Lesson Proper for Week 16

CONFIGURING AND MANAGING REMOTE ACCESS FOR CONTROL SYSTEMS

Remote access is defined as the capacity for an organization's users to access non-public computing resources from locations other than the organization's facilities in this text. A user or operator can access private computing resources, data, and systems from outside the organization's network.

This definition is useful in many circumstances, an in particular in control system domains and has several security elements that are applicable to this practice guide:

- It allows a single operator to manage several systems within an organization's information enclave.
- In other words, it admits that remote access can be interrupted, halted, captured, or hijacked by a third party without having to breach physical or logical security protections.
- It can limit communication within physically protected zones like compounds or buildings (security of communications within physically protected boundaries is still an important issue but should be considered separate from and beyond the scope of remote access).
- An area of communications security that has traditionally received inadequate attention covers all communications over equipment whose physical and logical security cannot be confirmed expressly by the entity utilizing the equipment.

This definition broadens the concept of remote access to cover previously excluded examples. Connecting two sites via private third-party telecommunications lines is not deemed remote access, even if the telecommunications lines are owned by another company and leased to the organization needing to connect two sites. But they are in this definition. The term includes long-range communication channels like fiber or microwave, where the data or service owner owns the equipment but not the physical security of the transmission media.

Remote access security features and functionality help construct electronic paths to provide permitted and authenticated access into a trustworthy network from an untrusted place. The non-public (trusted) network is the control system network.

This paper is designed to be used for any architecture, including industrial control systems, process control systems, SCADA, or distributed control systems. Industrial control systems refer to all system types that share common characteristics and are defined by current communities of interest and other standards bodies.

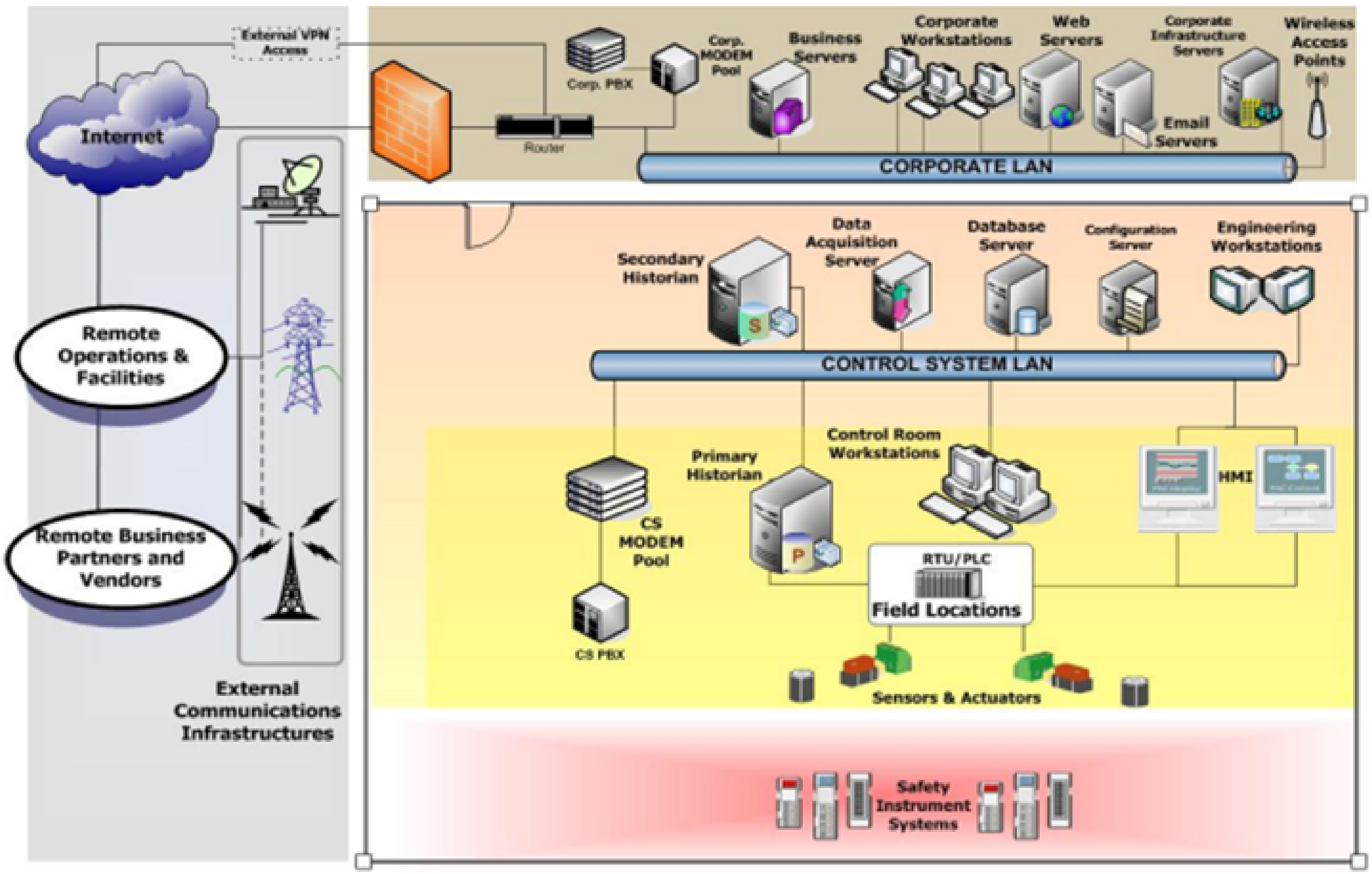
Background

Critical infrastructure systems like industry, water, transportation, and energy rely heavily on information systems for command and control. While legacy industrial control systems remain vital, essential industrial control systems move to new communication technologies. As a result, open architecture standards and common communications protocols replace proprietary industrial control systems mechanisms. This change can have beneficial or negative effects on system integration and support.

In the past, maintenance of the control system was required onsite by integrators and vendors, but new communication techniques allow remote connectivity from nearly anywhere. This enhanced compatibility will enable operators and asset owners to connect to their control systems remotely. The cyber risk is proportionate to the security countermeasures employed to protect against unwanted remote access.

More interoperability in industrial control systems is based on and uses technologies that have been exploited and compromised in the internet and business networking domains. The same is true for remote access technologies, leading to unwanted security vulnerabilities in industrial control systems. According to research, modern ICT mitigation measures do not always fully correlate with industrial control systems due to the complexities of control system designs' availability and integrity.

Figure 1 depicts the separation of a control system environment from supporting corporate architectures and peer locations. This simplified depiction shows that access to the control system domain was either physical access to the facility or remote access via telephone (modem). This image depicts a classic legacy architecture with dial-in vendor access. Onsite service was generally the norm, and firms sought to decrease expenses wherever possible. Security policies and procedures were created assuming external environments featured malicious and hostile threats.

