A Review of Cyber Security Assessment (CSA) for Industrial Control Systems (ICS) and Their Impact on The Availability of the ICS Operation

Nor Afiq Bonandir¹, Norziana Jamil¹, Md Nabil Ahmad Nawawi¹, Razali Jidin², Mohd Ezanee Rusli¹, Lam Kwok Yën³, Loviana Lenyu Anak Dunstan Maudau¹

¹College of Computing & Informatics, Universiti Tenaga Nasional, Putrajaya Campus, Selangor, Malaysia
²College of Engineering, Universiti Tenaga Nasional, Putrajaya Campus, Selangor, Malaysia
³Nanyang Technological University, 50 Nanyang Ave, Singapore

norziana@uniten.edu.my

Abstract. The equipment in industries in this digital age is controlled by systems connected via internet either wired or wireless connectivity. This technology is demanded in almost all organizations to perform their daily industrial operations. Hence, the system must run without any failure and the rate of system availability is a priority. Most importantly, the entire system must be secured from cyber security threats, vulnerability, and risks so as to ensure that the system is not exposed to the possibility of any cyber attack. Thus, initial security assessment must be conducted to ensure the security aspect of the system. Nevertheless, the evaluation shall not impact the system's regular operations. As such, the study reviews and discusses the Cyber Security Assessment (CSA) for Industrial Control Systems (ICS) and their possible effect on the availability of ICS operations.

1. Introduction

Industrial Control System (ICS) is a broad name arising from the convergence of many forms of systems, namely Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS) and several configuration control systems, like the Programmable Logic Controllers (PLCs), which can be used in industries and essential infrastructure. Usually, ICS is used in a number of sectors, such as power systems, water and sewage, oil and natural gas, chemical, and transportation [1].

ICS vulnerabilities are due to malfunctions, configuration issues, and inefficient system maintenance, which include hardware, operating system (OS) and ICS systems. These vulnerabilities can be minimized by a number of security mechanisms, such as OS and program patching, physical security systems, and network security [1].

Cyber-attack can be carried out in ICS because most ICS inventions do not comply with the security condition of a specific order, which requires confidentiality, integrity, and availability (CIA). For instance, cyber threat towards availability involves leaving vital control and efficiency tools and sensitive information at all times inaccessible. Threat to integrity manipulates sensitive information on resources, while a threat to confidentiality, involves eavesdropping to relevant information. [2]. Therefore, it is important to perform cyber security assessment (CSA) in order to minimize and close
the gap of the cyber security issues present in ICS. Malicious attacks on ICS in recent years, it has risen dramatically. The Stuxnet and BlackEnergy attacks have shown that a single spear-phishing email or compromised USB drive allows all attackers to infiltrate a remote network. Conventional safety and security is insufficient to better protect industrial systems against cyber-attacks. Given the significant increase in the threats to critical infrastructure, it is crucial to choose the best consultant and technology provider to protect our systems and infrastructure.

2. Problem Statement
Attacks towards ICS have increased on annual basis. Some have greatly affected at national level, while some reflect minor incidences. With the reported recent cyber incidences that happen to target ICS industry, a pressing need is present to conduct CSA so as to understand the strength of ICS from the stance of cyber security. Most CSAs are primarily designed for IT systems that do not specifically address the constraints in ICS. Thus, this study outlines several suitable approaches that are required to perform CSA in ICS.

3. Industrial Control System
Within the information security domain, the CIA triad is a well-known model for security policy development. Each feature reflects a primary purpose of data protection in order to have the following:

**Integrity**: Defense from unauthorized alteration or loss of information which requires declaration of non-repudiation, accuracy which authenticity of information [3].

**Confidentiality**: Preserving permitted access and transparency limitations providing a protection for data privacy and classified information [3].

**Availability**: Ensure that information has timely and accurate access and use [3].

The ICS safety triad mainly focuses on availability and integrity, more importantly than confidentiality. They aim to optimize availability so that systems operate and perform without interference or unintended interruption. In control systems, data integrity is very critical. If somehow the operator's screen in the command center would not correctly reflect what is happening, there may be a major effect on the operation or even security. [4].

