



Emergency Notification: When Failure is Not an Option

**By Jeremy Krinitt
VP Product Marketing
REACT Systems, Inc.**

UNIFYING CRITICAL COMMUNICATION™

IPD-WP1-RSI-0062-081218



www.reactsystemsinc.com

Introduction

A rigorous study conducted by the Georgia Institute of Technology revealed that most third-party Emergency Alert System (EAS) services are unable to deliver a high volume of emergency messages in a short period of time. The study further found that many such services are even counter-productive for emergency notification and response because they disrupt other critical communications.

At best, these services do provide a cost-effective means to issue at least some critical alerts in an emergency situation. At worst, though, these services may provide only a false sense of security that is preventing organizations from implementing the genuinely mission-critical solution required.

The lessons learned from the early adopters of EAS services reveal that while the Short Message Service (SMS) technology employed by EAS services is necessary, it is not sufficient for implementing a robust critical response notification system.

This white paper, intended for a management audience, is organized into two sections followed by a brief conclusion. The first section highlights some of the shortcomings being encountered by the early adopters of EAS services. The second section outlines a complete list of requirements for implementing a comprehensive critical response notification system.

Common Limitations with Emergency Alert System Services

The early adopters of any new technology are inevitably the first to experience its benefits. These pioneers are also, however, the first to learn of any shortcomings. Because very few EAS services have actually been tested in a real emergency situation, the Georgia Institute of Technology (Georgia Tech) decided to conduct a rigorous study to assess how well such services might perform in a real-world scenario.

The scenario Georgia Tech employed is a familiar one: the shootings at Norris Hall in April 2007 at the Virginia Polytechnic Institute. Indeed, it is this tragic event that has motivated many public and private organizations to become better prepared for responding quickly and effectively in an emergency situation. The findings produced some disturbing results, forcing Georgia Tech to conclude: "Accordingly, it is critical that legislators, technologists and the general public understand the current limitations of these systems."

This important study and the real-world experience of early adopters have uncovered the following six dependencies that together serve to undermine the effectiveness of Emergency Alert System services:

Dependence on a single network infrastructure. During a widespread emergency, different networks are impacted in different ways. For example, the local cellular

network may be overwhelmed with mobile calls, while the Public Switched Telephone Network continues to have ample capacity—or vice versa. An exclusive dependency on any single network infrastructure can make it impossible to notify everyone in the vicinity in a timely manner.

Dependence on communication without time sensitivity. Methods of communication that lack time sensitivity in the delivery mechanism can have a huge adverse impact on response effectiveness during critical situations. In fact, the situation can get worse when people do not receive key messages in time or receive them out of their sequence.

Dependence on a single form of communications. As the Georgia Tech study noted, a growing number of people now utilize SMS communications on their mobile phones, especially in a university environment. But many people still do not, perhaps opting not to subscribe to such services. Different people prefer communicating in different ways, of course, so to use an old cliché: One size does not fit all. Even office workers who do utilize SMS but spend most of the work day at their desks, for example, may not check messages frequently enough to be of value during an emergency.

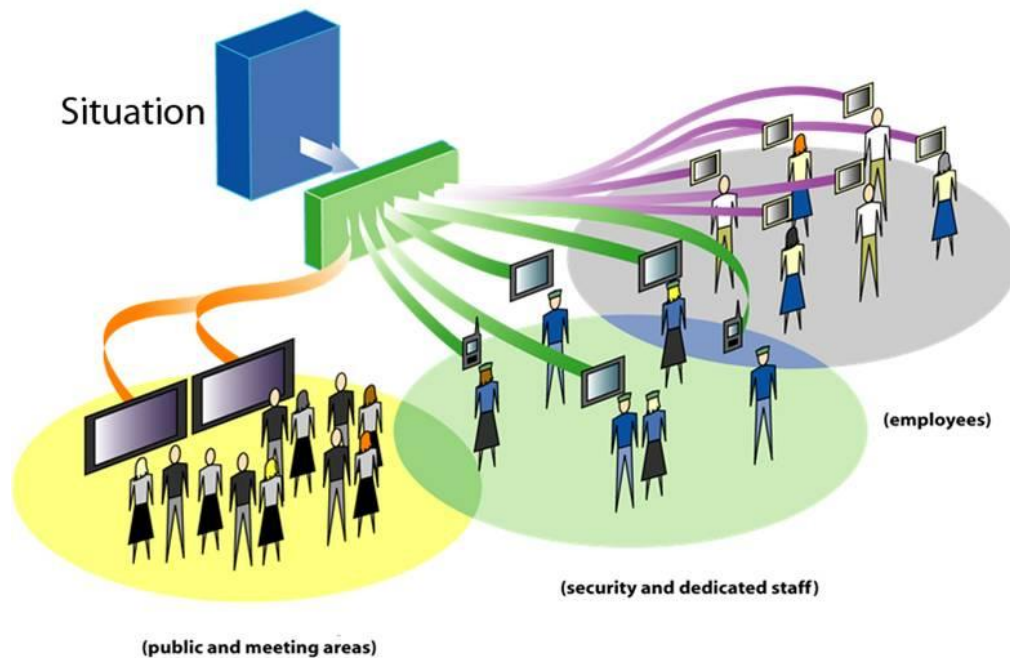
Dependence on an insufficiently robust outsourced service. Outsourcing is a proven technique for leveraging economies of scale to save money, and an increasing variety of applications is being outsourced, in whole or in part, as a result. But these cost savings should not be achieved by sacrificing critical capabilities, as is often the case. For example, many services suffer from some of the other limitations outlined in this section, particularly the dependence on a single network. The most robust services will satisfy all of the requirements outlined in the next section and, therefore, suffer from no such limitations. The most comprehensive outsourced services are also far more flexible, which is key to satisfying specific needs.

