e-ISJN: A4372-3114
p-ISJN: A4372-3115

ISSN: 2321-7782 (Online)
ISSN: 2347-1778 (Print)
Impact Factor: 7.52

Volume 8, Issue 8, August 2020

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

A Conceptual Model for the Implementation of Cyber Security Measures in a Process Control Network Environment

Joseph Dube[1]
Department of Process Control
Afrox, Member of Linde Group
Johannesburg, South Africa.

Barend W Botha[2]
Department of Mechanical Engineering
University of Johannesburg
Johannesburg, South Africa.

Abstract: ***This paper presents a hybrid framework for the implementation of cybersecurity measures in the process control network for manufacturing plants across industries. While the objective of the framework is the preservation of data confidentiality, integrity, and operational availability of critical infrastructure systems, it seeks to adopt the defense-in-depth strategy approach as an efficient and secure cybersecurity tool. As studies have shown that the threat posed by cybersecurity in key infrastructure systems has the potential to shutdown these installations with catastrophic consequences. Lives could be lost, and equipment destroyed. Accordingly, the paper explores the islanding of the process control network to limit any unauthorized access and also, examines a battery of network security measures and the activities to be applied to the process control infrastructure hosted in the corporate and process control networks. Effectively securing the devices in the process network ensures continued productivity. As such, only tested and certified security measures must be deployed in unison.***

Keywords: Process control network, cybersecurity measures, confidentiality, integrity, availability, defense-in-depth.

I. INTRODUCTION

The fourth industrial revolution (FIR) brought about system connectedness in industries, however, it inevitably created cybersecurity vulnerabilities [1] which threaten automation and control system operational availability, plant integrity, confidentiality [2], [3] from unauthorized access, and create security risks [4]. History is awash [5] with such cyber-attacks. Stuxnet, Flame [6], and a host of other worms and Trojans caused extensive damage to the production plants in the recent past. Subsequently, the Cyber-Physical System (CPS) attacks climaxed with the Stuxnet-virus attack in 2010 which targeted the physical control systems, and the scale of destruction could have been catastrophic, had it not been detected. A year later in 2011, the Duqu attack [4] focused on data theft, a threat that has the potentially to shut down key utility services like energy, water, and refineries [7]. According to Saydjari [8], cybersecurity risks have become a reality with an increased "frequency, severity, and sophistication" to the production environment

Arguably, the solution to the cyber-attacks lies with the segregation of the plant and corporate networks. The islanding of the networks makes the process control network “unreachable”, thus providing organizations with relief from cyber-attacks.

Conceptually, the framework is an enhanced security model whose envisaged measures are based on a multi-layered security system built on the "defense in depth principle" [9]. The defense-in-depth principle is premised on the attacker being able to successfully get through the layers of defense to access the physical assets, but the security layering built in the systems create honeypots [7] and delays the extent of the damage. The multi-layering has three core areas namely:

1. The physical security
2. Network security

3. System integrity

According to Anton [6], an industrial application attack first breaks the perimeter (physical security), then propagates towards the control system (network security) and finally delivers the deadly blow (system integrity) at the plant. Hence, the practicability of the defense-in-depth approach ensures multi-layer protection, with each layer protecting the other layers and ensuring the attacker spends time and effort at each transitional layer. In addition, the multi-layering protection acts as an information assurance concept in which the security control layers are spread throughout the network and counter checks each other from being exploited.

II. Literature Review

Traditionally, the process control network was considered secure [6], however, control systems network connections are increasingly becoming part of the wide-area networks. The plant control rooms which usually used to sit on the process control networks are shifting towards remote centers spread across continents. Added to this, the network system has become a physical link between the control room and the control system, hence securing the network system has evolved into an iterative process. According to Faravo [10], the design, implementation, and operation of a safety system require a "defense-in-depth and observability-in depth" approach. The advantage of adopting the Faravo approach lies in its safety principles which can be used to model the cybersecurity network system framework. Security researchers Denning [11], and Chen [12] examined the vulnerabilities of the industrial control system security which can be exploited and deliver precision-guided destruction.

