White Paper

Top factors to consider for Remote Connectivity to your Connected Enterprise in the cellular age

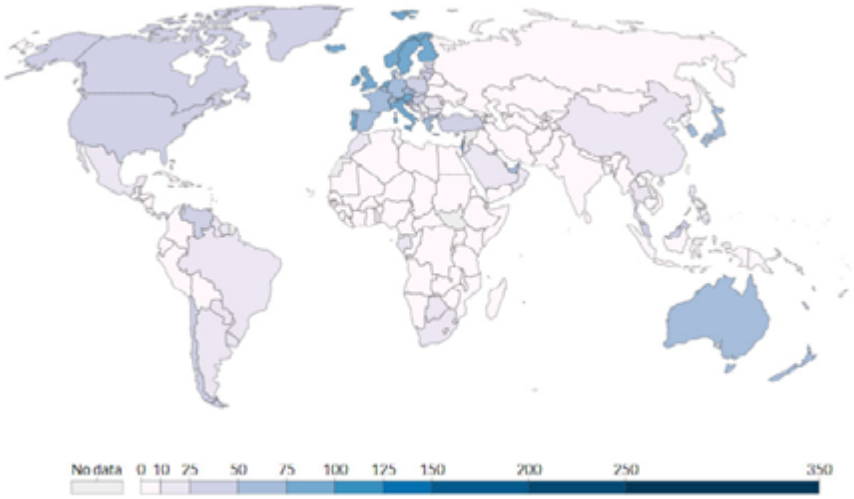
By Vishal Prakash, Product Manager, ProSoft Technology

Table of Contents

Copyright ©2022 ProSoft Technology, Inc. All Rights Reserved.

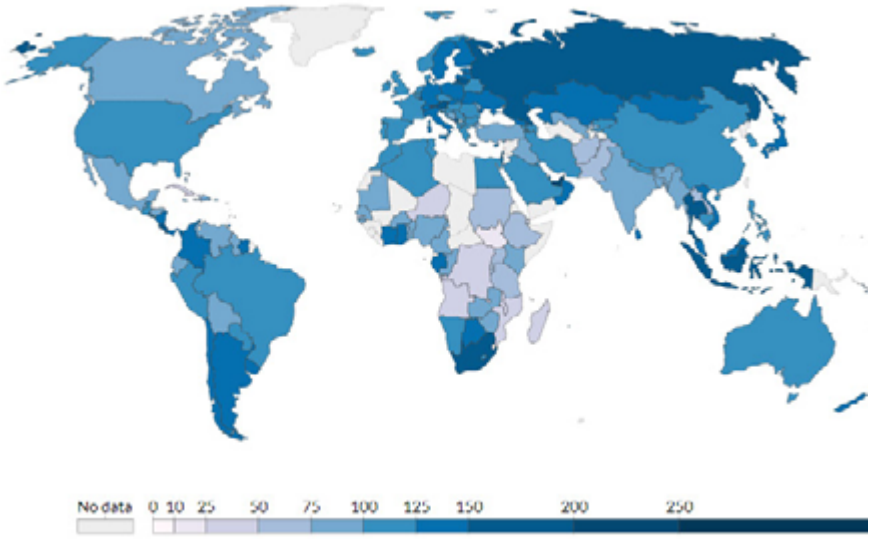
Introduction

The concept of monitoring remote industrial infrastructure assets began circa the 1970s. Since then, the types of communications media used to monitor the remote assets have come a long way - trunk mobile radio (TMR) to analog FSK radios to high-speed serial communications to fiber optic links to satellite and, now, different types of cellular WLAN communications.



Mobile Cellular subscriptions (per 100 people), 2001
Source: World Bank via Our World in Data, https://ourworldindata.org/internet

Over the last decade or so, cellular wireless communication coverage and technology has changed significantly. It is now ubiquitous and is the primary form of communications for more than 75% of the world's population. Today, the two most abundant things available on this earth is the air we breathe and cellular coverage!