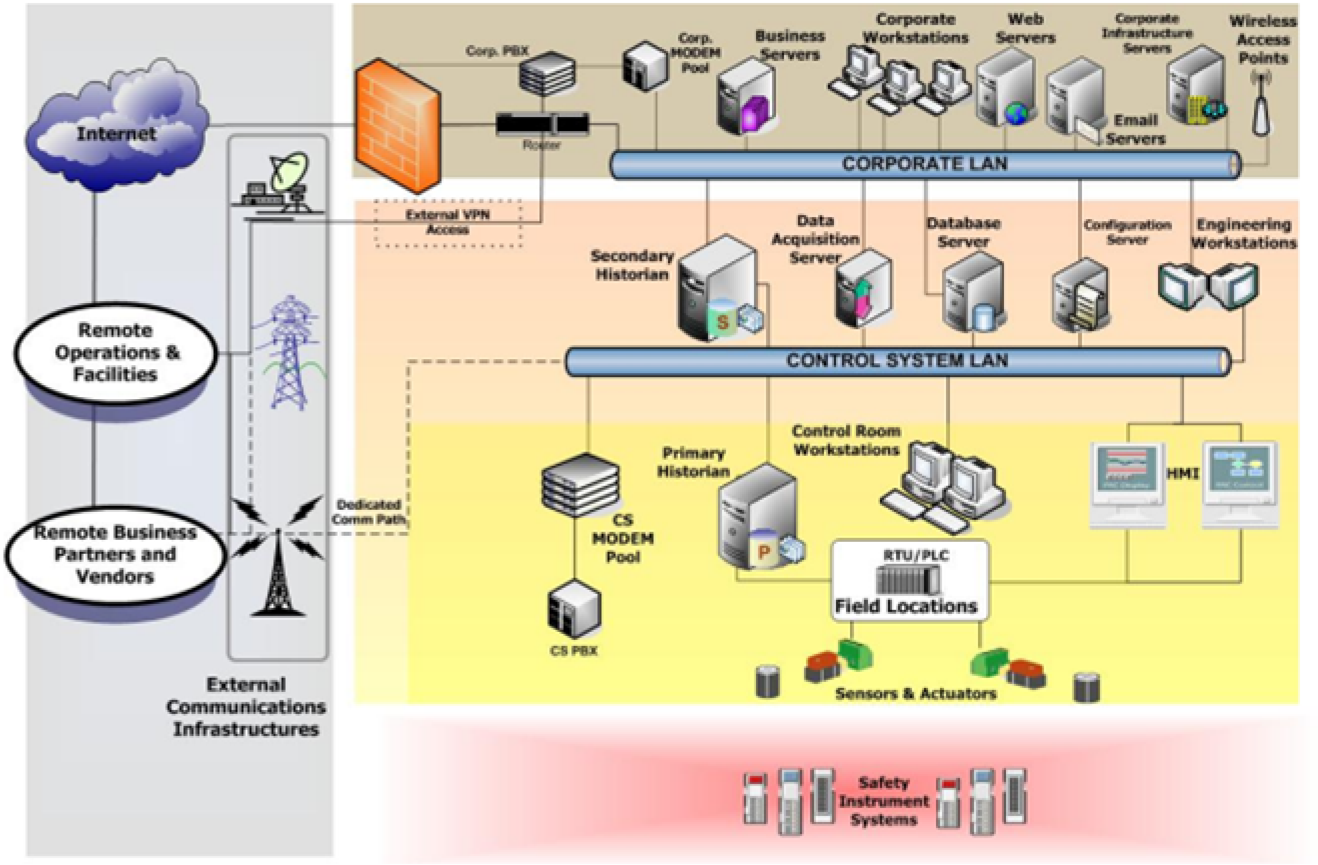


(Figure 1: Traditional Isolation of Corporate and Control Domains)

Because interoperability reduced costs and increased simplicity of use, access to control systems went beyond mere modem and physical access. As firms grew, so did reporting and corporate oversight responsibilities. This necessitates sharing operational information with regulatory authorities, remote operations, peer sites, partners, application and hardware vendors, and third-party service providers.

Remote access in industrial control system architectures

Figure 2 depicts an integrated architecture with links to the corporate LAN, peer sites, vendor sites, and the internet. External communications infrastructure is a frequent aspect in control system topologies, whether locally or distributed across wide geographic areas. This external communications infrastructure connects remote activities, remote facilities, business partners, and vendors to the enterprise. The external communications infrastructure connects to the internet, which is currently the de facto method for remote users accessing business or managing system operations (i.e., telecommuting).



(Figure 2: Integrated Networks)

Figure 2 shows how hacked integrated architectures could give an attacker multiple ways to access vital systems, especially when remote access options are included. The convergence issue raises worries about attackers compromising trusted resources in remote operations, facilities, business partners, and even vendors. These concerns highlight the need for robust and secure remote access solutions for mission-critical control systems. However, as previously stated, implementing secure remote access techniques can be difficult due to the need for availability and integrity. More critically, deploying a secure remote access solution may enhance a control system's cyber risk profile and negatively impact high availability and data integrity.

Roles and remote access in control system architectures

As part of any defense-in-depth approach, safeguarding remote access must involve both users and the technology to be accessed remotely. It's impossible to generalize control system architectures and produce a suggested strategy for protecting remote access that works for everybody. The uniqueness and diversity of both vendor and purpose-built systems create a landscape of diversity that cannot be addressed with a single solution. On can evaluate and use common aspects like users and roles to leverage existing technology and architecture types. It may help organizations shape their remote access strategy by determining who requires access to specific resources and understanding attack vectors that can be created unintentionally.

Understanding users and responsibilities can help shape a remote access strategy. In most control systems operations, the roles that would require remote access to control assets may include, but are not limited to:

- System operators and engineers for local systems
- System operators and engineers for remote systems
- Vendors
- System integrators
- System support specialists and maintenance engineers
- Field technicians
- Business partners
- Reporting or regulatory entities
- Customers
- Supply chain representatives
- Managed service providers

It is impossible to develop a list that covers all systems in all sectors, so it should be updated as needed. The responsibilities of users who need remote access to mission-critical operations can be complex, and assigning particular access based on those roles can be difficult. The assignment of remote access responsibilities and credentials should be part of the organization's cyber security policy, as outlined in this article. Developing a control system remote access strategy involves many roles.

System operators and engineers for local systems

Regular system operators and system maintenance engineers will have the most need for access to a control system environment. Remote access to local systems is required when a control system's growth or expansion requires an operator or engineer to oversee divergent (but connected) resources. Modern networking does not always automatically build access control authorization structures, and if it does, it is not free. Flat networking allows operators and engineers to access mission-critical equipment locally and remotely. Local systems are defined as information resources not connected to the control system network. Not only that, but they share domains that handle tasks like gathering operational data or creating content for client web services.

Modern control system access is usually LAN-based but should be deemed remote if the operator moves between networks. Virtual Private Networking (VPN) is frequently recommended for safeguarding network communication. The trust relationship between operator consoles and services requiring access makes many organizations believe these safeguards are unneeded.

Most control system domains require trust connections between operators and field device technology. Exclusive trust between operators and field devices was the core of control system operations, appropriate for entirely isolated networks. Unfortunately, current control system architectures carry this inherent trust, which can be easily abused by an attacker who has compromised the control system or administration networks.

System operators and engineers for remote systems

As control systems environments develop in size and capabilities, asset owners will be challenged to maximize operations while minimizing labor costs. An organization will need to have an operator manage many systems to maximize operations. Asset owners must consider the complexity of dispersed settings that allow single operators to manage many parts more critically. In many cases, the operator will not need the same levels of authoritative access across all environments. This affects access profiles for engineers managing operations across several system domains.

Vendors

Vendors' remote access operations used to be unimportant to asset owners. Entities felt comfortable with vendor remote access when systems were completely protected from external connectivity, and only physical or modem access was available. Vendors often integrate remote access (e.g., a modem) inside their technology in modern control systems environments to speed up support operations, including system restoration, updates, and performance monitoring. Vendors can do this as part of a more significant support contract. In many circumstances, these contracts require remote vendor access without operator engagement.

