Security Through VLAN Segmentation: Isolating and Securing Critical Assets Without Loss of Usability

Garrett Leischner and Cody Tews
Schweitzer Engineering Laboratories, Inc.

Presented at the
9th Annual Western Power Delivery Automation Conference
Spokane, Washington
April 3–5, 2007

Security Through VLAN Segmentation: Isolating and Securing Critical Assets Without Loss of Usability

Garrett Leischner and Cody Tews, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—SCADA infrastructures, which traditionally were isolated from outside systems, have now become highly integrated via internal and external communication paths. These integrations increased efficiency greatly but introduced security vulnerabilities.**

This paper presents a solution for mitigating those security vulnerabilities by integrating VLAN and VPN technologies. VLAN segmentation provides virtual isolation of devices from other network segments, but it inhibits usability. Integration of VPN technology implements a controlled border that protects critical assets while preserving usability. This paper introduces network topologies that use VLAN and VPN technologies with equipment in existing SCADA implementations to harden the system and make it more resistant to attack.

I. Introduction

Many different classes of network traffic (such as SCADA data, engineering access, video streams) can share common network resources so the interconnection of diverse data streams has become routine. However, allowing different classes of traffic to traverse through a single flat network can result in undesired accessibility or failure to achieve service requirements.

Most new substation equipment is Ethernet-enabled, so many of the difficulties substation networks confront, such as traffic separation and privacy, are similar to those for which sound resolution techniques exist in corporate local area networks (LANs). It is possible, therefore, to apply these protection techniques to substation networks.

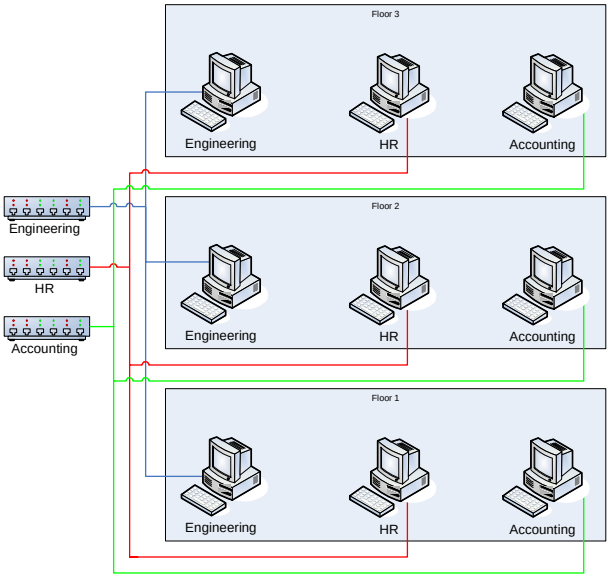

Fig. 1. Traditional Network Topology

Ideally, different classes of traffic would be separate and physically isolated, as in Fig. 1. This separation often requires redundant equipment and cabling, which may be unfeasible because of physical or fiscal restraints. However, while it may not be possible to physically place critical systems on separate networks, network administrators may achieve the same effect by creating a virtual LAN (VLAN). A VLAN separates devices by media access control (MAC) addresses on Open Systems Interconnection Reference Model (OSI) Level 2. Effectively, this is similar to physically separating traffic with completely independent infrastructure, except that network traffic separation occurs through the switches, as shown in Fig. 2.

