# Improving Cybersecurity Defenses In Oil And Gas Applications

By **Scott Howard** and **Tim Wallaert,**
**Belden Tofino Security**

In recent years, there have been a number of high-profile, advanced malware threats that targeted or attacked the energy sector such as Dragonfly, Stuxnet, Flame and Shamoon. And while these threats need to be taken into account when analyzing and preparing for potential security risks, they actually only account for a low number of overall threat sources.

Industry research shows that internal — not external — sources make up more than 60% of all cybersecurity threats.

Oil and gas networks, in particular, can be more susceptible to internal incidents because many devices on the network run 24 hours a day, seven days a week, and often lack the security updates and antivirus tools needed to protect against vulnerabilities. In addition, "wide open" network layouts and a lack of isolation between subsystems make it easy for problems to spread quickly throughout the network.

| Threat Source | Percentage of Industrial Network Incidents | Incident Type | Location of Source |
|---|---|---|---|
| Hackers and terrorists | 9.4 percent | Intentional | External |
| Malware | 30.4 percent | Unintentional | |
| Insiders | 10.6 percent | Intentional | Internal |
| Human error | 11.2 percent | Unintentional | |
| Device and software failure | 38.4 percent | Unintentional | |

Most cybersecurity threats and incidents are unintentional and occur inside industrial networks.
***Source:*** *The Repository of Industrial Security Incidents, 2011.*

A firewall protecting the edge of a network can defend applications against many external cybersecurity threats or attacks. However, with more threats originating from inside the network — whether via a USB keys, maintenance systems or visitor laptops — additional security measures need to be taken in order to harden control networks.

To protect oil and gas operations, engineers and network designers must identify new cybersecurity measures.

## Solutions Industrial Networks

Information technology professionals have been successfully dealing with cybersecurity threats for years. However, IT teams are concerned mostly with privacy and protecting data, while industrial control systems (ICS) security measures focus on the concern for safety and protecting overall operations. With a focus on privacy and data protection, the solutions applied by IT don't work for industrial control networks.

Here are a few additional reasons IT solutions won't work for oil and gas operations:

- Critical, industrial networks can't be shut down for testing, configuration and maintenance, as is done with business networks. Instead, industrial security products must be set up and maintained while the network is running.
- Industrial networks use unique communication protocols not seen in the IT world and not addressed by IT security products.
- Patching or updating programmable logic controllers (PLCs) is usually not practical.
- Control devices cannot be secured with automated third-party tools.
- Oil and gas applications require hardened equipment that can survive harsh electrical and environmental conditions.
- Industrial networking equipment needs to work for decades, whereas IT gear has a life cycle measured in years.

Finally, engineering staffs need cybersecurity solutions that are simple to use. While they are experts in making products or programming PLCs, they are likely not cybersecurity experts. Thus, industrial security solutions need to be easy to use in order to minimize human error in set-up and ongoing use.

## Layered Security Approach

The best approach is to implement a defense in depth strategy in which multiple layers of security are in place and working together to harden the network and prevent incidents.

A key best practice is to implement the zone and conduits model as defined in the ISA IEC 62443 standard. This model provides a framework for network segmentation that prevents cybersecurity incidents from spreading.

"Zones" are logical or physical assets that share common security requirements. The zones then communicate exclusively through secure "conduits." A conduit is any pathway of communication that enters or exits a security zone.

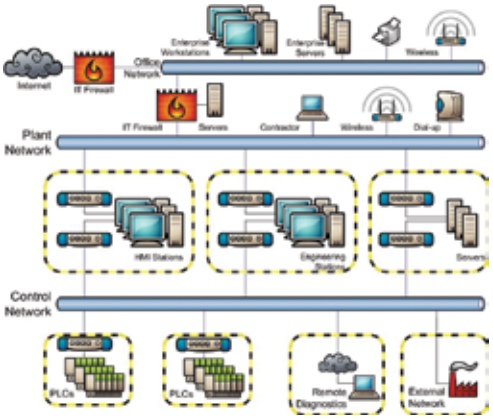



**Figure 1:** Implementing zones and conduits enable a layered approach to network security.

To apply a zones and conduits concept, first, you need to define the security zones. In the network diagram (Figure 1), there are groups of PCs that act as human machine interface (HMI) stations, engineering workstations and servers — each of these fall into their own security zones. In addition, the two groups of PLCs and two remote network

connections make ideal security zones.

