Readiness**	**System Accessibility**	**System Reliability**	**Magnitude of Effort**	**Cross-System Integration**	**Templates**	**Timeliness**	**Message Accuracy**	**Location Accuracy**	**Real-Time System Feedback**	**Skills/Competencies**	**Understanding**	**Practice**	**Security**	**Responsibility**	**Historical System Feedback**	**Public Feedback History**	**After-Action Review Data**	**Alert Frequency**	**Message Understandability**	**Public Awareness/Outreach**
127	0	0	0	U	1	0	0	U	U	0	U	1	U	1	U	1	U	U	1	1	U	0	1	1	0	1
128	1	1	1	1	U	0	0	1	U	U	0	0	U	1	U	U	U	0	1	1	U	0	U	U	U	0
129	0	U	U	U	1	1	0	0	1	U	U	0	0	1	1	1	U	0	U	1	0	U	0	0	U	0
130	0	U	U	U	0	1	U	U	1	U	0	0	1	U	U	0	0	U	U	1	U	0	U	1	0	0
131	0	1	U	1	0	U	0	U	U	0	U	U	U	0	U	U	0	0	1	1	0	U	1	1	U	1
132	U	0	0	0	1	0	1	U	U	U	U	U	U	1	1	1	1	0	U	0	U	U	1	1	U	0
133	0	1	1	0	0	1	0	U	0	0	1	1	1	1	0	U	0	U	0	U	0	U	U	0	0	0
134	1	1	1	U	U	0	0	0	0	U	1	U	U	U	U	0	U	U	U	0	0	0	0	U	U	U
135	0	1	U	U	1	U	0	U	0	U	U	0	0	0	1	1	1	U	0	U	0	0	U	1	U	0
136	U	0	U	U	0	1	1	U	1	1	U	0	U	1	1	1	1	0	1	0	U	0	0	U	U	1
137	1	0	1	0	0	1	0	1	U	1	U	0	1	0	0	0	U	U	0	1	U	U	1	1	U	0
138	U	1	U	1	U	1	U	0	1	1	1	1	0	U	U	1	U	U	1	1	1	1	U	U	1	1
139	1	U	U	0	U	1	U	U	0	1	0	0	0	1	U	1	U	1	1	1	1	0	0	0	U	U
140	U	U	0	U	1	U	0	1	0	0	U	U	U	U	0	0	1	1	U	U	0	0	1	U	1	1
141	0	U	U	0	U	U	U	0	U	U	1	1	0	U	1	0	1	U	1	1	U	U	U	U	0	1
142	1	0	U	0	U	0	0	1	U	0	0	U	1	U	U	1	U	1	1	0	1	U	1	U	1	0
143	0	1	U	1	1	0	0	U	0	1	0	0	0	1	1	1	U	U	1	U	U	0	0	1	0	0

Table 22: Random-Input Simulations (0 = 0% probability, 1 = 100% probability, U = uniform probability distribution)