It's intriguing how vendor access affects control system security. The electronic security perimeter protecting data ingress and egress becomes ethereal and difficult to define. Unlike the conventional isolated paradigm, where the asset owner defined the security perimeter, remote access vendors are now responsible for protecting the information enclave. Technically, the vendor's entire internet presence might potentially expose the asset owner, substantially altering the risk profile of the control system once remote access is gained. To provide acceptable security countermeasures for remote access into the systems they support, control system solution vendors must provide adequate security countermeasures for remote access into the systems they support.

Asset owners that rely on remote access from vendors to support their operations should consider a number of different factors in developing their overall remote access strategy. These can include, but are not limited to:

- A secure remote connection between the vendor and the owner's control system can be agreed upon using the procurement guidance language (Reference 1).
- Vendors may be exposed to untrustworthy and hostile settings. An attacker can gain access to the control system by exploiting a vendor network.

- For emergency operational assistance and system maintenance, vendors frequently request remote access. Owners of assets should know that remote access connections can be scheduled and monitored.
- A vendor's remote connectivity solutions (i.e., modems) may be deployed in a standardized fashion, and so the authorization credentials required to access a large number of control systems may be highly similar, if not identical.

Integrators and system support specialists

Integrators differ from suppliers in many ways. The involvement of an integrator in solution provisioning typically prohibits the asset owner from directly interacting with the vendor. This single degree of separation can significantly impact an organization's cyber risk posture. Remote access difficulties for vendors may equally apply to integrators. Security has a nontrivial cost. Some integrators are unwilling to go beyond the default defenses built into remote access technology to ensure secure remote access. Most integrators have a standard solution for remote access, which usually involves a modem or other low-cost way of giving support from a remote location.

Field technicians

One new issue is how field technicians access key systems for operations, maintenance, or performance metric supplying. As many industries implement programs to acquire field operations data quickly, the technologies employed for remote connectivity must be investigated. Traditionally, field technicians reported operational data at the end of each shift, generally physically and centrally. New business needs, such as grid operations or water safety, necessitate regular communication between personnel and engineers operating control systems. Field technicians must send data to utility management systems.

In many cases, the data required to optimize control system operations are housed within corporate or commercial settings. Because penetration of these communication channels can give an adversary extensive access to fundamental system activities, several distant communication techniques need to be assessed from a security standpoint. Furthermore, field data are crucial to achieving high availability demands, so remote access for field personnel must be maintained.

Modern secure remote access systems offer many benefits to asset owners supporting industries that demand continual field support. Remote access solutions integrating virtual networking and multifactor mutual authentication to centralized servers can protect vital communications pathways while maintaining business objectives.

Physical security must be considered in remote access protocols for field personnel. Field technician computing devices are more likely to be stolen than other computing resources. Suppose the organization's remote access solution allows field computer users to access control devices. A thief or attacker in possession of the stolen computing equipment may also obtain access to control system assets unless appropriate security measures are applied.

Business partners

Whether the connection between an asset owner and a business partner is new or old, there is always concern about data theft and exfiltration. Business partners may now easily extract information from peers with current network connectivity. This access is typically allowed by default due to prior business and asset ownership agreements. Because a business partner has direct access to a control system environment, asset owners must manage and safeguard this access.

Aside from dedicated lines and cyber security standards, limiting a business partner's access to control system operations is required. When a business partner's remote access is poorly handled, the ramifications of a hacker or disgruntled insider compromising crucial control systems can be overlooked. Cyber incidents involving business partners might have devastating consequences that could (in the worst instance) lead to the business's demise. Situations requiring business partners to access mission-critical activities necessitate a new viewpoint on remote access solutions. This study's output can help determine appropriate remote access controls.

Customers

However, current advances in data aggregation methods and customer service needs are changing this. The conventional barrier between end-users and crucial control system operations is increasingly blurred by intelligent grid technology. To put it simply, a utility network and a web presentation server farm can separate vital energy distribution processes from the consumer residence. The remote access provided by asset owners to their consumers’ needs a thorough cyber-security examination.

Supply chain operations

Supply chain management is typically disregarded when considering remote access options. In many modern production contexts, the supply chain ensures timely and correct delivery of raw materials and services. Many manufacturing and utility asset owners would fail without providing materials and support from their supply chain. Because a company's success is connected to its ability to create products or services quickly, supply chain operations must have fast access to information. This access often involves a direct connection with control systems environments, focusing on stock levels and outputs. Supply chain operations impact the firm in many ways, including quality assurance, transportation, and safety monitoring.

Managed service providers

Asset owners allow managed service providers (mostly employed in ICT domains) to control system operations directly. These services are frequently offered as cyber security services, requiring control system access to assess security postures. Vendors also sell these services with full access to the control systems environment to ensure operational stability.

Financially, it makes sense to outsource system operations to a reputable third party, reducing the need to staff specific operational tasks. The advantage could outweigh the risk if the managed service provider can deliver services that support system integrity and availability. However, remote access to the managed service entity must be carefully structured under an extended security agreement, and the service provider is responsible for safeguarding the communication line. Security must be handled by the provider, not the company that helped set up the remote-access feature.

It creates problems in many areas, mainly when the service provider actively works to limit threats in production situations. Many service providers are empowered to remediate cyber issues by utilizing remote access actively. In many cases, this is a viable and desirable activity, but the sensitivity and unique nuances of control systems contexts make this a risky move. For example, they introduce new antivirus software into a production environment or mitigate peer-to-peer interaction vulnerabilities in the control system. In addition to ensuring only the managed service provider has access, implementing untested security updates and mitigation techniques might negatively impact production settings.

Other considerations

Owners of assets requiring remote access to any aspects mentioned earlier have several options, including tunneling, direct application access, access portals, and remote desktop access. Given the high availability and integrity requirements for control systems, asset owners must carefully balance remote access solutions with business objectives. Companies should be mindful not to establish inadvertent entry points when evaluating remote access solutions. Regardless of the resolution, the following elements are universal:

- Remote access allows users to store critical information locally on their computer or device.
- Remote access solutions are not restricted to using single modes of authentication. The risk associated with information disclosure or compromise can sometimes demand several modes of authentication combined with several different modes of server access.
- Cryptography has and will continue to be part of the remote access solution, but cryptographic communications may impact the timeliness of communications expected and the processing capacity of control system elements within some critical operational environments.
- All remote access solutions depend on the physical security of the devices and authentication elements (e.g. passwords, tokens) initiating the remote connection.

The hazards in industrial automation environments are distinct in defining the roles required for access to control systems domains. Without understanding the intricacies of high availability networks, a secure remote access strategy cannot be developed, including current and older architecture aspects. To prioritize issues, factors such as interconnected IP and serial networks and other communication mechanisms bereft of security protections are considered. Several difficulties should be considered when developing control system remote access solutions.

Unintentional entry points

Control systems have typically converged with other designs at a rate that allows for unintended and unsecured access. Technical capabilities typical in isolated systems often remain in updated contexts because removing them appears to hinder productivity or because they are required to meet cultural standards. Data servers and printers are two prominent examples, both network-enabled and considered low-risk from a cyber-risk standpoint.

These complicated machines have enormous processing horsepower that can easily be used to support numerous activities, including those that benefit a cyber-attacker. Printers are utilized for network diagrams, productivity reports, and other operational duties that require printed hard-copy information. Printing machines are frequently deployed as trusted information resources that can connect to many networks. This is a standard practice because the printer is deemed low-risk.

