White Paper

Security for Industrial Automation and Control Systems

Abstract

The security of industrial automation and control systems becomes increasingly critical as different networks are connected and systems are integrated in a collaborative manufacturing environment. For industrial automation and control systems the potential impact of an attack may be more serious than for computer systems in general. Users of industrial automation 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, security improvement needs to be a continuous activity.

This white paper provides background and a general overview of different elements of information system security, with specific emphasis on how it applies to industrial automation and process control. 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.

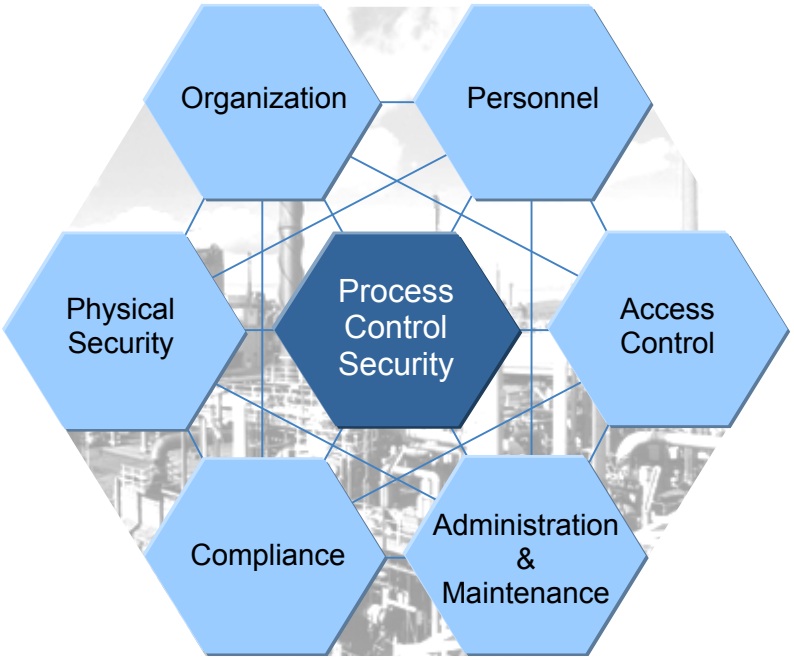

ABB AB

NOTICE

This document must not be reproduced or copied, in whole or in part, without written permission from AB,B 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 industrial automation and control systems 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.

TRADEMARKS

All rights to registrations and trademarks reside with their respective owners.

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

1. About this document

This white paper presents an overview of security for industrial automation and control systems, and describes measures and practices that a user of an automation system may want to consider. In this context the term *security* means the protection of a system's confidentiality, availability, and integrity. This is often also referred to as *electronic security* or *cyber security*.

Chapters 2 and 3 provide some background information and a general overview of different elements of information system security, with emphasis on how it applies to industrial automation and process control. In chapter 4, 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. Chapter 5, finally, provides some examples on how software updates for the automation system can be arranged, including updates to operating systems and security related software.

Warning! Caution!

Security breaches may lead to system unavailability or failure, or to situations where unauthorized users gain access to or control over a system. Depending on the nature of the system installation and the process controlled, this could lead to corruption of the system's software, degraded process performance, damage to equipment, and environmental and health hazards including personal injury or death.

While the purpose of this document is to discuss security measures that a user of an automation system should consider to apply, the described measures are not necessarily complete or effective for all possible applications and installations.

Users of automation systems must assess the risks of their particular applications and installations. The described security measures represent possible steps that a user should 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.

A wide range of literature on information system security in general is available. For industrial automation and control systems in particular, several standardization activities are in progress. The probably most comprehensive and most influential initiative is the IEC 62443 series of standards, which is based on the work of the ISA 99 committee. This standard is currently partially published, partially in draft. ABB is actively engaged in the preparation of these specifications.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is part of the Control Systems Security Program, an initiative by the United States Department for Homeland Security. ICS-CERT publishes reports and advisories on cyber security incidents and identified vulnerabilities specifically in relation to industrial automation and control systems.

2. Background

Providing and managing security for industrial automation and control systems is a moving and dynamic target, complicated by continuous technical, organizational, and political changes, global interconnections, and new business models. It is a complex challenge requiring procedural as well as technical measures.

The frequency of security incidents has increased significantly over the last several years. Incidents include directed and malicious intrusion attempts as well as undirected attacks from viruses, worms, and other malicious code, and 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 criminal or terrorist attacks against infrastructure and critical process industries.