Simulation Run	**Factors**																									
	Urgency	**Severity**	**Certainty**	**Geographic Breadth**	**Time of Day**	**System Readiness**	**System Accessibility**	**System Reliability**	**Magnitude of Effort**	**Cross-System Integration**	**Templates**	**Timeliness**	**Message Accuracy**	**Location Accuracy**	**Real-Time System Feedback**	**Skills/Competencies**	**Understanding**	**Practice**	**Security**	**Responsibility**	**Historical System Feedback**	**Public Feedback History**	**After-Action Review Data**	**Alert Frequency**	**Message Understandability**	**Public Awareness/Outreach**
144	U	U	U	1	U	1	1	0	1	0	U	U	1	U	1	1	0	U	0	U	0	U	0	0	0	U
145	1	1	1	U	0	0	U	1	1	0	1	U	0	1	U	0	1	0	U	1	0	1	U	0	U	U
146	0	1	1	U	0	U	1	1	0	0	U	1	U	U	0	0	1	U	U	U	1	1	U	0	0	U
147	U	U	1	0	0	U	1	1	U	1	0	0	1	U	U	1	U	0	1	0	1	U	0	U	U	U
148	0	1	0	1	1	1	1	U	1	1	1	0	1	U	0	U	1	U	0	U	U	U	1	1	U	1
149	U	U	U	0	1	0	1	U	U	U	1	0	0	0	1	0	1	0	0	U	0	1	1	1	1	1
150	1	U	U	0	1	1	0	U	1	U	U	0	1	U	0	U	0	0	U	1	1	1	0	0	1	1
151	1	U	0	1	0	0	U	1	0	1	1	0	1	0	1	0	1	U	U	0	1	0	U	0	0	0
152	U	0	U	U	U	U	U	1	U	1	U	0	0	U	0	U	0	U	1	1	0	U	1	1	U	U
153	1	1	1	0	1	U	0	0	0	1	0	0	1	U	1	U	0	0	1	U	1	U	U	1	0	U
154	1	1	U	U	U	0	U	1	U	0	U	0	1	0	1	U	1	U	U	1	0	U	U	1	U	0
155	1	1	U	1	1	U	U	U	U	1	0	U	U	0	0	U	0	1	1	0	0	U	U	U	1	0
156	0	U	U	0	U	1	0	U	1	U	0	0	1	U	0	U	0	1	1	1	0	1	0	0	U	U
157	0	0	0	0	0	U	0	U	U	U	1	U	U	U	0	U	1	U	U	1	U	U	U	U	U	1
158	1	U	U	0	1	1	1	0	0	0	U	0	0	U	0	0	U	U	0	1	1	0	U	U	1	1
159	0	1	U	0	U	1	0	U	0	U	0	1	0	0	0	1	U	1	1	1	0	U	1	U	U	U
160	U	0	U	1	0	U	U	0	U	1	0	0	0	0	U	1	0	1	1	0	1	0	1	0	0	U

4.1.4 Special-Case Input Simulations

In the last set of simulations with the AO trust model, we ran 12 special cases involving the inputs shown in Table 23. These simulations were designed to drive the model outputs to extreme values.

Table 23: Special Cases (0 = 0% probability, 1 = 100% probability, U = uniform probability distribution)

	Factors																									
Simulation Run	Urgency	Severity	Certainty	Geographic Breadth	Time of Day	System Readiness	System Accessibility	System Reliability	Magnitude of Effort	Cross-System Integration	Templates	Timeliness	Message Accuracy	Location Accuracy	Real-Time System Feedback	Skills/Competencies	Understanding	Practice	Security	Responsibility	Historical System Feedback	Public Feedback History	After-Action Review Data	Alert Frequency	Message Understandability	Public Awareness/Outreach
161	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
162	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U
163	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
164	1	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
165	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
166	1	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	0	0	0	0	0	1	0
167	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1
168	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	1	0	0	0
169	1	1	1	1	1	1	1	1	0	1	0	0	0	1	1	1	1	1	1	1	1	0	0	1	1	1
170	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
171	1	1	1	1	1	1	0	1	0	1	1	1	1	1	0	1	1	1	0	1	1	1	1	0	1	1
172	0	0	0	0	0	1	0	1	0	1	0	0	0	1	0	1	1	1	0	1	1	0	0	0	1	1

4.2 Simulation Results

Table 24 shows the results of the previously defined 172 simulation runs. The primary outputs of the model are the following nodes:

