

We've Got to Talk: Emergency Communications and Engineering Ethics

Karl D. Stephan

*Department of Engineering and Technology
Texas State University—San Marcos
San Marcos, TX 78666
kdstephan@txstate.edu*

Abstract

Emergency communications technology has rarely been considered from the point of view of engineering ethics. But as recent large-scale disasters such as the World Trade Center attacks and Hurricane Katrina have shown, the failure of emergency radio systems to work as expected can lead to casualties that could have been avoided.

The problem is not a purely technical one. While advanced digital communications systems are available to first-responder agencies, the way these systems are designed and procured by individual jurisdictions means that the interoperability and excess capacity needed in large-scale disasters is usually unavailable.

In this paper, we show some of the main causes of emergency communications failures in major disasters, how they arise from structural and managerial as well as technical causes, and how these problems may be addressed more effectively in the future.

1. Introduction

When Hurricane Katrina hit the Gulf Coast on Aug. 29, 2005, it killed over a thousand people, destroyed billions of dollars' worth of property, and caused a flood that forced the evacuation of most New Orleans residents for months. The sheer magnitude of the disaster and the sense that more could have been done to prevent loss of life and property have eclipsed some less visible but nonetheless important lessons that the Katrina disaster taught us. This paper deals with the question of emergency communications: how they can fail in disasters such as Katrina and the World Trade Center attacks, why they are so nearly invisible except in times of crisis, where ethical responsibility lies when communications systems fail, and what might be done to improve matters.

There is abundant evidence that emergency communications failures contributed to the magnitude of the Katrina disaster. According to a report entitled *A Failure of Initiative* which was issued in February of

2006 by the U. S. House of Representatives, most of the communications infrastructure of the New Orleans police, fire, and emergency response organizations was destroyed in the early hours of Katrina's landfall. This left the city's emergency responders without means to issue orders or gather information from the field. As any general knows, communications is vital to command and control of operations, and the almost complete failure of electronic communications (landlines and radio) left policemen, firemen, and EMT personnel on their own, dissolving organizations into isolated individuals [1]. The Federal Emergency Management Agency could have positioned sophisticated portable emergency communications facilities in New Orleans, but waited to be asked by the city. The request failed to come before the hurricane struck [2]. With many cell-phone towers down and telephone exchange buildings flooded, almost the only electronic communications devices that could operate immediately after the storm were satellite telephones. In 1999, the State of Louisiana had used Federal funds to provide each of the state's parishes with a satellite phone. However, a year before Katrina, the state notified the parishes that it would no longer cover the monthly \$65.00 access fee. As a result, all but three of the parishes sent the phones back to the state rather than pick up the fee [3]. Jefferson Parish, which includes most of New Orleans, was one of the three, but a single satellite phone did little to alleviate the communications problems that arose after Katrina hit.

A similar tale could be told about emergency communications failures at the World Trade Center during the attacks of September 11, 2001. The 9/11 Commission's report issued in July 2004 described how difficulties with the Fire Department of New York's radio communications probably contributed to the failure to evacuate the North Tower after the collapse of the South Tower [4]. As a result, numerous firemen and other emergency personnel died needlessly. On the other hand, a report on the local emergency response to the crash of a jetliner into the Pentagon the same day shows how enough foresight, resources, and coordination among Federal, state, and local officials can create communications systems that survive unexpected kinds of

emergencies and enable fast and effective rescue efforts [5].

2. Basics of emergency communications technologies

In order to understand the way emergency communications systems can fail in a crisis, one should have a basic knowledge of how the various systems operate and intercommunicate. A comprehensive picture of such systems would include telephones (mobile and fixed), computer-network-based systems using the Internet and private fixed networks, public broadcast media such as radio and television, and mobile radio communications. In order to narrow the scope of this paper to manageable proportions, we will concentrate on mobile radio communications, which are both the most critical in the early stages of many emergencies and the most prone to certain kinds of failure.

