Cyber Security for Pipelines Other SCADA Systems

By Kevin Finnan & Jeff Melrose

Supervisory control and data acquisition (SCADA) systems have been part of the process industries for many decades and cyber security measures need to grow as technology advances. SCADA systems are used in oil and gas pipeline and other remote control and monitoring applications, such as electrical transmission and distribution, and water/wastewater.

While the technology continues to evolve, the underlying use case remains: gathering and transmitting data from distributed sensor networks and sending control commands. The term SCADA itself has come to mean many things and often is used interchangeably with distributed control system (DCS) and other automation system configurations.

A SCADA system supports bi-directional communication between distributed field devices and a central control area. For example, an oil and gas company might use a DCS to control a refinery, but a SCADA system will be used to control the pipelines coming into and leaving the refinery. As a result, the SCADA system can cover longer, more linear distances than a DCS, like supporting a pipeline. In many respects, SCADA systems are a proto-Industrial Internet of Things (IIoT) application with respect to their basic functionality.

Traditional Deployments

For example, refer to Figure 1, a hypothetical remote pipeline pumping station. All the field instruments and actuators connect to a remote terminal unit (RTU), which serves as a data consolidation and translation point. The RTU also works with whatever backhaul transmission medium is in use, such as 900 MHz radio, satellite, or any other media necessary to handle the required bandwidth and distance.

Figure 6. *Remote condition and performance monitoring for large pieces of critical equipment by the OEM already is happening. The result is often multiple SCADA systems working in parallel at the same site. The way these systems interact must be carefully controlled.*

The various field devices may use assorted communication methods to connect to the RTU, but the RTU serves as a gateway, converting it all to one protocol—such as Modbus or something proprietary—so it can transmit everything in one data stream. Some local control functions may be necessary at the site. Additionally, the RTU can perform the local functions or a programmable logic controller (PLC) or other small controller may be used, but it too will report its activity through the RTU.

Older radio communication methods for many of these systems often proved unreliable with 900 MHz systems susceptible to interference. New approaches offer improvements, but many pipeline operators retain the older platforms, problems and all, for cost reasons.

The RTU frequently serves as the focus for cyber-attack methods. Hackers often find older RTUs poorly defended with unsecured communication, so they become the path of least resistance into the network.

One of the most famous hacks relating to this cyber-attack method was in western Ukraine. In December 2015, attackers started shutting down an electrical grid by gaining access to devices similar to RTUs spread among substations. In this particular case, the units themselves were the weak links and were targeted because of their poor defenses and strategic positions. Once reached, tripping one caused a high level of disruption.

SCADA 2.0, IIoT Development

As old as the SCADA concept is, it has not lost any of its importance. In fact, the role of SCADA systems is growing, which is broadening their definition. With a higher degree of protocol standardization and greater connectivity to corporate information technology (IT) networks, the potential for a cyber-attack also increases and is growing.

The trends toward business systems using and processing SCADA data create new avenues and reasons for system exploitation. Sharing data is often the lifeblood for many companies, but new threats can emerge in the process.

On the other hand, developing technologies also are changing the current situation as the IIoT merges with SCADA to become “SCADA 2.0.” This still has some time before development is complete, but there are many possibilities, including its design and how it could affect security considerations (Figure 2).

The RTU, at least as a gateway, no longer will be included since it won’t be needed. The individual field instruments and actuators at the hypothetical pipeline pump station will all communicate directly with the ubiquitous network, just as a technician visiting the site might call back to the office on a smartphone. The data from the devices goes to the cloud and can be captured and used by whichever part of the company

needs it, from anywhere. At this point it's difficult to say exactly what the network might look like, however it most likely will be 4G or 5G capable, but the communication will be direct. New networking technologies like low power wide area network (LoRa WAN) may be included as well.

Setup for these installations will be easier than with current SCADA systems. It will be as easy as installing the field device, turning it on, and connecting it to the cloud. This will get rid of all the expensive and dangerous manual operations still being done at many sites. If a level instrument is added to the storage tank, the need for a worker to be sent out for maintenance no longer will be necessary.

However, there may still be a need for control functions at the site. A natural gas compressor or other complex equipment may need fast-loop control, which will require a local PLC. Control via the cloud is still under development. These installations may use the PLC as a data consolidator, but it depends on each use case.

If the cloud architectures are what they need to be, this type of system should be very secure. By eliminating the RTU/gateway and less-reliable backhaul communication methods, a hacker will have to gain access to multiple field devices one at a time rather than gaining access through the RTU. A single IIoT device is not connected to the network in the traditional sense as its wired predecessors are, so while it might be possible for a hacker to disrupt the individual device, this will not provide a means to access the larger network.

The reality of this concept is some time away since the networks with the necessary requirements don't currently exist. Coverage and speed are improving all the time, but 5G or even 4G in all the areas where pipeline pumping stations are located is not there yet.

Accommodating Multiple SCADA Systems

One current aspect of monitoring technology is the idea of multiple SCADA systems at one location, and the user might not even realize it. How does this happen?

