A Strategic Approach to SCADA Cyber Security – Water and Wastewater Network Architecture and Segmentation

Norman Anderson, PE\(^1\)*, Bill Phillips, PE\(^1\)

\(^1\)CH2M HILL, 3011 SW Williston Road, Gainesville, FL, 32608
(*norman.anderson@ch2m.com)

KEYWORDS
Cyber Security, Supervisory Control and Data Acquisition (SCADA), Process Control Systems (PCS), Network Architecture, Network Segmentation

ABSTRACT
Network security for Water sector Process Control Systems (PCS) such as Supervisory Control and Data Acquisition (SCADA) systems continues to be increasingly important and ever evolving due to the need for secure and reliable control systems. Additionally, PCS systems continue to grow and the management of network connected devices and expansion of PCS networks can be difficult and cumbersome. To properly secure PCS networks, a multi-stage process is needed incorporating risk assessment, planning, design, implementation, and maintenance for a comprehensive defense-in-depth strategy. A critical aspect of defense-in-depth is the overall network system architecture and the network segmentation plan. A properly planned and executed network architecture and segmentation strategy lays the foundation for security and simplifies expansion and maintenance of the network.

This paper will discuss industry accepted methods for Industrial Control System network architecture and segmentation strategies as related to Water sector PCS and SCADA systems. Industry standard techniques, based on recently published standards and network design guides, will be discussed showing a layered network architecture approach to security and the use of logical subnets and VLANs for segmentation. The advantage of this approach is that it allows for simpler configuration of network security appliances and for simpler management and expansion of the network leading to increased network availability and a reduction in threat risk. A case study will be used to provide examples of actual methods implemented for a water sector utility.

Introduction
As cyber attacks and the threat of compromised network security continue to rise, so does the need for securing of Industrial Control Systems (ICS). ICS include many different types of systems with Water sector PCS being one of higher profile targets due to it being critical infrastructure affecting large populations [1-3]. Past statistics from the Cyber Emergency Response Team (CERT) show recorded cataloged vulnerabilities and reported incidents continuing to rise through the years [4] and a set of...
“honeypot”² ICS set up by Trend Micro to look like vulnerable Power and Water plants were attacked by hackers 25 times within a 28 day period [5]. Security is important for the Water sector since attacks can damage critical infrastructure that affects public safety, can lead to significant operational downtime, cause financial impacts such as the loss of revenue for the utility and its customers, and attract significant media attention causing a loss of confidence and fear from the public. There are many resources available providing guidance on where to start and how to secure networks [1, 6-10]. In general, there are four key steps in the process of planning and designing to secure networks for defense-in-depth [11] as shown in Figure 1:

![Figure 1: Planning and Designing for Defense-In-Depth](image)

In this paper the design of network architecture and network segmentation for securing Water Sector PCS will be discussed and examples presented. It is proposed to use a layered network architecture separating components within a Water Sector PCS by levels using Access Control Lists (ACLs) for communications between levels and keeping the most critical parts of the network in the deepest and most secured level of the network. In order to effectively organize this architecture, it is further necessary to logically segment the by following industry standard subnet organization and by further dividing network connected equipment into Virtual Local Area Networks (VLANs) to allow robust communication between critical components that need to communicate and segregating components that do not require communications with each other but communicate over the same media. Subnet

¹ A honeypot is trap designed to look like a real functioning computer network, but is actually isolated and monitored, and used in this case to look like a SCADA system to detect and research attacks on Water Sector ICS.
organization refers to organizing similar components within a network by IP addresses and more precisely IP address blocks, or subnets, as discussed in subsequent sections. By designing a layered network architecture that uses logical network segmentation and organization, the network implementation and maintenance can be simplified further enhancing overall network security.

Differences Between Corporate IT and Water Sector PCS

In modern Water Sector PCS the use of commercial-off-the-shelf (COTS) network components has risen as these systems continue to adopt more Ethernet connected control system components and budgets for upgrades continue to decrease. The use of COTS solutions provides benefits to utilities such as ease in getting replacement components, reduced cost, and simpler system integration, but has also been part of the rise in Water Sector PCS security concerns.

