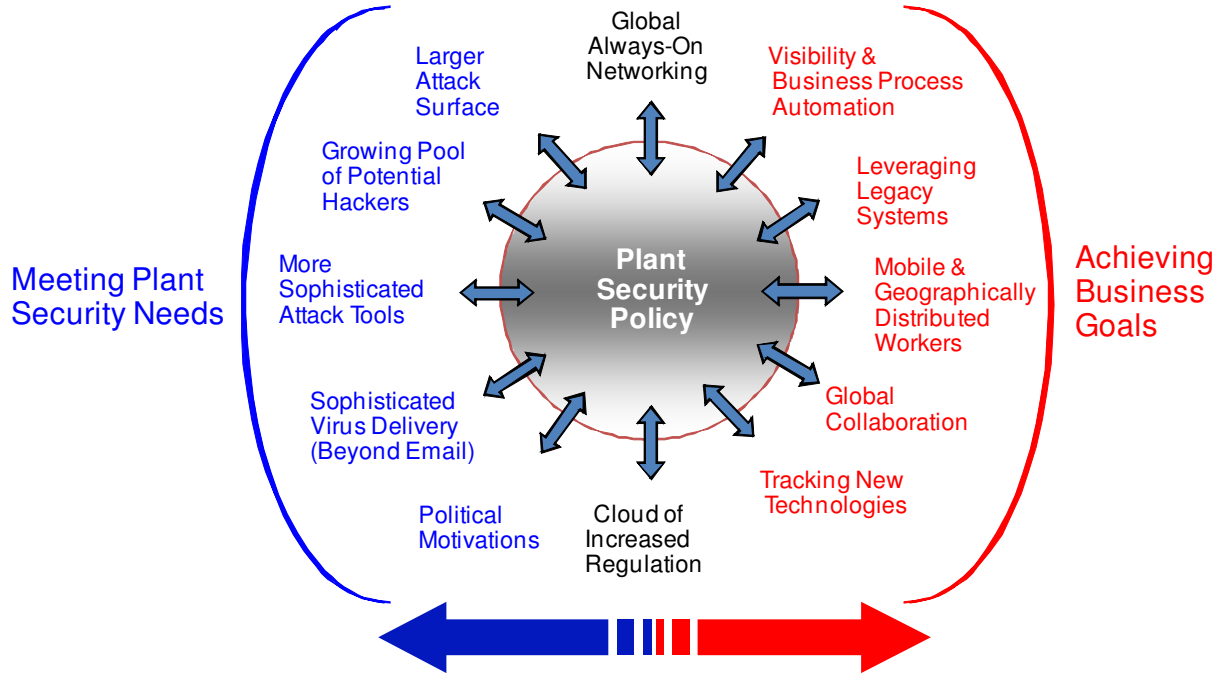
ARC WHITE PAPER

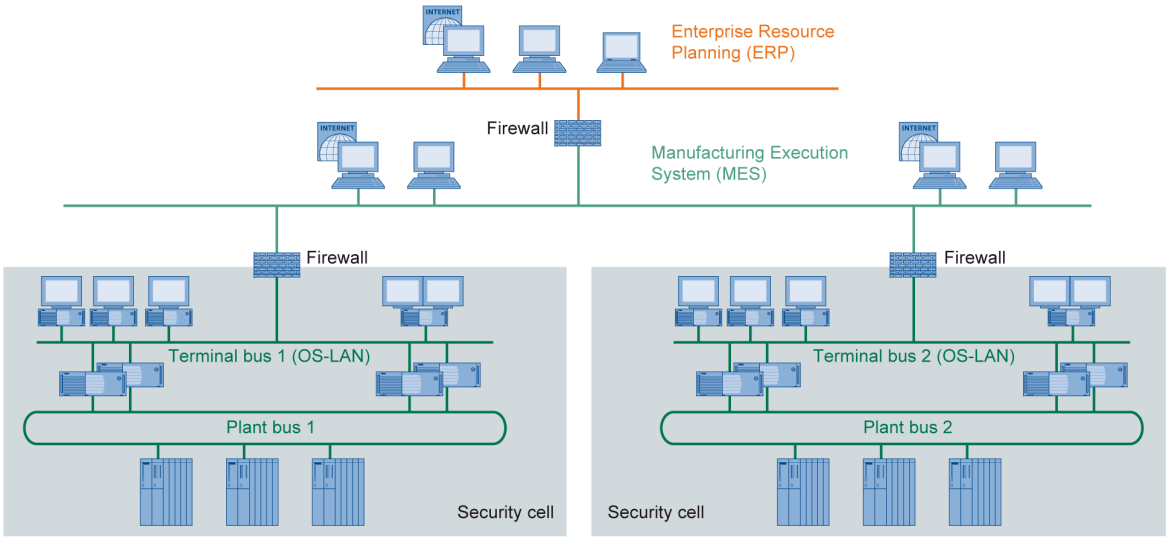
By ARC Advisory Group

SEPTEMBER 2007

IT Security for Process Control Using Siemens SIMATIC PCS 7



A Plant Security Policy Brings Together Disparate Facettes of Plant Operations. The Challenge is to Strike the Right Balance of Meeting Security Needs While Achieving Business Goals.



Implementing a Security Concept Starts with Dividing the Plant into Security Cells by Physical and Functional Layouts, Network Design and Security Concept.

Executive Overview

Ensuring the security of industrial control systems is hardly a new topic. The earliest users of modern control systems in power stations and chemical plants saw the need to protect access to vital control functions from unauthorized use. Similarly, in industries such as fine chemical or pharmaceutical where "the process is the product", manufacturers have always sought to protect the secrets of their unique processes from the prying eyes of industrial spies.