It is typical for confidentiality to have lower priority in ICS, in comparison to integrity and availability. This is because; data that are traverse in an ICS environment, such as temperature, vibration, and speed, are temporary data [4].

Generally, ICS is constructed to operate consistently for as long as possible. Often it is probable, ICS is designed to operate for 20 years. Hence, it is challenging to upgrade the security patch. Additionally, performing CSA on ICS with varied approaches is difficult especially in ensuring that the CSA does not cause system downtime.

3.1. Industrial Control System in Electric Power Grid
The IT infrastructure for electricity utility currently uses various forms of ICS to interconnect generation, transmission and distribution functions. These broader connectivity and network connection have escalated the risk from the cyber security perspective. The attack of the power supply sector is being extended through the convergence of information technology (IT) and operating technology (OT) systems. These two aspects have in the past been separated, but in many contexts they are still associated. The ICS platform in the OT sector is also based on a commercial IT OS. This indicates that vulnerabilities in the IT environment have been evident in the OT environment [5].

A typical method for improving security of system in an OT environment is usually not to patch or retain the IT environment because, due to application software compatibility, it is mainly funded by the Original Equipment Manufacturer for software updates. This indicates that OT systems are defensively lagging behind their IT counterparts. Eventually, many ICS networks do not have authentication protocols or managed access policies, and cyber security management can be inadequate to non-existent, rendering them vulnerable [5].
3.2. The Importance of Cyber Security Assessment In Industrial Control System Of Electric Power Grid

CSA in ICS aids the asset owner or the organization to reckon the strength of its infra from the perspective of cyber security. It also helps to identify the vulnerabilities or loopholes that may exist and allow an attacker to disrupt or to take control of the system. Upon detecting the vulnerabilities and loopholes, rectification and mitigation of the drawbacks are performed in the attempt of preventing cyber-attack that may jeopardize the ICS.

Many cyber incidences have occurred due to poor CSA, as listed in the following Table 1.

| Cyber Incident Name       | Place Happened             | Year | Impact                                                                 |
|---------------------------|----------------------------|------|------------------------------------------------------------------------|
| Blackenergy               | Ukraine Power Grid         | 2014/2015 | 6-hour electric disruption happens in Ukraine that affects, estimatedly ~230,000 people [8]. |
| Industroyer/Crash Override| Ukraine Power Grid (North City of Kiev) | 2016 | 1 hour of electric disruption that causes Ukraine, estimatedly to lost 1/5 their electric capacity [17]. |
| Triton                    | Oil & Gas Plant Saudi Arabia | 2017 | Attacker plan to trigger plant-wide explosion but it was failed because of flaw and bug in their malware [11]. |

The ICS has often made the availability of security triad a top priority. Some systems dismiss the application of patch or system update as this may affect the availability of the system. The absence of update or the latest patch version can lead to disastrous cyber-attack events. This causes the ICS to run with a lot of vulnerabilities and security flaws. In order to detect these vulnerabilities and security flaws in ICS, it is necessary to perform CSA. To do so, the information security practitioner must be knowledgeable about the ICS that they wish to assess. A single mistake in performing CSA within the ICS environment can lead to downtime and disrupt the normal operation [6], [7], [8], [9], [10], [11].

As such, this study discusses the possible approaches that can be applied to conduct CSA in ICS.

4. Cyber Security Assessment Approach in Industrial Control System

A common system or software program is used to perform CSA in the ICS environment. Most of the tools employed are similar to those used by the analysts to assess the IT environment. Some tools that are run in the IT environment can cause availability impact on the ICS, such as disrupting the operation and causing some systems to crash, due to the assessment itself [12].

