SANS Institute
Information Security Reading Room

Secure Architecture for Industrial Control Systems

Luciana Obregon

Copyright SANS Institute 2021. Author Retains Full Rights.

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Secure Architecture for Industrial Control Systems

GIAC (GSEC) Gold Certification

Author: Luciana Obregon, lucianaobregon@hotmail.com
Advisor: Barbara Filkins
Accepted: September 23, 2015

Template Version September 2014

Abstract

Industrial Control Systems (ICS) have migrated from stand-alone isolated systems to interconnected systems that leverage existing communication platforms and protocols to increase productivity, reduce operational costs and further improve an organization's support model. ICS are responsible for a vast amount of critical processes necessitating organizations to adequately secure their infrastructure. Creating strong boundaries between business and process control networks can reduce the number of vulnerabilities and attack pathways that an intruder may exploit to gain unauthorized access into these critical systems.

This paper provides guidance to those organizations that must secure their ICS systems and networks through a defense-in-depth approach to security, achieved through the identification of key security patterns and controls that apply to critical information security domains. The goal is a visual explanation that allows stakeholders to understand how to reduce information risk while preserving the confidentiality, integrity and availability of critical infrastructure resources in the industrial control environment.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

1. Introduction

Industrial Control Systems command a large percentage of the world's critical infrastructure, such as air traffic control, electrical and nuclear power plants, waste water treatment plants, refineries, pipelines and dams. ICS have traditionally been developed using specialized hardware and software and deployed as stand-alone platforms employing vendor proprietary communication protocols to interact amongst like systems. In the past, this compartmentalized architecture met manufacturing and business goals while eliminating the risk of cyber intrusions that could arise from the exploitation of well-known vulnerabilities found in commercial systems and applications. The majority of ICS were confined to a particular physical plant and detached from external computer networks. As a result, organizations had to strengthen their physical security to ensure that the systems were accessed and operated by only those individuals that had authorization to do so.

The increasing need to reduce manufacturing and operational costs, enhance productivity and provide access to real-time information have been some of the key drivers for organizations to evolve towards utilizing modern networking systems to interconnect ICS with business and external networks. This new trend has reduced the isolation previously found in ICS networks, exposing the critical infrastructure to a wide array of external and internal threats as well as misconfigurations and computing errors.

Different organizations have different information security goals which are determined and driven by their business objectives. Generally speaking, information security organizations aim to protect the confidentiality, integrity and availability of critical information assets. In an ICS environment the availability of control systems, safety of human life and the integrity of the data that is processed is of paramount importance.

ICS have distinctive performance and reliability requirements. Their system lifecycle is usually 10 to 20 years and they are typically not built with security in mind. Most often than not, these systems are maintained by outside vendors, are not routinely patched or upgraded, and are deployed with default configuration settings. Because ICS

© 2015 The SANS Institute Author retains full rights.

need to be highly available at all times, it becomes extremely difficult to get authorization from the business to take these systems offline for security related maintenance. Given these challenges, it is important for organizations to develop and implement a security program for the protection of their critical infrastructure that follows a defense-in-depth strategy. Defense-in-depth defines the implementation of layered security controls to defend a system against different types of attacks. The goal is to reduce information risk while preserving the availability and integrity of ICS environments and, above all, to protect human life.

This paper establishes the fundamental concepts behind ICS using the Purdue Model for Control Hierarchy, mapping these logical concepts into a reference architecture for ICS. This reference architecture will be used as the basis for presenting the architectural patterns defined in four security domains deemed critical in ICS: access control, log management, network security, and remote access. This will allow information security professionals and process control engineers that are responsible for protecting an organization's most valuable assets to visualize how to protect against a security breach, whether involving confidentiality, integrity and/or availability.

2. ICS Security Architecture

This section introduces the logical architecture for an ICS network that will be used to identify the security controls and patterns. The Purdue Model for Control Hierarchy logical framework, developed by the International Society of Automation ISA-99 Committee for Manufacturing and Control Systems Security, forms the baseline for the ICS reference architecture presented in Figure 2.

2.1. Purdue Model for Control Hierarchy

The Purdue logical framework identifies five zones and six levels of operations as shown in Figure 1 (ISA99 Committee, 2004):

© 2015 The SANS Institute Author retains full rights.

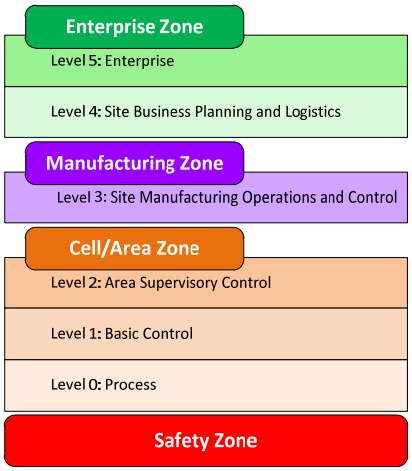

Figure 1 - Purdue Model for Control Hierarchy logical framework

The Purdue model uses the concept of zones to subdivide an Enterprise and ICS network into logical segments comprised of systems that perform similar functions or have similar requirements.

Enterprise Zone - Level 5: Enterprise

Level 5 is where corporate IT infrastructure systems and applications exist. Typically, VPN remote access and corporate Internet access services live in this level, to name a few. Direct communication between systems in the enterprise zones and the ICS environment is usually discouraged based on the level of risk that this would expose the organization to. A better approach is to manage access into the ICS environment through a Demilitarized Zone (DMZ) (Cisco and Rockwell Automation, 2011).

Enterprise Zone - Level 4: Site Business Planning and Logistics

Level 4, often seen as an extension of Level 5, houses IT systems that deal with reporting, scheduling, inventory management, capacity planning, operational and maintenance management, e-mail, phone and printing services. The services, systems and applications in Levels 4 and 5 are normally managed and operated by the IT organization (Cisco and Rockwell Automation, 2011).

