TECHNOLOGICAL FAILURE AND DISASTER RESPONSE: WHEN THE LIGHTS GO OUT, CAN YOU SEE THE INSTRUCTIONS TO START THE GENERATOR?

Charles Kelly
Disaster Management Consultant
Suite 309, 7758 Wisconsin Ave., Bethesda, Md., 20814, USA,
Internet:72734.2412@Compuserve.com

KEYWORDS: disaster management, system failure, appropriate technology

ABSTRACT

Responding to disaster involves a variety of technological devices to collect, store, process and deliver information and assistance. Technology is seen as a means of making disaster response more effective and efficient. However, technology is not 100% reliable. A failure of a key technology can cripple a response effort and make a mockery of the concept of disaster response.

The paper defines what constitutes a key technology in disaster response and summarizes the roles technology fill in the disaster response effort. A preliminary description of the types of technology failures and their impacts is developed. Suggested methods to minimize the impact of technology failures include fault analysis, redundancy, limiting reliance on technology and redefining technological needs. Potential problems with using these methods are identified, as are areas for further research.

I. INTRODUCTION

Technologies are vulnerable to failure. The impact of a failure is more severe if the probability of failure is not considered in the use of a technology.

The use of technology in disaster response should include steps to counter-balance failure through mitigation measures. Mitigating the impact of technological failures on disaster response makes the disaster response effort more effective by minimizing diversions from the main objective -- dealing with the disaster and saving lives.

A common concept is that more, and more advanced, technology makes for better disaster response. This paper is based on a different perspective, that disaster response technology can become an end in and of itself, with the disaster victim forgotten in the glare of shinny new gadgets. The paper assumes that: (1) disaster response technology does not need be complex to be effective, and (2) a critical review of the roles of technology in disaster response will improve the use of technology in dealing with disaster.

The paper is a preliminary attempt to define relationships between the use of technology and the effectiveness of disaster response. The materials presented are intended to serve as a point of departure for work to improve the use of technology in disaster response.

II. TECHNOLOGY AND THE RESPONSE TO DISASTER

In this paper, technology is defined as "the application of knowledge for practical ends (Random House, 1994)." At a basic level, a specific technology is composed of a power source, which, when engaged, initiates a process with a definite outcome. The power source can be mechanical or electrical and the process can be transparent or opaque (i.e., black box).

An operator initiates a technological action in anticipation of a specific outcome. However, the outcome is not always either controlled or what is intended by the operator. The relation between the actual and intended outcome defines the degree of success or failure of a technological action.

A technology requires neither complexity nor elaborate form to be effective. Three levels of technology can be identified: (1) the unit, the smallest functional piece able to accomplish an action, (2) the system, an interdependent grouping of units intended to produce a specific outcome; and (3) the structure, composed of systems which operate with each other directly or indirectly, depending on the user's intended outcome (after Perrow, 1984).

The term *disaster response technology* refers to technology used at some stage of dealing with disaster. A response technology can be developed specifically to deal with disaster problems or, more often, is a common technology adopted for disaster response use.

This review is based on the concept of a "key" technology as one where a failure of the technology to perform as anticipated results in a serious threat to life or well being. A technology used incorrectly or

inappropriately, resulting in a threat to life or well being, is considered a key technology. The key nature of a technology can exist at the level of a threat to individual well being or at the level where the technology serves a vital role in the operation of broad efforts to save lives.

Technology fills important roles in disaster preparedness, planning and mitigation. Most often, these uses are within the context of a technology's normal purpose and address no key need vis-a-vis immediate life or well being. The difference between disaster preparedness, planning and mitigation and disaster response is the presumption for the latter that action is necessary within a specific time frame to prevent immediate death or damage.

