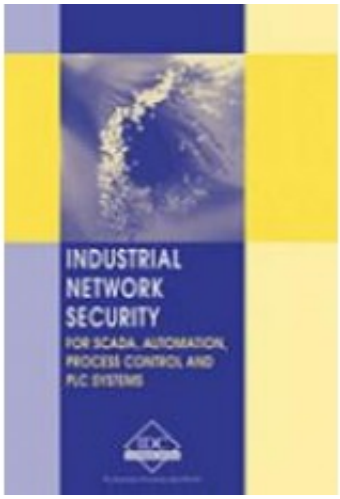
IDC Technologies - Books - 1031 Wellington Street West Perth WA 6005

Phone: +61 8 9321 1702 - Email: books@idc-online.com

NS-E - Industrial Network Security for SCADA, Automation, Process Control and PLC Systems



Price: $139.94

Ex Tax: $127.22

Short Description

This manual will give you a fundamental understanding of security in effective industrial networking and data communications technology. It will also present you with the key issues associated with security in industrial communications networks and will assist managers, system operators and industrial data communications specialists in setting up secure systems. Topics covered include: introduction and terminology; firewalls; authentication, authorization and anonymity; remote access to corporate networks; cryptography; VPN's; data security; desktop and network security; security precautions in a connected world; and internet security.

Description

This manual will give you a fundamental understanding of security in effective industrial networking and data communications technology. It will also present you with the key issues associated with security in industrial communications networks and will assist managers, system operators and industrial data communications specialists in setting up secure systems. Topics covered include: introduction and terminology; firewalls; authentication, authorization and anonymity; remote access to corporate networks; cryptography; VPN's; data security; desktop and network security; security precautions in a connected

world; and internet security.

Table of Contents
Download Chapter List

Table of Contents

First Chapter
1 An Introduction to Industrial Network Security

1 An Introduction to Industrial Network Security

Objectives

In this chapter you will learn about:

- The evolution of computer networks
- Network security and its importance
- Security in the context of industrial automation systems
- Information networks and industrial networks - the similarities and differences
- Organizational aspects of security *vis-à-vis* the technical aspects
- Network security solutions
- The need for security testing

1.1 Course overview

In this course we will take the reader through the evolution of computer networking, the basic communication principles involved, and the various types of networks. We will also address the fundamental principles behind the Internet and the TCP/IP protocol suite. We will cover the concepts of industrial networks used for control and data acquisition and the common architectures used in these networks.

We will look at the threats surrounding a network, particularly the vulnerability of industrial networks. We will learn about the ways in which these threats are addressed such as AAA (Authentication, Authorization and Accounting), data encryption, access control using routers and firewalls, and intrusion detection.

We will broadly cover the principles behind Virtual LANs and Virtual Private Networks and how they help to ensure a secure environment. We will cover the issue of wireless networks and their security issues and finally conclude with the subject of security testing.

1.2 The evolution of networking

Networking has been one of the greatest driving forces behind the growth of the computer industry. While low cost desktop computing brought the power of the digital age to millions of users, the real power of distributed computing has been unleashed by interconnecting the computers via networks, which made sharing of hardware and data resources possible. This, in turn, enabled optimal use of resources and resulted in improved Return on Investment. Simultaneously, network components and protocols were brought under active standardization initiatives, notably by bodies such as the Institution of Electrical and Electronics Engineers (IEEE) and the International Organization for Standardization (ISO) which made widespread, vendor independent interconnectivity a reality.

Networking started with simple Local Area Networks (LANs), which connected the computers of a building floor, a department of an office or a small office itself. This was followed by campus networks connecting several individual LANs spread over one or more buildings of a campus with a network backbone. This was followed by Metropolitan Area Networks (MANs) operating within a city, and by Wide Area Networks (WANs), which, as the name implies, connect networks over long distances, even on a global scale.

LANs, MANs and WANs are all configured around dedicated connections. This means that, for reliable operation, a sufficient degree of redundancy of communication circuits had to be built in. LANs traditionally do not provide redundancy since the degree of disruption is not very high and restoration through repairs is fairly easy and not very time consuming. Redundancy is, however, a common feature in industrial automation system networks as evident by the frequent use of redundant data buses. In the case of MANs and WANs, multiple routes and routers that can automatically select the best available routes are a matter of necessity. One of the main advantages of dedicated networks is the use of dedicated circuits that prevent any casual attempts at intrusion. If, at all, a breach of security occurs, it has to be largely internal. Any external attempt has to involve sophisticated equipment and a thorough understanding of

communications within the network.