Mobile Cellular subscriptions (per 100 people), 2001
Source: World Bank via Our World in Data, https://ourworldindata.org/internet

Advances in Cellular Technology

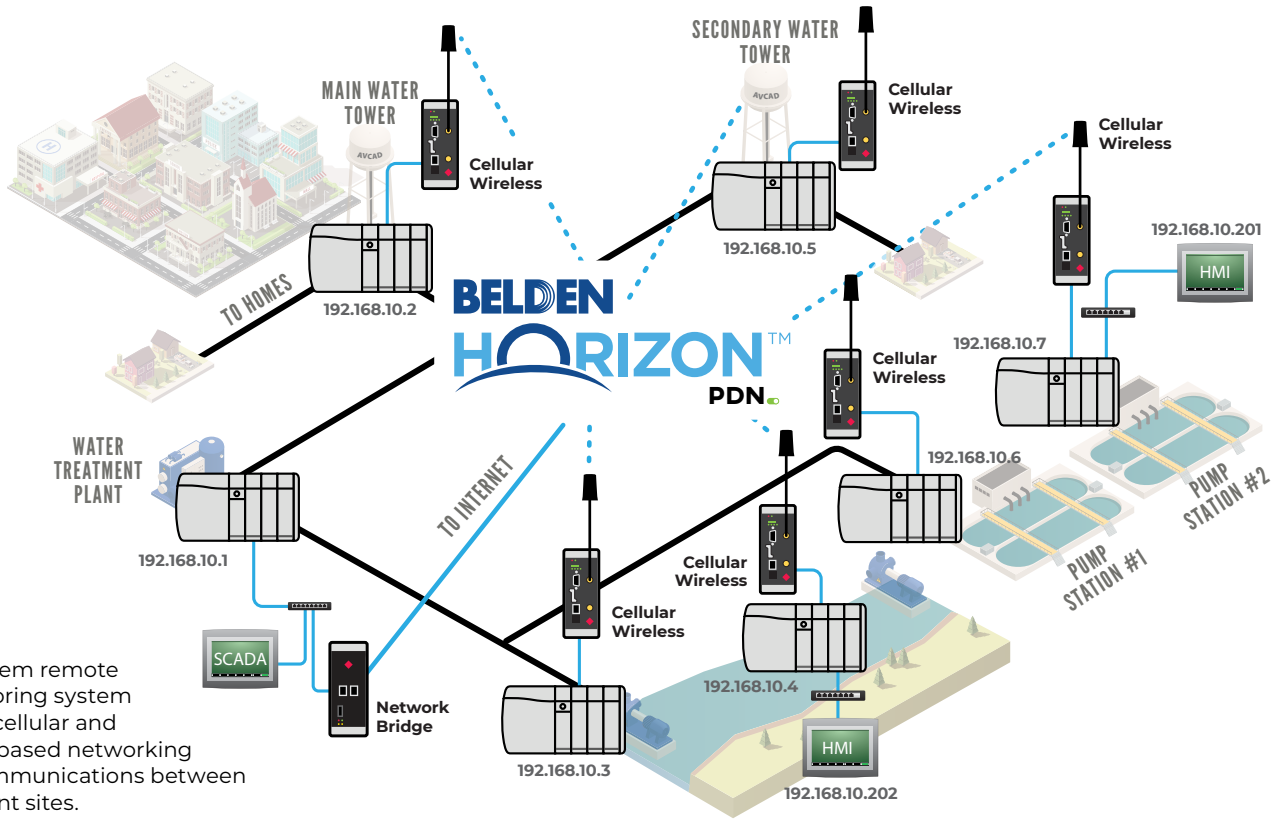
The very first cellular device was introduced in the late 1970s/early 1980s. Coverage and use was very limited and there was no support for data. In the 1990s, when 2G was introduced, coverage and reliability were still poor. By early 2000, 3G was introduced. With increased coverage, higher speeds, and reliability, industrial users were starting to take notice, but adoption was slow. The advantages of RF communications and the cost-to-performance ratio outweighed any benefits of 3G. But by the end of the first decade of the 21st century, wireless cellular coverage had increased significantly. More importantly, the speed and reliability of 3G networks meant that industrial M2M users had a viable option for remote communications. 3G speeds were approaching 40Mbit per second compared to IP-based RF radios over the air speed of 4Mbit per second.