In the past most reported security incidents were initiated by people with legitimate access to the system. In general, such 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. However, for the last decade the share of externally sourced incidents has increased drastically[1], in particular in the form of virus and worm infections. In many cases, infections are caused by connecting a portable computer or storage device that has previously been connected to an infected environment. Recent events[2] have also clearly demonstrated the possibility of complex, directed attacks on specific control systems, crafted by dedicated and resourceful organizations.

Security for industrial automation and control systems is similar to general information system security, yet different. Automation and control systems put higher requirements on integrity, availability, performance, and immediate access. Also, the potential impact of an attack on automation and control systems may include not only financial losses and loss of public confidence, but also violation of regulatory requirements, damage to equipment and environment, and endangerment of public and employee safety.

The table below summarizes the main differences between requirements on security for general information systems and automation and control systems:

	Information systems	Automation and control systems
Primary subject for protection	Information	Physical process
Primary risk impact	Information disclosure, financial	Safety, health, environment, financial
Security focus	Central server security	Control device stability
Availability	95 – 99%	99.9 – 99.999…%
Determinism	Hours to months	Milliseconds to hours
Operating environment	Interactive, transactional	Interactive, real-time
Problem response	Reboot	Fault tolerance, on-line repair

100% security is not possible to achieve. A system 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 system that is perceived as being totally isolated from the outer world is vulnerable to security breaches from sources such as the occasional connection of portable computers or memory devices, unauthorized installation of software, or deliberate attacks by insiders.

[1] Byres, Eric; Lowe, Justin; The Myths and Facts behind Cyber Security Risks for Industrial Control Systems. VDE Congress 2004

[2] Stuxnet, a computer worm specifically developed to target industrial automation and control systems, was first discovered in June 2010. www.us-cert.gov/control_systems/ics-cert/ en.wikipedia.org/wiki/Stuxnet

3. Approaches to security

3.1 Objectives

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 objective is to raise the level of sophistication needed for an attack to succeed, and lower the time it takes for the system user to identify and respond to an attack

Similar to process and safety improvements, security improvements need to be a continuous process, including not only technical solutions, but also procedural and organizational measures. A very important element is the knowledge and mindset of the system's users and other stakeholders – security begins and ends with human behavior.

There is no single solution or technology for security that fits the needs of all organizations and applications. 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. It is also necessary to balance security and usability requirements, e.g. for immediate access for quickly responding to a process upset. A good balance is found when the assessed value of additional incremental risk reduction is smaller than the cost for additional incremental security measures, within boundary conditions set by imperative usability requirements.

Note that the probability of a successful attack must not be confused with the probability that anybody would want to attack the system, or that anybody would know how to do it. The basic assumption in this type of risk assessment must be that there is somebody who wants to attack the system and has the necessary skills. With this assumption, the probability of a successful attack depends only on how well protected the system is.

3.2 Security Policy

A key element in implementing and maintaining the security of a system is the establishment of an adequate 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 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 also recommended.

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 networks.

The security policy should be based on the principles 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. Access to functions or areas that is 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.

3.3 Virus scanning

All computers in the system should be scanned for viruses, on access and at regular intervals. A virus scanner of good reputation should be used and it should be updated regularly. However, virus scanning may have a significant impact on performance and response times of the system. It is therefore important to follow recommendations from the system vendor on how to configure and use the virus scanner. Also, when a virus is found, damage may already have been done. For a mission critical system it is therefore even more important to effectively prevent viruses from at all being introduced into the system.

3.4 Security Zones

IT resources vary in the extent to which they can be trusted not to be compromised. A common security architecture is therefore 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. All resources in the same zone must have the same minimum level of trust. The inner layers, where communication interaction needs to flow freely between nodes, must have the highest level of trust. This is the approach described in the IEC 62443 series of standards.

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. Internet access, coming e-mail, and instant messaging, for example, represent very high risks.

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.

