

CHEMICAL PROCESSING

LEADERSHIP | EXPERTISE | INNOVATION

Protect Process Control Systems

sponsored by

Honeywell

secure plan(t)




Proactive Protection for your Process Control Systems.

Honeywell offers a systemic approach to help mitigate the risks of the evolving cyber threat landscape. Industrial IT Solutions is a complete portfolio of services and tools that employ best practices in process control and cyber security. Honeywell global experts help users develop a security scheme to preserve key assets and ensure data availability, integrity and confidentiality. Honeywell's Industrial IT solutions deliver a more predictable and secure environment – regardless of control system vendor or location.

Securing a reliable, productive operation.

Honeywell

For more information go to becybersecure.com Or visit our blog at insecurity.honeywellprocess.com

 Also, follow us @inseculture

©2013 Honeywell International, Inc. All right reserved.

TABLE OF CONTENTS

Better Protect Your Control System 4

"Defense in depth" is crucial, and new and maturing technologies may help.

Cyber Security Challenges Continue 8

Countermeasures to protect control systems increase as more vulnerabilities surface.

Case Study: Reduce Cyber Security Risks 12

A vulnerability assessment reveals critical gaps in the security of a natural gas pipeline.

Mitigate Security Risks in Legacy Process Control Systems 14

Several steps can help protect against threats and extend the life of legacy equipment.

Better Protect Your Control System

“Defense in depth” is crucial, and new and maturing technologies may help.

By Jason Urso, Honeywell Process Solutions

CHEMICAL MAKERS are increasingly focusing on protecting their process control systems from intrusion both from the inside and outside. Many manufacturers have made great strides in building this defense; a small percentage of top-tier enlightened control system suppliers and customers are applying best practices.

To get started addressing the security challenge, companies will benefit by implementing a security feedback loop as depicted in Figure 1. The process involves assessing threats to identify vulnerabilities and then providing appropriate counter-measures to minimize risk to assets. Its goal is to build consistency and confidence in how threats are addressed.

The loop represents an ongoing process. Security awareness and defense continue to evolve to meet the ever-changing threats and new vulnerabilities.

Security depends not only on such a process but also on attitude. You must assume the attacker is at least as intelligent and motivated as the defenders. While the weakest points in the system are the most likely targets, small actions and inactions may incrementally improve or compromise security. One of the most significant vulnerabilities is complacency; security demands ongoing vigilance.

TODAY'S TOOLS

Several aspects of security now are relatively robust, including:

Risk assessment. One of the logical first steps in determining the exposure of a control systems environment, it provides a summary of risk areas and actionable recommendations to

either remove or neutralize the risk.

Policies and procedures. Rectifying issues found during the assessment may demand developing or enhancing policies and procedures governing the control system — many requiring that people within the organization have an awareness of security and best practices (i.e., a security mindset).

Segregated process and information technology. Security areas are defined and then segregated using firewall technology, including specialized firewalls for critical process control devices.

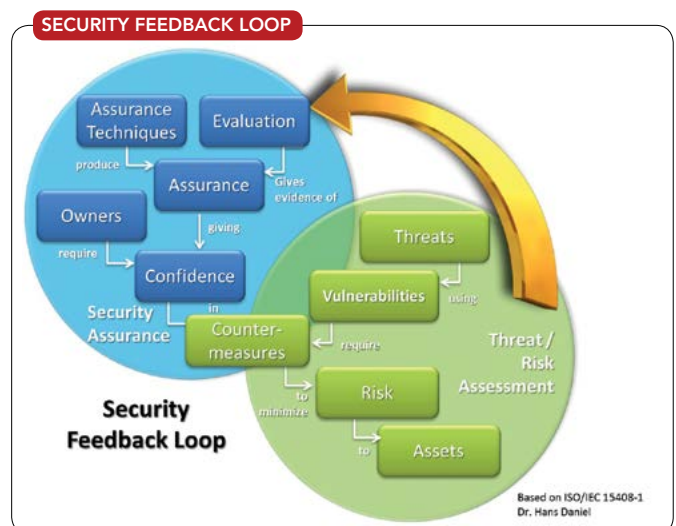


Figure 1. A systematic approach for identifying vulnerabilities and developing counter-measures is crucial.

Locked down/least privileged approach. Interaction of personal computers with the control system defaults to an access level that avoids risks.

Dealing with “Denial of Service” attacks. This involves recognizing vulnerabilities and developing avoidance policies and procedures for squelching such attacks.

Virus protection. Providing an organized approach for verifying anti-virus software and definitions are up-to-date is essential.

Microsoft patches. Procedures must ensure the patch level is maintained and appropriate for the environment.

Backup/recovery. A company must understand its backup/restore requirements and develop procedures that make sure backups occur at appropriate times and are stored for later availability, and that the process for recovery is well-understood and communicated.

Security audit log monitoring. Capturing and reviewing network history can lead to insights about areas needing attention.

The understanding of these aspects varies among control systems personnel today; some have an in-depth program to address risks and vulnerabilities, while others are unaware of the risk and impact of an intrusion. The idea that control systems aren’t vulnerable is eroding because we have recent history, such as the Stuxnet attack, that indicates vulnerabilities do exist (see: “Industry Gets Cyber-Security Reality Check,” www.ChemicalProcessing.com/articles/2011/cyber-security-reality-check.html); the ill intentioned can exploit these vulnerabilities and uninformed internal sources inadvertently can trigger them.

Education of personnel is a key element in establishing an effective security strategy. Realizing that things such as unauthenticated connections between endpoints and cleartext communication can compromise current systems leads us to understand that this vulnerability enables the potential for a man-in-the-middle (MITM) attack, a form of active eavesdropping. Coupled with a lack of accountability

— inadequate authentication and authorization to strongly enforce access — it’s easier to make unauthorized changes to the configuration of systems.

WHERE DO WE GO FROM HERE?

Properly addressing the aspects cited above provides a foundation for effective security. However, as technology advancements are introduced into the control systems environment, the need for vigilance will increase, as will the importance of applying best practices and techniques. Fortunately, new technology and process evolution should help us make a step change in control system security.

Four techniques should play a significant role in improving security over the next five years: 1) whitelisting; 2) encryption; 3) incident detection and response; and 4) remote security operations centers.

Whitelisting. Perhaps you’re familiar with use of the “white list” approach in e-mail management — specifically, for eliminating spam and allowing messages you want to receive. We see it today as a way to prohibit unapproved software/applications from running on the protected system. “Good” software makes its way onto the white list, while unauthorized software is kept from executing. Many enthusiasts believe whitelisting is a good safeguard against “zero day” intrusions (i.e., ones where defenders have no prior awareness of a vulnerability) — preventing some, but not all.

