



**Romel Cabiling** ▾



[Home](#)

[Home](#) > [My courses](#) > [Network Defense and Remote Access Configuration](#) > [17 \[Enter Module Title Here\]](#) > [Lesson Proper for Week 17](#)

# Lesson Proper for Week 17

## Remote access in control systems architectures

Companies must abandon the traditional (and sometimes ideal) concept of total domain isolation as control systems architectures, corporate architectures, peer sites and other operational entities interconnect. In reality, remote access has always been a part of industrial control systems. As previously stated, vendors had access to support systems, and the communications infrastructure was typically quite extensive, allowing for remote data control and acquisition. The data acquisition mechanisms use a variety of communication media, many of which are shared by multiple entities. Many of the security features and concepts used by ICT can be used in control system architectures. The challenge is to apply cyber security best practices to remote access programs while meeting business needs.

This section will look at remote access solutions for industrial control systems and how the lessons learned in ICT can be applied here. Examine the differences between the environments and how they limit the available security techniques.

A comparative matrix is one of the best ways to understand the differences in remote access requirements between business ICT and industrial control systems. These distinctions lay the groundwork for addressing some of the more unique aspects of deploying remote access and control system architectures. The table below compares and contrasts key remote access requirements between ICT and control systems domains.

<b>Remote Access Requirements</b>	<b>Information &amp; Communication Technology</b>	<b>Industrial Control Systems</b>
Direct internet access	Not common, protected by firewall and intrusion prevention system.	Control system components are sometimes exposed directly to the internet
Modem access	Rare	Common/widely used, legacy equipment
Leased lines	Common/widely used	Common/widely used
Remote access through Firewall with virtual local area network (VLAN) segmentation	Common/widely used	May be segmented from corporate network, little segmentation within control system network
Remote authentication	Multiple form factor	Usually single factor, some multifactor solutions ineffective due to speed or process control reliability requirements
Remote authorisation	Usually role based or based on confidentiality of data	Usually a single level with full authorisation
Access control lists	Usually well defined	Not always utilised or clearly defined. Not maintained as it should be
Audit trail	Robust and actively monitored	Sometimes limited capability, not actively monitored
Authorisation server	Maintained and monitored in a DMZ	Authorisation servers deployed directly on the control system network
Demilitarized zone	Access through DMZ only	DMZ not always deployed
SSL Encryption	Commonly deployed	Rare
IPSec	Commonly deployed	Very rare

**(Table 2: Comparison of control systems and ICT remote access requirements)**

### **Remote access security considerations unique to control systems**

Culture has always influenced how control systems implement cyber security. Creating security solutions that account for interoperability can be difficult when security foundations are built in complete isolation from untrusted domains. While control system functionality is based on requirements for high availability and data integrity, it provides opportunities to leverage proven security technologies and adapt to operational needs. Those responsible for developing remote access solutions for industrial control systems may not consider cyber security a major concern, but rather how the access solution can be managed to maintain critical operations. The perceived obscurity of the system justifies many direct connections, and the risk is mitigated by the assumption that little understanding of how the system actually works. This approach is not only dangerous but also poses a significant operational risk (i.e. the lack of awareness that mission-critical systems are directly connected to the internet).

Most control systems environments are deployed in critical infrastructure domains. The company running the infrastructure is not the only one at risk. Remote control of a control system exposes some architecture to remote manipulation. Remote access may be an exploitable attack vector, increasing the control system's availability risk. Remote access security cannot

impede or degrade the normal operational processes required for the control system to function.

For example, remote access security must consider the need for real-time operations. Deploying security countermeasures without properly analyzing their impact performance is often dismissed by organizations who fail to recognize the real-world impact security can have on real-time operations. Many control systems environments require real-time operation, with some requiring millisecond polling. Encryption, for example, creates latency that can cause process delays or shutdowns. Also, much of the data on a control system is non-confidential, eliminating the need for encryption between critical system components.

Environments for control systems are often geographically dispersed, if not cross-border. Due to the nature of these deployments, many field locations are unmanned, so remote access solutions often address connectivity rather than security. This may limit some procedural security protections like temporary system access. Adding security features that slow down field equipment management, like calling a help desk to enable remote access, may justify keeping an 'always on' remote connection.

Because many control systems environments require real-time operation, the need to quickly connect to a system is critical. Operators may feel hampered by the multiple steps required for remote access and may want to disable security features that slow down connectivity or create workarounds. An example of this is an organization using the default administrative credentials for remote access or creating passwords that are not complex and are not changed frequently. Given the urgency of the situation, many users will want (or be required to) connect to a remote system as quickly as possible, without having to worry about using a complex password or one they haven't used in years.

These practices, along with using the same password for every field device, greatly reduce the security of remote access. Rapid remote access can justify omitting more robust security measures.