Luciana Obregon, lucianaobregon@hotmail.com

© 2015 The SANS Institute Author retains full rights.

Manufacturing Zone - Level 3: Site Manufacturing Operations and Control

The systems in Level 3 are often responsible for managing control plant operations to produce the desired end product. Applications, services, and systems that are found at this level include:

- Plant historian
- Production reporting system
- Production scheduling systems
- Reliability assurance
- Engineering workstations
- Network File servers
- IT services such as DNS, DHCP, Active Directory, and NTP
- Remote access services
- Staging area

The systems and applications in Level 3 communicate with the systems in Enterprise Zone through a DMZ. Direct communication between systems in Manufacturing and Enterprise zones is discouraged. Additionally, systems in Level 3 may communicate with systems in Levels 1 and 0 (Cisco and Rockwell Automation, 2011).

Cell/Area Zone - Level 0: Process

Level 0 includes the sensors and instrumentation elements that directly connect to and control the manufacturing process. These devices are controlled by devices found in Level 1 (Cisco and Rockwell Automation, 2011).

Cell/Area Zone - Level 1: Basic Control

Level 1 includes process control equipment that receives input from sensors, processes the inputted data by using control algorithms, and sends the outputted data to a final element. Devices in this level are responsible for continuous, sequence, batch and

© 2015 The SANS Institute Author retains full rights.

discrete control. Some devices that exist in the level are Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), and Remote Terminal Units (RTU). These devices run vendor-specific operating systems and are programmed and configured from engineering workstations (Cisco and Rockwell Automation, 2011).

Cell/Area Zone - Level 2: Area Supervisory Control

Level 2 systems include the manufacturing operations equipment for an individual production area. Level 2 typically includes:

- Human Machine Interfaces (HMI)
- Alarms/Alert systems
- Control room workstations

These systems may communicate with systems in Level 1. Additionally, they may also interface with systems in the Manufacturing and Enterprise zones through the DMZ (Cisco and Rockwell Automation, 2011).

Safety Zone

Systems in the safety zone monitor processes for anomalies, automatically return processes to safety if they exceed a defined threshold and alert the operators of unsafe conditions. These systems are usually air-gapped from the rest of the control systems (Cisco and Rockwell Automation, 2011).

2.2. Practical Implementation of an ICS Network

Given the disparate security requirements of ICS and IT systems coupled with the criticality of control systems, a rigorous risk assessment should be conducted prior to interconnecting ICS and business networks. The majority of IT systems are concerned with achieving high performance and throughput while control systems focus on high availability and integrity of the data for continuity of operations. The ICS risk assessment should take into account industry best practices and regulatory standards that the

© 2015 The SANS Institute Author retains full rights.

organization must comply with. The risk assessment process should identify the threats and vulnerabilities that are most likely to impact the organization; it should assess the likelihood and business impact of those threats and recommend the implementation of security controls that will reduce the risk to a level that is acceptable to the organization.

If ICS and IT business networks must be connected, it is recommended that the number of entry points into the ICS environment be kept to a minimum. This will reduce the number of attack pathways that could lead an intruder into the ICS environment. Direct communication between IT business and ICS networks should be prohibited unless absolutely necessary for business operations.

Figure 2 illustrates an ICS reference architecture. The architecture uses the concept of zones to split the network into smaller, more focused environments where security controls can be consistently applied. A zone is a logical network segment within a networking environment that has a well-defined perimeter.

In the reference architecture, Level 5 is divided into an enterprise DMZ and an internal enterprise sub-zone. The enterprise DMZ is where systems that need to be directly exposed to the Internet live, such as VPN and e-mail gateways, Web and FTP/SFTP servers. The VPN gateway in the enterprise DMZ should be the only access point into the ICS environment for remote users. The internal enterprise sub-zone is where enterprise applications, business-to-business, and business-to-customer services live. For instance, if the organization has a business requirement to share records with a partner company, the server storing those records would exist in this sub-zone.

Systems containing ICS data that need to be accessed by systems or users in the enterprise network should be placed in a DMZ and the connections between the Enterprise network and the DMZ must be scrutinized by a stateful inspection firewall. Similarly, ICS systems that need to communicate with the enterprise network should do so through the DMZ. These connections must also be inspected by a stateful inspection firewall. The firewall should follow a “deny all” security policy, allowing only those connections that are authorized.

Luciana Obregon, lucianaobregon@hotmail.com

© 2015 The SANS Institute Author retains full rights.

As shown in Figure 2, pair of firewalls are used to create a DMZ between the Enterprise and ICS environments. The first firewall blocks inbound attacks destined to systems in the ICS network and inspects traffic into and out of the DMZ. The second firewall controls traffic into and out of the ICS environment and contains attacks originated inside the ICS network. The two-firewalled architecture increases the organization's security posture by adding additional layers of security that would need to be penetrated in order to compromise systems in the ICS environment. Security can be greatly increased by using firewalls from different manufacturers. These two firewalls would have different sets of vulnerabilities and in order for an attacker to tamper with both firewalls he/she would have to find and exploit a vulnerability that is common to both devices. Another benefit of implementing dual firewall architecture is separation of duties. One set of firewalls can be managed by the IT department while the process control group can be responsible for the other firewall.

Figure 2 includes two additional zones, a monitoring zone and a database zone. The purpose of the monitoring zone is to isolate systems that store and process security-related and system event data. Security-related events contain valuable information that an attacker could use to create a blueprint of the network to launch an attack. On the other hand, following an attack an intruder may want to cover their tracks and delete security-related events so that forensics investigation is unsuccessful.

The purpose of the database zone is to isolate database servers that contain sensitive records. Databases can store employee's username and passwords, trade secrets, personal identifiable information, human resources information, to name a few. Database servers should be isolated to their own zone protected by a stateful inspection firewall. The firewall should only allow access into the zone to those systems and users that have been authorized. Although Figure 2 only shows a database zone inside the Enterprise zone, the database servers in the ICS environment can be further isolated to their own database zone inside the Manufacturing zone. ICS databases can be high-value targets for attacks because they store command and control and historical data that are used for reporting and decision making.