<table>
<thead>
<tr>
<th>Water Sector PCS</th>
<th>Corporate IT Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Time</td>
<td>Non-Real Time</td>
</tr>
<tr>
<td>Mainly used for equipment and processes to function</td>
<td>Mainly used by personnel to create and store data</td>
</tr>
<tr>
<td>Response time is critical</td>
<td>Consistent response time desired</td>
</tr>
<tr>
<td>Generally low bandwidth</td>
<td>High bandwidth requirements</td>
</tr>
<tr>
<td>Rebooting must be scheduled or avoided</td>
<td>Frequent rebooting is acceptable</td>
</tr>
<tr>
<td>Human safety and process uptime are paramount</td>
<td>Data confidentiality and integrity is highest importance</td>
</tr>
<tr>
<td>System uptime is most critical</td>
<td>System and data protection is most critical</td>
</tr>
</tbody>
</table>

Table 1: Comparison of Water Sector PCS vs. IT Network Operational Requirements

While the COTS components may be the same between corporate and industrial networks, there are critical differences between the requirements of Water Sector PCS networks compared to corporate IT networks [6] as illustrated in Table 1.

These differences are centered on the fact that Water Sector PCS are critical systems that must be kept online and running while a corporate IT environment can tolerate downtime much easier and are focused more on the availability and security of data. The differences in these two environments lead to different methodologies in how the similar network components within these systems are configured and used and how these networks should be designed. For example, corporate IT is fairly flat to allow many users within a facility access to the same data. Additionally, VLANs on an IT network are generally used to segment services and not necessarily to separate portions of the network where data is still required to communicate between devices. A typical corporate network may consist of the following VLANs:

<table>
<thead>
<tr>
<th>Typical Corporate Network VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
</tr>
<tr>
<td>Data</td>
</tr>
<tr>
<td>Server</td>
</tr>
</tbody>
</table>
This structure allows for a large number of users on the corporate network to have access to the same resources and provides a system where data is highly accessible. For a Water Sector PCS, it is not desirable for a lot of users to have full access to all data on the network. Conversely, for an ICS and specifically a Water Sector PCS, data is needed between control processes and by a few operators. Allowing many users access to this data could be detrimental to process operations and the overall operation of Water and Wastewater Treatment Plants. For these systems then, a different network structure is needed. Here, a hierarchical layered network architecture is recommended where VLANs are used not only to segment specific types of network traffic but also user and equipment groups to limit the accessibility of the data to specific users and processes.

**A Layered Approach to Network Architecture for Increased Security**

The starting point for a hierarchical layered network architecture is to divide the network into functional zones and to provide a hierarchy from most trusted to least trusted networks to control information flow between zones and access across zones. This description is similar to the nomenclature of zone and conduits described in the ISA 99 standard [6, 7, 8] and the cell and area zones described in the Cisco and Rockwell Automation CPwE design and implementation guide [10]. Typical zones might include the Process Control Zone (most trusted), the PCS Data Zone, the PCS DMZ, the Enterprise Zone, the Enterprise DMZ and the External Zone (untrusted). The zones are usually arranged bottom-to-top with the most trusted Process Control Zone at the bottom and directly connected to the process and the most accessible untrusted External Zone at the top. Information flow between zones is restricted at the boundaries between zones and access to each zone, except the External Zone, is limited. A general method for devising a layered network architecture can be seen in Figure 2.

This figure shows a simplified version of the organization of a Water Sector PCS and a recommended method for separating equipment into zones based on trust level. In general, the Internet and utility or municipality business networks should be seen as untrusted networks and ideally would be air gapped i.e., not connected. However, there are many advantages to leveraging these untrusted networks to support remote access, reduced communications cost and to provide remote system vendors with access for maintenance and troubleshooting of package controls systems. Other valuable uses of Internet connectivity include remote alarm notification, and software and firmware update management. When these services are needed or desired, the remote networks used should be given the
lowest trust level (0) possible and direct access should not be allowed to the SCADA or PCS PLC networks. Only the DMZ should have access to the Business networks and Internet in order for the layered architecture to be effective.

