NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Security Guidelines for the Electricity Sector:

Control System Electronic Connectivity

The Control Systems Security Working Group (CSSWG) of the Critical Infrastructure Protection Committee (CIPC) developed this security guideline to share and enhance industry practices that help to maintain Bulk Electric System reliability. The guideline is voluntary and does not create any mandatory obligations. It is not intended to establish new requirements under NERC's Reliability Standards, to modify the requirements in any existing reliability standards nor provide an interpretation of any NERC Reliability Standard.

Executive Summary

The reliability of the Bulk Electric System (BES) depends on the performance of control systems. Intrusions to control system networks may originate from the other networks (internal or external) to which they are often connected.[1] This guideline identifies some key recommendations associated with securing control system networks that are electronically connected to external networks thereby enhancing the security and reliability of the control system infrastructure.

This document provides a guideline for security architecture that appropriately segregates control systems networks and data flows from business systems networks and data flows. As a part of this guideline the document also:

- Defines general principles to provide a foundation for the development of an entity-specific security architecture framework using the guidelines in this document, including network segmentation, monitoring, defense in depth, and configuration management;
- Discusses network design considerations and the associated challenges in a control system environment;
- Applies included general principles and network design considerations to provide guidelines on disconnecting and reconnecting control systems from non-essential communications in order to protect control system integrity when a potential threat to the control system has been identified; and,
- Provides generally accepted practice examples of specific connection topologies for control systems and business systems, as well as control systems with other control systems.

[1] See NIST IR7628 for examples and additional information

Introduction

This guideline addresses specific network segregation practices that can help mitigate security risks to electricity sector organizations. This guideline can be used by electricity sector owners/operators as a part of their risk management process to define appropriate architectures for connecting and disconnecting different types of systems.

Scope of Work

The purpose of this guideline is to provide recommendations to effectively and reliably secure control system networks that are electronically connected to business networks. Specifically, this guideline offers recommendations that can decrease the likelihood of a cyber security intrusion into the control system originating from the business network.[2]

The reliability of the bulk electric system depends on the performance of control systems. Intrusions to control system networks may originate from the external networks to which they are often connected.[3] This guideline identifies some key recommendations associated with securing control system networks that are electronically connected to other networks thereby enhancing the security and reliability of the control system infrastructure.

Physical security is generally not included in the scope of this document. That being said, a given organization may want to protect their physical access control system as it can open doors and impact operations of a given facility and is often associated with the control system infrastructure.

This guideline is limited to connectivity considerations. A complete control system security strategy will include additional considerations, including risk assessment, change management, training, recovery processes, information protection, incident response, etc.

Document Structure

The remainder of the document is organized as follows:

- Section 4 defines general principles for consideration in developing and implementing a security architecture for control systems;
- Section 5 addresses network design considerations that should be taken into account when designing a security architecture for control systems;
- Section 6 provides specific guidelines for disconnecting and reconnecting control systems and other systems;

[2] This document also provides references to other standards and guidelines as appropriate [e.g. The IEC 62443 (ISA-99) series of standards is internationally recognized for providing standards and guidelines for the protection of Industrial Control System (ICS). NIST SP-800-82, "Guide to Industrial Control System (ICS) Security" is another source of information on securing ICSs and addresses most of the principles and concepts presented in this document.]

[3] See NIST IR7628 for examples and additional information

- Appendix A provides a bibliography for this document;
- Appendix B provides a list of acronyms used in this document; and,
- Appendix C provides best practice example topologies for connecting control systems and other systems.

General Principles

The following are general principles for consideration in developing and implementing a security architecture for control systems.

Segmentation

For the purposes of this paper, segmentation will indicate logical separation of systems and associated networks that have varying degrees of impact on the reliability of the control systems. Segmentation is implemented through the use of firewalls, Demilitarized Zones (DMZs), and other capabilities that filter and otherwise limit and control communications between networks.[4] Logical separation does not mean isolation. Rather, it indicates that inbound and outbound communications between control systems and other less essential systems is rigorously controlled. For example, the exchange of data may be made using proxy systems with access controls restricting data required to traverse into the control systems.

Appendix C, Diagrams 1 and 2 further illustrate the above concept.

Monitoring

Monitoring is generally viewed as the means to be aware of the state of a system, and awareness is considered one of the more important security functions. There will always be unknown vulnerabilities, creating risk to the business processes and control systems. This has been seen with Stuxnet, Regin, and BlackEnergy as the most well-known Advanced Persistent Threats (APT) targeting control systems.

For the purposes of this paper, monitoring is not just the collection of security related information, but their active analysis on a 24x7 basis. Monitoring should be comprised of:

- Installation of appropriate devices or applications to capture communications with the control systems;
- Activation of proper event notification capabilities;
- Collection, preferably in real-time, of event notifications to a separate and secure, access controlled, central repository;
- Identification and baselining of what is normal for given control system communications (e.g., IDS); and,
- Analysis and alerting, in real-time, of the relevant data (e.g. logs) from abnormal communication conditions.

[4] Though further segmentation internally to a single security zone can be achieved via VLANs, this document focuses on the interconnectivity between multiple security zones where VLAN based segmentation may not be appropriate.

An important item to remember regarding monitoring is the maintenance of the overall infrastructure. Vulnerabilities continue to change over time as new discoveries are made and attack methods are developed. Just as control systems need to be maintained with updates and adjustments, monitoring systems also need to be updated and adjusted to address the evolving vulnerabilities and attack methods. Monitoring systems are not a set-it and forget-it type of system. They require not only consistent oversight of their usage, but adjustments for changes in vulnerabilities and attack methods. Failure to manage and maintain these systems will slowly erode their capabilities and provide an organization with a false sense of security.

Monitoring is included in many key security guidelines, including:

- NIST Cybersecurity Framework – Detect, Continuous Monitoring – DE.CM;
- NIST SP 800-53 – AU, Audit and Accountability, and CA-7, Continuous Monitoring;
- NIST SP 800-82 provides additional information on monitoring for control systems;
- NIST IR 7628 - Guidelines for Smart Grid Cybersecurity: SG.AU – Audit and Accountability, SG.CA-4 - Smart Grid Information System Connections, SG.CA-6 – Continuous Monitoring;
- ISO/IEC 27002 – 12.4 – Logging and Monitoring;
- The Critical Security Controls for Effective Cyber Defense (a.k.a 20 Critical Controls) – CSC14, Maintenance, Monitoring, and Analysis of Audit Logs;
- SP-800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations is dedicated to the concept of monitoring as a critical component of the overall risk management process; and,
- IEC 62351-7 - Power systems management and associated information exchange – Data and communications security – Part 7: Network and system management (NSM) data object models.

Differences and Intersections of Functionality, Security, and Compliance

Functionality can be defined as “the quality of being suited to serve a purpose well; practicality”, “the purpose that something is designed or expected to fulfill”, or more precisely in information systems, “the range of operations that can be run on a computer or other electronic system”.

For control systems that support power system operations, functionality can be seen as the combined capabilities of power system applications and equipment to achieve operational goals in a cyber secure manner, such as maintaining reliability, safety, and efficiency of the power system. For business networks the functionality can be seen as supporting the business of the organization providing ways of exchanging information, communicating within and outside of the organization, and housing a variety of information required to run an organization. Connections and data flows between business networks and control system networks may benefit both operational and business sides of this equation by facilitating exchange of information between the two networks such as operational reports and weather forecasts. However, connections and data flows between two networks or systems may also provide additional entry for intrusions and malware, which may be harmful both to the control systems (and ultimately power system operations) and to business operations of the organization.

Resilience, as a subset of functionality, means that the system can operate, potentially in a degraded manner, under duress and is able to recover in the event of a cyber-attack, system failure, or other potentially damaging situation. Resiliency results from a combination of architecture, design, engineering, and security strategies, processes, mechanisms, and operations combined to protect against deliberate attacks or inadvertent events, detect such attacks and events, cope with these situations while they are on-going, recover from the results of these attacks or events, and to take actions to improve resilience in the future.