The fact that not all remote connectivity occurs in or from a controlled location adds to the complexity of security requirements for control system architectures. This can cause issues when using advanced secure remote access features that require multifactor authentication. There are many control environments deployed in factories, large processing plants, warehouses, isolated stations, and even outside.

Due to environmental concerns, operators may be unable to use advanced authentication technology. Many organizations struggle to implement remote access security strategies that match the system's value. However, using biometrics or other technology that requires a clean environment is useless if the operators are covered in dirt, grease, oil, or other impurities. Dirt, oil, and grease can affect two-factor authentication using advanced biometric thumbprint scans. Using voiceprint technology can be difficult because background noise from large processing plants or outdoor environments can affect the voice wave length for recognition.

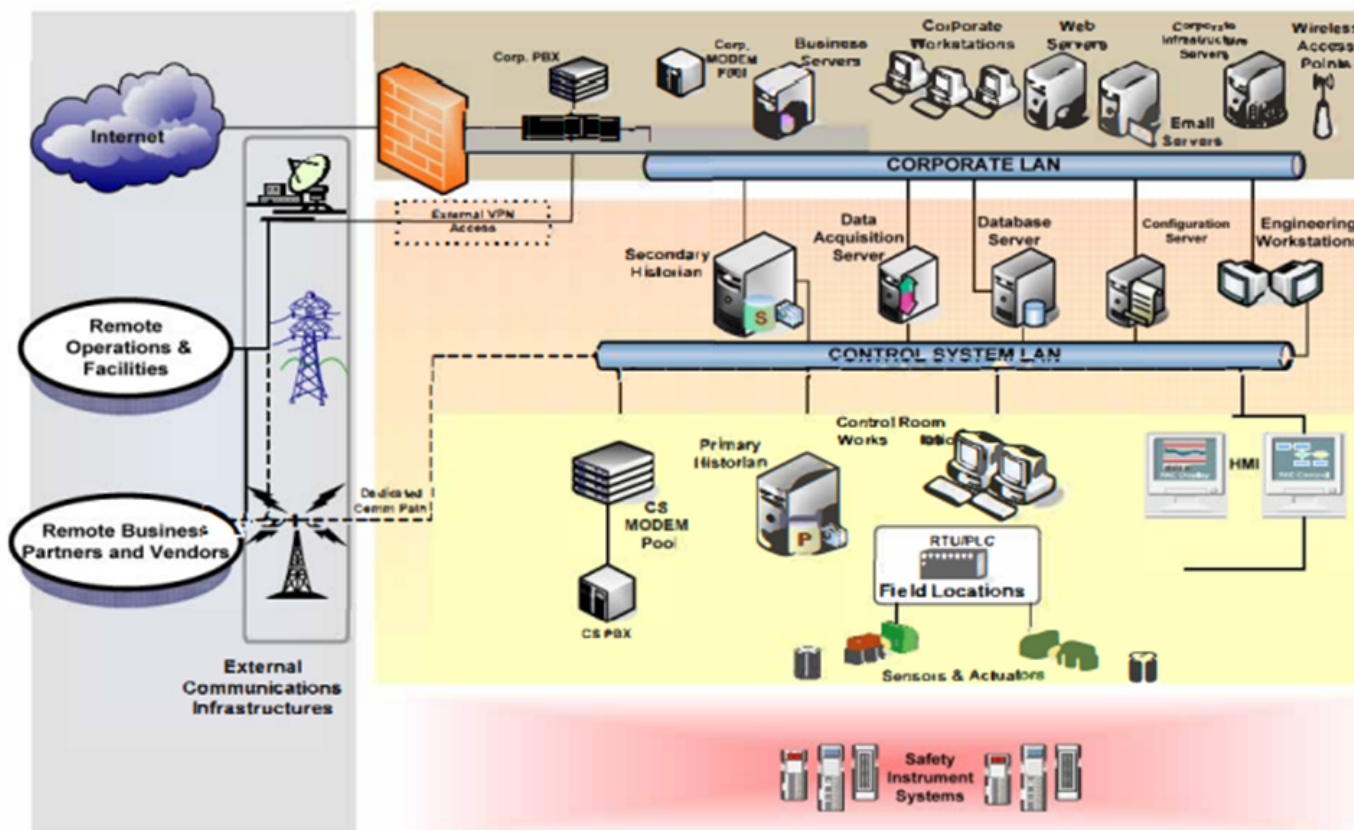
Finally, many control system devices or implementations may not be able to use basic security features like authentication or authorization. With control systems having a life cycle of up to 20 years, effective remote access security countermeasures are simply not feasible. A new system is expensive, and the cost of implementing an effective remote access solution is greater than the cost of buying a new system. This situation benefits the vendor rather than the operator, leaving the operator with little choice. Secure remote access is possible, but asset owners should expect full vendor support to secure existing remote access capabilities.