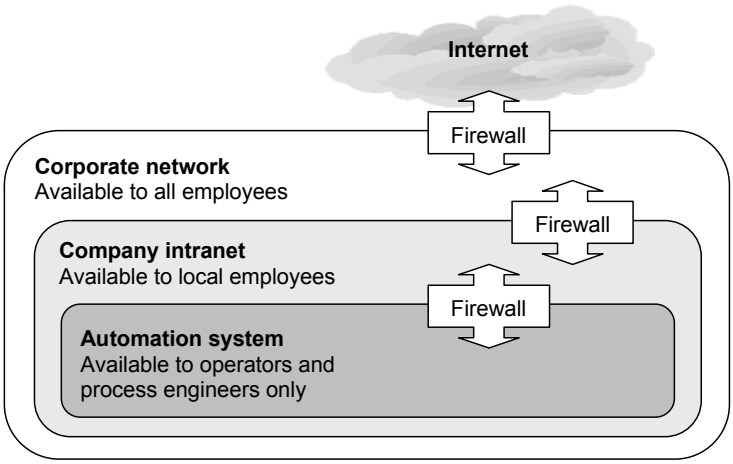

Figure 1 Security zones

Figure 1 shows three security zones, but the number of zones does not have to be as many or as few as three. The use of multiple zones allows access between zones of different trust levels to be controlled to protect a trusted resource from attack by a less trusted one.

High security 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. A high security zone should obviously not be dependent on

resources in a less secure zone for its security. Therefore it should form its own domain that is administered from the inside, and not depend on e.g. a domain controller in a less secure network.

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 also upon the types of measures taken to detect and prevent compromise of resources and violations of the security policy.

3.5 Measures for higher security

To establish a certain level of trust in a zone requires that all resources in the zone have a certain minimum level of security as determined by the organization's security policies. For a high security zone the trust level must be very high. Meassures to achive this include (but are not necessarily limited to) the following:

- Keep the trusted network zone relatively small and independent from other network zones. It should form its own domain, and be administered from the inside.
- Physically protect all equipment, i.e. ensure that physical access to computers, network equipment and cables, controllers, I/O systems, power supplies, etc., is limited to authorized persons.
- Harden the system by removing or disabling all unnecessary network connections, services, file shares, etc., and by ensuring that all remaining functions have appropriate security settings.
- When connecting a trusted network zone to outer networks, make sure that all connections are through properly configured secure interconnections only, such as a firewall or a system of firewalls, which is configured for "deny by default", i.e. blocks everything except traffic that is explicitly needed to fulfill operational requirements.
- Allow only authorized users to log on to the system, and enforce strong passwords that are changed regularly.
- 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. Users should not have more privileges than they need to do their job.
- Do not use the system for e-mail, instant messaging, or Internet browsing. Use separate computers and networks for these functions if they are needed.
- Do not allow installation of any unauthorized software in the system.
- Use a virus scanner configured according to the automation system vendor's recommendations on all system nodes.
- Restrict temporary connection of portable computers, USB memory sticks and other removable data carriers. Computers that can be physically accessed by regular users should have ports for removable data carriers disabled.
- 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, USB memory sticks 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.
- Continuously monitor the system for intrusion attempts.
- Keep the system updated with all relevant and vendor recommended security updates, including updates to operating system, automation system software, 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.

4. Network configurations

This chapter provides an overview of different security measures 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.

4.1 Isolated automation system

For a “traditional” automation system configuration that is not connected to any “external” network, security is primarily a matter of physically protecting the automation system, and preventing unauthorized users from accessing the system and from connecting or installing unauthorized hardware and software. The security measures described above should be applied as relevant.

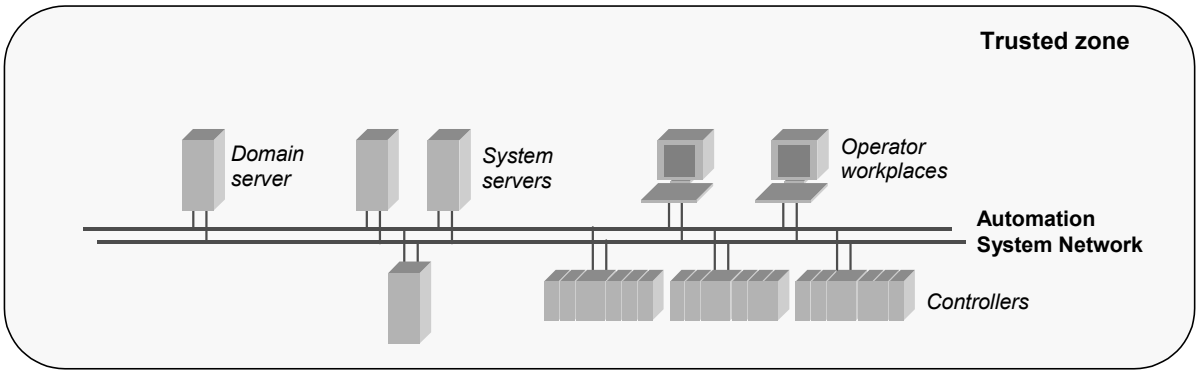

Figure 2 Isolated automation system

Servers and workplaces that are not directly involved in the control and supervision of the process should preferably be connected to a subnet that is separated from the automation system network by means of a router, as shown in Figure 3. 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.