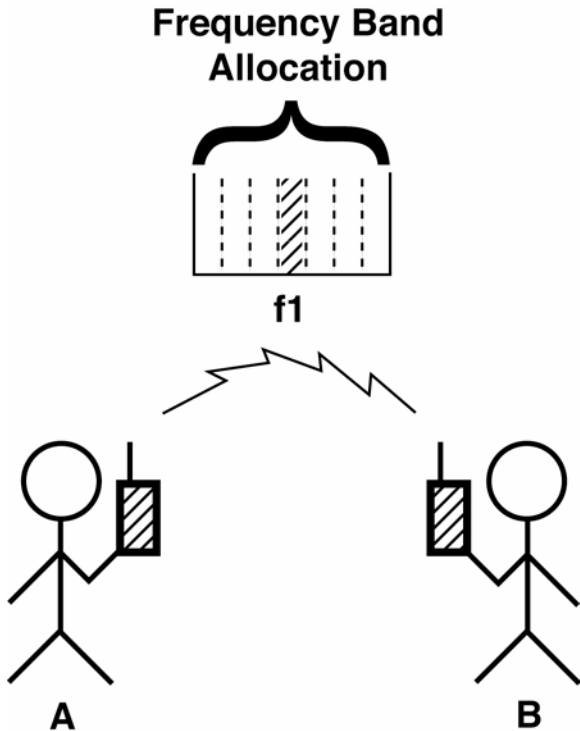


Fig. 1. Elementary two-way radio system.

The most elementary two-way mobile radio system is shown in Fig. 1. Persons A and B each have a two-way radio which contains a transmitter and a receiver. When A wants to talk with B, she keys her transmitter, which broadcasts on its assigned frequency, and the transmission is heard by B. When B wants to talk, A must cease transmitting so that B can transmit. Only one

user can transmit on a single frequency at a time. In this system, one frequency channel allocation is required, and is shown in the "Frequency Band Allocation" diagram as a single line marked f_1 . The radio spectrum is a limited resource whose users must abide by the regulations of the Federal Communications Commission, which determines who can use what frequencies in a given band. The exact details of frequencies and channel spacings are not germane to this discussion, except for the fact that they are a limited resource. Most frequencies used by handheld radios are in the VHF or UHF portions of the radio spectrum, and can travel basically only by line of sight. This is both a disadvantage and an advantage. It means that parties A and B in Fig. 1 can talk with each other only when they are within radio range, which can be a distance as great as several km in open country, or only a few meters inside a cluttered building. On the other hand, the fact that their signals die out after a certain distance means that other users in other parts of the state (or country) can *re-use* the same frequency f_1 without causing interference, as long as they are not too close to A and B. If a nearby third party on the same frequency attempts to transmit while A and B are having a conversation, a blockage or interference occurs, and no one can hear anything intelligible. So although the system in Fig. 1 works well between two persons over a limited distance, it is clearly inadequate for larger-scale operations.

The basic technological design of the typical police or fire mobile radio system was established in the late 1930s by radio experts such as Daniel Noble, who originated many of its features when he designed the first two-way FM police radio system for the State of Connecticut [6]. A form that is in widespread use today is shown in a simplified version in Fig. 2. Mobile users each have access by a control on their radios to one of two channels denoted as 1 and 2. In this system, each channel number is associated with a unique fixed slot in the frequency band allocation. Channel 1 might be reserved for conversations with the dispatcher, whose *base station* usually has a more powerful transmitter than the mobile stations and can cover the entire region of interest. Another channel, f_2 , might be reserved for communications between mobile units. This basic idea can be extended to more than two channels, but it is clear that along with the hardware, some protocols must be established as to who will use which channels for what purpose. In a well-coordinated communications organization, these protocols determine who can use certain channels and what procedures for avoiding congestion and confusion should be followed. With two or more channels available to the organization, two or more independent conversations can be carried on without interference, but only if all parties know which channel to use and when.