### **Applying good practices**

The current interest in secure remote access has created a situation where defining good practice is difficult. Although highly regulated ICT systems, such as those used in the federal government, financial or health care sectors, have specific good practices, these are not straightforward. As stated earlier in this document, creating a remote access good practice that is applicable to every possible control system architecture is extremely difficult. However, asset owners can establish effective baselines for secure remote access programs. Operational mandates can be met while protecting critical information assets by understanding their organization's accessibility requirements and cross-correlating those with users and services required for remote connectivity.

Most operational environments have limited options for remote connectivity technology. Defining guidelines is simple when you recognize the critical assets that must be accessed. Guidelines for control systems environments include:

- Undertake a formal threat and risk assessment;
- Eliminate all direct connections to critical operational assets;
- Secure modem access beyond default means;
- Use DMZs to segregate business and control architectures;
- Establish user-specific authentication servers;
- Create a security assurance policy for all remote access;
- Use only full tunneling cryptographic technology;
- Use a password policy specific to remote access elements;
- Wherever possible, use multifactor authentication;
- Use role-based authorization levels;
- Use dedicated hardware and software to support the remote access solution.



(Figure 6: Basic industrial control systems network with no security)

Figure 6 shows an unsecure industrial control systems network. The corporate network is protected from the internet, but not the industrial control systems environment, business partners, or remote office locations. The following sections will illustrate the various environmental controls and conclude with reasonable security controls.

### Periodically undertake formal threat and risk assessments

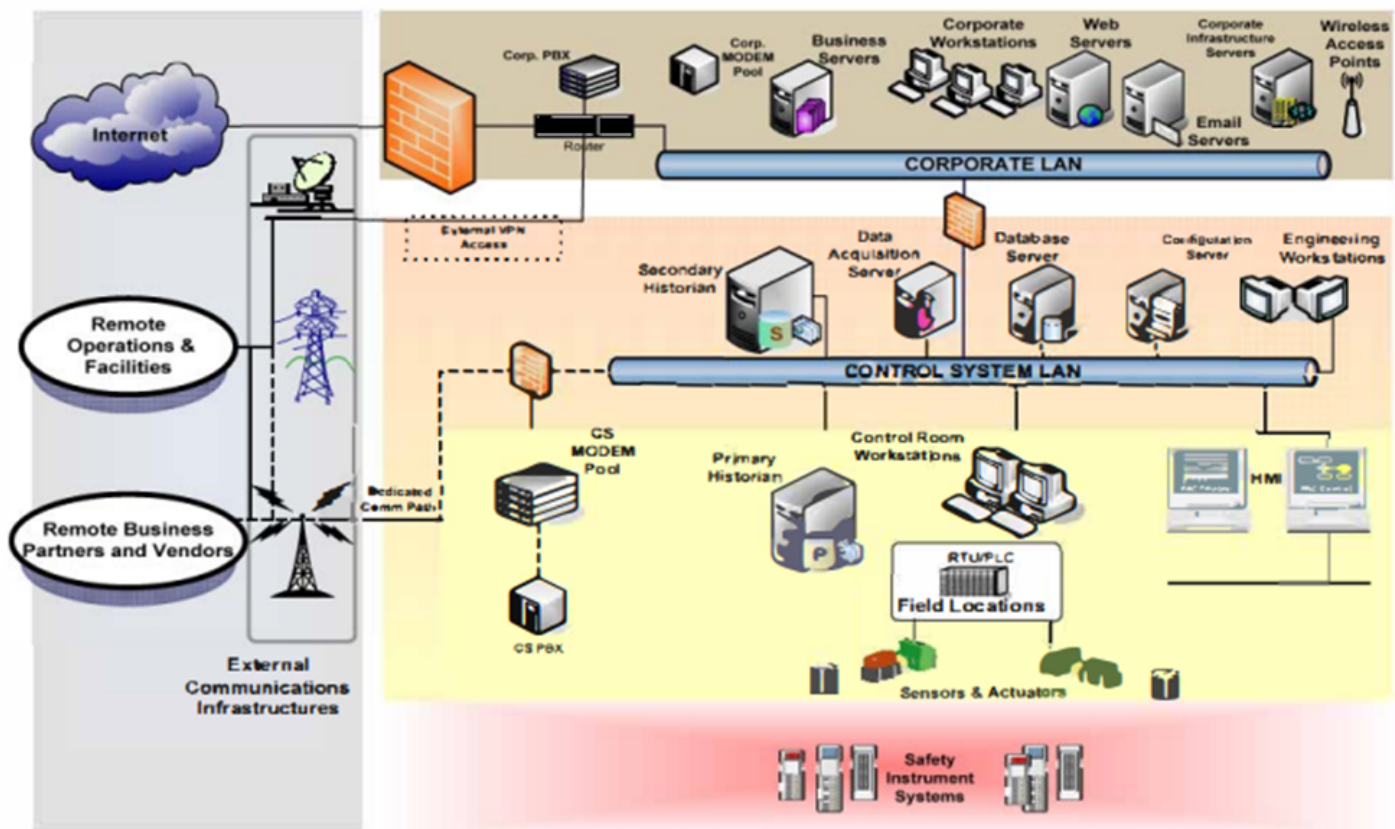
Threats and risks must be understood. Risk management is a common practice among project managers and organizational managers. To be sure, project managers and managers are concerned about margins and efficiencies, and the risks they routinely consider reflect their perceived priorities. The subject rarely shifts to threats of system failure or deliberate sabotage due to lack of security controls. As a result, managers don't get a thorough understanding of the cyber threats to their industrial control systems infrastructure.