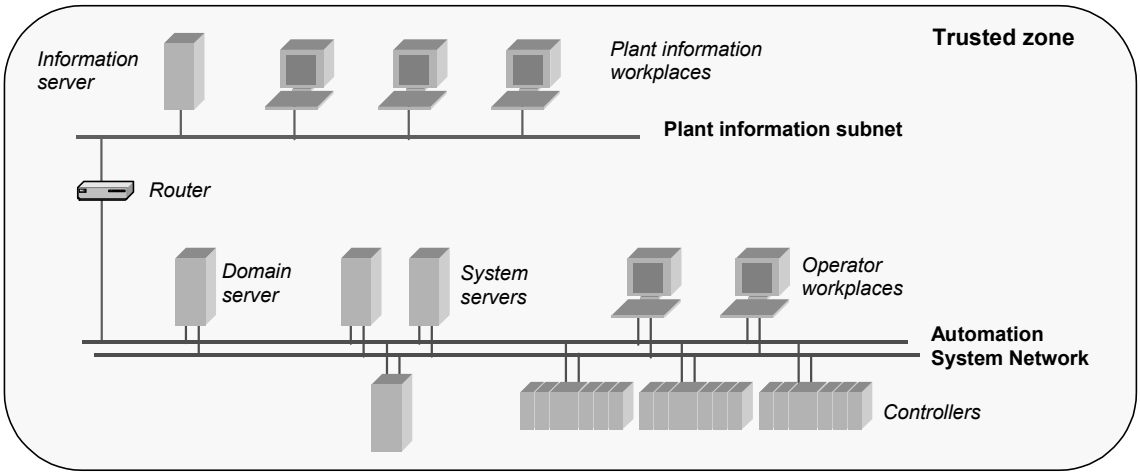

Figure 3 Plant information network connected to an automation system

4.2 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, not the least since such networks are normally further connected to the Internet or other external networks. The IS network is therefore a different lower security zone, and it should be separated from the automation system by means of a firewall, as illustrated in Figure 4. The IS and automation system networks should form separate domains.