For control systems, resiliency may be implemented by combining security controls and techniques with engineering data validation, equipment redundancy and failover, and configuration designs to isolate different types of network traffic. These controls and techniques cannot be successful without corresponding operational procedures carried out by appropriately trained personnel.

Security can be viewed as risk mitigation. Security can be implemented as a series of strategies, processes, controls, and mechanisms that reduce vulnerabilities in the system and therefore make it less susceptible to cyber-attacks.

Compliance means that the system and corresponding operation and business practices are as defined in applicable laws, regulations, or standards. Compliance in general is designed to improve safety and reliability. Due to the complexity of compliance requirements, control system architectures and processes can become increasingly complex. For instance, to maintain compliance, a company can have a procedure to disconnect communications in case of an attack to meet its incident response plan requirements. This procedure needs to be designed to ensure that the disconnecting action does not negatively impact the operation of the system.

It should be noted that the optimal functional solution (e.g., low cost/simple design) may not necessarily be the optimal security and compliance solution. Similarly, the optimal security solution may not be the optimal functional and compliance solution. These three properties intersect but do not necessarily align completely. Thus, the best solution would consider all three aspects and would exist in the intersection at the center of Figure 1.

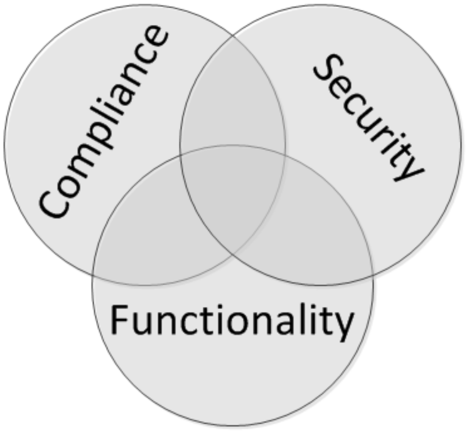


Figure 1

Functional Data Flow and Inventory

Operational control systems consist of interconnected devices that communicate with each other through the use of well recognized communication technology (e.g. Ethernet or RS/232) or through a proprietary communications interface. In order to properly design, support, and operate these complex systems it is important to ensure adequate system documentation exists. Most commonly, documentation depicts the communications path:

- In a logical manner that displays the various devices within groups and how they communicate with each other. The logical/communication diagram can provide a quick understanding of which devices are in common segments, domains, or locations; and,
- In a physical manner that displays each connection in and out of a device and where each connection terminates. The detailed physical drawing can be used for expansion planning, to troubleshoot connectivity issues, or to identify isolation points in a communication path for incident containment efforts.

Neither of these approaches provides sufficient detail around system purpose, function, and interdependence on other systems or processes for operation. The system purpose and function is typically the focus of the design, engineering, and specification. As a system transitions into the operational phases of the system lifecycle, the documentation transitions to traditional logical and physical diagrams. To maintain system-to-system operational understanding, it is important that asset owners develop and maintain **functional data flow diagrams**.

There are many ways to develop a functional data flow diagram to show the level of system interdependence. The specific approach will largely depend on the organization's current capability and maturity to accurately map the existing assets within an environment and the functions those assets perform in the larger system. For example, a team working on developing functional data flow diagrams may begin by examining system procurement specifications and '*as-built*' diagrams provided by the vendor. **Current asset inventory** is an important input into the process. Current asset inventory can be very challenging to obtain depending on the age and complexity of the system, and the number of modifications from the 'as-built' documentation. With an accurate asset list, an entity can begin the process of interviewing subject matter experts in a defined process of detailing the functions performed by each device during normal and emergency operating conditions. The assembled tabular listing of compiled data that details the system purpose, individual asset inventory, and the functions performed by the assets can be converted into a graphical functional data flow diagram (may include ports and services information). This diagram, in conjunction with the logical and physical diagrams, can be utilized for future system planning, maintenance, troubleshooting, and incident response.

There are many approaches[5] to developing a functional data flow diagram. Such a diagram could be created internally by an entity or in a joint effort with their control system vendor/integrator for each control system.

[5] An example data flow diagram is available in a presentation by Ralph Langner
https://files.sans.org/summit/icsamsterdam14/PDFs/Ralph%20Langner%20.pdf

The physical and logical diagrams, in conjunction with a functional data flow diagram, provide enough information to identify key processes and key communication paths. With this information you can take a systematic approach to the design, operation, and security of your interconnections: internally and externally to the control system.

Functional Data Flows and Inventory are included in many key security guidelines, including:

- NIST Cybersecurity Framework – Identify. Asset management – ID.AM;
- NIST SP 800-53 – AC-4, Information Flow Enforcement, CM-8, Information System Component Inventory, PM-5, Information System Inventory;
- NIST SP 800-82 provides additional information on data flows and inventory for control systems;
- NIST IR 7628 - Guidelines for Smart Grid Cybersecurity: SG.AC-5 - Information Flow Enforcement, SG.CM-3 - Configuration Change Control, SG.CM-7 - Configuration for Least Functionality, SG.SA-5 - Smart Grid Information System Documentation, SG.SC-2 - Communications Partitioning, SG.SC-7 - Boundary Protection;
- ISO/IEC 27002 – 8 – Asset Management; and,
- The Critical Security Controls for Effective Cyber Defense (a.k.a 20 Critical Controls) – CSC1, Inventory of Authorized and Unauthorized Devices, CSC2, Inventory of Authorized and Unauthorized Software.

Defense in Depth

There is no such thing as perfect security. However, there are effective countermeasures that can be deployed, such as multiple defense mechanisms between the attacker and the protected assets. For example, deploying firewalls at both outer and inner network boundaries is an example of a layered defense.

Defense in Depth is an information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.[6] Its intent is to provide multiple complementary controls in the event a security control fails or a vulnerability is exploited that can cover aspects of personnel, procedural, technical and physical for the duration of the system's life cycle. It is a “best practices” strategy that relies on the effective application of techniques and technologies that exist today. The strategy recommends a balance between the protection capability and cost, performance, and operational considerations.[7]

Defense in Depth is a way to layer diverse security controls, methods, processes, and technologies in a way that impedes incursion into the protected system. It can provide a variety of alert generation points, thus potentially increasing the likelihood that a breach is detected. It also forces the attacker to evade multiple systems, thus hindering the attack and providing more time for the security personnel to react to

[6] Committee on National Security Systems Instruction No. 4009

[7] https://www.nsa.gov/ia/_files/support/defenseindepth.pdf.

the event. For example, technologies that control access, like 802.1x based Network Access Control systems, may be appropriate for some environments. The principles and concepts presented in this document implement Defense in Depth approach to architectures for connecting control systems to external systems.

With regard to electronic connectivity of control systems, Defense in Depth principles may be implemented in any design where the control system is connected to external systems. The connectivity design(s) should implement technology and operational processes that are appropriate to the risk profile and function of the control system and provide the appropriate level of security to achieve the business objectives of the entity.

Configuration Management

Configuration management establishes baselines, tracks controls, and manages changes. It is the integral process that facilitates and maintains secure configurations. Security-focused configuration management (SecCM) is defined as the management and control of configurations for information systems to enable security and facilitate the management of information security risk. System configurations should be managed through the implementation of security controls and approved hardware and software products. Baseline configurations serve as the basis for future builds, releases, and changes. Configurations should be monitored via SecCM to ensure that they do not deviate from the approved baseline due to changes, for both security controls and device settings.

A formal change management process is utilized to identify, propose, review, analyze and evaluate, test, and approve changes prior to implementation. Automated file integrity and change management solutions provide real-time continuous monitoring, visibility, and auditing of hardware and software configuration to ensure compliance with an established governance, risk and compliance framework. In addition, these solutions alert staff of unauthorized changes and attempts, support situation awareness, document deviations from baseline configurations, and confirm whether security controls are functioning as intended.

