TELECOM SITES PHYSICAL SECURITY

How Telecom Network Operators and Tower Companies Can Improve Physical Security at Base Stations and Protect their Networks
## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>03</td>
</tr>
<tr>
<td>Understanding Cell Tower Physical Security Threats</td>
<td>04</td>
</tr>
<tr>
<td>Mobile Network Operators Across the Globe Taking Action to Deal with Theft and Vandalism</td>
<td>08</td>
</tr>
<tr>
<td>Telecom Site Automation - A New Opportunity to Manage Physical Threats</td>
<td>09</td>
</tr>
<tr>
<td>Conclusion</td>
<td>13</td>
</tr>
</tbody>
</table>
Introduction

This report provides details of the role of physical security in maintaining telecom networks' reliability. For the purposes of this document, physical security relates to the situation of people directly harming a telecom site intending either theft or vandalism. Physical security is paramount for the telecommunications industry and one of the biggest challenges that telecom network operators have to face while managing their networks of base stations. This document discusses the main physical factors that may lead to network outages and some innovative approaches to prevent telecom base stations breakdown due to physical security.

“It is imperative for telecom operators to integrate specific solutions to ensure all physical threats can be detected and corrected...”

Communication infrastructure is the backbone of modern societies and economies, and are a critical component of national security and emergency preparedness. Without uninterrupted communication, modern economies can’t function. Emergency services, finance, and even many traditional industries depend heavily on telecommunications networks. Physical security is a major challenge that telecom network operators and tower companies face while managing their network of telecom sites. Cellular base stations and other unmanned locations are vulnerable critical infrastructure components that require constant physical security monitoring.

It is imperative for telecom operators to integrate specific solutions to ensure all physical threats can be detected and corrected before they affect customer service. This report takes a closer look at the physical threats that telecom network operators and tower companies have to deal with in different countries around the world and explores some solutions that may be taken in order to pro-actively detect physical threats and reduce their impact. Telecom site automation is an effective solution, with significant short-term and long-term advantages for telecom site operators.
Part 1

Understanding Cell Tower Physical Security Threats

Theft and vandalism are common physical threats that telecom network operators have to prepare for when managing their cell base stations. Less common, but still a concern are more coordinated efforts to damage the ability of the telecom network to operate by damaging the sites themselves.

Theft and Vandalism

As cell towers are often located in remote locations, cellular base stations are prime marks for thieves and vandals in search of an easy target. These sites contain a wealth of valuable copper wire, high-performance batteries, and diesel fuel. Thieves and vandals take advantage of remote locations of cell sites by trespassing freely, without the fear of being identified. Copper wires and battery theft exploit the second-hand market fuelled by the worldwide demand for these goods. The most common reasons for people to deliberately harm a telecom site:

Cable Theft

The cable is stolen from various telecom sites as well as telephone poles, work centers, construction sites, and open cable pits. Cables are cut into short lengths (2 ft. to 6 ft.), and prepared for resale. As scrap metal dealers prefer raw copper and pay cable thieves more for raw copper, thieves coil or cut cables into sections and remove sheathing and outer skin. Raw copper is easier for dealers to resell and to conceal. The process by which thieves strip sheathing is also an environmental hazard, leaving localized contamination of ground and water sources.

Copper theft represents a special case due to the wide use that copper has. Copper’s value transforms remote cellular base stations into prime targets for thieves. The costs for telecom and tower operators to replace the cost of the cable and damage to the site can be thousands of dollars per incident. This is not taking into consideration the additional costs of loss of network service. Even the theft of a small amount of copper can cause extensive damage to site equipment, costing cell towers owners thousands of dollars in repairs, replacement, and network downtime.
Cable Theft (Continued)

There are several expensive copper items at cell sites that are very attractive to thieves, such as the ground wires, copper grounding busbars, and waveguides. A copper grounding busbar can cost telecom operators and tower companies upwards of $500 apiece and is usually resold on the black market for $10-80. Waveguide from microwave towers is attractive to thieves as it is typically a higher quality of copper, is run in long lengths to the top of towers, and the amount of copper is higher than in other types of cable in similar lengths.

In the United States, according to the ForeCASTsm report that analyzes copper, aluminum, brass and bronze theft claims identified in Insurance Service Office (ISO) ClaimSearch, there were a total of 27,514 claims for the theft of copper, aluminum, brass, and bronze submitted between January 1, 2014 and March 31, 2018 of which 98% pertained to the theft of copper.
**Cell Site Batteries**

While not as widespread a problem as copper theft, battery theft can easily become the root cause of cell services outage. Similarly to the case of cable theft, telecom towers are increasingly affected by the rise of battery theft and vandalism. According to NorthStar Battery, 10% of battery failings in the tower industry is caused by theft and vandalism.

