BULETINUL Universităţii Petrol – Gaze din Ploieşti	Vol. LX No. 3B/2008	55 - 60	Seria Tehnică

Industrial Process Control Network Security

Nicolae Paraschiv, Emil Pricop

Universitatea Petrol – Gaze din Ploieşti, B-dul Bucureşti nr.39, Ploieşti
e-mail: nparaschiv@upg-ploiesti.ro

Abstract

The industrial control systems became real data networks and usually they are connected to the IT business network and even to the Internet, for remote operation. For this reason the security of these networks is a very important issue. In this paper we will present a security strategy considering access control problems, process safety, and network and operating system issues. We propose a biometric access control system for securing the physical layer of the industrial control network and the separation of the network zones for securing the logical layer.

Key words: *process control, security, Internet, remote access, remote control*

Introduction

The industrial control systems became real data networks and usually are connected to IT business network and even to the Internet, for remote operation. Nowadays the sensors use wireless communication to transmit measured data, the controllers could be operated from virtually any place around the world using an Internet connection. The production environments rely on computer based control systems to precisely command and monitor the processes. The operating systems used now by industrial computers are widely spread and used in business networks, so there is an increased need for antivirus and antimalware protection. Process control systems for refineries, SCADA networks for electric, natural gas or water distribution, or factory automation systems, any of these need protection from hackers, disgruntled employees and cyber terrorists.

Control system cyber incidents have occurred in electric power (transmission, distribution, and generation-hydro, fossil, and nuclear), water, oil/gas, chemicals, and manufacturing. Recent control systems security events include increased 'probing' and analysis of critical infrastructure as noted by the FBI. There is also an increase in 'chatter' about control systems vulnerabilities on hacker Internet message boards known as black hat boards and vulnerability boards.

Among the different types of actual events targeting controls systems in a specific company, there are three broad categories: (1) intentional hits such as hacking (unauthorized entry into secure electronic files), denial of service - an attack designed to bring down a network by flooding it with useless traffic; (2) unintentional consequences or collateral damage from worms and viruses; and (3) unintentional internal security breaches, such as inappropriate testing procedures of operational systems or inadequate control systems architecture.

Of the three, targeted attacks are the least frequent, being the most damaging, but also requiring detailed knowledge of the entity and supporting infrastructure. Consequently, the most likely attacker is a disgruntled employee, ex-employee, or someone who has worked with, or for, the entity being attacked [4].

The most typical result is erratic behavior of the system, including slowdown, loss of response, and shutdown. Compromised manufacturing and control systems can include endangerment of public or employee safety, loss of public confidence, violation of regulatory requirements, and loss of proprietary or confidential information, economic loss, and impact on national security. The human factor is the weakest link in this system, so the most important security measure is to control the physical access in the plant and especially to the control room.

A Proposed Biometric Control Access System

Physical access security means protecting the site from threats like: vandalism, theft, violence to staff, unauthorized access to confidential, commercial and personal records, misuse of assets, fraud and sabotage. A powerful person identification system is needed for ensuring physical access security. There are mainly three categories of methods for personal identification. The first category contains the techniques that rely on an object that is in the possession of the user (a card, a badge). The methods in the second category are based on the knowledge of the user (passwords, PIN – Personal Identification Number). The third category is composed by methods that use anatomical characteristics of persons, known as biometrics. Biometrics are by far the best methods used today in recognition technologies, especially fingerprints being widely used for this purposes, both in military and commercial environments. The cards could be stolen, the passwords could be forgot or discovered, but the fingerprints cannot be reproduced, forged or stolen. A system that uses biometrics along with another method (card or PIN) is considered highly secure [1], [2].

