BlackBerry

White Paper

Airports: Emergency Notification, Interoperable Communication, and Beyond

Best Practices for Civil, Government, and Military Aviation Operations

Captain LaPonda Fitchpatrick (Ret.)
Commanding Officer - Los Angeles Airport Police Department (LAXPD)

Assistant Chief John Linstrom
Business Development Manager - Public Safety & Aviation, AtHoc, Inc.

ARFF Chief Jim Lonergan
Natl. Coordinator of Aircraft Rescue & Firefighting (ARFF) Training and Certification Programs

Table of Content

Executive Summary

Ensuring public safety on airport properties across the globe requires a complex coordination of emergency response services, advanced alerting systems, and tightly integrated operations.

Communicating critical information during an emergency event as soon as possible is one of the most important capabilities necessary for effective emergency response and recovery. Airports are dependent on a wide range of organizations and agencies to assist them in times of crisis and disruption. These partnerships and networks rely heavily on the timely sharing of accurate information with each other, stakeholders, passengers, and the general public.

As with the transitory system that aviation presents, airport leaders are always searching for ways to improve the coordination of emergency responses to better protect passengers, staff members, vendors at an airport, plus organizations and businesses in their nearby communities, including the public officials who will judge an airport's emergency response leadership and efficacy.

This white paper describes the evolution of Emergency Mass Notification Systems (EMNS) employed by airports. Today, integrated safety and security solutions have grown from stand-alone, hard to manage physical systems to sophisticated communication networks that support an effective, real-time emergency response.

This paper also offers proven critical best practices[1] and advice for airport executives seeking to improve operational efficiency and interoperable communications, along with safety, security, and regulatory compliance at the airport and into surrounding communities.

Real-Life Aviation Emergencies

In July 2013, Asiana Airlines Flight 214, a Boeing 777 wide-body jet inbound from South Korea, struck a seawall during landing at San Francisco International Airport. In many ways, the emergency response system functioned precisely as planned. Air traffic control worked with security, police, fire, and rescue units to respond rapidly to the situation, minimizing the danger and injury to passengers on the plane and people at the airport.

There were more than 300 people on the flight, and unfortunately, three people died in the tragedy. Airfield operations were restored to routine status relatively quickly. Mass notification and having a response plan were key parts of the effort. However, this success was due in part to the event occurring in a controlled environment, and contained in the Air Operations Area where access is restricted.

In contrast, a chaotic response can occur when communication among key stakeholders is through multiple modalities and systems. An airport shooting at Los Angeles International Airport that began in the public, unrestricted area of the airport led to more than 20 different agencies responding to the incident, without the benefit of a true interoperable communications platform to coordinate efforts among the various commanders. It took more than 45 minutes to unify multiple command posts, and the first meeting among commanders didn't occur until more than 90 minutes after the shooting began.

It is exceedingly difficult to quickly alert multiple groups to a major, immediate risk – especially when organizations other than airport emergency personnel, police, fire, and air traffic control are involved. See the LAX shooting after action report here.

When this raw data is mixed with unconfirmed rumors and a social media-style of citizen journalism where "everyone is a reporter," the ability to deliver accurate, verified emergency messages and notifications becomes even more difficult.

Consider the following scenario: Control tower personnel observe an "Alert III," an aircraft accident or crash on the airport. Airport emergency response teams are activated. Police, fire, and follow-on resources are integrated into a live communications system, so they can monitor unfolding events – and the extended airport staff is able to request assistance from any connected resource.

In near real-time, the same system automatically alerts airlines operating at the airport, as well as vendors, hotels, and medical teams. The airlines become aware of interruptions to their flight schedules and can immediately make adjustments. Airlines and vendors can accelerate or delay shift changes, minimizing traffic into and out of the airport, which facilitates more rapid responses from emergency personnel. Travelers and family members on their way to the airport for any diverted flights can be advised to go to a different local airport, or wait at home or in their offices for updates on alternate flights.

Area hotels can be notified that passengers stranded in the airport may need accommodations. In coordination with emergency management officials, schools, homes, and businesses in the affected area can receive warnings that a potentially dangerous situation is developing, and receive ongoing updates regarding the severity of the threat. Hospitals and triage teams can prepare for injuries.