Furthermore, the literature views the process control network as an integrated network comprising of four main segments [4]; business network, monitoring network, control system, and field system. Each segment adds vulnerability complexities [3] which need to be factored in when developing a cybersecurity framework.

In addition, the national institute for standards and technology reference model [13], [14] for industrial control networks provides a baseline for the design of the process control network. Al Ghazo, in his thesis [15] describes the Scada security problem and proffered a framework to mitigate the problem. However, it falls short in scope and scale to address the ever-changing complex environment of cyber-attacks. This view is shared by Abie and Skomedal [16] who outlined the "FARM" conceptual framework as a methodical approach to assimilating security requirements, policies, and risks to efficiently secure the process control network.

Others like Krutz [7] provide guidelines and standards on how to secure systems and infrastructure within the process control network.

Consequently, it is clear that any framework for network security needs to assess and evaluate the following:

1. Analyze the vulnerabilities and threats
2. Construct the policies
3. Design the network architecture
4. Integrate the control measures
5. Implement the design

III. Methodology

In order to map the security measures required for a manufacturing plant, a 6-hats thinking approach [13] is used to invigorate the defense-in-depth strategy. The first step is to assess and analyze the performance and criticality of the whole network including the enterprise layer for vulnerabilities. Figure 1 below is a graphical security assessment designed to secure and preserve equipment availability, integrity, and confidentiality of the processes in the plant network.