Whitelisting does put in place a capability to enable better change management, protecting against unauthorized alterations to the system configuration — an approach that might have provided some defense against Stuxnet. Some power companies now are implementing whitelisting as part of their critical infrastructure protection programs.

Forward-thinking whitelisting advocates are looking at advancements in the technology as a way to quarantine unauthorized software upon discovery, quarantine

after blocking, enhance whitelist management, and produce a file system inventory that can accelerate verification of software on a hardware platform.

Whitelisting will be available for process control systems. Regardless of the depth of its initial usage, the technology will provide another layer of defense.

Encryption. A key issue today is that almost all communication on a control system is cleartext (a term sometimes used synonymously with plain text). This unencrypted text makes an MITM attack possible — allowing the intruder to “fake out” its victims, passing information as though it were a trusted endpoint, operating in a “trust the sender” scheme.

A solution is to encrypt communication. Encryption is the process of using an algorithm to transform text so “the message” is unreadable to anyone not possessing the encryption key. Encryption has a long history with the military and governments for secret communications. Today, we see it as a common method for protecting information in commercial systems and with wireless communication. One of the questions is where to encrypt the data — at rest or in transmission.

Encryption by itself can safeguard the confidentiality of messages, but protecting the integrity and authenticity of a message requires other techniques.

For process control, we recognize the need to defend against modification from sender and receiver endpoints. Today, with Internet Protocol security (IPsec), we can perform end-to-end authentication, protecting the message without encrypting the data. As an IPsec configuration option, data can be encrypted as well. However, encrypting data can cripple network intrusion detection capabilities. The security strategy for the control system environment must balance the benefits and select the appropriate set of options.

Incident detection and response. An intrusion detection system (IDS) is an application that can include

both hardware appliances and software solutions. The IDS resides on the network and notifies the network administrator of intrusion attempts; it records all alert information according to parameters set by the administrator. Traditional information technology (IT) organizations have used these systems for many years, and we have found them equally useful in the control systems environment.

Some control systems today are integrated with network-based IDSs. However, over time we expect greater pervasiveness of this technology as well as the application of host-based IDSs.

An IDS can inspect network packets as they flow through the system. Today, however, IDSs understand very few control system protocols; we see that changing in the future as more of the protocols are defined and implemented, making IDSs more effective for control systems.

While detecting an intrusion is worthwhile, an even more attractive option is thwarting the intrusion. Intrusion prevention systems (IPSs) are relatively new but have a role to play in the future — by inspecting and validating communications attempting to pass between levels in the hierarchy, for instance, between business and process control networks.

Remote security operations centers. These help ensure optimal performance and administration of a process control network and security infrastructure via a set of remote services.

Many process control organizations today face challenges in addressing areas requiring specialized skills — ones that are more closely aligned with the IT organization. While these capabilities are both valuable and necessary, achieving business results commands higher priority for in-house resources. So, over the coming years, we expect growing use of this type of remote service to keep the process control network running in a secure environment.

SECURITY STRATEGY FOR TOMORROW'S PLANTS

Process plants of the future will be compliant with the IEC 62443 standard for industrial network and system security. This means IT best practices for security increasingly will be applied to process control.

Plants will implement “defense in depth” — realizing a single “Magenot Line” won’t suffice (see: “Protect Your Plant,” www.ChemicalProcessing.com/articles/2008/127.html). They will strive to safeguard control systems from physical, electronic and cyber attacks (Figure 2).

We will see a move toward more individual accountability — achieved through more role-based control and access-enforced endpoints instead of “in the middle” approaches. Today, change points are detected and made on the server. In the future, they will move nearer to where the impact of the change resides, in other words, closer to the controller.

For role-based access control, a way of increasing individual accountability, we will see encryption used as a step in the right direction. We must adopt a security mindset — based on the premise that all trust is limited. One element of that mindset is compartmentalization, to minimize what must be defended and potential loss.

We also must understand that unverified trust decays over time. So, we must re-verify the basis for trust, ensuring the verification testing isn’t predictable. As part of our mindset, we must assume that “the attacker” has compromised some personnel and equipment, yet another reason why a single “Magenot Line” isn’t enough.

As we move forward, we must recognize the management challenges involved in the security process. It requires never-ending effort, and involves more uncertainty than other business processes, with mostly indirect measures of success and potentially catastrophic demonstrations of failure.

Management must foster a culture in which security is every employee’s personal responsibility. As with

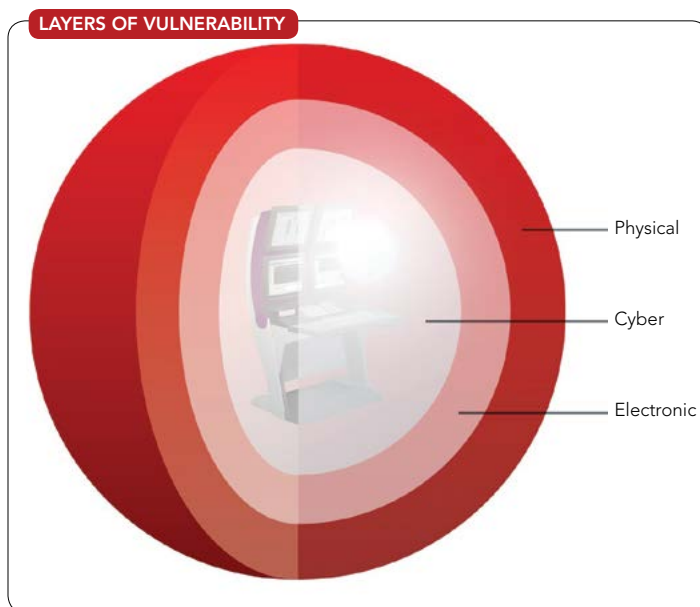


Figure 2. Defense in depth requires addressing vulnerabilities in all three layers.

all continuing processes, people become complacent or develop workarounds without regard to consequences. So, ongoing use of the security feedback loop is crucial.

As we consider the next five years or so, we can see the “plant of the future” will take advantage of additional security technologies, more and more integrated into the control systems, with easy-to-use management and configuration tools. The security mindset will become ingrained in our control systems, just as safety has. Being prepared, informed and optimistic will help ensure continued success. Remember, it’s an evolution — not a revolution. ●

JASON URSO is vice president and chief technology officer for Honeywell Process Solutions, Phoenix, Ariz. E-mail him at BeCyberSecure@honeywell.com

Cyber Security Challenges Continue

Countermeasures to protect control systems increase as more vulnerabilities surface.

By Seán Ottewell, Editor at Large

IN THE decade before Stuxnet attacked process control systems in Iran, there were just five known supervisory control and data acquisition (SCADA) vulnerabilities for all control systems in the world, according to the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In 2011, the year after Stuxnet, that vulnerability count jumped to more than 215. Last year, it reached 248 (Figure 1).

