American Journal of Artificial Intelligence
2019; 3(2): 17-22
http://www.sciencepublishinggroup.com/j/ajai
doi: 10.11648/j.ajai.20190302.11
ISSN: 2639-9717 (Print); ISSN: 2639-9733 (Online)

Implementation of Defense in Depth Strategy to Secure Industrial Control System in Critical Infrastructures

Tschroub Abdelghani

Direction of Telecommunications, Sonelgaz, Algiers, Algeria

Email address:
tschroub.abdelghani@grte.dz, tschroub.abdelghani@gmail.com

To cite this article:
Tschroub Abdelghani. Implementation of Defense in Depth Strategy to Secure Industrial Control System in Critical Infrastructures. *American Journal of Artificial Intelligence.* Vol. 3, No. 2, 2019, pp. 17-22. doi: 10.11648/j.ajai.20190302.11

Received: November 18, 2019; **Accepted**: December 13, 2019; **Published**: January 16, 2020

Abstract: The goal of this communication is to examine the implementation of defense in depth strategy to secure the industrial control systems (ICS) from threats, hackers, vandals and other ones that can damage the critical infrastructures (gas transportation network, power transmission network, power generation, power distribution grids, air traffic, petrochemical industries, rail traffic, military industries) and others big infrastructures that affect large number of persons and security of nations [1]. The defense in depth concept ensures the physical access protection of the infrastructure, using network access control system (NAC) and traditional security measures, and implements policies and procedures that deal training and cybersecurity awareness programs, risk assessment (analyzing and documenting), and the plan of security. The philosophy of defense in depth uses also the IT technologies in order to ensure separation and segmentations of the networks to the VLANs, demilitarized zones, VPN, using firewalls, switch and routers. The hardening of different systems installed like routers, firewalls, switches and other devices on the network such as SCADA servers is a very sensitive operation of defense in depth. The last important operations are monitoring and maintenance, the monitoring serve to detect and stop intrusions attempts before they can damage the control system with using detection and protection system (IDS/IPS), and the maintenance operations control system (soft and hard), schedule updating of anti-virus software on different devices installed in the network like (computers, SCADA servers, routers, switch and other devices). The defense-in-depth recommendations described in this document can decrease the risk of attacks can target industrial network architectures, like VLAN hopping, SQL injection on SCADA, IP spoofing and DoS (denies of service) and others ones. The risk of attacks can use a common point of access as point of failures (RTU, corporate VPNs, database links, wireless communication, and IT controlled communication equipment). The implementation strict of the defense in depth concept can avoid important damage of critical infrastructures such as loss of production, damage to plant, impact on reputation, impact of health, impact of safety, impact of environment and impact on nation's security.

Keywords: ICS, SCADA, Cybersecurity, IDS, IPS, Defense in Depth, Demilitarized Zones (DMZ), Firewall, Next Generation Firewall

1. Introduction

Industrial control systems (ICS) are an integral part of critical infrastructures, helping to facilitate operations in vital industries. The growing issue of cybersecurity and its impact on ICS highlights fundamental risks to the Nation's critical infrastructure. [1]

Efficiently addressing ICS cybersecurity issues requires a clear understanding of the current security challenges and specific defensive countermeasures. SCADA, PLC, IED, RTU, HMI, DSC fall into categories of ICS [5, 13]. In this situation, only technical solutions are not capable to ensure the entirely security of industrial infrastructure, but it need a large concept like defense in depth strategy. This philosophy is adopted and implemented by the different developed countries, and the manufacturers (multinational companies) of different equipments like routers, firewalls, IDS/IPS, switch, servers, software. To look at the important of defense in depth strategy, we can imagine the huge blackout in Venezuela in March 2019, more than a week after a power grid cyber attacks. On 2014 at Ataturk airport, an attacker was shut down the passport control system using malware, passenger stood in line four hours and plane departure were delayed. On 2015, the Russian cyber attack on Ukrainian grid, cut power to the 225 000 customers.