Formal Threat and Risk Assessments (TRAs) on industrial control systems environments should be conducted on a regular basis to help organizations understand these risks and make risk-aware project or operational decisions.

### Eliminate all direct connections

Direct connections to control system architectures should be avoided due to security concerns and attack path ease. The prevalence of flat network control system architectures may result in unrecognized direct connections. Because many control system architectures rely on remote access for functionality, direct connections could easily compromise the control system. Field devices and equipment require special care, and their access requirements make direct connection removal difficult. If organizations cannot eliminate direct connections, they should deploy authentication and authorization countermeasures. Authentication and authorization mechanisms on field equipment should be enabled whenever possible, and disabled if remote access to field equipment is not required.

Due to the rapid expansion of control systems environments, some organizations are unable to connect remotely. Relays, intelligent electronic devices, remote telemetry/terminal units (RTUs), and Programmable Logic Controllers (PLCs) should never be connected to the internet. The organization should determine what functionality can be removed to reduce the risk profile and work with vendors to establish unique access capabilities that significantly limit the control system's exposure. Entities should use procurement language guidance to ensure that technology purchased has security capabilities and that vendors can support secure remote access to the device. When direct connections to critical information assets are required, remove functionality that is not required for operation but could be exploited by an adversary.



(Figure 7: Eliminate 'direct connections' by adding firewalls around the industrial control systems environment.)

Figure 7 depicts a partially isolated industrial control systems network. Previously, the industrial control systems network was completely isolated from other environments. For industrial control systems, firewalls can be configured to allow appropriate traffic in and out.



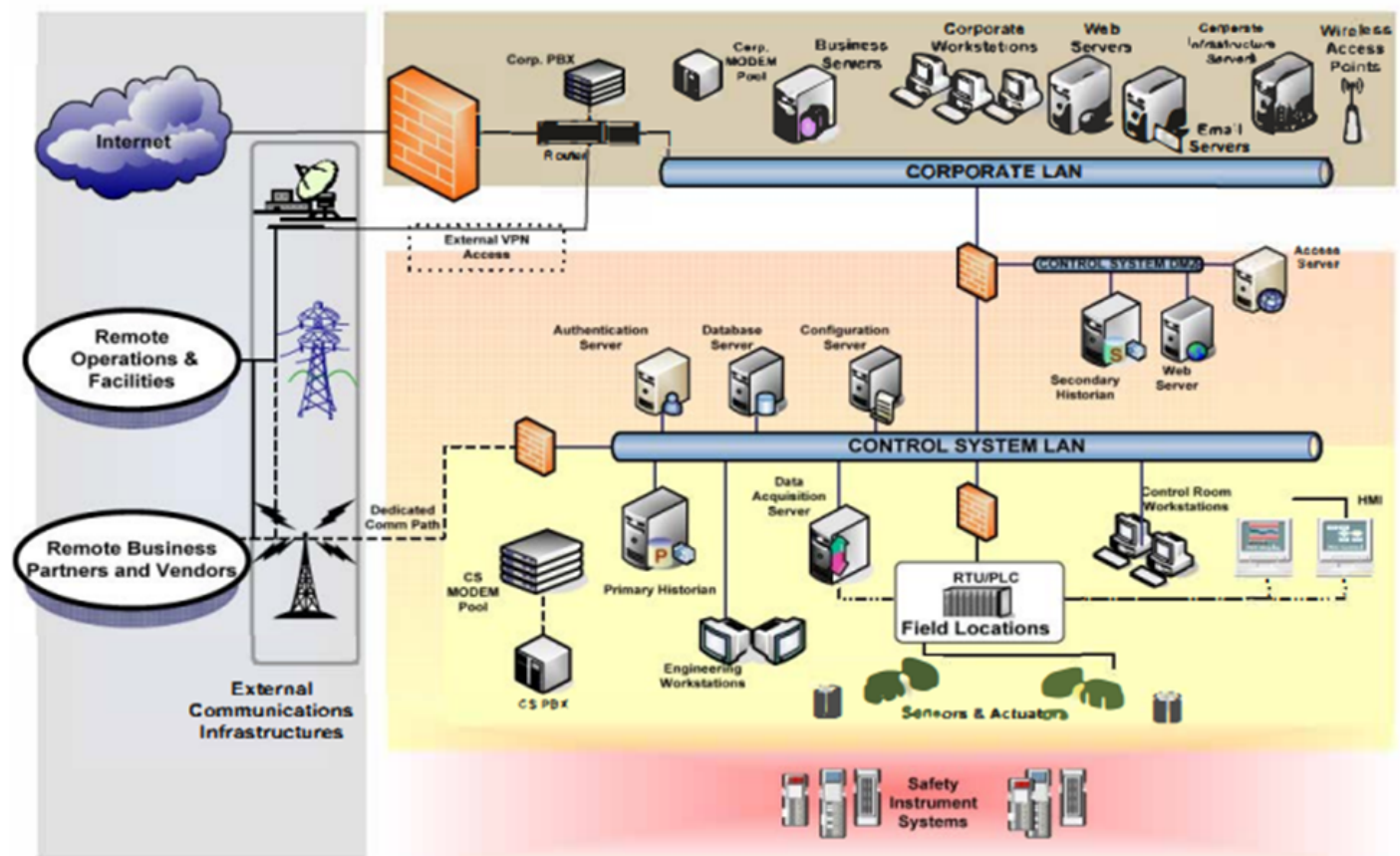
To prevent modems from compromising the industrial control systems environment, the modem pool is moved outside the industrial control systems to a DMZ-like network.

