Security of Geographically Dispersed Infrastructure

A White Paper

# Table of Contents

1. Introduction .......................................................................................................................... 1

2. Protecting Geographically Dispersed Infrastructure................................................................. 2

   3.1 Detection/Identification ......................................................................................................... 3
   3.2 Assessment .......................................................................................................................... 3
   3.3 Response and Evaluation ...................................................................................................... 4


5. Using All Available Components ........................................................................................... 7
1. **Introduction**

Protecting critical, geographically dispersed infrastructure requires solutions that provide a common operating picture for decision-makers for all locations, at all times, throughout a security event. An effective security solution must address security detection, assessment, and response requirements in a way that maximizes the use of available information and manpower, minimizes the response to false positives, and integrates data from multiple locations and agencies. By integrating multiple tools into a single workspace and automating as much of the security process as possible, decision makers will be able to more rapidly and cost-effectively protect our infrastructure.
Protecting Geographically Dispersed Infrastructure

Protecting our critical infrastructure and key assets represents an enormous challenge, particularly when those assets are geographically dispersed, separated by hundreds of miles. Damage to federally built or operated civil works – dams, power plants, roads, and other structures – could cause severe economic damage and the loss of countless lives, making them targets of constant threat. However, most security solutions focus only on local assets and do not address all phases of the security life cycle, failing to give decision makers a view of the larger security picture. Cost-effectively assuring the protection of geographically dispersed assets requires integration of many technologies from many locations in a single, easy-to-view format.

Lessons learned from September 11, 2001, indicate the greatest challenge to security is the integration and sharing of information from multiple agencies and jurisdictions. Most systems were designed for the needs of specific agencies, which complicates interoperability and hinders first responders from communicating and coordinating during a crisis. The need for interoperability or integration among disparate systems is critical. Security personnel need to be able to detect and monitor critical events as they happen, assess their impact, and respond in real time – all from a single system. Such integration requires a secure and robust IT infrastructure. In addition, many well-intentioned solutions can overwhelm security personnel with the sheer volume of information that they generate. Security systems must also provide intelligence and automation to streamline event management.

Effective security solutions must take into account detection, assessment, and response in a way that maximizes the use of available information and manpower, minimizes the response to false positives, and integrates data from multiple locations and agencies. The goal is to take advantage of the vast array of sensors, closed circuit television (CCTV) technologies, and security personnel to provide security for our nation’s infrastructure in a cost-effective manner. This can be achieved by integrating currently available technologies and utilizing the existing IT infrastructure.
3. **Security Life Cycle Requirements**

Security and emergency management agencies often discuss emergency events as a life cycle that includes threat identification, assessment, response, and evaluation. When a threat appears, security personnel must identify and locate the threat. They must assess the threat – who, what, when, and how it will strike. They must respond to the crisis according to defined policies. And they recover and evaluate post-crisis needs. In some cases, separate agencies address only a single phase. For example, the Federal Emergency Management Agency (FEMA) focuses primarily on response and recovery. Most technology devices also focus only on one phase, usually in a small geographic area, which means they only can improve a small part of the security process. Although these devices are all necessary, successful security solutions require decision-makers to be able to get an overall picture of security at multiple locations and manage events throughout all phases, from detection to recovery. A common operating picture of widely dispersed facilities must be available to drive the response.

3.1 **Detection/Identification**

Detection has traditionally focused on physical devices ranging from low tech to high tech to detect, deter, and delay access and reduce or negate risk. Barriers such as fences and walls coupled with security personnel has been the traditional approach to securing physical assets through deterrence and sight detection.

Video cameras and CCTV cameras can sometimes provide an extra set of eyes for detection and surveillance as well as assessment. This can sometimes serve as an effective deterrent but is less effective at deterring terrorist actions. Sensors and alarms ranging from motion detectors to balanced magnetic switches on doors and windows also provide detection information. Many organizations use standalone systems tied to external information and sensors. However, in many cases, these systems are isolated from each other and have only local application. The data yielded from the sensors is usable only in a very limited context, and their systems require additional personnel to monitor or man at that site.