![Why are telecom batteries failing so early?](image)

**Diesel Theft**

Diesel fuel is a major asset at telecom sites that can easily and directly be sold by thieves. The threat of diesel theft is widespread in many emerging markets and even in the rural areas of the developed markets. Diesel fuel often gets stolen at multiple points in the supply chain. Diesel theft has been estimated as high as 30% by tower companies around the globe. For instance, between 20% and 35% of the fuel intended for powering a tower site in Africa is estimated to be stolen. The mitigation of physical security risks is a business necessity especially for those telecom network operators whose fuel costs amount to 25% of their total network operations costs.

In emerging markets, administrative diesel theft - staff or contractors in charge of provisioning the cell sites with diesel - can account for up to 50% of total stolen diesel. Here are two of the most common practices of administrative fraud:

- The diesel theft happens at the gas station when trucks are not filled up correctly.
- When fuel tanks are filled up on the site, some part of the diesel fuel is replaced with some other liquid in order to meet the billed quantity. If the fuel is contaminated with water, for instance, generator damage will be the consequence.
Challenges even well-prepared telecom networks operators are facing while trying to ensure the physical security of their cell sites against theft

Physical security threats at cell sites are widespread, affecting cell sites network operators all over the world. In the past mobile network and other telecom operators implemented solutions known as remote site management, remote monitoring systems (RMS), or simply "site alarming". Years ago there was a general class of products referred to as remote terminal units (RTU’s). The attempts to protect cell towers often relied on basic motion or door sensors. Motion sensors could create a perimeter around the cell base station and an alarm would be generated to the network operation center whenever something would enter the marked off area or a door were opened.

False alarming that requests unnecessary cell site visits drive operational costs increase

In many situations, as cell sites are located in remote locations, alarms are triggered by animals or other “false positives”. Telecom network operators have to dispatch tower technicians to the remotely located site following disturbances, wasting money on unnecessary site visits. Worse, if enough false positives are detected, then eventually alarms might be ignored causing theft to go unnoticed until a site failed.
Part 2

**Mobile Network Operators Across the Globe**

**Taking Action to Deal with Theft and Vandalism**

---

**Africa - Telkom South Africa**

Copper cable theft has been a major problem for telecom operator, Telkom South Africa over the years. Back in 2016, the company admitted it had lost over R200 million ($13.8 million) due to copper cable theft during the 2015 financial year. About half of that was due to direct cable theft repair costs and the other half was spent on the cost of security services. In 2018, cable theft was still affecting South African residents and business owners, interrupting Telkom’s customers’ services. In 2019, Telkom decided to proactively move customers from legacy copper which was installed since 1974 to new fiber technology and investigate ways to remove copper from their systems. Telkom is managing the pressure of the investment cost of deploying the fiber network, with the reduction in cable theft and reduced maintenance costs, improved social impact, better customer experience, and a stronger long-term positioning of the group.

**Africa - The Botswana Telecommunications Corporation (BTC)**

BTC experiences copper cable theft both underground and overhead resulting in telecommunications service disruptions and loss of hundreds of thousands of $USD both in replacement costs and revenue lost during service interruptions. In 2018, the organization started technical partnerships and prioritized the network modernization and optimization deployment.

**Latin America - Claro Brasil**

One of the major mobile operators in Latin America offering voice and data service suffers from vandalism and theft, which is a big issue for the company. They have a specific department that deals with security issues and are using modern access control and surveillance systems that guarantee theft reduction and allow them to efficiently control and monitor their assets.

**Asia - edotco Group**

In 2015 the leading telecommunications infrastructure services company in Asia, edotco Group was facing diesel theft in their 15,000 tower network. They now use innovative technologies to monitor diesel readings which allows them to have a thorough view of the diesel consumption without being onsite and also detect and prevent theft. Over the last few years, edotco Group managed to achieve a 30% reduction of theft and vandalism through the usage of smart padlocks. These are examples of savings possible through their own homegrown efforts into telecom site automation.
Part 3

Telecom Site Automation - A New Opportunity to Manage Physical Threats

Telecom site automation delivers the necessary real-time management to increase the security of mobile network operator’s cell site networks. In case of physical threats like theft and vandalism, telecom site automation allows mobile network operators and tower companies to proactively act and mitigate the damage caused by the event and prioritize post-event response efforts. Here are some telecom site automation features that can help avoid, minimize consequences and deal with physical threats:

Access Control

Access control gives mobile network operators and towercos the opportunity to see exactly who is accessing a base station and for how long. Telecom site automation systems allow for centralized software to give rights to individuals to enter remote sites, reducing the administration of physical keys. Administrative theft is a real and widespread problem especially when multiple contractors are involved, and often require either leaving doors open or passing keys to unapproved persons. A modern telecom site automation door access control system will control who can enter and leave an audit trail of visits. If theft occurs, it can be correlated to particular service visits. Many non-telecom specific access control management systems expect you to have one or a few sites each with many doors. In a cell site network, you have 100s or 1000s of sites each with a small number of doors. Access control for cell sites requires unique control features not offered by normal access control systems.
Cell site remote security with video surveillance integration