2. Defense in Depth Strategy

Defense in depth is a concept developed by the US National security agency that target high level security of nation's critical infrastructures. This approach is an information assurance concept in which multiple layers target the high level security controls, which are placed throughout an information technology (IT) system. It is also known as the (castle approach). [7, 16]

Its intent is to provide redundancy in the event a security control fails or vulnerability is exploited. [6]

The idea behind the defense-in-depth strategy is to defend a system installed in the industrial infrastructure against any particular attack using several independent methods. It is a layering tactic, as a comprehensive approach to information and electronic security that ensure multi-layer high-level protection to avoid damage of industrial infrastructures, each layer protects the other layers and the attacker must spend more time and effort at each transition. [1-3]

Defense in depth strategy is based on technology, people and processes, and the different axes dialed by the defense in depth are:

i. Policies and procedures and awareness.
ii. Physical.
iii. Network.
iv. Computer.
v. Applications.
vi. Devices. [3]

The different norms those deal cybersecurity of critical infrastructures are: NIST 800-53, IEEE P 1686, NERC CIP, ISO 27K, IEC 62443, CIGRE D2.22 and ISA 99 [4, 15].

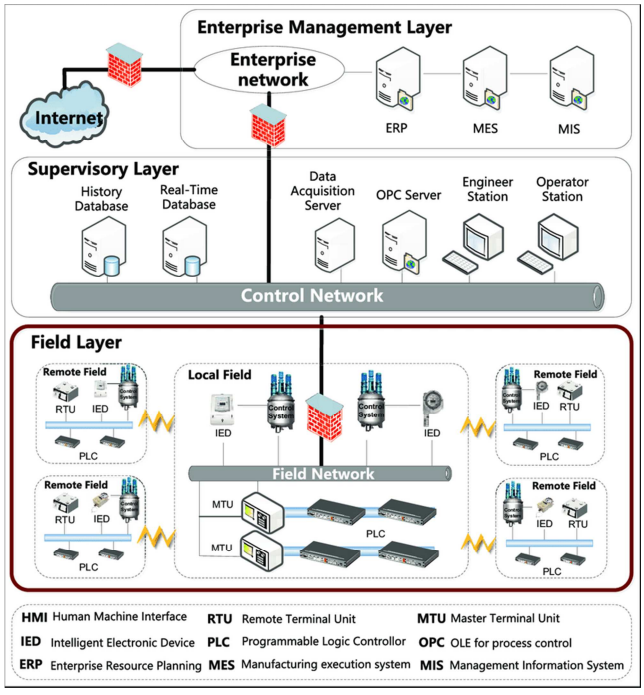

Figure 1. *Recommended Defense-In-Depth architecture [2].*

The security of control must ensure availability, integrity and confidentiality;

1) Availability; increase plant availability through prevention or reduction of faults caused by attacks or malware.
2) Integrity; protection of system and data integrity to avoid malfunctions, production errors and downtimes.
3) Confidentiality; protection of confidential data and information as well as intellectual property. [6, 16]

The goal of defense in depth is to ensure the protection of process network from the following risks:

1) Backdoors and holes in network perimeter.
2) Vulnerabilities in common protocols.
3) Attacks on field devices.
4) Data base attacks.
5) Communications hijacking and (man in the middle) attacks. [3]
6) Spoofing attacks.
7) Attacks on privileged and/or shared accounts. [7]

The defense in depth can also ensure a defense against advanced persistence threats (APT), that provide a new challenge for the administrator because APT has the ability to adapt at zero day vulnerabilities into an attack.

The basic components of defense in depth concept are:

2.1. Physical Access Protection

To control physical access, traditional security measures must also be used like perimeter defenses (fences, locked gates and doors, CCTV, etc) and logical access to the system using firewalls, authentication and authorization, VPNs, anti-virus software and intrusion detection/prevention systems.

The different computers must be checked, configured and protected from malwares before their integration to the industrial control networks. This operation must be manually and automatically by using network access control (NAC) to perform their security.