Restricted access mode should be maintained to prevent unauthorized access to configurations and security settings for the control systems and associated systems. This can pose a significant challenge to organizations due to the security needs of the control systems. While the corporate configuration management tools are scalable and may support the functionality of configuration management of control systems, those tools are typically located on the corporate network and are not afforded the level of protections required to mitigate security risks to the control system. Similarly, the configuration management tools should not be placed internally to the control system, unless there is no external access to the tools. The ideal placement for these tools would be in a protected DMZ. As they would be supporting an interactive user session with the control system (during configuration implementation) the configuration management tools should be treated as intermediary systems, and be protected as such – see Appendix C, Diagram 4. Optionally, such a configuration management tool can manage non-control system configurations, provided that the appropriate level of security is still applied to the overall toolset. The configuration management tool should be accessed with read-only permissions whenever write-access is not required.

Configuration management is included in many key security guidelines, including:

- NIST Cybersecurity Framework – Protect. Information Protection Processes and Procedures – PR.IP;
- NIST SP 800-53 – Configuration Management – CM;
- NIST SP 800-82 provides additional information;
- NIST IR 7628 - Guidelines for Smart Grid Cybersecurity: SG.CM Configuration Management
- ISO/IEC 27002 – 12.1.1, Change Management;
- The Critical Security Controls for Effective Cyber Defense (a.k.a 20 Critical Controls) – CSC3, Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers;
- SP-800-128 Guide for Security-Focused Configuration Management of Information Systems; and,
- IEC 62351-7 - Power systems management and associated information exchange – Data and communications security – Part 7: Network and system management (NSM) data object models.

Network Design Considerations

The following are network design considerations that should be taken into account when designing a security architecture for control systems.

Virtualization

Virtualization of workstations, servers and storage continues to grow within the control system environment. The efficiencies realized in IT operations with the use of virtualization also create potential mixed trust environments that can impact the security posture of control systems such as:

- Placement of control system Virtual Machine (VM) clients on the same VM Host alongside general business system VM Clients; and,
- Placement of control system data on virtual storage environments which also contain data for general business functions.

The following concepts should be considered when implementing virtualization in control system environments:

- Physical separation of VM Host hypervisors running control system applications (i.e., ESX, Hyper-V) so those VM Clients are the only VM Clients running on the VM Host;
- In cases of mission critical applications, virtual mixed trust environments may not be appropriate, and physical separation, where possible, is recommended;
- There should be physical separation of virtual storage / SAN for the control system applications; and,

- The VM Host hypervisor should be considered to have a level of criticality consistent with the most critical system that is hosted on it, as a compromise of the VM Host hypervisor may potentially lead to a compromise of all hosted systems.

The treatment of Virtual Private Networks (VPNs) is described in detail in Appendix C, Diagram 5.

Remote Access

Remote access, as used in this guideline, refers to the ability to access control systems via a communication network from another (potentially less trusted) network. Remote access is generally thought of as an individual accessing a system they are not in front of, but machine-to-machine interprocess communications[8] must also be addressed in an entity's security policies. The increase in risk presented by remote access must be carefully considered, since remote access reduces the security of a system by increasing the opportunities for compromise of the trusted network. No matter the method, remote access must be securely controlled to maintain the integrity of the control systems.

Design considerations[9] for human-initiated remote access are:

- Direct access to the control systems from outside of a defined protected network is not recommended;
- An intermediate system that is placed in a DMZ with strictly controlled access from the outside may be used as a proxy when connecting to control systems remotely;
- Communication protocols allowed between the remote and intermediate systems should be restricted to permit only the required processes and applications;
- The type and version of all communication protocols in use should be documented. Discovery of new vulnerabilities within these protocols should be monitored via external sources (e.g. E-ISAC, vendors, industry forums, ICS-CERT);
- Use of communication encryption[10] from the external remote system to the intermediate system should be commensurate to the risk profile of the control system;
- Authentication to the intermediate system should always be required, and may involve multi-factor capabilities to assure the remote user is approved for the intended access where appropriate; and,
- Communication from the intermediate system to the control system should only allow protocols necessary for proper interaction between the two systems. As an example: If not required for the operation of the control system, file sharing (e.g. drive mapping) between the intermediate system and the control system should be disallowed.
- Role based access control is recommended for all communications.

[8] Machine-to-machine interprocess communications are those processes that traverse networks without human interaction.

[9] Design Considerations for remote access should follow strong acceptable-use policies as defined by the entity.

[10] Encryption may or may not be appropriate depending on the application in question. Other methods may be used to achieve data integrity.

Design considerations for machine-to-machine interprocess communications are:

- Inbound communications should be limited as much as possible;
- Direct remote system to control system communications from outside of the secured network should not be allowed; [11]
- Use an intermediate system between the external system(s) and control systems;
- Any intermediate system should not reside on the same protected network as control systems;
- Data received by the control system should have input validation filters to verify it is within acceptable bounds before being used;
- All interaction between control systems and remote systems should require authentication and authorization between the sender and receiver systems;
- Communications traversing different security zones should be limited to needed IP addresses and protocols, and secured as appropriate; and,

Remote access controls for control system communications are addressed in multiple guidelines including NISTIR 7628, SG.AC-15 Remote Access and NIST SP800-82.

Data Diodes

Many data communications protocols require bi-directional communications in order to establish communications and acknowledge receipt of data packets. The bi-directional nature of this communication presents risks of undesired access to the protected network. Unlike firewalls which allow bi-directional traffic to traverse between a trusted and an untrusted network, data diodes only allow for a uni-directional communication from the protected network to the untrusted network. This security mechanism is very effective as there is inherently no traffic that can traverse the data diode from a less trusted interface to a more trusted network. Though this solution may not be appropriate for systems that require bi-directional communications with other, less secure, systems, it can be effective in reducing the risk of exploitation of an outbound connection. This approach has similar benefits and vulnerabilities as presented in the Complete Isolation section.

Complete Isolation

Complete isolation of the control systems can be an effective security method and involves the placement of the control systems into their own logical or physical network(s) that have no wired or wireless connectivity to untrusted networks. Logical separation[12] is not as secure as physical separation, since the hardware/software providing the logical segregation can be accidently or knowingly modified or misconfigured to allow untrusted or unintended communications. In addition, the device providing logical separation may have unknown vulnerabilities that can be exploited to defeat the segregation. Physical separation may require more effort and different tactics to defeat, but it cannot be considered completely secure (for example, Stuxnet, or a USB introduced compromise).

[11] This would normally be non-real time communications such as historian data exchange.

[12] Use of firewalls or similar type of device employing Access Control Lists (ACL), or Virtual Local Area Network (VLAN).

In many of today's operating environments complete isolation is generally not practical. There are instances where a given control system is required to communicate with external systems for business or operational reasons, such as:

- Remote access to control systems due to staffing considerations; and,
- Data exchange between OT to OT and OT to IT systems.

Isolation also does not guarantee security due to maintenance needs of the systems and applications. Maintenance at some point in the control system's life-cycle will require the introduction of removable media which could contain malware that may not be discovered using traditional malware scanning features.[13]

Four-Legged Firewall

The concept of the four-legged firewall is to create segmentation into different security zones, referred to as legs. The four legs of the firewall are:

- **The Trusted zone** of the firewall which is understood to be the protected network where the control system(s) resides. The communications to and from the Trusted zone needs to be tightly controlled to limit the exposure of the control system to external threats.
- **The Untrusted zone** of the firewall is understood to be the least secure portion of the network from the point of view of the control system. (e.g. corporate networks, Internet, or any other untrusted network).
- **The Inbound DMZ** of the firewall is recommended to create an additional layer of defense for the control system. By creating this additional layer the entity is able to apply multiple access control rules and authentication filters on the traffic entering the control system environment. Within this DMZ one or more servers can be used as intermediate systems[14], or jump servers, where a user requiring interactive remote access can first pass through the firewall access control lists and be authenticated against the intermediate system (jump server) prior to initiating communications with the trusted control system. Thus, direct access from an untrusted computer on the internet or corporate network to the control system is denied. Indirect access through the jump server can be managed in a secure manner. The Inbound DMZ typically has a higher security posture than the Outbound DMZ due to the fact that communications can be initiated into the control system directly from Inbound DMZ networks.
- **The Outbound DMZ** follows a similar concept as the Inbound DMZ, only in the opposite direction. The Outbound DMZ is recommended to create a buffer between communications that leave the

[13] BadUSB is one example of the possible introduction of malware which could escape traditional scanning methods. With the capability to hide malware in a common maintenance tool (Announced in July 2014), the USB flash drive could evade the most diligent organization with strict internal controls on media use. Such an organization then could still become compromised by a BadUSB device, due to future vulnerabilities.