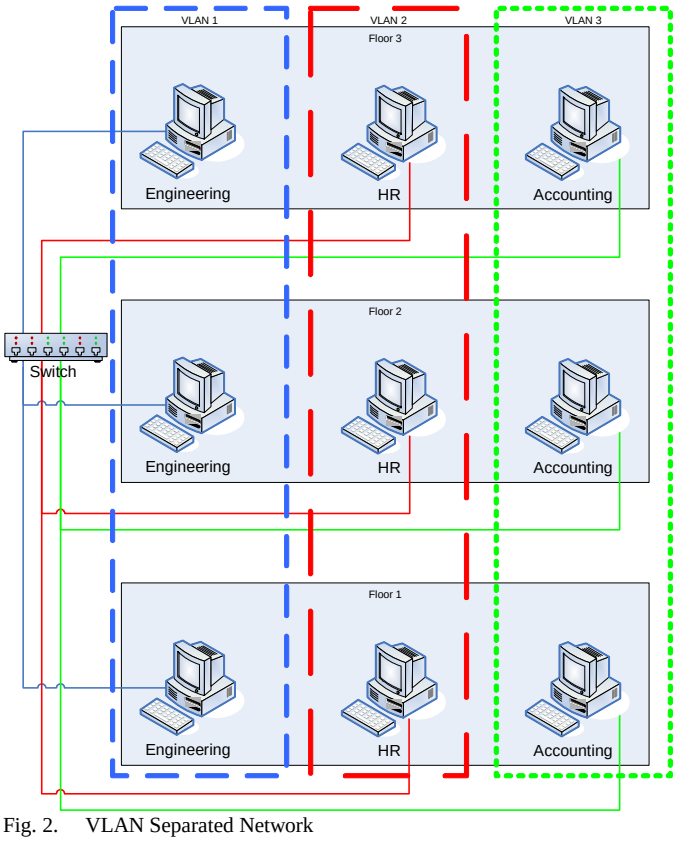

Fig. 2. VLAN Separated Network

While this virtual separation may not eliminate as much risk as a dedicated communications topology, it minimizes asset visibility more than previously possible within the limitations of a flat infrastructure. Existing flat network topologies have many similarities to the ordinary egg. The shell or perimeter acts as a boundary between internal processes and the hostile

outside. However, once an outside agent penetrates the shell, it will find the fluid center easy to move through and be able to monitor or alter other internal objects without much resistance.

As devices inside the substation increase in sophistication, so also does the diversity of traffic that moves within as well as traversing the physical perimeter of the substation network. This traffic can include real-time data about power system operation, time-critical messages between protective relays, live video surveillance streams, Voice Over Internet Protocol (VOIP), SCADA, engineering access, and other nonutility-related traffic. Separating different classes of traffic is essential for service and protection of substation devices and infrastructure.

The role and potential benefits of an Ethernet-based substation LAN are well known and have been extensively documented [1]. This paper discusses design alternatives in which switch-based VLAN technology provides traffic separation inside the substation, and Ethernet IPsec virtual private network (VPN) technology provides privacy for traffic traversing the perimeter of the substation network. This paper also presents an application example implemented with native switch-based Ethernet.

II. Network Hardware

Most networks employ a variety of hardware to ensure that traffic from one device can reach its destination at another device. This equipment is categorized according to features and capabilities. Typical categories include: hub, managed/unmanaged Layer 2 switch, Layer 2/3 switch, and router.

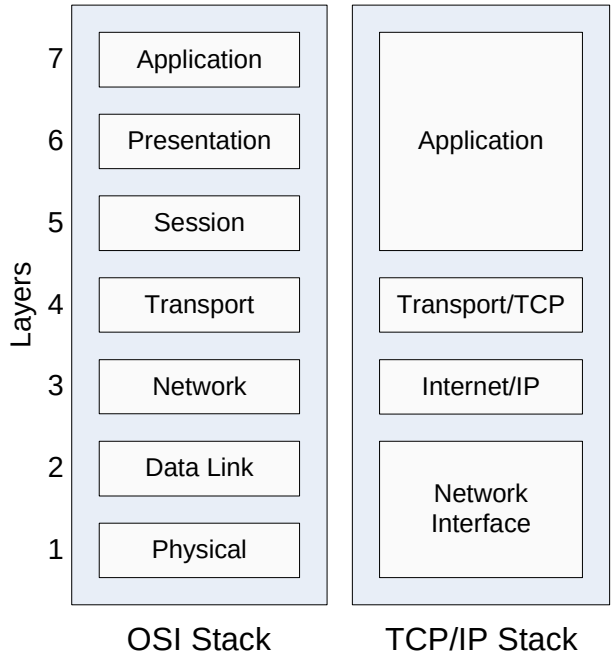

Fig. 3. Comparative Graph of OSI vs. Hybrid TCP/IP Model

The OSI model provides a method of abstracting the structure and function of each layer of network protocols. Evolved from ARPANET, TCP/IP describes what is implemented in a majority of networks. A description of each layer of the OSI stack is available in the Appendix.

