Router Security

Although cellular data is very secure, when it comes to using an industrial cellular router that security can be bolstered even further, to make your system extremely robust.

Typical elements of your infrastructure would be an Industrial Cellular Router, SIM card and the devices connected to it such as servers, PLC's or anything that requires an internet connection.

First element to consider:

SIM Cards: IoT SIMs and conventional SIMs both serve the same basic purpose of maintaining an Internet connection for linked devices.

IoT SIMs employ a private APN rather than the common, shared MNO one. In contrast to standard cellular, which allows you and any other users with the same carrier to use the same network, this only permits devices with the proper credentials to connect to your network. Additionally, M2M SIM cards are frequently set up with fixed public or private IP addresses, and each connectivity provider provides an additional layer of network security against network attacks.

Using private APNs has a number of advantages, mainly security based. The only authorised network that can reach devices with a private APN is that network. Your IoT devices cannot be accessed without also gaining access to your entire network. Additionally, having a small number of verified devices on the network will avoid congestion brought on by consumer-level devices using the network's bandwidth.

Second Element to consider:

Wi-Fi: As you would with a HOME Network. It is recommended to change the default SSID (service set identifier) or name of your Wi-Fi network.

Change the default password to a more complex longer (at least 20 characters) that includes numbers, letters and symbols. The complex the password will be, the harder for hackers to access your network.

While less scalable, using an Access Control List makes monitoring specific Wi-Fi clients more simple by preventing all MAC addresses from joining the relevant SSID (wireless network).

Third Element to consider:

VPN: A virtual private network, or VPN, is a technology that was initially created to help corporations. Its main goal was to offer business networks secure, affordable, and adaptable solutions. Employees had access to work resources and data, while everyone else was denied access.

A VPN connection uses the internet to securely send data via an encrypted tunnel, rather than relying on expensive hardware to establish

Siretta Ltd
Basingstoke Road
Spencers Wood
Reading
Berkshire RG7 1PW

sales +44(0)118 976 9000
email sales@siretta.com
web www.siretta.com

closed-off networks. Siretta Routers
support GRE, IPSec, L2TPv3, OpenVPN and PPTP/L2TP. Depending on where your endpoint is, there are many options to keep your data and network secure.

Siretta Ltd
Basingstoke Road
Spencers Wood
Reading
Berkshire RG7 1PW

sales
email
web

+44(0)118 976 9000
sales@siretta.com
www.siretta.com