- Utilization
- Appropriateness
- Effectiveness
- Availability

Table 24: AO Simulation Results

Simulation Run	Outputs			
	Utilization	Appropriate	Effectiveness	Availability
1	39	72	69	71
2	40	73	69	71
3	39	73	69	71
4	39	72	69	71
5	39	72	69	71
6	39	72	69	71
7	40	72	69	73
8	39	72	69	71
9	40	72	69	72
10	39	72	69	71
11	38	72	69	71
12	39	72	69	71
13	39	72	69	71
14	38	72	68	71
15	39	72	69	71
16	39	72	69	71
17	39	72	69	72
18	39	72	69	71
19	40	72	69	73
20	39	72	69	71
21	39	72	69	71
22	39	72	69	71
23	40	72	70	71
24	39	72	69	71
25	39	72	69	71
26	39	72	69	71
27	38	70	69	71
28	38	71	69	71
29	36	69	69	71
30	37	70	69	71
31	38	70	69	71
32	39	72	69	71
33	38	72	69	70
34	38	72	69	71
35	37	72	69	70
36	38	72	69	71
37	38	72	69	71
38	38	72	68	71
39	37	72	66	71
40	38	72	68	71
41	38	72	68	71
42	38	72	69	71
43	38	72	69	71
44	38	72	69	71
45	37	72	69	69
46	38	71	69	71
47	38	72	68	71
48	38	72	68	71
49	36	72	65	71
50	39	72	69	71
51	38	72	68	71
52	38	72	68	71
53	41	74	69	71
54	40	73	69	71
55	40	73	69	71
56	35	67	69	71
57	38	71	69	71
58	39	72	69	71
59	39	72	69	71
60	31	59	69	71
61	40	72	69	72
62	38	72	69	70
63	40	72	69	73
64	38	72	69	70
65	39	72	69	72
66	39	72	69	72
67	37	72	69	70
68	37	72	69	69
69	40	72	70	71
70	39	72	69	71
71	37	72	66	71
72	37	72	66	71
73	38	72	68	71
74	38	72	68	71
75	37	72	66	71
76	35	72	64	71
77	41	72	69	73
78	37	72	69	69

Table 24: AO Simulation Results

Simulation Run	Outputs			
	Utilization	Appropriate	Effectiveness	Availability
79	36	72	69	68
80	40	72	69	73
81	37	72	69	69
82	40	72	69	73
83	40	72	69	73
84	36	72	69	67
85	40	72	71	71
86	37	72	66	71
87	39	72	70	71
88	36	72	64	71
89	40	72	70	71
90	37	72	66	71
91	39	72	69	71
92	35	72	64	71
93	34	69	68	67
94	41	71	71	72
95	37	67	70	72
96	34	69	64	71
97	38	74	68	67
98	41	74	69	70
99	40	74	68	70
100	40	73	69	71
101	36	69	65	74
102	35	71	66	69
103	40	71	69	73
104	36	73	66	69
105	38	73	69	68
106	42	75	70	70
107	33	70	68	67
108	37	69	69	71
109	39	72	66	73
110	39	70	66	74

Table 24: AO Simulation Results

Simulation Run	Outputs			
	Utilization	Appropriate	Effectiveness	Availability
111	38	69	69	72
112	36	70	64	73
113	39	71	68	73
114	37	72	67	70
115	41	74	69	71
116	39	69	69	73
117	39	71	70	70
118	35	70	65	72
119	39	71	69	71
120	39	69	69	74
121	37	71	70	67
122	38	69	70	71
123	37	72	67	70
124	37	70	67	72
125	34	66	70	68
126	41	71	69	74
127	36	67	69	72
128	41	75	66	72
129	34	71	61	71
130	36	69	67	72
131	41	72	69	72
132	36	64	70	73
133	33	71	68	63
134	35	74	64	68
135	33	73	63	66
136	36	69	63	75
137	35	70	69	67
138	43	74	68	74
139	34	71	59	72
140	36	69	70	69
141	37	69	67	73
142	40	69	71	72