"Thanks to Stuxnet, the bar has been lowered on what the bad guys know and what they do. SCADA and process control was really off the hacker radar before, but now everybody has heard of it," cautions Eric Byres, CTO of Tofino Security, Lantzville, B.C.

And the bad guys come in many different guises. The Shamoon attack, for example, is thought to have been designed by a group of students. "It was a very amateurish code, but it successfully wiped out 30,000 hard drives at Saudi Aramco," he notes (Figure 2).

At the other end of the scale is state-sponsored information gathering, for example by Nitro malware. This attacked 25 manufacturers of chemicals and advanced materials for the purpose of industrial espionage.

"Stuxnet has thrown the hidden underside of process control systems into the open. While companies such as Windows, Linux and Apple have constantly got more sophisticated with their security over the years, this simply isn't the case for process controls. Overall, we have increased the capability and interest of attackers and not done enough for the control systems," adds Byres.

KEY CHALLENGES

Byres believes that the chemical industry has three main cyber-security struggles to overcome.

First is the big difference between the information technology (IT) and the process control worldviews. For example, IT might say "software will be replaced next year when the next upgrade comes — any security problems will be sorted then." However, process controls have a 20–30 year life span. Hundreds of billions of dollars worth of process controllers are sitting out there, most of which weren't designed with security in mind and are very problematic in terms of patching.

A case in point, says Byres, is a plant in Texas that put good Cisco firewalls — the same as used by Tofino — in its distributed control system/programmable logic controller (DCS/PLC) network. The supplier assumed the firewalls would be used in an IT environment and left them with their default settings during installation. Default IT settings assume that incoming traffic is untrusted and, so, should be blocked. "Unfortunately in this case, incoming traffic from the DCS to the PLCs was critical. The firewalls blocked the incoming traffic from the DCS and tripped the plant. The plant went down for three hours." So while the firewall in itself was fine, the worldview was wrong: an unexamined assumption such as "incoming traffic is untrusted" can have devastating consequences on the plant floor.

The second challenge relates to differing priorities. For IT, confidentiality is king. In chemical plant operations, safety and reliability are key. IT will shut a system down if it thinks the system has been hacked. In chemicals, the last thing

CONTROL-SYSTEM-SPECIFIC VULNERABILITIES

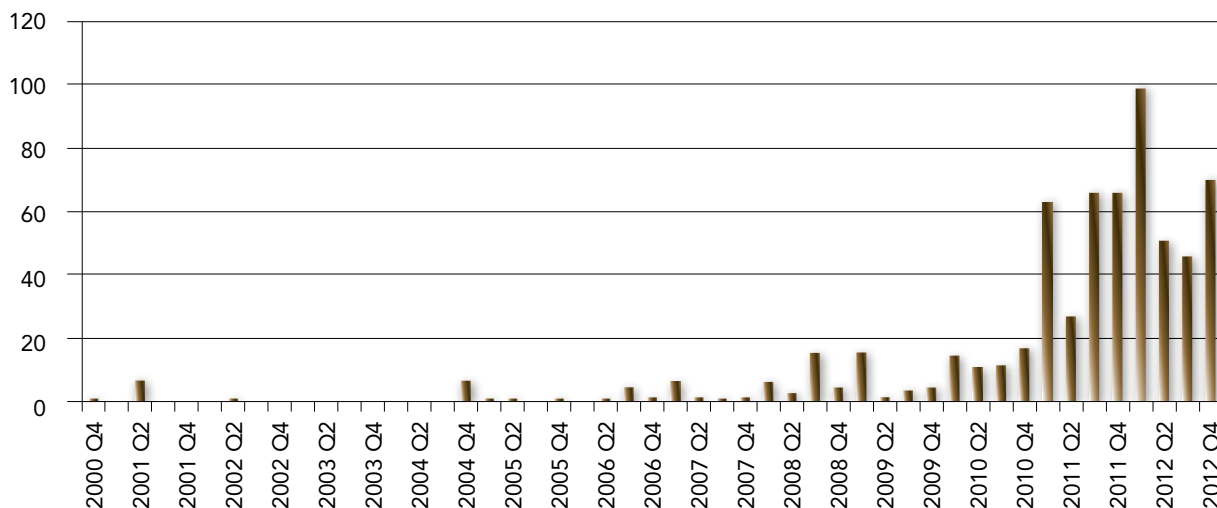


Figure 1. In 2011, ICS-CERT experienced a 753% increase in reported disclosures of vulnerabilities in industrial control system products.
Source: ICS-CERT.

you want to do is shut down the process. Here, Byres cites the example of a client that converts natural gas to fuel oil in a converter. “If for any reason the process stops, the paraffin in the process solidifies. Then you have a serious problem. So you have to approach security issues differently in an industrial process versus an IT process.”

Many major chemical companies — for example, Dow Chemical — are very good at having IT and operations staff work together to make joint decisions, he adds. However, it can be a different story with medium-size companies: “Here it’s like the IT and process control departments are not aware of each other’s existence. And the need for cyber security has made it all worse.”

The third issue is avoiding panic. The scale of the problem is causing some people to look like deer caught in a car’s headlights. Byres knows of smaller chemical companies that have scrapped all plans for cyber security because they have been told it is a \$1-million project. “I think companies have to realize that they don’t need to eat the elephant in the first bite. Just get started.”

A STARTING POINT

Aggressors usually will strive to do the most harm possible — and, for the chemical industry, that means attacking safety and reliability. There are a number of ways to rise to this challenge, according to Byres.

For example, Tofino has worked on a project that involved turbines built by Caterpillar for use by the oil and gas industry in remote locations. The solution chosen here was read-only firewalls. The process can be analyzed remotely but not altered. “You have to be onsite to make such changes. I think that’s a reasonable approach; I think there is good justification for separating remote monitoring from remote programming.”

Another option is to use a rendezvous site to which both the local user and remote control engineer connect. The link ends when the action in question is complete.

For those many chemical plants that shut down only rarely, Tofino — working alongside Honeywell, Invensys and Schneider — has developed drop-in firewalls. Now one of the company’s biggest businesses, these firewalls typically

are used in front of safety systems and clusters of controllers.

Then there's the question of patching versus compensating controls. Often older control equipment can't be patched because the vendor has discontinued it and has stopped offering patches.

Time also is a factor. Every change made to base PLC or DCS code has to go through a detailed validation process before patches can be released. Byres notes that one PLC vendor took four months to issue a patch after vulnerabilities in its products were published on the Internet. In contrast, it only took Tofino ten days to build and validate the necessary compensating controls for these vulnerabilities. This is because the compensating control rules are independent of the PLC software and, so, are a lot easier to create and test. "For firewalls, the same validation process is there, but there is less to test — basically: 'Do the rules block the bad messages and allow the good messages?' That is a lot simpler and quicker," he says.