### Secure modem access

If no modems are used, they should be removed or disabled. If a modem is required despite the available alternatives, it should be turned off and deployed according to best practices. 3 For more information on securing modems, consult the DHS practice guide Securing Controls System Modems.

### Create a physical and logical DMZ separating corporate and IT environments

Place all authentication and access servers in a DMZ. This separate logical and physical network prevents direct corporate or external access to the control domain. While it does not affect business operations, it can greatly increase an attacker's workload. Additional security can be implemented by locating the authentication servers required to access mission-critical assets. To support network isolation, these authentication servers should be on a separate VLAN. Using this approach with the isolation of critical operational assets like field devices makes it easier to provide specific guidance in remote access credentials. Much progress has been made in creating DMZs within control system architectures. See the OHS practice guide Improving Industrial Control Systems for more information on network architecture. Cybersecurity and Defense-in-Depth.



(Figure 8: Illustrates network segregation. The network is divided into functional areas and the architecture is similar to that of an internet connection from corporate.)

## **Create separate authentication servers for separate roles (vendors/integrators)**

Owners of operational assets should be aware that operational assets can be trusted or untrusted. Operators and engineers are trusted elements, and their access to the operational domain of the control system is restricted by policy. Vendors and integrators create a situation where the electronic boundary is difficult to perceive and untrustworthy. Once connected, trusted operators (internal) and untrusted support entities (external) should have different mechanisms for provisioning access into the environment. This will help with security auditing and incident management, as well as granularly restricting access based on user profiles.

A separate server should be set up for authorized external users like vendors or integrators. This allows for vendor-specific access levels and control mechanisms that limit factors like time of day and traffic patterns. To quickly mitigate and secure a cyber-incident, dedicated authentication servers for different roles are used. This will also allow the asset owner to dynamically restrict vendor or integrator access, which can be re-granted as needed.

Depending on the architecture, servers can be deployed in multiple locations connected to the external communications infrastructure. Authentication servers can also be deployed to support existing or future media formats and enforce compliance with agreements made during system procurement. The authentication servers should have different user names and passwords than the corporate or ICT networks.

## **Enforce a security assurance policy for all remote access**

All users of remote access systems should sign a policy statement outlining their expectations. In this policy, legal and acceptable use conditions for the system to which remote access facilitates connection are clearly defined. In addition, the security assurance policy should be flexible enough to accommodate different users and requirements.

The remote access policy development life cycle should align with existing ICT security policies mandated by overarching business functions. Control system architectures help define the scope under which remote access users must function and clearly states the organization understands the consequences associated with remote access channel misuse.

The remote access policy defines device management and how devices are identified as critical to the control system architecture's core operations. Unless otherwise specified, critical device access is read-only, with exceptions for other operators. A policy and threat model for remote command, control, and change access should identify appropriate mitigation techniques to ensure core operational devices can be effectively monitored, alerted, and archived. Every requirement for remote access should be addressed in the policy. Pre-approval is required.