The next task is to locate the conduits of communication in the network. Conduits are the perfect place for implementing security measures such as industrial firewalls to ensure that only the necessary traffic is allowed to pass. These security measures compensate for the fact that the devices they protect have insufficient built-in security measures. This approach is cost-effective because it doesn't require upgrades to every device or computer in a zone to meet security requirements.

## Cybersecurity For Pipelines

The primary goal of a cybersecurity strategy is to improve safety, reduce network downtime and improve overall productivity.

When issues arise it can be costly. Here's a real-world example of how cybersecurity incidents can inadvertently happen. The controls for an existing oil pipeline were being made. In this situation, it's an industry best practice to always test and verify in the engineering lab before deploying new code into the field. This time, however, the software was accidentally uploaded to a PLC on the plant network instead of the test network. The oil pipeline was shut down for nearly six hours. Fortunately, no spills or accidents occurred, but the downtime alone cost the company well over $250,000.

To really understand how to improve defenses, here's a look at how the zone and conduit model can be used to protect pipeline infrastructure.

A pipeline system includes the pipeline itself, pump stations and connections to one or more wide area networks (WANs). There are usually several points in the system where custody transfer of the resource occurs with the resource being measured by flow meters. In this case, there are two approaches for defending against cyberattacks.

The first approach is to focus on securing only the critical assets. For example, in the pump station network (Figure 2), the zone that protects critical assets, including PLCs, sensors, pumps and actuators, is the priority zone within the network. Other zones that may group together physical security elements, such as cameras and alarms, are a secondary concern when the main goal is to keep the network up and running and the pipeline operational.

The second approach is to take into account that flow meters connect to two networks for custody transfer — the seller's PLC and the buyers' PLC — the latter being an untrusted network. In this situation, the best solution is to insert the flow meter into a demilitarized zone (DMZ) and separate all zones with a multiport firewall. A DMZ is a zone created to allow dual access to a shared resource, but with no direct access — this protects the networks of the buyer and seller.

## Establishing Defense Methods

The best method for securing oil and gas applications against cybersecurity threats is to establish multiple layers of defense that not only work together to prevent network incidents, but also work to contain them, should an incident occur.

Relying on single-layer defensive solutions exposes a network to a single point of failure. Abiding by a defense in depth approach, in conjunction with a comprehensive risk assessment and the ISA IEC 62443 zone and conduit guidelines, will

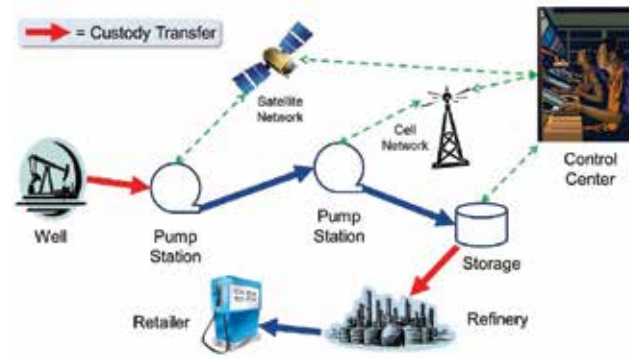



**Figure 2:** A simplified diagram of a pipeline system showing custody transfer points.

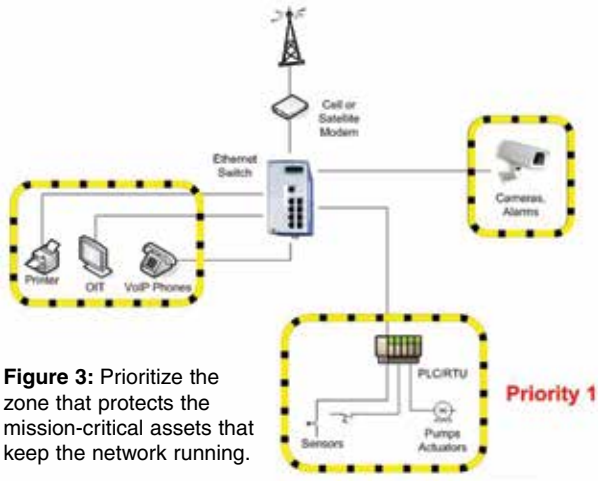



**Figure 3:** Prioritize the zone that protects the mission-critical assets that keep the network running.

help build strong defenses throughout a pipeline's network.