A. Hub

The network hub is the simplest device serving as a physical layer interconnect. The network hub electrically replicates all incoming traffic on a port and indiscriminately distributes it to all other ports. The hub makes traffic transmitted on one port visible to all ports, creating higher volumes of traffic on the network. When two ports attempt to communicate at the same time, this causes a collision, resulting in both ports retransmitting after random delays. The limitations described have made hubs virtually obsolete. They should not be used in modern substation installations.

B. Layer 2 Switch

The Layer 2 switch is a more complex device that operates on the OSI data link layer of an Ethernet packet. In general, a network switch reads the destination MAC address from an Ethernet packet and then forwards the packet to the port on which the address's owner resides. As its name implies, a Layer 2 switch only recognizes information residing in the layer 2 header of the packet, and is oblivious to all information above it (in higher layers) in the OSI stack, such as IP information. The switch is therefore unable to route traffic across different subnets. Layer 2 switches can either be unmanaged or managed.

Unmanaged switches have no configuration interface, so installation is much like that of a traditional network hub. However, because the switches send packets only to the destination port, throughput and latency performance are improved dramatically over that achieved with a network hub that broadcasts packets to all ports.

While a Layer 2 managed switch is still limited to handling MAC addresses, it can provide such features as port control, port prioritization, MAC filtering, and VLAN settings. These features give an operator a higher level of flexibility and control over the handling of traffic on the switch.

C. Layer 2/3 Switch

Some switches, commonly referred to as Layer 2/3 switches, support operations on the OSI network layer (Layer 3) of the Ethernet packet. The managed switch can therefore perform routing functions commonly associated with a standalone router.

D. Router

The network router is a device that operates on the OSI network layer (Layer 3) of an Ethernet packet. Typically this operation is associated with the IP layer. Routers help translate communications between two different IP subnets. Segregating traffic between LANs effectively stops transmission of broadcast and unroutable traffic. Many routers can also support security features such as IPsec (Internet Protocol Security) tunnels and Network Address Translation (NAT).

An IPsec tunnel creates a protected encrypted private communication channel over an untrusted network for site-to-site communication. With such a channel, devices at one site can communicate securely over an untrusted network with a device at another site.

NAT masks/translates all communication passing through it, giving internal devices a different IP subnet than that of the

external network. This translation provides some security benefits, but it can also pose problems for some types of network communications. TCP connections that must initiate from outside the NAT device can fail, because these packets cannot find their destination. Widely used communication mechanisms, such as the FTP passive mode, have resolved many of these issues but not all embedded networking devices handle all use cases correctly.

III. VLAN Technologies

Virtual LANs (VLANs), defined by the 1998 IEEE standard 802.1Q, operate at level 2 of the OSI model [2]. As Fig. 2 shows, VLANs provide segregation between logical workgroups that may or may not be in physical proximity to each other. As shown in Fig. 4, by attaching an extra 4-bytes to the original Ethernet header, multiple classes of traffic can share the same physical infrastructure and maintain traffic separation similarly to physical separation. This 4-byte area contains a 3-bit user priority field for setting the priority level of the frame, as well as a 12-bit VLAN ID to designate VLAN association [1].

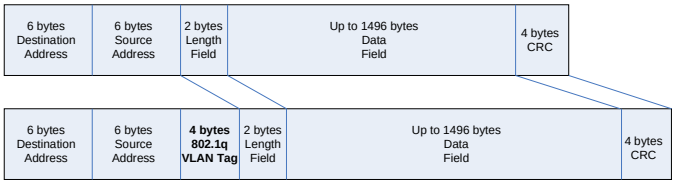

Fig. 4. VLAN Frame[EC1]

Quality of Service (QoS), defined in IEEE standard 802.1p, use the VLAN 3-bit priority fields to provide eight unique traffic priorities [3]. Typically, the highest priority QoS tags are utilized for critical time sensitive traffic such as protection and routing information. Historically, QoS technology has provided switches and routers the ability to prioritize bandwidth allocation. QoS now enables them to prioritize VLAN traffic.

By implementing VLANs, one can configure a switch to allow a given edge device to only talk to other devices on the same VLAN or on other trusted VLANs. As Fig. 5 illustrates, use of traditional technology would have required a unique physical infrastructure for each bridged network.