Despite these early roots, the concept of and attitudes toward security in control systems have undergone a necessary overhaul in the past few years, driven primarily by the move to open, commercial off-the-shelf (COTS) technologies such as Ethernet and Microsoft Windows. New threats continue to emerge, most of them not targeted at process users, who can nonetheless be victimized by attacks with far more dire consequences. Process users also face another challenge – the coordination of plant IT configuration and maintenance with corporate IT departments that may not recognize the different goals and specific needs of process users.

Plant engineers should not assume that security concepts borrowed from the IT world will help them both ensure a secure plant environment **and** reach their production goals.

While process users struggle to keep up with the latest security threats and technologies, there is help on the way from automation suppliers. While all suppliers recognize security as a key issue, the approaches taken vary from the support of "secure" components to a full systems point of view. Siemens AG takes a holistic, comprehensive approach to security with its PCS 7 Security Concept. This means that the PCS 7 Security Concept takes into account the specific requirements of process control which in general differ significantly from the requirements of Corporate IT. This approach bundles key security measures in several specific areas to create a deep hierarchy of security known as "defense in depth".

What is Security?

In the world of corporate Information Technology (IT), security means different things to different people. "Security" is sometimes used interchangeably with "safety", especially in terms of access control to secure areas. In, the process industries, "safety" normally refers to the controlled shutdown of a process following an unsafe or abnormal condition. "Security" for the purpose of this white paper refers to electronic access control to industrial control systems and the protection of these systems against unauthorized access, whether intentional or unintentional, as well as against targeted attacks and untargeted attacks via malware.

No security policy is 100% foolproof. Users need to balance costs of security against benefits of interconnectivity and probability and criticality of a security breach.

The use of open communication technologies in the plant such as Ethernet and OPC have exposed formerly closed systems to outside threats, but no technology has increased the risk as much as the use of Microsoft Windows as the *de facto* operating system in most industries. While this has brought many benefits to plant operations such as lower development, deployment and training costs, it has at the same time exposed control systems to all of the threats and dangers of the IT world.

Process automation assets have long lifecycles. In fact, many control systems installed over 20 years ago are still in use today. Rather than invest in and migrate to modern systems – a costly and potentially disruptive process - many automation users have instead kept legacy control systems in operation and upgraded their connectivity to extract more information out of them. The consequence is that formerly closed systems are suddenly connected to open enterprise networks and the internet, exposing ill-prepared systems to modern IT threats.

Conflicts With Corporate IT

Manufacturing industries use IT in many areas of their business - corporate, operations, engineering, R&D, laboratories and others. Practices for developing and managing these various systems are likewise diverse, having evolved along different paths, driven by different requirements, priorities and budget allocations. Historically, the impact of different practices was manageable, but the growing need for capabilities like information sharing across IT domains, cross-functional business process optimization and cor-

porate-wide compliance requires a more integrated approach. Many companies are actively addressing these needs from a technology perspective.

Office Systems	Manufacturing Operations Systems
1) Confidentiality, 2) data integrity and 3) availability are the top three security goals in order of importance (Source: ISA SP99 Part 1)	1) Availability, 2) data integrity and 3) confidentiality, are the top three security goals in order of importance (Source: ISA SP99 Part 1)
Typically used for one shift and downtime can often be recovered	Often run continuously Downtime translates into loss production
Life cycle typically 3 years	Life cycle typically 10 to 20 years or more
Many nearly identical systems (off-the-shelf PC/server systems and standard network components)	Typically unique systems, but also rugged industrial PCs using Microsoft operating systems that are exposed to Windows threats
Never customize the operating system	Use operating systems extensions and unique drivers, making updates complex
Have been maintained in mass	Have not been kept current — may be running MS-DOS or Windows 3.1, 95, NT, and security fixes may not be feasible
Run common office applications	Run a large variety of applications that are closely coupled with the operating system and expensive to upgrade
Applications seldom need to stretch the rules	Applications tend to rely on scripting, proprietary APIs and behaviors to achieve performance, determinism and operations functionalities
Use standard operating system security almost exclusively	Applications provide security extensions for production needs

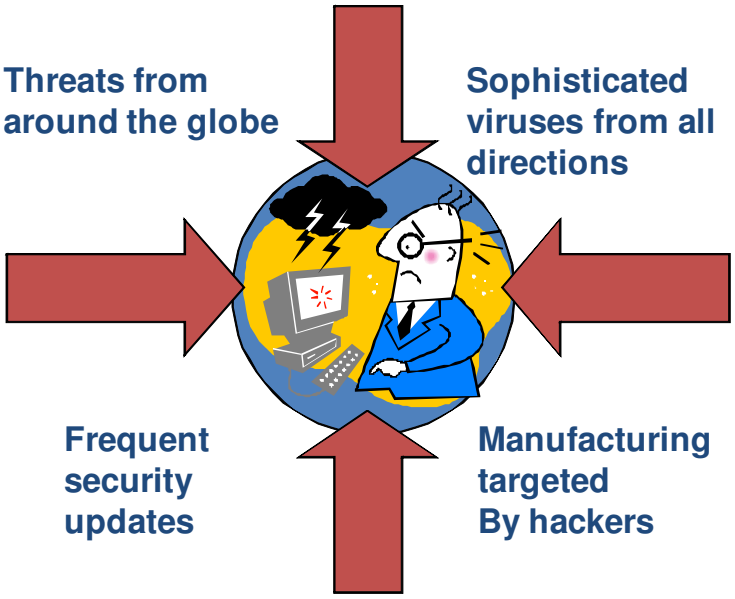
Contrasting Office and Manufacturing IT: The Basis Requirements Are Vastly Different

Security is a critical issue for both corporate IT departments and plant operations. While IT-based security tools traditionally have been implemented and maintained by IT departments, experience has led to a divergence in the underlying philosophies of these two groups due to the fact that each group pursues different goals. IT departments strive to deliver global accessibility to information for all authorized users while maintaining confidentiality. Process automation users, on the other hand, aim to maximize plant uptime and system availability. For this reason, plant engineers should not assume that security concepts borrowed from the IT world will help them both ensure a secure plant environment *and* reach their production goals.

