

## White paper

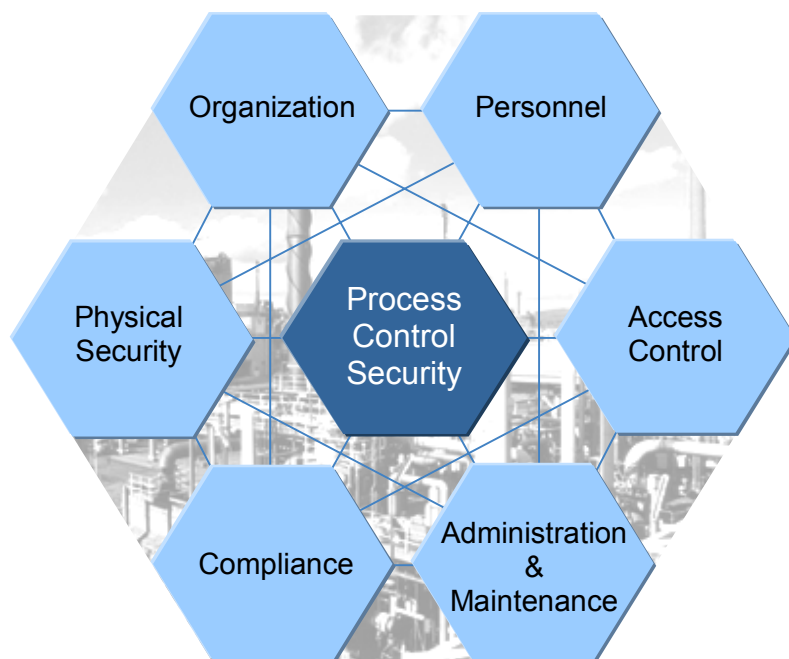
# IS Security Considerations for Automation Systems

### Abstract

The security of computer systems in general, and of manufacturing and control systems in particular, becomes increasingly critical as different networks are connected and systems are integrated in a collaborative manufacturing environment. For manufacturing and control systems the potential impact of an attack may be more serious than for computer systems in general. Users of manufacturing and control systems need to pay correspondingly increased attention to these issues.

Security measures aim at protecting the confidentiality, integrity, and availability of a computer system from being compromised through deliberate or accidental attacks. Similar to process and safety improvements, network security improvement needs to be a continuous activity.

This white paper provides background information and a general overview of different elements of information system security, with specific emphasis on how it applies to process control security. Different security measures that should be considered when an automation system is connected to external networks of different kinds are discussed, including connections to general purpose IS and corporate networks, remote connections, and wireless connections.



**NOTICE**

*This document and parts hereof must not be reproduced or copied without written permission from ABB and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.*

*The information in this document is subject to change without notice, and should not be construed as a commitment by ABB. ABB provides no warranty, express or implied, for the information contained in this document, and assumes no responsibility for the information contained in this document or for any errors that may appear in this document.*

*The purpose of this document is to discuss possible security measures that a user of an automation system may consider to apply. The described measures are not necessarily complete or effective for a particular application and installation.*

*In no event shall ABB be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB be liable for incidental or consequential damages arising from use of any software or hardware described in this document.*

*The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license.*

*Copyright © 2005 ABB. All rights reserved.*

**TRADEMARKS**

*Registrations and trademarks used in this document include:*

*Windows Registered trademark of Microsoft Corporation.*

*Industrial IT Trademark of ABB.*

**WARNING AND CAUTION NOTICES**

*This document includes Warning and Caution notices where appropriate to point out safety related or other important information.*

- *A Warning notice indicates the presence of a hazard, which could result in personal injury or death.*
- *A Caution notice indicates important information or warning related to the concept discussed in the text. It might indicate the presence of a hazard, which could result in corruption of software or damage to equipment and/or property.*

*Although Warning hazards are related to personal injury and Caution hazards are associated with equipment or property damage, it should be understood that operation of corrupt software or damaged equipment could, under certain operational conditions, result in degraded process performance leading to personal injury or death. Therefore, comply fully with all Warning and Caution notices.*

**CONTENTS**

<b>1. ABOUT THIS DOCUMENT .....</b>	<b>4</b>
<b>2. BACKGROUND.....</b>	<b>5</b>
<b>3. APPROACHES TO IS SECURITY.....</b>	<b>6</b>
<b>4. THE 800xA SYSTEM NETWORK ARCHITECTURE .....</b>	<b>8</b>
4.1 Overview.....	8
4.2 The 800xA system network.....	9
<b>5. AUTOMATION SYSTEM NETWORK SECURITY .....</b>	<b>10</b>
5.1 Network security zones.....	10
5.2 Isolated automation system.....	12
5.3 Connecting to a general purpose IS network.....	13
5.4 Connecting to a corporate network.....	14
5.5 Software updates.....	16
5.6 Remote connections .....	17
5.6.1 Remote access.....	17
5.6.2 Site-to-site connections.....	19
5.7 Wireless communication .....	20
<b>6. CONCLUSION.....</b>	<b>21</b>

## 1. ABOUT THIS DOCUMENT

This document presents an overview of information system (IS) security, and describes measures and practices that a user of an automation system may want to consider:

- Chapter 2 explains why IS security is something that should be taken into account.
- Chapter 3 provides an overview of different elements of IS security in general.
- Chapter 4 describes the network architecture that is used in the Industrial IT Extended Automation System 800xA.
- Chapter 5 presents different network security measures that a user may want to consider when an automation system is connected to external networks of different kinds.

For further studies of IS security in general a wide range of literature is available. For security in manufacturing and control systems in particular, several standardization activities have been initiated recently. Examples are ISA SP99 “Manufacturing and Control Systems Security” and IEC SC65C WG13 “Industrial-Process Measurement and Control, Cyber Security”.

### **Warning! Caution!**

While general network security measures are described in this document, users of an automation system must assess the risks of their particular application and installation. The described security measures represent possible steps that a user of an automation system may want to consider based on such a risk assessment. The risk assessment, as well as the proper implementation, configuration, installation, operation, administration, and maintenance of all relevant security related equipment, software, and procedures, are the responsibility of the user of the automation system.

The purpose of this document is to discuss possible security measures that a user of an automation system may consider to apply. The described measures are not necessarily complete or effective for a particular application and installation.

## 2. BACKGROUND

Providing and managing enterprise-wide information system (IS) security is a moving and dynamic target, complicated by continuous technical, organizational, and political changes, global interconnections, and new business models such as Internet-based e-commerce. IS security is a complex challenge requiring procedural as well as technical measures.