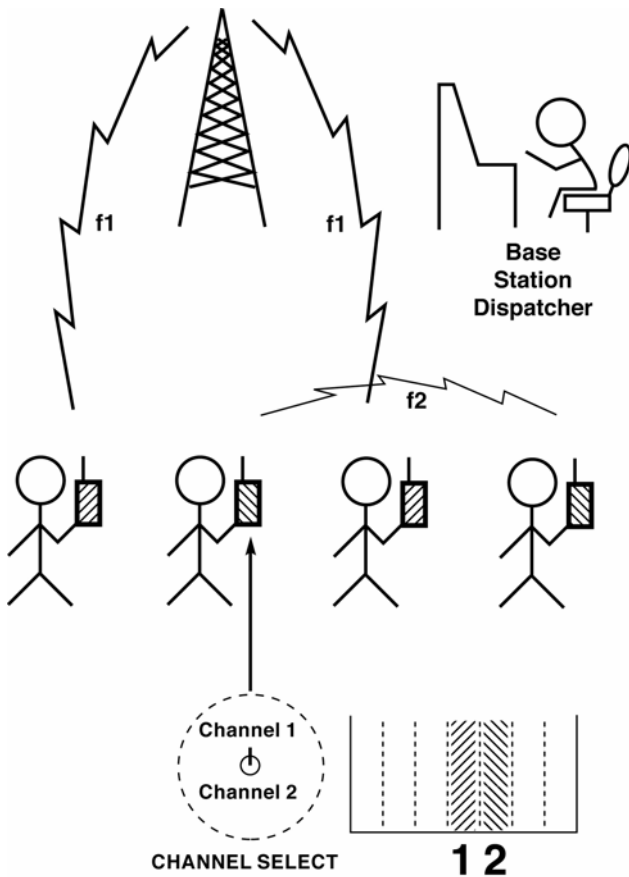


Fig. 2. Multichannel two-way radio system.

One drawback of the system in Fig. 2 is that each user is responsible for choosing which channel to use. If too many users start talking at once, it becomes difficult or impossible to find an "open" (unused) channel. Because certain channels are assigned for certain purposes, one cannot simply go to an unused channel and start talking without causing even greater confusion.

Many of these problems are addressed by a development made possible by computer technology. Known as the *trunked radio system*, a simplified version is illustrated in Fig. 3 [7]. In a conventional system, the choice of actual frequency channels is up to the individual user, who must hunt for an open channel if the system becomes congested. A trunked radio system relieves the user of this responsibility by remotely assigning frequencies in real time based on channel congestion and other factors. In a trunked radio system, a computer at a base station controls the actual frequencies used by each radio. In this system, the channel designation is replaced by the term *talkgroup*, meaning a certain group of users. All the paramedics in a given town might form one talkgroup, for example. In Fig. 3, there are two talkgroups denoted "FIRE" and "POLICE." When a radio

user selects a certain talkgroup, the computer finds open frequency channels and coordinates the transmit and receive frequencies of the proper radios on a moment-by-moment basis, instructing each radio which frequency to use for transmitting and receiving. The computer has the flexibility to use any available frequency for any purpose, unlike the users in the conventional system in Fig. 2, which must abide by agreed-upon frequency designations. This flexibility typically allows the trunked radio system to accommodate more users in a given frequency band allocation than the conventional system of Fig. 2. However, the trunking computer must be in constant contact with every radio in the system, which puts additional requirements on the base station. If for any reason the base station fails, the trunked system reverts to a simpler mode of operation, and many of the trunked system advantages are lost.

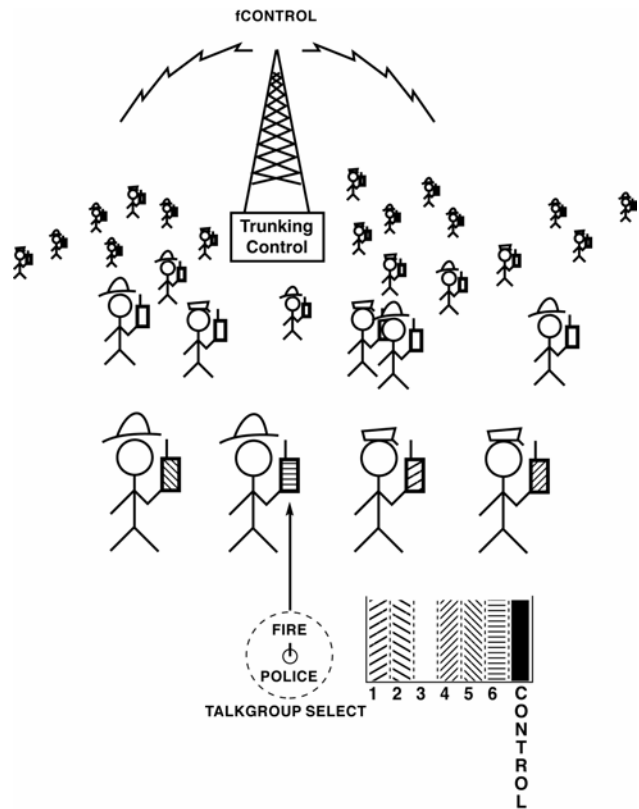


Fig. 3. Trunked two-way radio system.