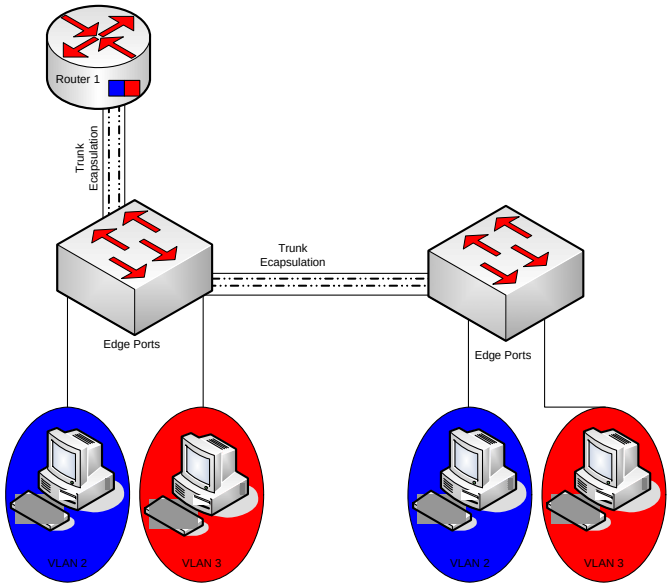

Fig. 5. VLAN Edge vs. Trunk Port

Typically on an Ethernet switch utilizing VLANs, each physical, enabled port will be configured as an edge port. If an edge port receives traffic with a VLAN tag already applied, the switch will discard the entire packet. Traffic entering an edge port of the switch is tagged with the VLAN ID of the port, so traffic such as IEC 61850 GOOSE tagged at the downstream device is blocked from traveling to a designated VLAN. For this IEC 61850 GOOSE traffic to traverse VLANs, the port would need to be configured as a Trunk port.

A Trunk port provides multiple VLANs access to a physical port. This port typically serves as a backbone port between two switches that support a common set of VLANs. A set of switches can then pass communication separated over multiple VLANs on one physical connection. By changing a substation device's associated port from an edge interface to a Trunk interface, one retains pretagged traffic entering the switch. Further details about practical application of this approach are described in [1].

Depending on the features a vendor implements on its switch, one can apply additional restrictions by configuring VLAN filters per switch port. VLAN access from Trunk ports can follow a white or black list access control scheme. In such a scheme, one can configure a Trunk port in one of two ways. A white list allows only the ports specified on the list to use Trunking. A black list prevents all ports on the list from using Trunking.

Although Trunk ports can send traffic to any VLAN to which they have access, they still possess a native VLAN. The switch or router tags any traffic that does not contain explicit VLAN tags (such as Telnet, FTP, and common SCADA messages) and assigns this traffic to the port native VLAN.

IV. VLAN Security Threats

Network administrators have utilized VLANs to implement data protection by contributing a layer of separation and security. However, VLAN tagging was not designed as a security measure. One should take this into account when implementing VLANs to achieve security. VLAN hopping is the common term associated with any method that allows a malicious

device to send packets to a VLAN port that it should not normally be allowed to access.

A malicious device can also bypass the security of a VLAN by knowing the MAC address of the target system. This serious threat to VLAN security requires attackers to possess inside knowledge of the device they are targeting and the locations of these devices. Once attackers know the MAC address, they can enter a static address entry for the target device into the local ARP cache of the attacking system. This allows for direct communication between the devices even though these devices exist on separate VLANs [4].

Switches use Trunk ports to create a communication channel that allows a common set of VLANs to span multiple switches. When a switch is connected to an existing infrastructure, it uses a Trunk port. Packets are passed between the switches with VLAN tagging intact, so each packet's VLAN designation is maintained, preserving traffic separation.

Trunking can be configured on a per port basis according to a white or black list and depending on vendor implementation. While switches use Trunking to create connections between multiple switches, a failure to disable access could result in a malicious device appearing as a switch that requires Trunking [5]. A Trunk port on a VLAN is a port that potentially has access to all allowed VLANs. If a malicious device were on a Trunk port, it could attempt to hop VLANs by sending a packet with a VLAN tag already attached to a normally inaccessible device/port on a different VLAN. Disabling Trunking on ports that do not need to use it, such as those not connected to another switch, can minimize this form of VLAN hopping.

VLANs offer a great solution for local segregation where the physical implementation can be trusted. For untrusted or partially trusted network segments, one must consider the use of confidentiality, authentication, and integrity to protect the transmitted data. VPN technology is helpful for such situations.

