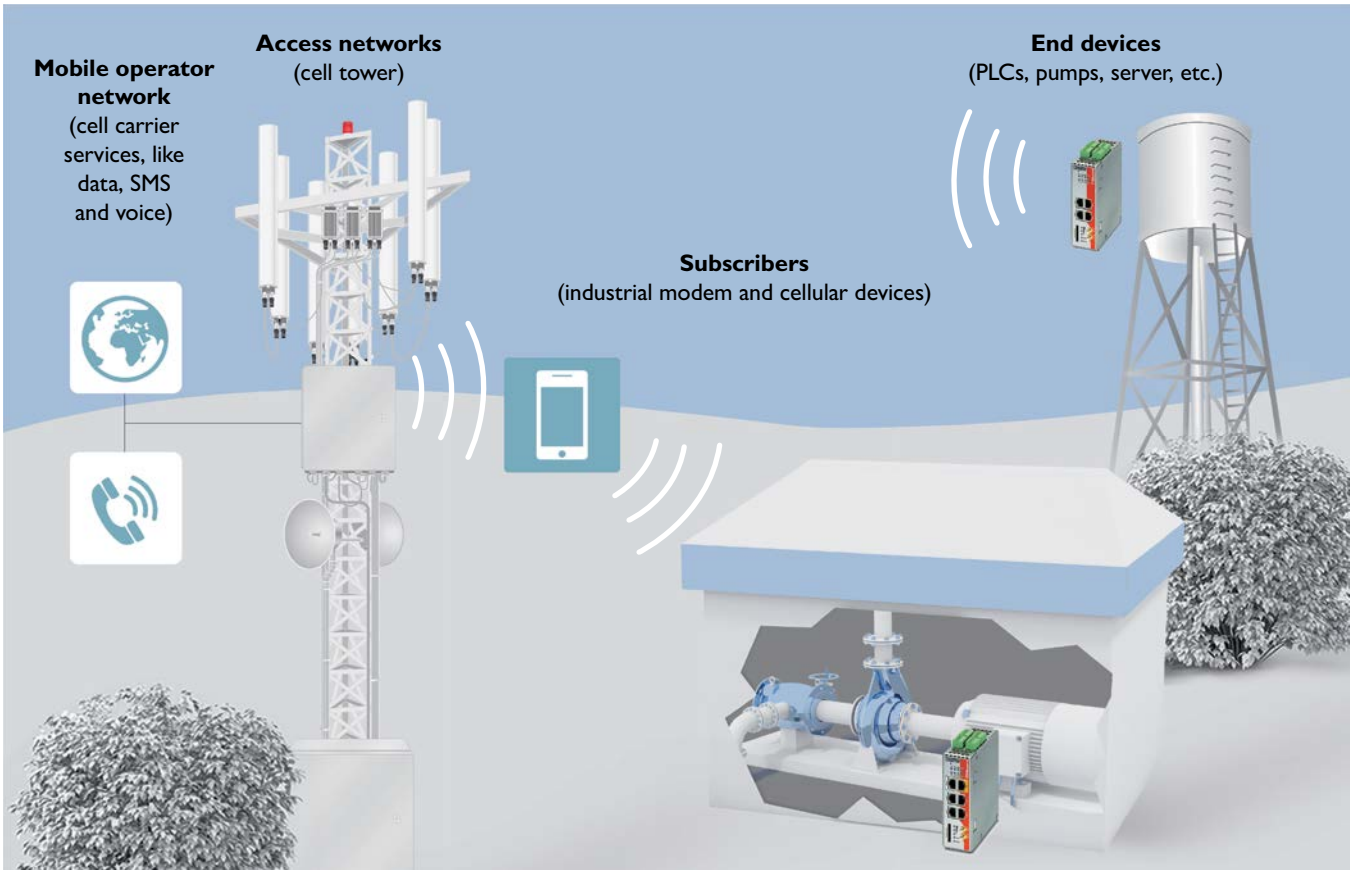

Figure 1: Simplified architecture of a cellular network.

Best practices to secure cellular modems in any industrial application

By Mariam Coladonato, Lead Product Marketing Specialist, Networking and Security, Phoenix Contact USA

INSIDE:

Introduction

Mobile communication follows the same general principle as telephones, wherein the goal is to connect two or more remote users. This is accomplished through the network equipment of an operator, such as AT&T or Verizon, who are responsible for managing the service. However, unlike fixed telephones, there are no copper or optical fiber pairs in the mobile network. Radio transmissions are the final link. The user's mobile phone or modem communicates through the air with an antenna. This antenna, in turn, communicates with the operator's central office, which then routes the communication to the corresponding part of the fixed network or through other antennas.