1.3 What is network security?

Let us first examine the meaning of security in the context of computer networks. Network security is analogous to security in the physical world. It involves preventing an intrusion by a person or persons into an area that is not meant to be accessed by them. Just as an intrusion in the physical world is followed by theft of material goods, the network intrusion usually involves theft of data. Sometimes the motive is not theft alone, but includes vandalizing a property, either physically or intellectually. In the case of computer networks it may involve corruption of a data resource; substituting data in a database or defacing a website by putting hate messages or obscene material in place of the original content. There is, however, another dimension to network security that does not have a direct analogy in the physical world. It is analogous to a case where a thief changes the lock on a house and thus prevents the rightful owner from gaining entry. It is called ‘denial of service’ in network security parlance.

Thus, network security involves three distinct aspects:

- *Confidentiality:* ensuring that information is accessible only to those authorized to have access
- *Integrity:* safeguarding the accuracy and completeness of information and processing methods
- *Availability:* ensuring that authorized users have access to information and associated assets when required

The goal of network security is to prevent an attack on the assets of the target system and in case it cannot be prevented, to minimize the undesirable consequences of a successful attack by early detection and countermeasures.

1.4 Why has security assumed more importance in recent times?

The subject of network security has assumed importance ever since global networking in the shape of the Internet has come into widespread public use. The ease and the low cost with which data can be accessed from hosts spread across the globe, carries with it a risk of unwanted attention from pranksters, persons with malicious or criminal intentions and worse. The Internet itself has a

broader purpose, that of making information available to anyone who accesses a host. This is subject, of course, to restrictions pertaining to which hosts can be accessed, which of the contents of a specific host can be accessed and who is allowed to modify the contents of a specific host. Such architecture, however, means that anyone connected to the Internet may listen to or intercept communications and therefore can pose a potential threat, at least in theory. This is the crux of the vulnerability of the Internet.

The protection of hosts, as well as users connected to the Internet, from intrusions has been a subject of extensive research. Several ways of tackling these problems have evolved over the years and are being continually improved and refined. New vulnerabilities, however, surface as regularly as the old ones are eliminated, which means that a connection to the Internet can never be one hundred percent safe. You have to be constantly on the move to maintain the status quo, a paradox but true all the same.

Whilst a dedicated network can protect resources from the outside world, it must be appreciated that the break-in is not always external. Quite often the problem is the odd disgruntled network administrator or an insider who can be socially manipulated. There could also be someone who has been bribed by a competitor in exchange for business secrets...

1.5 Security in the context of industrial automation systems

The use of computer based systems for industrial automation is now commonplace. These can be broadly divided under the following classifications:

- Automation systems such as Programmable Logic Controllers (PLCs), several of which are networked to form an industrial automation network. A Distributed Control System (DCS) is a higher-end industrial automation network used for the control of more complex, special purpose equipment and processes and often uses proprietary hardware and software, unlike a PLC based network
- Supervisory Control And Data Acquisition (SCADA) systems, which collect data from geographically dispersed resources and allow remote monitoring and control usually used in utility systems such a electric power and water supply

A new scenario has been emerging in the field of automation networks. These systems traditionally used proprietary hardware and software. These were quite secure from an intrusion point of view. But, as in the case of general computing hardware, open systems have been catching on in the industrial network arena too, primarily driven by the low cost of ownership of the open hardware and software. The need for remote monitoring of infrastructure systems has been driving the developments in this field, with the result that many systems are required to provide remote access from, to and through the Internet. Given the fact that, historically, network security was never an issue in the industrial automation segment by virtue of its closed nature, the possibility of intrusion is very real in modern industrial networks that provide connectivity to public networks.

The terrorist attack of September 11, 2001 on US targets has given this issue a totally new dimension. In the USA, several of the utilities such as power distribution, power generation, water supply systems, gas distribution systems etc. are connected to the Internet and use the networks to gather status information through SCADA systems from remote locations. The effects of a break-in could range from minor inconvenience to widespread disruption of operations over a large geographical area and, in worst-case scenarios, substantial delay or even failure to restore the affected system.

1.6 Information networks vs industrial networks - the similarities and differences

We will deal extensively with the security of general IT networks and business networks. This is because the underlying principles are valid in both business networks and automation networks. Consider these factors:

A business network and automation network:

- Have the same owners and general goals
- Use the same technologies (Ethernet, TCP/IP, Windows, etc.)
- Share common facilities
- Are interconnected at one or more points

Thus, the security practices adopted in IT networks are often quite valid for automation systems.