SECURING THE CYBER PERIMETER

Two main factors account for the success of unauthorized, unqualified people in accessing safety-critical networks within chemical companies, says Andrew Ginter, VP industrial security for Waterfall Security Solutions, Calgary, AB.

First, is the tendency for large chemical companies to centralize engineering functions. "So remote access is used to handle engineering issues and Waterfall is particularly concerned that it is being targeted by hackers. Centralized support might be great for saving money, but it's very bad for security," he notes.

Second, is the perennial problem of the difference between how IT and control systems are managed. "There has always been a significant difference, but people are only now just beginning to realize quite how big this really is."

As an example, Ginter contrasts how standard IT network management works versus how the safety instrumented systems (SISs) for a chemical plant are implemented.

While both have some elements of engineering change control in them, standard IT management has a greater focus on ongoing aggressive change for anti-virus signature and

ATTACK IN SAUDI ARABIA



Figure 2. In 2012, Saudi Aramco was hit by a virus that spread across as many as 30,000 computers at its sites. Source: Saudi Aramco.

patch/security management. IT networks face constant and pervasive threats — every web page and email could be an attack — and threats continually evolve. To an extent, staying ahead of the bad guys requires ongoing change. In contrast, he notes: "The SISs are the devices and controllers whose sole purpose in life is to watch for unsafe conditions and trigger safety shutdowns when those conditions are observed — and their management is inevitably extremely cautious."

In terms of how chemical companies are approaching cyber security, the focus is very much on DCSs and the technologies and processes unique to control systems. Ginter highlights three main ones:

1. *Device firewalls.* These control which equipment can send commands to devices and, sometimes, what commands can be sent. Thus, compromised hosts can't sabotage device operations simply by sending commands — more sophisticated attacks are needed.

2. *Application control* (also known as whitelisting). Rules describe software that is recognized and authorized to run, and forbids any unrecognized software to run. This effectively

blocks conventional malware and even most zero-day attacks (i.e., ones where defenders don't have prior awareness of a vulnerability). The rules may contain file names, file sizes, modification dates and cryptographic checksums. However, as software changes the rules must be updated, too — a process that modern application control systems use sophisticated software packages to manage. "Maintaining this list of approved software is in a sense an expected and welcome part of the process of reviewing and approving changes in a tightly change controlled environment," says Ginter.

Some vendors now are installing whitelisting systems. For example McAfee has partnered with Siemens Industry Automation Division, Hannover, Germany, to develop its Application Control solution against disruptive software, advanced persistent threats and zero-day malware attacks. Honeywell also promotes whitelisting as one of a number of valuable cyber-security techniques (see: "Better Protect Your Control System," www.ChemicalProcessing.com/articles/2012/better-protect-your-control-system/).

3. *Unidirectional security gateways.* Waterfall developed its hardware-enforced unidirectional security gateways in Israel in 2004. They now are widely used by process companies in that country. Currently the company's biggest installed base in North America is in power generation, with the chemicals and refining sectors growing quickly in importance.

While traditional firewalls essentially are software, a unidirectional gateway is hardware. In Waterfall's case, it's made up of two boxes, with a laser in the first and a receiver in the second. A short fiber-optic cable links the two boxes. Standard fiber-optic components include a laser and a photocell in each chip, so that a computer using the chip can both send and receive information. Waterfall's chips have only one or the other. As a result, the transmit gateway only can send information and the receive gateway only can receive information. There's no laser in the receive gateway to send any malware, or remote control attack, or anything at all back over the fiber to the transmit gateway.

While such a solution initially appears to rule out any kind of remote support, actually a number of options exist, with the choice depending upon the needs and sophistication of the user, notes Ginter.

Within the hierarchy of plant control, two kinds of network interfaces are proving equally popular locations for unidirectional security gateways. One is the interface between SIS and DCS networks. "This interface is ideal because, as a rule, you want to monitor the safety systems to determine if they are operating correctly, but you do not want to change them much at all. You do not routinely send commands to safety systems — this is where engineering change control kicks in big-time. Ideally, safety systems do their thing continuously and without depending on any other system or commands for correct operation. You want to protect the safety systems absolutely from tampering from outside networks, but you still want to see that they are working correctly," he explains.

The second is the more traditional interface between plant/operations and corporate networks.

Ginter believes the jury is still out on whether the future of control system cyber security includes routinely applying to DCS systems "host hardening" techniques — such as host firewalls, anti-virus, security updates, per-user passwords and device communications encryption — or on having a network full of soft targets such as control systems that are protected by strong physical security and network perimeter security mechanisms. Applying "constant aggressive change" techniques to systems directly or indirectly involved with the safe operation of chemical plants can pose serious risks, he notes.

"Whatever the answer, chemical control systems protections must always lag IT protections to some extent and, so, the cyber perimeter protections will always be disproportionately important in protecting the soft center of control systems," Ginter concludes. ●

SEÁN OTTEWELL is *Chemical Processing's* editor at large. You can e-mail him at sottewell@putman.net.

Case Study: Reduce Cyber Security Risks

A vulnerability assessment reveals critical gaps in the security of a natural gas pipeline.

AS A result of Honeywell's cyber security vulnerability assessment solution, a natural gas pipeline company was able to empirically identify and quantify all of the steps required to improve the security and reliability of its natural gas distribution pipeline network, and therefore increase the uptime and availability of its system.

The Honeywell cyber security assessment identified all critical gaps within the enterprise. Once gaps were identified, Honeywell helped the customer develop, implement and manage a comprehensive information security program to ensure current compliance with applicable industry regulations and ongoing protection of information and systems.

Thanks to the Honeywell solution, company personnel are now more aware of potential cyber security threats and can take action to ensure gas continues to reach residential and commercial customers throughout the company's service area.

BACKGROUND

The pipeline organization, which was incorporated in the United States in the early 1900s, is one of the largest combination natural gas and electric utilities.

Approximately 20,000 employees carry out the transmission

and delivery of energy. The company provides natural gas and electric service to approximately 15 million people. They operate tens of thousands of miles of natural gas distribution and transportation pipelines.

While large interstate natural gas pipelines may serve major wholesale users such as industrial or power generation customers directly, it is the distribution system that actually delivers natural gas to most retail customers, including residential natural gas users.

A gas utility's central control center continuously monitors flow rates and pressures at various points in its gas distribution system. Sophisticated computer programs are used to evaluate the delivery capacity of the network and to ensure that all customers receive adequate supplies of gas at or above the minimum pressure level required by their gas appliances.

