

Balancing security needs

Marilyn Guhr and Kevin Staggs,
Honeywell Process Solutions, USA,
describe how to secure a facility at
the control system level.

A few hard facts make cyber security a key issue in today's hydrocarbon engineering environment:

- If platforms aren't running, neither is your business.
- Without a comprehensive secure solution, there is a high risk of being stopped in your tracks.
- Without a security strategy, even recovering in a timely fashion may prove difficult.

Security is no longer a choice. It is essential, and must be integral to the underlying control system. Today's contemporary control systems are based on open system platforms, use standard networks, and are connected to external systems and the enterprise network. Even systems that are not (i.e. air-gap) require security measures to prevent them from becoming infected by viruses or worms.

There are many security measures that one can apply to these systems. However, security is always a balance of the value of the assets being protected, the cost of the security measures protecting the assets, and the inconvenience imposed by the security measures.

How does one begin developing an appropriate strategy? The most practical advice is to assess the current situation to determine the vulnerabilities at the site; then evaluate risks if left unchecked, and determine how to neutralise every vulnerability. It is rather like understanding vulnerabilities in physical security, with one major difference: the vulnerabilities are not as easy to spot.

Assessing the current situation will therefore involve understanding security objectives; evaluating current practices against established 'best practices' and using some kind of tool to detect vulnerabilities. In some situations, the process control vendor can help with this assessment, and a well documented set of findings should be expected after such an assessment. One should also expect to receive an overall security rating for the system, with clear explanations about each rating.

Separating the PCN

One way to enhance security is through a design that separates the process control network (PCN) from the enterprise network. Here are some definitions:

- The PCN is the protected asset. Considered a real time, mission critical asset, it is key to the success of the

corporation. It may also contain data and information that is extremely valuable in making business decisions. The contents of the PCN vary widely from industry to industry, and even company to company. For the purposes of this discussion, the PCN systems are therefore Ethernet connected, run on open operating systems and communicate via the TCP/IP protocol.

- The enterprise network is anything outside the PCN, including the local site network, corporate WAN network, and possibly engineers working at remote locations through the internet. From the current perspective, the enterprise network is viewed as the unsafe entity from which the PCN is protected. However, many measures to be implemented would help to protect the enterprise network from the PCN.
- The demilitarised zone (DMZ) is a critical piece of the PCN security puzzle as it can be used as a buffer/proxy zone for communication between the PCN and the enterprise network. The servers/systems on the DMZ should be hardened and continually updated with the latest

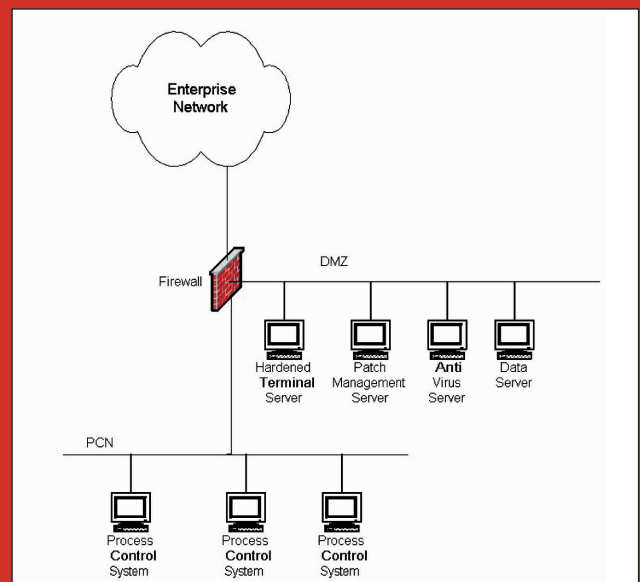


Figure 1. Generic and simplified representation of an interface between a PCN and an enterprise network.

security patches and antivirus files. Communication to and from these systems needs to be restricted by a firewall to the greatest extent possible. Servers on this segment address several of the issues in today's environment.

In an ideal environment, the enterprise network and the PCN will not communicate directly. All communication will take place through the hardened DMZ servers (Figure 1). Although this process is not always possible, it should be the goal.

The following examines some of the PCN connectivity issues that companies usually experience.