Today, 4G/LTE can operate at speeds of over 100Mbit per second! The increased speed, reliability, availability, and security mean that a wireless cellular network is like having a switch in the air. As the world moves forward with 5G implementation, speeds will be in the GB-per-second range, which will only lead to increased use of the wireless cellular communications for industrial applications like remote monitoring.

Copyright ©2022 ProSoft Technology, Inc. All Rights Reserved.

Advances in Cloud-based Networking

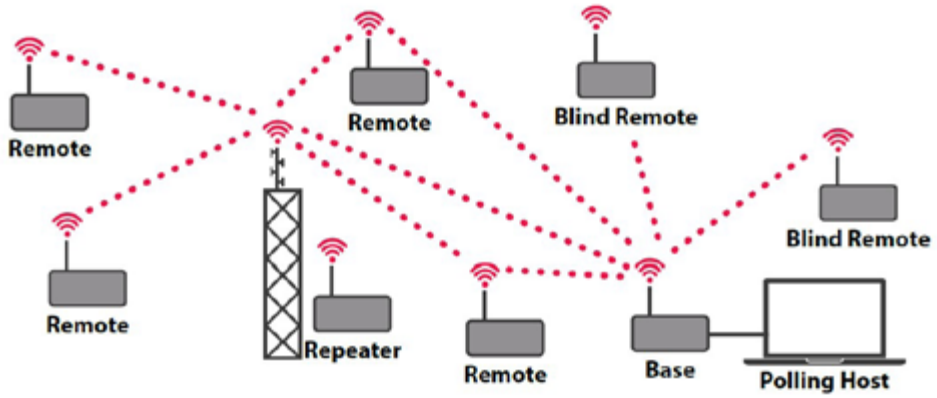
Put simply, an analogy for cloud-based networking is taking the Ethernet switch on your desk and placing it in the cloud. Devices connected to this switch can communicate with each other, a streamlined extension of your Connected Enterprise. A more complete definition is that cloud-based networking exists and operates within a cloud environment/infrastructure. The infrastructure, resources, cloud network management, monitoring, maintenance, and other network administrative and operational processes are performed within or through the cloud. The advances in cellular technology as described in the previous section have made cloud-based networking secure and reliable.



A modem remote monitoring system using cellular and cloud-based networking for communications between different sites.

Remote Monitoring and Control

What does the significance of this change - the ubiquitous global cellular coverage and cloud-based networking - mean for remote monitoring and control? To understand the impact of this universal coverage, we need to look at how information gathering from control systems has evolved over the last three decades.



A traditional SCADA system architecture based on licensed or unlicensed radio communications to remote sites.

Control system hardware, protocols, and architectures have also changed significantly, but the concept remains the same – digital and analog I/O that interface to field instruments which provide feedback to Programmable Automation Controllers (PAC) which is then used to make control decisions. The field data is then sent to a central location – typically a SCADA system - for viewing and recordkeeping.

Copyright ©2022 ProSoft Technology, Inc. All Rights Reserved.

Previously, only binary status data was brought back from remote control systems. This provided the user with basic information such as equipment status from remote locations.
The proliferation of the capabilities of control systems and significant advances in cellular wireless technology means that connectivity to remote assets can provide a very accurate and detailed picture of operational status at the remote location.

So, does this mean that everyone with responsibility for a remote control and monitoring system should adopt cellular communications?

The answer is not a simple yes or no. One has to consider multiple factors before making the decision:

1. Is the current system secure and adaptable to cloud technologies?
2. Can the system be expanded easily?
3. What about short-term and long-term maintenance costs?
4. Is there remote access for diagnostics?
5. Can my current system handle the increased data requirements to ensure operational efficiency?