CHALLENGE

Today's natural gas transmission and distribution systems are heavily dependent upon computer technology and supervisory control and data acquisition (SCADA) systems to operate safely and efficiently.

For gas utilities, the challenges involved in ensuring effective cyber security are similar to those faced by bulk electric system and local power distribution providers, except that natural gas systems transport molecules, not electrons, and are equipped with safety devices, which are, in most cases, manually operable as federally required. But all of these groups depend on communications infrastructures, computer technologies, and people to safely and efficiently transport the energy product to the end user.

Designing, operating and maintaining a pipeline facility to meet essential availability, reliability, safety and security needs as well as process control requirements requires the careful evaluation and analysis of all risk factors. Attacks on a cyber system may involve only the cyber components and their operation, but those impacts can extend into the physical, business, human and environmental systems to which they are connected. A cyber event, whether caused by an external adversary, an insider or inadequate policies and



Figure 1. The organization recognized the importance of the cyber security profile of its gas distribution pipelines and equipment.

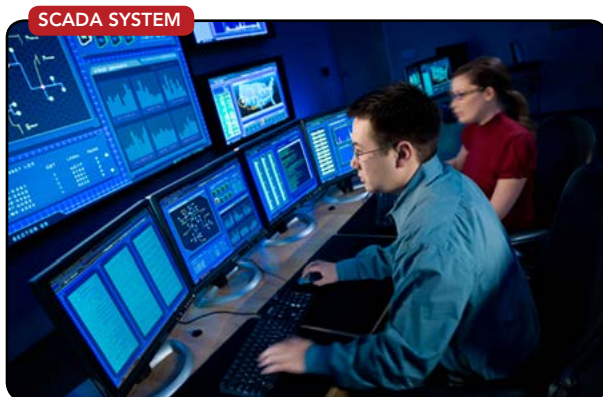


Figure 2. Today's natural gas transmission and distribution systems are heavily dependent upon computer technology and SCADA systems to operate safely and efficiently.

procedures, can initiate a loss of system control, resulting in negative consequences.

The client recognized the importance of the cyber security profile of its gas distribution pipelines and equipment. An operational incident underscored the need to better manage networks and data access. It had become clear that the company required expertise in the niche market of IT security as applied to critical control networks.

SOLUTION

Honeywell Industrial IT Solutions provided quality service and professional results to the client on more than one previous occasion. In this instance, they needed help assessing and remediating the cyber security vulnerabilities of their gas distribution pipelines and equipment.

Honeywell's solutions for oil and gas pipelines promote safety, environmental responsibility, and efficient operations. The company's industrial cyber security expertise has been evolving over the last decade, combining best practices from traditional IT with the needs of a complex process control environment.

The cyber security vulnerability assessment is designed to examine the three core facets of an organization's cyber security:

- **People:** What is the cyber security awareness level in the organization? Are staff members following security

policies and procedures? Have they been adequately trained to implement the security program?

- **Process:** What are the cyber security policies and procedures in place in the organization? Do these policies and procedures meet key requirements?
- **Technology:** What cyber security technologies are in use in the organization? How are these technologies configured and deployed?

The assessment process takes inventory of all cyber assets, how they're connected, and how they're programmed. This includes:

- Servers
- Network switches
- User terminals
- Desktop and laptop PCs
- PLCs and controllers
- Terminal racks
- Wireless transmitters and receivers
- Mobile devices on the network

Through the assessment, Honeywell's team documented the vulnerabilities in all facets of the client's pipeline operation, interpreted and assessed the associated cyber security threats, and provided a roadmap to mitigate risks. This included:

- **Site and system assessment:** Review of particular site- and system-specific vulnerabilities.
- **Policy and procedures assessment:** Review of current policy and procedure documents.
- **Compliance assessment:** Review of operations and processes against applicable compliance standards and best practices.
- **Security baseline:** Gauge progress against current status and operating model for security.
- **Risk assessment:** Identify appropriate levels of security for each asset.

The final analysis included suggestions for improvement by order of importance, a project plan, and order-of-magnitude costs for budgetary purposes.

Going forward, Honeywell will help the client further develop or refine and execute their cyber security program. ●

TO LEARN more about how Honeywell's Industrial IT Solutions can help improve cyber security at your facility, visit www.honeywellprocess.com.

Mitigate Security Risks in Legacy Process Control Systems

Several steps can help protect against threats and extend the life of legacy equipment.

By Mike Baldi, Honeywell Process Solutions

THE TERM “legacy process control system” has different connotations for different people.

To many, it refers to proprietary systems from a past era. To others, the term may imply the new generation distributed control systems (DCS) that have been founded on open technology, or systems using no-longer-supported Microsoft operating systems. These systems have fundamentally different architectures and present different risks.

It’s important to note that proprietary systems weren’t impervious to security risks. The mechanisms of attack were different in those days, generally relying on physical access and inside knowledge in the absence of external network connections. The mechanisms to attack today’s process control systems (PCSs) allow attackers to target assets across vast geographical distances.

Different attack scenarios have been developed and executed over the years. An attacker can sneak through the network, from firewall to firewall, to penetrate into a process control network. Today’s client-side attacks could start anywhere, including:

- Within internal corporate networks
- From communication with external parties
- From a home computer

The discovery of the Stuxnet attack had a significant impact on the process control world. Suddenly everyone became aware that targeted, client-side attacks on PCSs could occur, and that the national critical infrastructure could be attacked.

Security researchers focused on SCADA systems and discovered many new vulnerabilities, placing more pressure on both vendor and owner/operator organizations to secure their process control environments. Internet sites allowed for the scanning of SCADA systems directly connected to the Internet. Some of these systems still used default vendor passwords. While system vendors improved product design processes and security for new products, many legacy systems still exist that have known vulnerabilities in their operating systems, communication protocols, control applications and computer equipment.

The continuous evolution of the DCS enabled organizations to protect the investment in equipment and control strategies over long periods of time. However, interfacing decades-old controllers with current technology also makes this equipment indirectly vulnerable to attack.

All these systems have one common denominator: they experience gaps in support. This makes them more vulnerable than contemporary systems. This gap can be caused by the unavailability of security patches, loss of skills and knowledge and outdated system support documentation. The inability to deploy specific security countermeasures on the older software and equipment also causes such support gaps.

Security isn’t equivalent to making every system component resistant to attack. Security is an approach used to create multiple layers of defense around the production process to protect it. It is architecture, a chain with many links, where the weakest link breaks first.

This weakest link in the chain often is a server or station with an outdated operating system, missing security patches, or a critical application for which software updates are no longer available. Each system component should contribute to overall resilience against attacks, but these components alone aren't sufficient to protect the entire system. They need to be embedded in an architecture with multiple layers of protection. There will always be areas in a system (such as areas that require real-time performance) that need to rely on the protection layers surrounding them for their resilience against attacks. This article will discuss various techniques for protecting legacy systems, the problems surrounding these techniques, and new methods for analyzing security.