Shelter security monitoring requires more than just a door sensor. Telecom site automation capabilities go beyond the typical door, motion, vibration detection and other simple on/off type of alerts that can be triggered erroneously giving “false positives”. Integrated with IP security cameras, these telecom site automation solutions collect images from motion events and then send alerts and email thumbnails back to the network operations center. A number of features relate specifically to managing large numbers of telecom sites. Modern telecom site automation solutions can work with most modern IP based cameras, allowing for a very wide choice in the functions and costs of the cameras used. A typical telecom site automation solution utilizing any standard IP camera would use the following basic escalation process.

1. IP Camera detects motion - The camera would detect motion, take still pictures, and these still pictures would be collected by the telecom site automation site appliance.

2. Site Appliance sends SNMP or other messaging upon receiving images from the camera - Many telecom operators are already using SNMP based software in their network operation center (NOC), and operational processes are built around alarms coming to these systems. The small size of an SNMP trap has the advantage of also causing very little IP usage across a telecom sites method of backhaul.

3. If the NOC thinks the IP camera’s triggering of a still picture is suspicious, they can access the site appliance and view the still pictures that are stored in the site device.

4. If there is still concern after viewing the still photos, NOC technicians can click directly through the site appliance’s web interface to directly stream live video from the IP camera.
Below is an example of the Asentria SiteBoss 550 site appliance being used as described above. The leftmost picture shows the SiteBoss 550 device’s own web UI. The UI shows many variables being watched at a solar hybrid site. The upper right picture shows what thumbnail images look like when an Asentria engineer triggered the IP camera’s motion detector. The images were sent to the SiteBoss 550 from the site camera. The picture at lower right shows the interface of the camera itself, which can be accessed by clicking the link within the SiteBoss units web interface (arrow).

Site Appliance - IP Camera Integration

(Click Here to View Larger Version)
Generator and Fuel Level Monitoring

Telecom site automation allows network operators to quickly address outages and other issues caused by extreme weather through real-time cell-site health monitoring, centralized generator exercising prior to events, and prioritized generator refueling during and after weather events.

Another primary use of diesel fuel values is as part of a larger diesel theft prevention action. The site appliance can be integrated directly to a generator, and will have many of the operational values of that generator. A site appliance might gather diesel fuel levels in multiple different ways depending on need. Integrations are possible to a wide range of fuel level and adulteration sensor types. The site appliance will know fuel level, amount of fuel added, drops in fuel due to normal generator usage, fuel adulteration issues, refuel points, generator run hours, etc. from the generator itself, as well as various sensors. These variables can be used by themselves, or can be correlated to other systems. A simple example is an alarm related to drops in fuel level that are not associated with running the generator, or decreases that are too rapid to be caused by only running the generator. Another example would be the use of the site appliance sensing diesel being re-fueled and comparing the amount of fuel directly being added to the tank vs. what the re-fueling company is billing for.
Conclusion

Cellular base stations are critical infrastructure components that require constant physical security monitoring. Telecom site automation is a cost-effective solution that provides mobile network operators and tower companies with improved resilience and efficiency of their telecom sites. Telecom site automation provides solutions to improve management of power, security, and environment at remote sites. Improved physical site security is only one of several major benefits that telecom site automation can provide.

Asentria provides solutions for mobile network and tower operators to manage security issues at remote cell sites from their network operations center. Telecom sites are evolving to include many new intelligent subsystem controllers for DC rectifiers, generators, cameras, access controllers, and HVAC. Asentria securely integrates these sub-systems into our hardware-based site controller to present a single interface for the management of security at remote sites. Beyond simple alarming, Asentria generates data for comparative site analysis and provides remote access to the underlying systems for OPEX reducing cell site optimization.
Resources

- https://herecast.us/861034
- https://www.law.cornell.edu/cfr/text/47/4.9
- https://ladysmithgazette.co.za/122751/theft-telkom-cables-leaves-residents-without-internet-telephone-lines/
Locations

Headquarters
1200 N 96 St
Seattle, WA 98103
USA

EMEA Office
20A Copilului Street, Hala 2
012178 Bucharest
Romania

Sales & Support

Americas - Asia Pacific

Customer Service: +1-206-344-8800
Sales: +1-206-344-8800; sales@asentria.com
Tech Support: +1-206-344-8800; support@asentria.com

Europe Middle East - Africa

Sales & Tech Support:
+40 37-499-1111
emeasales@asentria.com

Follow Us

©2019 Asentria Corporation. All Rights Reserved.