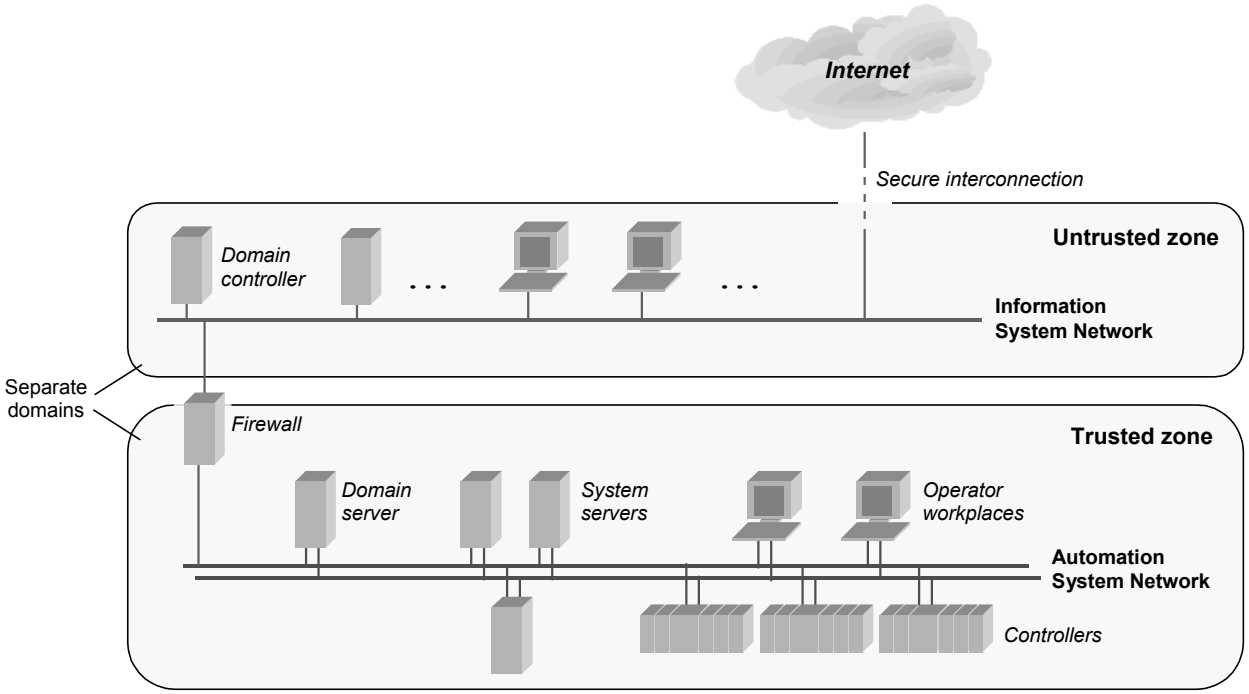

Figure 4 Connecting an automation system to a general purpose IS network

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 4.3, should be considered.

4.3 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. On such networks 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 through a more elaborate secure interconnection. Figure 5 below indicates how this could be organized.