A NAC can control access to a network by applying a set of rules to a device when it first attempts to access the network. These rules typically regulate anti-virus protection level, applications, operating system patch levels, and configuration.

NAC systems may also integrate the automatic remediation process (fixing non-compliant computers before allowing access) into the network systems before communication is allowed.

NAC systems control access to a network with policies, including pre-admission end point security policy checks and post-admission controls over where users and devices can go on a network and what they can do. [3]

2.2. Policies and Procedures

A comprehensive set of policies and procedures which covers all aspects of cyber security such as:

1) Training and cybersecurity awareness programs, both employees and subcontractors are concerned by this operation.
2) Risk assessment (analyzing and documenting), a systematic security analysis that include:

a. Identify and document all potential threats.
b. Prioritize these threats; severity, business impact, and safety criteria.
c. Processing order.
d. Possible threats examinations, internal sources (disgruntled employees and contractors) and external sources (hackers and vandals).

3) Security plan is a set of rules detailed in the next points:
a. Roles and responsibilities.
b. Actions, activities, and processes.
c. Consequences of non compliance.
d. Incident response policies and procedures.
e. Details the equipment, software, protocols, procedures, and personnel.
f. Security plan; team representing management, IT staff, control engineering, operation, and security experts.
g. Security plan; changes in threats, environment, and adequate security level. [3]

2.3. Network Segmentation and Separation (Security Cells)

This part uses physical separations using of firewalls demilitarized zone (DMZ) and segmentation using VLAN and others like firewalls, switch and routers.

2.3.1. Physical Separation

To separate control network from other networks, a concept of demilitarized zone (DMZ) must be used, and the division of the control network itself into functional zones connected by secure conduits using different devices like Ethernet switch, router and firewall.

A firewall demilitarized zone separates the industrial control networks from the enterprise (administrative area) and other external communication paths. Demilitarized zone provides a security layer to protect the control room's operations network and the deeper control and device networks.

Demilitarized zone (DMZ) area can contain:
i. Data servers such as historian.
ii. Patch management servers.
iii. Proxy servers for web-connectivity or other protocols.
iv. RADIUS and VPN servers and others servers. [3]

2.3.2. Network Segmentations

Can be established by using devices like managed Ethernet switches, which provide virtual LAN and access control list (ACL) management capabilities. Segmentation facilitates the establishment of security zones for several goals mentioned below. [3]

Different factors influence the method that how the zone will be organized. The zone organization must take in considerations; function, location, and security requirements according to IEC 62443. For instance, a zone contains network segments and devices.

Network segmentation and the establishment of security zones must be implemented in order to:
i. Limit malware infections to one network segment.
ii. Improve security by limiting node visibility.
iii. Stop intruder scans at the network level before they reach a potential target system.
iv. Limit the impact of a security breach.
v. Restrict broadcasts and multicasts to particular VLANs.
vi. Improve network performance and reduce network congestion.
vii. Control communication access between segments providing critical devices or systems get a higher level of security. [3]

2.3.3. Firewall and VPN

1) *Firewall*

Firewalls protect the networks by denying unauthorized access and allowing authorized access (ex: using ACL). A firewall is a device or set of devices configured to permit, deny, drop, encrypt, decrypt, or proxy traffic between different security zones based upon a set of rules and other criteria according to security policy.

Additionally, firewalls can support event logging to a syslog server or to an internal event log. Event logging is used to monitor security events and alarms that occur on an industrial network and can be used to identify network threats that target different systems.

Typical events that can be monitored are:
i. Firewall interface up/down.
ii. Attempted log-in to firewall.
iii. Packets matching firewall rule allow or deny.
iv. Denied packets that do not match a rule.
v. Power failure or power recovery. [3, 6]

2) *Stateful Inspection Firewalls*

Is the most recommended in the ICS security because it combines features of all of the other firewall types (Application-Proxy gateway firewall, deep packet inspection firewall, and host firewall). The different operations that can be ensured by the stateful inspection firewalls are:
i. Filtering packets at the network layer and validate that the session packets and their contents at the application layer are legitimate.
ii. Keeping track of the network connections (such as TCP and UDP connections).
iii. Allowing packets that match known good connections and rejects those that do not match.
iv. Checking that inbound packets are the result of an outbound request.
v. Providing a high level of security, good performance and require less configuration effort.