Having one printer serve many networks saves money. The compromise of a modern printer (together with access across conjoined domains) can provide an attacker with extensive entry into the operational environment.

Wireless interoperability solutions, for example, can unintentionally establish unintended entry points. The operational domain entry points do not have to be from the control system. Compromised wireless access to an automation environment might have a similar impact on an organization's cyber risk profile. Securing wireless networks often goes beyond the vendor's essential recommended advice. Organizations tend to reduce the rigor required to safeguard wireless communications environments when availability is critical due to the variety of wireless solutions available.

Modern networking technology has given control system operators new tools for controlling day-to-day operations. Web-based control systems and field device capabilities have allowed operators to manage many assets across a large area.

However, an attacker can quickly exploit underused or mishandled communications functionality, especially when the asset owner is unaware of its existence or the default deployment requires its activation. Remote monitoring, system diagnostics, and firmware updates are possible with embedded systems in field devices. This can generate unintended entry points into a system that an attacker can exploit if left unattended.

Unintentional access paths created by remote access solutions are a major risk. Businesses must be ready to install intrusion detection and prevention systems to limit the risk. Fortunately, there is a long history of successful ICT-oriented remote access solutions. Traditional solutions must be tailored for the control systems environment, while cyber security mitigation measures must be harmonized with business requirements.

REMOTE ACCESS IN MODERN ICT ARCHITECTURES

Requirements

Understanding the fundamental prerequisites for implementing remote access programs is crucial. Access to and from mission-critical environments is not usually confined to automation operations. In many circumstances, legitimate aspects of the business operation architecture demand data from control system resources. Remote access requirements are assessed from an ICT perspective to design these requirements.

The following list covers some of the more popular remote access priorities for traditional ICT systems. Anyone who needs crucial information or services to accomplish their job must have easy and meaningful access to them.

- The solution must ensure that resources can access their information and essential services from any location if required and allowed by policy.
- The solution must ensure that resources can access their information and essential services from multiple device categories.
- The solution must ensure that critical information is available for use at a moment’s notice (according to expected service level), that the critical information is always accurate and complete and that confidential information is provided only to those who require it.

Important, private information must be safeguarded against misuse or loss. When examining data sets, security professionals assess the data's confidentiality, integrity, and accessibility. The business consequence of not maintaining these security requirements varies depending on the data set. Indeed, the definition of a cyber-risk varies depending on the sector that employs industrial control systems.

Types of remote access solutions

A user (or system) connects to another system via remote access (or information asset). There are technology disparities between solutions, much as there are access needs. Some companies do not question the ability of the service provider to safeguard communications across their infrastructure.

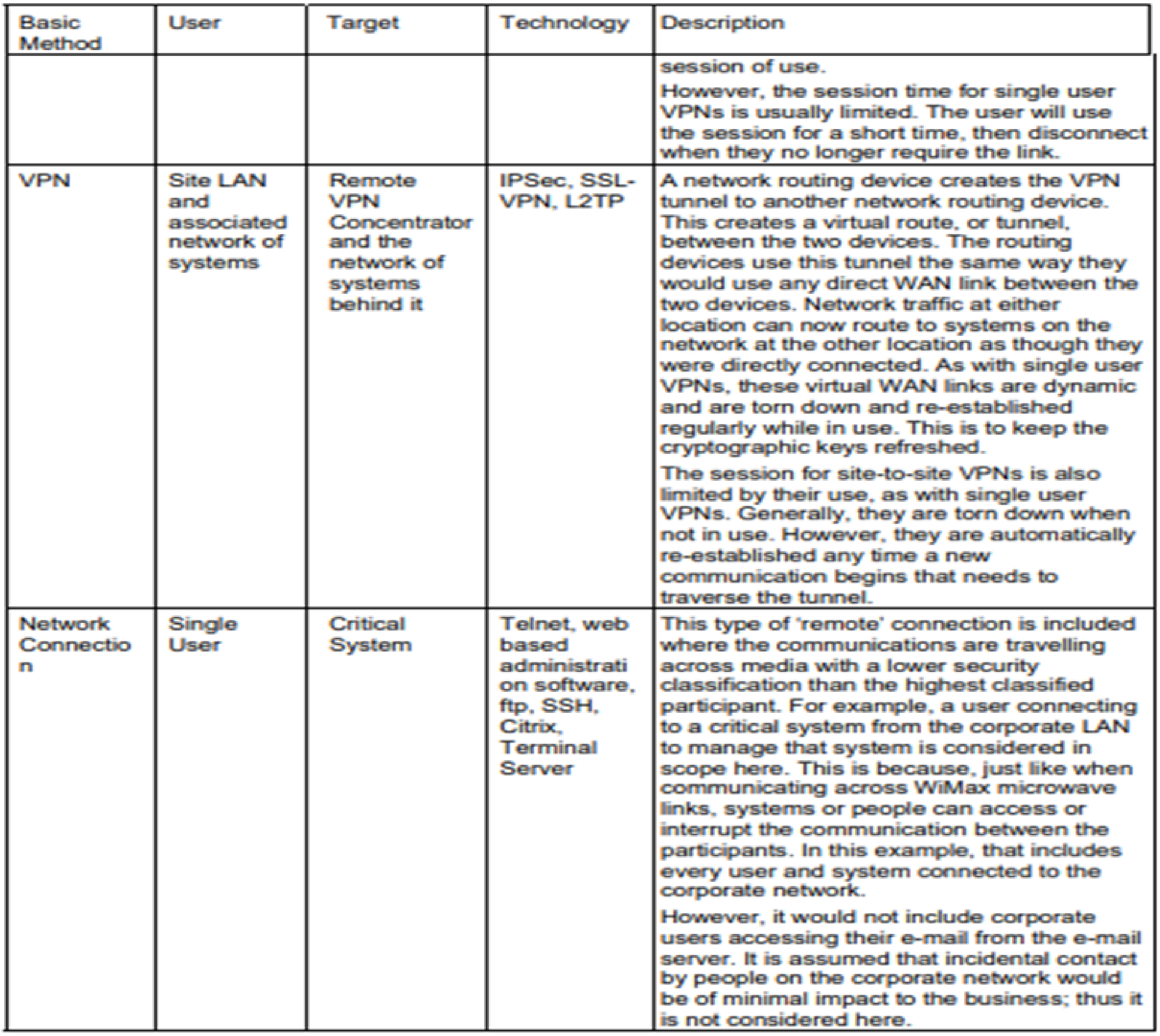
Satellite and POTS modems are examples of this. Microwave links, long-range fiber optics, and copper lines are examples of third-party infrastructure. The technologies are the same as the previous example; the communicating party owns and operates them. VPNs, telnet, secure shell (SSH), and others are used to connect places.

Remote access has become a hazard due to modern application technology. Recognizing the applicability of technological solutions for both people and services can be difficult. HTTP and HTTPS channels are now encapsulating several communications protocols, and web-based applications are managing them. Web-based apps that present data to multiple user populations are becoming more globally accessible.

Table 1 shows a sample of different remote access solutions that have been used over the years in the ICT domain that has found applicability in control systems environments.