Today, disparate communication systems are operating across too wide a range of technologies and media, with too many constituencies to coordinate, and too many moving parts to manage effectively. This leads to chaotic responses and inefficiencies, with the potential to cause delays and disruptions worldwide.

Nevertheless, a solution does exist, and it is known as networked crisis communication, the next step in the evolution of emergency notification technology.

A Brief History of Emergency Communication

The first technological attempts to notify people en masse were called Emergency Mass Notification Systems (EMNS). These basic systems utilized physical wire-based hardware, such as telephones, fire annunciators, two-way radios, and PA systems, to alert response personnel in a command center. First responders relied on public safety communicators to sort out the various types of input and recommend appropriate action.

In 2005, the speed, ubiquity, and robust nature of Internet Protocol (IP) networking enabled some of those uncoordinated systems to be connected to each other, and to laptop and desktop computers. Rather than having to listen to a cacophony of audio and visual signals during a crisis, operators could see alerts on a central screen with minimal distraction.

Moving to IP-based emergency communications allowed existing physical systems to be integrated into a broader response infrastructure, without having to completely replace older legacy technology. These cost savings became critical, as airports sought new ways to upgrade safety, security, and emergency response, while maximizing return on investment (ROI) and doing the best with limited financial resources as a result of 9/11 and the economic downturns.

For example, passengers and airline personnel depend on flight information display systems (FIDS) for departure and arrival times, gate assignments, baggage claim deliveries, and other travel-related information. FIDS are supplemented by ramp information display systems (RIDS) that allow ground personnel and flight crews to dock aircraft at gates, move baggage and aircraft, refuel planes, and provide on-ground maintenance and inspection.

In order to maximize efficiency and minimize aircraft turnaround times, the two systems in this example need to be connected to each other, along with the emergency response system, so that any threat to operations is communicated as accurately and quickly as possible. Ground personnel should be notified immediately if severe weather is in the area, or if they need to be aware of an inflight emergency on final approach. Inside the terminal, airline staff must be advised that ground crews may not be available until a situation has been resolved, and that flight delays are imminent.

With the next step in the evolution of EMNS, innovative airports were able to move to a facility-wide, enterprise approach for governing emergency management. Increasing numbers of network-capable devices meant more data could be brought into the command center to provide improved situational awareness. Airport operations could be monitored from multiple remote locations, and could connect large numbers of mobile personnel via smartphones or tablets. Using alert templates, pre-defined response scenarios, and employee profiles, airports could centrally manage mass notification and control “sub-systems,” which eliminated redundancies and errors in data management across the enterprise.

Future technology advances are now expanding communications beyond airport management to vendors, communities, and other entities directly affected by airport operations. These connections need to bridge a much wider range of communications technologies, while providing the real-time response and secured flow of information that, up until now, had only been possible inside the physical and networked perimeter of the airport property.

Expanding our Communications

Future technology advances are now expanding communications beyond airport management to vendors, communities, and other entities directly affected by airport operations.

Interoperable Communication: Next Frontier of Crisis Communication

Aging communications infrastructure, legacy technologies, and incompatible systems are challenges for many airports. Additionally, a large number of these legacy systems are proprietary, with minimal levels of technological support threatened by attrition of employees and technology products experiencing end-of-life issues.

The difficulty lies in economically transitioning these stand-alone systems into a single unified experience, which allows operators to control all inputs and outputs, and extend rapid response capability beyond the airport property. History has shown that airport operators need to inform their tenants, surrounding infrastructure, and even the broader community, to coordinate an effective response.

Communication Needs to Extend Beyond Four Walls

Most major airports with domestic and international traffic have to accommodate passenger, freight, and other ancillary operations that maintain these services. Beyond the airport itself, each airline, cargo company, maintenance business, and vendor has its own organizational processes, procedures, and cultures.

These challenges can be overwhelming. Each entity maintains a workforce of great diversity with regard to language, size, role, disability, security level, and access level. The entire aviation system must be considered, because it is an interconnected network where an individual airport does not operate in isolation.