3. The interoperability problem

With these technical basics understood, it is important to realize that the emergency communications systems in the U. S. are owned and operated by thousands of

individual municipalities, counties, authorities, regions, and states. Emergency communications technologies follow paths of governmental authority. This means that while a given system may provide reliable communications within the governmental unit that purchased it, that unit may not be able to talk with other organizations nearby. This is known as the interoperability problem.

In most small- and medium-scale emergencies—traffic accidents, fires, crime scenes—the average emergency communications system performs so well that it receives little attention. But in large-scale emergencies that call for the attention of two or more organizations, the need for members of different organizations to talk with each other presents a problem. None of the systems shown in Figs. 1 to 3 is designed to deal with other systems. In fact, in order to *prevent* interference between systems in adjacent municipalities, frequency assignments are usually completely different for systems in close geographic proximity. This means while everyone in City Z's fire and police departments may be able to communicate with each other, no one working for City Z may be able to talk with emergency workers in Suburb Y right next door, whose system was sold by a different vendor and whose frequency assignments are different.

The need for interoperability has been recognized for some years and has been addressed in different ways. A relatively inexpensive solution is for organizations in a given region to agree on what are called "mutual aid" channels. These are frequency channels that each organization sets aside for the express purpose of communicating with other organizations. Since these channels are seldom used, there are usually not many of them, and their capacity is therefore limited. A more costly interoperability solution is the purchase and use of an interface device. An interface device consists of multiple transmitters and receivers with computerized crossover switching that can be set up quickly to provide communications channels between two or more incompatible radio systems, as well as between the radio systems and land-based communications networks such as telephones and the Internet. Vendors such as Raytheon and Communications-Applied Technology sell radio interface devices that are portable enough to be trucked or airlifted to an emergency site and set up within the first hours of a disaster [8]. When these systems are set up properly, they can alleviate many of the problems that arise when first responders from multiple jurisdictions need to communicate. But since these units are expensive and receive little or no use except in the rare large-scale emergency that requires extensive communications among jurisdictions, they are often not available, or if available, not used when needed because of lack of training or proper procedures.

In the Katrina disaster, nearly everything that could go wrong with communications systems did go wrong. With the main New Orleans base stations physically demolished, little coordination was possible among individual emergency workers, whose battery-powered radios failed after a day or so of use without electric utility power available for recharging. Admittedly, the New Orleans flood was a rare mega-disaster which no technological system of any complexity was likely to survive. But simple measures such as making satellite telephones more widely available could have been taken to deal with the unlikely event of such a widespread crisis. At the World Trade Center disaster, witnesses recounted how the existing radio systems were simply overwhelmed by the number of users trying to communicate at one time [9]. Why did so many emergency communications systems fail precisely when they were most needed? And who, if anyone, is responsible? To gain a better understanding of this question, we must look beyond the technology to the way emergency communications systems are developed, funded, and sold.

4. Systems on the margins

In researching this article, I consulted several books on telecommunications and emergency preparedness. The subject of emergency communications seems to fall on the margins of most treatments. In the 500-plus-page *Essential Guide to Telecommunications*, a total of seven pages are devoted to various aspects of emergency communications such as portable cell-phone towers and satellite phones [10]. The *Transportation Disaster Response Handbook* has only a two-page section on "communications and information," including public-relations information as well as emergency first-responder communications [11]. And public-health-oriented books scarcely mentioned the issue, although one did have several pages describing the basic types of communications technologies available [12].