The Next generation firewall (NGFW) includes IDS/IPS functionality that combining a traditional firewall with other network device filtering functionalities:
i. Deep packet inspection (DPI).
ii. Intrusion detection and prevention system (IDS/IPS). [4]

3) *VPN*

VPN ensure security using both encryption and authentication, in order to protect the data as it moves over the public internet. A VPN client uses the internet to create a virtual point-to-point connection with a remote VPN server.

VPN used both SSL and IPsec.

IPsec is a suite of standards for performing encryption, authentication, and secure tunnel setup. IPsec essentially creates private end-to-end tunnels out of the public bandwidth available on the Internet. IPsec uses internet key exchange (IKEv2) or authentication header (AH) or encapsulating security payload (ESP).

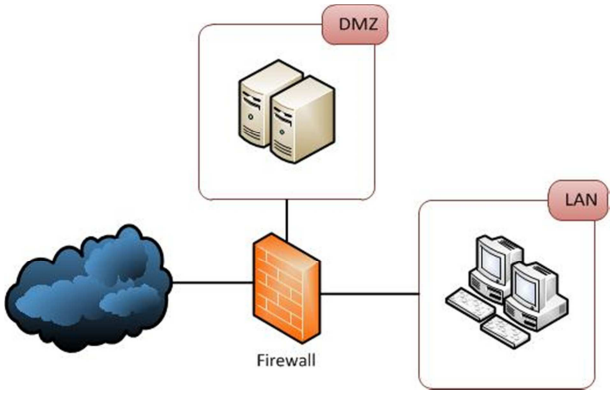

Figure 2. *Implementation of firewall and DMZ zone. [2]*

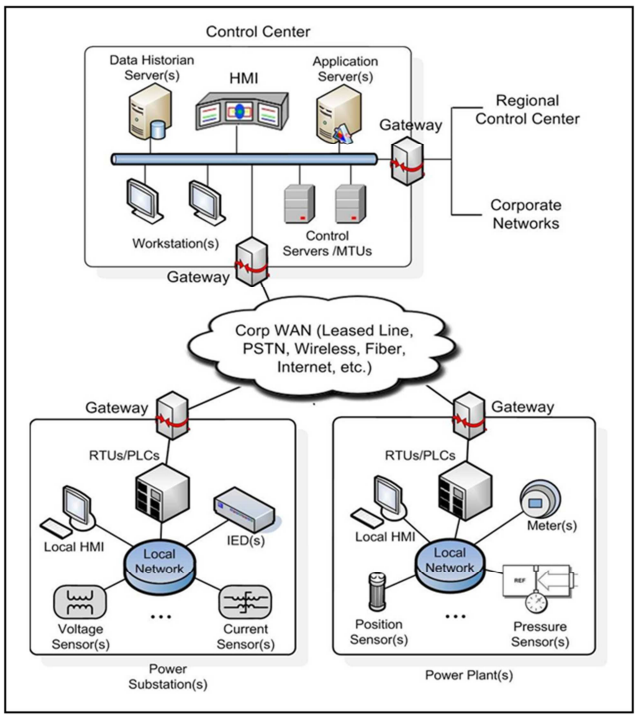

Figure 3. *Implementation of VPN and IPsec. [2]*

2.4. System Hardening

Device hardening applies to routers, firewalls, switches and other devices on the network such as SCADA servers. The different device hardening operations include:

1) Password management including encryption.
2) Disabling of unused services.
3) Access control.
4) Patches, hot fixes, application updates.
5) Strong authentication. [3]

2.4.1. Authentication and Use Administration

The external authentication and authorization to the control system ensured by RADIUS server, providing secure access with remote access services and VPN.