V. VPN Technology

With traffic traversing the substation boundaries over permanent, not fully trusted connections, the increased risk that a malicious entity will gain access raises concerns. Often, the goal of a cyberattack is to transmit data to critical electronic equipment to cause some effect (misoperation, suspension of critical protection functions, etc.). By implementing technologies such as VPNs, it is possible to prevent unauthorized data transmission to critical infrastructure devices, and to prevent interception of authorized data transmissions (i.e., passwords and other sensitive data) to and from these critical devices.

VPNs create secured communication links between geographically distant locations with the purpose of providing the same level of security that would be available within a fully trusted network. The two types of VPNs are trusted and secured. A trusted VPN provides computers in different locations with the ability of being members of a common LAN, with access to the network resources located within its constraints. A trusted VPN does not establish privacy. A secured VPN uses cryptographic tunneling protocols to provide privacy. Within a secured VPN, confidentiality, sender authentication, and message integrity establish privacy. Table 1 shows the elements necessary for achieving privacy.

TABLE 1
SECURITY TYPES FOR ACHIEVING PRIVACY

Confidentiality	Sender Authentication	Message Integrity
Prevention of Snooping or Monitoring	Prevention of Identity Spoofing	Prevention of Message Alteration

With all VPN solutions, there must be two end points at which the added protection of the VPN is removed from the traffic. The most likely termination location is either the device itself or an IPsec gateway located within the physical security area of the device. However, many substation devices are unable to support VPN termination, so termination occurs at an inline network infrastructure device within the locality of it, which is capable of supporting VPN termination. IPsec is the most widely supported variant of VPN on network infrastructure.

A. IPsec

The IPsec stack, shown in Fig. 6, is an OSI Layer-3 protocol for securing Internet Protocol (IP) communications by encrypting and/or authenticating IP packets.

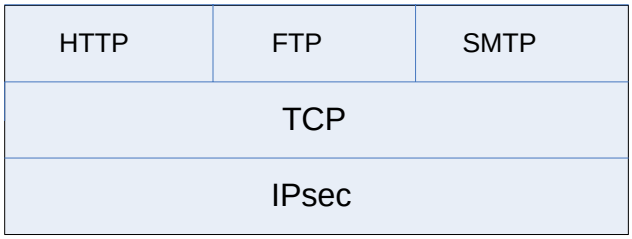

Fig. 6. IPsec Stack Implementation

Either an Encapsulating Security Payload (ESP) or Authentication Header (AH) secures the data for communication. As Fig. 7 illustrates, ESP provides each type of security necessary for privacy (Table 1). AH provides only authentication and message integrity but does not encrypt the data within the packet.

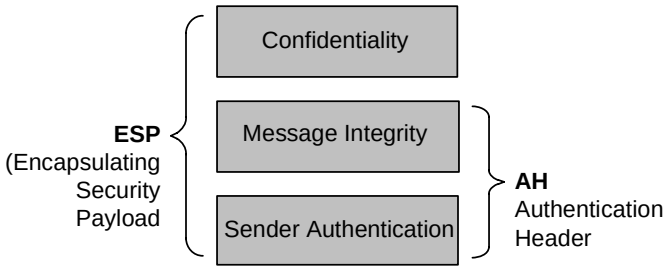

Fig. 7. IPsec Encryption and Authentication Methods

IPsec can operate in either transport mode or tunnel mode. Transport mode authenticates the two peers and establishes a secure communication channel. This secure channel ensures that communication between two computers remains tamper-free and private. This channel provides client-to-client and client-to-server communication. The IPsec tunnel mode secures traffic routed between two gateways over an untrusted network. In this case, a device at one site must communicate to a device at the other. The traffic passes through the IPsec gateways. Tunnel mode should only be used for site-to-site

communication. Tunnel mode does not support client-to-client or client-to-server communication.

A NAT-enabled router can cause difficulties with IPsec tunnels created from within the NAT as parts of the IP header change and affect the AH. IPsec operates only on routable protocols, so broadcast and non-routable messages such as IEC 61850 GOOSE cannot traverse an IPsec tunnel. Therefore, most VPN solutions are not viable for transmitting messages such as IEC 61850 GOOSE.