The number of security incidents reported to CERT/CC<sup>1</sup> increased significantly over the last few years, from a few thousand in 1998 to well over a hundred thousand in 2003. Incidents include directed and malicious intrusion attempts as well as unintentional security breaches done by mistake. Besides the threats from viruses and hackers breaking into computer systems, there is a growing concern over the possibility of network based terrorist attacks against infrastructure and critical process industries.

Many of the reported incidents were initiated by people with legitimate access to the network. In general, these attacks are the most difficult ones from which to protect a system, because insiders (or former insiders) are the most likely persons to have access to passwords, codes, and systems, and to have knowledge about the nature of the system and its potential vulnerabilities. Recently, however, the share of externally sourced incidents has increased drastically<sup>2</sup>, in particular in the form of virus and worm infections. In many cases, virus and worm infections are caused by connecting a portable computer or storage device that has previously been connected to an infected environment.

There is no single solution or technology for network security that fits the needs of all organizations and applications. While basically all computer systems are exposed to intrusion attempts, the potential consequences of such attempts are vastly different for different types of applications. For manufacturing and control systems in particular, the potential impact of an attack may include, for example, endangerment of public or employee safety, violation of regulatory requirements, loss of proprietary or confidential information, loss of production, damage to equipment, and loss of public confidence.

IS security measures aim at protecting the confidentiality, integrity, and availability of a computer system from being compromised through deliberate or accidental attacks. This is accomplished by implementing and maintaining a suitable set of controls to ensure that the security objectives of the organization are met. These controls should include policies, practices, procedures, and organizational structures, as well as software and hardware implemented security functions.

The security measures that are applied to a specific installation should be proportional to the assessed risk in terms of probability of a successful attack and the potential consequences. For a small system with a few users controlling a non-critical process this risk is obviously smaller than for a large system spanning multiple sites with safety critical processes in several countries and continents and thousands or even tens of thousands of users.

100% security is not possible to achieve in an interconnected environment. A network that is arranged with state-of-the-art security measures may still be vulnerable through connections to the networks of suppliers, contractors or partners. Even a network that is perceived as being totally isolated from the outer world is vulnerable to security intrusions from different sources, such as the occasional connection of portable computers or unauthorized installation of software.

---

<sup>1</sup> CERT, Computer Emergency Response Team Coordination Center is an institute run by the Carnegie Mellon University

<sup>2</sup> Byres, Eric; Lowe, Justin; The Myths and Facts behind Cyber Security Risks for Industrial Control Systems. VDE Congress 2004

### 3. APPROACHES TO IS SECURITY

A key element in implementing and maintaining the security of a computer system is the establishment of an adequate IS security policy. This should be based on an analysis and assessment of the functional needs and security objectives of the organization, current and planned network structures and information and control flows, risks in terms of probability of different types of attack and potential consequences, and available technical security solutions.

Besides plans for how to avoid risks, a security policy should also include plans for regular audits of the IS security, for training of personnel and partners, and for incident response, including how to recover from potential disasters. The distribution of responsibilities between different parts of the organization should be defined. A tightly managed security administration, with enforcement of strong passwords and good user practices as well as regular implementation of all vendor recommended updates for operating systems, application software, and security related software, is obviously also required.

A generally recommended approach to IS security is the onion approach, also known as “defense in depth”. The inner layers, or zones, of a network, where communication interaction needs to flow freely between nodes, are referred to as *trusted*. Trusted network zones should be kept small and independent. They need to be physically protected, i.e. physical access to computers, network equipment, and network cables, must through physical means be limited to authorized persons. When connecting a trusted network zone to outer network zones, additional layers of security measures should be applied, isolating the network zones from each other and providing additional security for the network as a whole.

Firewalls, gateways, and proxies are used to control network traffic between zones of different security levels, and to filter out any undesirable or dangerous material. Traffic that is allowed to pass between zones should be limited to what is absolutely necessary, because each type of service call or information exchange translates into a possible route that an intruder may be able to exploit. Different types of services represent different risks. Incoming e-mail, as an example, represents a very high risk.

Security mechanisms should not only include defensive and preventive means, but also means for detection and reaction. By continuously monitoring a system for intrusion attempts, users can be alerted to potential threats and take suitable actions, such as isolating an inner network zone from outer zones.

The security policy should be based on the principle of least privilege and compartmentalization, i.e., every application, user, or subsystem should be restricted to the minimum number of rights for the minimum number of resources that is necessary to fulfill its purpose. Network access to functions that are not explicitly required should be disabled. This reduces the possibilities that an attacker can exploit and limits the damage in case an intrusion attempt is successful.

All computer systems should be scanned for viruses at regular intervals. A virus checker of good reputation should be used and it should be updated regularly. However, when a virus is found, the damage has probably already been done. For a mission critical system it is therefore more important to effectively prevent viruses from being introduced into the system than to run frequent virus checks.

Virus checking has a significant impact on performance and response times on any computer system. For computer systems that are used for real-time applications, such as process control systems, virus scanning should therefore be done at times when normal system activity is low.

Protecting a computer system from intrusion and virus infection typically requires a range of security measures to be applied. Such measures may include (but are not necessarily limited to)

- Physically protect the system, including all nodes, network equipment and network cables, from access by any unauthorized personnel
- Isolate the system from other networks, allowing access only through properly configured and sufficiently hardened firewalls
- Restrict the number and types of services and information exchange that are allowed to pass through firewalls to the minimum that is needed to fulfill operational requirements
- Harden the system by removing or disabling all unnecessary network connections, services, file shares, etc., and ensure that all remaining functions have appropriate security settings
- Allow only authorized users to log on to the system and enforce strong passwords that are regularly updated
- Continuously maintain the definitions of authorized users, user groups, and access rights, to properly reflect the current authorities and responsibilities of all individuals at all times
- Do not allow the installation of any unauthorized software in the system
- Carefully scan portable computers and storage media for viruses and other malicious software before they are allowed to be connected to the system
- Carefully scan all software updates for viruses and other malicious software before introducing them to the system
- Configure firewalls to scan e-mail for viruses and to filter out active content
- Continuously monitor the system for intrusion attempts
- Regularly scan the system for viruses
- Continuously update the system with all relevant and vendor recommended security updates, including updates to operating system, applications, and security related software
- Define and maintain plans for incident response, including how to recover from potential disasters
- Regularly review the organization as well as technical systems and installations with respect to compliance with security policies, procedures, and practices.

