

Fact Or Fiction

Cyber Security for Industrial Control Systems

In the post-9/11 era, protecting Europe's critical infrastructure is paramount to ensuring public safety. The potential for industrial plants to release toxins during a serious accident, or if intentionally caused, could have catastrophic consequences for industry, environment, government and the public. An intentionally malicious control system attack could potentially put workers and the surrounding environment at risk, as well as having serious business impact and causing long-term damage to a company's reputation and position in world economics.

The situation is serious enough that the European Union (EU) published in 2005 a green paper entitled, "A European Programme for Critical Infrastructure Protection" (EPCIP). While drawing attention to the cyber threats faced by Europe's industrial plants, the paper also called for increased security measures and raised the possibility of introducing legislation to standardise security.

With cyber threats showing no sign of abating, an increasing number of chemical manufacturers are looking to increase their protection through adoption of robust security and safety measures against these threats.

What Are The Threats?

The Process Control Network (PCN) is a communications network used to transmit instructions and data between control and measurement units and Supervisory Control and Data Acquisition (SCADA) equipment. As such, the PCN is the most critical area of a chemical facility: No production means no business. This greatly increases its vulnerability to the growing number of cyber threats. With many modern plants having fully integrated systems monitoring production, safety, ERP and access functions, a virus or worm could wreak havoc throughout the facility.

In the past, process control systems, with their reliance on proprietary networks and hardware, were once considered immune to the network attacks that have plagued corporate IT systems. Business performance has pushed vendors to open standards such as Ethernet, TCP/IP transmission protocols and web technology and has created new routes for hackers to take advantage of the process industry's ignorance.

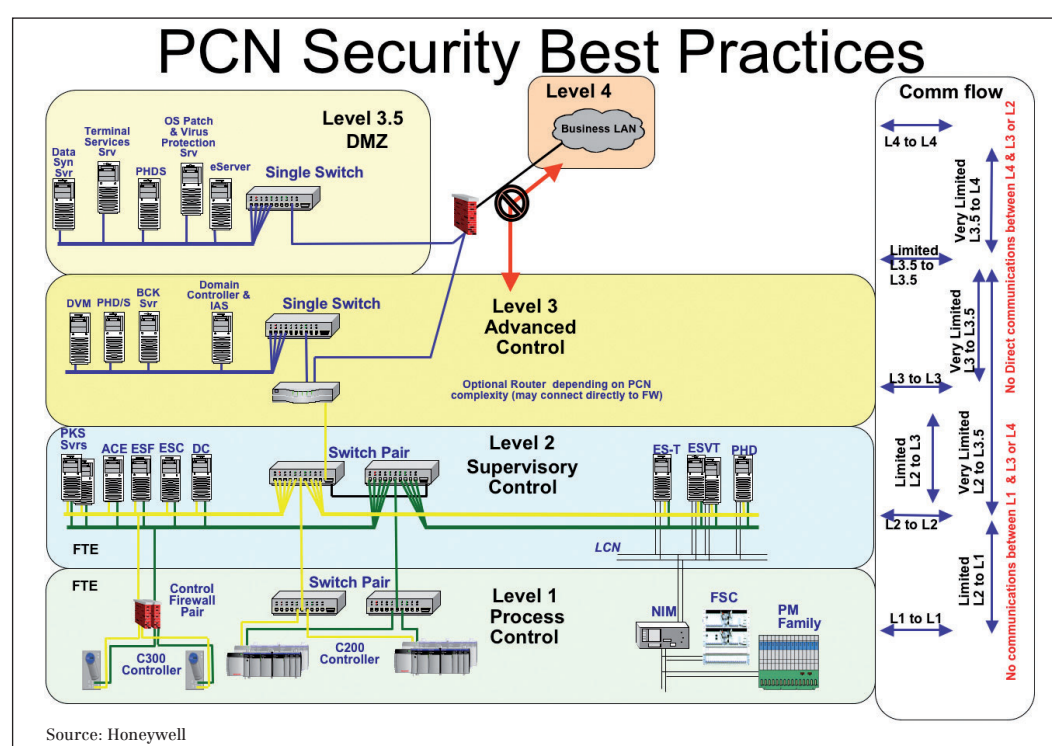
The Industrial Security Incident Database (ISID), maintained by the British Columbia Institute of Technology (BCIT), tracks network cyber incidents that directly impact industrial operations. The ISID monitors and validates through a rigorous process both malicious and accidental incidents and it reveals that cyber attacks have increased significantly since 2001. This rise has primarily been driven by the changing nature of malicious programs (malware) such as worms, Trojans and viruses, the widespread adoption of Ethernet and SCADA systems in industrial facilities and the increased interconnection of process systems. In addition, in the post-9/11 age, SCADA has suddenly entered the hackers awareness as a cool way to cause trouble.