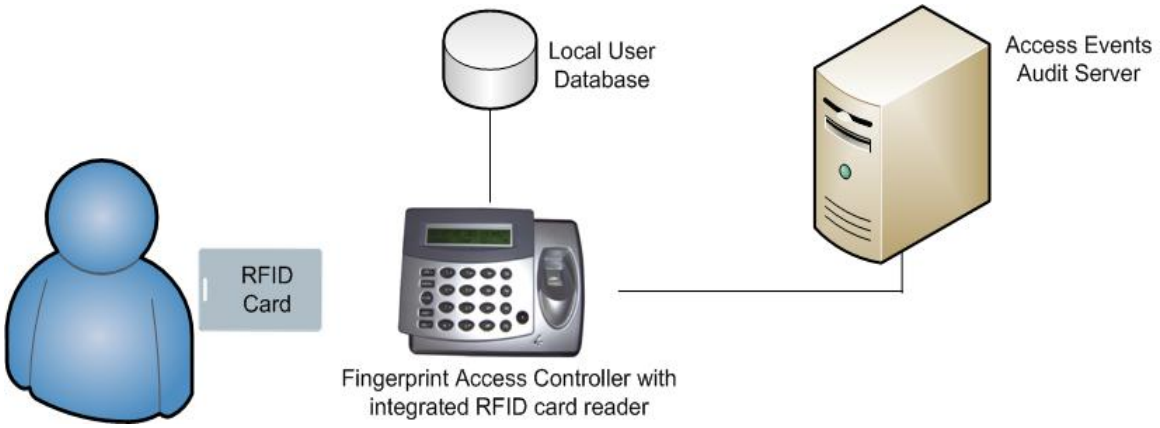

Fig. 1. Local control access system

We propose a modern and powerful system that uses a two-factor identification model: the RFID card and the fingerprint of the user. When a user wants to enter or exit a building or a zone in the enterprise he must place the RFID card in the nearby of the reader, which is integrated in the Fingerprint Access Controller. The system will then ask the user to place his finger on the sensor to read the fingerprint. After the data obtained in real time is process, a fingerprint template is computed and it is compared with the one stored in the local database in correspondence with the data in the RFID card. If the comparison result is over a threshold the user is recognized and has access granted. Each event is journalized in an event log in the Fingerprint Access Controller memory. The event log is then downloaded using TCP/IP

interface in the Audit Server where various reports are created. That way the administrator knows who and when entered or left the building, what person tried to enter and was not recognized, etc. These reports are available as web pages dynamically generated in real-time using PHP or ASP scripts and could be accessed from any location in the world where an Internet connection with the Audit Server could be established.

Having a TCP/IP interface the Fingerprint Access Controller could be configured remotely. The user enrollment could be done from a central workstation that has a fingerprint reader and compatible software. The whole data is transmitted to the device using a secure protocol, and optionally is stored in a central database.

The system could be extended for usage in distributed environments as displayed in Figure 2. An administrator in Central Location operates the system. There are stored the user data, scripts for generating reports and databases. The data from each location is transmitted using a secured Internet connection such as TLS/SSL. The reports are available from any location in the world, using a simple Internet browser. Using this control access system and specialized software, a powerful distributed time & attendance system could be created.