For mission critical systems, such as manufacturing and control systems, it may be appropriate to prevent the use of functions that are known as common infection routes, for example e-mail, instant messaging, and Internet browsing.

## 4. THE 800xA SYSTEM NETWORK ARCHITECTURE

### 4.1 Overview

The System 800xA network architecture is illustrated in Figure 1:

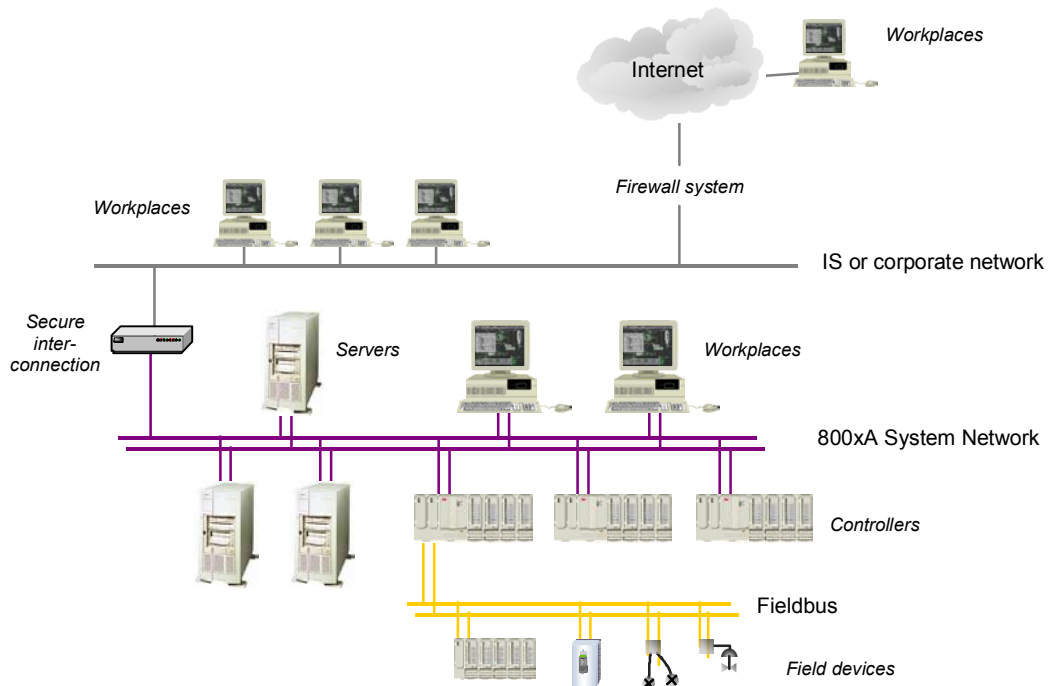


Figure 1 Conceptual communication network configuration

The *800xA system network* is used for communication between *workplaces*, *servers* and *controllers*. It is a local area network (LAN) that is optimized for high performance and reliable real-time communication with predictable response. Servers run software that provides system functions. Workplaces run software that provides various forms of user interaction. Controllers are nodes that run control software.

*Fieldbuses* are used to interconnect field devices, such as I/O modules, smart sensors and actuators, variable speed drives, PLCs, or small single loop devices, and to connect these devices to the system, either via a controller, as indicated in Figure 1, or directly to a server.

The automation system network can be connected to an IS or corporate network via some form of secure network interconnection. The nature of the secure interconnection depends on the nature of the plant network and the level of security that is required for the automation system – it may actually be a set of interconnected computers and devices that cooperate to provide the level of security that is required in a particular installation.

Further connection of the plant network to the Internet or any other type of external network should be performed in accordance with adequate network security practices.

#### 4.2 The 800xA system network

The 800xA system network is based on TCP/IP over Ethernet. The routing protocol that is used is RNRP (Redundant Network Routing Protocol). This protocol supports redundant network configurations based on standard network components. Detection of a network failure and switch over to the redundant network takes less than one second, with no loss or duplication of data. A redundant network consists of two fully separate Ethernet networks. It operates as a standard TCP/IP network, with the addition of RNRP, which works as follows:

Each node cyclically sends a routing vector as a multicast message on both networks. The routing vector indicates which other nodes this node can see on the network. Each node uses received routing vectors to build a table, listing which nodes can be reached on which of the two networks. One of the networks is designated as the primary network, the other as the back-up network. As long as the primary network works, all traffic is sent on that network – only routing vectors are sent on the back-up network, verifying that it works.

The 800xA system network is a private IP network. IP addresses are static, and must be selected according to a scheme defined by RNRP. Each node has two IP addresses, one on the primary network, and one on the backup network.

Authority checking in System 800xA is based on Windows security. It is strongly recommended that the automation system network is defined as a separate Windows domain, i.e. it should not be part of a larger domain, such as a corporate network domain.

## 5. AUTOMATION SYSTEM NETWORK SECURITY

This chapter provides an overview of different network security considerations that should be considered in different situations, depending on to what extent the automation system is connected to external networks and the nature of such networks.

### 5.1 Network security zones

IT resources vary in the extent to which they can be trusted not to be compromised. A common network security architecture is based on a layered approach that uses zones of trust to provide increasing levels of security according to increasing security needs. Each zone is inside the next, leading from the least trusted to the most trusted. Connections between the zones are only possible through secure interconnections, such as a firewall or a system of layered firewalls.