Ultimately, industrial cybersecurity doesn't have to be hard. With the right approach and defenses, oil and gas operations will be able to protect their networks and establish robust cybersecurity solutions.

For more information, view this presentation with tips and advice about improving cybersecurity defenses in oil and gas operations: http://info.belden.com/cyber-security-oil-gas-bc-lp. ***P&GJ***

***Authors: Scott Howard*** *is a commercial engineer for Belden Tofino Security, which he joined in 2007. He has nearly 30 years of experience in embedded system development and has worked with organizations worldwide to help them improve the reliability of control systems through enhanced cybersecurity.*

***Tim Wallaert*** *is director of Oil & Gas Solutions for Belden, where he leads the company's expansion into oil and gas, as well as power utility markets. He has spent more than 20 years in industrial automation, helping improve production operation across a range of industries.*

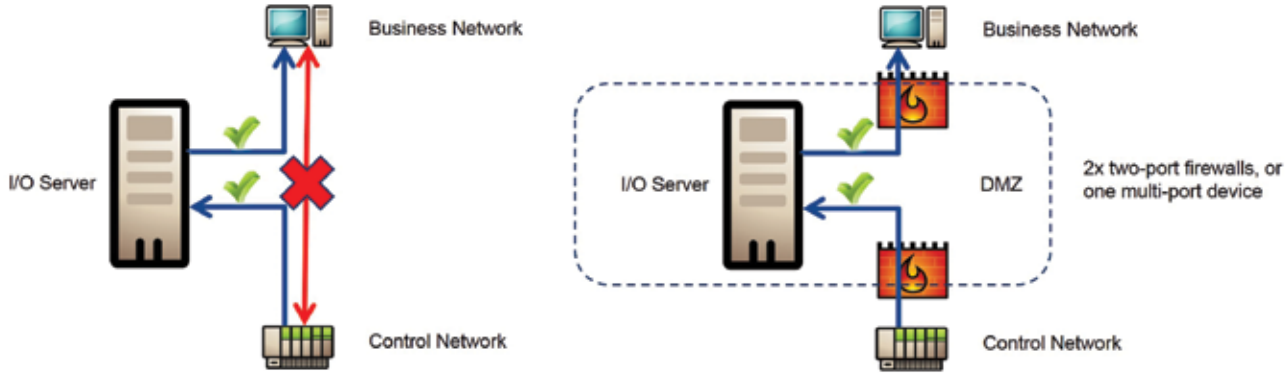



**Figure 4:** A demilitarized zone, right, allows dual access to a shared resource, without enabling direct access for additional network protection.

# Achieving Vital Security With Cloud Services

By **Steven Bjarnason, Certified Information Systems Security Professional (CISSP)**

Are your company's business systems connected in any way to the industrial control systems (ICS), including Supervisory Control and Data Acquisition (SCADA), which are used to manage the company's critical infrastructure? If they are, and the best guess is they are, then the ICS/SCADA could be vulnerable to cyberattacks in addition to the business side of the networks.

In 2013, the Department of Homeland Security (DHS) ICS Cyber Emergency Response Team (CERT) responded to 256 reported industry incidents and 59% of these were in the energy sector, including the pipeline and gas industry. The disturbing fact on this was not only that the number of actual incidents was probably much higher but that 120 of the reported incidents were of an "undetermined/ unknown" nature.