Airport managers typically know how to handle internal communications within their physical grounds. True interoperability, however, has to include collaboration with a broader range of public and private stakeholders[2], including:

- **Federal and state government authorities**: Federal Aviation Administration (FAA), Transportation Security Administration (TSA), National ransportation Safety Board (NTSB), Federal Bureau of Investigations (FBI), North American Aerospace Defense Command (NORAD), Centers for Disease Control (CDC), Immigration and Customs Enforcement (ICE), and Customs and Border Protection (CBP)
- **Public and private security and protective service organizations:** Law enforcement, fire, paramedics, and ambulances
- **Airport and contract employees, including full- and part-time, on- and off-site:** Retail vendors, supply chain providers, aerospace services companies, fueling, and maintenance
- **Geographic and functional neighbors:** Industrial, supply chain, hospitals, schools, hotels, rental car, air freight facilities, and food vendors

It is difficult to coordinate the interactions of these entities on a daily basis. Emergency situations put these relationships under tremendous strain, precisely when seamless communications are most urgent. While some essential stakeholders may be part of the airport's communications infrastructure, most of the ecosystem remains outside these frameworks.

Contact List Management: Exchanging One Problem for Another

Some airports and emergency management organizations have tried to establish interoperability by including external emails and contact lists within their own information distribution lists. While logical and laudable, these efforts are counterproductive in practice, for four reasons:

1. Contact lists must be constantly updated to ensure that critical information is sent to the appropriate personnel.
2. Email and other passive communications rely on someone to open and read the message. Critical information may not reach essential external personnel simply because that person is not online.
3. List-based contact management is very resource-intensive. Staff must work diligently to confirm information about thousands – or tens of thousands – of individuals. A more intuitive, automated solution frees staff for higher priorities.
4. Airports do not control the level of security and access to the external emails and servers.

Interoperable Communication: Next Frontier of Crisis Communication

Social Media Is Not the Answer for Interoperability

Many emergency notification systems allow surrounding organizations and the general public to sign up for email alerts via social media without permission or vetting by the originating authority.

This open-access approach makes it difficult for safety and security personnel to isolate the communications they need from the inevitable noise that arises during an emergency. More significantly, these notification systems are not secured, which creates a major risk when proper control of information is critical.

The lack of a true, interoperable system means that subscription services via social media offer no practical interoperable value other than getting the word out. Social media produces unreliable information from unknown sources that cannot be relied upon to make informed decisions during an event.

Control and Security Are Mandatory, Not an Afterthought

Control is another major concern of interoperability. Enterprise businesses expect their systems to grant them the ability to adjust roles and permissions across their organization to ensure individuals see only what they need to see, at the times they need to see it. These controls should also extend to customers, external partners, stakeholders, and the general public.

Security, likewise, needs to be inherent to the system, and is especially relevant for interoperability. By statute and as a business practice, personally identifiable information (PII), confidential operational information, and other critical data need to be protected and stored in secure failover systems, especially when essential details must be revealed on very short notice and to specifically targeted populations.

Adherence to Market and Government Policies

Airport executives are increasingly encouraged to follow a collaborative approach to integrating local and regional communities and response agencies into the emergency planning process, as described in many reports – most notable is the 2014 Airport Cooperative Research Program (ACRP) synthesis of airport practice, sponsored by the FAA.

"Waugh and Streib (well-known scholars in disaster studies and emergency management) demonstrated that 'collaboration is a necessary foundation for dealing with both natural and technological hazards and disasters and the consequences of terrorism.' They recommend a number of methods for improving collaborative activities, such as optimizing the use of networks," the Transportation Research Board noted.[3]

Furthermore, the U.S. federal government has enacted several laws and policies adding to the momentum and need for interoperable communication and emergency response notifications:

- **H.R. 615: DHS Interoperable Communication Act – enacted on July 6, 2015:** DHS is now mandated "to achieve and maintain interoperable communications among the components of DHS, for acts of terrorism, daily operations, planned events, and emergencies."[4]
- **H.R. 2206: Statewide Interoperable Communications Enhancement Act – passed house on July 28, 2015:** Amends the Homeland Security Act of 2002 to "require governors of each state to designate a Statewide Interoperability Coordinator, or indicate that the state is performing the functions of such a Coordinator in another manner."[5]
- **H.R. 720: Gerardo Hernandez Airport Security Act – enacted September 24, 2015:** TSA is "to conduct outreach to all TSA U.S. airports the implementation and performance of security measures, and verify that such airports have in place individualized working plans for responding to security incidents inside the airport perimeter, including active shooters, acts of terrorism, and incidents that target passenger-screening checkpoints."[6]