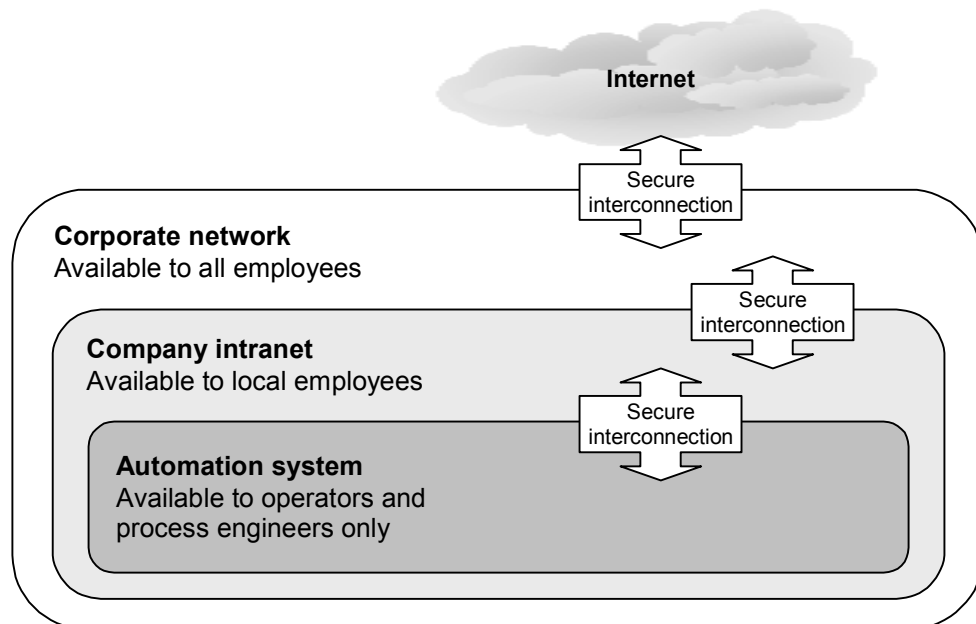


Figure 2 Network security zones

This approach is similar to protecting a castle using multiple walls that form concentric rings with the castle at the center, and with only one gate in each wall and a security guard watching each gate. It is hard for people in outer rings to attack people in inner rings, but less hard if they are in the same ring. Thus those in the same ring need to have the same minimum level of trustworthiness.

Figure 2 shows three security zones, but the number of zones does not have to be as many as three or as few as three. The use of multiple zones allows access between zones of different trust levels to be controlled to protect a resource from attack by a less trusted one.

Even if a network zone is regarded as trusted an attack is still possible, by a user or a compromised resource that is inside the trusted zone, or by an outside user or resource that succeeds to penetrate the secure interconnection. Trust therefore depends upon the types of measures taken to detect and prevent compromise of resources and violations of the security policy.

To establish a certain level of trust in a zone requires that all devices in the zone be certified to have a certain minimum level of security as determined by the organization's security policies. For the inner and most trusted zones, this may include (but is not necessarily limited to) the following:

- A trusted network zone should be kept relatively small and independent from other network zones. It should form its own network domain, and be administered from the inside.
- All equipment should be physically protected, i.e. physical access to computers, network equipment and cables, controllers, I/O systems, power supplies, etc., should through physical means be limited to authorized persons.
- Only authorized users should be allowed to log on to the system. Users should not have more privileges than they need to do their job.
- Installation of non-authorized software should be prohibited, and temporary connection of portable computers should be restricted. If portable computers need to be connected, e.g. for service or maintenance purposes, they should be carefully scanned for viruses immediately before connection.
- All CDs, DVDs, and other removable data carriers, and files with software or software updates, should also be checked for viruses before being introduced to the trusted zone.
- When connecting a trusted network zone to outer networks, the networks should be isolated from each other by means of a properly configured secure interconnection, that blocks everything except traffic that is explicitly needed. The network should be monitored for intrusion attempts.
- All computers should be regularly scanned for viruses, and kept up to date with relevant and vendor recommended security updates.
- The compliance with security policies, procedures, and practices should be reviewed regularly.

## 5.2 Isolated automation system

For a “traditional” automation system configuration that is not connected to any “external” network, network security is primarily a matter of physically protecting the automation system. The security measures described in section 5.1 should be applied as relevant.

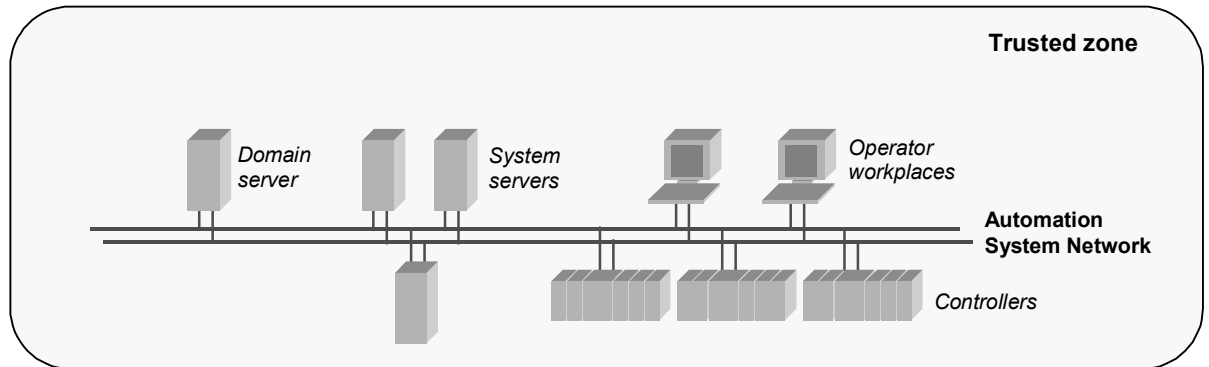


Figure 3 Isolated automation system

Servers and workplaces that are not directly involved in the control and supervision of the process are preferably connected to a subnet that is separated from the automation system network by means of a router, as shown in Figure 4. This makes it possible to better control the network load and to limit access to certain servers on the automation system network. Note that servers and workplaces on this subnet are part of the trusted zone and thus need to be subject to the same security precautions as the nodes on the automation system network.

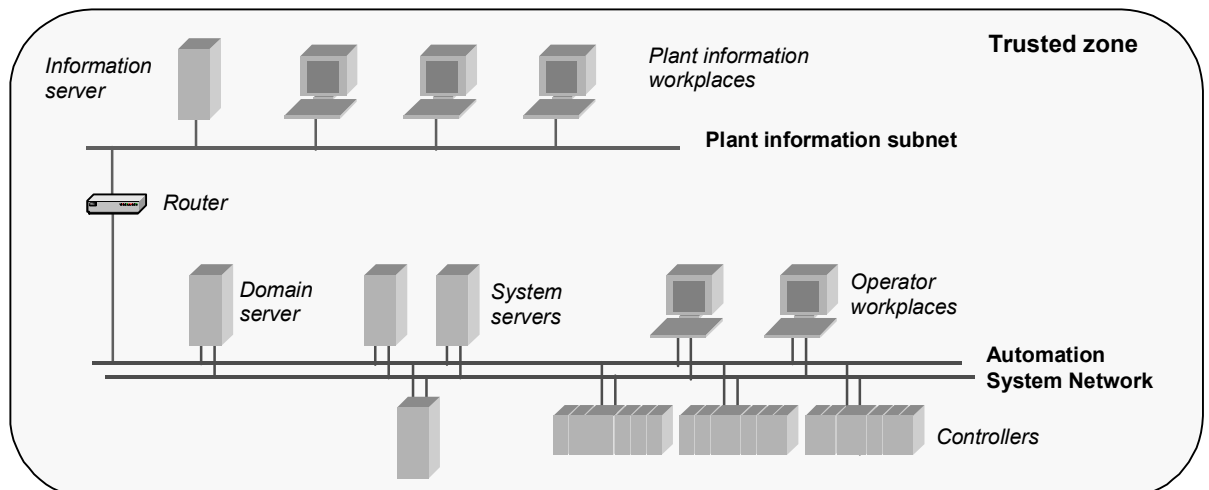


Figure 4 Plant information network connected to an automation system

### 5.3 Connecting to a general purpose IS network

For the purposes of process control security, a general-purpose information system (IS) network should not be considered a trusted network. It is therefore a different security zone, and it should be separated from the automation system by means of a firewall, as illustrated in Figure 5. The IS and automation system networks should form separate domains.