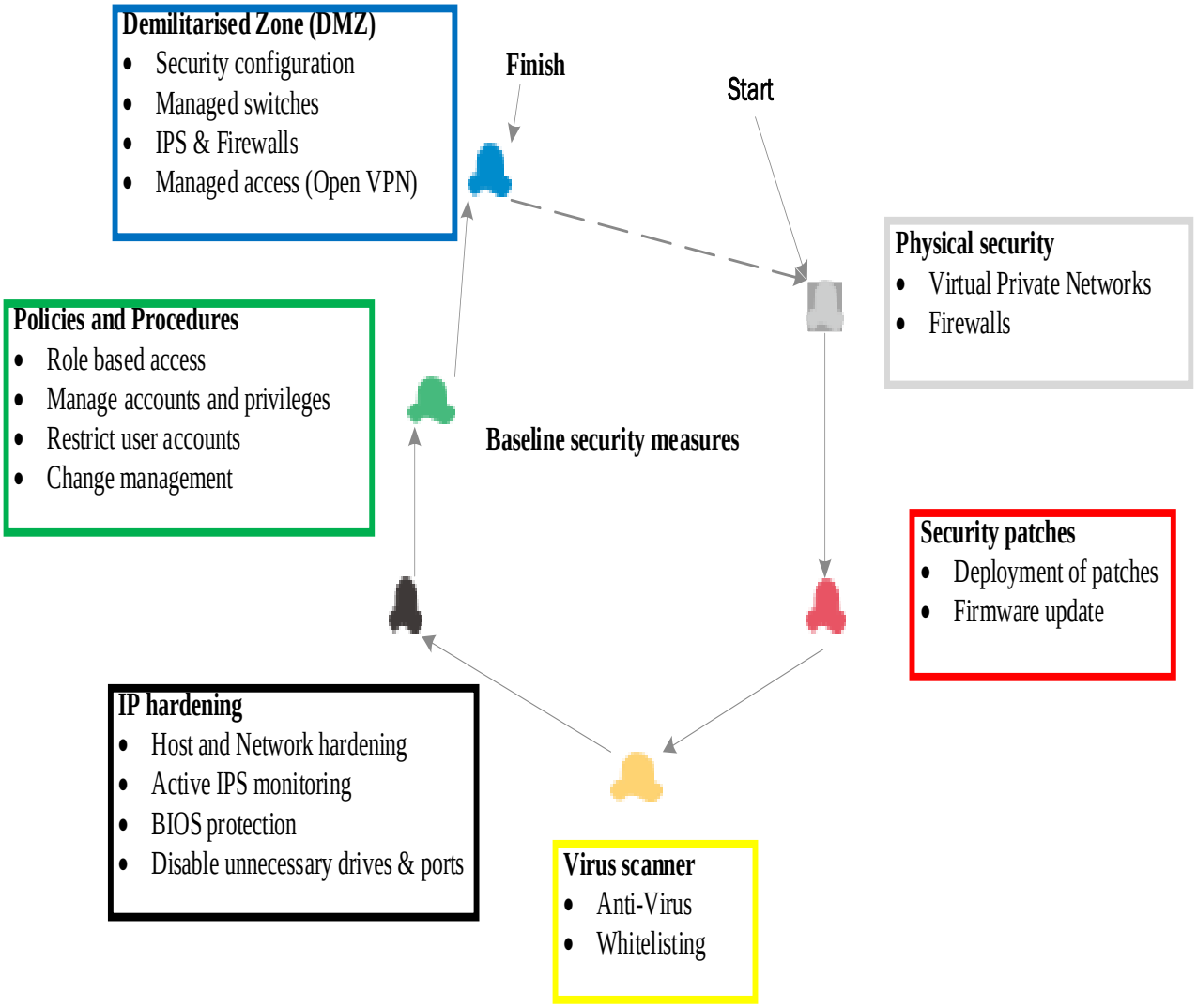

Figure 1: The nexus of cybersecurity system

After the network separation, the correct right patches are deployed and are designed to fix exploits caused by the vulnerabilities in the security weaknesses from the operating or application systems. It is imperative to get patches that have been tested and certified by control system vendors. At the same time, the use of anti-virus software has been the cornerstone of the defense-in-depth strategy to detect, block, and eliminate harmful programs and malware.

In addition, the hardening of the control systems improves the security situation and minimizes the probability of a cyber-attack. Some authors have described hardening as a tool used to delay the attack. If it is viewed from the defense in defense strategy as it provides a warning in addition to the protection. It is further complemented by using designed procedures and policies to limit unauthorized access to the equipment. Furthermore, islanding of the network serves to ensure that only authorized entry is permitted. Unwanted service ports, unwanted applications, and software are removed or disabled, making them unusable to the would-be cyber attacker. The premise is prevention is better than cure.

As with segregated networks, the DMZ or demilitarized zone is designed to enhance security by preventing straight-through connections from untrusted sources. To complement the DMZ, routers, switches, and firewalls are intelligently configured to pass well-defined traffic.

IV. RESULTS

The proposed framework for the implementation of cybersecurity measures is given in Figure 2. It has three physical layers, each designed with security features to complement the other layers. It is a myriad of network activities encompassing Information Technology (IT) standards and control system best practices. The first step is to secure the process control network

through VLAN network segregation. The network separation is done at the corporate network through firewalls, access control lists (ACL) and intrusion prevention system (IPS). A basic network scanning is then performed to test the islanding of the networks. Furthermore, penetration tests are done to check the integrity of the system.

As the process control network hosts the physical hardware and application software of the plants, delicate and specific security measures are applied. As studies have shown that the devices in the process control network are increasingly being targeted, the security measures vary between computer and control system based.