Luciana Obregon, lucianaobregon@hotmail.com

© 2015 The SANS Institute Author retains full rights.

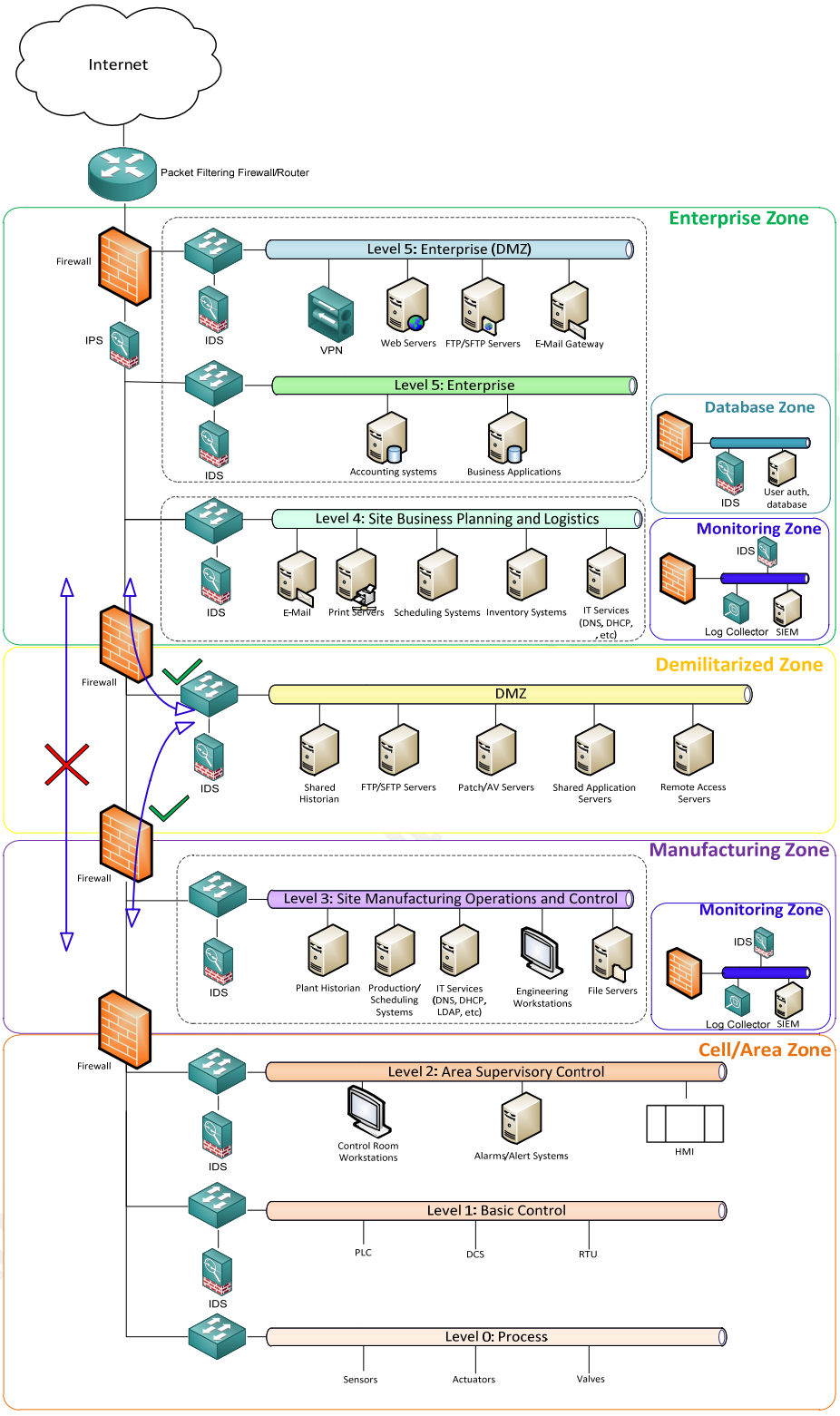

Figure 2 – Modified Purdue Model for Control Hierarchy architecture (NIST special publication 800-82.)

Luciana Obregon, lucianaobregon@hotmail.com

© 2015 The SANS Institute Author retains full rights.

2.3. Architecture Security Patterns for ICS

The Open Security Architecture defines security patterns as "a general reusable solution to a commonly occurring problem in creating and maintaining secure information systems" (Open Security Architecture, n.d.). This paper will identify security patterns in the following domains and explain how they apply ICS networks:

- Access Control
  - Access control mechanisms guarantee that the person who is attempting access to a system or application is who she/he says it is. Access control involves a user submitting a unique identifier, such as a user ID, and the corresponding authenticating information, such as a password.
- Network Security
  - Network security protects the confidentiality, integrity, and availability of information systems against internal and external threats using a variety of security controls.
- Log Management
  - Critical applications and systems should generate important security-related events to assist in identifying threats to information, troubleshooting network or system-related issues, and comply with regulatory requirements.
- Remote Access
  - Remote users and vendors seek access into the ICS environment for remote maintenance and support.

Note: The four domains listed above are not all-inclusive as it relates to ICS environments, but are those most commonly seen in these environments.

Luciana Obregon, lucianaobregon@hotmail.com

© 2015 The SANS Institute Author retains full rights.

2.3.1. Access Control

To prevent unauthorized access into the ICS environment users must be uniquely identified, authenticated, and authorized before gaining access. User authorization should follow the principle of least privilege which grants users with sufficient privileges to enable them to fulfill defined roles.

Users must be assigned a unique user ID and should use strong passwords enforced by a security policy that ensures that:

- Passwords are comprised of a minimum number of characters
- Passwords use a combination of alphanumeric and special characters
- Passwords are changed regularly
- Passwords do not contain dictionary words
- Password are not reused

Increased security can be achieved by using two-factor authentication mechanisms for all access into the ICS environment. Two-factor authentication prevents credential reuse and thwarts password guessing attacks. Two-factor authentication involves using two out of three possible factors to authenticate users:

- Something you know, such as a password, passphrase or PIN.
- Something you have, such as a token or digital certificate.
- Something you are, such as biometrics.
- Some place you are, such as country code.