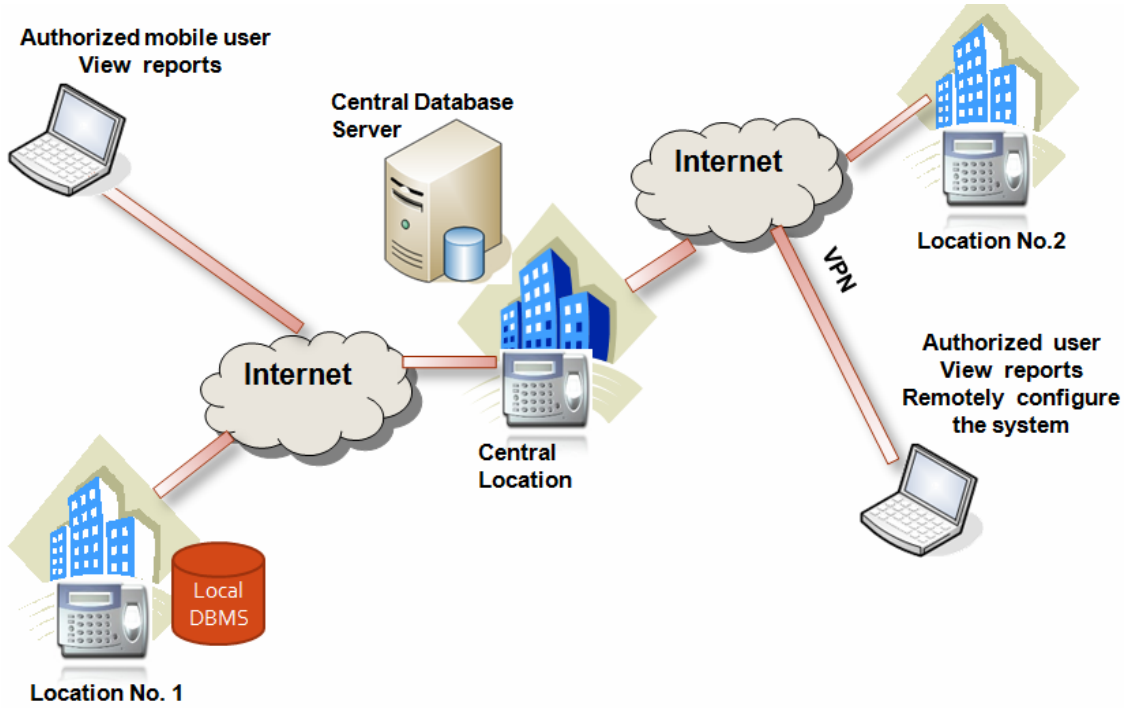

Fig. 2. Distributed control access system

It is important to know who and when issued a command. It is recommended to clearly identify the user at the console, integrating a biometric scanner with the HMI. This way the system can take account of user permissions, only the authorized person being able to change a parameter or issue a command. Every action could be recorded in an event log that is stored in a central database. Analyzing that log it is possible to generate reports of activity and to simply investigate who do a mistake and in what context.

Process Control Network Security

Many of the systems used in automation are embedded systems, incorporating specific operating systems that are not exempt from serious threats: virus attacks, malware, and worms. Also many manufacturers install common operating systems such as UNIX or Microsoft Windows, improved with special software. These systems must be protected using powerful antivirus, antispyware and antimalware software, taking account on the performance impact of these programs on the real-time operation capabilities.

Any computer connected to a network is vulnerable to attackers. The solution to remove the connection and to keep the computer standalone or connected only to the process is not viable anymore. This way is justified to install a firewall between a critical computer and the rest of the network. It seems to be a common task for a simple PC, but we cannot install a firewall on a PLC so there is needed a hardware firewall.

In Figure 3 is displayed the network diagram. The Process Control Network is the protected zone that contains data and information extremely valuable for the business. It is connected via the TCP/IP protocol to the Enterprise Network and to the Internet.

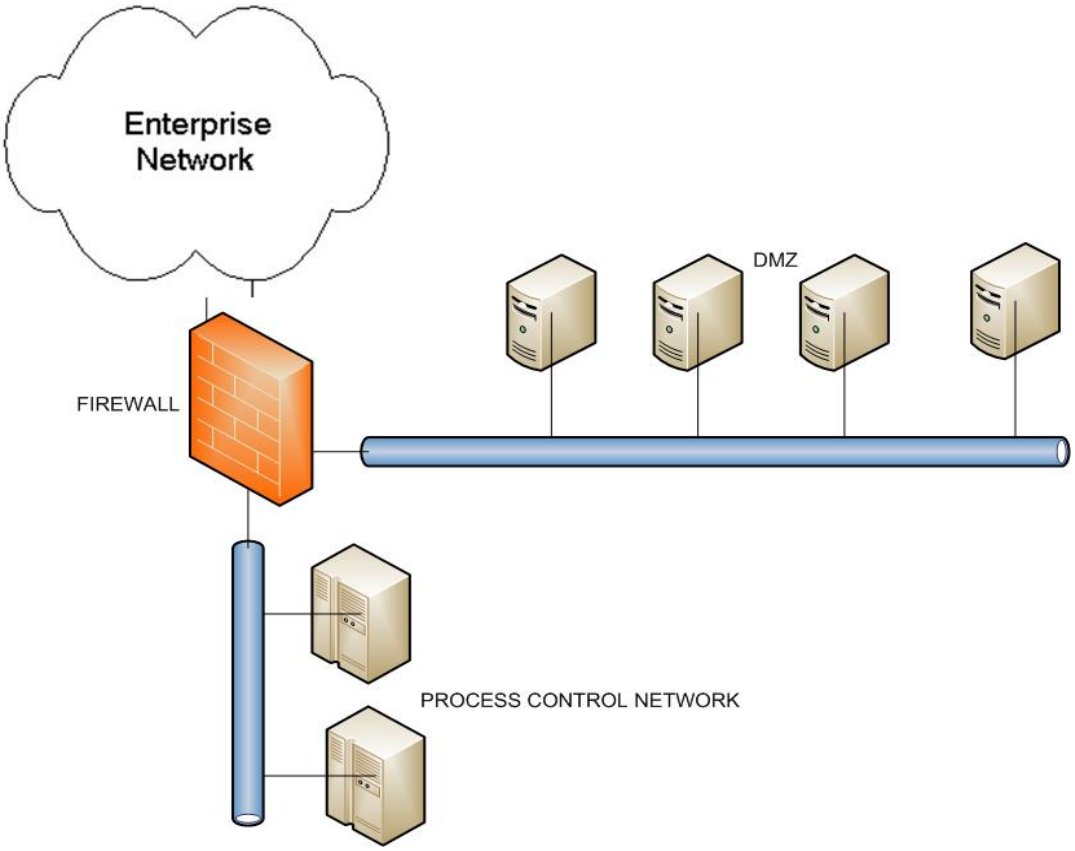

Fig. 3. Process control network connections diagram

The Enterprise Network represents any network outside the Process Control Network, such as: local area network, WAN network. This allows the employees to connect from any location in the world to the enterprise's data.

