ENTELEC 2002
REEVALUATION OF PIPELINE SCADA EMERGENCY PLANS IN LIGHT OF THE 9/11/2001 TERRORISM

By Donald B. Ashton
UTSI International Corporation

INTRODUCTION

Many aspects of American life were changed forever on September 11, 2001. Terrorism in the U.S. is now a viable threat that must be addressed. Pipeline SCADA emergency plans need to be reevaluated to address this new reality. This paper presents some ideas on this critical subject.

GENERAL PRINCIPLES THAT STILL APPLY

It may seem like it is a whole new world, since September 11, 2001, but the big picture is unchanged in many ways. Here are some of the enduring truisms:

- **Costs Should Be In Line with the Benefits and Risks**

  Terrorism has changed the risks of doing business in the United States. The budgets to alleviate these new risks are likely to rise. However, the benefits of new security projects must be in line with the costs.

- **Emergency Procedures Need To Be Taught and Practiced**

  Emergency preparedness depends upon the ability of those individuals who are expected to carry out the procedures to actually implement them in the case of a real emergency. A revised emergency response manual is of little value if the operational staff is not trained to follow the new procedures. Emergencies are now more likely to happen, and thus training is more critical than ever.

- **Abnormal Operating Procedures Are Error Prone**

  Many accidents and mistakes occur when workers deviate from their normal routines. Since emergency procedures need to be practiced, there is a risk that the practice will cause problems. This risk needs to be addressed along with the risk of not being prepared for an emergency.

- **Balance is the Key**

In order for a pipeline company, or any other private sector company, to thrive, it needs to remain competitive in its market. To some extent, emergency preparedness is a means of promoting survival, but over-attention to emergency preparedness must not distract attention from tasks that directly enhance profit and success.

- **Many Threats are Unknown**

The real challenge in emergency preparedness is to be in a position to survive *ANY* catastrophe, envisioned or not. An emergency response plan needs to be flexible and adaptable to unforeseen situations.

- **CYA**

Unfortunately, in today's world, being on hand for an emergency makes one immediately a suspect for malpractice and/or criminal liability if things turn out less than ideally. Emergencies are more likely since September 11, 2001. Accordingly, the attention that needs to be paid to CYA preparation is greater than ever.

SOME AREAS TO REEVALUATE

The proper response to the threat of terrorism is to reevaluate the ability of pipeline SCADA systems to survive a catastrophe. The remainder of this paper presents a few areas that should be reviewed. The answers arrived at will vary widely between individual pipeline companies, as they always have.

- **Threats to Address**

A key element of an emergency response plan is to identify the types of known emergencies that are specifically addressed by the plan. The list of addressed threats varies from location to location. For instance, natural disasters such as floods, hurricanes, tornados, earthquakes, and ice storms do not occur in all parts of the country. Some companies will probably now decide to add bio-terrorism, chemical terrorism, attack by airplanes and trucks, and even a nuclear detonation as addressable threats.

- **Size of Emergency Response Budgets Due to Increased Risks**

The risk to gas and liquid pipelines in the Untied States is undoubtedly greater than it was a year ago. Budgets for pipeline emergency preparedness should be increased accordingly.

- **Location of Control Center**

Pipeline control centers are presently located in a great variety of settings. Some are public relations showcases, in clear view of the public. Some have world-class views of mountains or harbors. Some control centers are deep in the ground in bunker-like facilities. Clearly, a wide variety of criteria has been applied to the selection of pipeline control center locations in the past.

It is likely that pipeline operating companies will now want to avoid high profile buildings as locations for their control centers. In addition, factors such as accessibility, defensibility, survivability and other issues will be more important than in the past.

- **Location of Offsite Backup Control Center**

The issue of where to locate the offsite backup control center has always drawn a lot of debate. On the one hand, the offsite center needs to be located where it is not likely to be susceptible to the same catastrophe that might cause evacuation or destruction of the primary control center. On the other hand, the offsite control center needs to be readily accessible and useable in the event of an emergency. Some pipeline operators end up locating their offsite backup centers a few miles from the primary center, while other pipeline operators locate the offsite centers hundreds of miles from the primary centers.

The terrorism of September 11, 2001, calls into question the basic assumptions that lead to either very close or very distant proximity of the primary and offsite control centers. On one hand, massive disasters that might result in the evacuation (or even destruction) of a large metropolitan area are suddenly no longer unimaginable, lending credence to the concept of a far distant offsite control center. On the other hand, pipeline emergency response plans that require jumping into an airplane and flying to the backup center at the onset of an emergency now seem flawed.