Figure 2: Layered Network Architecture Approach
The PCS Network DMZ is the location that relays communications between networks external to the PCS network and systems internal to the PCS network. Computers and applications located in the DMZ should be limited to only those necessary for remote access and notification such as webservers or terminal servers for SCADA HMI monitoring, remote alarm notification servers, and software and firmware update servers [12]. In some instances, it may also be necessary to locate a PLC or separate SCADA server in the DMZ to manage data communications with remote facilities communicating through the Business network or Internet, and these devices should be separate from those located at higher trust levels within the PCS network. Other systems are likely to also be present in the DMZ, or preferably separate DMZs, such as physical security related systems, reporting systems, and VoIP equipment. These systems should be fully separated from process control systems, and using separate hardware is recommended where feasible. A PCS Domain Controller is necessary at this level in order to authenticate and authorize users and apply group policies to further limit access to equipment and applications. It is recommended that the Domain Controller at this level be a read-only Domain Controller reading from the Domain Controller in the SCADA network layer. Within this layered architecture, the DMZ is the first layer of protection for the PCS network and the most vulnerable area of the PCS network. Equipment located in this layer and the functions and applications available in this layer should be carefully selected to ensure critical system components are not compromised.

The next higher trusted level in the layered architecture is the SCADA network. This is the main operator access level into the overall Water Sector PCS. Within this layer are components such as SCADA servers, operator workstations, terminal servers (supporting local SCADA users only), and printers to support the main HMI interface structure of the PCS and may also include other subsystem devices, segregated on separate VLANs and filtered by the firewall, such as physical security servers and VoIP equipment. The SCADA servers are the central devices in this layer requiring communications to operator interfaces and communications to the PLC network and DMZ to support process control and remote system monitoring and alarming. A domain controller is required at this layer in order to support authentication and authorization of SCADA system users. This domain controller is the primary device of where user accounts and groups are added and maintained for the SCADA system and should not support other systems such as the security system. This layer does not have direct communications with outside business networks or the Internet as it is buffered by the DMZ. The SCADA network level is a critical network for operator access and process control, but is also often required to communicate to devices in less trusted layers in order to implement remote functions. Communications between layers should be limited to the SCADA servers and Domain Controllers only to minimize available routes across layers. Domain Controller communications should be limited to an IPSec tunnel to the read-only domain controller in the DMZ.

The most trusted level in the layered approach is the PCS PLC network, sometimes referred to as the plant floor. This level is the most critical layer in the network and contains the components required for process control and system safety. Ethernet protocols are increasingly being used at this layer but this layer may include other digital communications protocols such as Modbus RTU, DeviceNet, ControlNet, Profibus, and Foundation Fieldbus which can be treated as separate sub-layers within the overall system. Within this layer are PLCs to control processes and often additional Ethernet connected devices
used within the process control system such as Variable Frequency Drives (VFDs), Motor Control Centers (MCCs), local Operator Interface Units, digital power meters, and instruments. A separate physical layer should be provided to support other end devices located in the field for the security and VoIP systems, if necessary, and these systems need to remain segregated from process systems using separate VLANs and Firewall rules. Communications between PLCs and process control components within this layer are critical for proper operation and safety for Water and Wastewater Treatment Plants and these systems must be maintained online and operational. By locating critical components within the most trusted layer, they are more difficult to gain access since multiple other layers need to be compromised first. Process control communications should be given the highest quality of service priority within this level.

Using a layered approach to network architecture provides multiple levels of protection for critical process components and the organization and security of this architecture can be further refined through additional network segmentation for a complete defense-in-depth strategy [13].

