CLEVELAND ELECTRIC LABORATORIES

How Manhole Sensors Protect our Critical Infrastructure

By Cleveland Electric Laboratories - September 20, 2017

Unmonitored manhole/vault covers pose significant vulnerability access points to sensitive governmental areas & critical infrastructure locations for physical attack, frequently missed in perimeter protection strategies, as evidenced for example, by the Metcalf attack (Image courtesy of Cleveland Electric Labs)

When dignitaries or high-profile individuals visit cities, municipal crews often weld manholes shut in vulnerable locations to ensure safety, costing tens or even hundreds of thousands of dollars each time they must be welded and then cut open again.

Manhole covers and similar access points related to sensitive areas as well as critical infrastructure locations have proven to be a source of significant vulnerability, and many malicious acts such as vandalism, material theft, and even terrorism have occurred due to ease of access through manholes that generally are unprotected.

Utility companies, telecom providers, and municipalities are increasingly installing cabling and other components of their physical infrastructures underground.

Power is carried over metal cables, but most data and telecommunications infrastructures utilize fiber optics, and these vital links commonly pass through underground vaults.

The data and telecom traffic carried on these lines is sensitive at a minimum, and the access points to such lines need to be secured to help maintain both the integrity of this vital infrastructure and the security of the information carried by it.

Although the jacket of a fiber optic cable may appear virtually identical to a cable containing copper wires, a thief in a hurry may not distinguish between the two; and as the Metcalf substation attack illustrates, metal theft may not be the only motivation for lifting a utility vault cover.

At the lower end of the threat continuum, thieves frequently enter manholes to cut power cables in order to steal metals to be sold for scrap.

Utility companies, telecom providers, and municipalities are increasingly installing cabling and other components of their physical infrastructures underground. (Image courtesy of Hitachi)

For these efforts, they may gain a few hundred dollars from a scrap yard, while causing thousands of dollars' worth of damage and the loss of critical public safety services, power, and telecommunications to nearby industry, the surrounding community and its citizens.

Soft targets

At the higher end of the threat continuum, literally hundreds of thousands (if not millions) of manholes around our nation give easy access for a physical attack against vital components of our infrastructure, and the Metcalf attack demonstrates this easy access.

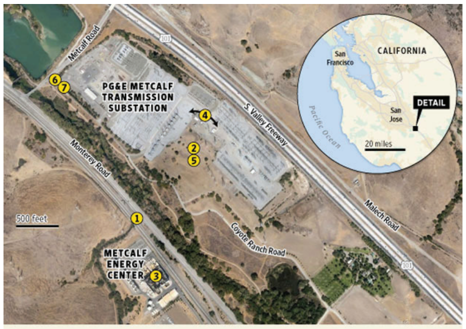
In addition to access points for vital components of our national infrastructure, manholes in and around city centers, stadiums, coliseums, hospitals, campuses, government agencies or similar public venues where large numbers of people gather at one time may also be points of vulnerability.

The Need

A safe and durable means of continuously monitoring the position of manhole or vault covers, in order to detect when they are opened and closed, is needed to help protect our vital communications and power infrastructures installed in manholes and underground vaults.

Monitoring of manholes near public venues where many people gather also would be beneficial to immediately alert authorities of any unauthorized entry; such monitoring would help maintain perimeter security and improve public safety.

The Vulnerability, an Example – The Metcalf Attack



Shots in the Dark

(Image Credit: WSJ)

On 16 April 2013, just before 1AM, intruders lifted the heavy cover of a telecom underground utility vault near the Metcalf power substation just south of San Jose, CA.

They cut fiber optic telecom cables in the vault, disrupting communications in the area; a few minutes later, they entered a second vault nearby and severed more telecom cables.

Then, starting around 1:30, they focused rifle fire on high voltage transformers inside the substation fence.

The shooting lasted nearly twenty minutes, and then the saboteurs vanished into the night.

Law enforcement officers arrived only a moment later, saw nothing suspicious, could not get past the locked fence, and left.

The attack caused leakage of 52,000 gallons of cooling oil and disabled 17 transformers; a blackout in portions of Silicon Valley was narrowly averted through power re-routing and conservation.

Jon Wellinghoff, then chairman of the Federal Energy Regulatory Commission, visited the site afterward and brought along military experts.

They concluded that it was a planned professional job, and Mr. Wellinghoff stated the attack was "the most significant incident of domestic terrorism involving the grid that has ever occurred" in the US.

The Department of Homeland Security defines terrorism as any activity involving an act that is "dangerous to human life or potentially disruptive of critical infrastructure or key resources."

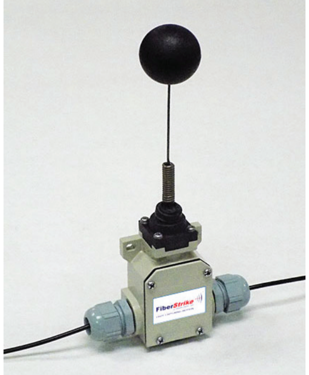
By this definition, the Metcalf attack was a double act of terrorism.