Basic Method	User	Target	Technology	Description
POTS or Integrated Services Digital Network (ISDN) Dial-Up	Single User System	Direct to Target System	Modem	A single user has a modem connected to either a POTS, or ISDN line and directly calls a computer system, which also is connected to a POTS or ISDN modem. This is a direct connection, which usually only allows a single user at a time to gain access to a single system. This method of remote access was very common prior to widespread use of the internet and is still in use today for accessing legacy systems.
POTS or ISDN Dial-Up	Single User System	Remote Access Server (RAS) and network of systems it serves	Modem	A single user has a modem connected to either a POTS or ISDN line and calls a RAS. This RAS does not provide application services to the user. Rather, it is a gateway to other systems that do provide the user with services and authorisation can be done at any number of access points. This method extends network connectivity to the user. The RAS server becomes, essentially, a router on the network, which has a network on one side and a single endpoint on the other.
POTS or ISDN Dial-Up	Site LAN and associated network of systems	RAS Server and network of systems it serves	Modem	A packet routing device uses a modem to connect to either a POTS or ISDN line and calls a RAS. This RAS does not provide application services to the calling device. Rather, it acts as a packet routing device (or bridge) to allow network traffic to pass from one network to the other. The phone line becomes a wide area network (WAN) link and packets are routed across it as needed. This method extends network connectivity between two arbitrary-sized networks, just like any other WAN network technology. In this example, the distinguishing factor is that the connection is usually temporary - established on demand and torn down when not in use. This is not a requirement and permanent WAN connections have been established over POTS and ISDN. However, this was the exception.

Basic Method	User	Target	Technology	Description
WAN Links	Site LAN and associated network of systems Single User System (rare)	Router/bridge and network of systems behind it	Varies	A WAN link is any telecommunications method to encapsulate network traffic and transport it over long distances. In the previous example, this was accomplished using POTS or ISDN lines from a telephone company. Other long-haul communications links are available. Some are wired such as leased Telco circuits (T1, T3, DS0-3, Frame Relay, ATM, MPLS, Broadband cable, DSL). Others are wireless (802.11, WiMax, Satellite uplink, other line-of-sight microwave, short-wave). Single user and point-to-point links using these technologies are possible, but very rare because of expense. In this example, the distinguishing factor is that these links are mostly permanent, rather than established on demand.
Local Wireless	Single User System	Wireless router and the network of systems behind it	802.11	A single individual with a wireless access card, or wireless local area network (WLAN) card, is connecting the one system to an organisation's wired network through a wireless access point. The wireless access point acts as a bridge, allowing the wireless-enabled device to connect to the local LAN, as though it were connected directly using a network cable. This connection method is not yet widely considered remote access. However, the wireless signals are not bound to remain inside a space under the physical control of the network owner. Therefore, it has all the vulnerabilities of any other type of remote access and should be included in remote access technology.
VPN (Virtual Private Network)	Single User System	Remote VPN Concentrator and the network of systems behind it	IPSec, SSL-VPN, L2TP, SSH Tunnelling	A single user applies VPN technology to create a layer of protection for the user's communications and then sends that communication over any of the previously mentioned links. The VPN technology essentially creates a tunnel, where the data inside the tunnel are protected using cryptographic techniques. It can be considered a virtual WAN link, which is encapsulated within typical WAN traffic. A VPN link is always dynamic in that it is established on demand and torn down when no longer desired. VPN links need to change their cryptographic keys regularly, so tunnels are re-established with new keys often, usually more quickly than any single



Basic Method	User	Target	Technology	Description
				session of use. However, the session time for single user VPNs is usually limited. The user will use the session for a short time, then disconnect when they no longer require the link.
VPN	Site LAN and associated network of systems	Remote VPN Concentrator and the network of systems behind it	IPSec, SSL-VPN, L2TP	A network routing device creates the VPN tunnel to another network routing device. This creates a virtual route, or tunnel, between the two devices. The routing devices use this tunnel the same way they would use any direct WAN link between the two devices. Network traffic at either location can now route to systems on the network at the other location as though they were directly connected. As with single user VPNs, these virtual WAN links are dynamic and are torn down and re-established regularly while in use. This is to keep the cryptographic keys refreshed. The session for site-to-site VPNs is also limited by their use, as with single user VPNs. Generally, they are torn down when not in use. However, they are automatically re-established any time a new communication begins that needs to traverse the tunnel.
Network Connectio n	Single User	Critical System	Telnet, web based administrati on software, ftp, SSH, Citrix, Terminal Server	This type of 'remote' connection is included where the communications are travelling across media with a lower security classification than the highest classified participant. For example, a user connecting to a critical system from the corporate LAN to manage that system is considered in scope here. This is because, just like when communicating across WiMax microwave links, systems or people can access or interrupt the communication between the participants. In this example, that includes every user and system connected to the corporate network. However, it would not include corporate users accessing their e-mail from the e-mail server. It is assumed that incidental contact by people on the corporate network would be of minimal impact to the business; thus it is not considered here.

(Table 1: Different Remote Access Solutions)

Security considerations

The goals of maintaining an asset's data integrity and availability are de facto fundamental reasons why businesses want to protect their control network assets. This approach aims to provide remote access programming assistance for the control system community. Thus, integrity and availability remain paramount. To achieve this purpose, two key ideas are generally applicable.

"One must allow access to information or services only to those who need it," argues the concept of least privilege. Alternatively, 'One must restrict access to data or service to only those individuals or systems that need it. This principle assumes or implies:

- One or more robust protection mechanisms must be in place to restrict access to data and services.
- The requesting users and systems can identify themselves in some fashion to whatever protection mechanisms are in place.

- The protection mechanism must be able to authenticate the identity provided to it. This is a proof mechanism, where the claimant must prove beyond a reasonable doubt that they are the owner of the identity presented for consideration.
- The protection mechanism(s) must control access to only the information sets and services that the authenticated user or system is permitted to access or use.

The idea of least privilege also requires an organization to consider default remote access options and access to vital field equipment. For example, default configurations can provide paths to the crucial equipment. Embedded remote access technology in field devices should constantly be analyzed for potential risks.

Defense in depth is the second premise that supports the first. Consider all possible data or service access vectors, especially those that separate business operations from mission-critical control systems. Defense in depth has three basic components, each with detailed controls. They are:

- Prevention - a series of controls to ensure the security of information, systems, or services;
- Detection and response - controls to detect when prevention fails and respond accordingly;
- Security management system - a set of practices designed to continually evaluate and adjust security controls to more closely meet the requirements of a particular environment, industry, or organization.

Determining requirements

Always comprehend the criticality of the system or service requested by a remote user. A security categorization system is essential to ensure that every system or information asset is protected to its worth.

This aligns the effort necessary to build and manage controls for an asset with the commercial effect of compromise or interruption. This technique is rooted in hazard operation management and has specific application in the control system area.