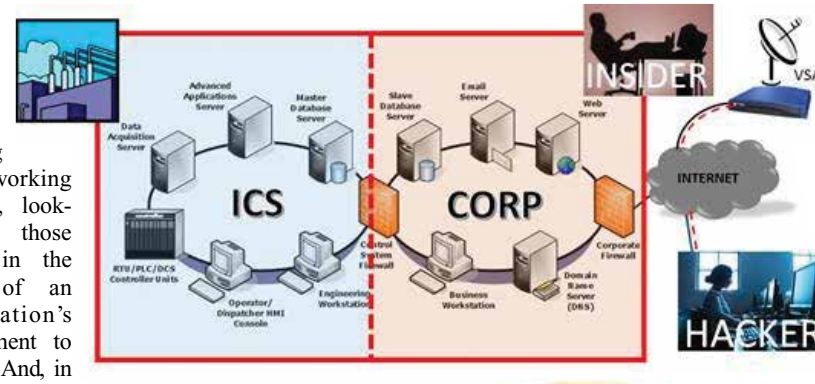
"Why?" you ask. An expert opinion, in the absence of investigation results, would say this was probably due to improper configuration of security and monitoring systems, the failure of these systems, the absence of these measures in place in the system's architecture, or the lack of proper training to manage these systems.

Imagine the ecologically damaging incidents. Now, imagine this incident on a massive and distributed scale as the result of malicious cyber-attackers taking control of oil and gas pipeline ICS/SCADA systems. Take this one step further and imagine your company is the target.

Unfortunately, this scenario is well within the realm of possibility and attempts have been made to carry out such harm in recent years. In fact, there have been a number of systems, identified as national critical infrastructure, that have experienced malfunctions that were likely cyberattacks that caused outages, loss of control, and physical damage.

Fortunately, the attacks to date have been far from severely impacting the long-term economic stability of any country involved; that remains to be seen.

Have we been lulled into a false sense of assuredness by the relative calm though? Do not be fooled; there is a cyberwar looming on the horizon and evidence abounds to indicate that nation-state actors and activists are actively practicing for such attacks. And, in 9/11 style, these cyber-rattackers are planning and working patiently, looking for those chinks in the armor of an organization's commitment to security. And, in these uncertain times, where major hacking attacks and terrorist activities seem to happen just about every few weeks, it is in everyone's interest to know the threats, targets, and risks involved in every aspect of our lives; especially those related to our occupation, local environment, travel, and nation as a whole.





In today's technology-driven society, the threats abound but the single most important element involved in avoiding cyberattacks are the people responsible for the maintenance and use of computer assets, networks, applications, and databases. The experts categorize the biggest threat today as the "Advanced Persistent Threat," or APT. These APT are a set of constant computer attack methods, often coordinated by humans, pursuing a particular target and operating stealthily over an extended period of time.

The people and organizations behind the APT are intent on gaining access to systems are motivated by various reasons to include financial gain (or harm) and political influence. There are many ways in which the actors behind the APT gain control or indirect access (and eventually direct access), but it usually involves an element of social engineering wherein people like you and me are deceived into providing the attackers a way into the network, either through explicitly revealing the information or simply clicking on an email or website link that is disguised to appear trustworthy.

However, the actors behind the APT also rely on the knowledge of internal system vulnerabilities. The attackers have already done their reconnaissance and intelligence gathering, so they know your systems have one or more specific vulnerabilities; all they need is an unintentional invitation to enter the corporate network and allow automated software to do the rest.

In countering the myriad of threats, the advent of cloud services has brought about a shift in the way corporations, and especially industry, are managing their information systems technology and security services and the budgets behind these. Utilizing a Cloud Service Provider (CSP) certainly has monetary advantages in economies of scale, but there is also the high level of security enjoyed by having access to tested and proven environments with layered security, guaranteed high availability, and data center geo-dispersal, that include such aspects as:

- Compliance monitoring;
- Finely grained policy control of system administrator and user access;
- 24/7 security monitoring and network

operations centers (NOC);
- Robust patch management;
- Next-generation firewalls and intrusion prevention;
- Secure multi-tenant database architecture, storage, and backups;
- Encrypted virtual machines (VM);
- Advanced virtualization techniques that include Virtual Desktop Infrastructure (VDI)
- Immediate replication and rebuild (self-healing) to secure baselines; and
- Third-party certified data centers.

The use of cloud services can help organizations achieve vital security through dedicated teams and facilities that continuously keep abreast of the latest technologies and capabilities and are certified to be experts in their field while serving a number of clients as a shared and scalable resource. The ability to implement this as an on-premises solution is something that companies grapple with all the time when tightening their budgetary belts.