The answers to these questions will be different for each use case. Rather than answering the questions listed above, let's look at this differently – Does today's wireless cellular connectivity solve the problems so that I can continue to operate my system easily, reliably, and securely, and meet all of my KPIs?

Factors to consider before selecting cellular wireless communications for remote communications

Security

Security is not a one-step approach – like a padlock on site or using usernames and passwords for login.
Control system security must take a holistic, multi-layered approach, called Defense in Depth. The Defense in Depth technique implies that:

- No single product, technology, or method is fully secure – it has to be a complete solution
- The solution must address internal and external threats
- The solution must utilize physical, procedural, and electronic means at separate Industrial Automation and Control Systems levels

Components of the Defense In Depth approach to control system security.

There are several components that must be addressed. The cellular wireless gateway is critical – this is the point of connectivity to the control system. The following are some of the considerations when choosing the right industrial remote access gateway:

- Ability to change the default password to a strong password
- Use of multi-factor authentication if managed by a cloud service
- Connection initiation restricted to outbound requests only – originates from the gateway to the authenticated server of the machine or plant network
- Only limited well-known ports used
- All traffic encrypted through these ports
- Ability to separate the tunneling or data channel from the control channel to prevent unwanted access to your machine or your end user machines unless authorized
- Use of digitally signed gateway firmware
- Does not use static public IP addresses
- Continuous third-party security evaluation is done (penetration testing, fuzz, (Achilles) for a proactive approach to addressing any vulnerabilities.

Copyright ©2022 ProSoft Technology, Inc. All Rights Reserved.

The next layer to secure is the network, which includes switches, routers, and firewalls. The network does not apply if using a cellular gateway in the connected network. Following known best practices in choosing the right device will help you ensure network security. It is important to use tools that can maintain device configuration compliance, monitor for changes and, more importantly, notify the appropriate person within the organization when there are changes.

The next layer is the internet or the type of access for secure remote connection – for example, an OpenVPN server or a cloud service. The considerations for each type are slightly different. The OpenVPN type of connectivity requires significant configuration and maintenance. For example, the user will have to issue security certificates for each device and client software will need to be kept up to date.

- If a cloud service is being used for connectivity, then the following considerations are important:
- Ensure the application architecture is designed for security and to natively operate in the cloud.
- Ensure the service employs multiple layers of security within the cloud applications where trust is not assumed and communications are encrypted – even between microservices
- Ensure any and all data kept in the cloud is encrypted
- Ensure deployment across different regions or even multiple clouds for resistance to Denial of Service attacks, high availability, and redundancy
- Only use secured service provider networks and services. Amazon Web Services, Microsoft Azure, and Google Cloud are very secure themselves but that doesn't ensure the application software is secured or cloud networks are secured
- Conduct regular security audits of the service, preferably by an independent security expert.
- Ensure that a one-time-use password is being used to initiate connection to the control system
- Ensure token-based two-factor authentication (2FA) is used versus less secure SMS-based 2FA
- Encrypt data when transmitted, with no less than AES 256-bit encryption
- Use a system that extensively maintains and records activities

The next layer, PC or a master PAC, is the device that is used to connect to the remote asset. If it is a SCADA PC, then the firewall should be enabled, the machine OS up to date, and a well-established and known virus checker needs to be active. The next layer, procedure, is a combination of security and safety for remote connectivity. It is important to ensure the right procedures to authorize, enable, and disable connectivity are written, understood, and enacted within the organization. Ideally, the remote access service employs technologies that help enforce the procedures, such as required access approvals for each connection request.

System Expansion

Any system can be expanded. But is it simple and cost-effective? Consider a system that is using typical licensed or unlicensed data radio communication – to expand, the user may have to conduct a radio survey, and add an RF tower, a repeater site, or store and forward through an existing site. Any of these activities are expensive and can be complex. If the system uses cellular communications, then expansion is simple – add a cellular modem to the new site(s), activate the modem, and connect it to the network. Communications will be direct, so no change to any of the other remote sites is required. If this simplicity is measured in dollars, then adding a complete data radio site could cost upward of $20,000, while a complete cellular site is likely to cost between $7,000 and $10,000 – a 50% CapEx savings!