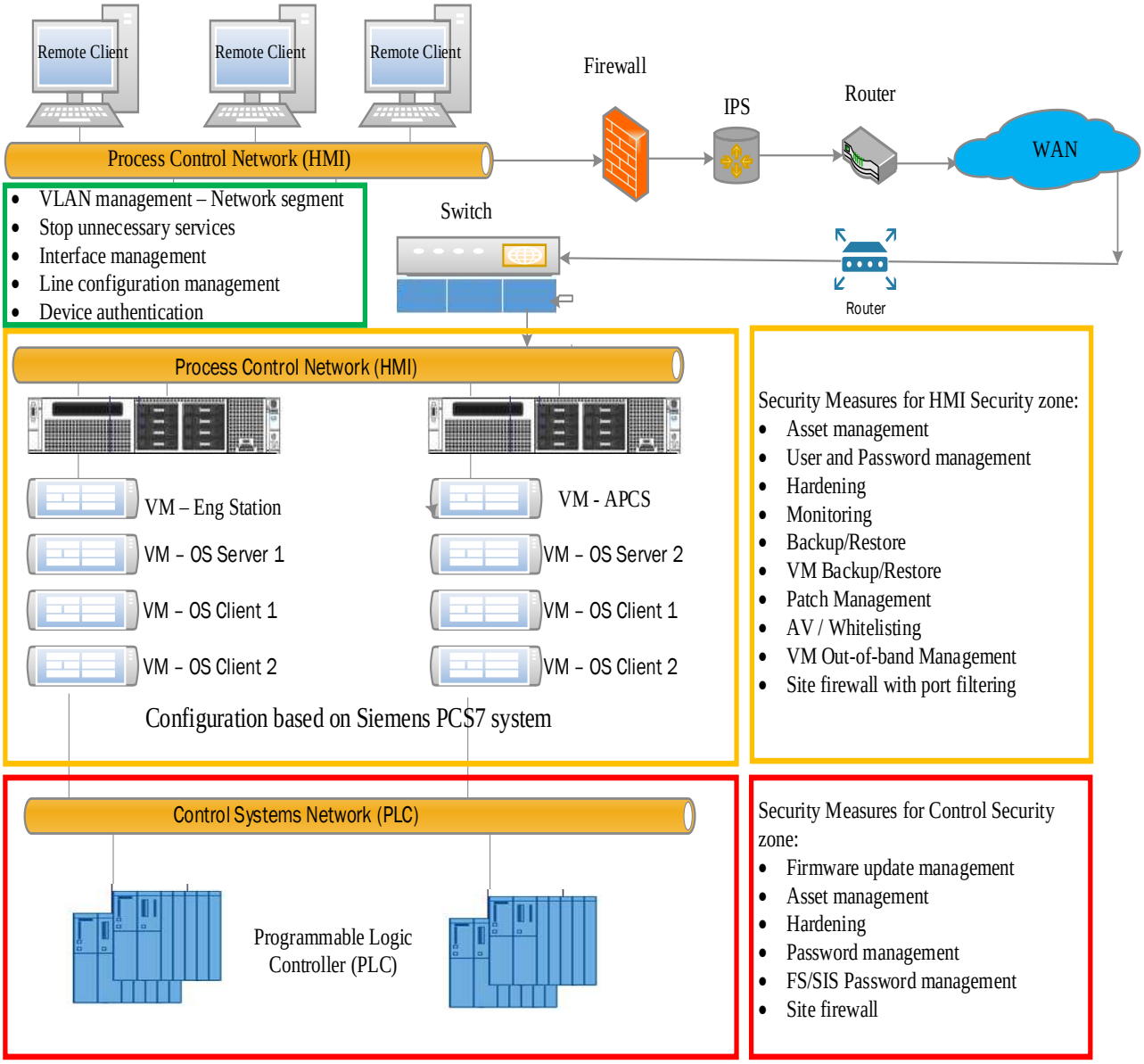

Figure 2: The conceptual framework for cybersecurity measure implementation

V. Conclusions, Limitations and Future Research

The framework for cybersecurity measures is presented as a hybrid network security model and offering the typical measures required for the process control network. Some of the control systems in the process control network are sensitive and defensive in nature which makes it impossible for researchers to get the data to evaluate.

Further work is required to build a knowledge base for the security requirements for a wide range of control systems. The effectiveness and resilience of the framework require further testing by industry and network experts.

ACKNOWLEDGEMENT

Joseph and Barend would like to acknowledge the Information System (IS) team at Afrox Limited whose involvement in the network separation and establishment of the process control network disaster recovery centre was immeasurable.