The exception is where immediate action is intended to mitigate an expected disaster. In this case, mitigation objectives are time defined and the mitigation actions have the same objectives and urgency as a post disaster response effort.
As discussed in an earlier paper (Kelly, 1994), the uses of technology for disaster management are wide and varied. Some technologies are event specific, many have multiple uses (e.g., satellites, computers). Areas in which technology can support the response to disaster include:

* Data collection and analysis
* Communications
* Transportation
* Personal protection
* Infrastructure
* Health care

The greater part of technologies used in disaster response are those immediately available to victims to respond to a disaster. These technologies include engineered structures; capacities that need not be imported to be used in a disaster response; or technologies not normally used for disaster management. The sophistication of these technologies relates to the developmental level of the affected locale (Kelly, 1994).

In responding to a disaster, externally provided technologies are usually intended to fill a perceived gap in local capacities or to provide support for external assistance providers. In filling this latter role imported technologies can be of little direct use to the disaster victims but of key importance to the assistance providers' efforts.

III. TECHNOLOGICAL FAILURES

Technology fails for a variety of reasons, under a variety of conditions and with a variety of impacts. The presumption in this paper is that a technology used in disaster response is either inconsequential (i.e., for appearance's sake) or important. Thus, failures either have no consequences on the delivery of assistance or a negative impact.

Failure occurs when a technology does not perform as anticipated. Technologies are designed to be used for a specific end. Getting an unanticipated result constitutes a technological failure: the user is not in control of the technology.

A generalization is that technologies fail when used in ways for which they were not designed. However, not all technologies fail when used in an unplanned manner, nor do all unanticipated technological performances have negative outcomes. For instance, failure can prevent a technology intended to do damage from accomplishing this objective.

Even when an unanticipated outcome does not contribute to the loss of life, the user must take other actions to recover from the unanticipated results and attain the desired objectives. This decreases the effectiveness of a response by increasing work to be done and draws resources from the basic objectives of saving lives and maintaining well being.

A technology used in a manner for which it was not designed, but with a correctly anticipated outcome, is not a technology failure as the technology is within the control of the operator. These unintended but innovative uses of technology are probably most common in disaster victims' own efforts.

The causes of failure can be divided into those arising from: (1) a physical failure of a technology or (2) a failure to design a technology to take into account an appropriate use or situation. A physical failure can arise from a design problem, from the misuse of a technology or from damage by an external agent. The failure of a technology can be classified under the following headings, expanded from materials in Normal Accidents (Perrow, 1984) and Guidelines for Hazard Evaluation Procedures (Center for Chemical Plant Safety, 1985).

* Component: failure of an element within a stand-alone unit due to design or physical problems relative to the ability of the component to function as intended. Component failure includes situations where a unit suffers physical damage, as failure is caused by the damage to a component of the unit.

* Unit: failure of a stand-alone piece of technology, as when a unit fails to perform as expected (or at all) when no physical damage is experienced, power is available and appropriate operating instructions are provided.

* System: failure of a group of interrelated technologies (i.e., sub-systems), with origins in: (1) the failure of one

unit to function, rendering dependent units inoperative; (2) a unit providing incorrect input into other units, resulting in unanticipated outcomes; and (3) a unit providing incorrect feedback (as opposed to instructions), resulting in the system failing to take or continue an action.

* Interface (non-controlled systems): failure of a system to operate due to the failure of an associated but non-controlled system to perform as anticipated. The difference from a system failure lies in the inability of the user or affected technology to control the associated system and directly prevent or resolve the associated system's failure.

* Inappropriate Use: failure of a unit or system as a result of use not appropriate for the intended outcome or for the circumstances (environment) under which the technology is used. Where used unconventionally with a realistic expectation of outcome, the technology would be used appropriately in an unconventional manner.

* Complexity: failure due to unanticipated interactions of units in the system. This type of failure is expected in complex systems where system integration poses design and operating difficulties. Causal events include: (1) an unintended use of the system; (2) unanticipated inputs (instructions or data), or (3) conflict between instructions originating from different parts of the system.

* Operator: failure due to incorrect actions by an operator, including a failure to provide power. These actions can be intentional or unintentional. Operator failures can have positive impacts, although the assumption is that operator induced failure is a negative event vis-a-vis the disaster management effort. The intentional misuse of a technology (i.e., use for which the technology is not designed, but with a correct expectation of outcome) would not be a technology failure, per se, although it would have a negative effect on the response effort.