Cellular mobile technology is a public telecommunications service. Its main objective is to facilitate communication without imposing restrictions based on geographic location and displacement. Smartphones and tablets are a prime example of common mobile usage; however, industrial cellular modems have proven to be useful and cost-effective for Supervisory Control

U001147A.10.18

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-7388 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
E-mail: info@phoenixcon.com • Website: www.phoenixcontact.com

and Data Acquisition (SCADA) applications for remotely located assets. Industrial cellular modems can facilitate remote monitoring, support and control, M2M applications, data logging, and alarming.

With all of the critical SCADA applications connected through modems into the public network, it is important to understand that the convenience of remote monitoring also comes with great risks. Cellular modems are a powerful tool in an Industrial Internet of Things (IIoT) environment, but there is a risk of malicious and/or unwanted users stealing sensitive data or, worse, sabotaging, disrupting, or even halting operations.

A proper security analysis model in mobile networks is quite broad and complex to define, as the entire infrastructure is ambiguous and converges multiple technologies that can be confusing to the user. However, the following white paper will explain some measures you can take to prevent the possible risks.

Using private Access Point Names (APN)

An APN is the name of an access point that must be configured so that a device can connect to the Internet using the networks of cellular vendors. These vendors can also provide private APN plans, which consist of direct access to local area network (LAN) connections, which allows the user to specify a fixed number of network and security parameters. Some of these parameters may include address allocation, authentication through RADIUS servers, completely blocked Internet access, and more.

At this point, the industrial modem will be connected directly into a private APN network that already prevents any intrusions, such as spam or viruses. It also reduces the access of public IPs directly at the modem, as this is an open-door invitation for malicious users to attempt log in and increase usage fees. However, there is a downside of private APNs. Every device or individual needing to connect to the private APN must also pay the private APN fee and set up secure access, such as a virtual private network (VPN), for data access.

VPNs for remote access and monitoring

A VPN can be used when private APNs are not an option. A VPN's goal is to extend private networks across a public network such as the Internet without the extra service fees that the private APN might carry. The most common VPN technology is called IP Security (IPsec); this client-server application uses a tunnel connection that carries data encryption and allows secure communications between two or more networks anywhere in the world. The three-key security attributes of the tunnel are:

- the authentication of users or devices through certificates or pre-shared keys (PSK)
- encryption of the data being sent through the tunnel
- and the use of hashing algorithms that identify and drop manipulated or corrupted data

Figure 2: Secure remote connection.

Most industrial cellular modems support some type of VPN tunnel already, so it's the most feasible option for any industrial application that needs cellular connectivity. The downside is that the VPN setup could become a technical challenge for the user, as it requires some networking and infrastructure knowledge even before setting up the devices.

Blocking all unused ports

Blocking all additional, unused ports is a security best practice that every SCADA application owner should follow. If there are unused physical ports in the device itself, you must physically block them. This can be accomplished either by locking the control cabinet or using low-cost physical security items. Additionally, if the device itself has the functionality to disable the ports, then you can virtually disable them from the device management page. This

prevents any malicious person or unwanted devices from connecting directly.

Figure 3: Example of low-cost physical security for unmanaged switches.

It is also important to block all unused service or application ports that could open insecure paths to your industrial equipment. Being in an industrial cellular modem, these services could be completely open to the Internet. To block these ports, the user must program the security and firewall functionalities inside the specific device. Even industrial modems can support basic firewall functionality. These can be configured for traffic-filtering capabilities of incoming and outgoing data, as well as for restricting all unnecessary ports and protocols. SCADA applications normally have a small number of necessary ports that users would need to reach for day-to-day operations. If the asset owners are properly using a VPN tunnel into the industrial modem, then all applications are available through the secure VPN connection, and everything around the firewall and port forwarding functions should be blocked. For example, every industrial modem user should avoid having the following services open from the Internet: FTP, SSH, Telnet, SMTP, DNS, HTTP and HTTPS. These ports are the most commonly used for malicious attacks.

User authentication and modem management

Data encryption through the VPN and blocking all unwanted ports are great initial steps toward the overall security solution, but they won't protect against everything. If the user does not change the cellular modem default/admin password, then a malicious user could easily access the device itself and its "secure" configuration. With a default password, a malicious user would have full control over the cellular modem's functionality.

Also, it is a good practice to note that a password should be personal and nontransferable, and it must be guarded properly. Standard security practices recommend using a password that combines uppercase letters, lowercase letters, numbers, and special characters.