In spring 2006, the ISID recorded 119 incidents across 22 contributor companies, of

which the majority of the external threats (68%) were due to malicious code such as viruses, Trojans and worms, while the remainder were denial of service (DoS) attacks (attempts by hackers to disrupt legitimate network traffic) and sabotage.

Were hackers successful in penetrating a chemical facility's PCN, the impact could be wide ranging, from reduced network performance or a breach in confidentiality to physical damage and danger to human life. In any case, the costs to the organisation would be significant.

Interestingly, the stereotype of the hacker as a geeky teenager trying to break into systems for the challenge is a misconception. Today's hackers are in it for financial gain – sensitive information is worth a lot of money to organised crime syndicates. An ever-increasing concern is that hackers are now designing



proprietary system. Considering the rise in highly targeted cyber attacks and the increase in vendors adopting Ethernet

security, including desktop and business computing systems, manufacturing and control systems and the value chain systems which interact with customers and suppliers. However, it is critical to set clear boundaries between business and control systems in order to facilitate secure data transfer. Creating a cross-functional security team can help ensure its smooth implementation.

A vital element of this approach is to create a demilitarised zone (DMZ). Taking its name from the buffer area separating two hostile countries, the DMZ sits between the business network and the process control network, meaning that nothing can pass directly from one to the other. By separating process control from the larger enterprise system, the risk of a cyber threat reaching the PCN is greatly reduced.

Companies should also adopt a "defence in depth" strategy to ensure that cyber security is built into all levels of the system. Although perimeter security is vital, it is not enough by itself. If a virus or worm gets through, there must be strategies and steps in place to deal with it. Having a multi-layered design can be extremely effective as it places security blocks at each level.

Good security will only be achieved through vigilance, so it is vital that security measures are kept current and regular assessments, tests and reviews are conducted. To make this happen, a formal corporate security policy for control systems should be enacted and a cross-functional

security team created. When developing a policy for securing the plant floor it is vital to identify which IT policies will not translate well to this environment.

Although implementing an integrated cyber security system will offer a greatly increased level of security, it is worth noting that no system can ever be 100% foolproof. Disaster recovery strategies, tools and procedures combined with a security response team can ensure that incidents and events are properly monitored and responded to quickly.

The Cyber Security Lifecycle

Unfortunately, there is no quick fix solution to cyber security: It is more of a continuous journey or a lifecycle. By approaching cyber security as a way to manage threats instead of a way to eliminate them, organisations will achieve a much greater level of success. The cyber security lifecycle is comprised of four stages: assess, design, implement and manage.

Assess – Organisations should have a detailed evaluation of all its potential weak spots. All factors from human interaction to customer and supply chain contact must be considered. For instance, if an employee takes a laptop home he or she may connect to the internet or install files, resulting in a threat once the machine is brought back onto the corporate network. This initial assessment should include a statement of goals and responsibilities and be designed to protect the integrity of data, whilst eliminating unauthorised access.

Design – Identify the hardware and software components required to implement the design. In this stage various options must be considered vis-à-vis their impact on other areas of the organisation. How well will they connect? Could they cause problems for other areas of the plant?

Implement – Implementing the security design needs to be done in collaboration with plant personnel to ensure a fully functional process control security infrastructure.

Manage – Organisations must take a 24/7 approach to managing the network and its security mechanisms. They must learn from attacks and adapt their approach. Security should become part of the way the organisation does business, in the same way that health and safety concerns permeate most industrial functions.

Advantages of an Integrated System

There are a number of advantages to integrating a cyber security system with other physical security and process systems. Firstly, by integrating security within the system architecture, access restrictions are established at each individual level, while still supporting the business requirements for shared information.

Secondly, with such a system, an unauthorised person in the plant would be automatically flagged and the system could shut down or isolate all terminals or computers in that area, in order to prevent access to sensitive applications and systems. In short, an integrated solution can be automated to make pre-emptive, predictable security decisions across the business.

Lastly, an integrated approach may also be much more cost effective. In a typical plant where there might be different suppliers and systems for video; fencing; visitor management; access control; network access; and asset tracking, staff become the integrators and need to manage each

solution separately. This can have a negative impact given the increased costs and resources associated with separate solutions.