If the IS network is connected to some form of external network such as the Internet, care must be taken to protect it from malicious attacks. There are many different ways to do this, for example by means of a so-called demilitarized zone (DMZ). Web servers and other servers that are to be accessible from the external network are placed on a separate network that is isolated from both the IS network and the external network by means of firewalls.

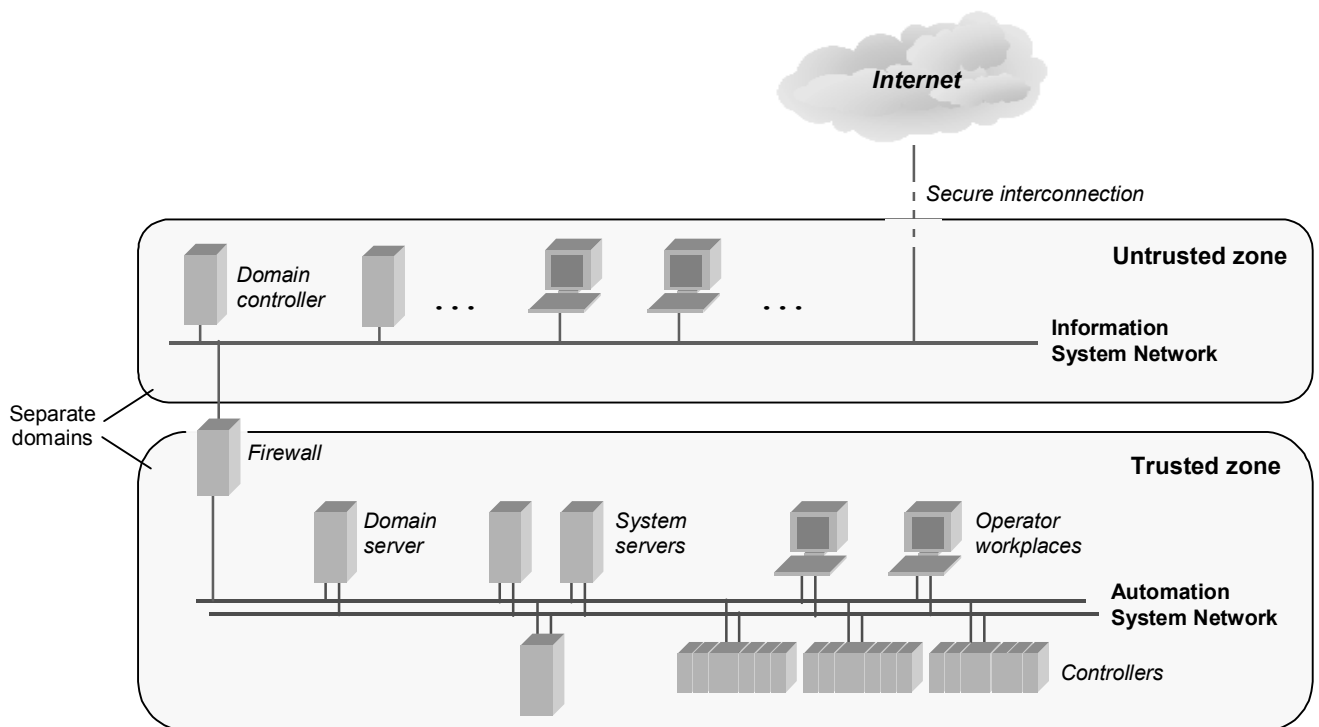


Figure 5 Connecting an automation system to a general purpose IS network

The firewall that connects the IS network to the automation system should be configured to allow access only to selected servers and services in the automation system, and only from selected nodes in the automation system to selected services and nodes on the IS network. Workplaces in the automation system should not be used for accessing the Internet or for incoming e-mail.

To ensure that intrusion attempts are detected as early as possible, the firewall should include an intrusion detection system. It should be possible to physically isolate the automation system from the IS network in the event an intrusion attempt is detected. This could, for example, be arranged by means of electrical switches that disconnect the network connections or the power supply to the firewall or to network equipment connecting the firewall to the automation system.

If security requirements are high a more elaborate isolation of the automation system from the IS network, as indicated in section 5.4, should be considered.

## 5.4 Connecting to a corporate network

As the number of users in the IS network grows, so do process control security concerns. A corporate network with thousands or even tens of thousands of users must, from a process control security perspective, be regarded as potentially as hostile as, for example, the Internet.

For the automation system the security measures described in section 5.1 should be applied. For the corporate network, however, it is reasonable to assume that portable computers will be connected and unauthorized software will be installed, even if this is prohibited by corporate policies. Since the network typically spans several sites or even countries, strict physical protection of all involved network equipment is difficult or impossible to implement and maintain.

In these cases, the automation system should be protected from the corporate network in a similar way as the corporate network is protected from e.g. the Internet. Figure 6 below indicates how this secure interconnection could be organized.