DON'T LET YOUR SYSTEM BECOME A LEGACY

Time converts state-of-the-art technology into legacy technology. Time also changes secure systems into vulnerable systems. This is why security must be viewed as a process, not a product. Security is a set of continuously evolving strategies to counter attackers, who are constantly finding new ways to reach the target. To remain secure in the long term takes effort and requires investment. But there are ways to reduce the costs, such as preventing systems from becoming legacy systems. This involves performing periodic system refreshes to maintain a system's serviceability, maintaining security patches to keep the system up-to-date with the latest vulnerability fixes and maintaining documentation so you can know your system and document the assets, network traffic flows and security controls.

Obviously, time can't be stopped, so new developments in the process control environment will impact the security stance of the process control system.

Twenty years ago, control systems were built with proprietary technology with a lifecycle of at least 15 years. In today's open technology world, operating systems undergo major changes at least once every three years, while hardware platforms change even more rapidly. Changes in CPU,

memory and storage technology enforce changes in operating systems to support this new technology. However, this evolution simultaneously creates gaps in the serviceability of the older systems. Legacy operating systems don't provide the system software to support the new technology, and legacy hardware platforms don't provide the performance and technology to support the new operating systems.

A five-year refresh cycle seems to be a reasonable compromise between a reliable and serviceable system with a high availability and the return on investment (ROI) for the new software and equipment. Changing the hardware and operating system will impact the DCS software. Migrating to a higher DCS release supporting the new operating system becomes unavoidable.

How does this affect security? Remaining secure requires the installation of a continuous flow of new security patches, which contain software fixes for vulnerabilities. Vendors of operating systems have a limited support window for security fixes; once the product is no longer sold, the support is generally limited to a three-to-five-year period. After this period, no more security patches will become available, resulting in a rapid degradation of the product's security. Software that protects the PCS, such as anti-virus (AV) and whitelisting applications, also has support limitations pertaining to legacy platforms. Therefore, legacy systems can suffer from the unavailability of security patches as well as the unavailability of security protection software.

Knowing your system is essential when building a secure system. In order to keep your PCS secure, you must have a good overview of its applications, configuration and communications. You need to know which protection layers exist and on which security controls these protection layers depend.

A network drawing showing a firewall doesn't explain how this firewall contributes to the overall protection. Zone and conduit channel diagrams (see Figure 1) are a better method to document the security architecture because they show how assets are grouped in security zones, the sequence of defenses protecting these zones and the interdependencies

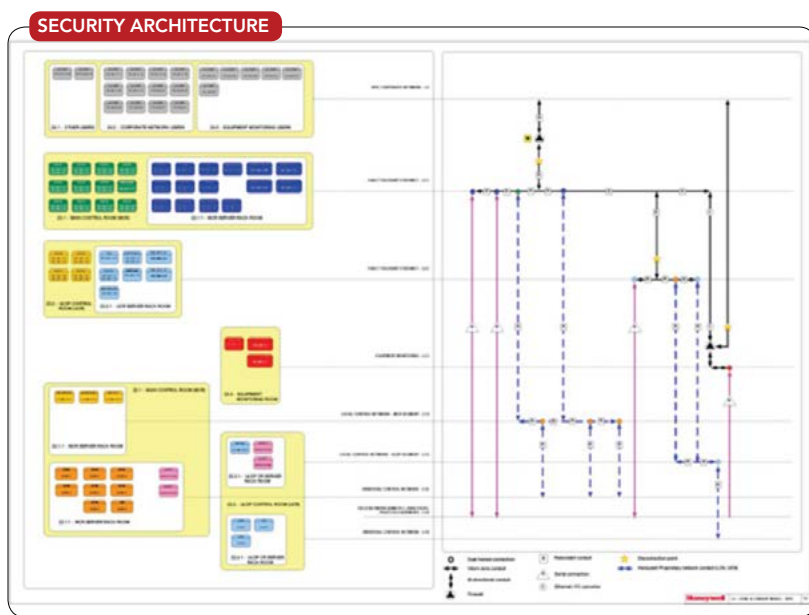


Figure 1. Zone and conduit channel diagrams clearly documents security architecture, showing how assets are grouped in security zones, the sequence of defenses protecting these zones and the interdependencies of defenses.

of defenses. These diagrams show how legacy systems are separated from other system components and how their vulnerabilities are remediated.

Security relies on proper configuration management processes and up-to-date documentation. If you aren't sure which components are in your system, you can't determine whether they are vulnerable. You must know the assets and network traffic flows to design effective security architecture.

DELAYING MEASURES

Can a system's transformation into a legacy system be delayed? Can the

serviceability of a system be extended? Yes, but maintaining accurate documentation is imperative for the serviceability of any system. Apart from out-of-date documentation, other factors contribute to the loss of serviceability, such as the aging of software and hardware, and having a backlog of security patches.

As previously discussed, operating systems must support new hardware, different storage technology, faster CPUs, better graphics and larger memory. Isolating hardware platform changes from their impact on the operating system by using server virtualization

can help delay the aging process. The virtualization software layer separates the new technology of a new server platform from the legacy operating system, allowing the operating system to interact with the new technology as if it was still the old server platform.

Software such as VMware creates a layer between the operating system and hardware. This layer, the hypervisor, simulates the server or station hardware and provides a virtual machine (VM). This virtual layer allows for the application of new hardware and storage technology. The result? A legacy Windows 2000 operating system can exist in a VM running in a brand new server. This extends the lifecycle of a system to at least the software lifecycle—which could be up to eight years. The capability to run multiple VMs on the same hardware platform also provides additional advantages, such as a smaller system footprint and reduced hardware cost.

How does virtualization support security? Virtualization runs legacy software on more capable hardware; it adds security functions between the VM and the hypervisor (Figure 2). Security functions can be implemented as a shield around the VM to do their job without being installed on the legacy software residing in the VM. Organizations can implement AV and virtual patching solutions without leaving a footprint on the VM that runs the legacy software. Additionally, the

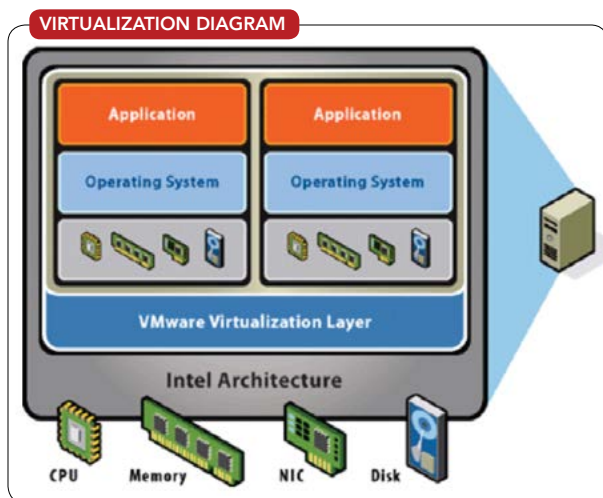


Figure 2. Software such as VMware creates a layer between the operating system and hardware.

way the VM communicates with the hypervisor reduces the attack surface of the virtualized function. Several types of attacks, such as a number of buffer overflow attacks, will fail because of the hypervisor limitations.