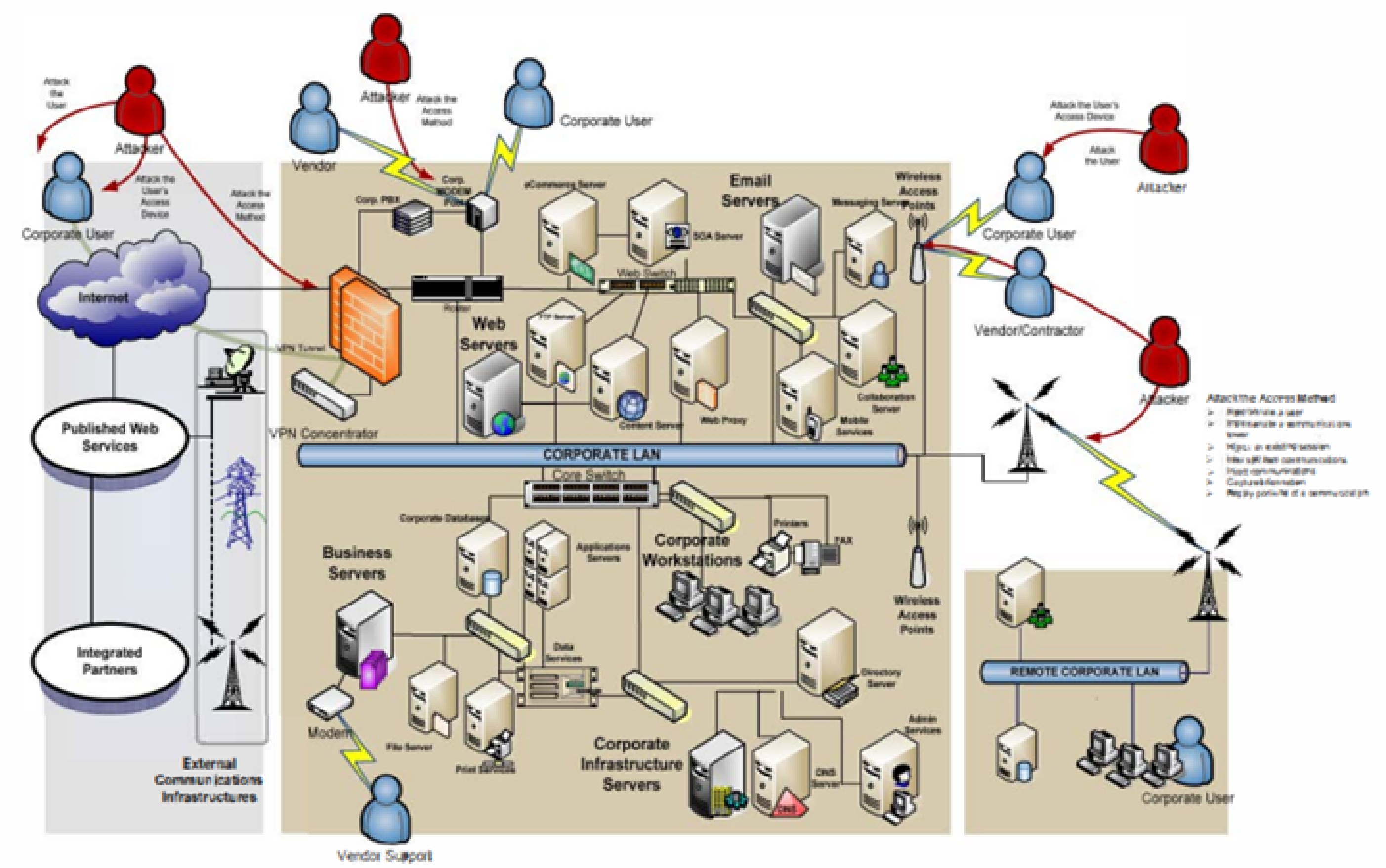
The organization's willingness to grant access to a system or information asset must also be evaluated. Using zone and conduit models requires understanding essential asset classification, who needs access to them, and when.

The next point to grasp is the controls required to adhere to the security standards. To comprehend the controls, one must understand the dangers and attack vectors. Figure 3 depicts a hypothetical vector access point diagram. The remote access components will be broken down and discussed independently, then joined to examine second-order difficulties.

Attack vectors

Beginning at the remote user and following the connection to the data or service, remote access can be compromised at any of the following points:

- The user or system can be impersonated to fool the target system;
- The attacker can use captured or guessed credentials to impersonate the user;
- The attacker can intimidate or coerce the user to provide valid credentials, or to perform activities at the attacker’s demand;
- The user’s access device (laptop, PDA, etc.) can be attacked and compromised and used to access the control system network;
- The target system can be impersonated by an attacker to fool the user and thus gain credentials or other information from the user system;
- The communication can be listened to by third parties anywhere along the communication chain;
- The communication can be interrupted or jammed;
- Communications can have data injected into them by an attacker;
- The communication can be hijacked after it has been initiated (does not rely on impersonation) or intercepted during initiation (impersonate both user and target, also known as a man-in-the-middle attack);
- Parts of a communication can be replayed to a target, even if the attacker cannot decipher the content (also known as a replay attack);
- The target communication software listening for requests can be attacked and potentially compromised;
- An attacker can impersonate a valid communications node and gain access to the underlying communications medium;
- Denial-of-service attack to authentication server (e.g. radius server or RAS);
- Denial-of-service attack to outward communication device (e.g., modem bank, outside router for remote access).



(Figure 3 Attack vectors when using remote access)

Secure communications

Media are not generally secure. An electrical device can intercept unprotected communications anywhere along their physical path. Wireless communications can be captured with a simple antenna, protocol analyzers, and other technologies. Advanced attackers can replicate part or all of communication, introduce bogus data into the communication stream, and even assume the identities of one or both conversing parties. Even fiber optics are susceptible to taps, interruptions, and forging.

These vulnerabilities require several preventative controls to remedy them.

- Secure Channel - a mechanism to prevent a third party from capturing the communication in an intelligible format. This is accomplished using advanced cryptographic capabilities.

- Robust Channel - a mechanism to ensure the integrity of the communications so that the communication cannot be altered in transit without detection. This is accomplished using advanced cryptographic capabilities.

- Available Channel - a mechanism to ensure the availability and timeliness of the communications so that a reliable data channel can be established. This is accomplished using various anti-distributed-denial-of-service techniques, load limiters and anomaly detection.

- Device Hardening - mechanisms to enhance and ensure the security of the systems at either end of the communication, so that they cannot be compromised. This includes robust access controls (see next section), patch management, configured according to the principle of least privilege, etc.

Access control

Systems that need to secure information and services or restrict access to information and services must use access control methods that follow the concept of least privilege. Historically, ICT architectures have had minimal trouble assigning users the least privilege. Historically, single users had authoritative access over the whole infrastructure, and physical countermeasures constrained access. If a system lacks access control functionality, it should be provided somewhere in the communication chain. For example, network firewalls protect systems against inbound communications by blocking all except the required techniques. Systems must include the following security aspects to safeguard essential resources, services, data, or communications. Although derived from ICT best practices, the principles can be applied to control systems.

Every system in the user-to-goal communication chain should have these features. Although these capabilities can be easily deployed in ICT frameworks, the requirements for availability and integrity (sometimes coupled with non-standard technologies) necessitate deployment in control system domains.

· Identity establishment - a framework for providing or exchanging unique identities. User IDs are a common method, but are difficult to make both unique and meaningful in large environments and are not portable. E-mail addresses are portable because they incorporate the organization name, but are difficult to make both unique and meaningful in large environments. Certificates are the preferred method. They can be federated (are portable) and the identity is an amalgam of many bits of identity data, rather than a limited user ID string, allowing them to be both unique and meaningful for very large groups.

· Identity validation - a mechanism designed to ensure the identity of each party to the others and one that cannot easily be forged. This can be as simple as a user password (called a 'shared secret' in the case of systems), but passwords are easily guessed, divined, or stolen; and therefore, identities that rely on them are easily forged. The preferred method is a one-time-password token or a password protected private key associated with the subject's signed, public certificate.