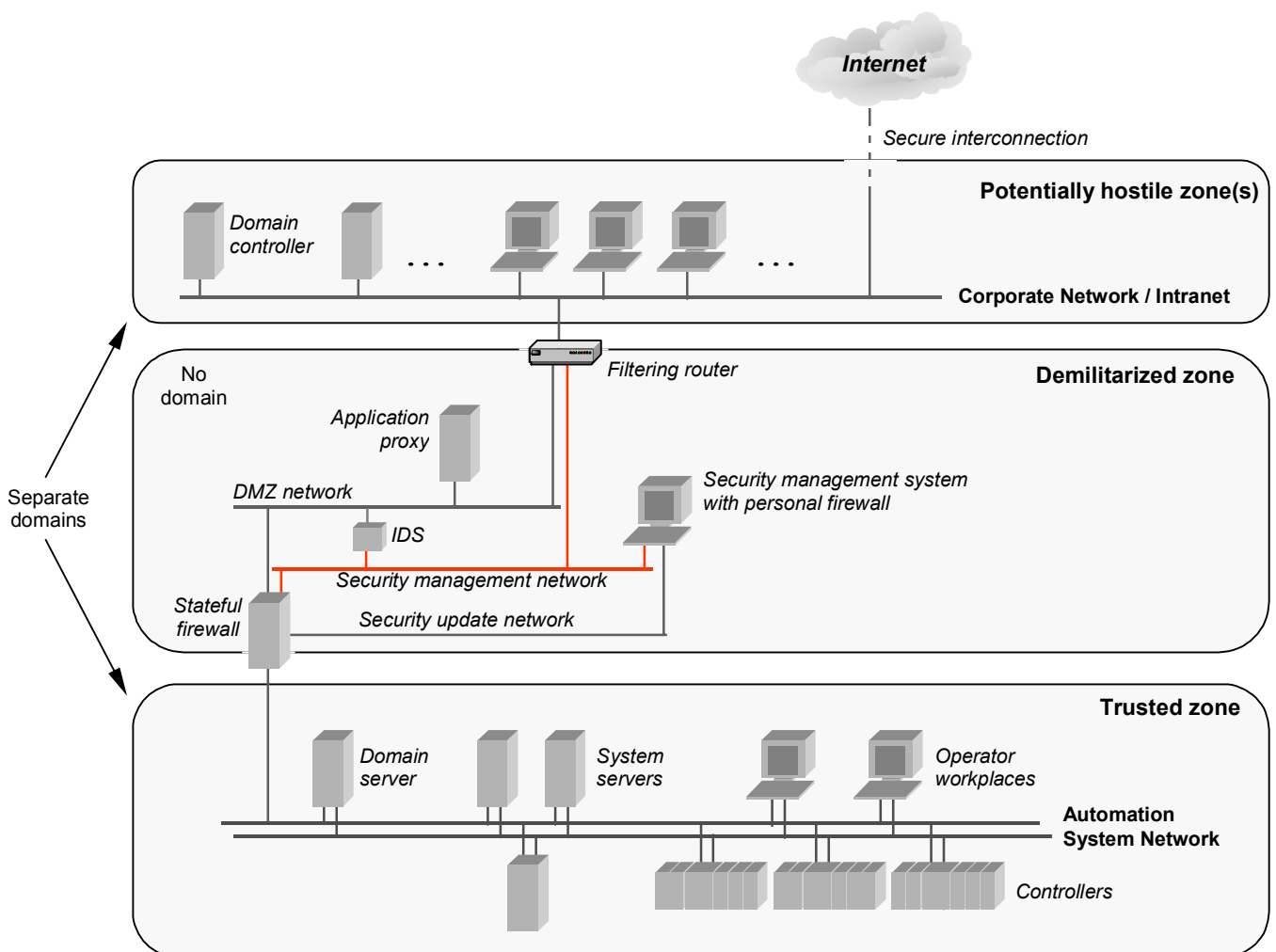


Figure 6 Connecting an automation system to a corporate network

The network between the two firewalls in Figure 6 forms a so-called demilitarized zone (DMZ). A filtering router forms the border towards the corporate network, while a statefull firewall interfaces to the automation system network. An application proxy is placed on the DMZ network. This proxy represents the servers in the automation system that shall be accessible from the corporate network. Additional security may be achieved by using a separate proxy server for each additional service that is exposed in this way. This principle makes it possible to configure each proxy server as secure as possible with respect to the service it provides, and prevents an attacker from using vulnerabilities in one service to attack another.

Several automation system installations at the same geographical site can be connected to the corporate network via separate firewalls through the same DMZ.

The firewalls and proxies should be configured to allow access from the corporate network to selected servers and services in the automation system only, and only from selected nodes in the automation system to selected services and servers in the IS network.

The automation system should be a separate domain, which should be administered from the inside. No domain should be defined for the DMZ, thus making it more difficult to penetrate.

To ensure that intrusion attempts are detected as early as possible, the firewalls and the DMZ network should include intrusion detection systems (IDS).

Workplaces in the automation system network should not be used for freely accessing the Internet or for incoming e-mail.

A separate security management system should be used to supervise the firewalls and intrusion detection systems. It should be connected to management ports of firewalls and intrusion detection systems through a security management network, which should be a separate non-routed screened subnet. The security management system should be able to collect logs from the firewalls and intrusion detection systems, analyze these and generate an alarm if it concludes that there is an attempted intrusion occurring.

It should be possible to physically isolate the automation system from the corporate network in the event an intrusion attempt is detected in the DMZ. This could for example be arranged by means of electrical switches that disconnect the network connections or the power supply to firewalls and network equipment in the DMZ network.

## 5.5 Software updates

The automation system and all related security equipment should be kept up to date with relevant software updates, including updates to operating systems, security related software, automation system software, libraries, and applications.

For an automation system that is not connected to external networks (section 5.2), software updates are typically done via CD or DVD. Care should be taken to verify that the CD/DVDs are of proper origin and do not contain viruses.

In cases where the automation system is connected to an external network (sections 5.3 and 5.4 above), updates can also be downloaded via the external network. The following is an example of a process that could be used.

- The system administrator for the automation system installation, or a central engineering department, makes the updates available on a dedicated distribution server on the office or corporate network, by installing them from CD/DVD or by downloading them from a trusted server, e.g. on the Internet.
- The authenticity of the origin and integrity of the content should be verified, e.g. by means of certificates and digital signatures, and all files should be scanned for viruses before they are made available on the distribution server. Preferably the files should then be protected with a digital signature.
- The files are then pulled from the distribution server through the interconnection by a system engineer or administrator working from an engineering workplace inside the automation system network zone
- Antivirus software installed on nodes in the automation system could be configured for automatic updates of virus signature files from a dedicated distribution server in the IS or corporate network, where they are made available in the same way as SW updates.

Also firewalls and intrusion detection systems need to have their software and rule-bases regularly updated. In the configuration described in section 5.4 above, this gets a bit more complex. The following is an example of a process that could be used (refer to Figure 6 above):

- The person who is responsible for managing the security installation regularly either creates rules or downloads them together with relevant software updates from some secure source. The rule set and software updates should then be protected with a digital signature and made available on a distribution server, on the corporate network.
- The updates are then pulled from the distribution server through the interconnection by the security system manager working from the security management system in the demilitarized zone. In the example this network traffic passes through the corporate network, the filtering router, the DMZ network, the stateful firewall, and the security update network (see Figure 6).
- After having verified the digital signatures of the updates, the security system manager updates the firewalls and IDS systems through the security management network.