Access privileges into the ICS environment should be subject to approval by senior management and should be reviewed on a regular basis. An automated way to revoke access into the ICS environment should exist in response to threats and vulnerabilities or information security incidents.

Luciana Obregon, lucianaobregon@hotmail.com

© 2015 The SANS Institute Author retains full rights.

Figure 3 identifies the security patterns for the access control information security domain. The yellow tags in Figure 3 represent the access control security patterns that can be consistently applied across the ICS network.

© 2015 SANS Institute, Author retains full rights.

Luciana Obregon, lucianaobregon@hotmail.com

© 2015 The SANS Institute Author retains full rights.

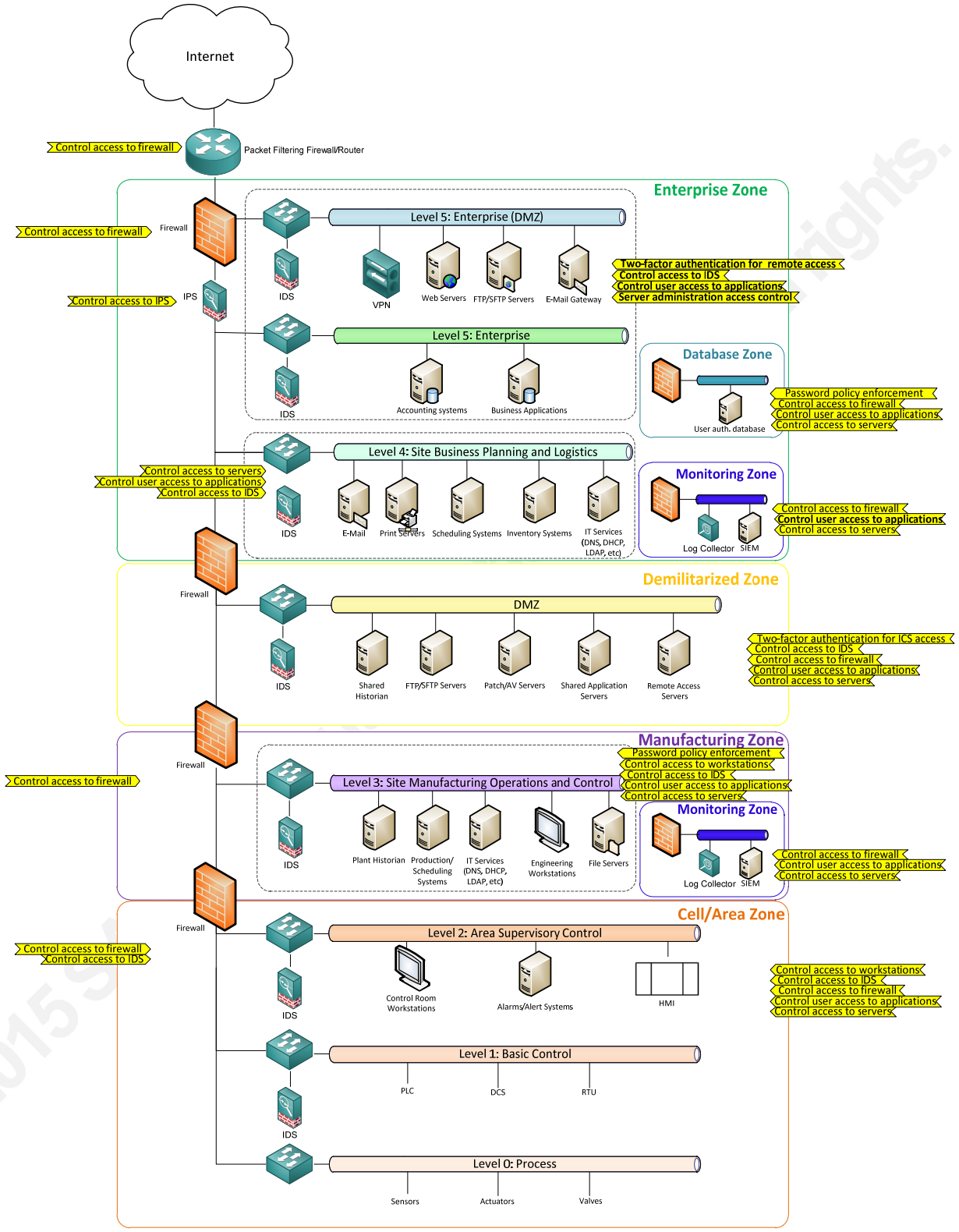

Figure 3 - Access Control Security Patterns for ICS

Luciana Obregon, lucianaobregon@hotmail.com

© 2015 The SANS Institute Author retains full rights.

2.3.2. Log Management

Most Enterprise and ICS systems and applications generate large volumes of events on a daily basis and should have mechanisms to forward security-related events to a centralized log collection server. The log collection server stores critical data, such as failed and successful login attempts, system boots and escalation of privileges that must be protected against unauthorized access and modification. The log collection server must be properly sized with enough space to store the event logs from all critical systems and applications for a stated retention period. The retention period must be documented in a policy and must take into consideration industry regulations.

Log messages should contain relevant system attributes such as IP addresses, ports and protocols used, day and time, username, method of access such as FTP, SSH, or HTTP. When correlating event logs from different systems time becomes an important factor. Systems and applications that generate event logs must use a consistent time source, such as a corporate Network Time Protocol (NTP), so that the event logs contain accurate time-stamps.