Another form of virtualization is application virtualization. This method combines the application and the operating system in one package, making the application less dependent on the server's operating system. Such "sandbox" architecture also reduces security risk and makes the application more tolerant of a changing environment.

But how should organizations address the unavailability of security patches or the inability to install them? There are two security controls that can be used: Application White Listing (AWL) and Virtual Patching (VP). Each method has advantages and disadvantages.

AWL prevents unauthorized executable code from running. Malware can install malicious software on the machine to carry out attacks. When this malicious code is initiated, AWL will stop it, acting during application execution time.

VP security control acts on the network level. This can be either the physical wired network, or it can be within the virtual network of a virtualization solution. VP inspects the traffic and monitors it for the exploitation of a particular vulnerability. It does this with vulnerability filters, which inspect the attack activity rather than monitor a particular bit pattern in the traffic. Vulnerability filters do not use static signatures.

AWL and VP work differently. AWL leaves a footprint on the legacy node. It needs to be installed on this node, so it must be compatible with both the operating system and the application. VP is network resident, so it doesn't leave any system footprints in the legacy node or the network (No IP or MAC address).

For a legacy node that supports AWL, the implementation can offer additional security when security patches are no longer available. For legacy nodes where AWL can't be installed, VP is still an option. Both methods reduce the risk of having legacy nodes in your system and therefore delay your system from becoming vulnerable to attacks.

HOW TO PROTECT LEGACY SYSTEMS

As previously discussed, knowing your system is essential. The security posture of a specific system component is also important to know, but it's not essential for securing this component. As an analogy, a person doesn't need to be bulletproof to be protected from being shot — he could instead wear a bulletproof vest. Similarly, the security architecture as a whole provides the layers of defense to protect the critical assets of the PCS, even if individual components differ in level of vulnerability. The security architecture will surround it and place the most vulnerable components in the internal layers of the architecture.

Security by design is a methodology used to structure such a layered defense. The Honeywell Security by Design process formulates five steps that can help you make the right security design decisions.

Step 1. What are the assets you are trying to protect?

How do systems interact, and what network traffic flows do you need to protect? This question might seem basic, but it is often ignored. For example, the following pose all different security problems that require different solutions:

- Securing a network connected to a camera network. Cameras create network access outside the physical security boundaries of the control room and server rack rooms.
- Securing a wide area network connecting multiple production systems. Connecting multiple systems to a common network create the risk of a security incident (such as a malware infection) impacting connected systems.
- Interfacing a process control network with a wireless network. Wireless networks don't stop at the physical boundaries of a plant like a fence and increase the risk of unauthorized access if not properly protected.
- Interfacing a DCS with a safety system. DCS and safety systems have distinct roles in an industrial control system. A security impact on the DCS shouldn't impact the safety system at the same time.
- Interfacing with terminal servers. Terminal servers connect the process control network to many different support systems.

A security breach in one of these systems can impact the main control system if not properly protected.

Step 2. What are the risks to these assets? Consider the need for security. Are you protecting exclusively against unintentional attacks, or are you including intentional attacks? Answering these questions involves understanding what is being defended.

National critical infrastructure obviously requires more security than a production process manufacturing soap. Considering the consequences of a successful attack, who wants to attack, which methods are available, and why they want to attack are important to determine the level of security required.

Step 3. How well does a particular security solution mitigate a risk? If a security solution doesn't solve an issue,

it's no good. Examples of this include demilitarized zones (DMZ) that don't provide any barriers to access, and network filters that are easily bypassed. These "solutions" create more insecurity than security.

Step 4. What other risks or unintended consequences does the security solution cause? For example, you can implement an AV solution, but then you must also secure the daily update of the signature files. Security solutions often have ripple effects and can cause new security problems. It's important that these new problems are smaller than the older ones.

Step 5. What are the costs and trade-offs of the security solution? Every security system has them. There could be investment required, less user convenience, or an impact on overall system resilience and availability. Installing security patches can also induce labor cost, risk of unavailability, and loss of functionality due software reboots.

These five steps by themselves do not lead to a secure system, but together, the steps provide tools to evaluate and analyze a design. This process may seem obvious when stated in the abstract form, but applying the steps to real situations is hard work.

It requires detailed information about all of the components that make up a PCS. It also requires experience with the techniques used, such as threat, security zone, conduit and channel modeling as well as defining security patterns for the authentication and authorization processes

A well-designed architecture that uses multiple layers of defense can protect legacy systems. Even if vulnerable to many attacks, a successive layer of protection mechanisms reduces risk.

CAN YOU AIR GAP LEGACY SYSTEMS TO PROTECT THEM?

Locking the doors at home and heading for the cellar isn't security — security requires constant vigilance and responding to new threats, rather than hiding from them. Similarly, removing all external access to a process control

system won't protect the control system. It will reduce what's called the attack surface, but only from server-side attacks. Popular client-side attacks aren't stopped by air gaps. The Stuxnet attack was a client-side attack, and it successfully targeted an air-gapped system. Of course, Stuxnet was an exception; this type of targeted attack is difficult to stop without also seriously impacting business processes. Security remains a trade-off between being secure and doing business. However, similar attacks launched since, such as Duqu, had a much bigger impact. This type of attack often propagates over removable media such as USB devices. The most common cause of malware infections in process control systems is the use of an infected USB stick, CD or DVD, or connecting an infected PC to the network.

Exchange of data for various supply chain and reporting processes is a crucial function for the business. Security remains a trade-off between the business benefits offered by the process control system and security counter measures restraining these benefits. Isolating legacy systems as an answer to security threats has a limited effect. Today's biggest threat is the client-side attack, because it has many mechanisms to propagate, including via the isolated network once it has entered into the system.

AWL is probably the most natural protection strategy. AWL allows what is explicitly authorized and blocks everything else by default. It is the opposite of traditional AV programs, which allow everything that is not explicitly blocked. This means AWL can cause false negatives, and AV (blacklisting) can cause false positives. The advantage to using AWL with legacy systems is that it protects the status quo and blocks new unexpected actions, which is exactly the kind of behavior that can occur if malware exploits a particular vulnerability and downloads or drops executable code into the computer. AV would only offer protection against known exploits that have a recognizable signature to detect. This means AWL offers better protection for legacy systems, because they become more vulnerable

for new (zero day) attacks over time due to lack of fixes for newly-disclosed vulnerabilities.