Ever changing and diverse use of technology has made IT organizational structure and ongoing system support a persistent problem for manufactur-

ing companies. Stories about conflicts between plant operations and corporate IT have been commonplace since the first general purpose computers were introduced into manufacturing operations. For many companies, the situation has only become worse as system complexity increases, technologies overlap and integration becomes more important.

Often, these conflicts are rooted in the different perspectives of the various IT groups. Corporate IT organizations responsible for business computing believe that their work on complex business computing problems gives them the knowledge and processes necessary to manage all computing technology for the organization. Functional units, such as plant operations, R&D and engineering, argue that IT decisions must reflect unique domain requirements and cannot be driven solely on the basis of general information technology considerations. They add that corporate IT's understanding and recognition of their needs is inadequate, and allowing them to manage all IT is too risky. Both sides have valid arguments and the debate continues in many organizations.



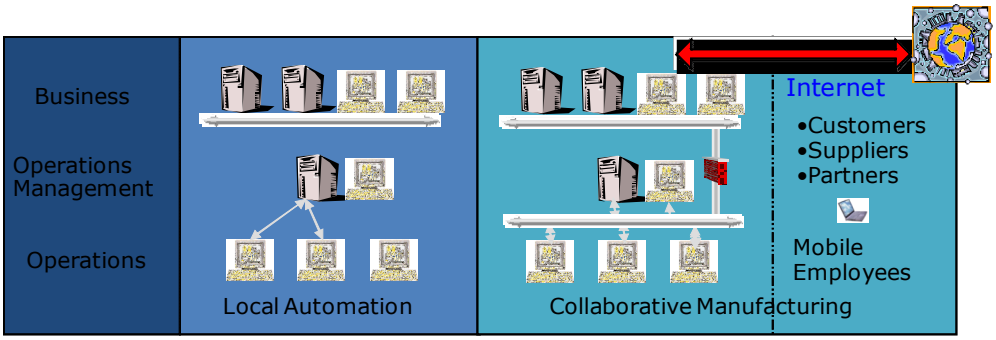
The Introduction of PCs and Ethernet in the Plant Suddenly Exposed Manufacturing Environments to All the Threats of the IT World.

One way out of this dilemma is for plant operations to create a clear industrial security vision based on the well proven methods of corporate IT, but tailored appropriately to the requirements of process control. Such a vision should articulate the specific needs and domain requirements of plant IT vs. corporate IT while defining areas of co-responsibility to ensure active collaboration between the two departments in the future.

The Business Case for Security

Industrial security solutions are sometimes viewed as an onerous cost burden or a necessary investment without a measureable return. However, modern security solutions go far beyond this notion. Many process end users now recognize that the deployment of a comprehensive security policy can directly affect their bottom line.

Process plants connect to the enterprise, which is in turn connected to the internet, to exchange critical process information in an ever-growing spectrum of applications ranging from production management to asset management. Gone are the days of the decoupled plant in which this information was transferred via printed reports. Even in slow clock speed industries, the importance of working with real-time information has increased in recent years due to growing pressures to cut costs in an increasingly globalized world. Thanks in part to the emergence of sophisticated software tools that provide tailored, relevant information in real-time, managers can make better quality decisions more frequently.



Collaborative Manufacturing Uses Technology to Optimize Communication with Supply Chain Partners, but it also Exposes the Enterprise to Global Threats and Risks.

All this information availability means that process manufacturers today are driven more and more by Key Performance Indicators (KPI) – business targets based on measured and forecasted process information. To meet these targets and improve business performance, users focus on continuously improving the performance of plant assets. Typical business metrics include Return on Assets (ROA) and Overall Equipment Efficiency (OEE), both of which are critical contributors to the overall goal of achieving Operational Excellence (OpX). The nemesis of all process plants is unscheduled downtime – stopping a continuous process due to equipment failure, operator error or security breaches. Achieving business goals

means ensuring constant, uninterrupted plant operation while having a contingency plan in place for rapid recovery should a disruption occur. A sound security policy, while not 100 percent foolproof, contributes substantially to the achievement of these business goals by reducing the risk of unexpected interruptions.

The Risks and Costs of Not Ensuring Plant Security

Plant managers sometimes view "9/11" (the terrorist attacks of September 11, 2001) as the day that redefined "security". After that date, security was transformed from an internal to an external issue as the threat of cyber attacks from outside the plant walls became real. New measures were necessary to prevent potential attacks on industries that provide critical infrastructures such as energy, water, transportation and chemical. In the United States, the government has taken active steps to research, develop and distribute guidelines for good cyber security practices for manufacturing industries.

Process users may feel that they are not the target of hackers, but a quick web search reveals sites with shockingly specific instructions on how to hack DCS and PLC controllers.

Similar to industrial safety technology, which can help reduce equipment downtime through intelligent analysis of safety trips, industrial security offers process manufacturers an economic benefit in terms of increased system availability by reducing security risks. Rather than simply looking at security as an additional cost, process users should take a holistic view and weigh the consequences of security breaches that result in unscheduled downtime, equipment unavailability, disruption of continuous processes, or even the destruction of plant equipment, possibly resulting in environmental or even catastrophic damage. Besides the obvious threat to life or physical condition, companies can also risk their public reputation – something that is extremely difficult to shake off as some chemical manufacturers have already experienced.

Security Threats are Real

Process users may feel like they are isolated from security threats for several reasons. They may believe that their proprietary control system is not connected to the internet and thus poses no threat. Or that they may feel that they are not the target of hackers; after all, which hacker would bother learning PLC communication protocols? The truth is different. Surveys have shown that the controllers of many process users who believe their systems are not connected to the internet are, in fact, connected. In addition, a short internet search reveals sites with shockingly specific

instructions on how to hack into DCS and PLC controllers, carefully sorted by type and model.