In the security architecture, depicted in Figure 2, the log collection server and SIEM tool are placed in their own zone named “Monitoring Zone”. There are two Monitoring Zones. The first is part of the enterprise zone and it receives and analyses security-related events from systems and applications inside the enterprise zone. The second is part of the manufacturing zone and it receives and analyzes security-related events from systems in the ICS environment. Both Monitoring Zones are firewalled. Only authorized source IP addresses are allowed to access this zone. Furthermore, access to the log collection server and SIEM tool requires a valid username and password.

At a minimum, network security hardware, such as VPN gateways, firewalls, intrusion prevention and detection systems, critical servers, such as domain controllers and database servers, and critical applications, such as historian applications should generate and forward security-related events to the corresponding log collection server in the zone

© 2015 The SANS Institute Author retains full rights.

for analysis. Figure 4 identifies the security patterns for the log management information security domain.

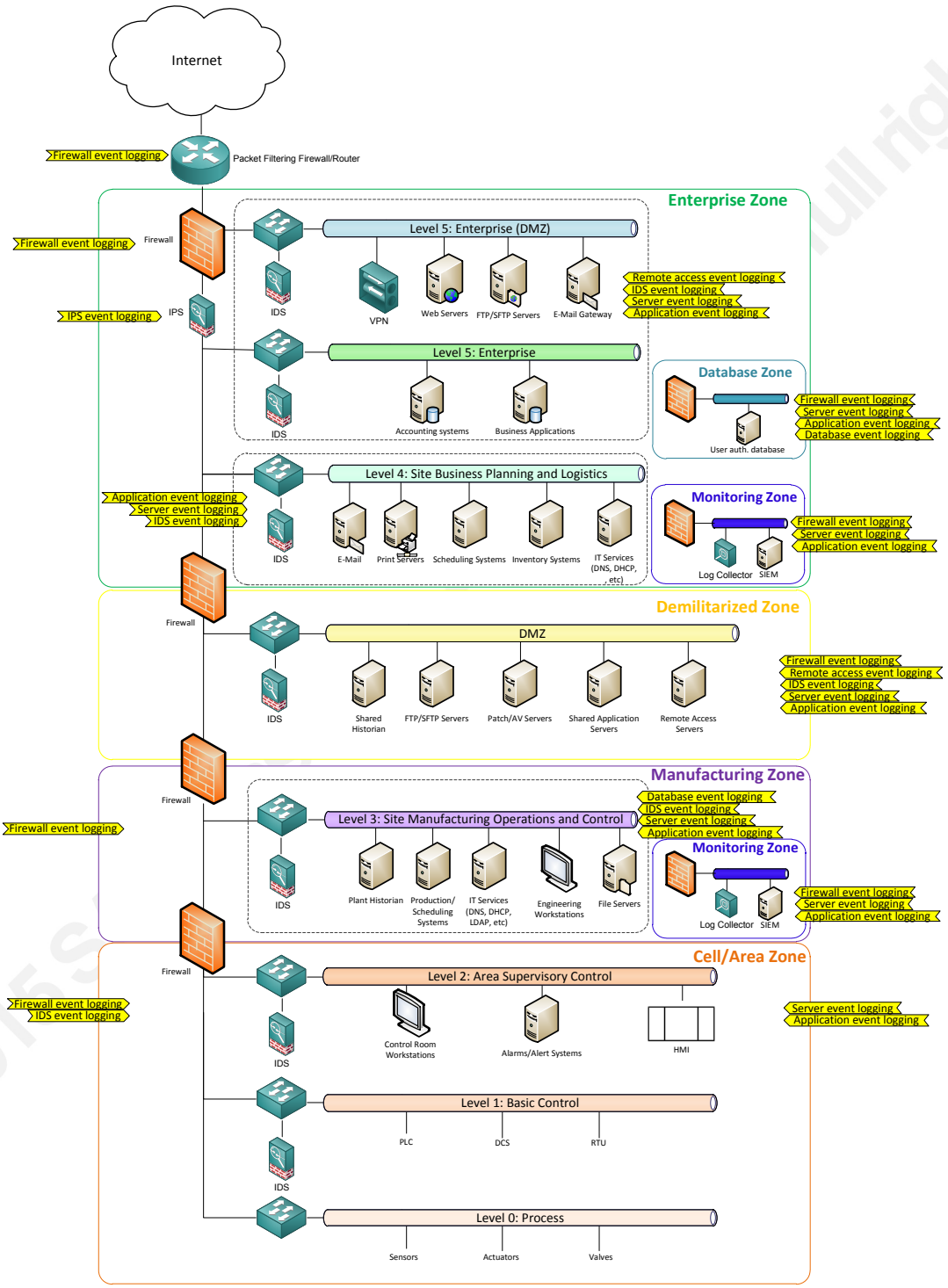

Figure 4 – Log Management Security Patterns for ICS

Luciana Obregon, lucianaobregon@hotmail.com

© 2015 The SANS Institute Author retains full rights.

2.3.3. Network Security

This section focuses on the following network security controls:

- Network Segmentation or Zoning
- Firewalls
- Network Intrusion Detection and Protection Systems

Network segmentation is typically achieved by placing a filtering device, such as a packet filtering or stateful inspection firewall at the zone's point of entry. A network zone should always have one entry point as depicted in Figure 5; all traffic entering and leaving the zone (also referred to as inter-zone traffic) should be subject to inspection by a firewall.