[14] Intermediate systems are systems that terminate a session either Inbound or Outbound of the Trusted zone before data transfer or user access is allowed. Examples are Web proxy, Terminal Server for user interactive remote access, Service Orientated Architecture/Data Broker, Remote Front Ends, etc…

control system for consumption in the Untrusted zone. The goal is to limit the exposure to the control system that direct communications between control systems and untrusted endpoints may provide. Thus, monitoring and historical data that is sent from the control system can be routed through a monitoring server that is located on the Outbound DMZ. Authenticated and authorized external users can then access and retrieve the desired data from the monitoring server without connecting to the control system itself. Inbound communications from the Outbound DMZ to the control system should be denied.

Figure 2 provides a concentric security representation of the four security zones.

Depending on the network architecture, this four legged schema can be replicated as needed to meet the security needs of the control system(s). There may be instances where the trust relationships between control systems may be equal, or opposite. (i.e. Trust levels may be reversed depending on the view of the respective control systems).

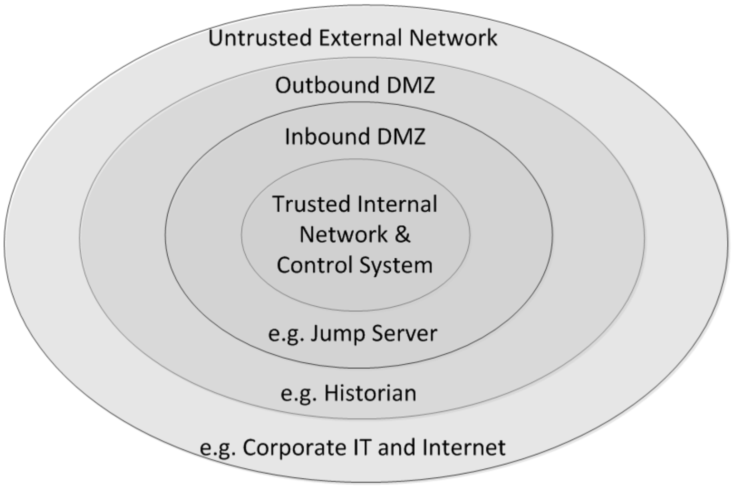

Untrusted External Network
Outbound DMZ
Inbound DMZ
Trusted Internal Network & Control System
e.g. Jump Server
e.g. Historian
e.g. Corporate IT and Internet

Figure 2

Connecting OT – OT and OT – IT systems

The above concepts can be applied to segregate protected environments from less trusted zones as well as separating multiple trusted networks. As an example: When a TOP's control system talks to a local TO's control system over ICCP links, the two control systems are both considered trusted by their local entities. However, the remote control system from the view point of either entity would be seen as untrusted, requiring each system to implement appropriate security measures. See Appendix C, Diagram 6.

If both OT networks are mutually trusted, a VPN can be used to communicate between the networks. This effectively extends the perimeter of a trusted network to another location. The VPN endpoints must not allow untrusted connections into either trusted network.

Another approach to extending the perimeter of a trusted network is through the use of a private network, such as a frame relay or MPLS network using a telecommunications carrier. Although more secure than using the public Internet, consideration must be given to the possible risk of intrusion into the private network.

When connecting multiple OT and IT systems, it is important to take note of the potential entry points into each trusted control system environment and apply desired security controls at those entry points. Additionally, those entry points may become the potential disconnect points where the control system(s) may need to be isolated in case of emergency. See Appendix C, Diagram 4 for examples of potential disconnect points identified by a red triangle.

The communication between two segregated control systems may be encrypted to increase the security of the data in transit.

Disconnecting and Reconnecting

The concept of system isolation, or disconnection has become more relevant in today's interconnected world. There have been many documented cases where a company's corporate network may be compromised, but the control system remained functional. The purpose of this section is to build on the segmentation discussion and ensure that proper procedures are in place[15] to disconnect control systems when the appropriate risk threshold is reached.

As the network and security mechanisms are designed to support the control system communication needs, the topology should identify the critical points where data flows can be disconnected to preserve the integrity of the control system. The identification of these critical points is dependent on fully understanding the communication needs of the system: links to IT/Corporate Systems, connections to other control centers, communication to remote terminal units, or the link to backup control system(s). Once the communication requirements are properly identified and inventoried, the system can be architected to include disconnect switches, and processes developed to identify when, where, and how to disconnect the control system from the outside world. Additionally, the processes for reconnecting the control system need to be documented to account for the checks necessary to validate trust in the restored connections to the outside world prior to reconnecting.

When to disconnect? [16]

While it is difficult to account for all risks and possibilities during an incident, a set of thresholds should be identified to guide the entity in its efforts to isolate, and preserve the functionality of the control system. These thresholds should be specific to each data flow.

With regard to IT interconnectivity, the disconnect threshold may be reached by an entity when[17]:

[15] When mentioning process creation throughout the document, the intent is not to create and file the document, but to also practice the processes during exercises, review on a regular basis, and update as necessary.

[16] 'When to Disconnect' discussion is not an all-inclusive list, and may not be applicable to all entities. Each entity should decide what thresholds are met before segregating their control systems.

[17] This list is provided for illustrative purposes only and is not all-inclusive.

- An active malware incident has been identified and is propagating on the corporate network;
- Abnormal communication from the IT link is continuously triggering alarms on the firewall;
- The IT/OT link is intermittently failing, and the failure is a high frequency occurrence; and/or,
- The identification of an event where unexpectedly large amounts of data leaves or enters the network.
- A Denial of Service attack appears to be interfering with operations

Where to disconnect?

As discussed in a previous section, it is critical to use segmentation principles when architecting the control system communication networks. Akin to the many layers of the onion, the control system communication network should have many layers, so that when one layer is compromised, the other layers of the communication system continue to support the operation of the control system. Thus, the concentric security diagram for such communication systems would consist of multiple levels:

- **Trusted Internal Network:** Communication between control system nodes and key local services.
- **Inbound DMZ:** Communication to/from other OT systems (Such as ICCP communications and interactive remote access for management purposes)
- **Outbound DMZ:** Communication link to provide information to external users or systems (via proxies)
- **Untrusted External Network:** Corporate Network, Internet, or Public network

In Figure 2, which depicts a security layers view of the network, the disconnection of each layer would only eliminate the communication capabilities related to the systems/users that have access to that layer and retain communication capabilities for higher security zones.

How to disconnect and reconnect?

There are two main considerations on how to disconnect a given connection:

- An **automatic disconnect** scheme would break the connection once a specific, predefined threshold is reached, similar to an Intrusion Prevention System that automatically blocks traffic upon detection of abnormal activity. While this would ensure a quick disconnect for the specific cases identified, the complexity of such a system may be extensive. Additionally, the risk of false positives should be weighed against the possibility of undesired disconnects. Also, a notification mechanism would need to be designed to alert the appropriate parties upon an automatic disconnect. Otherwise, a disconnect triggered by a false-positive could result in adverse operational consequences that could be difficult to troubleshoot; and,
- A **manual approach** may reach the disconnect decision slower, however, expert evaluation of the situation would mitigate some of the risks that go along with an automatic shut-off. Since the disconnection of a control system may make the system less functional, it may be beneficial to not

only rely on the preset thresholds of the system, but also on the situational awareness of the operational staff.