Dependence on non-specific information. Information provided at the time of a critical event must be specific and easily comprehended. And even when information is limited, the response need not be. Disaster plans lay out specific response instructions that are initiated when an event occurs. These response instructions must be fully and effectively communicated to people at the time of the event.

Dependence on individuals or a chain of command for initiation. When an event occurs, mass notification is often initiated via a chain of communications from one person to another. Such a complex process can introduce error and add time to getting the response initiated in a timely manner.

To overcome the limitations caused by these dependencies and other shortcomings in outsourced services, some organizations are now attempting to develop internal systems that integrate with their existing infrastructures. Naturally, some are having greater success than others at overcoming the usual challenges confronted when integrating multiple systems by developing custom software. And even when

successful, custom systems generally have a higher total cost of ownership owing to ongoing management complexities.



A robust mass notification system utilizes multiple means to reach multiple audiences in a timely and effective way.

Requirements for a Successful Mass Notification System

Whether implemented internally as a custom or packaged solution, or outsourced to a service provider, there are several fundamental requirements that are essential in any mass notification application. Significantly, a purpose-built and comprehensive mass notification system can cost little more than an outsourced service, while providing substantially greater versatility and effectiveness.

This section outlines these requirements in two categories. The first is a set of five specific “multi” requirements that address the singular dependencies in most EAS services. The second set is more general, constituting those basic requirements that any robust solution must possess. Satisfying both sets of requirements in their entirety is critical to implementing a genuinely mission-critical mass notification system.

“Multi” Requirements

Overcoming the problems encountered with most EAS services requires eliminating the dependencies on single points of failure and avoiding “one size fits all” forms of communication. There are five such “multi” requirements outlined here.

Multiple Networks – During a widespread emergency, networks can become clogged with traffic or completely fail when infrastructure is affected. A robust mass notification system should, therefore, employ any and all networks available: cellular, PSTN, enterprise LAN/WLAN, Internet and municipal wireless/Wi-Fi. Most users will have access to at least two of these networks throughout the day, thereby dramatically increasing the chances they can be notified—one way or another.

Multiple Devices – Just as most people have regular access to multiple networks, most people now have multiple devices: a telephone, a smartphone or a mobile phone and a PDA, and a desktop and/or a laptop PC. Organizations also have many shared devices that could be used for emergency communications, such as public kiosk displays and videoconferencing systems. With so much diversity in the equipment people now use to communicate, it would be irresponsible to omit any from an emergency notification strategy.

Multimedia – SMS messages are limited to 160 characters of text. That’s certainly enough to alert people to an emergency, and even provide fairly detailed instructions for what to do. But the old adage that a picture is worth a thousand words is still true, perhaps even more so during an emergency. With so many devices now possessing multimedia (data/text, voice/audio and video) capabilities, there is no excuse for not using every form of media available. A pop-up message on a PC, for example, can instantly alert office workers. Such a message could potentially sound an alarm and display a map showing the best evacuation route. A text message or phone call could direct users to check email or a kiosk display for detailed information.

Multiple Messages – Different people in different capacities or locations need to receive different messages at different times. Emergency response personnel should receive instructions before the masses are notified about what to do, for example. As events unfold, the situation changes, making it important to deliver all subsequent messages in their intended order. Some services simply cannot guarantee the order of message delivery, and an “old” message could contain instructions that are now counter-productive or worse. The ability to send multiple messages sequentially—tailored and targeted for individual audiences—is fundamental to coordinating response effectiveness and preventing mistakes.

Multiple Initiators – Children are instructed from a very early age to pull the nearest fire alarm if they smell smoke or see flames for a very good reason: In an emergency, time is of the essence. A good mass notification system should, therefore, make it possible for anyone to push the “panic button” at the first sign of an emergency. Naturally, such an ability also comes with some responsibility, which necessitates adequate training for every individual so equipped. But the alternative approach—having only one person or a few people authorized to initiate an emergency response—can carry even greater overall risk with its built-in delay.