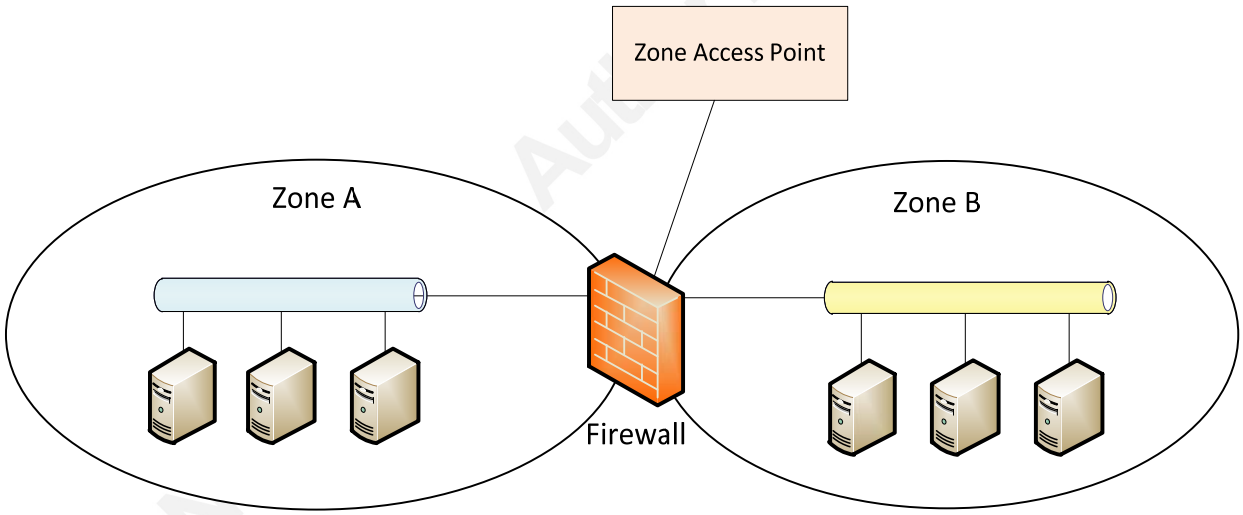

Figure 5 – Network segmentation or zoning

Systems can be segmented into network zones based on their functionality, criticality to the business, risk levels, or other requirements defined by the organization. Regardless of the segmentation scheme the systems within a given zone will be susceptible to common threats and vulnerabilities. It is therefore important for each zone to have a well-defined security baseline that is applied consistently across all systems within the zone. The security baseline will define the minimum level of protection required to achieve certain security level within the zone.

© 2015 The SANS Institute Author retains full rights.

The purpose of the firewall is to control traffic flow amongst network zones while preventing unauthorized network traffic from entering or leaving a particular zone. Firewalls should be configured to deny all traffic by default and explicitly allow those connections that are authorized to enter or leave a zone. There are many different types of firewalls, such as stateful inspection firewalls, application proxy firewalls and packet filtering firewalls.

In the reference architecture, depicted in Figure 2, stateful inspection firewalls are placed amongst the defined zones to ensure that:

- Authorized traffic is able to cross between zones
- Unauthorized traffic is denied, inbound and outbound
- Authorized traffic is directed to specific systems within a zone

Additionally, a packet filtering firewall is placed at the network perimeter between the Internet and the first border firewall. The purpose of this firewall is to stop the most basic type of attacks and filter out noisy protocols, such as inbound ICMP, syslog, and SNMP. Any traffic that gets past the perimeter packet filtering firewall will be further inspected by the stateful inspection firewall.

Application proxy firewalls can be placed at the perimeter behind the packet filtering firewall. These types of firewalls introduce latency that decreases network performance and are not widely used in ICS networks.

Additional layer of security can be achieved by requiring the firewall to authenticate users prior to accessing a zone. The firewall can be configured to forward authentication requests to an external user database and grant access into the zone if the user is authenticated.

Luciana Obregon, lucianaobregon@hotmail.com

© 2015 The SANS Institute Author retains full rights.

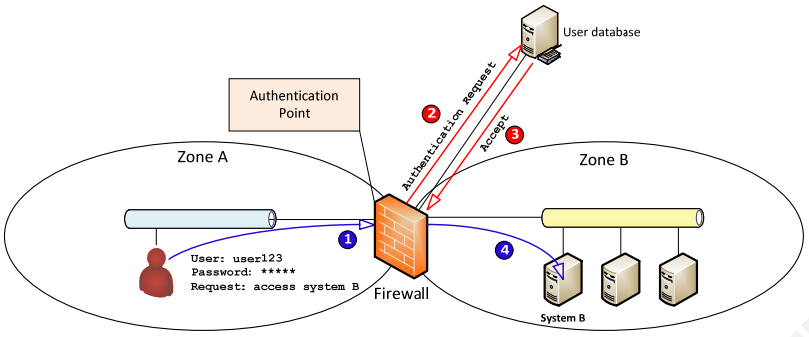

Figure 6 – Firewall acting as authenticator- Login successful

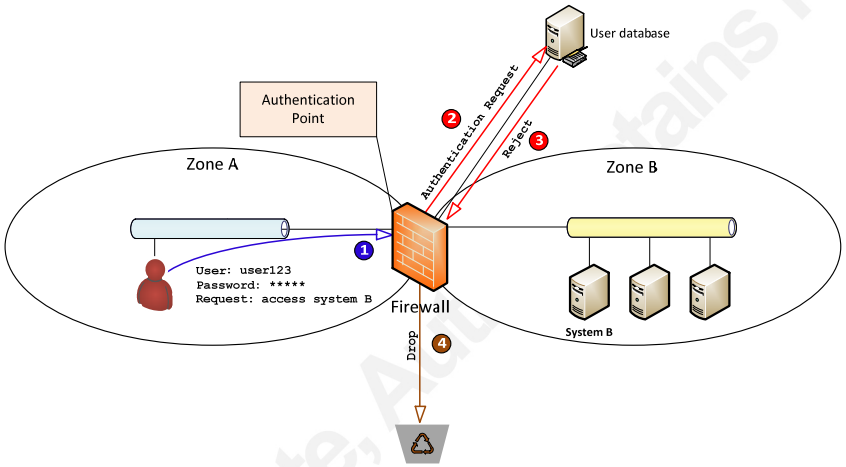

Figure 7 – Firewall acting as authenticator – Login failed

Intrusion detection and prevention sensors should be strategically deployed across the network and configured to detect those attacks that are most likely to succeed against systems in the environment. The biggest problem with intrusion detection systems are false positive alerts. When legitimate network traffic is identified as malicious or anomalous a false positive alert is triggered. If an IDS is not tuned for the environment in which it is installed it can generate hundreds of false positives and irrelevant alerts. This can easily overwhelm the security analyst causing him/her to miss the real attacks.