2.4.2. Patch Management

In order to minimize or avoid vulnerability to attacks that can target industrial infrastructures, the different systems should be patched to the latest vendor-recommended software and firmware levels. This is particularly true with the different computer systems, such as SCADA hosts, servers etc.

Patch management and deployment methods can be automatic, semi-automatic, and manual. It should be systematically planned, tested, and executed. [3]

Patch management protects different systems against zero day vulnerabilities.

2.5. Monitoring and Maintenance

2.5.1. Monitoring

The monitoring operation detects and stops intrusions attempts before they can damage the control system. The monitoring operation includes:

1) Routine examination of log files.
2) SNMP authentication traps.
3) Network load monitoring.
4) Use of an intrusion detection and protection system (IDS/IPS). [2, 6]

An intrusion detection and protection system (IDS/IPS) monitors activity on the network for malicious traffic using different analysis like (penetration test), and logs and reports traffic anomalies to detect failures (like breaches in the network, or intruders) and secure immediately the systems. An IDS/IPS monitors:

1) Traffic patterns.
2) File access.
3) Changes in port status.
4) Invalid password entries.
5) Inoperable equipment.

There are two types of IDS/IPS:

1) Network intrusion detection and protection system (NIDS/NIPS); monitors the traffic by analyzing individual packets for malicious traffic. NIDS/NIPS are often located at demilitarized zones or network boundaries. The latest technology uses:
   i. Pattern or signature based.
   ii. Protocol anomaly detection.
   iii. Behavior based rules (learning mode).

Passive scanning of network traffic applied by NIDS/NIPS brings additional functionality:

i. Network monitoring and supervision of all devices.
ii. Collection of asset inventory information.
iii. Aggregation of security event logging information.
iv. Vulnerability assessment.
v. Threat and anomaly detection. [3]

Host intrusion detection and protection system (HIDS/HIPS); is an agent that runs on an individual host or device on the network and monitors traffic in and out of the

host or device. It analyzes:

i. System calls.
ii. Applications logs.
iii. File system modifications. [3]

There are other host activities and states to identify intrusions.

2) The Next generation firewall (NGFW) includes IDS/IPS functionality that combining a traditional firewall with other network device filtering functionalities, such as:
   i. Deep packet inspection (DPI).
   ii. Intrusion detection and prevention system (IDS/IPS). [4]

The techniques of penetration test used by IDS/IPS for IT systems are not the same for OT systems, because there are risks of crashing the systems. To avoid the damage into systems, IPS must be used with extreme care with control systems! [4, 9, 11]

2.5.2. Maintenance

Permanent maintenance of the control system includes the routine operations, scheduled updating of anti-virus software with the latest signatures and installing the latest patches for software and firmware used on different devices installed in the network like (computers, SCADA servers, routers, switch and other devices).

A periodic assessment and test of the control system network for security risks should be performed. Check that device configurations are appropriate with security in mind. Use the latest security standards and practices and update as needed. [3]

3. Methods of Attack

The defense-in-depth recommendations can decrease the risk of following attacks:

i. VLAN hopping.
ii. SQL injection on SCADA.
iii. IP Spoofing.
iv. DoS.

The common methods of attacks (VLAN hopping) are:

i. MAC flooding attack.
ii. 802.1Q and ISL tagging attack.
iii. Double-Encapsulated 802.1Q/nested VLAN attack.
iv. ARP attacks.
v. Private VLAN attack.
vi. Multicast brute force attack.
vii. Spanning-tree attack.
viii. Random frame stress attack.

DOS attack includes:

i. TCP SYN flood attack.
ii. Land attack.
iii. ARP spoofing.
iv. ICMP smurf attack.
v. Ping of death.
vi. UDP flood attack.
vii. Tear drop attack. [3, 8]

There are others kind of attacks that can damage infrastructures.