How does one get data, information and/or graphics from the PCN to help people and systems on the enterprise network make business decisions?

A data historian server or data Web server usually provides this information. These servers collect data from on process control systems, and make the information available to users on the enterprise network. There is nothing new about these data servers, so why put them on the DMZ? Communication to a data server should be restricted as much as possible. This guideline is applicable whether the server is collecting/receiving data from a PCN system or providing data to an end user or system on the enterprise network. By locating the data server on the DMZ, full firewall controls can be applied on all communications to and from the data server, whether the communication is with the enterprise network or the PCN.

How does one allow engineers who are not physically on the PCN to access the systems that are on the PCN?

Engineers may need access for a number of reasons, including tuning, troubleshooting, maintenance or screen design. There are definite issues with an engineer accessing PCN systems directly from an enterprise network.

One consideration is that a PCN system may not be running the latest operating system security patches or antivirus files. This situation is not necessarily because the site is behind in patching the systems. It could be because the patches and/or antivirus files have not been tested, certified and blessed by the process engineer and/or process control vendor. In such cases, the PCN systems are vulnerable to worms and viruses. Therefore, it is necessary to ensure the remote engineer's PC is hardened, patched and is up to date from an antivirus perspective.

Unfortunately, tracking and controlling all the engineers' desktops, laptops and home systems is not always possible or practical. For this situation, the terminal server on the DMZ provides a reasonable solution. If all remote engineering access to the system on the PCN comes through a terminal server on the DMZ, then the only system communicating directly with the PCN systems is a single terminal server. This makes it very easy to ensure this single system is hardened, patched and equipped with the latest antivirus defenses.

How are authentication, authorisation and accounting handled?

The terminal server approach for remote engineering access to the PCN addresses another issue: authentication, authorisation and accounting. The terminal server will force the engineer to authenticate him or herself by providing a username and password. Additional security can be provided by requiring two factor authentication. This approach is much more secure than simply allowing an IP address through a firewall, as access is based on 'who' someone is rather than 'what IP address' he or she has. Once logged

into the terminal server, the terminal server can control the specific systems on the PCN to which the engineer has authorisation to connect. In addition, the terminal server can keep an accounting record of which engineers were connected to which PCN systems and at what time.

How does one keep current and consistent?

Another potential issue is updating patches and antiviruses on the PCN. If this function is performed directly from the enterprise network, the goal to avoid direct communication between the PCN and enterprise network has failed. It is therefore recommend that a 'patch manager server' function and 'antivirus server' function are located on the DMZ. It is likely that these reside on a single server platform. Dedicating PCN Patch Management and Antivirus Management allows for controlled and secure updates that can be tailored to the unique needs of the process control environment. This approach also helps address the issues that arise when the antivirus product supported by the process control vendor is not the same as the antivirus product supported by the corporate IT department.

Choosing a secure process control system

Security measures should not be viewed in a vacuum. It is always necessary to consider the importance of:

- Intrusion detection.
- Security policy.
- Physical security.
- Security education.
- Security incident response.
- Contingency.
- Disaster recovery.

Some of the security needs and issues unique to the process control environment have been highlighted, with, perhaps, a few ideas for solutions

Finally, if a new process control system purchase decision is in your future, consider the 'must have' attributes of the new system from a security perspective. Ask these questions:

- Does the vendor offer a secure system that is delivered in a 'locked down' configuration, resulting in lower initial security configuration costs at installation?
- How rapid is the vendor's response and testing of security hotfixes and patches?
- What antivirus software is qualified? Is there a choice?
- Are 'best practices' documented and available to you?
- Does the network offer high availability and deterministic configuration with qualified switches and routers?
- Is there a network configuration tool provided with the base system?
- Is 'lockdown' configurable, and what guidance and/or templates are offered?
- Are cyber security services available and mature?
- Does the vendor offer cyber security design and implementation services?
- Does the vendor offer network management services?
- Is physical security integrated into the control system, and does it provide operator alarming and awareness?
- Does the vendor offer integrated digital video for control system and plant surveillance?

If the answer to any of these questions is 'no', then consider the potential risk exposure. With the answers in hand, it is possible to make an informed decision that will protect the security of operations. ■