IV. MITIGATION OF POTENTIAL TECHNOLOGICAL FAILURES

Several possible approaches to mitigate the impact of technology failures on disaster management efforts are suggested below. A division between approaches to mitigating problems by exercising more control over technology and ones of minimizing problems by limiting the reliance on technology should be recognized.

Realistically, a combination of approaches will be most successful in mitigating technological problems in disaster response efforts. The review of the role of technologies in disaster response, integral to each approach suggested, is probably the most important element in defining ways to deal with technological failures.

A. Fault Analysis

The most evident way to limit technological failures is through an analysis to identify possible faults and define mitigation measures. Several techniques are available to conduct fault analysis (Center for Chemical Plant Safety, 1985). When associated with the scenario approach to developing disaster response systems, fault analysis can play a central role in improving response systems.

Fault analysis faces three significant limitations. First, the analysis must cover all possible technologies to be used in the response effort. This is a major task, given the variety of technologies which can be used in disaster response and the possible variations in the use of technologies dependent on the size of a disaster.

Second, it is difficult for personnel to perform fault analysis about technologies on which they are not specialists. Assembling a group competent to review a major portion of the technologies used in disaster response may be impractical. There may be a tendency to presume some technologies are fault free, a presumption that contradicts the purpose of the analysis.

Third, disaster response requires flexibility and innovation, which are difficult to fully define in advance. Thus, a pre-disaster analysis cannot easily review technologies as they may actually be used. This presents a particular problem with the unconventional use of technology.

The unconventional use of technology poses significant risks of failure. The operator is not, in advance, fully certain of the outcome of the technological action. Until an anticipated outcome occurs, the conventional expectation is that the unconventional use will be a failure. Conducting a comprehensive fault analysis under these conditions may not be practical.

B. Redundancy

The simplest, but possibly most expensive, way to minimize technological failure in disaster response is by creating redundant systems. Logically, to keep costs down only those systems filling key functions would be backed by redundancy.

Three limitations in this approach are evident. First, how much redundancy is enough? The answer may be based more on financial limitations than on an analysis of failure risks and operational requirements, thus limiting the usefulness of redundancy in mitigating failure.

Second, adding redundancy increases a structure's

complexity, with the risk of failure then also including the failure of the redundant system. If the same fault exists in both the basic and redundant systems, only an illusion of safety exists. Building redundancy using systems based on different operating methods to produce the same outcome avoids this problem but can significantly increase cost and complexity.

Third, in-depth analysis (i.e., the fault analysis discussed above) is needed to define failure risks, their interrelationships and redundancy requirements. Once the analysis is completed, decisions are made to either upgrade (i.e., remove the fault) or reinforce through redundancy. These actions then need to be reviewed by an analysis of the changed system. The process can become progressively more complex as more and more technology is involved in removing faults and building redundancy.

C. Limiting Reliance on Technology

Another logical approach to avoiding technological failure is to avoid using technology. The reality of operating in a technological world makes it unlikely this approach can be followed. At the same time, an approach of minimizing the reliance on technology could be practical. The concept is not to avoid technology, but to limit the disaster response system's reliance on key technologies.

This approach can be implemented in pre-disaster planning as a process of answering the following questions:

* What is the purpose of the technology? If the technology does not address an immediate life saving need, then it is probable the technology does not fill a key need. When this technology fails, damage to the response effort will occur only if an operator thinks the technological action is necessary and diverts attention to a failure of no importance.

* Can I do without this technology? Part of answering this question involves defining what is a key technology; part requires identifying the string of systems which must operate for a key technology structure to be successful. Technologies which are not critical to the response process need not be discarded, but their failure should not be treated as significant events.

* What do I do if I have to do without this technology? Answering this question meets three needs for an effective disaster response: (1) developing alternate methods to respond despite a technological failure; (2) identifying redundancy priorities (for those few technologies which cannot be done without); and (3) verifying what are key response technologies (as a confirmation to the first question).