· Duress alerting (optional, but recommended where available) - an Identity Validation solution that provides secondary credentials to users who can supply them to an attacker when needed. The use of secondary credentials will provide access to systems, data and services, but will alert operators and authorities that the user is under duress so that they may take appropriate action. This allows the user to protect themselves from a physical attacker who demands credentials to gain access to critical services.

· Roles - groups of users or systems organized according to their responsibilities. This can be centralized or distributed. Modern systems are centralizing this function more and more, though there are designs that can provide decentralized role management.

· Access rules - lists of access rules that govern which groups and individuals are allowed access to certain resources at what times. These should be carefully planned to ensure that they follow the principle of least privilege. This function can be centralized or distributed. Modern systems are centralizing this function more and more, though designs can provide decentralized access rule management.

Logging and reporting

So far, this guide has concentrated on preventative security measures. But this is only one aspect of security. Anomaly detection and reporting are critical to any security architecture. Preventive strategies are rarely thorough, and some of the techniques outlined above struggle in specific situations. Although control system domains are meant to detect aberrant activity (typically by events and alarm management), it has generally been the duty of IT, not automation.

A company may not have the resources to deploy a fully federated identity management solution that works with all legacy systems and apps. Patch management cannot always keep a system up to date since updates may break important business software, leaving security vulnerabilities unpatched. Also, network encryption cannot always be used over WAN networks due to the added delay, which prevents some real-time systems from working properly. Real-time or near-real-time data acquisition is required in some critical infrastructure control systems to ensure system availability and sustainability.

For example, to ensure that preventative measures are not evaded or to recognize when someone or anything gains access to something they shouldn't, it is vital to monitor activity on or directed toward critical assets and services. The following list contains some examples of events that your logging system should identify and inform someone or something about.

- Monitor failed authentication attempts - all devices or processes that require identity authentication should log and/or alert when an identity validation attempt fails.
- Monitor successful authentication attempts from different sources - If available, all devices or processes should log and/or alert when the same user logs in simultaneously from two different source locations.
- Monitor successful authentication under duress - for critical systems, consider deploying an authentication mechanism that supports duress codes. This allows a user under duress to log into a system using a secondary credential, but alerts that the access was performed under duress.
- Monitor failed access attempts - all devices or processes that manage access control to communications, data, or services should log and/or alert when access is requested that is not allowed.
- Monitor successful access attempts - all devices or processes that manage access control to communications, data, or services should log when access is requested and allowed.

Set up procedures for processing these notifications. In modern control system architectures, user demand has prompted providers to build comprehensive monitoring capabilities into their solutions. Aspects of performance monitoring rather than security are generally highlighted. Abnormality detection functionality can be utilized to help mitigate cyber security risks. Failure to authenticate or access can be utilized to support a robust remote access policy. So, this technique works for both users and services inside the control systems information architecture.

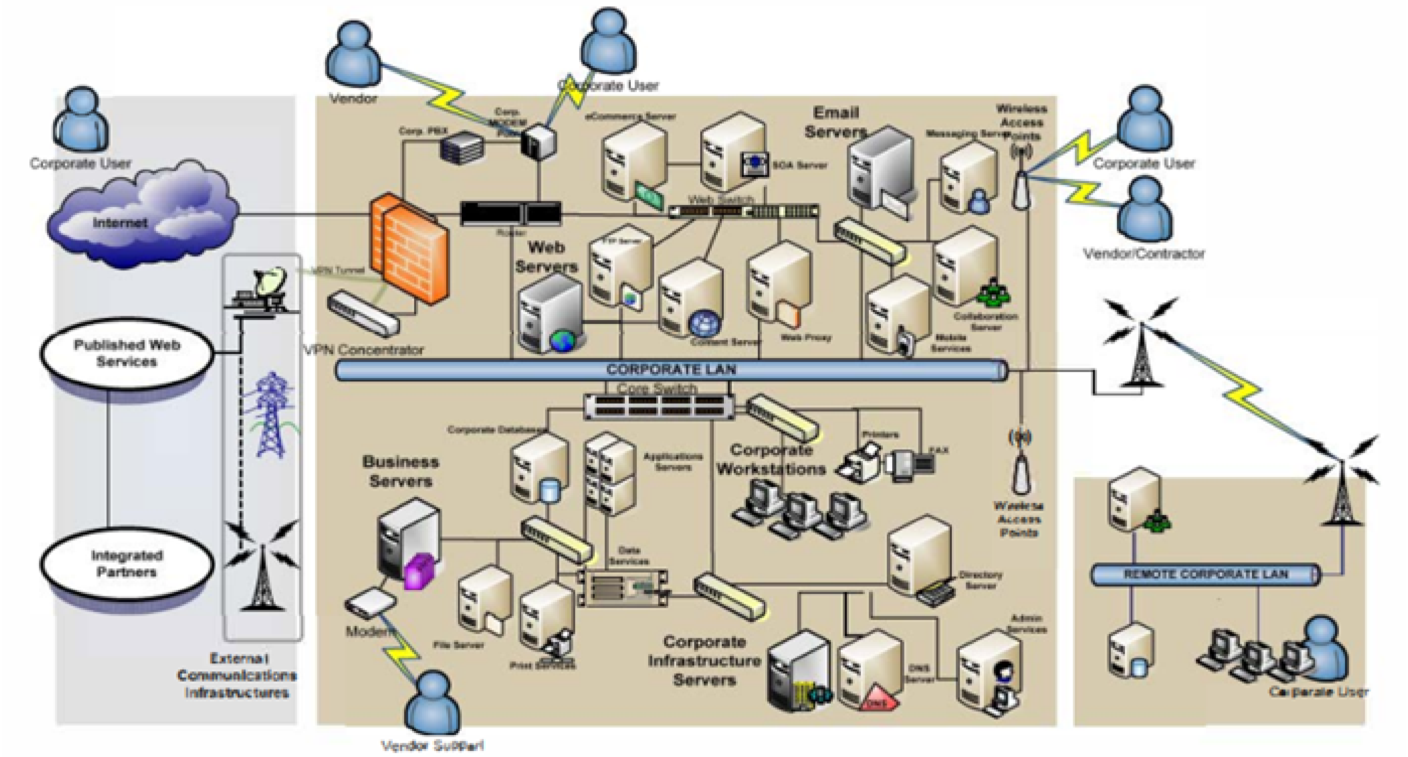
Network Architecture Security

Again, remote access is a subset of network architecture and the techniques to secure it are the same techniques used for securing the whole network. After putting all the items mentioned above together, an example illustrates how to secure remote access into an ICT infrastructure. First, create a list of assumptions:

1. Multiple types of 'remote' users require access into the network for different reasons. Some require access to non-critical systems, others require access to multiple critical systems and others require access to only a single critical system.

2. Multiple WAN connections compose the corporate network, so not all critical systems are necessarily located in the same physical structure.

3. Attackers are prevented from physically accessing resources that are inside buildings or compounds. In these examples, all attacks are against remote access mechanisms as defined earlier.



(Figure 4: Example of Poor Network Security)

As shown in figure 4, the network has poor network architecture. The security of this network is poor as the following security elements are not present:

- Segregation of critical systems;
- Standardized method of remote access;
- Visible distinction between corporate roles to ensure access rights can be granular;
- Acknowledgment of the risks associated with unprotected telecommunications that traverse unprotected physical space.