References

1. M.-M. H Abdo, "A safety/security risk analysis approach of industrial control systems: a cyber bowtie-combining new version of attack tree with bowtie analysis.," Computers & Security, vol. 72, pp. 175-195, 2017.
2. I. S. a. K. Shadmanova, "Summarization of Various Security Aspects and Attacks in Distributed Systems: A Review," ACSIJ Advances in Computer Science: an International Journal, vol. 5, no. 1, pp. 35-38, 2016.
3. A. P. Bhatt, "Computer & Network Security Threats," International Journal of Advanced Research in Computer Science and Management Studies, vol. 1, no. 1, pp. 5-9, 2013.
4. Z. X. L. W. K. C. C. C. W. Z. Xiaojun Zhou, "APT Attack Analysis in SCADA Systems," MATEC Web of Conferences 173, 2018.
5. E. S. a. J. S. Suhaila Ismail, "Towards Developing SCADA Systems Security Measures for Critical Infrastructures against Cyber-Terrorist Attacks," International Federation for Information Processing, vol. 428, pp. 242-249, 2014.
6. A. H. D. S. Simon D. Duque Anton, "Devil in the Detail: Attack Scenarios in Industrial Applications," 2019 IEEE Security and Privacy Workshops (SPW). IEEE,, 2019.
7. R. L. Krutz, Securing Scada Systems, Indianapolis: Wiley Publishing, 2006.
8. O. S. Saydjari, "Engineering trustworthy systems: A principled approach to cybersecurity," Communications of the ACM, vol. 62, no. 6, pp. 63-69, 2019.
9. D. a. F. M. Kuipers, "Control Systems Cyber Security:Defense in Depth Strategies," 2006.
10. J. H. Francesca M. Faravo, "Observability-in-Depth: An essential complement to the defense-in-depth safety strategy in the nuclear industry," Nuclear engineering and technology, vol. 46, no. 6, pp. 803-816, 2014.
11. D. E. Denning, "Stuxnet: What Has Changed?," future internet, vol. 4, pp. 672-687, 2012.
12. S. A.-N. Thomas M. Chen, "Lessons from Stuxnet," IEEE Computer Society, vol. 44, no. 4, pp. 91-93, 2011.
13. J. F. a. K. S. Keith Stouffer, Guide to Industrial Control Systems (ICS) Security, Gaithersburg, National Institute of Standards and Technology, 2011.
14. S. L. M. A. P. A. H. Keith Stouffer, "Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology Special Publication 800-82, 2014.
15. A. A. Ghazo, "A framework for Cybersecurity of Supervisory Control and Data Acquisition (SCADA) Systems and Industrial Control Systems (ICS)," 2020.
16. H. A. a. A. Skomedal, "A Conceptual Formal Framework for Developing and Maintaining Security-Critical Systems," International Journal of Computer Science and Network Security, vol. 5, no. 12, pp. 89-97, 2005.

AUTHOR(S) PROFILE

Joseph Dube, received an MPhil in Engineering Management from the University of Johannesburg in 2019 and BSc Honours in Technology Management from the University of Pretoria in 2015. He also holds a Bachelor of Technology degree in Electrical Power engineering from the University of South Africa. He started his career as a Robotics engineer in the automotive industry in 1998 and in 2000 moved on as an automation specialist in pulp and paper industry. He is currently a lead process control specialist responsible for remote operations and network security for a gas company.

Dr Botha, started his engineering career as systems engineer at Denel in 1992 and registered as professional engineer with ECSA in 1994. He joined Potchefstroom University in 1995 where he lectured at both under and post graduate level till 2008. In parallel he acted as consultant to PBMR and quality manager to M-Tech Industrial. He completed his Ph.D. in Engineering in 2003 at the North-West University. In 2008 he joined PBMR full-time as Senior Systems Engineer. After the closing of PBMR in 2010 he joined the University of Pretoria lecturing in Reliability Engineering, Reliability Based Maintenance and Mechanical Design as part of the Maintenance Engineering programme. He then joined SNC-Lavalin as Design Manager until SNC-Lavalin closed their South African office due to the slump in the mining industry. He is currently a lecturer in Mechanical Engineering Sciences at UJ where he lectures in Design and provides study guidance at postgraduate level in both Mechanical Engineering and the Postgraduate School of Engineering Management.