Using Networked Crisis Communication to Address Interoperability Needs

Internal alerts through multiple systems and devices are becoming more prevalent as many airports develop stronger communication programs to alert their employees. (See the Appendix for system best practices.) The ability to communicate with other organizations, however, is still a critical need, and must be achieved just as quickly to protect the airport ecosystem.

The first requirement is to develop the Airport Emergency Plan and protective measures that can either execute – or prevent – a mass, uncontrolled movement of travelers, or make shelter available to those who may be stranded. Next, a community approach would suggest a phased response that includes the organizations and people located closest to the incident, followed by a reinforced response with those farther away. Mutual aid relationships must be nurtured, practiced, and maintained at local and regional levels.

Typical interoperable communication scenarios encompass:

- Emergency events that require stakeholder notification (workforce, customers, and partners)
- Public alerting, 911 reverse dialing, and enhanced 911 (if available)
- Business operations notifications, such as workforce management roll call or mustering, callouts, severe weather, and important meeting reminders
- Context-based alerting triggered by a process or event, such as a flight delay, work availability options by locale, or incoming injured patients
- Potential public alerting and emergency warnings of an impending emergency by local, regional, or national authorities

At the forefront, two-way interactive alerting is an essential element to begin responding to any incident. Targeted recipients who receive alerts can respond with their status. They can, in turn, equip their own decision-makers with the information necessary to protect people and facilities, and then focus on arranging assistance for those impacted.

Next, airport operations need to reliably and rapidly send an alert that can reach all of its personnel across all personal and mass communication devices to ensure both visual and audio alerts are received within the ecosystem.

As the situation unfolds, airport responders need to notify on-site tenants, as well as the extended community and political authorities about the event and its level of emergency. A true state-of-the-art solution empowers each subscribing organization to create a unique, customized network of people and groups, so that the quality and fidelity of the information remains high and actionable as it is disseminated by member organizations, while maintaining their own operational protocols.

Finally, given that most commercial and certificated airports are owned or operated by local, state, and national jurisdictions, emergency response requires expanding networks of shared information and intelligence to include federal, state, and regional agencies, such as[7]:

- Department of Homeland Security (DHS)
- NORAD
- CBP
- TSA
- FAA
- CDC
- FBI
- US Coast Guard (USCG) • Department of Defense (DOD)
- ICE
- Health and Human Services (HHS) • American Red Cross

Networked crisis communication should support collaboration among different functions, so responders can neutralize the event, while maintaining situational awareness among all responding entities. The system should also have a sophisticated reporting capability to capture all the system and personnel activities for post-event assessment and compliance requirements.

Outcome: Secure, Interoperable Crisis Communication Network

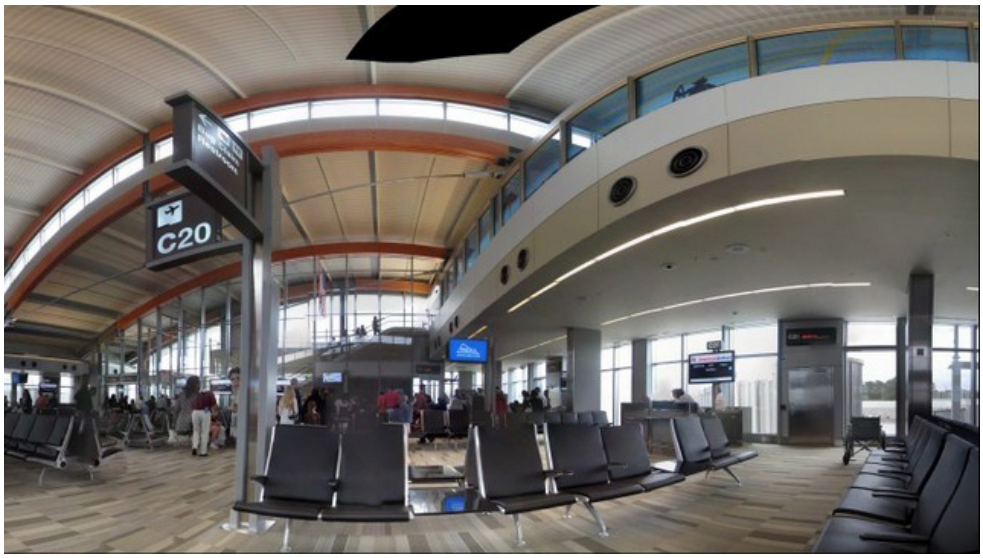
Airports are hubs for more than aircraft. They offer a centralized point of interaction for people, organizations, technology, and communities. Airports are also an integral part of our national security. Given the unique position of an airport within its geographic and economic surroundings, it is critically important for aviation facilities to deploy secure crisis communications systems that deliver essential information, situational awareness, and real-time alerts and warnings during emergency situations.