Here are the common tools that analysts use, which may have an impact on availability.

| Software | Objective                                                                 | Impact on Availability |
|----------|---------------------------------------------------------------------------|------------------------|
| Nmap     | To detect and identify hosts that reside on a network and gain details about them, such as the services that they are operating and the opening port on the hosts. | Yes                     |
Shodan | To conduct and perform scanning and searching on services or host that run on devices connected to the internet. | No
---|---|---
Nessus | To perform host exploration and vulnerability analysis about a host that has been detected as well as to give an overview of the detected vulnerability along with the solution to rectify the vulnerability. | Yes

4.1. NMAP

Nmap is a tool that is commonly used to detect and to identify hosts that reside on a network. Simultaneously, this tool gathers information details about the host, such as the services that they operate and the opening port on the host [13].

Running Nmap in ICS can create chaos in the environment since this tool can cause the system to crash. A system crashes if the tool scans legacy devices or system. Some systems that reside on the legacy systems might have issues on how the system has been built in handling the stack of TCP/IP requests from the scanner, and in some cases, the system cannot accept multiple request from Nmap, thus causing the system to misbehave or crash. The impact of this tool is that the scanned system or devices can crash and the ICS operation might be disrupted [14].

In conclusion, Nmap should be properly tuned to adapt to the ICS environment. Nmap should not perform intrusive scan and the threshold or timing of the system should be well tuned. This can minimize the possibility of system crash, misbehavior during the scanning activity, and ensure that the network is not congested with scanning activity.

4.2. SHODAN

Shodan is a search engine that is used to search for devices that are connected to the internet and it works differently from other popular search engines, such as Bing, Google, and Yahoo. Visibility of the devices or system on Shodan reveals misconfiguration issue [16].

Shodan detects devices that are linked to the network. It searches for accessible terminals and by using Shodan, a user can search for specific services that run on a host. As a result, if a single IP address hosts more than a service, Shodan lists all the open services at that address [16]. The following is an example of the Shodan search result.
The data collected by Shodan are in metadata format and contain information, such as the host name, OS, geographic location, and properties related to the application or transport layer protocols, e.g. server message block, SSH protocol, TLS, and SSL.

The visible device or system detected in Shodan should be assessed to determine if it is safe. The device or system should be configured in order to limit the accessibility of Shodan search engine scan in gathering information.

4.3. NESSUS

Nessus is a tool that is commonly used to conduct host discovery and vulnerability analysis on detected host, as well as to give an overview of the detected vulnerability, as well as the solution to rectify the detected vulnerability [13].

Nessus does have the ability to continuously test each method used to establish internal service to identify possible vulnerabilities based on the response mostly from host on each probe and request. After that, the Nessus compares the vulnerability signature with the Nessus database to identify potential vulnerability.

The dangerous plugin, such as denial of services (DoS) testing, brute force or dictionary attack plugin, should be disabled first. These two plugins can cause the system to crash or misbehave. Performing active probe on the host can lead to system crash and DoS, which disrupt the ICS availability. This incident can happen either in IT or OT environment [15].

As a conclusion, Nessus should be properly tuned to adapt to the ICS environment. The full overview of the system should be reckoned prior to Nessus scanning. Proper mitigation planning should be done first to check if the system misbehaves, so as to hinder crash and allow the ICS to run as normal.

A typical method for improving security of system in an OT environment is usually not to patch or retain the IT environment because, due to application software compatibility, it is mainly funded by the Original Equipment Manufacturer for software updates. This indicates that OT systems are defensively lagging behind their IT counterparts. Eventually, many ICS networks do not have authentication protocols or managed access policies, and cyber security management can be inadequate to non-existent, rendering them vulnerable [5].
5. Conclusion

The past cyber security incidences highlight the significance of performing security assessment in ICS, especially to identify the gap and to close the loopholes of the system. Not only that, the CSA is to also address cyber security threats. However, the main concern is CSA should not affect the daily operations of the ICS since most industries make the availability of the system as their top priority. This paper has discussed the challenges to conduct CSA in ICS and the impact it has caused to the ICS in general. We are in the opinion that CSA can be performed by setting up a virtual lab to simulate the real ICS environment. With the challenges highlighted in this paper, it is hoped that the company that owns or operates ICS can take necessary actions to ensure that their ICS is secure and reliable.