Maintenance

All systems will require some sort of maintenance – just like a car, regular servicing and upkeep will ensure the longevity and smooth operation. Maintenance on a data radio-based system may include retuning every radio and base-station in the network; antennas, connectors, and long lengths of cable exposed to the elements; and possibly antenna towers. Maintenance for cellular systems is minimal, limited to low profile antennas and possibly some RF cable, significantly reducing OpEx costs.

Remote Access for diagnostics

The benefits of secure remote access are well-documented – reduced downtime and support costs. Remote access is a necessity for today's control systems. With older systems featuring data radios or leased line, remote access was complex to set up and maintain. Remote access to the PAC required the remote user to connect to a central location and then access the PAC because it was unlikely that the user would have a radio modem connected to his PC at home or on the beach! The same is true with leased line or fiber optic setups. A cellular-based wireless remote infrastructure network provides anytime, anywhere secure remote access, direct to the PAC. This direct, secure remote connection means that the system operates uninterrupted, with increased speed and bandwidth allowing the user to diagnose the issue quickly, increasing productivity.

Copyright ©2022 ProSoft Technology, Inc. All Rights Reserved.

More data from remote sites = a truly Connected Enterprise

It is no longer acceptable to just bring back status information from a remote site. Control systems and smart field devices can provide a plethora of information like operation parameters, advanced diagnostic data, time-stamped data, asset identification data, and performance data. This information is extremely useful in analyzing the overall process efficiency, and potentially making improvements to your Connected Enterprise in real time. To process all of this data efficiently, a high-speed connection and increased bandwidth will be required. A wireless cellular infrastructure communications network can cost-effectively provide the increased bandwidth and speed.

Simple and Managed

We have mentioned the advances of wireless cellular technology, including the reliability, availability, and security - factors a user must consider prior to using this form of communications. What about simplicity and management of these networks? A traditional communications network is complex to manage and maintain. Hidden engineering and support costs can make it very expensive. This is a challenge with limited monetary and personnel resources. So, in choosing the appropriate cellular wireless gateway for your remote monitoring and control needs, simplicity should be a factor. Simplicity should be measured in the connection and recovery time of the gateway, ease of installation, support, and compatibility. The cellular networks are managed by the cellular service providers. If a cloud service is used to provide the secure connection within the network, then it is recommended that this service be fully managed so that you can remain focused on what is important to you – ensuring smooth operation of the control system and maintaining the service to your customers.

Conclusion

The evolution in cellular and cloud networking technologies has led to this combination for remote monitoring and control, which integrates into the Connected Enterprise. The advantages of a cloud-native simple, secure, and managed remote communications network that operates using the global wireless cellular network are clear – increased speed, bandwidth, reliability, security, availability, and cost-effective. The always-on nature of wireless cellular communications and cloud-based networking provides real-time connectivity and allows control systems to operate efficiently. Investment in this technology ensures that organizations needing to monitor remote assets will have better access to real-time data, and will lead to better system performance and increased operational efficiencies.

Support and expertise for your projects

ProSoft provides a variety of resources and services for wireless applications from initial system design to site surveys to launch support and configuration support.

Contact Us

Asia Pacific

Regional Office
Phone: +603.2242.2020
asiapc@prosoft-technology.com

Regional Tech Support
support.ap@prosoft-technology.com

North America

Regional Office
Phone: +1.661.716.5100
info@prosoft-technology.com

Regional Tech Support
support@prosoft-technology.com

Europe/M. East/Africa

Regional Office
Phone: +33.(0)5.34.36.87.20
europe@prosoft-technology.com

Regional Tech Support
support.emea@prosoft-technology.com

Latin America

Regional Office
Phone: +52.222.264.1814
latinam@prosoft-technology.com

Regional Tech Support
support.la@prosoft-technology.com

Copyright ©2022 ProSoft Technology, Inc.
All Rights Reserved. December 2022

ProSoft® TECHNOLOGY
www.psft.com