Internal communications within airport perimeters have historically been systems of stand-alone modalities, using mobile fire and police radios, PA systems, fire annunciators, and strobe lights, with little coordination among the individual elements. The growing need to deliver alerts and warnings to external organizations and governmental agencies has only served to highlight how existing communications at airports are ready for an upgrade.

Airport executives often regard EMNS as a commoditized service where inexperienced vendors compete on price, using limited feature sets that inadequately address the full range of airport requirements. However, networked crisis communication already delivers secure, cost-effective communications platforms that streamline internal communications, empower people, and enable emergency communication and collaboration to an entire airport ecosystem.

Secure, scalable networked communication transcends devices, firewalls, radio frequencies, channels, jurisdictions, and talk groups. As the ability to share important information about an incident is enhanced, people and organizations gain the knowledge and perspective needed to respond appropriately. Credibility is increased for airport operators and responding partners, demonstrating that they are capable of acting in a highly coordinated manner. Synchronization must take place across a broad geographical area – with the airport at the center.

Airport authorities need to protect passengers, employees, vendors, and surrounding neighborhoods, as well as their reputations. A carefully researched investment in networked crisis communication is central to safety and security for each of these constituencies.



Best-of-Breed Networked Crisis Communication

Ease of Use

- ☑ The technology must be simple to adopt, with a tiered permission structure to protect emergency content.
- ☑ The system should be intuitive to deploy, manage, and operate, with real-time operation fully secured against attack or misuse.
- ☑ It must be possible to alert surrounding communities within the same workflow of the core emergency communication system.

Positive Control

- ☑ Privileges should be based on role, not personal identity, so that unexpected changes in personnel do not interrupt emergency response.
- ☑ Rapid coordination is possible with key personnel across an airport's extended ecosystem, including federal, state, and local agencies, onsite commercial tenants, healthcare, and offsite vendors.
- ☑ An activity log and customizable reporting for the after-event assessment and compliance is critical.

Comprehensive Reach

- ☑ The technology should foster collaboration and communication between on- and off-site airport agencies and organizations, passengers, and the general public at-large to improve daily operations and emergency crisis management.
- ☑ Real-time communications should be possible with any device, including two-way radios, wired telephones, mobile phones and tablets, email, and SMS.
- ☑ Integration is needed with existing systems, including passenger and crew information displays, VoIP telephone equipment, perimeter fencing, and public announcement (PA) devices.

Situational Awareness

- ☑ Integrated data should be available from a wide range of safety, security, and operational resources, including images and videos received directly from on-scene first responders.
- ☑ The airport operations center must be able to deliver maximum situational awareness and ground zero intelligence to protect lives and property during any crisis to authorized internal personnel and external industry partners.

Performance Standards

- ☑ Acceptable solutions must include secure, flexible technology that exceeds industry and government standards, and should have a proven, global record of accomplishment.
- ☑ The system must be scalable with the ability to adapt to existing workflows and scenarios.