With the beginning of widespread use of Ethernet in plants as of about 2001, the number of successful attacks sharply increased, with most of the increase coming from external attacks, according to the Industrial security Incident Database (ISID), which has logged and documented about 140 incidents in the past six years. How many incidents go unreported is unclear, but the number is likely to be quite large due to the reluctance of companies to publicize security breaches. While most incidents can be attributed to the rise in connectivity of control systems, at least part of the reason may be the targeting of public infrastructure facilities by hackers in an increasingly dangerous world.

The Many Faces of Process Security Infrastructure

Security infrastructure includes all the hardware, software and associated policies that protect information systems and thereby mitigate business risks. For example, firewalls, intrusion detection software, access control tools and virus scanners are among those considered to be security infrastructure. To be effective, security infrastructure must be applied throughout the enterprise. Accordingly, each security strategy must include an enterprise security architecture that identifies where and how to use selected infrastructure elements to achieve a desired level of security and reduce risk to an acceptable level.

Security infrastructure elements are the technical building blocks for securing systems, and their deployment and management is one of the key tactical activities in any enterprise security strategy. The ISA SP99 team (ISA-TR99.00.01) and others (CIDX) have categorized and discussed security technologies in general terms. This helps to provide structure to the growing list of security products and facilitates the creation of security architecture and design.

The selection of the right security measures and products is a complex task requiring detailed analysis of capabilities and behavior, giving strong incentive for a collaborative enterprise security program. Security products come in many combinations and most network and application products

have security features. For example, firewalls can be purchased separately but are also available in network routers and operating systems.

Attribute	Comments
Authentication and Authorization	User directories, password management, two factor authentication, tokens, bio-metrics, Kerberos
Filter, blocking, access control devices	Firewalls, VLAN, routers, packet filters, intrusion prevention
Encryption and data validation	Public and private keys, VPN, IPSec, SSL, digital certificates
Audit, measurement, monitoring and detection	Intrusion detection and prevention, log and audit tools, virus and malicious code detection, vulnerability scanners, network forensics and analysis tools, automate software management tools
Operating Systems	Workstation, servers embedded, real-time embedded, custom, IP hardening, domain management, patching
Physical Security Controls	(not in the scope of this report)

ISA-99 Categories of Security Technologies

Firewalls

Firewalls are one of the best known security devices and are commonly used at the perimeter of security zones to manage external access to the networks inside the zones. Note that a physical site may be comprised of multiple security zones, such as enterprise, production management and process control networks, and firewalls to provide isolation.

Firewalls come in a large variety of configurations and packages including standalone software, dedicated hardware appliances and are sometimes even part of the operating system. They are not all the same and must be configured to suit the intended purpose. Accordingly, their selection, deployment and management must be carefully planned.

VPN and IPSec Provide Pipes

Virtual Private Network (VPN) technology provides secure connections between manufacturing sites and is in common use. However, the use of VPNs assumes that both ends are trusted and does not limit what is passed over the connection. Accordingly, other protection methods must be applied to provide necessary filtering and isolation. IPSec is similar and some suppliers even suggest using IPSec between two stations on a large net-

work to protect sensitive communications from access by other network participants.

Security Cells

Implementing a security concept starts with the division of the plant into logical security cells along the lines of its physical and functional layouts, network design, and security concept. A security cell may consist of several smaller segments, but must ultimately be able to operate autonomously for a certain period without connection to other plants or functional units if cut off from the rest of the plant. All members within the security cell are considered to be trusted, so no further security measures are required inside. Therefore, neither data encryption nor firewalls between cell devices are necessary. This means that access to security cells may take place only via well defined access points that include authentication.

Dividing cells by function also means that most network communication takes place within the cell, reducing the overall plant communication load and simplifying an analysis of network traffic should an intrusion occur. Security against incorrect operation is achieved primarily through the mutual authorization and authentication of users and devices. Typical standards used to check security credentials are Kerberos (via Active Directory) or IPsec.

Patch Management in Manufacturing Businesses

Manufacturing businesses have more complex patch management situations than other businesses because of the unique requirements of manufacturing operations relative to office systems. Both use the same platforms, typically PCs with Microsoft Windows operating systems, but the applications, risk of failure and consequences of failure differ dramatically, dictating segmentation in enterprise patch management processes.

The most important differences stem from reliability, availability and compliance requirements. Systems used in manufacturing operations such as for Human Machine Interface (HMI) allow plant personnel to visualize and control the process. Their failure can often place people, the environment and even public safety at risk. These systems typically must run "24/7" and the cost of downtime can be high and unrecoverable. Finally, some product is only usable when its manufacturing conditions and quality are documented and this is only feasible with electronic systems.

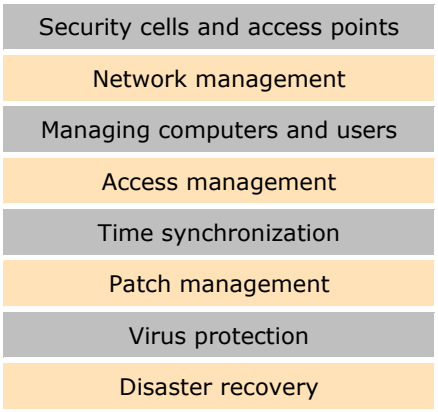
Siemens' Security Concept for PCS 7

Process plant operators employ personnel who are not always knowledgeable when it comes to IT security. In today's environment, process engineers work closely with corporate IT departments to design, implement and maintain a security strategy around their plants. This job can be made easier, of course, if automation suppliers play an active role in providing guidance and support for security issues. While all suppliers recognize security as a key issue of concern to process users, the approaches taken vary from the support of "secure" components to a full systems point of view.

Siemens AG, a major supplier of both discrete and process automation solutions, has taken a comprehensive, systems approach ever since the Simatic PSC 7 distributed control system (DCS) was introduced. The PCS 7 Security Concept bundles key security measures in several specific areas to create multiple levels of security, commonly known as "defense in depth".