In some instances a hybrid model may be appropriate, where predefined situations would allow for an automatic shutdown of specific, non-critical links that would preserve key communications in place. Once a higher threshold during a cyber security incident is reached, manual analysis may be required for the shut-down of more critical communications paths.

Regardless of how the disconnect is achieved, the restoration of the external electronic connectivity for a given control system should always follow a manual process. The restoration procedure may include a root cause analysis for the initial disconnect, validation of normal communication patterns within the external and internal networks, vulnerability assessments and/or security scans.

Since the disconnection and reconnection of a control system may be disruptive to the functionality of the control system, the processes that define how to disconnect and reconnect the control system should be entity specific, detailed, approved by management, and exercised during mock events.

7. Recognition of Contributors

In Appreciation

This working group was comprised of individuals representing asset owners and operators, academia, national labs, and industry consultants. Each member brought their unique perspectives, talents and abilities to the effort and participated in an exemplary collaborative manner. Their donation of time and their company's donation of support to the assignment are greatly appreciated.

Task Force Members

Chairman	Mikhail Falkovich	PSEG
Vice Chairman	Paul Skare	Pacific Northwest National Laboratory
	Nadya Bartol	UTC
	Laura Brown	NERC
	Larry Bugh	ReliabilityFirst Corporation
	Marc Child	Great River Energy
	Dustin Cornelius	Southern Company
	Tim Conway	SANS
	Frances Cleveland	Xanthus Consulting International
	Cynthia Hill-Watson	TVA
	Michael Johnson	Burns & McDonnell
	Carter Manucy	FMPA

Appendix A: Bibliography

Council on Cybersecurity, The Critical Security Controls for Effective Cyber Defense, Version 5, https://www.sans.org/media/critical-security-controls/CSC-5.pdf

Draft IEC 62443-3-2, *Security for Industrial Automation and Control Systems, Security Risk Assessment and System Design*

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27002:2013, Information technology — Security techniques — Code of practice for information security controls

National Institute of Standards and Technology (NIST) Cybersecurity Framework, Version 1.0, February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82, *Guide to Industrial Control System (ICS) Security*, Revision 2, May 2015, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-128, *Guide for Security-Focused Configuration Management of Information Systems,* August 2011, http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011, http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

National Security Agency, *Defense in Depth, A practical strategy for achieving Information Assurance in today's highly networked environments*, https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

National Institute of Standards and Technology (NIST) Interagency Report (IR) 7628 Revision 1, Guidelines for Smart Grid Cybersecurity, Volume 1, September 2014, http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

IEC TS 62351-7 – Power systems management and associated information exchange – Data and communications security – Part 7: Network and system management

IEC TS 62351-8 – Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control

IEEE 1686-2013 - IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities

Appendix B: Terms[18]

Acronym

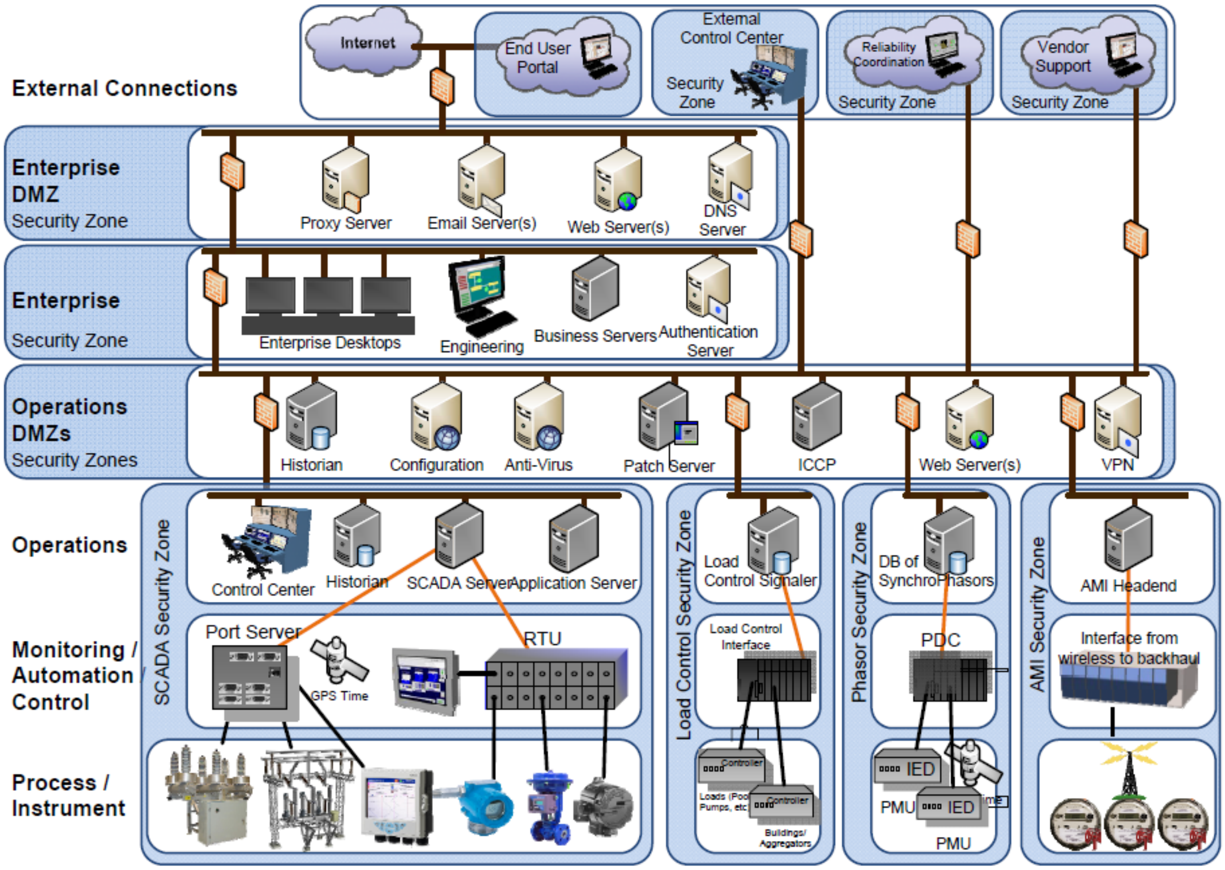
AAA	Authentication Authorization and Accounting
ACL	Access Control List
APT	Advanced Persistent Threat
BES	Bulk Electric System
DMZ	Demilitarized Zone
EMS	Energy Management System
ESX	Elastic Sky X (VMware Hypervisor for deploying and serving Virtual computers)
E-ISAC	Electric Information Sharing and Analysis Center
HMI	Human Machine Interface
ICCP	Inter-Control Center Communication Protocol
ICS-CERT	Industrial Control System Cyber Emergency Response Team
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
NIST	National Institute of Standards and Technology
OT	Operational Technology
PLC	Programmable Logic Controller
SAN	Storage Area Network
SNMP	Simple Network Management Protocol
TO	Transmission Owner
TOP	Transmission Operator
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network

[18] This guideline intentionally does not reference the 'Glossary of Terms Used in NERC Reliability Standards' as the goal is to provide guidance for any implementation of control system electronic connectivity.