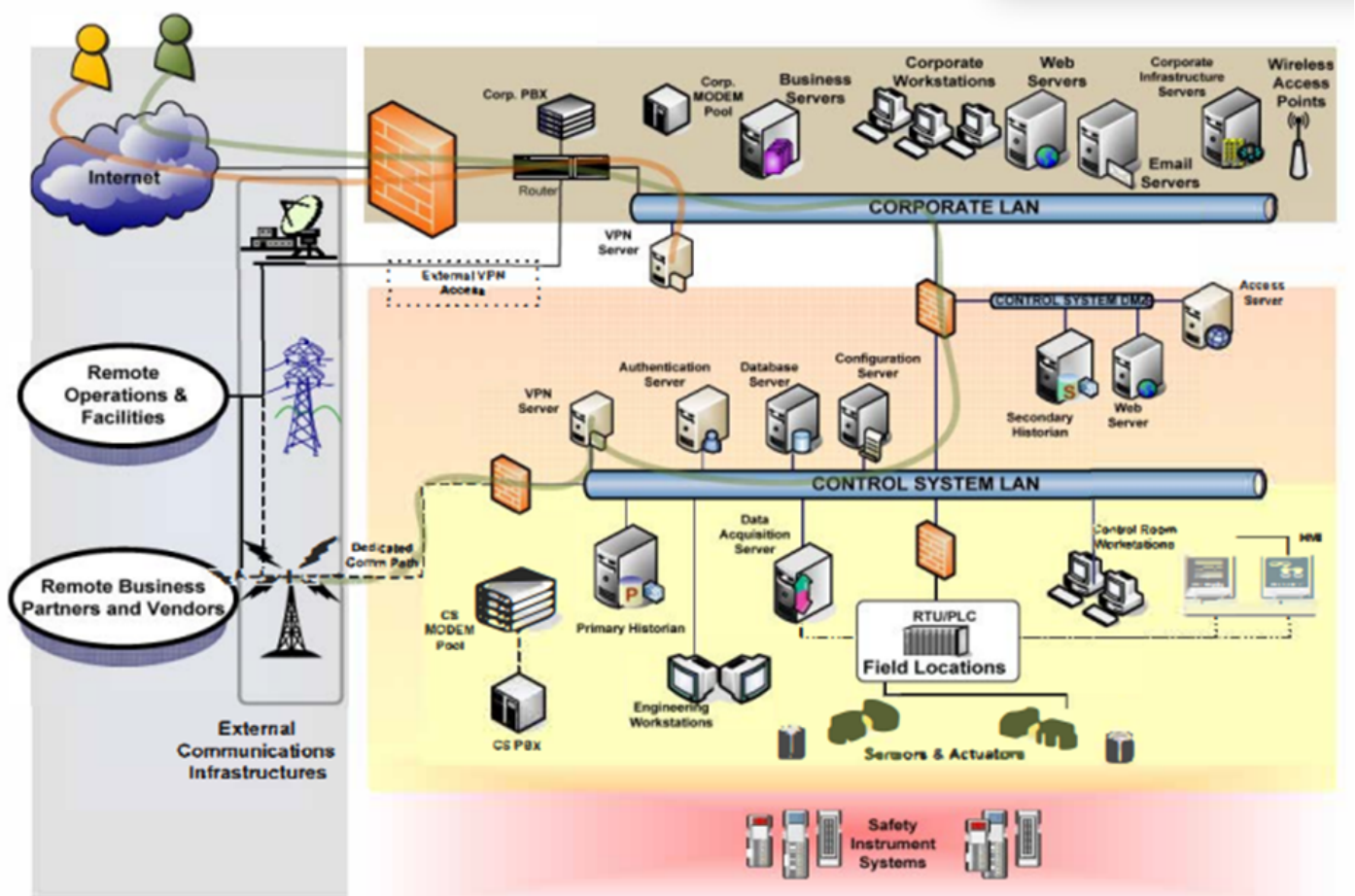


## Full tunnels

Remote access security countermeasures prevent an adversary from accessing data. A compromise of the command and control instructional information could have a significant impact on the system. This implies that remote access to the control system should be encrypted and authenticated whenever possible. The best solution for point-to-point encryption in the control system arena involves 'full tunnels,' which is beyond the scope of this paper.

An adversary can still inject himself into what is assumed to be a secure connection if the preferred solution does not prevent it. In this case, full-time roles prevent the attacker from acting as a gateway between the control system network and the source network of the trusted resource. In addition to ensuring authentication and authorization, the solution can reduce the risk of viruses and worms being introduced into the data stream.