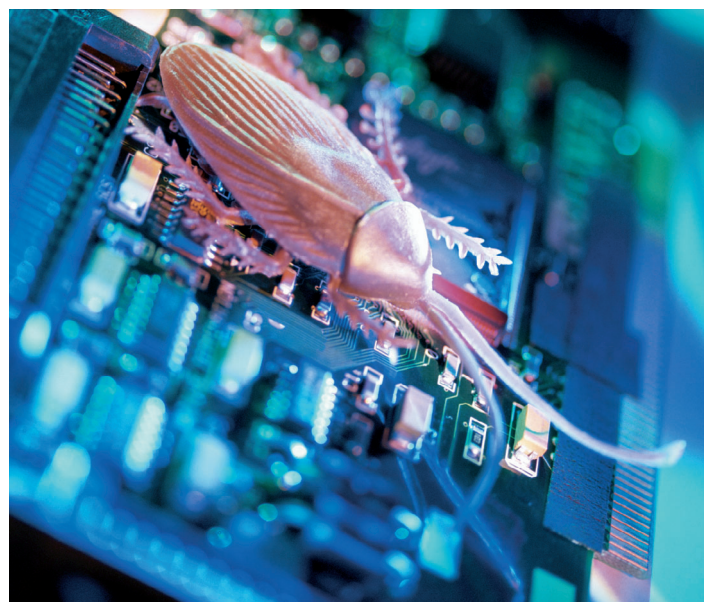
The Way Forward

There is increasing evidence that demonstrates the threat from cyber crime continues to grow and become more targeted, while attacks from viruses, worms and Trojans are relentless. It is no longer acceptable for companies to take the risk of an attack lightly, as the consequences can be far reaching.

To protect its information, people and physical assets, chemical companies must evaluate their vulnerabilities, design and implement a system to counter them, and continuously re-evaluate and fine tune their approach to security. Most importantly, this process needs to be ongoing, with security permeating every relevant part of the organisation's processes.

Contact:

David Boyle
Honeywell
Brussels, Belgium
Tel.: +32 2 728 25 71
Fax: +32 2 728 22 45
david.boyle@honeywell.com
www.honeywell.com



worms and viruses to attack specific applications and organisations. With such highly targeted malware, it has been documented that criminals can obtain sensitive information or attempt DoS extortion.

Never underestimate the inventiveness and creativity of the criminal mind.

How Real Are the Threats?

Recently, the U.S. Department of Homeland Security warned of possible attacks on control and data systems at power plants and chemical companies. In fact, there have already been some close calls. In January 2003, the Slammer worm penetrated a computer network at Ohio's Davis-Besse nuclear power plant, disabling a safety monitoring system for five hours, and in 2000, a cyber attack was launched on a SCADA-run waste treatment plant in Australia, causing a diversion of millions of gallons of raw sewage into local parks and rivers. The list of known but unpublicised events is far more extensive than generally understood.

The financial impact of cyber attacks should also not be underestimated. Interestingly, accidental infections introduced by employees are far more costly than external attacks perpetrated by hackers. In fact, ISID found that with incidents where the impact was less than US-\$100,000, malware was responsible 68% of the time, but where the impact was greater than US-\$100,000 accidental incidents were responsible 79% of the time. Deliberate sabotage was a new factor introduced in recent analyses and can cause even greater losses due to their targeted nature.

"Security by obscurity" is a common misconception regarding process control systems. This is the belief that the PCN is not vulnerable because the platform is based on a pro-

technologies to supply network connectivity this concept is entirely misplaced.

Surprisingly, some organisations claim that their systems are not at risk because their PCN does not connect directly to the internet. However, there are numerous ways for malware to reach a process control system. For instance, access could be gained through the corporate wide area network (WAN), business network, telecommunications system or third-party virtual private network (VPN). Even the humble floppy remains a risk. Since business networks are generally secured to support business processes and not critical process systems, the PCN is left vulnerable. The bottom line is that there are many ways into a complex process control system, and if a hacker is determined, they will find a way to penetrate a network.

Best Practices

Much can be learned from the petrochemical industry, which is meticulous about implementing different protection methods for data and process networks. Security measures that are appropriate for simple data networks could be disastrous if they compromised a key process in a volatile environment. This means that the security infrastructure needs to be carefully thought out and although many security practices can be "borrowed" from corporate IT, their suitability for process control must be thoroughly considered first.

Special attention should be paid to Ethernet and internet technology as their origins do not lie in process control networks. With appropriate planning these systems can be made extremely secure, but it is necessary to properly plan the network architecture around process control requirements.

For a security programme to be truly effective, it should integrate all aspects of cyber

IT'S
NICE TO REMEMBER ALL THE THINGS
YOU CAN NOW
FORGET.

Compliance-Management

The next set of rules and regulations is just around the corner. In fact, it's often closer than you think. The penalties are considerable for companies that don't know all the regulations or even violate one, but compliance solutions from Technidata stop it getting to that stage. Our business compliance services for environment, health and safety ensure that your company remains on track. In full compliance with all regulations in force. And with your success in focus. www.technidata-bcs.de

TECHNIDATA BCS
Business Compliance Services