Appendix C: Best Practices and Examples

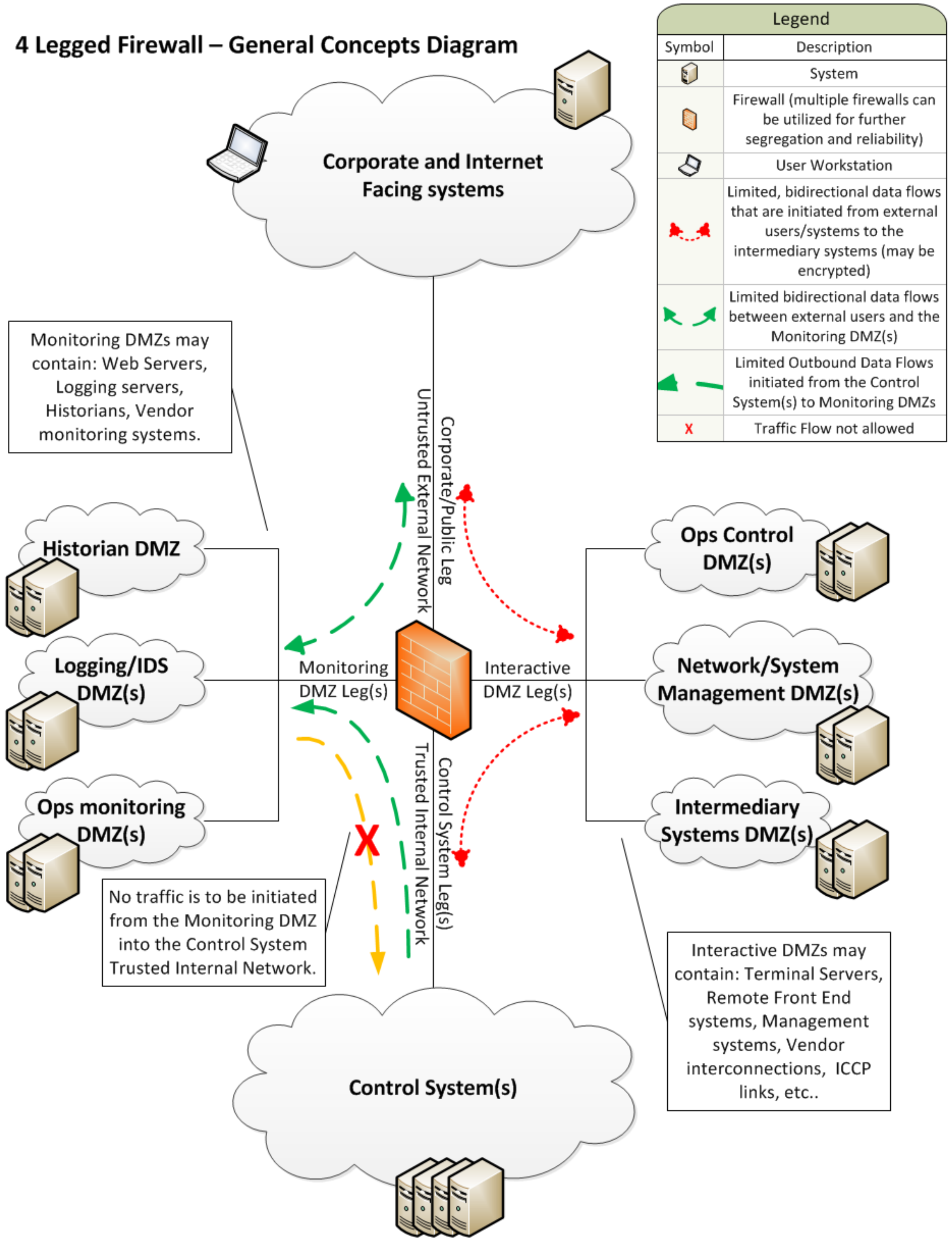
Diagram 1

Notional Utility Architecture for Business Networks and Control Systems



The above diagram provides a high level view of potential security zones for control system electronic connectivity to other business and control networks.

Diagram 2



4 Legged Firewall – General Concepts Diagram

Legend	
Symbol	Description
🖥	System
🧱	Firewall (multiple firewalls can be utilized for further segregation and reliability)
💻	User Workstation
↔	Limited, bidirectional data flows that are initiated from external users/systems to the intermediary systems (may be encrypted)
↔	Limited bidirectional data flows between external users and the Monitoring DMZ(s)
←	Limited Outbound Data Flows initiated from the Control System(s) to Monitoring DMZs
X	Traffic Flow not allowed

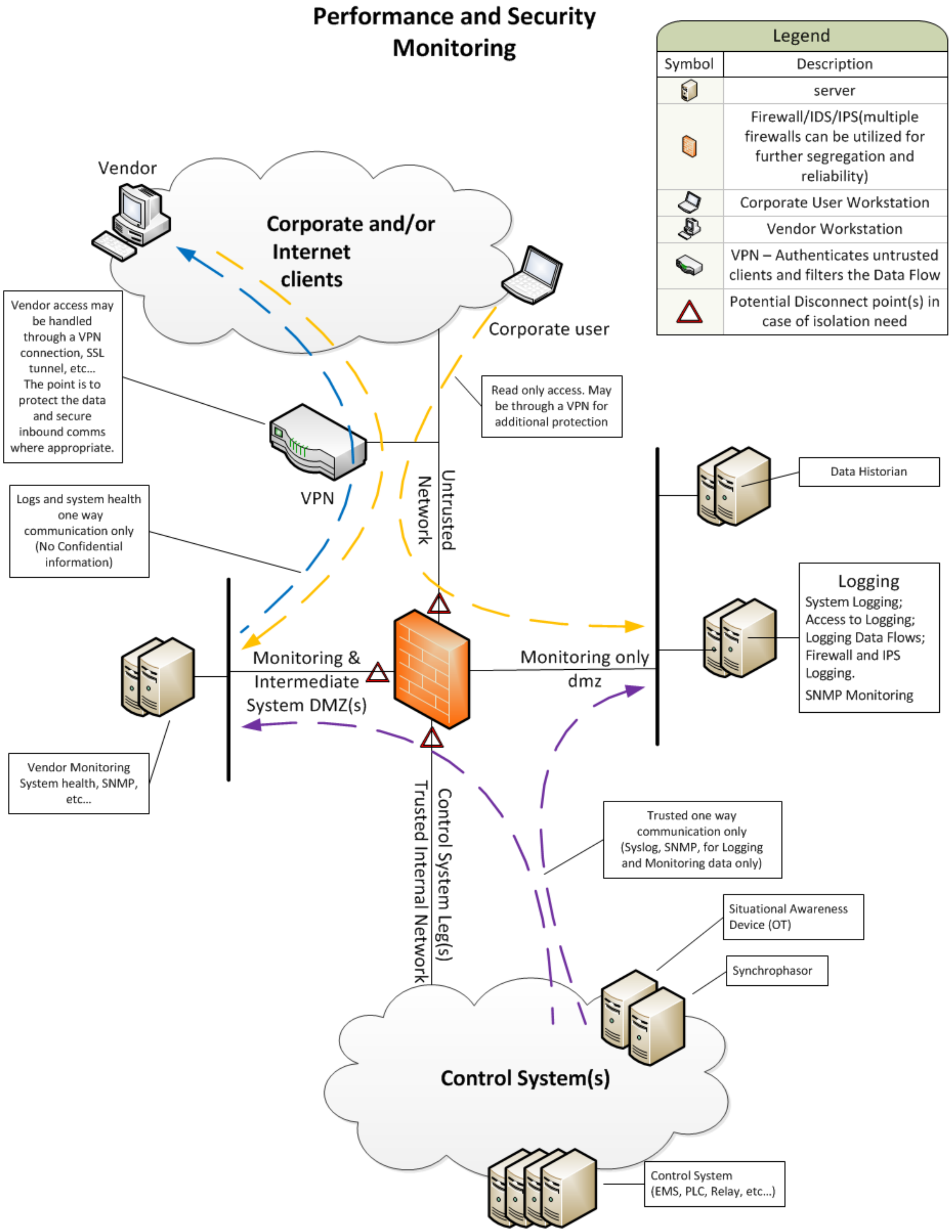
Monitoring DMZs may contain: Web Servers, Logging servers, Historians, Vendor monitoring systems.

No traffic is to be initiated from the Monitoring DMZ into the Control System Trusted Internal Network.

Interactive DMZs may contain: Terminal Servers, Remote Front End systems, Management systems, Vendor interconnections, ICCP links, etc..