But then there are some differences between the systems. For example:

- Industrial networks place stress on reliability. Hardware is therefore designed with this aspect in mind
- Performance requirements such as response time are far more important in industrial networks compared with their business counterparts
- Operating systems of industrial networks are quite often proprietary and not the usual commercial OS, which, if at all used, is limited to specific segments of the system such as database management or HMIs
- The security architecture can be different because of the special needs of industrial automation systems. For example, safety of humans and machinery is a prime consideration in industrial automation systems, whereas delivery of services takes priority in business networks
- Risk management goals are different in view of the functional differences between the two categories of systems

1.7 Organizational issues

One cannot solve security problems by depending on technology alone. The solution relies, instead, on appropriate controls based on a clearly defined security policy. To determine the security policy of an organization, it needs to think about the business, examine the risks, and place a value and a probability on the risks. It needs to budget, find the best way to spread the available money across the security options, and accept the unpalatable fact that the solution is not going to be perfect. The implementation needs to be planned, and the entire organization (including management as well as the users) need to understand and cooperate in the security measures that they are expected to follow. We will look at this aspect in detail in the chapter titled ‘A comprehensive approach to network security’. These principles are applicable to business networks as well as automation networks.

1.8 Network security solutions

Network security threats are countered using the following approaches:

- Authentication, Authorization and Accounting (AAA)
- Encryption of data

- Access control, boundary routers, firewalls and filtering
- Remove Div Intrusion detection and response

We will review these in detail in later chapters. Two other technologies need to be mentioned in this regard. One is the Virtual LAN (VLAN) and the other is the Virtual Private Network (VPN). Internal security violations can be reduced by using VLANs to provide a degree of control not usual in a normal LAN. Security was not, however, the primary objective of the VLAN; it was rather the need to reduce congestion of the networks.

The breach of closed LANs became a possibility when Remote Access Systems (RAS) came into use, allowing authorized users to access corporate systems from outside the dedicated network. RAS therefore had to provide adequate safeguards for authenticating remote client connections. RAS is based on direct dial-in access to a network and uses the PSTN (Public Switched Telephone Network) for communication. With this method, connectivity from remote locations involves long distance dialing, which is both expensive and not very stable. This gave rise to the emergence of remote connectivity using the communication infrastructure of the Internet. The result was Virtual Private Networks or VPNs. VPNs provide access to both remote users and remote networks; for example a remote branch office LAN connecting to the LAN at Corporate HQ.

There were two issues to be addressed in this approach. The first is the need to convert the native format of data transmission protocol used in the network to that of the Internet viz., TCP/IP and vice-versa. The second is that of security. VPNs, which use the Internet infrastructure, have to guard against the possibility of security incidents and secure the communications in the open routes against eavesdropping and interference. Since VPN communications are permitted only between specific remote hardware, which is readily identifiable, the task of security is made easier.

1.9 Wireless networks

Another technological wave in networking is the fast spreading use of wireless networks, both for general computing and in automation systems. Wireless networking first came into being for connecting remote users to a LAN but without using a telephone connection. The second requirement was flexible connectivity

to handheld devices or portable computers used in warehouses, construction sites etc., where it would be impossible to provide LAN connectivity outlets by conventional wiring methods. Wireless has also been the medium of choice in large dispersed industrial networks and in SCADA systems for the purpose of remote data acquisition and control.

Wireless networking is now being extended to Internet connectivity as well. Wireless Internet connectivity is offered to users at public places such as shopping malls and airports. Wireless has always been easier to intercept as anyone with the right equipment can listen in without the need for physical connectivity, as is the case with traditional networking over copper or fiber. So now we have the risks of the Internet, added to the vulnerability of wireless transmission. The same is also true for industrial networks such as those of large geographically dispersed utility systems, which use wireless communication extensively for data transfer between the control station and Remote Terminal Units (RTUs). Security of wireless networking has been, of late, receiving a lot of attention and standards are being evolved keeping in view the security needs. The same general principles such as authentication, encryption and access control used for security of conventional networks are also applicable to wireless networks.

1.10 Security testing

Finally, it is not enough that an organization has the best security policies in place and the most expensive hardware and software to back up these policies. It needs to ensure that everything works as intended and really protects the integrity of the data resources it is supposed to. This is ensured by actual testing, which should occur throughout the life cycle of the system, especially after any major change to the network architecture, hardware, or operating system. Security testing is covered in detail in the final chapter.