PCS 7 Security Concept Takes a Systems Approach

Siemens has designed its PCS 7 Security Concept to address the most relevant critical areas of process IT security, including security cells and access points, network management, managing computers and users, access management, time synchronization, patch management, virus protection and disaster recovery. While this may look complex, a modular approach helps keep the complexity to a reasonable level. In addition, the use of standard, web-based technologies means that many tools are already familiar to IT personnel. This comprehensive approach is not limited to the use of single security methods like data encryption or devices like firewalls, but rather is based on the interaction of multiple security measures deployed throughout the control system. The PCS 7 Security Concept guidelines document is updated regularly and is available for download.

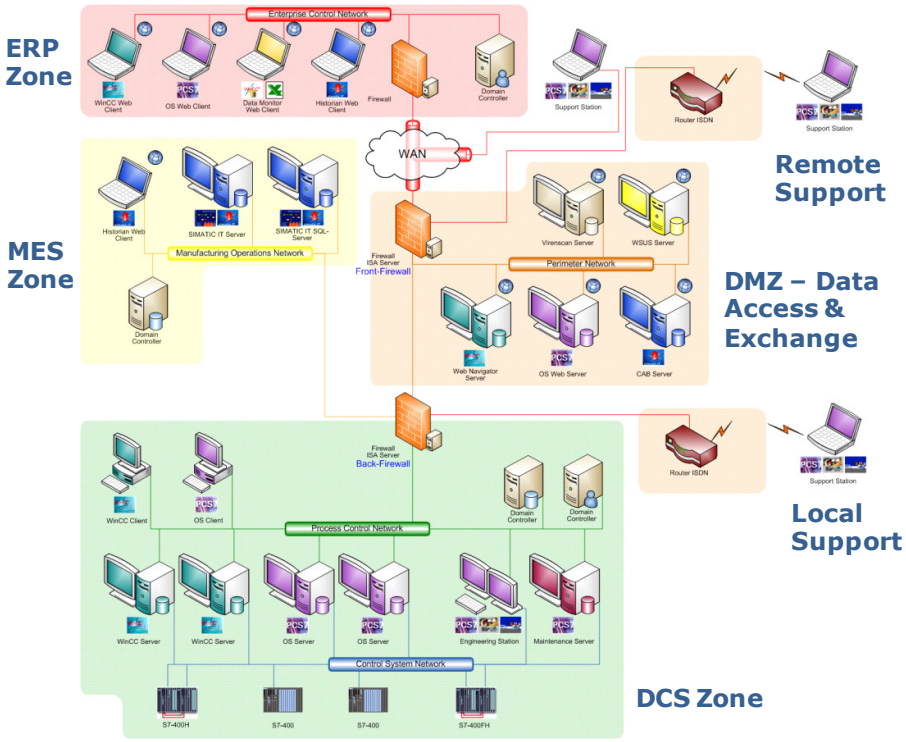


PCS 7 Security Concepts Addresses the Critical Areas of Process IT Security

Siemens is the only process supplier that currently develops and manufactures the full array of control hardware and software as well as secure network components that are designed for industrial applications. This allows the company to offer its customers one-stop shopping for a process solution combined with network security components that are optimized for industrial process control applications.

Creating Secure Architectures

Security cells can be of any scalable size – from a small automation unit up to a whole building. Cells are defined by dividing the plant into logical segments along the lines of its physical and functional layouts. To comply with FDA Part 21 CFR 11 security requirements that define physical and logical access restrictions, security cells may need to constitute a "closed system". Firewalls are used to isolate cells from the rest of the plant at network access points.

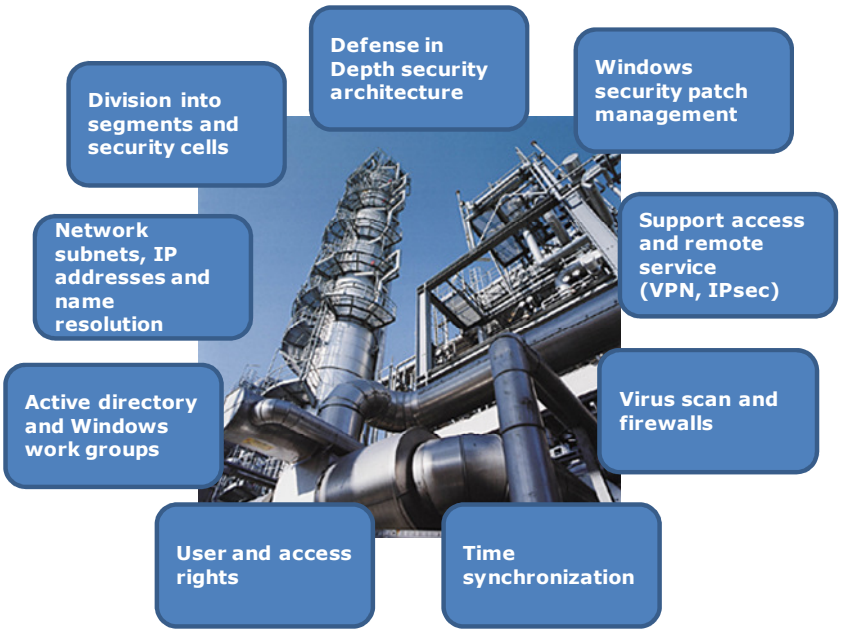


Security Cells are Created by Dividing the Plant into Logical Segments Along the Lines of its Physical and Functional Layout

In many cases, it is necessary to allow access to a security cell by a trusted device located outside of the cell, such as a workstation running an MES application. This can be accomplished using the standard IPsec protocol, making the work station a part of the security cell but with limited access rights. Non-trusted devices used by trusted partners should be connected in a way that allows all actions to be checked for potential dangers. For this, standard web server technology can be used on a server located outside of the cell in a "demilitarized zone" (DMZ). Devices in the security cell write information to the web server that in turn makes this information available to outside devices, but does not allow any information to be written back to the cell.