Additionally, the modem's configuration port should not be opened directly into the Internet. The access to the device itself could be done through the authenticated VPN tunnel or, if supported at the device level, using two-factor authentication. The mechanics are simple: when the user logs into the device configuration page, this tool asks them to authenticate ownership of the account, providing two different factors. The first of these is the admin password. The second can be several things, always depending on the function supported. In the most common case, it is usually a code that is sent to a mobile phone via SMS or an email account. The fundamental essence of this tool is that if you want to log in to one of your devices, you must "know something" and "own something."

Is failover necessary?

Depending on how remote the SCADA application is and what other network infrastructure is available, you can reduce the attack surface for a denial of service (DoS) through failover if the cellular modem supports it.

The objective of a DoS attack is to interrupt access to services and resources for an indefinite period of time, aimed at specific networks to make them completely inaccessible to legitimate users. For example, when the industrial cellular modem is saturated by a DoS attack, a user who wants to consult the specific modem will find it unavailable. A DoS attack would overload the device until it collapses. It can also take over the whole bandwidth, preventing the device from processing real requests. To achieve this, the attacker floods the system with information that obviously exceeds the processing capacity.

Industrial cellular modems with failover capabilities won't prevent the DoS attack from happening, but if it does, the device will drop the cellular communication vector. The failover on the secondary infrastructure is then used to maintain the availability of the industrial communications.

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-7388 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
E-mail: info@phoenixcon.com • Website: www.phoenixcontact.com

Monitor data usage

Proactive monitoring of device events is an often overlooked aspect of cellular modem security. Actions such as unauthorized access attempts, configuration changes, excessive port scans, and more can be recorded, and the user can be alerted about the suspicious activity through email or text message. Additionally, the devices can also forward those logs to a Syslog server or Simple Network Manager Protocol (SNMP) server, which could store and analyze security-related events.

Also, your cellular carrier could provide additional insight through your Subscriber Identity Module (SIM) state and usages through a portal, as all SIM cards are unique.

Enable security on end devices, if available

SCADA applications also have other industrial devices such as controllers, sensors, and even computers, which are vulnerable by nature. Hence a defense in depth strategy should be applied, default passwords should be changed before deployment, and physical security like perimeter fences or closed cabinets with tampering detection should be put in place. These measures are an added layer of security to the overall remote SCADA network.

Conclusion

Unlike many other available network infrastructures, the traditional cellular network exposes your devices directly to the public Internet, and all the risks that are incurred with that access. While this gives you efficient and high-speed access to remote sites, device-level security is not a concern for the cellular vendors. They might be protecting their network infrastructure but not considering end devices like smartphones or industrial cellular modems. If these modems are connected to critical applications such as power plants, city water pumps, etc., these systems can become targets for malicious attacks through the direct and easy access of the cellular network thanks to the user's cellular provider.

A layered approach is the best practice for SCADA security applications that use industrial cellular modems as means of communication. When purchasing or implementing cellular modems in your critical application, make sure your cellular modems support most of the following security mechanisms: VPNs, firewall, failover, logs, and alarming.

Phoenix Contact offering

The TC mGuard product family provides all the benefits and features of a security appliance with an intelligent firewall and IPsec VPN, while adding the ability to connect to cellular networks. It is ideal for tough environments, including Class I, Division 2, for hazardous locations and suitable for a wide temperature range (-40 to +60 degrees C). The devices also come with an integrated four-port switch. SMS support is one of this product's strongest features, allowing you to monitor certain digital alarms and obtain text messages based on input changes. It provides SMS functionality based on other alarms, such as loss of network connection via a wired interface (only TC 4000), VPN status, and other alarm notifications. The TC mGuard RS4000 focuses on the highest level of availability for the system. It allows for a physical wired connection with failsafe over to cellular networks in case of loss of connectivity.

For more information visit **www.phoenixcontact.com/mguard**

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-7388 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
E-mail: info@phoenixcon.com • Website: www.phoenixcontact.com

PHOENIX CONTACT
INSPIRING INNOVATIONS

ABOUT PHOENIX CONTACT

Phoenix Contact develops and manufactures industrial electrical and electronic technology products that power, protect, connect, and automate systems and equipment for a wide range of industries. Phoenix Contact GmbH & Co. KG, Blomberg, Germany, operates 50 international subsidiaries, including Phoenix Contact USA in Middletown, Pa.

For more information about Phoenix Contact or its products, visit **www.phoenixcontact.com,** call technical service at **800-322-3225,** or e-mail **info@phoenixcon.com.**