

How Secure Cellular Routers Promote Connectivity in a Scalable Power Network



Why Moxa

- IEC 62443-4-2 certified cybersecurity systems, such as firewalls, NATs, and VPNs, are effective against cyberattacks.
- MXsecurity network management software visualizes distributed data on a centralized, intuitive, and user-friendly interface. Real-time alerts are automatically issued for any abnormal status of devices.
- GuaranLink and WAN redundancy technologies ensure quick connection recovery to promote cellular connectivity between FTUs and FRTUs.

System Requirements

- An IP-based cellular architecture for reliable communication between FRTUs and FTUs.
- Both serial and Ethernet ports to accommodate devices with different interfaces.
- The network management software requires 8 GB RAM and 64 GB disk space to show data and alerts in real time.

Featured Products

OnCell G4302-LTE4

Industrial LTE Cat 4 serial/Ethernet-to-cellular secure routers



MXsecurity Series

Industrial network security management software designed for OT networks



Background

Preventing cyberattacks from affecting critical operations is essential to every operator. Therefore, organizations are integrating comprehensive cybersecurity into their OT/IT architecture because of the growing importance of protecting network data.

Feeder Terminal Units (FTUs) are primarily used for monitoring and controlling the operation of distribution lines. Many FTUs, however, are often distributed in unmanaged areas, making them particularly vulnerable to cyberthreats. In each district, Feeder Remote Terminal Units (FRTUs) collect data from several FTUs. Secure cellular routers with reliable cybersecurity features protect data communication between the FRTUs and FTUs, minimizing risk of disruptions and damage to critical infrastructure.

Moxa's Solutions

Moxa's LTE cellular routers offer high-speed performance and reliable communication between FTUs and FRTUs at substations, enabling immediate detection of any issues or anomalies in the system. They also provide protection against potential cyber threats to ensure system security. The OnCell G4302 secure cellular router is suitable for an FTU thanks to its small size, dual SIM slots, GbE RJ45 Ethernet ports, a RS-232/422/485 serial port, and built-in cybersecurity features. It helps the FTU establish secure LTE cellular connections to and from the FRTU in power substation, detect device status, and determine the interface for connection recovery.

In a scalable power network, FTUs are distributed across different areas. GuaranLink technology is embedded in the OnCell G4302 cellular router, offering redundancy to maximize connectivity. When data to and from FRTUs—which is transmitted via a physical connection—is interrupted, the OnCell G4302 provides WAN redundancy as a backup. Such redundancy makes it possible to switch between physical and cellular interface, effectively reducing downtime and stabilizing data communication between FTUs and the control center.

The OnCell G4302 offers advanced security features based on an IEC 62443-4-2 certified OS, thus supporting cybersecurity for IP-based cellular architecture. You can set up the firewall to only allow logins from recognized IPs, adding a powerful protection against DDOS attacks. The VPN allows data to be encrypted and protected against many intrusions.

The OnCell G4302 cellular router offers MXsecurity management software to monitor distributed devices and alert in case of link failure. MXsecurity benefits managers as they stay aware of the statuses of various OT devices and the overall state of network communication. Managers are kept up to date on network health as notifications are issued when any FTU within the network exhibits any abnormal status or behavior. Furthermore, centralized control of the security policy, firmware, and configuration enhance the overall security for the entire power system.