When using full tunnels, most entities create remote access solutions that require first authentication and authorization to the corporate network, then to the control system's DMZ authorization server this protects against a compromised corporate account, preventing one of today's most common methods of control system compromise. A remote access solution that prevents the exploitation of corporate trust while maintaining critical access to control operations is valuable as adversaries continue to do so.



(Figure 9: VPN Remote Access)

Figure 9 depicts the use of VPN technology. In some cases, like modems, it can replace the access method. On the other hand, it can add security by encrypting traffic or requiring endpoint authentication.

Concerning cryptographic solutions, the discussion is incomplete without addressing latency. Almost every cryptographic solution designed to secure point-to-point communications has the potential to slow down network data throughput. The latency depends on both the type of cryptography and the algorithm used to secure the data. Point-to-point cryptography uses symmetric key algorithms, where the key used to encrypt and decrypt data is the same. Symmetric key cryptography is not as secure as asymmetric key cryptography, but the ease of key management makes it appealing for large-scale environments with multiple devices. These features make symmetric cryptography the best choice for control system operations, even if the compromise of the single symmetric key renders the solution useless. Despite this risk and the potential to increase latency by up to 30%, many vendors still use the Advanced Encryption Standard (AES) in 128 or 256-bit versions.

Concerning remote access, organizations must recognize that the algorithm's use does not have to be a stumbling block. In some cases, advanced compression algorithms used in cryptographic solutions can actually reduce latency and increase communication speed. Many vendors have developed technologies to enable field technicians to remotely access mission critical devices and have extended their solutions to create secure channels for remote data acquisition from centralized servers.

Some of the cryptographic solutions may not have been fully vetted by the research community. For some organizations, the assurance of data security without compromising the speed of data acquisition is sufficient to justify its implementation.

### **Password policy**

In an ideal deployment, authentication mechanisms should include not only passwords, but also other mechanisms (see the section on 'Two form factor authentication'). Strict password policies with upper and lower case letters, numbers, and symbols should be enforced by secure remote access systems. Also, as part of the organization's cyber security program, passwords should be audited for strength on a regular basis. Each user ID should be unique and protected by the corporate cyber security policy.

For remote access programs, user IDs and passwords should be generated by a process specific to the user or service and its enclave.

Organizations should categorize users and services into levels of trust and implement password policies accordingly.

Vendor-provided remote access technologies should be covered by the password policy. The passwords must also work with remote control system technology. Alternatively, if the vendor provides both remote support technology (modems) and embedded remote access functionality in ICT field devices (RTU, PLCs), the organization should have a password policy for both. Traditionally, vendor password policies were rigid, and only large customers could request changes. Many vendors do not allow customers to change their administrative credentials for field equipment. Furthermore, some vendors still hardcode supervisory passwords into their control systems, making them unchangeable. These issues, coupled with the historical cultural barriers associated with cyber security and control systems, increase an organization's cyber risk.

Vendors should help organizations develop mature cyber security programs to mitigate remote access risk. During the procurement process, asset owners should demand that vendors include the ability to update administrative credentials for control system equipment.

### **Two form factor authentications**

Authentication is the process of validating identity. Methods of validation can be broken down into three categories, or factors. They are:

- Something you know (a secret, like a password or PIN);
- Something you have (a token or object that is unique);
- Something you are (biometrics, such as fingerprints, retinas, or gait).

Making something more secure by using two passwords to access it is the same as making it more secure by using one password that is twice as long as the other. The use of multifactor authentication means that the mechanisms are unrelated and require independent means of 'cracking'.

To protect the link or at least access to the information resource or device, critical control system assets should be deployed with dual-factor authentication. Multifactor authentication is now required for remote communications between main control centers and backup facilities. This procedure is also used when field technicians connect remotely to critical operational resources for system recovery, diagnostics, and upgrades. Clearly, an attacker gaining access to these channels could cause significant damage, because once granted, instruction sets are interpreted as coming from trusted sources.

Using centralized servers for multifactor authentication is critical for remote access security. The software should be standardized across all remote connections and should be installed on permanent servers or mobile tablet computers. These standards enable organizations to create remote access control lists and audit functions that ensure only authorized activity occurs in the operational domain.

While it is incorrect to assume that every organization must prevent attackers from capturing static usernames and passwords that can be reused, organizations must conduct risk assessments to determine the level of protection required to secure remote access credentials. Some organizations prefer multifactor authentication over cryptographic channels for primary critical systems and force initial authentication connections to demilitarized servers. A defense-in-depth strategy can be used to secure remote access without impeding business needs.

Managing the supporting technology comes with the deployment of security counter-measures, particularly those used to control access to operational assets. If multifactor authentication is used, a standardized method for administering remote access is required, which may entail a dedicated server or services. The location of these servers will determine who bears the costs of ownership and management. Predefined server responsibility, like managing firewalls and intrusion detection, will help speed up a more robust remote access solution. Incorrectly managed access control capabilities could be exploited by an attacker.