In the reference architecture, depicted in Figure 2, IDSs are placed inside each zone. The IDS detects inter-zone attacks (attacks amongst different zones) and intra-zone attacks (attacks amongst systems within a zone). The zone IDS should be deployed as a focused sensor; its signature set should be configure so that it only detects those attacks

© 2015 The SANS Institute Author retains full rights.

that are relevant to the systems that are being monitored. For instance, if only Windows systems are being monitored it would only be necessary to enable Windows-based attacks.

In the architecture, depicted in Figure 2, an IPS is placed at the network perimeter. The job of this IPS is to filter out any inbound malicious traffic that may have gotten past the perimeter firewall. Additionally, this IPS detects malicious outbound traffic such as C&C, and it can block outbound traffic from unauthorized applications, such as P2P and anonymous proxy applications.

Figure 9 identifies the security patterns for the network security information security domain.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

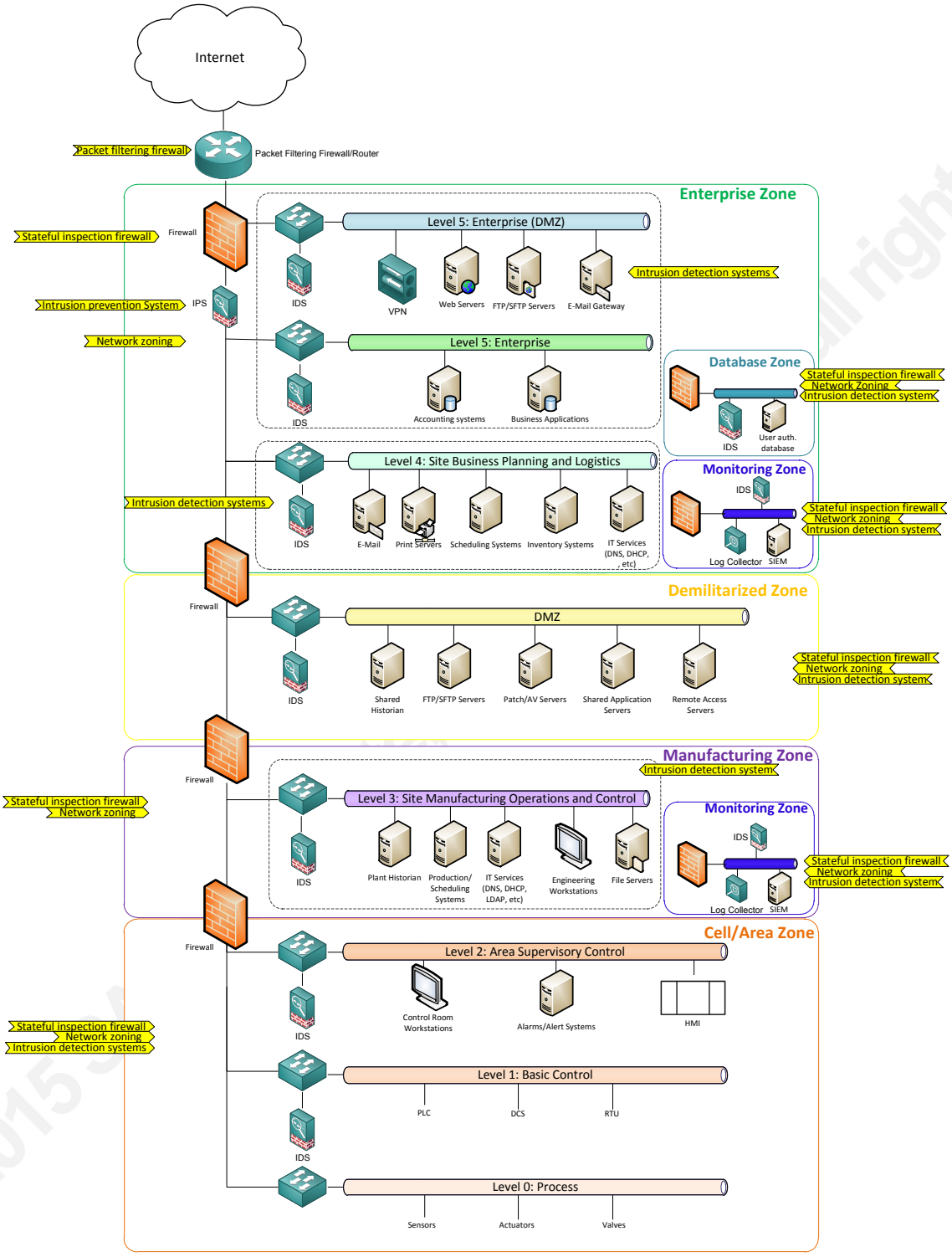

Figure 9 – Network Security Patterns for ICS

Luciana Obregon, lucianaobregon@hotmail.com

© 2015 The SANS Institute Author retains full rights.

2.3.4. Remote Access

Access to the ICS environment should control by two-factor authentication mechanisms. In the reference architecture, depicted in Figure 2, a VPN gateway is placed in the Enterprise zone DMZ. Users attempting to gain access to the organization's network will first be required to establish an encrypted VPN tunnel to the organization's VPN gateway. The VPN gateway will authenticate the user by requiring a valid username and password combination as well as a second form of authentication, usually a one-time password (OTP) generated by a token device. The VPN gateway will act as the authenticator forwarding the authentication requests to an external user database. If the authentication is successful the user will be authorized to access a remote access server in the DMZ between the enterprise and manufacturing zones. Authorization should follow the principle of "least privilege."

To gain further access into the ICS environment the user will be required to connect to a remote access server located in the DMZ. The connection between the user and the remote access server should be encrypted to prevent sending sensitive data in clear-text. The user will then be required to provide a valid username and password as well as a second form of authentication. If the user is successfully authenticated he/she should only be authorized to access those systems in the ICS environment that are required to perform a specific job function.