**Logical Segmentation Enhances System Performance**

A multi-level network architecture provides multiple layers of protection for critical process systems and is a critical component of the defense in depth protection strategy. Network organization and segmentation provides additional network security, improves network performance and reliability, and aids in maintaining the network. Networks can be organized using appropriate subnets and VLANs, where all devices on each subnet are members of the same VLAN. Both VLANs and subnets define a broadcast domain which significantly reduces network traffic by reducing the number of devices that receive each Address Resolution Protocol (ARP) broadcast. VLANs allow segmentation at Layer 2 where subnets are a Layer 3 construct, so pairing VLANs with subnets allows subnet segmentation to be extended across a layer 2 LAN environment improving network security and further reducing broadcast domains. In this way, overall network costs can be reduced by allowing different VLANs, i.e., separate networks, to reside on the same Layer 2 devices and share communications media (Layer 1).

In order to begin organizing the network addressing, a logical IP addressing strategy tailored to the applications is required to ease network management and support, as well as to provide for easy network expansion, upgrade and adaptation to changing needs. The Internet Assigned Numbers Authority (IANA) has developed guidelines for private, public, and reserved IP address ranges through a series of Request for Comments (RFCs) which are managed by the Internet Engineering Task Force (IETF). For the purposes of organizing a PCS network, the private IP address ranges, listed in Table 3, are of the most interest and are published in RFC 1918. These addresses are based on IPv4 which uses 32-bit IP addresses where the bit block refers to the number of bits, or IP addresses, available for use within the network and the Class slash ( / ) notation refers to the number of static bits used to define the

<table>
<thead>
<tr>
<th>RFC 1918 Name</th>
<th>Address Range</th>
<th>Network Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>24-bit block</td>
<td>10.0.0.0 – 10.255.255.255</td>
<td>Class A (10/8 prefix)</td>
</tr>
<tr>
<td>20-bit block</td>
<td>172.16.0.0 – 172.31.255.255</td>
<td>Class B (172.16/12 prefix)</td>
</tr>
<tr>
<td>16-bit block</td>
<td>192.168.0.0 – 192.168.255.255</td>
<td>Class C (192.168/16 prefix)</td>
</tr>
</tbody>
</table>

**Table 3: Address Allocation for Private Internets**
subnet. These addresses can then be used without any coordination with the IANA or an Internet Registry. Organization within the Water Sector PCS network should be selected based on the size and topology of the PCS network as well as existing enterprise wide policies and procedures. A small PCS may not require large class networks. The following is an example recommendation for a large utility or municipal network:

- 24-bit block: Devices and equipment within a treatment plant or facility.
- 20-bit block: Used for connections on private networks between facilities such as Metro-Ethernet or wireless links such as Microwave or Frequency Hopping Spread Spectrum (FHSS) radios.
- 16-bit block: WAN or MAN connected devices such as connections on City or County wide networks where the network may be shared with other users.

For large networks, particularly when the business network and the PCS network share resources or network infrastructure, the PCS IP addresses should be carefully coordinated with network administrators to ensure addresses are not duplicated within a private network. By following a standard methodology for IP addressing within a private network, it becomes simpler to prevent address duplication and to manage the different PCS networks. The steps involved in developing the IP addressing scheme include:

- Making a list of primary network segments
- Laying out a rough network topology with layer 3 interfaces separating primary network segments
- Developing an initial IP numbering strategy
- Creating a strategy and continue to add detail and make adjustments as required
- Ensuring that the scheme has the capacity and flexibility to accommodate expansion and to adapt to the ever-changing network environment

For each subnet assigned on the network a VLAN number and description needs to be assigned. The default or native VLAN is VLAN 1 and IP addresses not assigned to any other VLAN will be assigned to this VLAN making it subject to intrusion. For this reason, it is generally recommended to avoid use of VLAN 1 to enhance network management and security. The following provides a recommended approach for the use of VLANs within a PCS network:

- Use VLANs in the range of 2-1001, various restrictions apply to other VLANs
- Do not use VLAN 1 (default or native VLAN)
- Use devices that support IEEE 802.1q VLAN Encapsulation Protocol
- Use a logical approach in VLAN number selection to support network management
- Incorporate VLAN numbers into IP Addresses