## 5.6 Remote connections

Connecting one or several computers remotely to a network typically involves using links across shared or public networks, such as a company intranet or the Internet, or a dial-up phone line. Special measures are required to protect such communication from being observed, intercepted, modified, or falsified.

There are two main scenarios where remote connections to an automation system may be required.

- *Remote access* – situations where a workplace client is remotely located
- *Site-to-site connections* – Situations where an automation system is split on two or more geographical sites.

In general, remote connections should be set up with the highest level of security that the organization can support. This should always include strong authentication, and if possible include the exchange and verification of certificates. Remote access policies should be set restrictively, allowing only the minimum number of rights for the minimum number of remote users that are necessary.

The availability of a remote connection that may cross public networks is obviously lower than that of an automation system network, which is physically protected and often fully redundant. Remote connections should therefore not be used for safety or mission critical communication.

### 5.6.1 Remote access

In certain situations it may be necessary to connect a remote workplace client to an automation system, either permanently to provide access to certain functions from remote workplaces, or temporarily, e.g. to allow specialists to access the system for support and maintenance. The connection can be established as a dial-up connection or as a Virtual Private Network (VPN).

Dial-up connections utilize the telecommunications infrastructure:

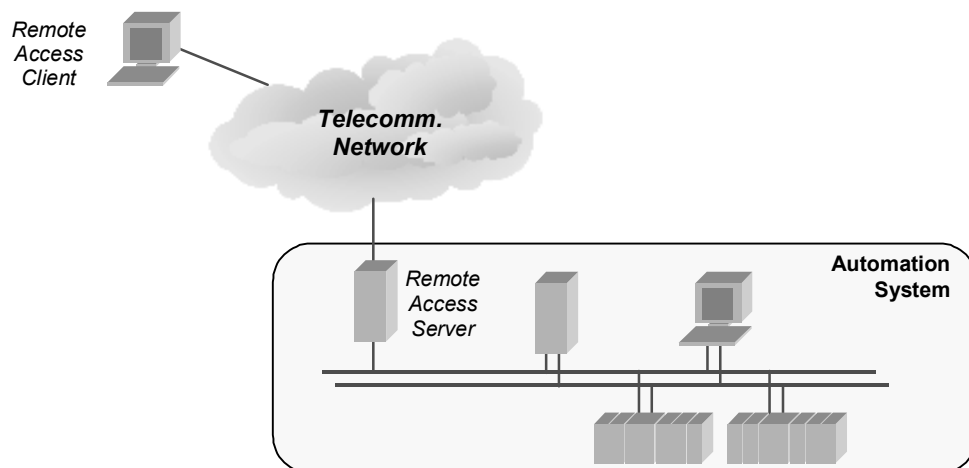


Figure 7 Remote access – dial-up connection

There are several technical solutions available for dial-up connections. The following are examples of solutions that can be configured to provide an appropriate level of security:

- Temporarily Enabled Dial In – the remote user dials in to the system, but the modem connection is disabled when there is no intended use, either physically by switching it off, or by software means.
- Dial In with Callback – the remote user dials in to a server in the system, which calls back to one of a limited set of pre-defined phone numbers.
- Dial Out – the connection is initiated from inside the automation system.

If dial-up connections are used, there should be procedures in place to ensure that all such connections conform to the security policy, and to regularly search the system for unintentionally enabled dial-up access points. An enabled access point that is left behind, e.g. after engineering or system maintenance activities, represents a vulnerability that can easily be found – attackers use automated tools that search for enabled dial-up access points.

A Virtual Private Network (VPN) connection is an extension of a private network across shared or public networks, such as a corporate network or the Internet. By encapsulating and encrypting data, the VPN emulates a private point-to-point link. The VPN connection thus forms a tunnel for secure communication between endpoints on either side of the shared or public network.

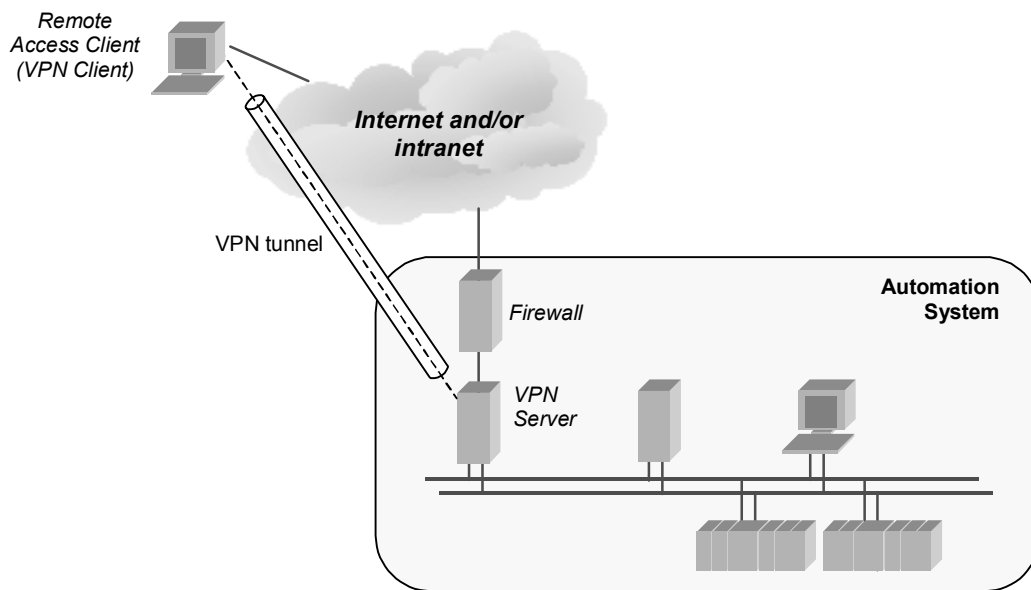


Figure 8 Remote access – VPN connection

A remote access client initiates a VPN connection to a VPN server that is on-site. For mutual authentication, the client authenticates itself to the VPN server, and the VPN server authenticates itself to the calling client. The VPN server can be placed either on the inside (as in Figure 8) or on the outside of the firewall. Placing it on the inside makes configuration of the firewall somewhat less complex. Both alternatives are generally considered adequate from a security standpoint, as long as strong authentication is used.