The first thing to go is usually the training dollars and then the planned upgrades being scrapped shortly thereafter. In the ever-evolving world of information technology (IT), it is in the best interest of companies to maintain the best-of-breed in the critical components and training that ensure technical security measures are adequately implemented for the management of (i) configurations, (ii) public key infrastructure (PKI), (iii) security information and events, (iv) IP address space, (v) identities and access, (vi) service desk support, (vii) updates and patching, and (viii) policy; to name a few.

Obtaining and implementing the best security measures your company can afford, whether on premise or through a CSP, can only take you so far. A sense of continuous awareness of threats and vulnerabilities is half the battle in any area of risk management, and cybersecurity is no different. To assess your personal risks and vulnerabilities, there is a series of questions you should ask yourself on a regular basis, that include:
- "What am I doing on a daily basis to protect my company's information?"
- "Do I know what the corporate policy is concerning my responsibilities?"
- "Have I been adequately trained to recognize things like social engineering attempts?"
- "To whom should I report suspicious activities?"
- "What are my actions when I become aware of potentially malicious activity?"
- "How do I best protect company assets?"

A commitment to policy is the key element to remaining vigilant in protecting your company and its information from malicious attackers. This commitment to policy must be a top-down activity. A true commitment to policy is demonstrated through:
- Planning for and providing resources and scheduling that support adequate levels of system security controls, maintenance of controls, continuous monitoring activities, updating/ revising of documentation, and the ongoing training and exercises related to policies and related security controls;
- Holding company personnel accountable for non-compliance with corporate information security policy in accordance with the company's HR policies related to performance management and adverse actions; and
- Supporting the implementation of information security policy through personal example throughout the organization.

It is important to know that a company's security can be taken down even when it possesses the greatest achievable security currently possible through detection, prevention, and monitoring systems when it does not have a commitment to policy.

Other threats that you and your company need to consider are:
- Terrorists/hacktivists — are individuals with intent to cause great harm, most-




*Pipeline & Gas Journal* / February 2015 www.pgjonline.com 50

ly ideologically motivated. The recent attack on a French satirical magazine is a perfect example where, even though the attackers did not use high technology, they were capable of achieving their goal of stopping specific people they saw as their enemy from being involved in an enterprise they objected to.

- Malicious insiders — are disgruntled individuals that actively work for, or have worked for, an organization and use their knowledge and level of access to perpetrate attacks to cause damage, deny services, steal information, or embarrass or destroy the reputation of individuals or organizations. The recent attack on Sony Entertainment, according to a large number of cybersecurity industry experts, may have been made possible by current or previous insiders that provided the real attackers (Guardians for Peace (GOP)) the ability to gain covert access to much of the Sony Entertainment's information systems, including personal emails. In this case, the purported reason for the attack was a movie that certain entities found objectionable. The results have been that the target organization lost a great deal of revenue and people had to apologize for statements they made about the president of the United States.
- Industrial espionage agents — are individuals working for, or on behalf of, another company, a government, or individuals with the intent to steal proprietary information and/or gain access to information systems through surreptitious means. These might be people visiting your facility for a conference, business meeting, or tour or they might be folks who are terminating employment with your company and taking thumb drives chockfull of company information with them to their new employer. In May 2014, the federal government accused the Chinese military of infiltrating a number of American companies and stealing trade secrets. This was accomplished by gaining access to emails and computer systems.
- Users losing or misusing mobile assets — this is either unintentional or purposefully. In any case, the effect can be disastrous. In one of the most epic breaches of personal information, an employee of the Veterans Affairs lost a laptop with the unencrypted private and personal information on 26.5 million people.

You might be thinking that you cannot be fooled; that you are computer-savvy and have done this for far too long not to recognize you are being "hacked." Yet, like a junk mail campaign through the postal system, the APT are able, over time, to craft some very convincing emails, called "phishing," that can make their way past the most sophisticated "spam filters" and appear to be from someone, or some entity, that you feel you know and trust.

The best ways to counter the attackers, that are intent on trying to beat their way into your business and ICS/SCADA systems, is to remain vigilant through adherence to policy, report when policy is not adequate, and, for the company, to balance the risk with the cost in continuing to operate an on premise IT vs. through a CSP. ***P&GJ***

***Author: Steven Bjarnason*** *is manager of Security and Compliance at DYONYX, LP, a Houston-based Internet security and computer network and systems integrator. He has spent the past 24 months assisting cloud service providers (CSP) in achieving federal cloud compliance. He served 22 years in the U.S. Navy, specializing in communications, computers and security.*

# How Network Segmentation Improves Operational Security For Pipelines

By **Kenneth Tom, Wurldtech**

Network segmentation is a fundamental component of cybersecurity, yet it is so difficult to implement in a gas and pipeline environment. There is flawed thinking in part due to an industry-wide focus on perimeter security, a carryover from the days of air gap protection.