General Requirements

The general requirements for implementing any mission-critical system are well understood, but this document would be incomplete without at least highlighting the six most important ones.

High Availability – As the title of this document indicates: Failure is not an option with an emergency notification system. The application should, therefore, operate on redundant servers with automatic failover. In addition, the failover should be stateful; that is, no failure should cause any critical information to be lost or corrupted in the transition.

Dependability – High availability provisions can only ensure that the application is up and running. With an application as mission-critical as emergency notification, it is also important to ensure that the application is running properly. And the best way to do that in this case is to confirm that the messages being sent are actually being delivered in a timely manner and in the order sent.

Security – To ensure the integrity of the system, critical communications must be secured, preferably with strong encryption, and the servers should be deployed in a secure area of the data center. Additional security provisions, such as firewalls and other perimeter defenses, should also be deployed to protect the private network, while still enabling use of public networks, such as the Internet and PSTN.

Comprehensive Logging & Reporting – Having a reliable and comprehensive audit trail is essential in an emergency notification system. Logs may need to be accessed in real-time to understand and validate actions taken so far. The logs may also be needed during a post-emergency review to assess performance and uncover areas for improvement.

REACT! Enterprise from React Systems

REACT! Enterprise is the industry's most comprehensive critical communication system, capable of simultaneously delivering targeted event-, location- and recipient-specific verifiable communications to first responders and those at risk. As a device-agnostic solution, REACT! Enterprise utilizes multiple networks and multimedia communications, such as rich audio/video, SMS text and voice alerts, to ensure warnings and instructions reach their intended recipients. The result is an unprecedented ability to mitigate and contain any crisis, interruption, risk or liability, and to better protect public safety and save lives.

Notifications and alerts can be launched from desktops, mobile devices or smartphones. They can also be triggered automatically through integration with leading security or other systems, either inside an organization or outside when required to reach entire communities. As information changes, alerts can be updated as needed to improve situational awareness, accelerate response times and optimize use of available resources. Users can receive multiple alerts simultaneously, with the highest priority ones displayed as they are sent. In addition, emergency managers can automatically provide detailed instructions globally, in any number of languages, with Unicode support.

Based on its fully scalable, open client-server architecture, REACT! Enterprise can reach millions of users within seconds. The open architecture enables interoperable, automated communications with other systems, including the interagency coordination required to reach anybody, anywhere, during crises. The open architecture also integrates easily with existing networks, alarms and surveillance systems, and all standard communications infrastructures. The server itself can be installed quickly and cost-effectively, allowing customers to start small and expand as needed. This innovative and unique design enables REACT! Enterprise customers to provide the highest degree of protection of lives and assets, as well as to assure compliance with regulatory requirements.

Simplicity of Operation – During an emergency, there is no time to waste checking reference materials for how to operate the system. Ideally, the system would offer something as simple and “fool-proof” as a single-button alert for point-and-click activation. The more advanced features should also be as straightforward and intuitive as possible. Nevertheless, given the seriousness of the application, rigorous training and frequent practice drills remain prudent even with most intuitive of systems.

Ease of Management – The system should be easy to maintain, upgrade, troubleshoot and otherwise manage. It should also be easy to take advantage of all advanced features, such as defining different classes and categories of recipients, tracking the communications capabilities of all users, creating a database of targeted messages for different circumstances, managing administrative privileges, etc.

Conclusion

Failure is not an option with an emergency notification system. But as the Georgia Tech study revealed, many Emergency Alert System (EAS) services are incapable of delivering a massive number of notifications in a timely fashion. Some systems and services also fail in other ways. They may have an exclusive dependency on a single network that becomes congested or fails entirely during an emergency. They may fail to reach all intended recipients because they rely on a single form of communications. Or they simply fail to provide the full set of capabilities that might be needed.

REACT! Enterprise from React Systems is designed not to fail. With support for multiple networks, devices, media, messages and initiators, REACT! Enterprise takes full advantage of available resources, and eliminates single points of failure and “one size fits all” limitations. REACT! Enterprise is also a carrier-grade solution with the mission-critical feature set needed for highly-available, dependable, secure and verifiable operation. But perhaps best of all is that such sophistication is remarkably easy to operate and manage, and surprisingly affordable.

To learn more about how your organization can implement a cost-effective and comprehensive critical communication system, visit React Systems on the Web at www.reactsystemsinc.com or call 866.982.7662.

#



REACT Systems, Inc. / 1731 E. Roseville Parkway #151 / Roseville, CA 95661
voice 866.982.7662 / fax 916.772.3424
email info@reactsystemsinc.com / www.reactsystemsinc.com