The major problems in limiting technological reliance lie in the pervasiveness of technology in daily life and the common perception that more is better. Performing an intensive review of a disaster response structure is time consuming, particularly if it needs to be done regularly to keep pace with changing response plans and new technologies.

Efforts to explicitly limit reliance on technology will run into problems with those who feel technology can be made fail safe or that technological fixes can minimize the risk of failure. Dealing with these objections can be more taxing and complex than defining what technologies are key to a response effort.

D. Redefine Technological Needs

A fourth approach is to rethink the basic approach to disaster response. The new focus would be on identifying the uses of technologies by disaster victims in their own recovery efforts. The assumption is that victims provide most of the response to a disaster and will use the most appropriate and dependable technologies available. External assistance would support the technologies being used by the victims, rather than trying to lead the response process. Once defined, the victim uses of technology would still need to be subjected to one of the mitigation approaches discussed above.

Two significant problems with this approach are: (1) the difficulties of identifying in advance how a particular group of victims will respond to a disaster, and (2) how to provide supporting technologies while providing training and materials for their use by the victims. Neither problem is insurmountable, particularly for agencies which work at the community level and are able to involve potential victims in the disaster planning and needs assessment process.

For this approach to be successful, procedures for providing assistance need to be flexible and adaptive to the victims' needs. Although straightforward, this process becomes more difficult the further an assistance organization gets from the disaster.

Applying the four methods described above is a progressive process which needs to take into account changes in technologies and response methods. A large disaster response organization should integrate a technology failure mitigation program as a core element of response planning. Smaller organizations should periodically use the reviews of larger organizations to develop mitigation actions.

The prioritization of work to mitigate the risk of technological failure can be accomplished through a two-step assessment of technological structures and

component systems. The first step is to define what are key and non-key technological systems. The second step is to rank the key technological systems by direct importance to life saving and welfare. The top ranked technologies become the priorities for risk mitigation assessment.

V. CONCLUSIONS

This paper raises concerns about the danger of an unquestioning dependency on technology for disaster response. Technology is presented as inherently prone to failure, resulting in risks that the failure of a key technology will cause a disaster response effort to collapse. The result could be additional and avoidable loss of life.

Four methods to identify ways to mitigate the risk of technological failure are suggested. No single method will be effective for all risks to all technologies. Using a combination of methods is practical, but should be based on a pragmatic balancing of a need to mitigate risks with keeping the response process as simple as possible. The terminology used in discussing technological failure affecting disaster response is the same as that used in assessing disaster potentials and response options in general. In short, technological failures affecting disaster response are no different from any technological (or non-technological) failure leading to a disaster.

Efforts to deal with technological failure that affect disaster response should follow the same general preparedness, planning and mitigation procedures used to deal with external events, and be an integral part of a comprehensive disaster management system. The priority is to ensure a response organization does not experience a disaster while attempting to assist victims of another disaster.

This paper provides a perspective on technological failure and disaster management as a base for further exploration. Topics for further work include: (1) defining a practical balance between technological fix and minimalist technology approaches to disaster response; (2) developing a catalogue of technological failures and their impacts on disaster response; (3) developing standard procedures for assessing and mitigating risk of technological failure; and (4) formulating criteria to identify circumstances where unconventional or innovative uses of technology will be used in disaster response. Work in these areas will contribute to making disaster management more effective and successful.

VI. REFERENCES

Center for Chemical Plant Safety, The. 1985. Guidelines for Hazard Evaluation Procedures. American Institute of Chemical Engineers, New York,

Kelly, Charles. 1994. "Responding to Disaster During Conflict: Need for Changes in Disaster Management Techniques". In Proceedings, The International Emergency Management and Engineering Society Conference 1994, James D. Sullivan and Suleyman Tufekci, eds. The International Emergency Management and Engineering Society Conference, Dallas.

Random House. 1993. World Electronic Dictionary (electronic edition).

Perrow, Charles. 1984. Normal Accidents: Living with High Risk Technologies, Basic Books, New York, p. 70.