### **Authorization levels**

Following the threat and risk assessment, the secure remote access system may need role-based authorization levels. The default user level should be read-only, just as access control lists in a newly deployed firewall prohibit all access (until access control lists have been established to provide only authorized connections). The concept of least privilege is used to restrict network access. When making changes on the network or controlling system devices, users must escalate their privileges.

In a control system environment, remote access to a single point should not automatically provide access to multiple points. Despite common sense, organizations must recognize that rapidly emerging interoperability with historically untrusted networks necessitates consideration of the consequences of trust exploitation. The security posture of organizations that provide a single level of authorization for remote access users, especially those that support operations across enclaves, may be compromised.

Organizations can reuse remote access authentication and credentialing capabilities for any operational domain or asset by simply allocating identity and value to it. Also, re-authentication and authorization are required for multiple control networks, as per the policy directive. Identity management techniques should be used to separate the corporate account of a user from the control system account. All changes to authorization levels and identity data are auditable and achievable for change management, incident response, and forensics. This approach has worked in many sectors and mission-critical domains.

### **Dedicated client hardware and software**

A remote access solution must provide users with both the software and hardware required to connect. As a result, both the hardware and software of a dedicated remote access client are vulnerable. Once an attacker has access to client hardware or software, their options are limited only by the system's local security.

Remote access software on standard mobile computing devices has allowed attackers to access both operational data and networks. Ideally, the technology for doing business and accessing it should be kept separate.

The organization should provide a dedicated PC or laptop for VPN access, centrally managed and hardened with a remote access-specific baseline image. On the PC or laptop will be anti-virus software and host-based intrusion detection systems software, as well as security counter-measures designed to meet the specific needs of field operations and control system functionality. It should be stated in the PC or laptop policy and procedure that this system is for secure remote access. Another option is to use the system's MAC address as an additional authorization factor. Many organizations find it useful to tune remote access resources to specific hardware identification metrics.

If a PC or laptop is not available, providing antivirus and spyware removal tools for the user's home computer is advised. Aside from dedicated ICT resources for remote users, personal computers should be configured to meet the specific security requirements for remote access.

Organizations that require remote access to control system operations should be able to secure any computer with cryptographic and disk encryption to protect operational data. The user's home computer should never be used for remote control operations, but if it is, secondary and tertiary identification/authorization methods should be established, as well as current antivirus, anti-Trojan, and anti-spyware software. Access procedures and security precautions must be taught regardless of whether the organization uses dedicated resources or personal home computers. The security element of a remote access solution is incomplete without adequate cyber security education covering threats, risks, vulnerabilities, and consequences.

### **Session termination**

An important concept in remote access is session establishment. When discussing secure remote access, managing and protecting that session is crucial. Session and session termination are essential components of secure remote access. Some remote access sessions may be set up permanently, usually to meet availability communication needs. Remote access solutions must be deployed with viable and effective termination mechanisms. For any secure remote access solution, session termination is required, either manually or automatically.

Some of the more serious oversights related to remote session termination that have been observed in control systems environments have led to the creation or the unintentional support of covert channels and situations of denial of service. Regardless of the method used for remote connectivity, communications channels need to be configured to terminate under certain conditions. These can include, but should not be limited to:

- Termination of the session after a set period of time;
- Termination of the session upon reaching predefined triggers (time of day, day of week, on request, data type, file size, etc.);
- Termination of the session based on inactivity;
- Termination of initial response capability based on number of failed attempts;
- Termination of session based on cryptographic key exchange failures;
- Termination of session based on quality service;
- Termination of session based on confirmed tampering.

◀ Preliminary Activity for Week 17

Jump to...



Analysis, Application, and Exploration for Week 17 ▶



## Navigation

Home

 Dashboard

Site pages

My courses

Capstone Project 2

Network Defense and Remote Access Configuration

Participants

General

13 [Enter Module Title Here]

14 [Enter Module Title Here]


15 [Enter Module Title Here]

16 [Enter Module Title Here]

17 [Enter Module Title Here]

 Preliminary Activity for Week 17

 **Lesson Proper for Week 17**

 Analysis, Application, and Exploration for Week 17

 Generalization for Week 17





Evaluation for Week 17



Assignment for Week 17

OJT/Practicum 2

Seminars and Tours

Courses



## Fair Warning

**NOTICE:** Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.***

**PROSECUTION:** Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following:  
Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense.  
Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

**COURSE OF ACTION:** Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.



## Activities



Assignments



Forums



Quizzes



Resources

Bestlink College of the Philippines  
College Department

Powered by [eLearning Commons](#)