Table 24: AO Simulation Results

Simulation Run	Outputs			
	Utilization	Appropriate	Effectiveness	Availability
143	34	74	57	71
144	38	72	66	71
145	41	74	67	72
146	40	72	69	72
147	37	70	66	74
148	41	72	70	72
149	37	71	68	71
150	40	72	70	71
151	35	70	66	70
152	38	71	67	73
153	40	74	68	70
154	41	74	68	72
155	42	75	67	73
156	36	69	66	73
157	31	60	68	71
158	34	72	65	68
159	37	71	67	71
160	36	70	64	72
161	50	75	72	75
162	39	72	69	71
163	20	58	52	61
164	27	74	52	62
165	37	60	72	75
166	26	63	55	70
167	37	64	72	72
168	25	58	70	61
169	39	75	61	73
170	25	58	52	74
171	41	75	72	66
172	23	60	59	66

5 Analysis of Simulations

5.1 Analysis Process

The purpose of the trust model and the multitude of simulation runs described previously is to identify factors and practices that enhance or degrade trust. To identify these factors, we analyzed the results of the simulations. In general, our analysis process had two goals:

1. Identify those simulations that predicted the highest levels of trust.
   - Examine those simulations to identify the input factors that appear most frequently. These represent the actions and practices to promote to maximize trust.
   - Examine those simulations to identify the input factors that are absent most frequently. These represent the actions and practices to avoid to maximize trust.
2. Identify those simulations that predicted the lowest levels of trust.
   - Examine those simulations to identify the input factors that appear most frequently. These factors also represent the actions and practices to avoid to maximize trust.
   - Examine those simulations to identify the input factors that are absent most frequently. These factors represent the actions and practices to promote to maximize trust.

Thus, the factors that enhance trust are those that are most often present in the simulations predicting high levels of trust, and the factors that are most often absent in the simulations predicting low levels of trust. Likewise, the factors that degrade trust are those that are most often present in the simulations predicting low levels of trust, and the factors that are most often absent in the simulations predicting high levels of trust.

Since the models have multiple outputs (e.g., Understanding, Believing, and Acting for the public trust model), we can perform this analysis process for each output to identify those factors that enhance or degrade that output.

Remember that the public trust model responds to input factors as listed in Table 2 and produces outputs as listed in Table 3. Likewise, the AO trust model responds to input factors as listed in Table 4 and produces outputs as listed in Table 5. We ran the simulations with input probability values set at 100% (input factor is present), 0% (input factor is absent), or probability uniformly distributed between 0% and 100% (input factor is unknown).

The analysis process used for each of the models consists of the following steps:

1. Choose a model output, and sort all of the simulation runs in decreasing order for that output. For example, sort the simulation runs of the AO trust model such that the runs that produce the highest values for the Utilization factor precede those that produce lower values.
2. Segment this ordered list into three categories of approximately equal size—those that have the *highest* output values, those that have the *middle* output values, and those that have the *lowest* output values. Since the list is ordered, this amounts to categorizing the first third of the list as the highest category, the second third of the list as the middle category, and the last third of the list as the lowest category.
3. For the set of simulations in each category, for each factor,
   a. note the frequency of presence; that is, count the number of times the factor is present (=100%)
   b. note the frequency of absence; that is, count the number of times the factor is absent (=0%)

4. Within each category, identify the factors that have the highest frequencies of presence and the factors that have the highest frequencies of absence.
5. Interpret the results as follows:
    a. The factors with the highest frequency of presence in the highest output category represent those factors that enhance trust.
    b. The factors with the highest frequency of absence in the highest output category represent those factors that degrade trust.
    c. The factors with the highest frequency of presence in the lowest output category represent those factors that degrade trust.
    d. The factors with the highest frequency of absence in the lowest output category represent those factors that enhance trust.
6. Repeat the previous four steps for each of the model outputs.

5.2 Analysis Results

Table 25 and Table 26 provide the results we obtained as an outcome of the preceding process.