Such classification may or may not deter would-be thieves or saboteurs depending on their determination, knowledge and speed, but the development of systems to continuously monitor access points and help protect the security of vital infrastructures located underground has not kept pace with the expansion of such infrastructures themselves.

If a well-coordinated attack on these systems were to occur again today, how quickly would we know the location?

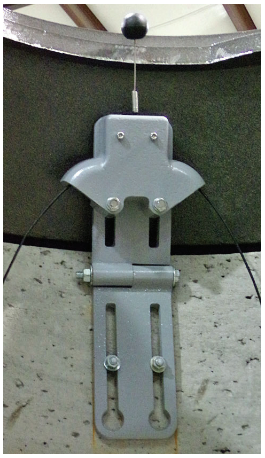
What if we could identify, in less than five seconds after it occurred, exactly which manhole cover was disturbed? Given this capability, might the Metcalf event have turned out differently?

Desirable attributes of a suitable manhole/vault cover intrusion detection system include the following:



LCM-610 sensor

- Reliably, continuously and simultaneously monitoring of the position of multiple manhole covers
- Individual and unique identifiers for every manhole or vault in which the system is installed
- Immediately report a change in the position of any manhole or vault cover
- Sensors that are environmentally rugged and resistant to corrosion
- Sensors that are intrinsically safe for use in explosive atmospheres
- Sensors located in each manhole/vault that do not require electrical power
- Sensors and interconnecting lines that emit no signals and are immune to electrical interference
- Sensors that cannot be bypassed without detection
- Sensors that may be deployed kilometers distant from remote monitoring equipment, if required



The CEL Solution

LCM-6100 systems are part of the FiberStrike suite of fiber optic sensing systems made by Cleveland Electric Laboratories (CEL), in Tempe, AZ, which have been deployed both domestically and internationally.

An effective solution exists in LCM-6100 manhole cover position sensing systems, which are specifically designed to help protect the security of underground utility infrastructures by monitoring the position of covers at the manhole or vault access points.

FiberStrike sensing systems use light (not electricity) to sense position or movement, and system attributes address all of the criteria listed above.

An LCM-6100 system for monitoring manhole or vault covers consists of LCM-610 sensors, LCM-2600 monitoring equipment at a remote location, optical fiber that links the sensors with the monitoring equipment, processing software, and a graphic user interface that is intuitive and easily used without requiring extensive training.

Protective mounting hardware also is available that adjusts to virtually any manhole wall configuration.

Value

"The ROI for a FiberStrike system may be estimated by comparing how many times a city has to go through the aforementioned process of welding manholes closed and reopening them (at top), or estimates of how much will be lost in the event of thefts, vandalism or terrorism, against the system installation cost," explained a representative of Cleveland Electric Labs.

"Up to fifty LCM-610 sensors may be multiplexed on one fiber, making efficient use of available fiber and further reducing installation costs."

Switch Properties

IP Rating	IP66
Housing Materials	Zamak with thermoplastic head, polyamide strain relief
Mechanical Life	1,000,000 cycles
Switching Principal	FBG strain state change
Max. Frequency of Operation	2Hz
Mounting Type	Two 5mm holes on 41mm centers

Optical Properties

Sensitivity	1nm between open and close states
Accuracy	N/A
Temperature range	-40°C to +80°C
Connection type	Armored fiber pigtail
Reflectivity	>70%
Wavelength range	Standard: 1512 to 1588nm in 4nm intervals; extended range of 1460 to 1620nm is available

FiberStrike® fiber optic interlock switches are the most advanced solution for monitoring the status of virtually any access portal (manholes, hand holes, doorways, vaults and power grids) today.

"Type SMF-28 fiber is commonly used in telecom systems, and if dark (unused) fiber of this type already passes through manhole/vault spaces to be protected and testing confirms it is suitable, installation costs may be reduced by using such fiber to link cover position sensors and the LCM-2600 remote monitoring equipment."

"The FiberStrike system continuously monitors the position of manhole or vault covers and immediately reports a change at any cover; the LCM-2600 equipment can simultaneously monitor hundreds of cover sensors if desired, with every cover individually and uniquely identified."

"Alerts also can be transmitted to multiple authorized recipients via voicemail or text."

"Individual identification allows exact location of any attempt to access a manhole or underground vault through a cover on which a sensor has been installed, and facilitates an immediate focused response by security or law enforcement personnel if appropriate," concluded Cleveland Electric Labs.

CONTACT

Corporate Headquarters
EAST COAST: Ohio Location
800.447.2201

Advanced Technology Group
WEST COAST: Arizona Location
866.914.3727

EMAIL: sales@cel-atg.com
WEBSITE: www.cel-atg.com