By using the recommended approach, VLANs can provide network segmentation and aid in network management and organization. Combining a well thought out VLAN approach into an IP addressing plan
can improve network management, device IP address assignments and identification, and security [14]. An example approach to combining VLANs into an IP addressing scheme is shown in Figure 3 below:

![Figure 3: IP Addressing Example](image)

The major components of the IP addressing example in Figure 3 are the FACILITY and VLAN numbers. FACILITY numbers can generally be selected by actual Facility numbers or Unit Process numbers associated with a Facility to make the IP address a usable and recognizable number making it easier to associate an IP address with a specific location. VLAN numbers can be anything in the allowable VLAN range, however, the following approach outlines a method of selecting VLAN numbers to aid in equipment identification and to aid in trust level identification and Firewall configuration:

- Organize VLAN numbers in a similar order as Trust Levels, e.g. VLAN 10 is most trusted and VLAN 900 is least trusted.
- Separate VLAN numbers selected to allow for future growth and make addresses more distinguishable. Use VLAN numbers such as 10, 20, and 40.

Figure 4 shows an example VLAN selection scheme based on the recommended approach for selecting VLAN numbers and a network topology similar to that shown in Figure 2. In this example, VLANs start with 10 with the highest trust level being the network management VLAN. This VLAN would be solely used by the network administrator to use network monitoring and management software and would be able to have access to all equipment on the network. The VLAN order then closely follows the Layered Architecture shown in Figure 2 where
the PLC network was the most trusted network and the Utility WAN was the least trusted layer in the example architecture. Additional VLANs can be assigned as required for other systems and networks to meet the requirements of the PCS. By completing a detailed network assessment and devising a network security strategy, a successful network segmentation scheme can be planned and designed to allow for logical segmentation of Water Sector PCS networks. This logical segmentation can aid in network organization and identification of networks, locations, and components with a PCS network and can be used in conjunction with a layered network architecture and security rules to provide an organized approach to overall system cyber security.

**Coordinating Network Architecture and Segmentation for a Complete Solution**

Adding VLANs as part of the network segmentation plan for a multi-layered PCS network architecture provides additional security, lowers network utilization, and allows for simpler network management. Combining these solutions helps to eliminate unnecessary routes through the layers and reduces network traffic which improves both network security and optimization. Figure 5 shows an example Water Sector PCS control center LAN architecture utilizing the network segmentation approach previously presented.
Figure 5 provides an example of a typical PCS network with remote access and communications to other remote PCS control rooms that are physically separated to allow coordination across the Water Sector Utility. Figure 5 provides an example for a PCS network for remote pump stations where pump stations have PLCs located remotely throughout municipality that must be polled and data reported to a central SCADA system for monitoring and control. In this example, the local network is broken into multiple VLANs as shown in Figure 6.

**Layer 3 Switch VLANs**

- V10 — SCADA 10.40.10.0/24
- V11 — LINKSTATE 10.40.11.0/24 SCADA server linkstate tracking (Layer 2, IP is on Firewall interface only)
- V20 — PLC 10.40.20.0/24 (Layer 2, IP is on Firewall interface only)
- V30 — WEBSERVER 10.40.30.0/24 (Layer 2, IP is on Firewall interface only)
- V40 — BUSINESS 10.40.40.0/24 (Layer 2, IP is on Firewall interface only, shared with CCTV devices)
- V500 — MUNICIPAL UTILITY NETWORK (Layer 2, IP is on Firewall interface only)
- V601 — METROETHERNET (Layer 2, IP is on Firewall interface only)
- V600 — PUBLIC (Layer 2, IP is on Firewall interface only, network provided by ISP provider)

