Research Article

Analysis of Cyber Threats in the Connection Section of the Control System and Countermeasures Required

Yangha Chun *

Computer Science, Yongin University, Cheoin-gu, Yongin-si, Gyeonggi-do, Republic of Korea
*Corresponding author. Tel. +82-10-8984-7658; Email address: yangha00@yongin.ac.kr

Article History: Received: 10 November 2020; Revised: 12 January 2021; Accepted: 27 January 2021; Published online: 05 April 2021

Abstract: In the past, the general practice for the control system network that manages and controls industrial facilities such as electric power, gas, oil, water, chemicals, automobiles, etc. was to install and operate this as an independent system, but over time the practice has gradually shifted toward the use of an open and standardized system. Until recently, most industrial control systems consisted of an independent network, and the possibility of cyber threat infringement was very low. As information storage media such as laptops or USB are connected to the control system for maintenance or management purposes, the possibility of cyber infringement is increasing. When the use of the control system's operational information increases due to beingVinked with the internal business system network or the Internet, countermeasures against external cyber threats must be provided.This paper analyzes and organizes the cyber threat factors that exist in the linking section connected to the industrial control system and other networks, examining domestic and foreign incidents of hacking of control systems to identify the vulnerabilities and security measures for each scenario in the control system network linkage section. Through this analysis, a method is suggested for establishing a control network that secures both availability and security, which are important in the control system, as well as the safe relay system in the configuration of the linkage between the control network and the business network, while addressing the vulnerabilities in the structure due to long-term use of the control system.This study analyzes cyber threat factors and real-life examples of infringements with the aim of providing approaches that will ensure industrial control systems can be operated safely and the risk of cyber hacking threats that occur in connection with other networks can be managed, and suggesting cyber security measures for the control system connection sections.

Keywords: Cyber Security, Instrumentation and Control Systems, SCADA, Vulnerability Analysis, Cyber threats

1. Introduction

To improve the management and maintenance efficiency and to share the facility operation management information, industrial control systems are connected or integrated with other IT networks. However, with the development of IT, cyber-attacks are becoming more intelligent and specialized, and incidents of infringement by organized hacker groups are increasing[1,2]. The boundary between the Internet and the business network has hacking vulnerabilities that can be breached, and the threat of cyber-attacks via these vulnerabilities is evolving and developing. As such, it is necessary to study the problems and countermeasure technologies for vulnerabilities caused by network connection and integration of the control system. In the past, industrial control systems used dedicated devices or proprietary software, but more recently standard protocols (TCP/IP, Ethernet, etc.) or general-purpose products (MS Windows operating system, R-DB, general-purpose language, etc.) are being introduced. Furthermore, industrial control systems are being connected or linked with other information systems such as the Internet or enterprise-wide information systems in order to improve the management and operation efficiency[3].

As a result, even the control system that had been operated as an independent closed network has become vulnerable to attacks or threats that exploit security vulnerabilities[4.5] that occurred in the general information system. The control systems that had been built without any security considerations in the past began to suffer a new problem of cyber security due to this shift to an open control system environment. In recent years, signs of cyber terrorism and hacking of the control systems of important national infrastructures have been gradually increasing, and diverse studies have identified such control systems as being vulnerable to cyber security breaches[6]

2. Cyber Threat Elements in Control Systems

2.1 Threat of control system's linkage section

With the progress in networking, there is always a possibility of creating a dangerous situation in cyberspace connected to an open network such as the Internet. In addition, potential cyber-security threats may inevitably occur through the setting of an access path from the outside to the internal network, or through the internal systems connected to external Internet networks, the internal wireless LANs, and external storage devices. In general, the infringement threats that can exist in internal networks can be classified into threats that attack the internal network directly from the outside, and threats from within the internal network.