Using Firewalls

While many firewall products are available in the market, the PCS 7 Security Concept recommends the use of Microsoft Internet Security & Acceleration Server 2006 (ISA Server 2006) for PC-based solutions due to its ability to filter HTTP traffic at the application layer, inspect data for viruses with a built-in virus scanner, and to receive and decrypt IPsec data as a proxy to analyze for anomalies. It also allows switching of security policies depending on events (such as the detection of a virus) up to and including completely blocking communication in case of a security incident. As an application proxy, ISA Server 2006 can accept data on behalf of the actual recipient and check packet content for malicious code before passing it on to the intended recipient. The proxy can also perform a user and computer authentication before forwarding the packets. The Security Concept also recommends the ISA Server 2006 firewall for dial-up connections via Virtual Private Networks (VPN), again due to its high degree of customization. Finally, the local firewall that comes with Windows XP may also be used. This firewall can be configured automatically by the PCS 7 set up routine to ensure correct configuration.



Siemens' PCS 7 Security Concept Provides Comprehensive Guidelines and Recommendations for All Facettes of Industrial Security

For hardware-based firewalls, Siemens recommends its own line of Scalance S security modules. These modules differ from office-type devices in that they are hardened for use in industrial environments (IP30) and they are optimized for communication of process control information. Scalance S security modules allow data packet filtering functions ranging from simple packet inspection up to stateful inspection. Stateful inspections, for example, memorize which of the outgoing packets are expecting answers. Only incoming packets containing expected answers are allowed to pass. Stateful inspection firewalls consider also established TCP connections and therefore provide more security than pure packet filter firewalls.

Patch Management

The management of patches in a process automation environment is another complex and challenging task for process users, especially those who still run older or even outdated versions of operating systems (OS). Even for an up-to-date OS like Windows XP, a paraphrase of the old saying "never *patch* a running system" does not completely apply. XP and the recently released Windows Vista remain the top targets for malware worldwide, so staying current with the latest fix is as crucial in the plant as in the office world. While process control systems may not be the intended targets of viruses, the consequences and resulting damage of a successful viral infection can be far more devastating than in the case of an infected office PC.

The PCS 7 Security Concept guides users in the use of standard Microsoft tools through the four phases of patch management: 1) assess threats and vulnerabilities, 2) identify relevant updates, 3) evaluate and plan the deployment decision, and 4) deploy updates. To accomplish this, the Security Concept describes how to use Microsoft's various tools, including Windows Software Update Service (WSUS) and Systems Management Server (SMS), greatly simplifying patch rollout. Some adjustments are necessary such as blocking automatic reboots.

To assess the security vulnerability of each computer, the Microsoft Baseline Security Analyzer (MBSA) is used to scan selected computers, analyze them, present a report of detected vulnerabilities, and list missing security patches. Based on this list, the user must then weigh the risk of continuing operation with uninstalled security patches versus the effort required to install the patches, which sometimes requires a reboot. This decision is supported by technical information from Microsoft that may shed some light on the severity of the risk such as the nature of the vulnerability (for example, it requires opening an email) or which particular part of the OS or application is affected.

Siemens takes IT security very seriously. The company operates a dedicated security laboratory in order to develop and document security concepts and recommendations, to ensure quick reaction to new threats, to harden PCS 7 proactively against attackers, to execute vulnerability scans, and to test virus scanners and security patches for compatibility. Test results are published on the internet shortly after patch release.

Detecting and Preventing Viruses (Malware)

Besides firewalls, virus scanners are the most popular security measures. PCS 7 supports the use of the three most commonly used virus scanners in manufacturing and control systems:

- Trendmicro™ Office Scan Corporate Edition
- Symantec™ Antivirus Corporate Edition
- McAfee™ VirusScan Enterprise

Virus scanners should be placed at the access points to filter incoming and outgoing traffic. However, security policies often dictate the installation of virus scanners on plant PCs such as operator HMI consoles or on engineering workstations where data is exchanged with the outside world. In this case, Siemens provides detailed recommendations on how to configure the virus scanner settings in order to obtain a good balance between real time requirements of the process and virus protection. Redirection of virus alert messages to competent personnel makes sure that plant operators are not distracted.

Controlling System Access and Managing Accounts

For plants with ten or more computers, the PCS 7 Security Concept recommends the use of Windows Active Directory to manage computers and user accounts. Active Directory, introduced with Windows 2000, standardizes the management of security and user accounts in a dynamic, flexible way, making it suitable for large configurations that may add or delete users or computers on a regular basis. Moreover, certain legal standards may require the use of Active Directory, for example, if Kerberos is required for authentication or for centralized logging of events. For smaller, fixed configurations, the Security Concept also contains provisions for using Windows Workgroups.

The management of user accounts is a sensitive area between corporate IT and plant operation that must be set up and coordinated with both technical and diplomatic savvy. If a separate domain is set up for the plant, this domain must be managed only by plant operations personnel. This responsibility cannot be transferred to others outside of the plant because such persons are not in a position to judge whether a given configuration change will have a negative effect on the production process. Active Directory has the advantage that plant personnel can configure the plant

network almost entirely independently of corporate IT and therefore protects the plant from the consequences of unintentional intervention by corporate IT.

If a company already has an Active Directory domain, it can form a dedicated or "embedded" organizational unit for managing the plant. This variation shifts domain management responsibility to corporate IT so that plant personnel do not have to manage their own domain. However, this requires a good working relationship with corporate IT because it transfers management responsibility for the plant organizational unit into their hands. In any case, it is important that unauthorized members of corporate IT do not gain privileges to change the configuration of plant PCs due to the great risk of disrupting and harming production processes.