Regardless of how a remote client computer is connected to the automation system, the net effect is that it becomes a member of the automation system. The remote computer should therefore be secured in the same way as computers that are inside the automation system trusted zone. This includes being updated to the latest operating system security patch level, and running approved software only, including anti-virus software with updated virus signature files. The remote computer should not be actively connected to other networks, and it should not be left unattended while the remote connection is enabled.

Access rights given to remote users should be as restrictive as possible. However, for remote support, the required privileges may be quite extensive, possibly even including administrator rights. There is also a certain risk that the connection is broken during a remote support session, leaving the system in an undefined or undesirable state. The benefits of remote support should therefore in each case be carefully weighed against the potential risks, and local people should always be available to take corrective actions in case something should go wrong.

### 5.6.2 Site-to-site connections

In situations where an automation system is split on two or more geographical sites, the different local area networks need to be connected over some form of wide area network. This can be accomplished by means of private or leased lines, but a more economical alternative may be to use a VPN connection over a shared or public network. This is referred to as a site-to-site (or router-to-router) VPN connection. To the routers, the VPN tunnel serves as a data-link layer connection.

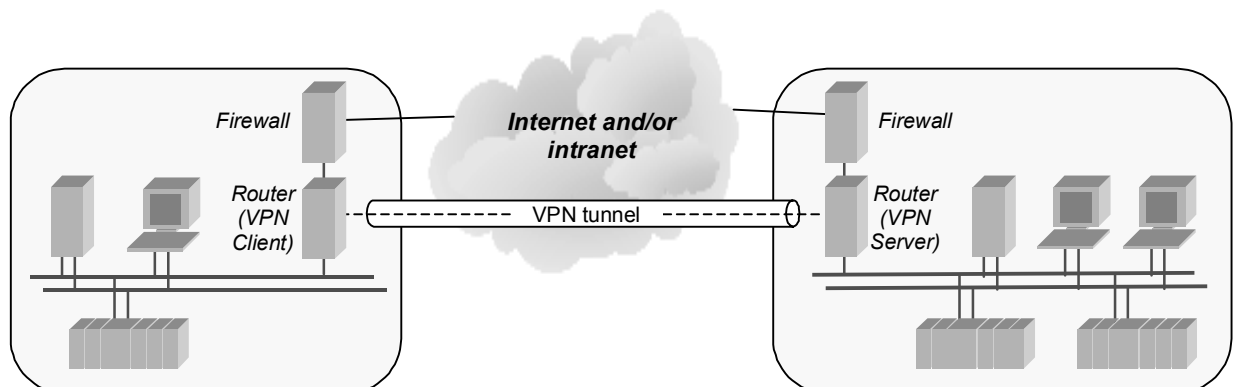


Figure 9 VPN site-to-site connection

The VPN connection, including routers and firewalls, can be duplicated for redundancy, but the connection is still exposed to the disturbances and occasional unavailability that characterize in particular the Internet. For safety or mission critical functions there should therefore be some form of fallback or emergency way of operating the system, and the overall system should be designed to react safely, also when there is a total loss of the remote connection.

## 5.7 Wireless communication

Compared to wired networks, wireless networks are generally exposed to additional threats, because an attack does not require physical access to any network cable or equipment.

- In a wireless network there is no strict control over the communication medium. Radio signals leak into uncontrolled areas, such as parking lots, neighboring offices, and public areas, where intruders can observe network traffic and potentially capture information about authentication credentials, protocols, network topologies, and devices. The acquired information can be used for a structured attack that could bypass firewalls and intrusion detection systems.
- Wireless devices are typically designed to constantly look for connections with other devices or network access points. An attacker could set up a rogue access point, which might trick wireless devices to connect to it.
- Radio transmissions can be disturbed by electrical interference or by radio jamming, or a rogue device can flood the network with garbage messages, causing a denial-of-service attack.

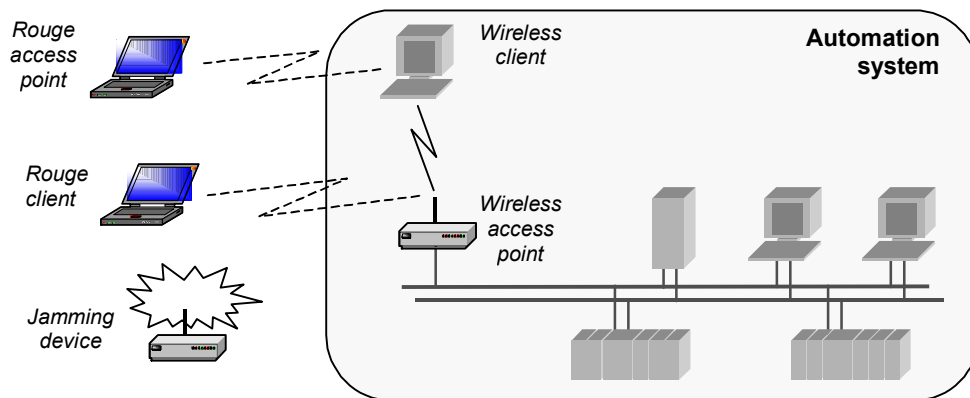


Figure 10 Additional threats to wireless connections

For applications where wireless communication is the only feasible alternative, or where the benefits outweigh the assessed risks, the security measures offered by modern wireless communication systems should be activated and properly configured, and the overall system should be designed to react safely to loss of the wireless connection. Security measures should include blocking access from devices with unknown identities, activating wireless link authentication and encryption, and deploying higher-level security measures such as virtual private networks (VPN). Privileges granted to users of wireless devices should be carefully considered. Network access points should be positioned and arranged such that the useful signal strength is limited as far as possible to within the physically secured perimeter, e.g. by use of directional antennas. A tight security management, with detailed and up-to-date asset registers, regular site surveys and audits, and frequent review of access logs, can help identify rogue devices and access points, and give an early warning of intrusion attempts.

## 6. CONCLUSION

The security of computer systems in general, and of manufacturing and control systems in particular, becomes increasingly critical as different networks are connected and systems are integrated in a collaborative manufacturing environment. Users of manufacturing and control systems need to pay correspondingly increased attention to these issues. Similar to process and safety improvements, network security needs to be a continuous activity. While the reality is that no security can be 100% effective, careful planning and implementation of security measures, based on a systematic risk assessment, can bring security up to a level that is adequate for any particular application and installation.