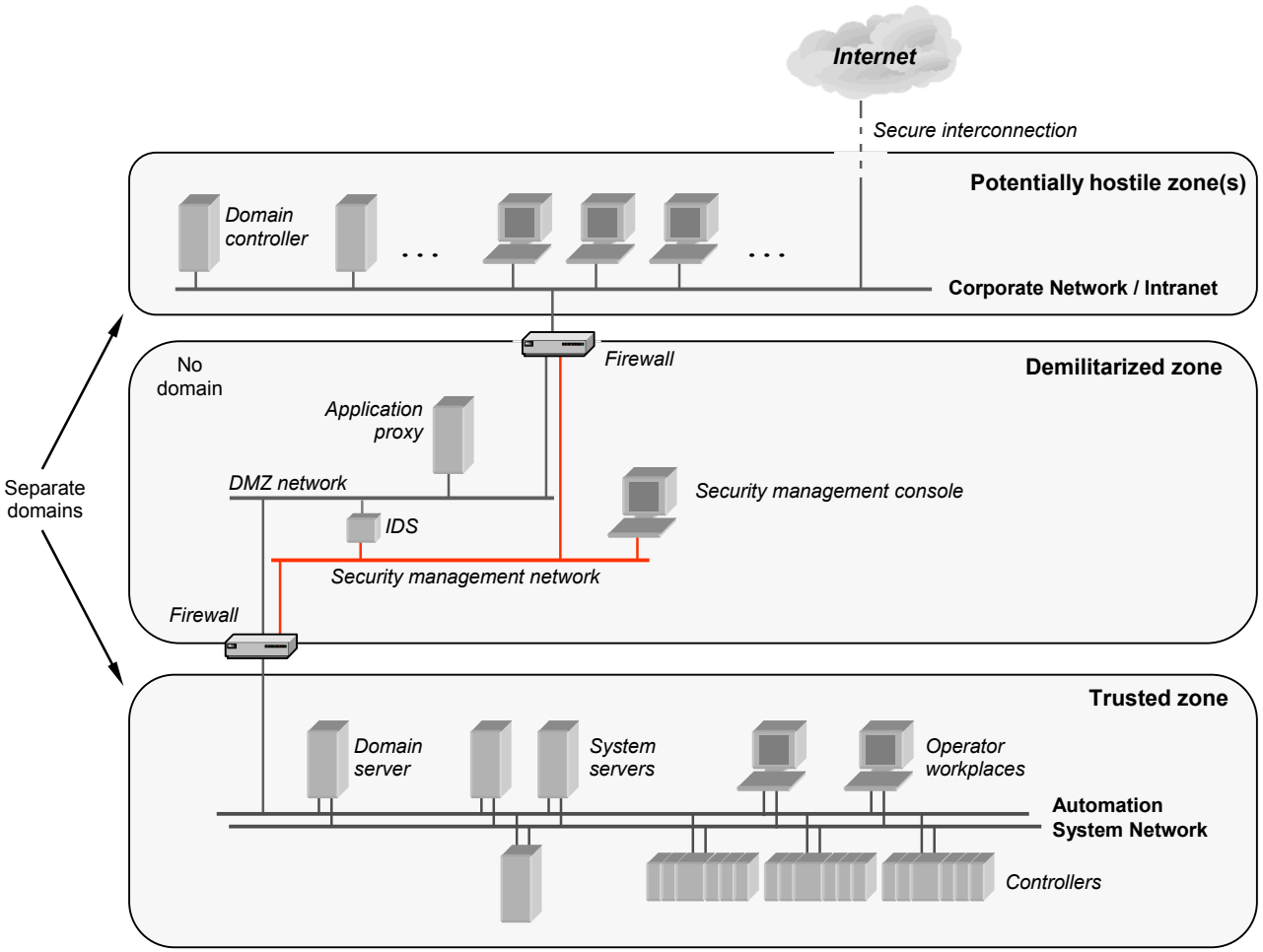

Figure 5 Connecting an automation system to a corporate network

The network between the two firewalls in Figure 5 forms a so-called demilitarized zone (DMZ). Firewalls form the borders towards the corporate network and 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. Examples are terminal services and data access services. External connections are terminated in the proxy, which establishes a new connection to the relevant server in the automation system to perform the requested services. This way no direct connections exist between the external network and nodes on the automation system 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 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).

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 quickly 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.

4.4 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.

4.4.1 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:

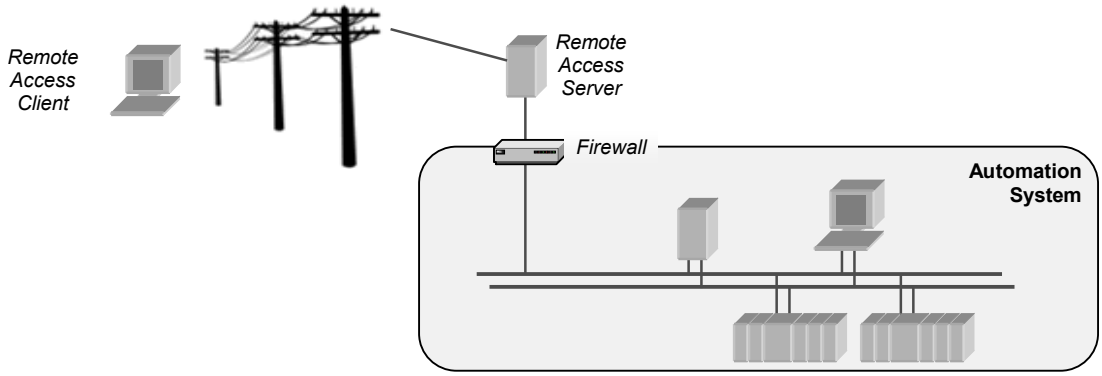

Figure 6 Remote access – dial-up connection

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 can 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, see Figure 7:

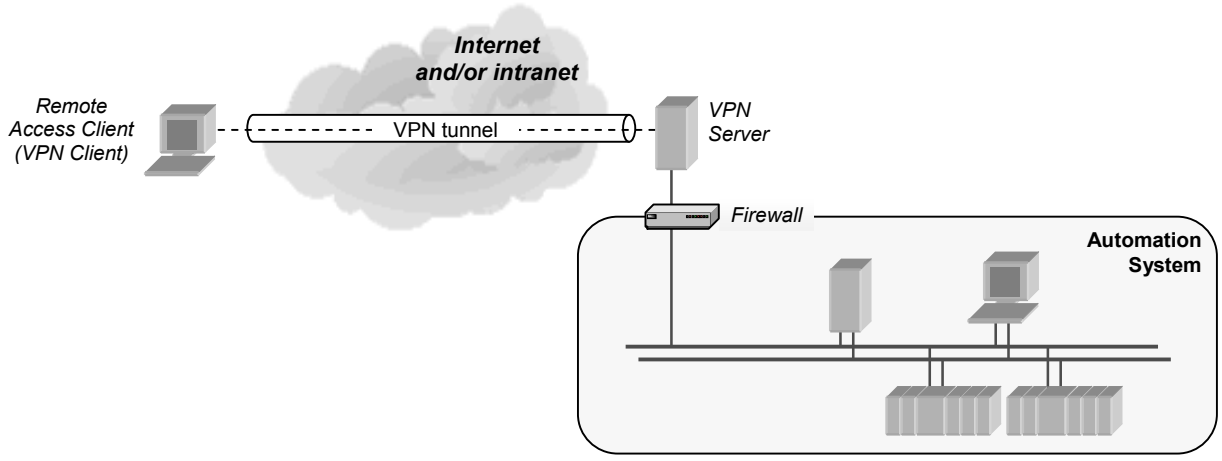

Figure 7 Remote access – VPN connection

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 is preferably placed in a demilitarized zone that protects the automation system as shown in Figure 5. Automation system vendors are normally able to provide a standardized solution for this.