A major problem that arises when implementing these technologies is a high incidence of false positive identifications. The technologies by themselves provide valuable capabilities, but together present an overwhelming flow of data that may not yield adequate information to assess a situation. The ability for one person to monitor multiple CCTV or sensor displays becomes greatly reduced as the number of devices increases. This seems obvious yet many security-monitoring facilities continue to use this technique.

One way of improving detection is to integrate sensors and video cameras in a single system to deliver critical information to security personnel. Wherever possible, authorized users need access to all data – video, audio, telephone, radio, intrusion sensors, infrastructure sensors, perimeter monitoring systems, etc. – through a single system.

3.2 **Assessment**

Once the operator identifies a potential intrusion, assessment occurs through video analysis, feedback from the sensor itself, or by dispatching someone to investigate. Video or CCTV
assessment may not provide adequate assessment if the number of cameras to watch is large, the image is unclear, or the operator misses the initial action and cannot replay the appropriate camera quickly. Human response becomes overwhelmingly expensive as our security net grows and the number of false positives increases. Clearly, the amount of data available in a command center requires additional processing and organization to be useful.

![Figure 1: The security/emergency life cycle follows four basic stages – identification, assessment, response, and evaluation.](image)

A geographic information system (GIS) can organize information in a format people are comfortable with and that models their real-world, everyday decision-making process. A GIS can rapidly organize and display useful data, convey vast amounts of information quickly to operators, and is adaptable to local and large geographic areas.

### 3.3 Response and Evaluation

If the operator determines that there is an intrusion, depending on the nature of the threat, the response can vary from one person to multiple agencies. Multiple agency responses become extremely complicated because of difficulties in interagency information sharing. If multiple intrusions occur across a large area, response becomes even more difficult.

A GIS that integrates local and regional situational awareness and communications devices such as radio interfaces and mobile data terminals can help decision makers effectively respond to and evaluate emergency situations. They can dispatch police, fire, emergency medical technicians, HAZMAT, or other agencies as needed. All evaluation tools should be available from one desktop. Using a Web-based common operating picture allows viewing local, state, regional and national events from any location.
4. **Security Decision Support**

In our approach, the operator sits in front of a single computer with one mouse, keyboard, and dual-screen display to maximize the ease of decision-making. One screen shows the map, and the other shows textual information. Instead of actively monitoring all alarms and monitors, the operator interacts with the system to receive and analyze data from all alarms at local and dispersed assets.

Each alarm point is in the database. When tripped, the alarm systems provide data to the integrated framework. The alarms can be an existing sensor or a newly acquired capability, such as cyber intrusion alarms. The system presents information such as alarm type and point of contact on the text screen and automatically zooms the map to the location of the alarm, indicated by a symbol containing a unique event number. This happens in a split second with no operator intervention. At the same time, the camera associated with that alarm pops up in a window and begins displaying video. The camera location, view angle, and orientation are also displayed on the map.

In a few seconds the operator receives a queued alarm with information on type and location – a fiber optic intrusion alarm on a fence, cyber intrusion alarms, a motion detector, or a glass shatter alarm, and so forth. A camera display helps to determine whether an alarm is a false positive, for example, a deer that bumped into a fence. If it is a false positive, the operator can type in a remark and close the event. All the information is logged in a database for later evaluation.

![Figure 2: Data Integration at the User Level](image)

If it is an intrusion, the operator can review all available information, determine the location of the alarms, and see the proximity of events on the map. The system provides the ability to manage response assets. It provides a recommended response and shows the location of available response vehicles, tracked by GPS. The operator sees the progress on the map display and can automatically initiate contact with responsible agencies or send updated images to field personnel.
using car-mounted computers or handheld devices. Within minutes, alarms start going off in other locations. The operator can then follow a preplanned standard operating procedure (SOP) to notify local police, area utilities, management, or other interested parties.
5. **Using All Available Components**

By considering the entire security environment and integrating all available technologies, organizations can use existing and evolving technologies in a way that is cost-effective and provides the appropriate level of protection. The design must maximize use of the existing security system, manpower, and policy while augmenting and integrating cutting-edge technologies and a means to communicate information to regional emergency operations centers. Such an approach is available today.