HURST TECHNOLOGIES

CYBERSECURITY: THE INDUSTRIAL CONTROL SYSTEM PERSPECTIVE

In August, 30,000 disc drives, representing 75% of the workstations of the petrochemical giant, Saudi Aramco, were hacked with a malicious virus called Shamoon. An image of a burning American flag replaced critical data on these machines.

According to experts gathered at the ICS Cybersecurity Conference, October 22-25, in Norfolk, Virginia, the cybersecurity threat is morphing. Owner/operators need to remain vigilant, but also understand that cybersecurity has a broader meaning in ICS circles.

There are several critical takeaways from the conference. First, the solutions that have been driven from the information technology (IT) side of the business are not necessarily appropriate for the operations technology (OT) side. That means that what works, for example, for the human-machine interface (HMI) may not work for the programmable logic controller (PLC) in the power plant or a remote terminal unit (RTU) at a substation. According to this group of experts, vendors are woefully behind in addressing the real cybersecurity issues in OT.

Second, this group of ICS cyber-experts has expanded the definition of cyber-security. They prefer the phrase cyber-incident, rather than cyber-attack. A cyber-incident is defined as "electronic communications that impair machine operation." If a peaking gas turbine fails to start because of a problem in the control system, that's a cyber-incident. Obviously, that casts a wide net. Instrumentation and control (I&C) systems have traditionally been the number one culprit of peaking units failing to start. Because automation and remote "push button" starts are now common with gas-fired plants, that's probably even truer today. The larger implication here is that what power industry engineers understand as control system and communications *reliability* is being re-defined as cyber-security.

Third takeaway is that, while power plant owner/operators are spending millions on compliance with NERC (North American Electric Reliability Corporation) Critical Infrastructure Protection (CIPS) standards, compliance does not necessarily equate to better security. Too much of the past and current effort has been focused on the HMI and attacks that are typically seen in the IT commerce world. Attacks in the ICS world are typically more focused on a particular outcome on specific hardware and software. Many cybersecurity standards efforts are limited to addressing the typical attack vectors but not the lower levels of communications in the ICS plant.

The fourth takeaway, and perhaps the most far-reaching, is that the morphing of cybersecurity has the potential to impact major gains in acquiring and propagating data, sharing information to break down silos within organizations, integrating "islands of automation" at the plant, and flattening organizations to improve productivity and reduce costs. Owner/operators of critical infrastructure (not necessarily power plants, but, for example, water treatment facilities) report that they are "dialing back to a dumber, less integrated" control and operating system and relying on "physical" security measures. Flexibility provided by allowing workers to use their own devices (cell phones, ipads, laptops, etc, also called "bring your own device" or BYOD) is now being restrained.

Here are several other thought nuggets gleaned from the conference for plant managers and their staff:

- Each line of computer programming code is an opportunity for malicious entry into the system. Of course, millions of lines of code govern critical infrastructure operation today.
- PLCs are especially easy to overwhelm because the code is relatively simple. According to one presenter, Rockwell PLCs are priority targets for hackers.
- While control and knowledge system vendors are designing and offering solutions, albeit ones that rely too much on the IT side, *system integrators are the missing link*.
- Many vendor security solutions cannot be implemented because of safety impacts
- Vendors are mixing safety and control logic to achieve savings, but cyber-security issues multiple because both use the same communications networks. For example, the burner management system and the turbine control system may be separate systems but both probably use the same network.
- ICS typically have no forensic capability to trace electronic signals, users, etc
- No accepted metrics exist on which to design ICS cybersecurity capability or to understand whether your facility is "secure" or not. NERC CIPS, for example, has no metrics, only procedures and policies, and "boxes to check off."
- Utilities are pulling routable protocols and going back to serial to avoid becoming a "critical asset" under NERC CIPs.

The cybersecurity experts at Hurst Technologies can help you design and implement solutions without sacrificing the other benefits of digital applications. Contact Lee McMullen at leem@hursttech.com or call 979-849-5068.