



# Suite attacks cyber-terrorism

## THE PROCESS CONTROL NETWORK (PCN)

Security Services suite from Honeywell Process Solutions, Phoenix, Ariz., enables chemical companies to respond to the growing threat of cyber-terrorism, while effectively exchanging information between business and control systems without compromising those systems or leaving them vulnerable to cyber-attacks. It provides an organized approach to the assessment, design, implementation and management of a PCN, identifying security vulnerabilities and recommending steps to remove or mitigate them.

The chemical industry clearly is a major potential target for terrorists. Underscoring that, in 2003, it became the first business sector that the Bush Administration sought to regulate to lessen the danger of terrorism. After all, many sites deal with materials that, if released, and processes that, if disrupted, could have severe consequences in neighboring communities.

Yet, today, many chemical companies find it a business necessity to share PCN data with external systems and to

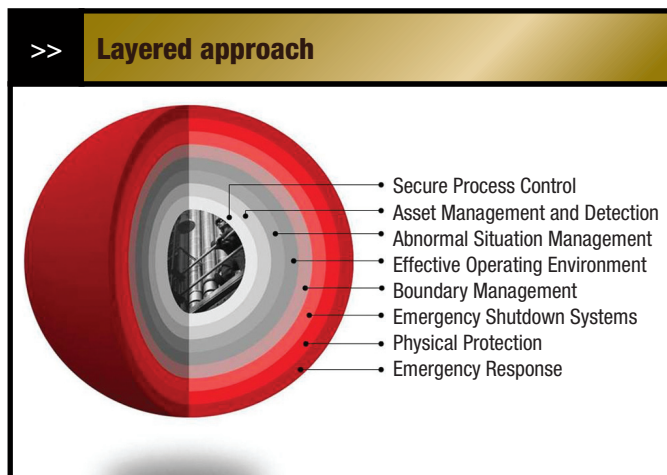


Figure 3. Cybersecurity for process control is at the core of an integrated approach to plant safety and security.

access PCNs externally. Add to this the increasing use of open hardware and software systems in PCNs and it is clear that vulnerabilities to cyber-attack are growing significantly. At stake is the preservation of confidentiality, integrity of data, and availability.

The Honeywell PCN Security Services suite takes a holistic approach to resolving PCN concerns and issues, putting the PCN at the core of efforts (Figure 3):

Its Assessment Service typically includes a review of the current PCN design and configuration, communication requirements and security processes, as well as an automated vulnerability scanning. This provides a baseline and leads to a set of recommendations.

The Design Service provides a detailed design of the security infrastructure connecting a PCN to a company's Plant Information Network. Deliverables include a list of all hardware and software needed, as well as descriptions of how to configure and use the security infrastructure.

The Security Implementation Service sends Honeywell engineers on-site to carry out the work. Operating company staff also may participate. The result is a fully functional PCN security infrastructure (Figure 4) that can be run by the operating company or handled remotely by Honeywell Security Management Services.

Security Management Services, based in Phoenix, can provide oversight, 24/7, over a wide range, from firewalls to operating-system patches to automated PCN vulnerability scanning.

The PCN Security Services suite complements other Honeywell offerings that have built-in cyber-security measures. And many customers are extending the suite to address aspects of physical security, such as visitor control, as well.

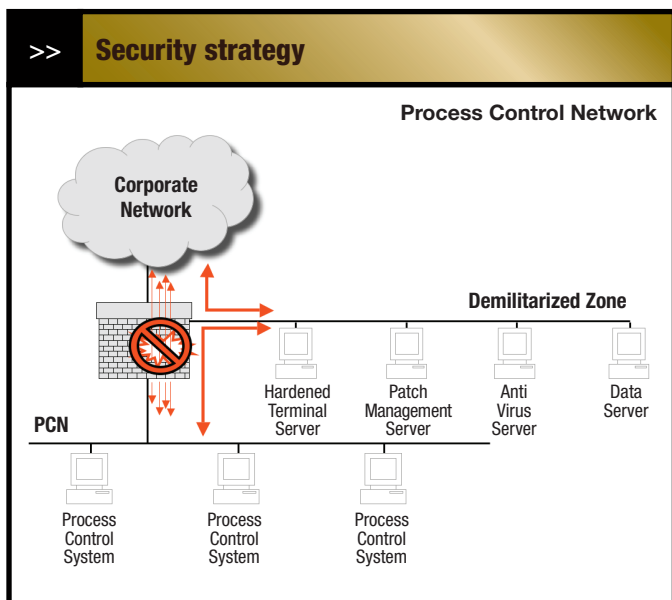


Figure 4. Having traffic go through a server on the "demilitarized zone" protects both the enterprise and process control networks.