**Figure 6: VLAN Assignments**

As can be seen, multiple VLANs reside at Layer 2 and can communicate with other components on the same VLAN using only Layer 2 devices, thereby allowing separation of different network components but allowing communications using less expensive Layer 2 devices for the PCS LAN. In this example, the SCADA network is the most trusted network since it is located in the innermost layer of the network.
The PCS PLCs are the next most trusted component in the network since they poll data from remote pump stations via point to point VPNs with data encryption. This is reversed from the network architecture shown in the example of Figure 2 showing that network assessment and planning are necessary to identify the critical components of a network and that Water Sector PCS networks are unique requiring customized solutions that follow a standardized practice. Continuing with this example, VLANs 10, 11, 20, 30, and 40 reside on the local network and are trunked at the local Firewall for the network. This Firewall provides both routing and access control lists that govern communication between the VLANs on the network. Additional communications routes are also provided to a remote control room. These communications consist of a primary route through the Utility/Municipality network as well as disaster recovery communications through a private Metro-Ethernet network. The configuration of the VLANs for each of these networks, simplifies the allowed communications between these networks.

As noted previously, communications between PLCs are done through remote VPN connections but PLCs are still all on the same VLAN to allow direct communication between PLCs without the need for a specific route to be established. Figure 7 shows the remote VPN connections needed for remote device communications. Note that only VPN connections are necessary and that additional routes are not needed to be established since devices that need to communicate with each other are on the same VLAN.
Figure 7: Remote Connections using VPNs

By combining a layered architecture with logical network segmentation, network organization and remote communications become simplified and the effort needed to established communication routes and access control lists is simplified making network configuration and management simpler. Figure 8 summarizes the VLAN and subnet organization for the example architecture.
Configuration and Management

One of the main features of a logical segmentation plan within a multi-layered network architecture is a simplified approach to firewall configuration thereby making network security and routing management simpler. By using VLANs to coordinate similar equipment having similar access rights and trust levels together, routing and access control lists configuration for communications between subnets on the network becomes easier. Communications routes between networks for devices added to a given VLAN are then already in place. Network expansion is then simplified since new routes and rules within
network security and routing appliances do not need to be added or revised each time a piece of equipment is added to the network. Figure 9 shows an example Firewall Trust Level configuration for the network presented in Figure 5. This example exhibits how trust levels can be defined simply for large groups of network connected equipment based on VLAN assignments.

![Firewall Interface Trust Level](image)

**Firewall Interface Trust Level**

- 0 — PUBLIC VLAN900 (least trusted, VPN end points for remote cellular pump stations)
- 10 — MUNICIPAL UTILITIES VLAN900 (IPsec endpoint for remote sites)
- 20 — METROETHERNET VLAN801 (Disaster Recovery IPsec endpoint for remote site)
- 40 — BUSINESS VLAN40 (shared with CCTV devices, Internet allowed, **No access to SCADA**)
- 80 — WEBSERVER VLAN30 (**No internet access, limited access to SCADA VLAN, remote access from remote workstations through user VPN**)
- 90 — PLC VLAN20 (**No internet access, limited access to SCADA VLAN**)
- 99 — LINKSTATE (**No internet access, limited access to site 50 for SCADA servers linkstate tracking**)
- 100 — SCADA VLAN10 (most trusted, **No internet access**)

![Figure 9: Firewall Trust Levels](image)

Figure 8 depicts the trust levels for the various VLANs and notes global rules for each VLAN such as what other networks or VLANs each trust level is allowed to access. In order to provide a complete security configuration additional access control rules are necessary to further define allowed communications between networks. Using VLANs with associated trust levels allows for simplified global rules which make implementation and management of the network simpler. Figure 10 provides an example of Firewall rules and allowed VPN tunnels for the example shown in Figure 5 and trust levels summarized in Figure 9. Figure 10 provides a summarized form of the rules to be implemented in an actual Firewall and shows how organizing a network into subnetworks using VLANs can greatly simplify the rules implemented in an actual Firewall.