However, AWL has its limitations, both in detecting attacks as well as applying the technology to legacy systems. AWL has difficulty intercepting attacks that are fully memory resident and attacks that are exploiting interpreted code, such as used for mobile code (JavaScript, Pearl) and web-based applications. Another limitation of AWL in relation to legacy systems is that the software needs to be installed in the system. This software might not be tested for compliance with the legacy system and could also overload system performance. Therefore, AWL always leaves a distinct footprint in the system and can't always be used. An alternative is VP.

VP is relatively new technology. VP is fully network-based, which has no impact on the legacy system. It's an appliance in the network with input and output ports. It's called a "bump in the wire." Honeywell's VP solution has no IP or MAC address, making it fully transparent to the network. It protects the system using vulnerability filters, which monitor the network activity and intercept the traffic if a particular known vulnerability is exploited. It doesn't use a static bit pattern signature as filter, but instead uses an activity filter evaluating every protocol step.

VP is inline with the network and works as an Intrusion Prevention System (IPS). The manufacturer of the Honeywell solution creates a filter as soon as a new vulnerability is discovered by their research institute or disclosed by others. Because one vulnerability is often exploited in various ways, a vulnerability filter can stop many exploits, including those that are brand new. VP is so valuable when protecting legacy systems because it doesn't require any software to be installed on the legacy system and doesn't impact performance. (The added network latency is less than one millisecond and therefore negligible.)

The limitations of VP are that the technology is restricted to the network. It will stop attacks over the network, but it can't stop attacks using removable media (e.g. USB drives) or file sharing as propagation methods. A combination of VP with AV is the most logical solution for remediating this security gap.

SECURITY STRATEGIES

Method	Characteristics
Application White Listing (AWL)	<ul style="list-style-type: none"> • AWL protects the legacy system if new security patches are no longer available. • AWL protects against unauthorized execution of executables at node level. • AWL requires that both the software platform (compatibility) and the hardware platform (performance) support the solution. • AWL protects against malware infections originating from removable media and file sharing. • AWL can be used for a particular node or at system level.
Virtual Patching (VP)	<ul style="list-style-type: none"> • VP protects the legacy system if new security patches are no longer available. • VP leaves no footprint on the network or on the legacy node, so it can always be applied. • VP intercepts attacks on network level using vulnerability filters. Vulnerability filters monitor the network activity and block illegal activity. • VP would typically be used to protect multiple nodes. • VP is a "bump in the wire."
Virtualization in combination with VP	<ul style="list-style-type: none"> • When used in combination with virtual machines, VP can protect one or multiple virtual machines. • Runs in its own VM and communicates with the VP device on the network. • Can be combined with VP "on the wire."
Creating an air gap	<ul style="list-style-type: none"> • Air gaps would protect against all server-side attacks. • Air gaps impact the business functioning, isolating the process control system. It eliminates the possibility for real-time integration of various business functions. • Air gaps offer no protection against client-side attacks. • Air gapped systems still require anti-virus, which would require an update mechanism to stay effective.

Table 1. There are many different situations and variables to consider when selecting an optimal mitigation strategy.

HOW TO CHOOSE THE RIGHT SECURITY CONTROL

Choosing the right security control depends on various characteristics of your particular legacy system. Is it a single node? Is it a system comprised of multiple nodes? Is the problem the operating system? Can you replace the hardware? Is the application the bottleneck? Is it a "ghost" system without documentation? There are many different situations and variables to consider when selecting an optimal mitigation strategy (see Table 1).

A single node can be best protected by installing AWL, but if for some reason AWL is not an option (due to an unsupported or slow hardware platform), then using VP is an alternative security strategy because its characteristics

of being fully network resident matches the requirement better. Multiple nodes can be protected by both AWL and VP in combination with AV. Using only AWL or only VP wouldn't provide sufficient protection. AV is supplemental for both solutions.

VP also can be used in combination with virtualization, where a specific VM protects the communication in the virtual server environment and the wired environment. In this way, VP can protect one or multiple VMs.

The diagram (Figure 3) shows the various protection solutions and where they are active. In principle, these solutions should be supplemented with each other, as each technology has its weak and strong points. AWL

struggles with attacks that fully remain in memory and replace authorized code, as well as attacks based upon interpreted software code. AV also struggles with memory-based attacks and is vulnerable to changing malware signatures.

Both AV and AWL do not protect against a denial of service (DDoS) attack. With VP, protection is limited to network traffic. Legacy systems will not always support all protection options. Therefore, methods often should be combined.

PROTECT AGAINST THREATS

Legacy systems form a weak link in the security chain. If a legacy system gets compromised, chances are that the other parts of the system are impacted. When protecting legacy systems, consider:

- Replacement or upgrade. The logical choice is to remove the vulnerable system. However, this requires budget and might not be opportune because of the impact on the continuity of the production process.
- Hardening. Every system should be hardened, including legacy systems.
- Apply the “least privilege” principle. Various legacy systems have limited, role-based access control functionality, providing users with more authority than

PROTECTION SOLUTIONS

	Allow Known Good (Block All Else)	Block Known Bad (Allow All Else)	Unknown
Execution Level	Application Control — Applications White Listing —	Resource Shielding	Behavioral Containment
Application Level	Application and System Hardening	Antivirus — Black Listing —	Application Inspection
Network Level	Host Firewall	Attack-Facing Network Inspection — Virtual Patching —	Vulnerability-Facing Network Inspection

Figure 3: This diagram shows the various protection solutions and where they are active.

needed. Try to restrict authorizations as much as possible.

- Apply strong passwords. Legacy systems often allow the use of weak passwords. Sometimes, even default passwords are used. Correct this. If available, use domain authentication rather than workgroups.
- Apply one of the discussed methods (AWL, VP) to compensate for the absence of security fixes.
- Consider virtualization to extend the lifecycle of a system.
- Apply a defense-in-depth security defense. Use the security by design methodology to evaluate the various design decisions.
- Make certain that there are

sufficient spare parts available.

- Make certain you have a backup that can be restored.
- Maintain the skill level. Often plants are confronted with legacy systems when one employee changes jobs or retires and the skills to support the system are lost.
- Maintain the system documentation.

If you can apply the above recommendations, it's a good start for protecting your systems against threats and extending the lifecycle of legacy equipment. ●

MIKE BALDI is chief cyber security architect for Honeywell Process Solutions. He can be reached at mike.baldi@honeywell.com.