Note that regardless of how a remote client computer is connected the net effect is that it becomes a member of the automation system. It therefore needs to be secured in the same way as the computers in the automation system trusted zone, including all the security measures discussed in this document. The remote computer should not have any other network connections besides the VPN, and it should not be left unattended while the remote connection is enabled. To further mitigate risks associated with remote access, the remote client may only be allowed to connect to a terminal server in a DMZ, which only provides remote interactive sessions but no file access and no other network services.

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 personnel should always be available to take corrective actions in case something should go wrong.

4.4.2 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.

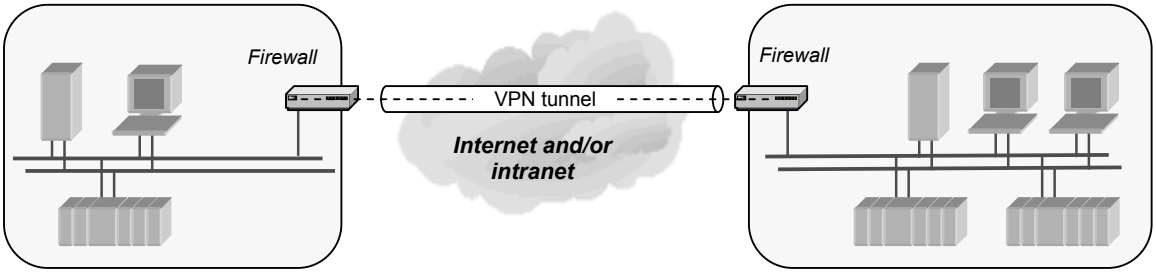

Figure 8 VPN site-to-site connection

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.

4.5 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 radio jamming, or a rogue device can flood the network with garbage messages, causing a denial-of-service attack.

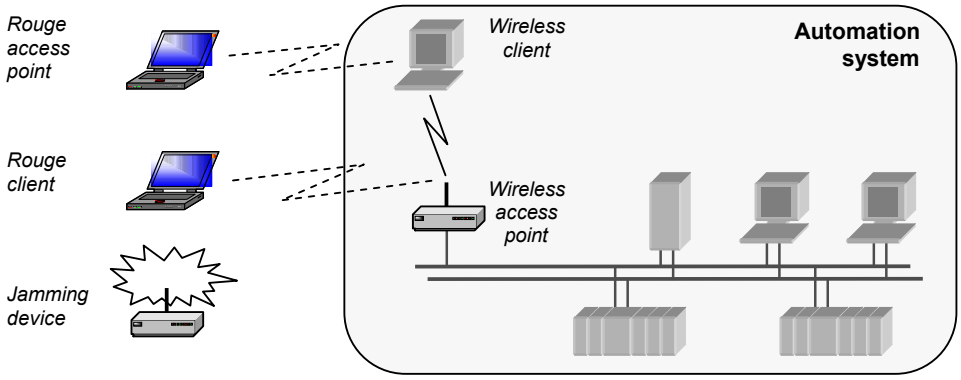

Figure 9 Additional threats to wireless connections

For applications where wireless communication is the only feasible alternative, or where the benefits outbalance the assessed risks, a wireless communication system that supports the strongest available security should be selected and properly configured. 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). Wireless systems that are designed for industrial use, e.g. Wireless HART, provide such security mechanisms.

Privileges granted to users of wireless devices should be carefully considered. 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. Since wireless communication can be jammed, the overall system should be designed to react safely to loss of any wireless connection. 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.

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, 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, updates can alternatively 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 other SW updates.

Also firewalls and intrusion detection systems need to have their software and rule-bases regularly updated. In the configuration described in section 4.3 above, this gets a bit more complex. The following is an example of a process that could be used (refer to Figure 5 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 (see Figure 5).
- After having verified the digital signatures of the updates, the security system manager updates the firewalls and IDS systems through the security management network.

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, 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.