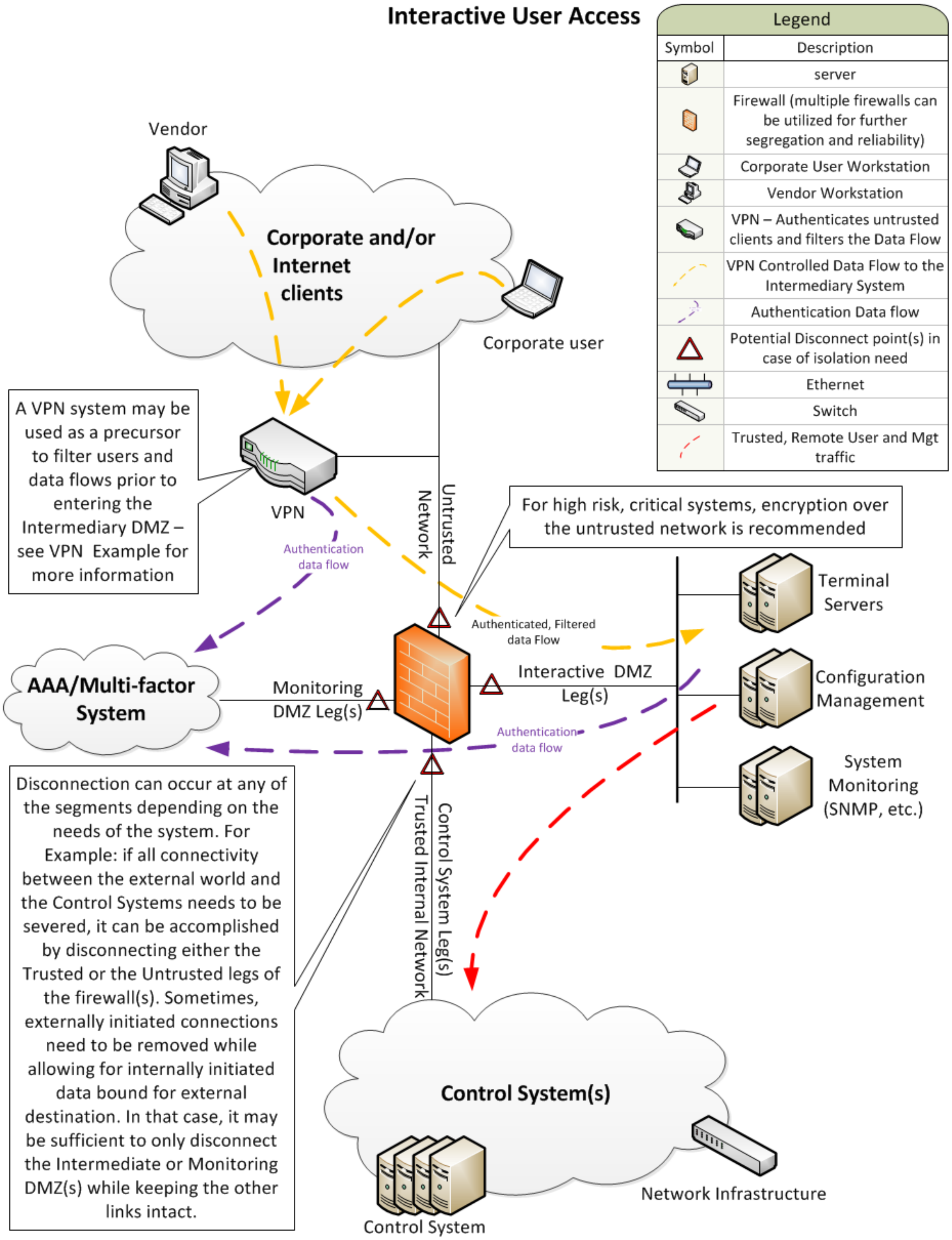
The above diagram provides an example of a segmented network infrastructure that supports control system electronic connectivity. Note: Each cloud may be its own DMZ, or network, with a dedicated interconnection through the firewall.

Diagram 3


Performance and Security Monitoring
Legend
Symbol
Description
server
Firewall/IDS/IPS(multiple firewalls can be utilized for further segregation and reliability)
Corporate User Workstation
Vendor Workstation
VPN – Authenticates untrusted clients and filters the Data Flow
Potential Disconnect point(s) in case of isolation need
Vendor
Corporate and/or Internet clients
Corporate user
Vendor access may be handled through a VPN connection, SSL tunnel, etc… The point is to protect the data and secure inbound comms where appropriate.
Read only access. May be through a VPN for additional protection
VPN
Untrusted Network
Logs and system health one way communication only (No Confidential information)
Data Historian
Logging
System Logging;
Access to Logging;
Logging Data Flows;
Firewall and IPS Logging.
SNMP Monitoring
Monitoring & Intermediate System DMZ(s)
Monitoring only dmz
Vendor Monitoring System health, SNMP, etc…
Trusted one way communication only (Syslog, SNMP, for Logging and Monitoring data only)
Control System Leg(s)
Trusted Internal Network
Situational Awareness Device (OT)
Synchrophasor
Control System(s)
Control System (EMS, PLC, Relay, etc…)

The above diagram provides an example of a network and application monitoring infrastructure that supports control system electronic connectivity.

Diagram 4



Interactive User Access

Symbol	Description
	server
	Firewall (multiple firewalls can be utilized for further segregation and reliability)
	Corporate User Workstation
	Vendor Workstation
	VPN – Authenticates untrusted clients and filters the Data Flow
- - -	VPN Controlled Data Flow to the Intermediary System
- - -	Authentication Data flow
△	Potential Disconnect point(s) in case of isolation need
	Ethernet
	Switch
- - -	Trusted, Remote User and Mgt traffic

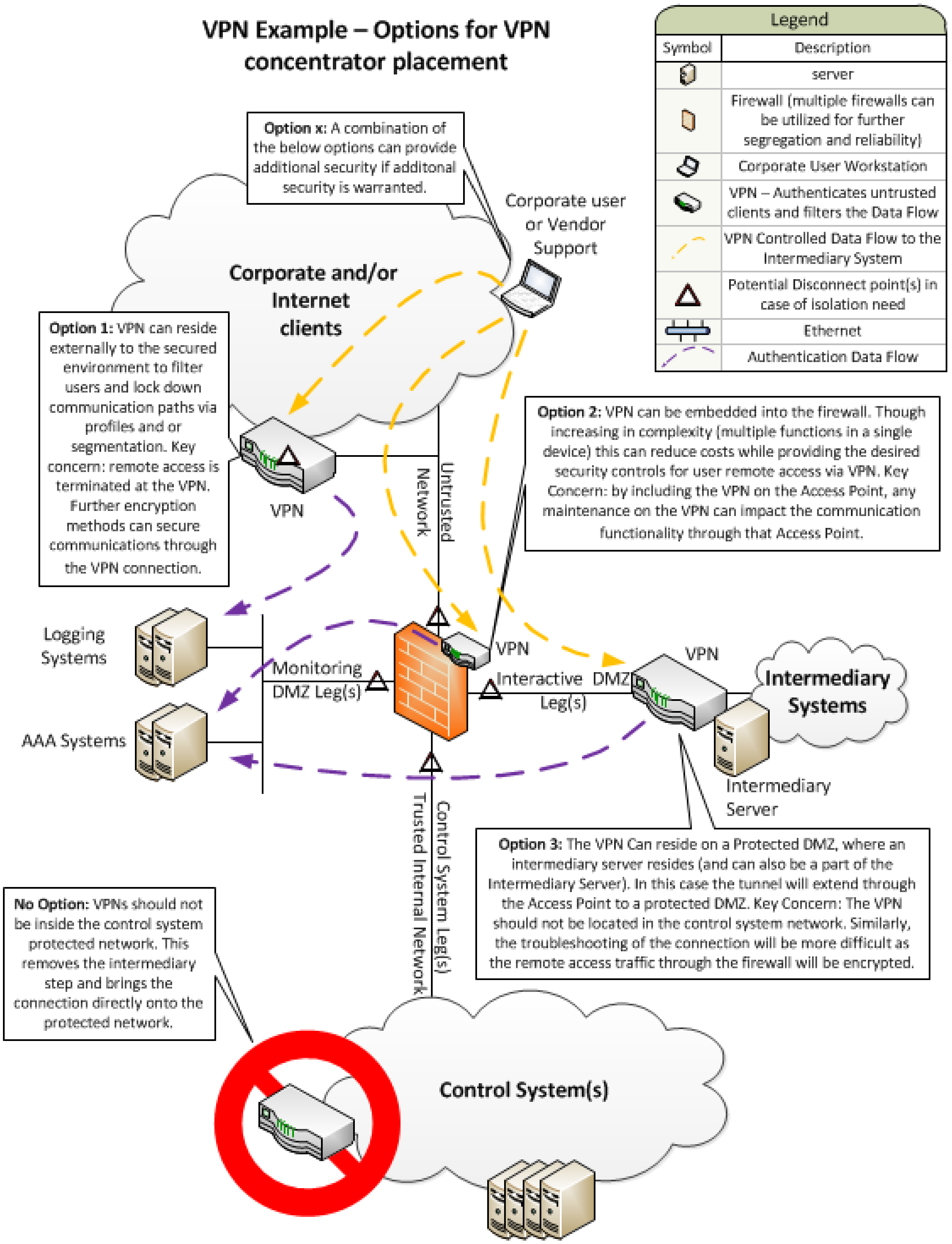
A VPN system may be used as a precursor to filter users and data flows prior to entering the Intermediary DMZ – see VPN Example for more information