This pattern of finding the subject of emergency communications on the margins of discussion prevails not only in academic circles but in public policy and budgeting as well. Statistics on how much money is spent on emergency communications systems by local, state, and federal agencies are difficult to obtain. But considering the budget priorities of the typical medium-size municipality, most public-safety money probably goes to salaries and personnel and to highly visible equipment in frequent use. Radio and communications gear is considered a type of utility in which maintenance of the *status quo* is often the best that can be expected. But as we have seen, the *status quo* is not nearly good enough in large-scale emergencies.

Some idea of how expensive it would be to make a significant dent in the interoperability problem can be obtained from a bill introduced on Mar. 10, 2005 in the U. S. House of Representatives. H. R. 1251 cited a Public Safety Wireless Network study which claimed that nationwide interoperability might cost as much as \$18 billion [13]. This study was performed on behalf of what is now the Department of Homeland Security's SAFECOM program, a communications program of the Department's Office for Interoperability and Compatibility which issues standards and coordinates efforts of local governments to deal with interoperability problems. The U. S. National Institute of Standards and Technology (NIST) also conducts several programs and research projects related to public-safety wireless communications [14]. Laudable as these nationwide efforts are, the recent experience with Hurricane Katrina shows that not all local or state jurisdictions have done all they can in this area. But is it really their exclusive responsibility? When an emergency communications system fails, who is to blame? And what can be done to prevent similar problems from cropping up when the next disaster arrives?

5. Ethics of emergency communications failures

Communications technologies have historically taken a free ride on the engineering ethics bandwagon. By that I mean they have been viewed by most parties as either close to ethically neutral or as a force for fairly unambiguous good. I have been involved in radio or microwave communication technology at some level for more than twenty-five years. The only situation I can recall in which communications technologies of any kind were even remotely involved in discussions of engineering ethics concerned the role of satellite television, and later the Internet, in spreading pornography. While the Internet has proved to be very profitable for pornographers, no one to my knowledge has attributed a basic moral failure to the designers who gave us the Internet simply and solely because it can be used to transmit pornography. There seems to be a general consensus both among ethicists and the general public that the responsibility for evil, wicked, or harmful communications lies primarily with those who originate the message, not with the engineers who provide the originators (and everyone else using the medium) with the technology required. And in the case of communications that result in good effects, which one hopes will include nearly all messages sent via emergency communications systems, there is no question that the presence of such technologies is a social good, not an evil.

But what if communications technologies expected to be available in an emergency suddenly fail? When an emergency technology is something mechanical like a fire escape that collapses in use, most people would ascribe some responsibility to the designers of the fire escape, or to the owners of the building who could have maintained it better. But in the case of a two-way radio that becomes unusable in an emergency due to channel overloading, the engineers who design these systems usually escape notice. Why?

One reason is that if a person falls to his death from a collapsing fire escape, the connection between the mechanical failure and the fatality is clear, obvious, and immediate. The harm that results from a failure in communications is less clear. The nature of time guarantees that we will never know for sure what people might have said and done if they had only had the opportunity. Nevertheless, a system that works well most of the time creates an expectation in the minds of users that it will continue to work well, no matter how big the emergency. When emergency communications systems fail, the results can be just as fatal as a collapsing fire escape, as the examples of the World Trade Center fires and Hurricane Katrina have shown.

Legally, when a vendor sells a system to a purchaser such as a municipality or public-safety agency, there are both express and implied warranties involved. An express warranty is spelled out in so many words in a contract or bill of sale, and specifies that under such-and-such conditions, the equipment will do so-and-so. Most radio-based communications technologies have such specifications, but they are highly technical and do not easily translate into actual performance specifications under the highly variable conditions to be found in the field. Emergencies are by definition unusual circumstances, and during them equipment may be used in locations and ways that would be either difficult to test in advance or simply inconceivable.

The other type of warranty is an implied warranty. An implied warranty is "based on the circumstances surrounding the sale" [15]. At a baseball game, if you buy a hot dog from a vendor you expect it to be at least reasonably edible, and not composed of sawdust and yellow paint, for example. Some things are established without explicit warranty simply by custom and tradition. The liquid that comes from a gas pump should be gasoline, not water; the electric utility delivers power at a voltage sufficient to light your lamps and not blow them out instantly; and when you pick up a telephone or a two-way radio, you should be able to communicate with someone.