As industrial systems continue to evolve and pipelines become more distributed, there are more requirements for greater connectivity between internal systems within the distributed environment. As a result, more traffic must be allowed through the perimeter, and if perimeter access isn't denied outright, it isn't really a gap. A more flexible approach is required.

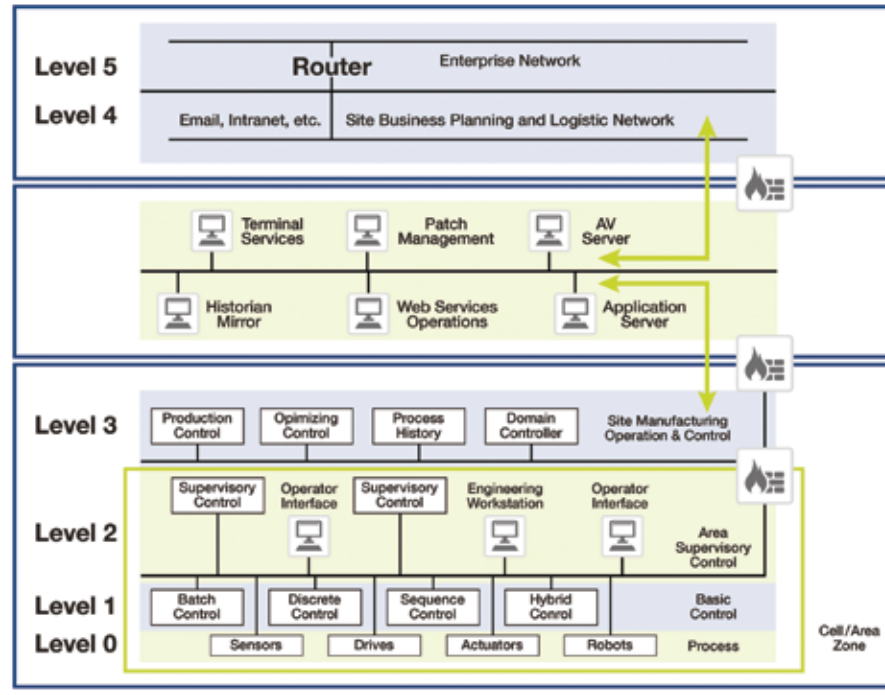
The flaw is that the term "perimeter" implies one big shell around an entire system, within which there are many devices in many zones, with different security levels and conduits, all unmanaged. In other words, the traditional definition of perimeter security does not mean the same level of granular access controls that a properly enforced conduit provides.

Perimeter security is able to properly secure zones, if the proper requirements are applied. Every zone has a logical perimeter that defines it. If all information flows are forced to cross this boundary via appropriate cybersecurity measures, then each conduit is made more secure. In order to secure a system with many zones:

- Many perimeters need to be created.
- Appropriate security controls must be in place around each perimeter, to inspect flows.
- These controls must map different policies to different information flows to properly protect each flow and conduit.

Using these criteria, it becomes obvious that, while there are many ways to segment zones and enforce perimeter security, they are not always feasible or adequate.

For example, traditional segmentation mechanisms using VLANs or routing would either prohibit the amount of zone separation (by using too few devices), or become unduly complex (requiring massive network redesign to accommodate VLANs and IP subnetting). Too simple, and the right security is not implemented in the right places; too complex, and the risk of misconfiguration can result in less effective security and unintentional vulnerability. The complexity of highly sub-networked or VLAN-separated systems also requires administrative overhead from operations teams already strapped for IT skills and resources.




There should be multiple perimeters within a given network to provide the specific protections needed for each segment.

And finally, ICS vendors may dictate specific designs of layer-2 and layer-3 configurations, making the implementation of new network segmentation contractually impossible. In other words, traditional segmentation is not feasible for deep segmentation of pipeline infrastructure.