4. Common Points of Access

Defense in depth concept takes care of the different points of access that an attacker can take this point or failure to access and damage the infrastructure. The different points of access are:

i. RTU.
ii. Corporate VPNs.
iii. Database links.
iv. Wireless communication.
v. IT controlled communication equipment. [3]

A network can be penetrated directly, indirectly, social engineering, known vulnerabilities or zero day vulnerabilities.

The most dangerous vulnerabilities are internal ones. One the attacker can penetrate to the process network; he can control the process, export HMI screen and change DATA base.

The GPS receptor is also a common point of access and a GPS spoofing attack and jamming can cause a very big damage to industrial infrastructures, but to deal the risks and security solutions of GPS it need another concept different of defense in depth approach. [10, 14]

5. The Consequences of Industrial Cyber Attack

The implementation strict of the defense in depth concept can avoid important damage of critical infrastructures like:

i. Loss of production.
ii. Damage to plant.
iii. Impact on reputation.
iv. Impacts of health.
v. Impacts of safety.
vi. Impacts of environment.
vii. Impacts on nation's security. [12]

6. Conclusion

This paper presents knowledge, which has been given for defense in depth security for ICS and their importance. Some details are given to ensure security and avoid different risks that infect systems and destroy the industrial infrastructure. Furthermore, a different type of attacks is given and the differences points of access. At the end of this communication, when we look at the evolution of nations in the domain of ICS security, we imagine the huge responsibilities of the governments and the different industrial companies to lift the challenge and plan the strategies to ensure an ideal security of their critical infrastructures. [1]

References

[1] TSCHROUB Abdelghani. Industrial control system (ICS) security in power transmission network. February 2019, Algerian Large Electrical Network Conference (CAGRE). IEEE conferences.

[2] Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams Adam Hahn. Guide to Industrial Control Systems (ICS) Security. Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC). NIST Special Publication 800-82 Revision 2. National Institute of Standards and Technology. U.S. Department of Commerce. May 2015.

[3] Cybersecurity Good Practices Guide HA032968 Issue 1 July 2017. Schneider electric. www.eurotherm.nl.

[4] Dylan Jenkins. Grid Automation Cyber Security. September 2019. ABB.

[5] Handbook for Self-Assessing Security Vulnerabilities & Risks of Industrial Control Systems on DoD Installations. December 2012. USA Departement of defence. www.wbdg.org.

[6] Homeland Security. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. Industrial Control Systems Cyber Emergency Response Team. September 2016. www.iiconsortium.org.

[7] NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses. The INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance. May 2010. www.fas.org.

[8] Matus Korman Industrial information and control systems, KTH. Cyber Security in Power Systems. 2016. www.kth.se.

[9] Rafay Baloch. Ethical hacking and penetration testing guide.

[10] Jason Allnutt, Dhananjay Anand, Douglas Arnold, Allen Goldstein, Ya-Shian Li-Baboud, Aaron Martin, Cuong Nguyen, Robert Noseworthy, Ravi Subramaniam, Marc Weiss. Timing Challenges in the Smart Grid.

[11] Richard Candell, Timothy Zimmerman, Keith Stouffer, An Industrial Control System Cybersecurity Performance Testbed, http://dx.doi.org/10.6028/NIST.IR.8089.november 2015.

[12] Dr EDWARD. G AMOROSO. 2017 Tag cyber security annual. Volume 1. Practical Handbook and reference guide for the working cyber security professional. Version 1.0 September 2016. attivonetworks.com.

[13] Arthur Gervais. Security Analysis of Industrial Control Systems. Master's Thesis Espoo, June 29, 2012. KTH Stockholm and Aalto University.

[14] Der-Yeuan Yuy, Aanjhan Ranganathany, Thomas Locherz, Srdjan Capkuny, David Basin. Short Paper: Detection of GPS Spoofing Attacks in Power Grids.

[15] Teodor Sommestad, Göran N. Ericsson. SCADA System Cyber Security – A Comparison of Standards.

[16] TALBANI Rachid. Industrial Security the essential basics for industrial automation. Siemens.