Depending on the application-based performance requirements, GOOSE messages can sometimes be distributed using secure tunneling protocols such as Layer 2 Tunneling Protocol[g2] (L2TP).

The protected tunnel created between the two end points is commonly referred to as an IPsec tunnel. Each IPsec connection is defined by a set of security associations (SA). Each SA can be filtered based upon source and destination addresses (IPv4 or IPv6), Name (User ID or System name), Transport Layer Protocol (TCP or UDP), and source and destination ports (port number) [6]. These SA selectors help determine eligibility of inbound or outbound traffic for association with a particular SA.

The IPsec security protocol supports very strong cryptographic authentication and encryption. Many routers and layer 2/3 switches support IPsec through the Access Control List (ACL) entry mechanism. Through the use of SA selectors, it is possible to write ACL entries that force a router to apply the IPsec protocol to very specific TCP/IP traffic profiles. Since IPsec is implemented at a lower layer, TCP/UDP header information is exposed, as shown in Fig. 6, so it is possible to filter all TCP/UDP traffic into a set of SA's. Thus, a filter handles all traffic that enters or leaves the IPsec device and no host between the endpoints of the IPsec tunnel can inject malicious packets or analyze the communication.

As Fig. 8 illustrates, the router drops all frames an attacker forms and sends to the substation computer because these frames fail authentication. This failed authentication occurs because the attacker has no knowledge of the secret encryption/authentication key that must be used to code any data the router accepts on the SCADA interface.

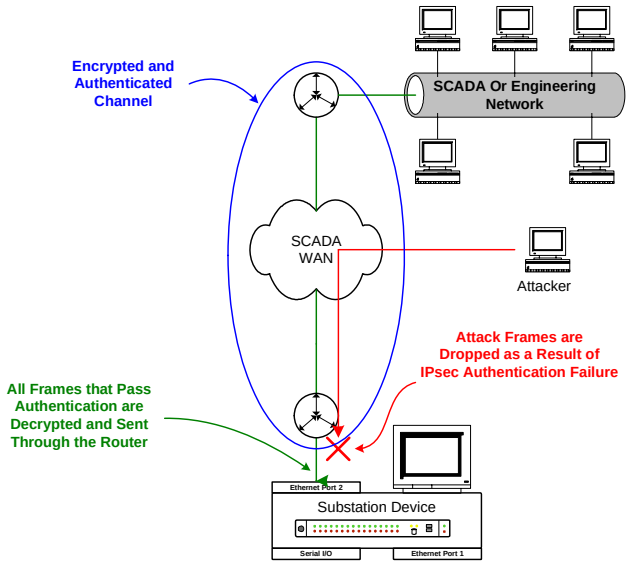

Fig. 8. IPsec Blocks All Unauthenticated TCP/IP Frames

These IPsec filters work in tandem with traffic filtering ACL entries to ensure that all suspicious TCP/IP traffic either is dropped because: a) it does not match the expected traffic profile, or b) it fails the strong cryptographic authentication mechanisms the IPsec protocol provides.

1) IPsec Vulnerabilities

While IPsec itself is not known to have security vulnerabilities, specific implementations have been known to introduce vulnerabilities. Vulnerabilities can also be introduced if IPsec is not configured properly.

Verifying cryptographic implementations, such as those utilized in IPsec, is unfeasible in most situations, so it is important to look for implementations that have been validated by third party experts. Common validation programs include Federal Information Processing Standards (FIPS) 140-2 and Cryptographic Module Validation Program (CMVP). These validation programs test the cryptographic strength and implementation to ensure that the cryptographic engine is implemented properly and that it can protect data to a predefined baseline.

While there is a relatively small likelihood of a validated IPsec implementation having security issues, there is a much greater chance that a misconfigured tunnel configuration will introduce a security hole. For example, in the case of a traffic filter implementation without any authentication verification on the packets, a knowledgeable attacker could send malicious TCP/IP traffic matching the expected traffic profile through the router. Thus, this rogue traffic survives being dropped by the IPsec traffic filter in the router. Posing as a legitimate device on the SCADA network, by faking or spoofing the IP address of a legitimate device, an attacker can send malicious traffic to the substation device. This is why proper implementation of cryptographic authentication and encryption technologies, such as IPsec, on remote communications links is so important.