Routing can enforce the security of information flows, as can VLANs. However, this security is not absolute, and these paths remain susceptible to attack. Generally, the higher up on the OSI stack, the more difficult the attack. VLAN 'hopping' is a relatively simple task that renders VLANs inherently insecure. Routers are more difficult to circumvent and application layer controls are hardest to overcome. Therefore, while VLAN and network segmentation can be effective, it is not entirely adequate for industrial systems.

The necessity for a secure segmentation of the network is the crux of the issue. Zones and conduits exist to restrict access to and between systems in an effort to improve the security and reliability of the overall systems. If the information flow is not secure, the zone is moot. If the logical perimeter does not adequately control access to its devices, the system remains vulnerable.

To deploy an enterprise-class IT security device in a pipeline environment to separate two discrete control zones would be to pound a square peg into a round hole. It would also

be difficult to justify. The device would be costly, cumbersome and may in many cases disrupt industrial communications due to latency and performance characteristics that are not tuned for sensitive industrial networks. Typically, there is undue complexity to help products differentiate themselves in the highly competitive enterprise security market.

The answer is not to develop entirely new tools, but to make existing cyber security tools more relevant. To do so, we must first look at the tools that are available and then determine how to make them more appropriate to industrial control systems.

The basic requirement is simple: limit the network traffic allowed into and out of any given zone. This task is easily accomplished with a firewall, using bi-directional traffic filters to prune out unwanted traffic on unwanted ports. It is a good idea and a necessary one as industry mandates require the use of a firewall or similar technology for this purpose. Because firewalls filter IP traffic, they can also filter industrial control traffic running atop IP.

While a firewall will narrow the scope of legitimate traffic to what is authorized, even legitimate traffic needs to be inspected more closely. Network-based exploits, denial of service attacks and insider attacks from disgruntled employees all utilize legitimate traffic in illegitimate ways. Deep packet inspection helps by looking into packets for an indication of malicious intent.

Content filtering (a feature in next-generation firewalls) looks at the application contents rather than simply matching packet contents to determine if an application is being misused (e.g. preventing access to a specific URL instead of blocking all web traffic).

However, content filters are intended for web content and email, not industrial applications. Therefore, most application-layer firewalls lack the ability to make decisions upon the specialized application-layer protocols used within industrial systems. Although industrial protocols ride atop TCP/IP, they establish their own application sessions, enact their own controls, and carry their own payloads.

To become relevant, the firewall must be able to understand these industrial applications, track application-layer sessions, and make decisions accordingly. To become highly relevant, the firewall should allow unwanted or unnecessary features to be disabled by default, so that they are more easily deployed and maintained in an environment staffed by operations managers and not IT managers.

With these modifications a firewall device can effectively protect the pipeline infrastructure and secure zones. Using relevant cybersecurity mechanisms, the complex network access policies that are required can finally be enforced. Through extensive filtering (using next generation firewalls that understand the nature of ICS application-layer protocols), the control network can be essentially "whitelisted."

Filtering the contents of industrial protocols provides highly granular control, capable of defining acceptable protocols, authorized devices and authorized tasks. If the firewall can act transparently (i.e., without altering or impacting IP communications), then it becomes feasible to enable zone-level separation without reconfiguring the network.

Such a firewall is much more practical for OT managers and staff because it will not interfere with approved control system designs. Therefore, zoning can finally be well defined and implemented by pipeline operators.

This necessary first step toward a mature cybersecurity profile — the separation of systems into functional groups — will do more for security, reliability and safety than almost any available security measure. Properly established zones and conduits will make unauthorized access to (and exploitation of) critical devices more difficult.

They will help to isolate functional systems to minimize the impact of an incident. Perhaps most importantly, they will create a strong architecture foundation upon which more sophisticated security controls can be built. ***P&GJ***

***Author: Kenneth Tom*** *joined Wurldtech, which produces the Achilles Industrial Next Gen Firewall, in September 2013 as a senior product manager, with product management and product marketing responsibilities. Prior to joining Wurldtech, he led the product marketing efforts at Juniper Networks for the SRX Series Services Gateway product line, and product marketing and product management efforts at companies including McAfee, Check Point Software Technologies and 3Com.*