Acknowledgments

This research is supported by Uniten UNIIG Grant with a Project Code J510050820, TNB Seed Fund 2019 with a Project Code U-TC-RD-19-09 and Uniten R&D Sdn Bhd.

References

[1] K. A. Stouffer, V. Y. Pillitteri, S. Lightman, M. Abrams, and A. Hahn 2015 Guide to Industrial Control Systems (ICS) Security Spec. Publ. NIST SP - 800-82 Rev 2
[2] C. Alcaraz and S. Zeadally 2015 Critical infrastructure protection: Requirements and challenges for the 21st century Int. J. Crit. Infrastruct. Prot. vol 8 pp 53–66
[3] G. S. Dardick 2010 Cyber Forensics Assurance 8th Aust. Digit. Forensics Conf. Ed. Cowan Univ. Perth West. Aust.
[4] Developing a Security Strategy to Cover ICS Assets « Developing a Security Strategy to Cover ICS Assets 2016 FireEye. [Online]. Available: https://www.fireeye.com/blog/executive-perspective/2016/08/developing_a_secure.html. [Accessed: 05-Sep-2018]
[5] © Stanford University Stanford and C. 94305 C. C. T. Notice 2017 Cybersecurity: Industrial Control Systems and the U.S. Electric Grid | MS&E 238 Blog. [Online]. Available: https://mse238blog.stanford.edu/2017/07/dilove/cybersecurity-industrial-control-systems-and-the-u-s-electric-grid/. [Accessed: 05-Sep-2018]
[6] U. Shamir, Analyzing a New Variant of BlackEnergy 3 p. 14.
[7] A. Cherepanov and R. Lipovsky, BLACKENERGY – WHAT WE REALLY KNOW ABOUT THE NOTORIOUS CYBER ATTACKS p. 8.
[8] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer 2016 Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid presented at the 4th International Symposium for ICS & SCADA Cyber Security Research
[9] Anton Cherepanov and Robert Lipovsky 2017 Industroyer: Biggest threat to industrial control systems since Stuxnet WeLiveSecurity, 12-Jun-2017. [Online]. Available: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/. [Accessed: 19-Nov-2018]
[10] Blake Johnson, Dan Caban, Marina Krotofil, Dan Seali, Nathan Brubaker, and Christopher Glyer, Attackers Deploy New ICS Attack Framework ‘TRITON’ and Cause Operational Disruption to Critical Infrastructure « Attackers Deploy New ICS Attack Framework ‘TRITON’ and Cause Operational Disruption to Critical Infrastructure 2017 FireEye. [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html. [Accessed: 19-Nov-2018]
[11] A. D. Pinto, Younes Dragoni, and A. Carcano, TRITON: The First ICS Cyberattack on Safety Instrument Systems p. 28
[12] T. Gary, ICS/SCADA Smart Scanning: Discover and Assess IT-Based Systems in Converged IT/OT Environments 2018 Tenable®, 12-Jun-2018. [Online]. Available:
https://www.tenable.com/blog/icsscada-smart-scanning-discover-and-assess-it-based-systems-in-converged-itot-environments. [Accessed: 19-Nov-2018]

[13] K. Coffey, R. Smith, L. Maglaras, and H. Janicke 2018 *Vulnerability Analysis of Network Scanning on SCADA systems - Supplementary Material.*

[14] *Legal Issues | Nmap Network Scanning.* 2018 [Online]. Available: https://nmap.org/book/legal-issues.html. [Accessed: 24-Nov-2018]

[15] S. Samtani, S. Yu, H. Zhu, M. Patton, and H. Chen 2016 *Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques* in 2016 IEEE Conference on Intelligence and Security Informatics (ISI), 2016, pp. 25–30

[16] S. Samtani, S. Yu, H. Zhu, M. Patton, J. Matherly, and H. Chen 2018 *Identifying SCADA Systems and Their Vulnerabilities on the Internet of Things: A Text-Mining Approach* IEEE Intell. Syst. vol 33 no 2 pp. 63–73

[17] *CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack* Joe Slowik, Dragos Inc [Online]. Available: https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf [Accessed: 10-Mar-2020]