VI. Substation Implementation

Individually, VLANs can help segment traffic, and VPNs protect traffic privacy. However, when used in combination within a substation environment, these technologies can create a tiered system of cyber protection. Where flat networks implement a fortress model, which closely resembles an egg with a hard shell and soft middle, VLAN and VPN technology facilitates a transition to a defense in depth model in which there are multiple levels to traverse before security is breached.

In Fig. 9, a switch manages communication inside the substation and passes traffic traversing the boundary of the substation to the adjoining router/firewall, overall minimizing the security obligations of any one device. While best practice would have the two functionalities separated, alternatively if the switch was a Layer 2/3 switch to achieve the same network functionality and minimize the equipment obligation. Additionally, since this equipment is already in place for a typical Ethernet connected substation, new equipment would not be needed.

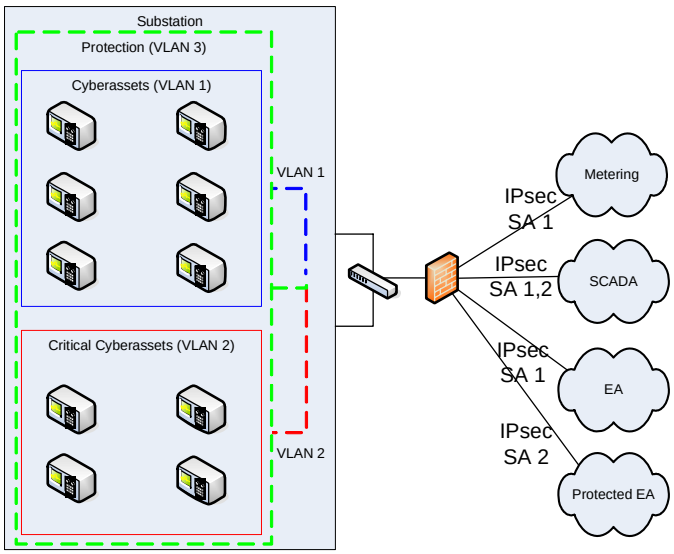

Fig. 9. Integrated Substation Solutions

Additionally, Fig. 9 demonstrates the use of three individual VLANs separating internal Protection, Cyberassets, and Critical Cyberasset traffic. Subscribing to these data are four IPsec tunnels with a subset of SA's creating the connection to outside the substation network. SA's are identified with an IP subnet and not a VLAN itself, so it is important that each VLAN communicates on a separate subnet with respect to routable traffic.

In the case of Fig. 9, imagine that a SCADA system must access both the cyberassets and critical cyberassets. Multiple SA's can be defined in one IPsec tunnel, so the SCADA system can receive access to both the critical and non-critical assets within the substation. We therefore define two SA's. One SA is associated with VLAN 1 for access to the cyberassets. The other SA is associated with VLAN 2 for access to critical cyberassets within the substation. The SCADA system can communicate to all the assets while keeping the traffic separated until it reaches the termination location for the IPsec, typically another router.

We can communicate protection information over VLAN 3, assuming that the IED allows per protocol VLAN specification (such as IEC 61850 GOOSE). The IED will be communicating over multiple VLANs, so the associated port on the switch must allow Trunking. Coincidentally, if Trunking is disabled, any VLAN tags the device attached will be removed at the switch. Trunking adds a potential security risk, but limiting the VLAN segment access for Trunk ports can mitigate this risk.

The protection communication traffic on VLAN 3 is the most critical, so the VLAN prioritization for this traffic will be set higher than the associated engineering access or non-real-time VLANs.

Traffic coming into the switch from an external location will not be allowed access to VLAN 3 and the associated protection information VLAN 3 transports. This is because VLAN 3 will be used only for traffic inside the substation perimeter. If a device outside the perimeter attempts communication with a device over the EA IPsec connection by pre-attaching a VLAN 3 tag to the packet, it will fail because the incoming VPN connection port does not have access to that VLAN. This traffic will subsequently be dropped since the port does not have access to VLAN 3. This ensures that VLAN 3 traffic remains protected and within the confines of the substation.

By separating different classifications of information into the intrasubstation realms for different VLANs, communication can be segmented according to protection needs. Creating different IPsec tunnels, with different SA's according to use, allows separation of communications according to specific end destinations.

