TECHNICAL ARTICLE

Still using 2G/3G SCADA modems? Plan to get them replaced with 4G/LTE

by Graham Nasby

Think 2G, 3G, 4G/LTE and 5G only apply to cell phones? Think again! These cellular technologies are also used for communication modems in many critical sectors such as power distribution, gas utilities, pipelines, and Municipal Water/Wastewater control systems.

If you are a Municipal Water or Wastewater utility make sure to regularly review which control system, fleet tracking, and SCADA modem technologies you are currently using. Cellular network providers are currently in the process of shutting down older 2G and 3G networks in order to make room for newer 5G and 6G networks. It is imperative that utilities transition away from older 2G and 3G equipment as soon as possible.

See below for more detailed technical information from the FCC in the United States. It's a similar situation at many other countries:

Phase Out of 3G Cellular Networks and Service

The Federal Communications Commission (FCC) has issued a reminder that "Mobile carriers are shutting down their 3G networks, which rely on older technology, to make room for more advanced network services, including 5G. As a result, many older cell phones will be unable to make or receive calls and texts, including calls to 911, or use data services. This will affect 3G mobile phones and certain older 4G mobile phones that do not support Voice over LTE (VoLTE or HD Voice)."

The plans and timing to phase out 3G services will vary by company and may change. Consult your mobile provider's website for the most up-to-date information.

- AT&T announced that it will finish shutting down its 3G network by February 2022.
- Verizon announced that will finish shutting down its 3G network by December 31, 2022.
- T-Mobile announced that it will finish shutting down Sprint's 3G CDMA network by March 31, 2022 and Sprint's 4G LTE network by June 30, 2022. It also announced it will shut down T-Mobile's 3G UMTS network by July 1, 2022, but has not yet announced a shutdown date for its 2G network.

If your mobile carrier is not listed here, you may still be affected. Many carriers, such as Cricket, Boost, Straight Talk, and several Lifeline mobile service providers, utilize AT&T's, Verizon's, and T-Mobile's networks.

TECHNICAL ARTICLE

New ISA Paper: How to Implement an Industrial Cybersecurity Program

From ISA news release

The International Society of Automation (ISA) and the ISA Global Cybersecurity Alliance (ISAGCA), with contributing author Gary Rathwell, have released a new white paper entitled, "Implementing an Industrial Cybersecurity Program for Your Enterprise."

ISA/IEC 62443 provides powerful tools to reduce the risk of financial, reputational, human, and environmental impact from cyber-attacks on Industrial Automation and Control Systems (IACS). ISA/IEC 62443 has been categorized as a "horizontal standard" by the International Electrotechnical Committee (IEC), validating its applicability for a wide range of industries. Any specific company is likely to find that while most of the standard applies to their IACS, parts of it may not. For example, some "normative requirements" that are appropriate for an interstate pipeline, may not be relevant to a chemical plant or a discrete manufacturing facility. There are also obvious differences between a large-scale corporation with many sites and thousands of employees, and a small company with a few dozen staff. It is therefore recommended that each company establishes their own IACS Cybersecurity Program to manage cybersecurity risks, and ISA/IEC 62443 2-1 provides guidance on how to establish such a security program for IACS asset owners.

The white paper is intended to summarize the guidance from the series of standards and address the specific needs of owner/operators of industrial facilities. The paper covers the following topics:

1. What is an IACS cybersecurity program?
2. Preparing an IACS cybersecurity program
3. How does an IACS cybersecurity program relate to IT cybersecurity?
4. Costs and benefits of an IACS cybersecurity program
5. What to do next

"Creating an IACS cybersecurity program is approachable, and companies should be working with their vendors and partners to build such a program if they don't already have one in place," said contributing author Gary Rathwell. "This paper gives a foundation for building a program, and there is no time to waste for companies and organizations looking for protection from, and mitigation of, cyber incidents."

Download it form here: https://gca.isa.org/implementing-an-industrial-cybersecurity-program-for-your-enterprise

In the coming months, ISAGCA plans to publish additional white papers intended to guide IACS vendors, suppliers of IACS products and services, integration/engineering services, and other stakeholders as they prepare IACS cybersecurity programs within their facilities and operations.