SECURING TELECOM INFRASTRUCTURE

Critical Security Points in Telecommunication Infrastructure

Vanma

BBI Int., a.s. official Vanma solution distributor in Europe
Address: Röntgenova 28, 851 01 Bratislava, Slovakia

Email: sales@smartkeysystem.eu
VAT ID: SK2023070357

The continuing existence of various natural disasters underscores the importance of the nation's telecommunications infrastructure and our country's reliance on these facilities. According to Chinese National Security Alarm System Standardization Technical Committee (CSBTS/TC100), there are more than 10 critical infrastructure sectors that are critical to our country, in other words, if they are not strictly protected, they may have a very bad impact on our country's security. Telecommunications is one of the key departments of the Department of Homeland Security. In emergencies, reliable and rapid communication services can help people get in touch in a timely manner, so that correct decisions can be made to reduce the loss of life and property caused by emergencies.

Telcos face many latent security challenges. The distribution of the telecommunication network is complex, it is very far from the urban area, there are many remote and isolated infrastructure sites, the terrain is a bit hard to do the work, and there are not many on-site personnel. For managing this huge network of resources, it is often difficult for managers to effectively manage staff to complete work on time and efficiently, but how and when they exercise their entitlements is vital to maintaining safe operations.

Unique Problems of Telecom and the Failings of Mechanical Security

When managing unattended, siloed sites, headaches often include vandalism and theft. These infrastructures contain expensive copper wiring, imported components and other valuable resources that are prime targets for thieves. While fences, locks, and sirens provide an essential layer of security, the easiest way for thieves to gain access to these resources is through brute force, uncontrolled key duplication, and negligence by staff. Once such a theft occurs, it will not only affect the security of this site, but also seriously affect the entire communication market, bringing latent hazards to human security.

Ease of theft is just one of the hazards. Managers must also monitor every site that has been set up and installed by R&D and technical staff. One of the difficulties is the inability to control the range of movement of workers, and the lack of visualization causes managers to worry. Mechanical locks and keys are often the first line of defense in securing telecommunications infrastructure. With a seemingly limitless variety, easy installation, and attractive prices, mechanical locks and keys provide entry-level security solutions. While very effective for basic needs, mechanical locks and keys can pose serious risks or facilities that require more sophisticated security systems.

Audit Importance and Electronic Options

Notably, mechanical locks and key systems lack auditing capacity. In other words, the ability to track who was where, and when. Furthermore, the risks associated with lost, stolen, or copied keys are innumerable. With no way to effectively trace when a key is copied, facilities can easily lose control of the number of keys in circulation. Another troubling problem that telecommunication operators must confront is the variability in the type of locks used to secure gates, doors, and equipment rooms. Each type of lock has a different manufacturer, and key control challenges can multiply. In addition to basic key control issues, mechanical locks and keys are vulnerable to prying and key slot damage, rendering the lock inoperable. They also cannot realize remote management to monitor the current site situation in real time which is dangerous for telecom security.

Electronic security systems, such as numeric pin pads, RFID card readers, and biometric devices, are commonly used in facilities requiring electronic tracking and precise, scheduled control over who is granted access. Although most electronic security systems offer enhanced security compared to mechanical solutions, electronic security systems require hard-wired power and network connections, which are often unavailable or impractical in remote locations. CCTV and digital video security systems are another popular line of defense against vandalism, theft, and other security threats at telecommunication sites. Although cameras may present a deterrent for some thieves and vandals, they ultimately supply no physical protection to safeguard equipment and other valuable assets. Additionally, bandwidth limitations and data storage requirements may be unsuitable for the scattered nature of telecommunication infrastructure sites.

Key Centric Access Control

Vanma came into being in this communication environment with the advantages of existing locks combined with the latest exclusive technology developed by senior developers. Although less familiar than mechanical locks and keys, and perhaps even electronic security systems, key-centric access control systems combine the precision of electronic systems with the simple installation, affordability, and ease of use of a mechanical system. Although less familiar than mechanical locks and keys, and perhaps even electronic security systems, key-centric access control systems combine the precision of electronic systems with the simple installation, affordability, and ease of use of a mechanical system. Vanma access control systems bring full-featured access control to every locking point without installing hardwired network or power connections. Electronic cylinders are easily deployed, not only on doors, but also on gates, trucks, shipping containers, and other mobile and remote assets. The batteries in the Vanma Key smart keys energize the Vanma cylinders, meaning organizations don't need to manage expensive battery replacement schedules. Keys are programmed with access permissions for each individual user. If a key is lost, it can easily be deactivated in the system, and the exclusive fingerprint program on the key can help lock control management to protect the communication infrastructure.

Conclusion

Telecommunications infrastructure is vital to the safety and security of people worldwide Mechanical locks and keys and hardwired electronic access control systems have serious limitations. And cameras do not provide the necessary physical security barriers for security systems. Based on audit capabilities and precise key control, Vanma electronic locks and Vanma smart keys are an excellent security solution for telecommunications infrastructure that people can trust.