Since every mobile radio communications system has access to a limited number of channels, they each have a maximum capacity which cannot be exceeded without

incurring problems. This is a fundamental property of communication over shared channels, and has been understood on a technical level for many decades. The sophisticated statistical analysis needed to estimate the likelihood that a given number of users will be able to "get through" in a given time was developed largely by telecommunications organizations such as Bell Telephone Laboratories, and is called traffic theory. Unfortunately, it is in the nature of such statistical theories that the answer to a given problem is also stated in terms of probabilities. That is, one cannot simply say, "Beyond x number of users, this system will absolutely fail," because the communications difficulties grow gradually as the number of users increases. Blockages become more frequent, wait times lengthen, and gaining access to a desired channel becomes more difficult. The situation is analogous to problems most people face with a more familiar kind of traffic: freeway travel in a large city. As rush hour approaches, it takes longer and longer to travel from one point to another, but only occasionally does the system totally break down. While it is possible to express the ultimate capacity of a given communications system in traffic-theory terms, most small and medium-size public safety organizations probably do not have the technical talent that would be needed to make sense out of the results.

The situation many municipalities find themselves in with regard to their emergency communications systems can be likened to a city which contracts with a builder to construct a pedestrian bridge across a river. When the builder finishes and is asked what the safe capacity of the bridge is, he simply says it is safe for all normal circumstances. But if too many people crowd onto the bridge, the bridge simply bends into a steep slope as more people try to use it. At some point, it will become unusable and even dangerous for everyone involved, but neither the bridge builder nor the buyer knows exactly what that point is.

The bridge analogy is not as farfetched as it might seem. The American Society of Civil Engineers maintains an "infrastructure report card" for the U. S., and states that "31.2% of the nation's urban bridges are structurally deficient or functionally obsolete" [16]. Many of the same municipalities and cities whose budgets are insufficient to repair or replace bridges do not have enough money to buy the new technology and training needed to overcome the interoperability problem. But you can be sure that as soon as a pedestrian dies by falling through a hole in a bridge, money will magically appear to repair that particular bridge. It is a sad fact of human nature that statistics and studies of possible future problems do not motivate politicians and public officials nearly as well as a single injury to a live constituent. If particular deaths could be tied to particular pieces of

communications equipment that failed, there might be a better chance to replace or upgrade inadequate systems. But it is the technical nature of such systems to degrade gradually and with little identifiable direct harm. Rather, what happens mostly takes the form of missed opportunities for good. Nevertheless, in the cases cited at the beginning of this paper, there is firm evidence that better emergency communications could have saved lives. The question is, how to get from here to there?

6. Some answers

The ways we can fix inadequate emergency communications systems that break down in large-scale disasters involve technology, but are not limited to technology. As we have shown, the design of current systems, including the interoperability defects we have described, has up to now been dictated by the limited scopes of particular jurisdictions. Much of the problem is economic, and not just in the sense of not having enough money to buy good equipment, but in the sense that no one is willing to spend the extra money to be interoperable if no one else is also spending a comparable amount. There is no incentive for each municipality to spend scarce resources on rarely-used interoperability equipment if the same funds can be used to improve the more frequently used communications systems within the jurisdiction. The technical problems of interoperability have been studied and several solutions have been found, including a computer-based approach that would change the basic paradigms of how emergency communications in a particular region are handled [17]. But as long as the jurisdictional and economic barriers to inter-agency cooperation and coordination remain, any technical solution will be difficult or impossible to implement.

As the efforts to introduce an interoperability bill in the U. S. Congress demonstrate, some believe that the answer lies in increased Federal funding for equipment that individual municipalities cannot afford. In these days of soaring budget deficits, the chances that significant new funds can be found for a problem that is as far out of the public eye as this one are slim, although they should not be discounted. Clearly, since the problem is at least regional in scale and crosses state lines, the federal government should play a critical role. But a federal mandate to play the interoperability game will not be welcomed by cities and towns unless the necessary resources are made available somehow.

Professional organizations such as the IEEE can play an important role in this problem. In April of 2004, the Department of Homeland Security issued a Statement of Requirements for full interoperability [18]. This 192-page document is largely qualitative and descriptive rather than quantitative and technical, but at least

represents an effort to describe in great detail the types of problems that lack of interoperability causes. Each of the numerous vendors of public-safety communications equipment offers comprehensive solutions to communications problems, but these systems are often incompatible with systems from another vendor. To those familiar with the history of technology, the situation is simply another example of how technological advances (in this case, the development of computer-assisted communications technologies such as trunked radio systems and digital communications) lead to improved but incompatible technologies in a given field.