Table 25: Analysis Results for Public Trust Model

	Enhancing Factors	
Output	**High Presence in *Highest* Category**	**High Absence in *Lowest* Category**
100 Hearing	• Local jurisdictions act uncoordinated • Degree of wasted alerts • Type of alert	• Frequency • Message in primary language • Local jurisdictions act uncoordinated • History of final communication
101 Understanding	• Message in primary language • Clarity of message spelling and grammar • Lead time provided	• Message in primary language • Explain why I should act • Frequency • Clarity of message spelling and grammar • Who should act
102 Believing	• Clarity of message spelling and grammar • Message in primary language • Type of alert	• Message in primary language • Clarity of message spelling and grammar • Explain why I should act • Action to be taken • Frequency
103 Acting	• Clarity of message spelling and grammar • Explain why I should act • Message in primary language • Action to be taken • Lead time provided	• Message in primary language • Clarity of message spelling and grammar • Action to be taken • Explain why I should act • Frequency
1 Relevance	• Explain why I should act • Where to go for more information • Who should act	• Explain why I should act • Message in primary language • Explain what has happened • History of final communication • Where to go for more information
4 Opt-out rate	• Local jurisdictions act uncoordinated • Degree of wasted alerts • Type of alert	• Frequency • Local jurisdictions act uncoordinated • Message in primary language • History of final communication

48 Alerts viewed as spam	• Degree of wasted alerts • Frequency • Action to take • Clarity of message spelling and grammar	• Frequency • Message in primary language • Action to take • Explain what has happened • History of final communication
	Degrading Factors	
Output	**High <u>Absence</u> in *Highest* Category**	**High <u>Presence</u> in *Lowest* Category**
100 Hearing	• Explain why I should act • Redundancy of alerting • Who should act • Time window to act • Message in primary language	• Redundancy of alerting • History of relevance • Type of alert • Who should act • Time window to act
101 Understanding	• Local jurisdictions act uncoordinated • Explain what has happened • Explain why I should act • Redundancy of alerting	• Redundancy of alerting • Local jurisdictions act uncoordinated • Type of alert
102 Believing	• Explain why I should act • Where to go for more information • History of final communication • Redundancy of alerting	• Redundancy of alerting • Local jurisdictions act uncoordinated • Type of alert • Who should act
103 Acting	• Local jurisdictions act uncoordinated • Where to go for more information • Explain what has happened • History of final communication • Redundancy of alerting	• Local jurisdictions act uncoordinated • Type of alert • Degree of wasted alerts • Redundancy of alerting • Where to go for more information
1 Relevance	• Message in primary language	• Type of alert • Time window to act • Degree of wasted alerts • Easy additional follow-on mechanisms • Local jurisdictions act uncoordinated
4 Opt-out rate	• Redundancy of alerting • Time window to act • History of final communication • Lead time provided	• Redundancy of alerting • History of relevance • Type of alert
48 Alerts viewed as spam	• Explain why I should act • Redundancy of alerting • History of relevance	• Redundancy of alerting • Explain why I should act • Who should act • History of relevance

Table 26: Analysis Results for AO Trust Model

	Enhancing Factors	
Output	**High <u>Presence</u> in *Highest* Category**	**High <u>Absence</u> in *Lowest* Category**
Appropriateness	• Urgency • Severity • Certainty • Geographic breadth	• Geographic breadth • Severity • Urgency • Time of day • Certainty
Availability	• Security • System accessibility • System reliability	• Security • Magnitude of effort • System accessibility • Historical system feedback

Effectiveness	• After-action review data • Understanding • Message accuracy • Time of day	• Timeliness • Message accuracy • Public feedback history • After-action review data • Historical system feedback
Utilization	• Severity • Urgency • Security • System reliability	• Geographic breadth • Time of day • Historical system feedback • Public feedback history
	Degrading Factors	
Output	**High Absence in *Highest* Category**	**High Presence in *Lowest* Category**
Appropriateness	• Magnitude of effect • System accessibility • Timeliness • Templates	• After-action review data • Security • System reliability • System readiness • System accessibility
Availability	• Severity • Templates • Understanding • Timeliness	• Urgency • After-action review data • Time of day • Responsibility • Skills/competencies
Effectiveness	• Geographic breadth • Security • Certainty • System accessibility	• Responsibility • Security • System readiness • Urgency • Location accuracy
Utilization	• Practice • System accessibility • Cross-system integration • Understanding • Alert frequency	• Responsibility • Practice • Skills/competencies • Location accuracy • System readiness

We identified these factors through a statistical analysis of the simulation results. As we have shown, some factors have stronger relationships to the output factors than others. For additional information concerning these relationships, refer to the report *Maximizing Trust in the Wireless Emergency Alerts (WEA) Service* [SEI 2013b].

