

the final say | Views from Automation Leaders

Build Layers of Protection for Safer Facilities

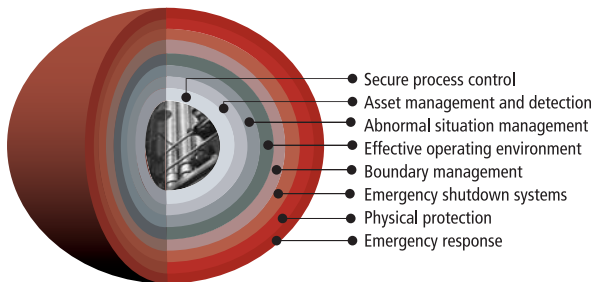
By Marilyn Guhr



"Security is a journey, not a destination."

Write it in big letters on a piece of paper, and put it on a wall where you can see it everyday. New threats to your people, your assets, and your facility emerge constantly. Random system enhancements—a security camera here, a required password change there—won't decrease your vulnerability. You need a plan that provides protection today, while allowing you to adapt to new threats as they arise.

Create layers of protection



Start with a vulnerability assessment of your site, and aim to create layers of protection from the process control network through the perimeter of the plant. The layers-of-protection concept is widely recognized in the process industries and IEC 61508 and IEC 61511 define as standard.

It starts with a secure process control network that establishes a safe networking infrastructure for the entire plant. Layers also include educating employees, implementing best practices, and regularly maintaining equipment. The layers also have different purposes—some intended to prevent or deter incidents; others designed to detect problems and mitigate their impact.

Deep understanding of site vulnerabilities is essential before you can take intelligent action to remove or mitigate associated security risks and establish comprehensive layers of protection.

Vulnerabilities you may uncover include both serious (high-risk) and non-serious (low-risk). Among the higher-risk vulnerabilities are poor or non-existent security policies, poor password management, lack of best practices, and ineffective processes for communicating policies. Problems with anti-virus software on open nodes, where either the software is missing or the definitions are out of date, also may be revealed. Many

of the security products in the market seem more suitable for commercial buildings and don't have the industrial strength expected in the process control environment.

Some assessments also will show use of outdated technology—such as camera systems. Technology that is long past its effective life and clearly beyond its functional capability is still at work in critical places. Another area of concern is the ability to muster and to coordinate with "first responders" effectively in the event of a safety incident.

One of the reasons a layered approach works so well is it addresses almost all vulnerabilities in one way or another and addresses some of the root causes of plant incidents. According to the Abnormal Situation Management Consortium, 42% of abnormal situations or plant upsets are due to people or their work processes. Another 36% of incidents result from equipment problems, of which half are a result of the equipment working beyond its operating standards.

The core layer of protection is the process-control system. Safety comes via a smart design that considers what's required to meet business, safety, and production goals. A secure process control network will extend across the entire plant and related business networks.

This layer illustrates why security is a journey, not a destination. Just consider the new cyber-threats that crop up each day—most are indiscriminant, but all are potentially destructive. In addition, as technology changes, these threats become more frequent and incredibly creative. Consider these threats to be weapons of mass disruption. You must match your security measures to the vulnerabilities these threats create.

Building out from the control network, layers at additional levels of the plant tighten safety and security. Once you've created the appropriate layers of protection, the focus can shift to retaining and sustaining safety and security. With the layers in place, you can substantially reduce threats and increase safety and security. And in today's world, that's one of the most important business investments you can make.

ABOUT THE AUTHOR

Marilyn Guhr (Marilyn.Guhr@honeywell.com) is manager of Global Marketing and Business Development for Cyber Security and Network Services at Honeywell.