User and Access Management in PCS 7 and Integration into Windows Management

Windows provides a flexible system to allocate users privileges. However, in critical process environments, privileges should be assigned according to the principle of minimal rights: each user should have just enough privileges to do his or her job, for example operations personnel should not be granted administrator privileges, according the PCS 7 Security Concept.

When working with projects in a PCS 7, Simatic Batch, or Simatic Route Control, administrators can define specific rules for rights and privileges for project sharing and project file access. In addition, the Simatic Logon Service allows the assignment of application specific user roles and rights, as well the use of a common login/password for the PC and the applications running on it. It takes advantage of Windows user management tools to provide capabilities such as auto-logout and password expiration.

Network Management

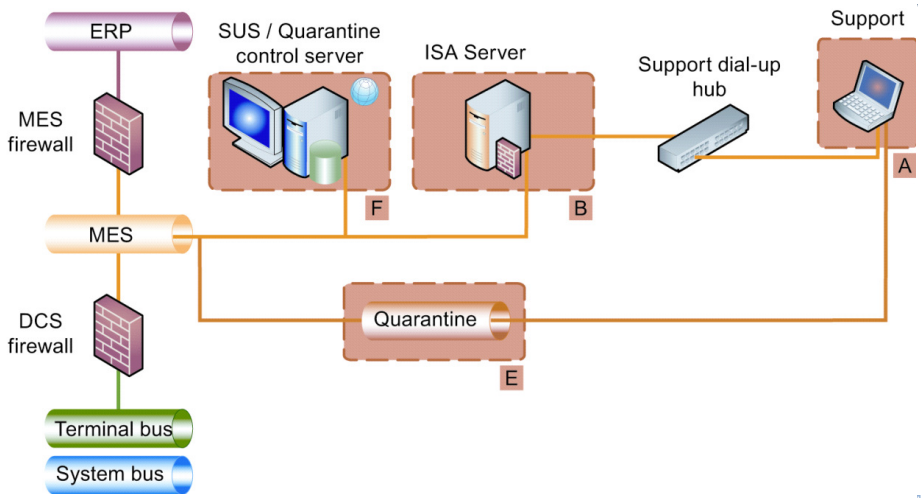
This part of the Security Concept provides guidance to users on the implementation of DHCP servers and the allocation of IP addresses. Process-specific tips are provided; such are the reservation of addresses for all plant PCs on the terminal bus to ensure that each PC always receives the same IP address even after they have been switched off for a long time.

Using VPNs and Encryption

Plant IT domain configurations are rarely static. System maintenance often requires adding a PC to the network, if only temporarily. Many process users today take advantage of remote monitoring and maintenance services

from system integrators or automation suppliers. While these services may add value, they also represent a high security risk to a secured system if a computer with an unknown security status is allowed access to the plant domain.

Virtual Private Networks (VPN) provide a reliable and secure connection from an outside device to a secured control system. Together with Network Access Quarantine Control, the Siemens Security Concept recommends this approach using Microsoft's ISA Server 2006. To access the system, the support computer connects to the ISA Server through a support dial-up hub. Although connected, the unknown support computer has no permissions in the network and cannot access the plant. Instead, the computer remains in the quarantine network where it undergoes a security check. This check may determine if the firewall and virus scanner is active and the computer is free of known viruses, and whether all the latest updates and patches have been installed. Only when these points are confirmed is the support computer given appropriate access to the plant.



VPNs and Quarantine Control Allow Temporary Network Access to Computers and Devices Outside of the Plant Domain

If access to plant data is provided via web-browsers, the Security Concept recommends using data encryption and server authentication by using either Secure Socket Layers (SSL) with HTTPS or IPsec and user authentication via user name and password. ActiveX application components are verified with certificates, allowing the user to check their trustworthiness from the information about the certification authority.

Time Synchronization

The synchronization of the clocks contained within all PCs and controllers in a plant is a critical, but often neglected issue. A surprisingly high number of large and small manufacturing processes depend on reliable timing and synchronization, and these time values are often generated from standard 12- or 24-hour clocks. Before standard tools were available to handle this, plants were subject to potential Y2K-like disasters whenever the clocks were changed for summer or winter time. One potential danger is that domain clients could be denied log on rights to their domain controllers. This is due to a security feature in Windows that is intended to prevent the hijacking of an established session if the configured time tolerance between client and server is exceeded.

The PCS 7 Security Concept supports most variations of clock synchronization, from small configurations that use a controller as the master clock to larger scenarios in which all workstation and controller clocks are synchronized with a plant's central clock.

Policies and Training

While Siemens provides a comprehensive set of guidelines for industry security in its PCS 7 Security Concept, the onus is still on process users to develop a clear security policy and properly train plant personnel. ARC recommends starting with the creation of a security vision that sets simple but sustainable goals for plant security into the future. This vision should encompass all of the enterprise's security needs – not just those of plant operations, but should clearly define the divisions of responsibilities between corporate IT and plant personnel.

With the security vision in mind, process users should then write and publish security policies based on the recommendations of process suppliers like Siemens. These policies can then be turned into company Best Practices – specific guidelines for each defined task in implementing the security policy. Best Practices contain the highest level of detail and therefore are more technical than policies. Many of the recommended procedures in Siemens' Security Concept can be taken over one-to-one as Best Practices.

Finally, the security policy should include specific guidelines on training to ensure that plant personnel possess the right level of IT skills appropriate for their job. Training should be documented by awarding IT certificates to leave a clear "paper trail". In the case of a security breach with resulting

negative consequences, this is crucial to prove policy compliance and to limit liability.

Disaster Recovery

Disaster recovery is an IT concept concerned with regaining access to the data, hardware and software needed to resume operations after a natural or human-induced disaster. As process manufacturing becomes more and more data-driven, the ability to restore data quickly to a pre-disaster state gains paramount importance. Traditional tape-based backup is often inadequate for disaster recovery situations because it involves too much human intervention and the management of too much data – two conditions that almost inevitably lead to error and delay. Network-based solutions exist for enterprise systems, but these may not always reach critical data stored in remote or laboratory PCs.