With this complete solution, it is possible to maintain usability throughout the system for intended traffic, while creating great obstacles to unintended or malicious traffic gaining access. Traffic can only traverse the substation boundary through defined secure tunnels, ensuring that privacy is maintained for all data communicated beyond the substation.

VII. Conclusion

This paper presents a methodology for using proven network topologies to separate and secure substation's networks. The paper explains the advantages and pitfalls associated with the technology and gives guidance for the design of reliable communication schemes, including an application example that demonstrates the use of VLANs and VPNs for communication protection purposes.

VLANs offer a preferred method for simplifying substation wiring, reducing installation cost, and enhancing overall protection of contemporary high-speed Ethernet communication networks. VPNs offer a method for ensuring privacy and separation of data from a substation to its end destination over an untrusted network. When applied properly, VLANs and VPNs offer a powerful new tool in the development of new and existing communication architectures.

VIII. Appendix

OSI—The Open System Interconnection (OSI) model defines a networking framework for implementing protocols in seven layers:

Layer 1—Physical Layer
Transmits bits over physical medium—copper, fiber, radio link, or any other medium

Layer 2—Data Link Layer
Moves data across one hop of the network

Layer 3—Network Layer
Responsible for moving data from one system through routers to a destination system

Layer 4—Transport Layer
Reliable communication stream between two systems

Layer 5—Session Layer
Coordinates sessions between machines—helps to initiate and manage sessions

Layer 6—Presentation Layer
How data elements are represented for transmission—order of bits and bytes in numbers—floating point rep.

Layer 7—Application Layer
Actual applications that use the communication channel

(http://www.webopedia.com/quick_ref/OSI_Layers.asp)

IX. References

[1] V. Skendzic and R. Moore, "Extending the Substation LAN Beyond Substation Boundaries: Current Capabilities and Potential New Protection Applications of Wide-Area Ethernet." [Online]. Available: http://www.selinc.com/techpprs/6231_ExtendingtheLAN_VS_03-03-06.pdf

[2] IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks, IEEE Standard P802.1Q, Jul. 1998.

[3] Information technology - Telecommunications and information exchange between systems - Common specifications - Part 3: Media Access Control (MAC) Bridges: Revision, IEEE Standard P802.1p, Nov. 1997.

[4] R. Farrow. (2007, Jan. 4). *VLAN Insecurity*. [Online]. Available: http://www.spirit.com/Network/net0103.html

[5] Cisco. (2006, Aug. 6). *Configuration Examples Related to VLAN Features*. [Online]. Available: http://www.cisco.com/univercd/cc/td/doc/product/lan/28201900/1928v8x/eescg8x/aleakyv.htm

[6] S. Frankel, *Demystifying the IPsec Puzzle*. Boston/London: Artech House, 2001, p. xx.

[7] S. Wooldridge. (2006, Aug. 6). "Application Security," *Electric Energy T&D Magazine*, IEEE 802.1Q, 2005, IEEE Standard for Local and Metropolitan Area Networks-- Virtual Bridged Local Area Networks. [Online]. Available: http://www.electricenergyonline.com/article.asp?m=5&mag=29&article=235

[8] Information technology - Telecommunications and information exchange between systems - Common specifications - Part 3: Media Access Control (MAC) Bridges: Revision, IEEE Standard P802.1D, Nov. 1997.

X. Biographies

Garrett Leischner is a Product Engineer with Schweitzer Engineering Laboratories Automation Integration and Engineering Division, where he manages the Rugged Computing Platform. Prior to joining SEL, he worked for Cray, Inc. He received his BA in Business from Western Washington University in 2003, and his MS in Computer Engineering from the University of Idaho in 2006. He is an active member of the IEEE Computer Society, Association for Computing Machinery, and the Software Engineering Institute, and has several patents pending. During his time at SEL, he has co-authored several technical papers and instructional courses.

Cody Tews is a Research Engineer with Schweitzer Engineering Laboratories Government Services Division. Prior to joining SEL, he worked for Comtech AHA developing multi-gigabit communication products. He received his BS in Computer Engineering and a BS in Economics from the University of Idaho in 2003. He is an active member of the IEEE Computer, Software Engineering, and Communications Societies.

20070329
TP6277-01