- **SCADA Architecture**

Most pipeline SCADA systems utilize either a single control room controlling the entire pipeline system, or a hierarchical network of control rooms with regional centers controlling local sites and a central site overseeing the regional sites. Hierarchical architectures were often initially designed to minimize the mileage-based costs of data communication lines between the control centers and the pipeline sites, a consideration which is largely outdated.

Redundancy has usually been provided by having a hot standby SCADA system at the same site as the primary system, and often a third SCADA system at an offsite location, capable of taking over in an emergency. The offsite backup system is usually manned only during emergencies.

A new SCADA architecture is now being discussed that combines some of the best aspects of traditional architectures. The new concept is to have two "primary" sites, at a considerable distance from each other. Each control room is a 24 X 7 operation and, under normal situations, the operational load of the pipeline is shared between the two centers. The personnel at each center rotate responsibilities in a way that the control of the entire pipeline system can be easily assumed by either center with a minimum of disruption. Such an architecture provides a high degree of emergency survivability, at the cost of some additional routine overhead.

- **Remote Dial-In GUIs for Primary and Offsite SCADA Systems are More Critical than Ever**

Many of the scenarios that would result in evacuation of a pipeline control center are very non-destructive, and will likely result in little to no actual damage to the SCADA system. Some examples are bomb scares, bio-terrorism alerts, chemical terrorism alerts, and poisoned water alerts.

Pipeline control organizations should have an easy way to continue operation of the pipeline during extended but non-destructive forced evacuations of the control center. This scenario might be accommodated by dial-in communications from mobile laptop computers, or from pre-selected contingency locations.

Part of this plan would require insuring that the control center itself is set up to support fairly extended periods of totally unattended operation.

- **Public Awareness of the Control Center Location**

It is debatable whether a pipeline control center would be considered an attractive target for terrorism. However, companies that have showplace control centers would do well to review the merits of the concept.

- **Physical Security of the Control Centers**

The physical security of a pipeline control center is important for many reasons. The fact that an emergency is now more likely than it was a year ago makes physical security even more important. Bad guys should be prevented from entering a control center and causing an emergency, but another important concern is to limit access to the control center to authorized personnel after an emergency is in progress.

- **Security and Survivability of the Communication Network**

Pipeline SCADA communication networks have changed dramatically in recent years. SCADA often shares communication paths with other company departments. Susceptibility of most SCADA communication networks to hacking and physical destruction is greater than it used to be. Many pipeline companies are implementing redundant communication routes to critical remote sites.

- **Vulnerability of the Control Center Versus the Pipeline**

An issue worthy of discussion within a pipeline company is whether terrorists are more likely to target a pipeline control center, or the pipeline infrastructure itself. A company policy on this matter would of course have a large impact on the direction of emergency preparedness.

- **Physical Security of the Remote Pipeline Sites**

Some countries that have traditionally been concerned about terrorist attacks to their infrastructure have standardized elaborate physical security at pipeline compressor/pump and meter stations. Round-the-clock armed guards and continual video surveillance from control centers are common in some countries.

The appropriate level of physical security of the pipeline infrastructure in the United States is an open question. The idea of highly secure stations seems a bit pointless considering the high degree of visibility and convenient access to most pipeline right-of-way in the U.S.

- **Protection from Sabotage**

“Inside jobs” are often the most devastating. Although pipeline SCADA is an area that seems rather unattractive to terrorist infiltration, there may be support functions within a pipeline company that could be targets. The general rule is that the current terrorist threat has “raised the bar.”

- **Assumptions Regarding Continuance of Basic Utilities and Services**

Some SCADA emergency response plans seem to focus primarily on the possibility of the SCADA hardware or software failing. In the new paradigm, consideration also needs to be given to the possibility of failure of the water supply, the gas supply for building heating, public transportation, as well as electricity. Air travel probably should not be an indispensable component of the emergency response plan.

- **Likelihood of New Government Regulations**

The Department of Transportation – Office of Pipeline Safety (DOT/OPS) has in the past responded to emergencies of different kinds with advisories and new regulations. It would not be a surprise if the OPS advised pipeline companies to review their emergency preparedness in light of the recent terrorism.

CONCLUSION

The events of September 11, 2001, have changed the landscape for emergency SCADA response planning. Pipeline operators should review and revise their plans.

Donald B. Ashton, Staff Consultant
UTSI International Corporation
1560 West Bay Area Blvd.
2nd Floor – Suite 300
Friendswood, Texas 77546 USA
(281) 480-8786, ext. 116
(800) 324-8874, ext. 116
(281) 480-8008, fax
dashton@utsi.com