Several examples of remote access are shown in figure 4:

- Vendors connect to individual systems through direct dial-up modem connections to provide support to critical business servers;

- Satellite offices connect to the main site through telecommunications WAN links that are not in the physical control of the organization;
- Both modems and VPN tunnels are available to corporate users and vendors;
- Wireless access is available to different user groups.

Each of these access methods is susceptible to attack.

IMPROVING SECURITY

Using the principles and techniques described in the section ‘Applying good practices’, the security of this implementation can be significantly improved by tackling each of the vulnerabilities one at a time.

Identify business critical items - This is the single most important part of all security plans, whether for network security planning, safety, secure application development, or reconfiguring systems to improve their local security posture. Knowing how to classify systems in alignment with the probable business impact if they fail allows one to group them physically, logically and conceptually to address their security issues in a coherent manner.

Organize network architecture - Create zones where systems, data sources and computing services are placed in groups whose members share similar security requirements. In the example below, web services have been moved to a demilitarized zone (DMZ) to protect them from both internal and external attackers. Critical services have been segregated to a secured zone to reduce susceptibility to attack from the corporate network should an attacker infiltrate the network that far.

Implement strong and granular access controls - This must be done on business critical systems and services as well as on network perimeters surrounding groups of systems with similar security requirements. The principle of least privilege must be followed when constructing these access controls. Granular access controls should be considered on every system, every application and every network border protection device such as firewalls and VPN concentrators. Figure 5 shows how communications into and out of the ‘Business Servers’ zone can be heavily restricted. For example, users might be granted broad access to the application servers’ web interface, but administrative access could be configured such that administrators would have to first connect to a special administrative server using a cryptographically secured connection and then manage the Business Servers from that one ‘jump’ server.

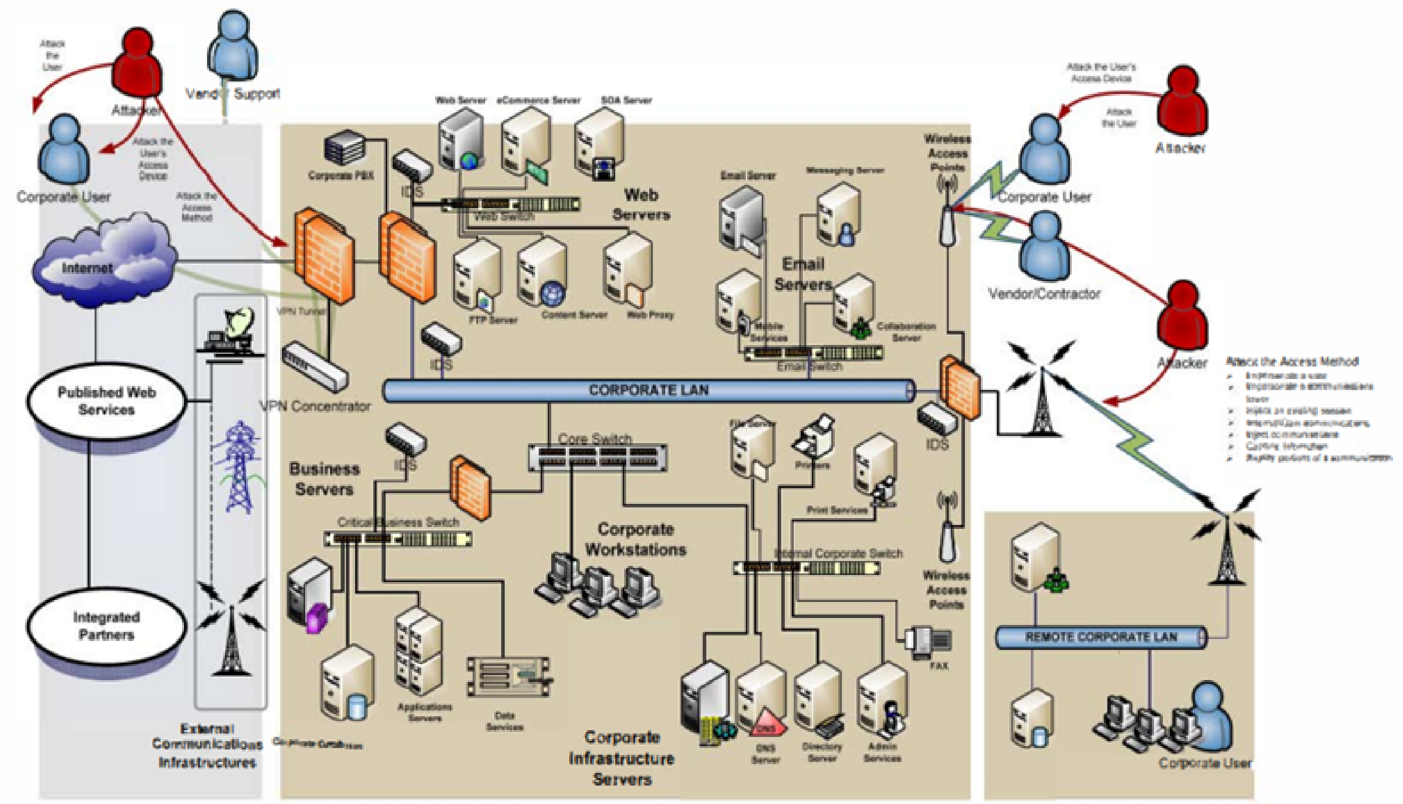
Standardize on one method of single-user remote access - The recommended method is to use a modern VPN, because all modern implementations of VPN technology include strong user and device authentication mechanisms. They also provide an extra layer of network access control, allowing different users to tunnel through to different systems using only allowed communications protocols. In Figure 5, all modems have been removed and vendor support access has been moved to VPN technology. This has normalized the security protocols for all external to internal access and reduced the number of possible points of attack.

Enable remote access only when required - Normal industrial control systems users may require on-demand remote access, but vendor support may only require remote access rarely. One can disable vendor user IDs until they are required to be enabled and then disable them once again when they have completed their task. This technique can be applied to any untrusted group of users who require only intermittent access to corporate resources.

Use strong authentication credentials – Users needing access to critical systems and services should be required to use strong authentication methods, such as one-time password tokens or certificates. These are also known as multifactor authentication methods. Devices such as wireless access points and microwave towers should use strong authentication to identify themselves to each other, so that access rules can prevent unauthorized wireless devices from participating in communications.

Protect wireless communications - Use modern cryptographic techniques to protect WLAN and microwave communications. This makes the wireless communications methods much harder to attack. Injection and replay are very difficult and eavesdropping and hijacking become almost impossible. Most microwave implementations and all WLANs have advanced cryptographic capabilities. The communication lightning bolts in the diagram have been changed from yellow to green to indicate that the end points use strong authentication to validate their identities and use encryption to scramble communications.

Logging, monitoring and alerting - Critical devices should log activity and alert on anomalous events. Devices in this category include all servers, applications, communications equipment and network perimeter devices, which are critical to business operations. In addition, the deployment of monitoring devices captures and examines network traffic for anomalous behavior. They are typically deployed behind network access control devices to ensure that changes to communications behavior do not go undetected.



(Figure 5: Security Countermeasures)

◀ Preliminary Activity for Week 16

Jump to...

Analysis, Application, and Exploration for Week 16 ▶

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]

Preliminary Activity for Week 16

Lesson Proper for Week 16

        - Analysis, Application, and Exploration for Week 16
        - Generalization for Week 16
        - Evaluation for Week 16
        - Assignment for Week 16
      - 17 [Enter Module Title Here]
    - 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 byeLearning Commons