A turbine-compressor set might have its own system to remotely monitor performance and conditions, and there is probably an existing SCADA system. These original equipment manufacturer (OEM) systems often are included to verify performance requirements written into purchase agreements. This kind of monitoring keeps everyone honest and helps the party responsible for maintenance stay informed with what's happening. The system is in communication with the OEM's headquarters and sends data back every day via its own network. Having this kind of communication is necessary and is ultimately a good thing for the most part, but there can be problems.

For example, at some point the 6-month-old turbine running a pipeline compressor inexplicably slows down by 20%, and product flow declines as a result. Nobody at the pipeline company called for the change and some investigation shows that it was initiated by the turbine OEM. A message from the OEM reports that a problem seen elsewhere in other units may be present here as well, and to avoid an outage, it is necessary to reduce capacity until it can be investigated. It sounds like a prudent idea, but now the OEM is controlling the process, using its connection to the unit. Situations like this call for negotiations as to who is allowed to do what.

Invariably, the OEM and the pipeline operator's SCADA systems will be interconnected, but there must be control as to how they're connected and to what extent. The OEM's network becomes an extension of the owner's network and vice-versa.

But who else is connected to the OEM's network? What if the OEM outsources some of the system monitoring? Since hackers typically attack a strong network via a weak one, someone wanting to attack the OEM might use the pipeline operator's SCADA system as the conduit.

The bottom line for the equipment owner is these situations are already part of the real world, and users must tolerate them for operational reasons. The defensive strategy is to be very careful as to how the two systems are interconnected. There are methods to control traffic between the two, avoiding open pathways creating opportunities for hackers.

Signs of Threats to Come

Cyber criminals looking to make money from their exploits have been stealing financial data, personal information, and credit card numbers for a long time. Major retailers and financial service companies have fallen prey largely for this reason. Fortunately, industrial companies don't necessarily have much in the way of such marketable data capable of being stolen. The scary alternative is ransomware, which has targeted hospitals and now spread to many other users in the recent "WannaCry" ransomware attacks.

Returning to the example of the hypothetical pipeline station for this scenario, say the operators at the central control room receive an alarm via the SCADA system because transportation has been shut off. Calling up the human-machine interface (HMI), they see a top-level screen saying that access to the RTU has been locked out and encrypted. The only way to regain control is by paying to get the access code.

The option for the company is to pay, or send somebody out to the site to take it offline and turn operations back on manually. This is only temporary because it is not practical to leave an operator at the site on a continuous basis. The only real solution is to take out the compromised RTU and replace it, at a cost significantly higher than the ransom.

This situation may seem unrealistic, however, as technology and cyber criminals become more advanced, predicting situations like this should be considered.

Defensive Strategies for SCADA Systems

SCADA systems need to be defended using the same strategies as other industrial networks. There are no unique approaches to this situation, but keep in mind, the size and complexity of the SCADA system provides many opportunities for determined hackers. They will scan for weaknesses, and a large, spread-out pipeline or similar SCADA system provides

many attack vectors hidden away. The following are a few defensive suggestions:

- Maintain physical security at remote sites: RTUs and other network-connected hardware should be in locked enclosures. Unused ports should be plugged with epoxy.
- Update old systems: Any company still running equipment using Windows 95, or even more recent but still obsolete versions, is asking for trouble. Platforms running un-updated software can be just as bad. WannaCry only worked on outdated and un-updated Windows platforms.
- Use network identification: Intrusion detection systems are very useful tools, but many companies fear they can disrupt networks. They can be designed for low-impact and with a passive response to make them easier to use on operating networks.
- Train personnel: Workers are still the weakest link in cyber defenses. Social engineering, phishing, and spear phishing remain effective hacking tools. Don't open unknown attachments, don't plug in unknown thumb drives, etc.
- Maintain network traffic logs: It's hard to know if something strange is happening if you can't identify right from wrong. Logs help establish baselines, so they can help determine where intruders have been and what damage may have been made or attempted.
- Use available cyber security resources: The International Society of Automation www.isa.org and the National Institute of Standards and Technology www.nist.gov ISA/IEC 62443 offers many helpful resources and provide best practices for network administrators and defenders, as do NIST 800-14 and 800-16.

It will be easier to implement more cyber security measures with new technologies, but many companies find themselves still working with yesterday's equipment and software. These installations will become increasingly vulnerable if cyber defenses are not kept up-to-date. The job is challenging, but it can be done. Defenses don't have to be air-tight to be effective. Hackers need to be resisted only to the extent necessary to make them look for an easier target.

YOKOGAWA

Yokogawa Corporation of America

12530 W. Airport Blvd.,
Sugar Land, TX 77478

yokogawa.com/us

Yokogawa Canada, Inc.

Bay 4, 11133 40th Street SE,
Calgary, AB T2C 2Z4

yokogawa.com/ca

Yokogawa de Mexico, SA de CV

Urbina No. 18
Parque Industrial Naucalpan
Naucalpan de Juarez, Estado de México
C.P. 53370

yokogawa.com/mx