DMZ or Demilitarized Zone is a critical component of the security system. Hardened servers with latest software patches compose this zone. These servers could be accessed from the

Internet directly. A usage scenario could be that DMZ server has Terminal Services running for Remote Access and the user could connect form Internet to the DMZ server and from the terminal to a process computer situated in Process Control Network [4].

It is important to divide the network in several layers such as: Field I/O, Controls Network Zone and Plant Network Zone [3].

Field I/O layer includes the communication that occurs in the direct hardwired communications between I/O devices, such as sensors, and their controllers. Security is accomplished at physical level. Nowadays the sensors are connected in large Wireless Sensor Networks (WSN), which are wireless ad-hoc networks, each sensor supporting a multi-hop routing algorithm. There is an increased need to take in consideration the security techniques of wireless communication such as data encryption or MAC address filtering.

Controls Network Zone is the zone that needs the highest level of security. It carries the process control device communications. This network segment is very sensitive to the volume of traffic and protocols used.

Plant Network Zone connects various network locations. This zone carries the general business network traffic such as ERP, file & printer sharing, Internet browsing.

Internet Zone is connected directly to the Internet and could have the lowest security level.

Each layer or zone must be separated using Intrusion Detection equipments or hardware firewalls. An Intrusion Detection System monitors packets on a network and determines if the activity is potentially harmful, such as a worm attack. A typical example is a port scan attempt that initializes a large number of TCP connection requests (SYN) to many different ports on a target machine. That way the administrator could prevent many problems in different zones of the industrial network.

Separating each zone of the factory automation system leads to three networks that have specific security issues. For administrative tasks, such as patch distribution, monitoring, antivirus scanning, it is better to have three small homogenous networks with the some kind of problems and similar security needs than one big network with various components, each of them having other security requirements.

Conclusion

In each company in the near future a security plan must be formed and implemented, establishing a standard, a consistent methodology, implemented throughout the whole enterprise. Security measures must be set up with caution. In critical process HMIs, the process operator always needs to have a view to the process. Even common practices such as a password lockout may create a situation where the operator can't view the process when he needs to. In critical event situations, when adrenaline is flowing—if he can't remember a password because he is excited or confused there is a bad situation, so there is the need to use a biometric characteristic for identification and authentication. The data that flows in the network must be secure because it gives the power of the business. Data corruption could lead to a business fall, various accidents or malfunctioning of equipments or even affecting the national security. In this paper we presented o solution for securing an industrial control network at the physical and logical layer. It is based on the modern identification technologies such as biometrics and RFID cards, two topics that have been studied in two national research project with acronyms AVPROT and AMPRENTA. The device for access control was realized as a prototype in AMPRENTA research project. In this paper we recommended to divide the factory network in security zones so another security policy could be implemented in each zone. Having such an industrial network could assure a high level of security.

References

1. Jain, L.C., Bolle, R., Pankanti, S. - *Biometrics: Personal Identification in a Networked Society,* Kluwer Academic Publishers, 1999
2. Lin, H. - *Automatic personal identification using fingerprints,* Ph.D. Thesis, 1998
3. *** - *Process network security – reference arhitecure,* Invensys – Whitepaper, 2007
4. *** - *Securing Process Control Network External Communications,* PCN Data Honeywell - Whitepaper, 2007

Securitatea rețelelor industriale pentru automatizarea proceselor

Rezumat

Asigurarea securității sistemelor de automatizare a devenit un domeniu de interes pentru lumea ştiințifică, datorită faptului că toate sistemele de automatizare sunt acum bazate pe adevărate rețele de comunicații între senzori, regulatoare şi calculatoare de proces. Sistemele automate sunt conectate la rețeaua IT a companiei şi pot fi controlate de la distanță prin Internet. In această lucrare vom prezenta câteva considerații privind securitatea accesului fizic la sistemele automate şi problematica rețelelor industriale pentru controlul proceselor.