When two or more companies field incompatible technologies, the consequences can be relatively minor, as when Sony introduced the Betamax video tape recording format in competition with JVC's incompatible VHS format. A few consumers bought Betamax tapes that eventually ended up being worthless, Sony lost some money, but eventually the market dominance of VHS led to its becoming a *de facto* standard. But in the case of incompatible and non-interoperable emergency communications technologies, more than a few dollars is at stake. The life of someone reading this article may depend in the future on whether emergency responders can communicate well enough to deal with the next large-scale disaster, whether it be another terrorist attack, another hurricane, or The Big One that is sure to shake California sooner or later. Such a situation cries out for a responsible professional organization such as IEEE to knock some industry heads together and produce a set of technical standards for the public-safety communications industry. These standards will undoubtedly cost some vendors some money. The adoption of standards always does. But experience has shown that the overall benefit to an industry of adopting uniform standards creates enough market stability and consumer confidence to outweigh, in many cases, whatever short-term losses are incurred by those firms whose technologies end up in the standards scrap pile. In the case of emergency communications, there is no excuse for letting the chaotic administrative and political situation continue. Technical solutions are at hand. What is lacking so far is the political and organizational will to decide upon a nationwide solution, and to pursue it in a united and coherent way.

7. References

- [1] U. S. House of Representatives, *A Failure of Initiative* (Washington, DC: U. S. Government Printing Office, 2006), p. 164.
- [2] *Failure of Initiative*, p. 163.
- [3] *Failure of Initiative*, pp. 172-173.
- [4] *Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, DC: U. S. Government Printing Office, 2004), pp. 306-308.
- [5] Public Safety Wireless Network Program, *Answering the Call: Communications Lessons Learned from the Pentagon Attack* (available at Department of Homeland Security website <http://www.safecomprogram.gov/SAFECOM/library/interoperabilitycasesstudies/>, January 2002).
- [6] "Daniel E. Noble, 1901-1980," excerpts from 1978 brochure at IEEE History Center's website http://www.ieee.org/organizations/history_center/legacies/noble.html.
- [7] An easy-to-understand explanation of the technical details of trunked radio systems is at <http://www.commttechreview.net/radoscan/faq.htm>.
- [8] Alan Joch, "Communications Breakdown," Dec. 5, 2005 article published on Federal Computer World's website <http://www.fcw.com/article91601-12-05-05-Print>.
- [9] Mark Benjamin, "Communications Breakdown," Sept. 9, 2005 article published on Salon.com's website http://archive.salon.com/news/feature/2005/09/09/comm_meltdown/index.html.
- [10] Annabel Z. Dodd, *The Essential Guide to Telecommunications*, 4th edition (Upper Saddle River, NJ: Prentice-Hall, 2005), pp. 209-210, 435-437, 465-466.
- [11] Jay Levinson and Hayim Granot, *Transportation Disaster Response Handbook* (New York: Academic Press-Elsevier Science, 2002), pp. 97-98.
- [12] Linda Y. Landesman, *Public Health Management of Disasters*, 2nd edition (Washington, DC: American Public Health Association, 2005), pp. 131-148.
- [13] Available at the Library of Congress website <http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.1251>.
- [14] See the NIST website http://w3.antd.nist.gov/comm_net_ps.shtml for a listing of several current and past projects.
- [15] "Warranty" definition, law dictionary at the website www.law.com.
- [16] American Society of Civil Engineers, "National Fact Sheet" at <http://www.asce.org/reportcard/2005/page.cfm?id=145>.
- [17] Balachandran, K.; Budka, K.C.; Chu, T.P.; Doumi, T.L.; Kang, J.H., "Mobile responder communication networks for public safety," *Communications Magazine, IEEE*, vol.44, no.1, pp. 56- 64, Jan. 2006.
- [18] Available at http://www.safecomprogram.gov/SAFECOM/library/technology/1200_statementof.htm.