Figure 10 identifies the security patterns for the remote access information security domain.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

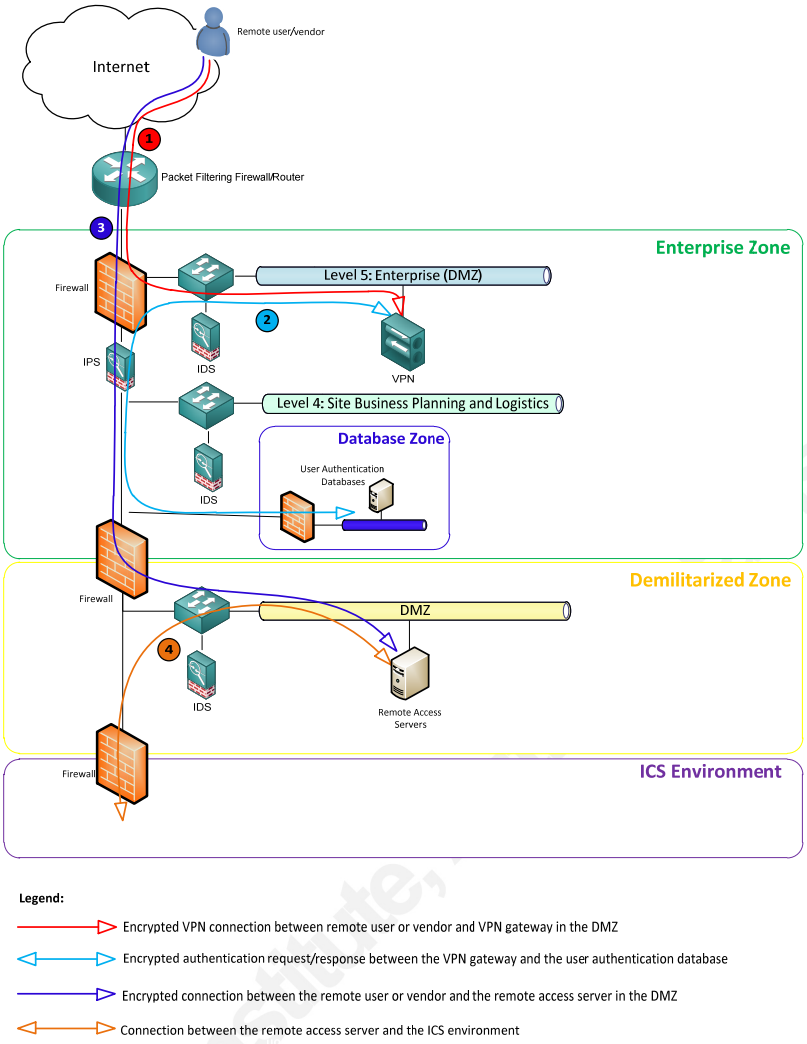

Figure 10 – Remote Access Security Patterns for ICS

3. Conclusion

This paper presents an overview of ICS and the components that make up an ICS environment. This overview is not meant to be all encompassing; it is meant to provide the reader with the necessary basic foundation and enough context to understand the sections which follow.

The Purdue Model for Control Hierarchy is briefly discussed and defined as a logical framework that organizations can use to understand how to build a secure ICS environment. We present a reference architecture built using the Purdue Model as a

© 2015 The SANS Institute Author retains full rights.

baseline, and modify it to include additional security zones and controls to show the reader how to reduce common risks that organizations face.

Security patters are identified in four core information security domains: access control, log management, network security and remote access. While there are many more information security domains, such as host security, vulnerability management and wireless security that apply to ICS environments, deploying appropriate security measures around these four domains can greatly reduce an organization's attack surface while increasing its security posture.

It is important to point out that a rigorous risk assessment should be performed prior to making architectural changes or introducing new systems into the environment that could potentially negatively affect an organization's security posture. The risk assessment should identify the potential risks that interconnecting ICS and enterprise networks can present to an organization.

Finally, information security requirements and controls should not negatively affect the company's ability to operate. Information security goals should always align to the company's strategic priorities and should create business value by protecting confidentiality, integrity and availability of the company's most critical assets and as a result, reduce the overall risk exposure.

© 2015 SANS Institute, Author retains full rights.

Luciana Obregon, lucianaobregon@hotmail.com

© 2015 The SANS Institute Author retains full rights.

4. References

Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG-22). Retrieved from https://www.cse-cst.gc.ca

Boyer, S. A. (2004). *SCADA: Supervisory control and data acquisition*. Research Triangle Park, NC: ISA-The Instrumentation, Systems, and Automation Society.

Cisco and Rockwell Automation (2011). Converged Plantwide Ethernet (CPwE) Design and Implementation Guide. Cisco Systems, Inc. (n.d.). Retrieved from http://www.cisco.com/

Homeland Security (2009). Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

Information Security Forum (2014). The Standard of Good Practice for Information Security. Retrieved from http://isflive.org

ISA99 Committee (2004). Manufacturing and Control Systems Security Part 1: Models and Terminology. Retrieved from http://isa99.isa.org/

Krutz, R. L. (2006). *Securing SCADA systems*. Indianapolis, IN: Wiley Pub.

NIST (2014). NIST Cybersecurity Framework Core: Informative Reference Standards. ISA 62443-3-3:2-13.

Open Security Architecture. (n.d.). Retrieved from http://www.opensecurityarchitecture.org/

Shaw, W. T. (2006). *Cybersecurity for SCADA systems*. Tulsa, OK: PennWell Corp.

Stouffer, K., Falco, J., & Kent, K. (2006). Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security.

Luciana Obregon, lucianaobregon@hotmail.com

© 2015 The SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to and Industrial Control Systems Security (ICS) Security. NIST special publication 800-82.

© 2015 SANS Institute, Author retains full rights.

Luciana Obregon, lucianaobregon@hotmail.com

© 2015 The SANS Institute Author retains full rights.