Direct external threats on the internal network can be broadly classified into 4 types: infection of malicious code on an internal PC connected to the Internet; attempts to access the internal network through the internal

***Corresponding author:** Yangha Chu
Computer Science, Yongin University, Cheoin-gu, Yongin-si, Gyeonggi-do, Republic of Korea
Email address: yangha00@yongin.ac.kr

wireless LAN; vulnerability of the application service exposed to the outside; the release of key internal information due to negligence in internal network management[6, 7].

2.2 Threat of control system's linkage section

With the development of industrial technology, electrical and mechanical control systems are changing into automatic control systems. In addition, the control network in which the control system is located is becoming linked with the business network or the security control network for the dissemination of disaster and crisis information, information linkage with a comprehensive threat management system, and integrated control[5]. The security threat factors of the control system can be divided into threat factors occurring in the general system and those occurring due to the specific properties of the control system.

In general, the control system is more vulnerable to cyber threats than general information systems because it has specific features that it cannot establish an information protection system to protect the control system according to the operation of the closed network, the OS of the control system and the operation program update and security patches are insufficient, and the production process for the installation of the security system is stopped, the introduction of the security system is insufficient, there are numerous bugs in the control system itself, and the security awareness and ability of the control network manager are insufficient, etc[8,9].

Vulnerabilities due to the specific nature of the control system include attacks spread by expanded use of standard protocols for connection of the control system, attacks through increased intrusion paths by remote access using public communication services, attacks by malicious former and current employees aggravated by increased pressures such as rationalization, automation and cost reduction, attacks for reasons of terrorism and information warfare, and attacks from other countries that are rooted in nationalism[9]. These factors lead to specific threats and attacks.

The vulnerabilities of the control system expose the vulnerabilities of the general system to the threats more strongly, and illuminate the limits of protecting a control system using a general security system[10].

3. Countermeasures against cyber threats in the control system linkage section

3.1 Cyber Threats in Control System Linkage Section

With the openness of the control system, the attack paths, which had been limited to the vulnerabilities of the control system itself, were increased through external hacking. [Figure 1] shows the structure of a general control system divided into stages. The levels of these are as follows:

Zone 1 is connected to the Internet, pier location and outside, Zone 2 has an outside connection for internal work, Zone 3 communicates with a control system from external services, and Zone 4 is a process-based or control system.

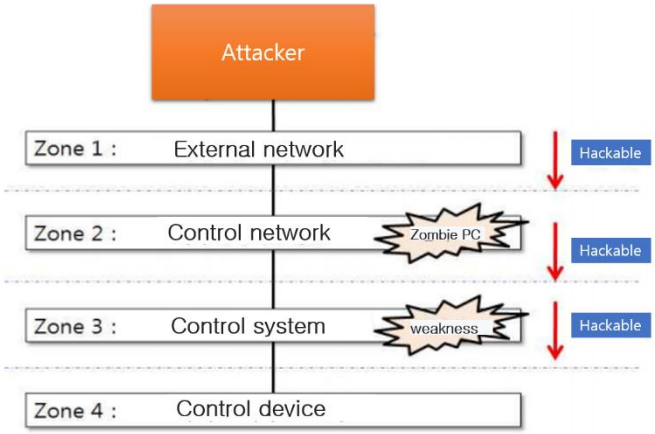


Figure 1 Hacking possibility and attack realization stages for control system

3.1.1 Internal network attack in the Internet zone

A scenario was created in which the internal system is hacked by an attack generated from the external Internet. In the scenario, the hacker on the Internet attacks the internal network system, which becomes a path into the internal network system that can cause serious damage to the control system[11].

3.1.2 Attack through connection point between business network and control network

Attack on a control network by accessing from the external network into the internal network and then, as a second level, from the internal network into the control network.

3.1.3 The attack on the internal section of the control system by Stuxnet

Executed through a special assembly like PLC code. PLC is mainly programmed on the Internet or even on a Windows computer that is not connected to the network, and the control system is also unlikely to be connected to the internet[11, 12].

Taking this point into account, the attack based on the technical features of Stuxnet targets WinCC which is SCADA HMI, STEP7 which is an engineering tool, and PLC which is an embedded controller. [Figure 2] is an example of the Siemens control system configuration.

