AS SEEN IN THE WINTER 2020 ISSUE OF ...
VALVE MAGAZINE

ONLINE CONTROL VALVE DIAGNOSTICS IN TODAY'S CYBERSECURITY WORLD

BY LEO HUGHES

The topic of cybersecurity usually brings to mind data breaches that impact financial or private information, stolen intellectual property or disruption of major events such as political elections. But even more severe threats exist, including cyberterrorism. Industrial leaders, in particular, need to be aware of the situation because of the risks associated with operating a plant. Power, gas and hydrocarbon derivatives are all essential to daily existence today, yet each of these resources involves highly dangerous processes that, if compromised, could become major weapons of cyberwarfare.

As we digitize our industrial plants to optimize operations and gain efficiencies, we add more intelligence and create easier access to data that drives process benefits. In the world of online control elements, we see advances in communication, sharing of data and real-time availability, while we simultaneously gain better control of critical processes. Compromising or losing control of one of these online control elements has the potential to turn a highly efficient plant into an immediate threat.

It's more important than ever to understand the power of the tools at our fingertips and to differentiate software functionality today to what is accessible online versus what is accessible offline, especially when it comes to system diagnostics and control override commands.

CONTROL VALVES IMPACT

Pressure control valves are critical for process management as well as for keeping downstream equipment safe from over-pressurization. In most cases, secondary safety devices in a plant protect the plant from dangerous events. But a loss of control to a power plant's steam line could result in over-pressurization of an entire steam system.

Secondary safety devices protect by causing safety valves to relieve line pressure. However, this also takes the plant offline from generating power until the system can properly restart and pressurize. A huge loss in productivity and potential impact on the electric power capacity available to a local area or damage to a regional grid can affect millions of people.

More severe impacts are possible when we're dealing with combustible

SUBJECT: Diagnostics have become a critical tool in digitizing our factories. But they must operate in a new world of cyberthreats.

KEY ISSUES:

- Today's cyber dangers
- The criticality of ICS and diagnostic tools
- Where the vulnerabilities are

TAKE-AWAY: The most secure diagnostic tools are designed so that the same software that provides needed data is not what is used to control the processes.

Executive Summary

fluids such as natural gas or oxygen service. Loss of pressure control to a residential pipeline, for example, could lead to immediate over-pressurization at homes, where backup safety systems may not be as robust. If a hack to a process yielded a spark that occurred within an oxygen line in a chemical plant, the results could be disastrous. In either scenario, whether a spark or a pilot flame is involved, the fluid could ignite, causing major destruction.

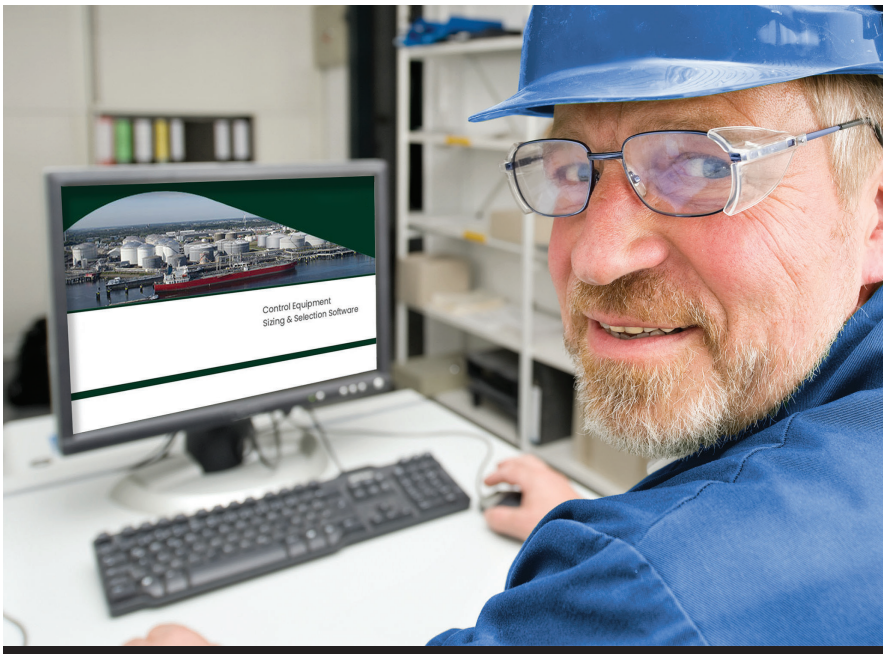
These are just two of infinite amounts of dangerous scenarios that exist every day. Yet plant optimization and the call for operational efficiencies demand real-time availability of data. Maintaining control and eliminating disruption are essential, which makes understanding the role of industrial control systems (ICS) in this whole scenario critical for avoiding possible compromises and to secure the safety of our plants.

