

## **1. Substations**

Sabotage could cause blackouts because many substations can be easily targeted. Substations present one of the greatest concerns for sabotage. Sabotage can be done by those who normally have legitimate access to the substation, such as construction crews, contracted services, customer or utility manpower, or those with no legitimate access, such as terrorists.

The destruction of well selected substations could cause a serious blackout. In many cases, service to most customers can be restored, depending on the extent of the damage, within a reasonable time. However, the outages would reduce reliability, making some areas vulnerable to additional blackouts. Virtually any major metropolitan area, such as New York, Boston or other multi-state areas would suffer major extended blackouts if key substations were destroyed.

Substations around the US are typically unattended but most have chain link fences, alarmed doors on the control buildings, and lighting. Some utilities have installed video monitoring equipment at key substations, but years of generally low investment in security and the impact of deregulation have cut back on utility security operations to the point where current security staffs are manned at minimum levels and the security technology is generally outdated and poorly maintained.

Security standards for electric power substation physical and electronic security are currently being developed. The standard is a guide that identifies and discusses security issues related to human intervention during the construction, operation, and maintenance of electric power supply substations. CMS has integrated these emerging standards into its energy facility checklist where appropriate. The standards also documents methods and designs to mitigate intrusions. The types of intrusions included are pedestrian, vehicular, projectile, and electronic.

Typical criteria used by IIA for recommending substation security programs are frequency and duration of security occurrences, cost of occurrences, safety hazards, severity of damage, equipment type, number and type, customers served, substation location, design type, criticality of load, cost, probability of occurrence, and quality of service at existing substations. With these criteria in mind, we have noted a number of substations where we recommend that security upgrades take place at a higher priority.

The types of perimeter protection identified at substations (as well as at remote gas facilities) include fences, lights, gates, entrance/equipment locks, guards and other security measures (e.g., gates and electronic security systems, such as Photoelectric motion detectors, Video surveillance systems, Building systems (e.g., alarms), and Computer security systems (passwords, dial back verification, selective access).

Employees can play a valuable role in substation security by taking reasonable precautions against damage or sabotage. Operational and inspection procedures can be utilized to reduce the potential for intrusions. These procedures should include inspection of the perimeter for breaks in the security measures, including padlocks, electronic security systems and alarms, the condition of all warning signs, and the integrity of the fence. Alertness, vigilance and reporting of suspicious incidents by employees will contribute to improved security.

The current overall status of security at most of the substation/remote gas facilities in the US is considered to be at a minimum level.

## **2. Transformers**

Extra high voltage and very large generation step up (GSU) transformers are manufactured mostly by foreign companies. Utilities often keep spare transformers at the substation site (FERC Form I data tells which substations have spares and whether a substation is attended), so a saboteur could destroy the spare at the same time as the operating transformers. The wide variety of transformer characteristics complicates the problem of locating spares.

The replacement of high voltage power transformers is a concern because of (1) the long time to manufacture replacements, i.e., 6 to 12 months, if the utility is willing to sacrifice efficiency and shorten the life expectancy. This is a matter of concern to many in the utility industry and there have been requests to Gov. Tom Ridge, the Director of the Office of Homeland Defense to follow up on a previously recommended initiative to have the government stockpile national spares in key locations. Homeland Defense of the energy infrastructure will be an expanding area of government-industry action.

## **3. Generating Facilities**

The protective measures at generation facilities along with current security upgradesCincreases in the guard, improvements in perimeter protection, such as chain link fences, additional CCTV camerasCgenerally will provide a minimal level of security. Priority generating facilities should receive more thorough security upgrades, particularly for their more vulnerable areas. For example, the switchyards adjacent to the power plants are probably the most vulnerable target for a generating station because, unlike the generating equipment, they are not protected within a building, and do not have guards and operating personnel available on a 24X7 basis. The switchyard contains the generation step up transformers, switchgear, and the connection to transmission lines that carry the power away from the plantCall vulnerable targets.

**4. Operating Centers.** Most electric control centers are not hardened, but do have backup sites that can pick up control if the primary site cannot function. Electric control centers are usually located in a facility that has layers of security –guards, access devices, CCTV surveillance cameras, etc., to prevent unauthorized access. The most serious

threat to control centers is through a cyber attack, specifically against the SCADA and telephone control systems, but IT is outside the scope of this panel.