For high risk, critical systems, encryption over the untrusted network is recommended

Disconnection can occur at any of the segments depending on the needs of the system. For Example: if all connectivity between the external world and the Control Systems needs to be severed, it can be accomplished by disconnecting either the Trusted or the Untrusted legs of the firewall(s). Sometimes, externally initiated connections need to be removed while allowing for internally initiated data bound for external destination. In that case, it may be sufficient to only disconnect the Intermediate or Monitoring DMZ(s) while keeping the other links intact.

The above diagram provides an example of an interactive user access (via an intermediate system) infrastructure that supports control system electronic connectivity.

Diagram 5



VPN Example – Options for VPN concentrator placement

Symbol	Description
	server
	Firewall (multiple firewalls can be utilized for further segregation and reliability)
	Corporate User Workstation
	VPN – Authenticates untrusted clients and filters the Data Flow
	VPN Controlled Data Flow to the Intermediary System
△	Potential Disconnect point(s) in case of isolation need
	Ethernet
	Authentication Data Flow

Option x: A combination of the below options can provide additional security if additonal security is warranted.

Option 1: VPN can reside externally to the secured environment to filter users and lock down communication paths via profiles and or segmentation. Key concern: remote access is terminated at the VPN. Further encryption methods can secure communications through the VPN connection.

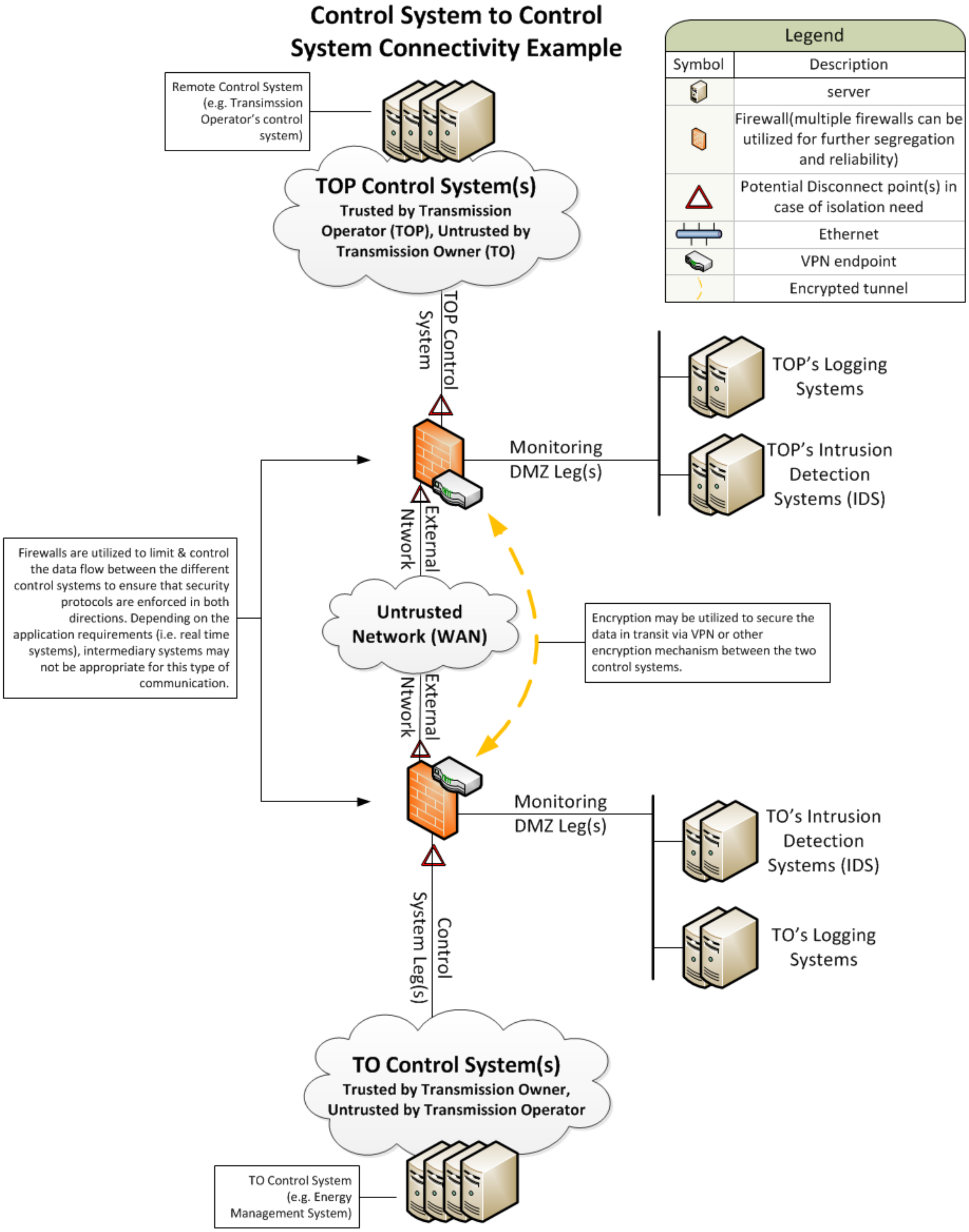
Option 2: VPN can be embedded into the firewall. Though increasing in complexity (multiple functions in a single device) this can reduce costs while providing the desired security controls for user remote access via VPN. Key Concern: by including the VPN on the Access Point, any maintenance on the VPN can impact the communication functionality through that Access Point.

Option 3: The VPN Can reside on a Protected DMZ, where an intermediary server resides (and can also be a part of the Intermediary Server). In this case the tunnel will extend through the Access Point to a protected DMZ. Key Concern: The VPN should not be located in the control system network. Similarly, the troubleshooting of the connection will be more difficult as the remote access traffic through the firewall will be encrypted.

No Option: VPNs should not be inside the control system protected network. This removes the intermediary step and brings the connection directly onto the protected network.

The above diagram provides examples of VPN concentrator placements that support control system electronic connectivity.

Diagram 6



Control System to Control System Connectivity Example

Symbol	Description
▯	server
▮	Firewall(multiple firewalls can be utilized for further segregation and reliability)
△	Potential Disconnect point(s) in case of isolation need
┼┼	Ethernet
◇	VPN endpoint
)	Encrypted tunnel

Remote Control System (e.g. Transimssion Operator's control system)

Firewalls are utilized to limit & control the data flow between the different control systems to ensure that security protocols are enforced in both directions. Depending on the application requirements (i.e. real time systems), intermediary systems may not be appropriate for this type of communication.

Encryption may be utilized to secure the data in transit via VPN or other encryption mechanism between the two control systems.

TO Control System (e.g. Energy Management System)

The above diagram provides an example of a network topology that would support control system to control system connectivity.