With PCS 7, should a loss of data occur, each plant PC includes a complete image of the system software with which the system partition can be restored anytime. For archiving of process data, Siemens provides several tools such as StoragePlus, the Central Archive Server (CAS), and Simatic IT Historian. Workstation PCs support RAID technology to improve MTBF of hard drives. PCS 7 network components support Syslog as the *de facto* standard for forwarding log messages in an IP network. Finally, PCS 7 supports redundancy on all levels.

Successful disaster recovery means following a defined set of Best Practices (disaster recovery plan) that may be implemented during times of pressure or even panic. These should include an analysis of the causes of a crash before disk restoration to prevent an identical crash happening right away. Plant personnel training should include disaster recovery training and the plant security vision and policies should include provisions for disaster recovery.

Standards and Certification

In the United States, the government has been particularly proactive in driving home the importance of industrial security. The Department of Homeland Security, created after the terrorist attacks of 2001, commissioned the Idaho National Laboratory (INL) to formulate and publish Best Practices for "Control Systems Cyber Security". These guidelines are aimed specifically at preventing attacks from "terrorists, nation-states, hackers and insider threats" on strategic industries including chemical, food, water and

other public infrastructures. Where security concepts cannot be certified, process users can minimize their liability by quoting and implementing these guidelines and recommendations wherever feasible.

Certification is difficult in times of lacking standards. Certificates of small, independent companies, even those with a proven record of expertise, are not comparable and put automation vendors in a situation in which they may need to undergo multiple certifications to meet end user requirements – an unreasonable cost burden.

This is one reason why ISA founded the ISA Security Compliance Institute (ISCI). Within ISCI, leading industry suppliers, government and end users can jointly develop standard test programs and test beds for evaluating compliance to industry standards such as ISA-99. Governments and insurers may put end user industries in different security categories depending on the threat level a potential incident may cause to the environment and population. The category could determine what security level has to be achieved by certification as well as the expiration date. With generally accepted standards, certification can be achieved more reasonably by certified bodies, making certification result comparable. Siemens is a founding member of ISCI.

Recommendations

Control systems security has made rapid and significant progress in recent years, but attacks continue to grow in sophistication and frequency. Comprehensive enterprise security strategies are new to many businesses and even those who are far along will benefit by examining their strategies and considering emerging technologies and practices. Techniques are available for establishing and maintaining a secure environment, but these can be costly. Accordingly, the state of the art must continue to evolve until security considerations are built into our processes and the systems and software we buy.

- Start by creating a security vision that sets simple but sustainable goals for plant security into the future. This vision should encompass all of the enterprise's security needs – not just those of plant operations, but should clearly define the divisions of responsibilities between corporate IT and plant IT. Then write a security policy to support the goals of the security vision.

- Develop business justification models for security including consistent ways of assessing risk and identifying the required level of security.

- Define enterprise and plant security architectures, including business and operations systems, as an umbrella for segmenting requirements, developing practices, and implementing security measures. Use standardization processes to find, evaluate and select security infrastructure that enables consistent use, common policies and better security.

- Develop a collaborative relationship with software suppliers, conveying requirements and developing methods to minimize exposure to vulnerabilities. Consider placing security related support requirements in purchasing contracts. Software suppliers often know best how to secure their products, are investing in security and want to help.

- Take advantage of the security consulting services offered by controls suppliers.

Analyst: David W. Humphrey
Editor: Larry O'Brien

Acronym Reference: For a complete list of industry acronyms, refer to our web page at www.arcweb.com/Community/terms/terms.htm

API	Application Program Interface
APS	Advanced Planning & Scheduling
B2B	Business-to-Business
BPM	Business Process Management
CAGR	Compound Annual Growth Rate
CAS	Collaborative Automation System
CMM	Collaborative Manufacturing Management
CNC	Computer Numeric Control
CPG	Consumer Packaged Goods
CPAS	Collaborative Process Automation System
CPM	Collaborative Production Management
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol
EAM	Enterprise Asset Management
ERP	Enterprise Resource Planning
HMI	Human Machine Interface
IT	Information Technology
MIS	Management Information System
MRP	Materials Resource Planning
OpX	Operational Excellence
OEE	Operational Equipment Effectiveness
OLE	Object Linking & Embedding
OPC	OLE for Process Control
PAS	Process Automation System
PLC	Programmable Logic Controller
PLM	Product Lifecycle Management
RFID	Radio Frequency Identification
ROA	Return on Assets
RPM	Real-time Performance Management
SCM	Supply Chain Management

Founded in 1986, ARC Advisory Group has grown to become the Thought Leader in Manufacturing and Supply Chain solutions. For even your most complex business issues, our analysts have the expert industry knowledge and firsthand experience to help you find the best answer. We focus on simple, yet critical goals: improving your return on assets, operational performance, total cost of ownership, project time-to-benefit, and shareholder value.

You can take advantage of ARC's extensive ongoing research plus experience of our staff members through our Advisory Services. ARC's Advisory Services are specifically designed for executives responsible for developing strategies and directions for their organizations. For membership information, please call, fax, or write to:

ARC Advisory Group, Three Allied Drive, Dedham, MA 02026 USA
Tel: 781-471-1000, Fax: 781-471-1100, Email: info@arcweb.com
Visit our web pages at www.arcweb.com

3 ALLIED DRIVE DEDHAM MA 02026 USA 781-471-1000

BOSTON, MA | WASHINGTON, D.C. | PITTSBURGH, PA | PHOENIX, AZ | SAN FRANCISCO, CA
CAMBRIDGE, U.K. | DÜSSELDORF, GERMANY | MUNICH, GERMANY | HAMBURG, GERMANY | TOKYO, JAPAN | BANGALORE, INDIA | SHANGHAI, CHINA