6 Links to Trust Models

Those wishing to run their own simulations and study trust factors in their own contexts of emergency alerting may download the public and AO trust models at the following URL:

http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=70032

References

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

[Fenton 2008]
Fenton, Normal. *What Is a Bayesian Network?*
http://www.eecs.qmul.ac.uk/~norman/BBNs/What_is_a_BBN_.htm (2008).

[Fenton 2012]
Fenton, Norman & Neil, Martin. *Risk Assessment and Decision Analysis with Bayesian Networks*. CRC Press, 2012.

[Giesbrecht 2004]
Giesbrecht, Francis G. & Gumpertz, Marcia L. *Planning, Construction, and Statistical Analysis of Comparative Experiments*. Wiley, 2004.

[Penn State 2012]
The Pennsylvania State University. *Introduction to Factorial Experimental Designs.*
http://methodology.psu.edu/ra/most/factorial (2012).

[Stoddard 2013]
Stoddard, Robert W. II; Elm, Joseph P.; McCurley, Jim; Sheard, Sarah; & Marshall-Keim, Tamara. *Wireless Emergency Alerts: Trust Model Technical Report* (CMU/SEI-2013-SR-021). Carnegie Mellon University Software Engineering Institute, 2013. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=70115

[Woody 2013]
Woody, Carol; Ellison, Robert; & Donohoe, Patrick. *Maximizing Trust in the Wireless Emergency Alerts (WEA) Service* (CMU/SEI-2013-SR-027). Carnegie Mellon University Software Engineering Institute, 2013.
http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=70004

[Wu 2009]
Wu, C. F. Jeff & Hamada, Michael S. *Experiments: Planning, Analysis, and Optimization*, 2nd ed. John Wiley & Sons, Inc., 2009.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE February 2014	3. REPORT TYPE AND DATES COVERED Final

4. TITLE AND SUBTITLE
Wireless Emergency Alerts: Trust Model Simulations

5. FUNDING NUMBERS
FA8721-05-C-0003

6. AUTHOR(S)
Timothy B. Morrow, Christopher Larkin, Robert W. Stoddard II, and Joseph P. Elm

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER
CMU/SEI-2013-SR-026

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

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

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

12B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

Trust is a key factor in the effectiveness of the Wireless Emergency Alerts (WEA) service. Alert originators must trust WEA to deliver alerts to the public in an accurate and timely manner. Members of the public must also trust the WEA service before they will act on the alerts that they receive. This research aimed to develop a trust model to enable the Federal Emergency Management Agency to maximize the effectiveness of WEA and provide guidance for alert originators that would support them in using WEA in a manner that maximizes public safety. This report overviews the public trust model and the alert originator trust model. The research method included Bayesian belief networks (BBNs) to model trust in WEA because they enable reasoning about and modeling of uncertainty. The report details the procedures used to run simulations on the trust models. For each trust model, single-factor, multifactor, random-input, and special-case simulations were run on each factor and group of factors investigated. The analysis of the simulations had two goals: to identify those simulations that predicted the highest levels of trust and those simulations that predicted the lowest levels of trust. This report includes the results for each trust model.

14. SUBJECT TERMS
Bayesian belief network, emergency alerting, trust factor, trust model, Wireless Emergency Alerts

15. NUMBER OF PAGES
49

16. PRICE CODE

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

NSN 7540-01-280-5500

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