Appendix: Best Practices for Leading Implementations

The Transportation Research Board of the National Academies report on Emergency Management Best Practices recommends the following attributes to ensure a strong, collaborative relationship between emergency management and airport officials:

- ☑ Demonstrated support from airport senior management
- ☑ An airport emergency manager, in a full-time position or major collateral duty, senior enough in the organization to have visibility and influence
- ☑ Clarity regarding roles and responsibilities
- ☑ Designation of liaisons within parties
- ☑ Consistent updating of information regarding roles, responsibilities, resources, capabilities, and constraints
- ☑ Joint training, drills, and exercises that are realistic and challenging enough to test procedures and relationships
- ☑ Effective after-exercise and after-action reviews
- ☑ Airport and general community awareness of the strong link between EM and business continuity planning
- ☑ Active airport participation in local and regional emergency and disaster organizations or boards
- ☑ All of the above are critical elements of a robust, scalable, networked crisis communication system.

About BlackBerry

BlackBerry is securing a connected world, delivering innovative solutions across the entire mobile ecosystem and beyond. We secure the world's most sensitive data across all end points – from cars to smartphones – making the mobile-first enterprise vision a reality. Founded in 1984 and based in Waterloo, Ontario, BlackBerry operates offices in North America, Europe, Middle East and Africa, Asia Pacific and Latin America. The Company trades under the ticker symbols "BB" on the Toronto Stock Exchange and "BBRY" on the NASDAQ. For more information, visit www.blackberry.com.

Authors

Captain Laponda Fitchpatrick (Retired) was responsible for ensuring the safety, security, and regulatory compliance of the global gateway known as LAX and its satellite airports for over thirty years, retiring as a commanding officer within the Los Angeles Airport Police Department (LAXPD). LaPonda is a nationally recognized aviation security and law enforcement expert that has developed security systems, methods and procedures, and professional standards that are utilized by a myriad of local, state, federal, and international aviation security and law enforcement agencies that secure the global aviation environment. LaPonda has been a member of the American Association of Airport Executives (AAAE) Transportation Security Services, Training, and General Aviation Airports Committees, and the National Cargo Task Force that have made recommendations to local, state, and federal agencies in the development of aviation security related policies, procedures, regulations, and training.

ARFF Chief Jim Lonergan has been involved in firefighting for thirty years with three additional years in fire service related teaching, training, and investigations. Jim was the National Coordinator of Aircraft Rescue and Firefighting (ARFF) Training and Certification programs at the American Association of Airport Executives (AAAE), ARFF Chief at Trenton/Mercer airport in Trenton, NJ, ARFF Chief at Boston/Logan IAP, and at Philadelphia International Airport. Jim has completed the National Fire Academy (NFA) Fire Instructor Level 1 and 2 through the University of Maryland, Fire and Rescue Institute as well as the Train-the-Trainer course for aircraft rescue and firefighter, initial and recurrent training. Jim served on the Mayor's Blue Ribbon Panel for Homeland Security and Emergency Management for Los Angeles International Airport.

Assistant Chief John Linstrom (Retired) is the Business Development Manager at AtHoc assigned to the Public Safety and Aviation markets. He has spent the past thirty years in military, municipal, special district, state, and federal government agencies as an emergency manager, fire chief, and mass fatality team commander. John wrote the Part 139/107 Airport Emergency Plan for Southern California Logistics Airport, and served on the Mayor's Blue Ribbon Panel for Homeland Security and Emergency Management for Los Angeles International Airport. He has also contributed to the Federal Interoperable Mass Fatality Concept of Operations Plan, and the National Transportation Safety Board (NTSB) Interagency Agreement (IAA) and Memorandum of Understanding (MOU) with the U.S. Department of Health and Human Services.

Sources:

1. FAA Advisory Circular AC No: AC150/5220-31C, May 1, 2010: http://www.faa.gov/documentLibrary/media/150_5200_31c_chg1.pdf
2. Transportation Research Board of the National Academies. (2014). Effective Cooperation Among Airports and Local and Regional Emergency Management Agencies for Disaster Preparedness and Response: A Synthesis of Airport Practice.
3. Ibid.
4. https://www.congress.gov/bill/114th-congress/house-bill/615
5. Ibid
6. https://www.congress.gov/bill/114th-congress/house-bill/720
7. Department of Homeland Security. The National Response Framework . Base Document. Washington, D.C., USA: Federal Emergency Management Agency. http://www.fema.gov/pdf/emergency/nrf/about_nrf.pdf