![Firewall Security Boundaries and VPN Tunnels](image)

**Firewall Security Boundaries and VPN Tunnels**

* PUBLIC VLAN900 — IP addressing provided by the ISP service provider; hosting remote Site-to-Site VPNs to the remote cellular pump stations and Remote Access VPN’s for the mobile workstations. NAT a public IP to the MS Exchange server allowing SMTP ingress.
* MUNICIPAL UTILITIES VLAN900 — MUNICIPAL UTILITIES shall provide at least a 256 fully meshed IP network at each remote control room to be used as the Site-to-Site VPN end points between Central Control Room and Remote Control Room.
* BUSINESS/CCTV VLAN40 — Grant access to the internet, remote sites business network across Site-to-Site VPN’s. Deny everything else.
* WEBSERVER VLAN 30 — Grant access to Primary SCADA Server destination host for remote cellular wireless workstations user VPN’s and internet connected user VPN’s.
* PLC VLAN20 — Grant access from Primary SCADA Server, destination for remote pump station’s Site-to-Site VPN’s.
* SCADA VLAN10 — Grant access to the remote control room’s Site-to-Site VPN’s and the two printers on the business network. Deny everything else.

![Figure 10: Firewall Access Control Rules](image)

As seen in Figure 10, each set of rules is defined by VLAN, or could be defined by subnet, but not by each device or each specific IP address. Having an organized network approach then allows for global definitions of access control lists and global management of devices within groups in lieu of having to manage each device separately. By combining similar devices into groups by planning and organizing the network, network configuration and management is simplified.

**Conclusion**

The approach for a multi-layered Water Sector PCS using VLAN segmentation for subnetworks provides a foundation for which secure PCS can be developed. By using the strategies and tools such as the four...
phase process of assessment, design, implementation, and procedures/maintenance, a Water Sector
PCS network can be customized using the framework presented to provide a secure and manageable
PCS network. As with any system, planning and design must be carefully coordinated to ensure
components are located within the correct layer of the architecture and that the proper firewall rules
and access control lists are implemented. By using VLANs, this segmentation can be extended across a
Layer 2 LAN. The advantage of the approach presented is that it allows for simpler configuration of
network security appliances and for simpler management and expansion of the network leading to
increased network availability and a reduction in threat risk as part of a comprehensive defense-in-
depth strategy.

References


   Cybersecurity Guidance is Available, but More Can be Done to Promote Its Use*. GAO-12-92,
   December 2011.


   2009.

   control system security*. ISA InTech, January/February 2011.
   (http://www.isa.org/InTechTemplate.cfm?Section=Current_Issue&template=/ContentManagem
   ent/ContentDisplay.cfm&ContentID=84829)

   800-82 (Revision 1), May 2013.

    Cisco and Rockwell Automation, September 2011.

11. *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-


---

**List of Acronyms:**

ACL .................. Access Control List
CERT ................. Cyber Emergency Response Team
COTS.................. Commercial-Off-The-Shelf
DMZ.................. Demilitarized Zone
HMI.................. Human Machine Interface
ICS .................... Industrial Control Systems
IP ...................... Internet Protocol
IT ...................... Information Technology
MCC.................. Motor Control Center
NIST .................. National Institute of Standards and Technology
PCS ................... Process Control System
PLC................... Programmable Logic Controller
SCADA .............. Supervisory Control and Data Acquisition
VFD ................... Variable Frequency Drive
VLAN ................. Virtual Local Area Network
VPN ................... Virtual Private Network
VoIP .................. Voice over IP

---

**Norman Anderson, PE:** Norman has over 6 years experience in the design and commissioning of Process Control Systems and Security Systems for the Water Sector. Norman has provided secure and reliable PLC, SCADA, and Network hardware and software architecture designs and provided control system automation solutions for a range of facilities. Norman has an M.S. in EE from Iowa State University and an M.S. in Physics from the University of Florida. Contact: norman.anderson@ch2m.com

**Bill Phillips, PE:** Bill specializes in delivery of secure and reliable process control and SCADA network and communications systems, cyber security vulnerability assessment, and facility automation and information system planning and implementation. Bill has over 30 years of process control and SCADA
system experience and has focused on control system network and communications cyber security for the last decade. Bill has a BSEE from Clemson University. Contact: bill.phillips@ch2m.com