How to protect your sites from theft of fuel and equipment

azeti Networks report on their roundtable at the TowerXchange Meetup

As the demand for mobile services increases steadily around the world, the telecom industry is facing certain challenges regarding the power supply of towers. Running a BTS in densely populated areas with full access to a power grid is in most cases unproblematic, but the whole story changes in remote places, where power supply is unsteady (unreliable grid) or is not given at all (non-grid).

The installation of around 75,000 new towers around the world every year that are off-grid, shows clearly the rising importance of this topic. In some African countries, up to 80% of the tower sites have no access to the power grid. Those sites have to be powered by other sources; in most of the cases diesel generators and batteries. But the operating cost compared to grid power is tremendous. While supplying a tower with commercial grid power costs about US$150 per month, these costs can easily rise to US$1,200-2,200 per month if the power supply solely depends on diesel, with an average price per gallon of US$4.50. This leads to soaring OPEX costs; up to 60% of OPEX is due to fuel expenditures for non-grid installations. Besides higher costs for running non-grid tower sites, another factor complicates the situation further: fuel theft.

Between 20% and 35% of the fuel intended for powering the tower site in Africa is stolen. However the theft does not take place at only one specific point; it differs by location, time and person. We distinguish between two forms: administrative theft and on-site theft.

During the TowerXchange Meetup at the beginning of October in South Africa, azeti Networks had a unique chance to discuss best practices in fuel security with market experts from the African tower business. Among the participants were professionals from RMS and Managed Service companies, towercos, as well as representatives from companies specialised in fuel delivery, site security and power supply.

Read this article to learn:
- A comparison of energy costs on-grid versus off-grid
- What percentage of fuel intended for African cell sites is stolen
- Options to combat administrative theft, including watering down of diesel
- Options to combat on-site theft by staff and by third parties
- Tools at tower operators' disposal including RMS, CCTV, access control systems with RFID or biometric, upgraded or dual perimeter fencing, security patrols and improved relations with local communities

As the demand for mobile services increases steadily around the world, the telecom industry is facing certain challenges regarding the power supply of towers. Running a BTS in densely populated areas with full access to a power grid is in most cases unproblematic, but the whole story changes in remote places, where power supply is unsteady (unreliable grid) or is not given at all (non-grid).

The installation of around 75,000 new towers around the world every year that are off-grid, shows clearly the rising importance of this topic. In some African countries, up to 80% of the tower sites have no access to the power grid. Those sites have to be powered by other sources; in most of the cases diesel generators and batteries. But the operating cost compared to grid power is tremendous. While supplying a tower with commercial grid power costs about US$150 per month, these costs can easily rise to US$1,200-2,200 per month if the power supply solely depends on diesel, with an average price per gallon of US$4.50. This leads to soaring OPEX costs; up to 60% of OPEX is due to fuel expenditures for non-grid installations. Besides higher costs for running non-grid tower sites, another factor complicates the situation further: fuel theft.

Between 20% and 35% of the fuel intended for powering the tower site in Africa is stolen. However the theft does not take place at only one specific point; it differs by location, time and person. We distinguish between two forms: administrative theft and on-site theft.
Administrative theft

Administrative theft accounts for 50% of the total stolen fuel. In this case, staff charged with the provisioning of diesel for tower sites are involved in criminal activities. Theft can take place at different stages of the delivery process. The fraud can already happen at the gasoline station, when trucks are not filled up correctly. Or during the transport to the site, substantial quantities (100 litres or more) can get stolen. Another opportunity to defraud is given when fuel tanks are filled up on the site. A common practice for concealing the short delivery is to replace part of the diesel by some other liquid in order to meet the billed quantity. If the fuel is contaminated with water, generator damage will be the consequence, which can easily cause costs of up to US$1,500.

One solution to tackle those issues is to outsource the delivery process to a fuel supplier together with the installation of a RMS (Remote Management Solution) based fuel management solution at the site, which gives detailed information about fuel level and purity. Another option besides the deployment of a RMS at the site would be to put one on the truck in order to maintain visibility throughout the transportation process and track down exactly where and when the fraud happens.

On-site theft

It is not only the delivery of fuel that offers a number of risks of thievery. The remote location of certain towers facilitates theft either carried out by insiders (staff) or other third parties with no work-related reason for accessing the site. The focus of criminal activities extends beyond fuel to include other site equipment like batteries or even whole tanks. Since two different groups are involved, measures have to be more comprehensive in order to secure on-site assets.

For work-related theft, a solution to counter those incidents can be the deployment of electronic key access mechanisms including person and role based access control. By using pin pads, electronic keys or other devices with RFID or biometric features, the security level of the site can be increased substantially. An even more efficient solution would be the installation of surveillance cameras with access control as well as motion control. In addition, fuel level and also fuel contamination monitoring including energy management capabilities like generator status checks will provide a comprehensive set of measures to keep tower sites up and running.

But in some cases, thieves do not worry about concealing their theft of equipment and fuel. They exploit the remote location of tower sites and the fact that they do not have to expect resistance. In those instances, only massive security provisions can help to protect assets. The main challenge is to impede or prevent external persons from accessing the tank by means of high fences, secure containers or underground installations. A dual fence concept could pay off, including a semi-secure fence for alerting and a hardened inside area, which keeps thieves out of the shelter until security patrols have reached the position.

Maintaining a relationship with the local community could also help to prevent site downtime by integrating locals into tower secure measures and explaining how they benefit personally (network coverage, phoning).

As mentioned before, batteries are also considered to be a target for theft, each worth of about US$5,000-20,000 per site. In order to reduce incentives for stealing batteries, one way could be not to source batteries inside the country. This means you’re not supporting the creation of a local market for stolen batteries. Underground installations or even concrete shelters would help to discourage external persons from entering the sites violently, as would the deployment of a RMS with energy management features including DC control combined with access control.

Conclusion

The theft of diesel or tower equipment is a widespread problem that needs to be addressed with appropriate measures. Specific threats require adjusted solution approaches. The deployment of a RMS with fuel management features would help to decrease administrative fuel theft. If this solution is extended by a role and person based access control system, theft committed by insiders could be lowered. Keeping external parties out of the tower site proves to be more difficult, since they have the advantage of the remote tower location. Therefore, only a combined solution that comprises underground installations or concrete shelters and camera-secured fences will be an effective protection.

Thanks to Thorsten Schaefer, CEO of azeti Networks AG for preparing this report