INDUSTRIAL CONTROL SYSTEMS

Industrial control systems (ICS) deliver the data necessary for optimizing a plant and taking direct control of the process. As such, they are the intriguing targets to hackers because they serve as a single point of access that controls an abundance of raw, unharnessed power. Because of this, gaining control of this point of access could induce severe disruption, chaos and catastrophe. This reality means considerable focus has been dedicated to securing ICSs as they come online and implementing additional layers of protection beyond a firewall, protection that prevents hackers from modifying the process if they break through the first line of defense.

However, inherent designs in older plants make this more difficult. These designs have vulnerabilities such as 1) 'back-door' access to facilitate remote service and troubleshooting, 2) improperly installed firewalls that can be breached, 3) insufficient training of users or contractors that have the ability to modify or override settings and 4) readily available auxiliary software that can communicate with control elements such as prime movers or automated valves.

In 2010, real disasters were caused by the release via portable thumb drives of the Stuxnet virus to sabotage centrifuges. Much like a biological virus, the infection spread rapidly, and within months, thousands of programmable logic controllers around the world were infected with this incredibly complex virus. Many of those affected were in the process control industries, including power plants, chemical plants and pipelines. It is widely believed this was the first shot fired in the battle to begin the industrial cybersecurity war. Malware with more complex designs such as Duqu, Flame and Gauss followed this trend, all targeting ICSs. Electricity, fuel and food sources were attacked, exposing vulnerabilities not only to plants but to entire populations should shutdowns occur for extended periods of time.



☐ An engineer uses software for selecting and sizing the proper valves.

ONLINE DIAGNOSTICS

Most leading control valve manufacturers today offer software tools for online valve monitoring that track performance trends and detect outliers while a valve is in operation. This is most often achieved with software integrated into the ICS and connected to the control valve digital positioner via data acquisition networks (depending on the communication protocol deployed). In a Foundation Fieldbus or Profibus system, all valves and positioners are connected to the control system directly through multi-drop buses. In a hybrid analog/digital HART protocol network, valves and positioners are connected to the control system via HART analog output cards. In either scenario, users must fully understand the override possibilities and ramifications of diagnostic monitoring software that has access to control valves at any time during plant operations.

As end-users' usage of these communication protocols has evolved, valve OEMs have continued developing online diagnostic software as part of their core portfolio scope. Along this journey, many OEMs have found the fastest path to market has been to simply expand their existing calibration and commissioning software platforms to include real-time online diagnostic feedback. While this method is initially attractive because of the ease of installation and speed to market, a deeper understanding reveals that this approach breaks the cardinal rule

☐ A digital valve positioner

of cybersecurity. If hacked, any online software that allows access to controlling the valve for closing or opening could result in an emergency plant shutdown, or worse, a lethal event.

This topic of online diagnostics that have the ability to control is especially important given that many plants typically prioritize their most critical valves for diagnostic monitoring. Because of this, hackers can make the greatest impact on the most critical applications by simply tapping into a misapplied online diagnostic tool. This type of indirect cyberattack is known as "Island Hopping," and it is a well-known tactic whereby attackers move laterally within a compromised network looking for less defended programs or systems, and penetrate quickly, often without detection.

Because of this reality, the ideal cybersecure approach to online control valve diagnostics is to separate software programs that continuously monitor valve performance from those tools that can be used to control and move the valve.

A U.S.-based cybersecurity firm specializing in ICS recently issued an alert identifying a cyberattack group that is primarily active in the Middle East whose sites are now set on disrupting the U.S. refining industry. The group's recent 2018 attack successfully infiltrated a refinery's safety instrumented system with the intent to cause a lethal explosion. The International Society for Automation (ISA) responded to this growing threat by forming a Global Cybersecurity Alliance that endorses cybersecurity standards, such as ISA/IEC 62443. This consortium of OEMs, end users, government agencies and expert consultants was created to share awareness, education, readiness and knowledge in the face of growing global cyber threats.

Today, valve OEMs play a critical role in this consortium, not only to develop safe software tools, but also to provide education so users understand the proper application of the tools. When designing a strategy for optimization and valve lifecycle management using online diagnostic software, system architects must consider not only the benefits of performance management but also the cybersecurity of their total solution.

CONCLUSION

Combining all-in-one, online solutions exposes plants to potentially catastrophic scenarios that could otherwise be eliminated with the right tools in place.

Online diagnostic tools are essential, and they offer a wealth of features via friction and error-trending algorithms for tracking trends, diagnosing and predicting failures during real-time operation before actual visible performance degradation occurs. However, recent events and increased awareness of potential threats emphasize that online monitoring programs should be scrutinized and separated from tools with the ability to command and override control.

Various options exist today, but only a few are designed specifically to provide the full, real-time benefits without the cyberexposure. The most secure designs include separate online diagnostic software that cannot write commands to any valve it is monitoring. VM

Leo Hughes is senior training manager for digital valve products, Baker Hughes. Reach him at Leo.Hughes@bhge.com.