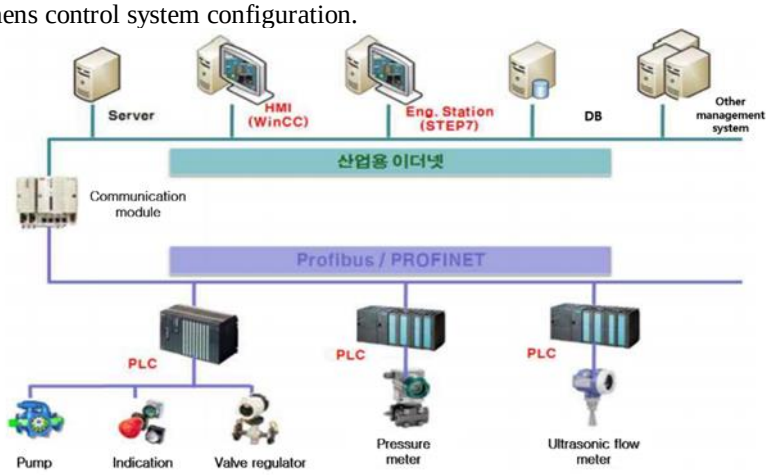


Figure 2 Example of Siemens control system configuration

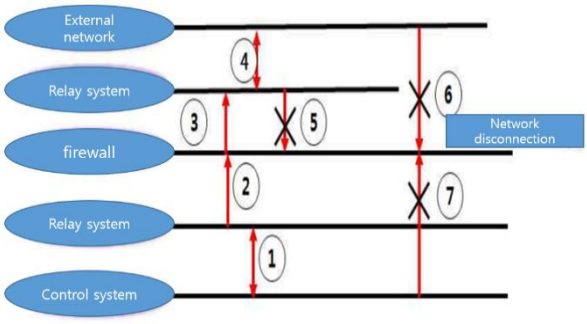
3.2 Threat of control system's linkage section

If the control system operating zone is attacked, the information resources in the control system can be made difficult to be manipulated. In many sectors, malicious attacks on control systems have real consequences. To solve this problem, it is necessary to establish security measures according to the connection with the control system. Direct communication between the control network and its connected network should be blocked, and all external access to the control network should be shut down. In addition, risk verification should be performed on all relayed data[10].

By blocking external access to the control system through building a one-way transmission system through the network disconnection model, as shown in [Figure 3], the attack path to the control system from the external network is removed.

Plan to thoroughly block the access to the control network through one-way communication configuration are as follows:

Figure 3 Network disconnection by relay system between control network and external network



3.2.1 One-way communication configuration of UDP method

In the TCP/IP communication protocol, the request for communication preparation is necessary for data transmission. Therefore, two-way communication between the sender and the receiver is inevitable. But in the UDP method, since the sender can transmit in one direction without a request from the receiver, one-way communication can be performed. This means that it can block access to the inside of the control network from the linkage section.

3.2.2 One-way data transmission configuration using a relay system

A relay system is configured to block impersonation by performing identification and authentication, and the data between the relay systems is encrypted to secure the integrity and confidentiality. As it plays the role of

checking the stability and permission rules of the relay data, it can block the relay of unauthorized data and data formats[9].

3.3 Security measures for internal control system

3.3.1 Basic security measures for control system

As a measure for control system security, technical strategies such as system security vulnerability scanning, systematization of physical server management, and minimization of invasion or construction of hacking and abuse(worm/virus) programs are required. In addition, it is necessary to restrict the access of users to the computer system by dividing the authority level between super user and general users of the control system.

In addition, the system must be supplemented with a function to enable the blocking of execution of codes (hacking, worms, viruses, etc.) that aim to change the monitoring and operating system. It is also necessary to train experts to strengthen the information protection technology capabilities while establishing the information protection organization for each institution and systematic management strategies.

3.3.2 Addressing structural vulnerabilities in older control systems

It is difficult to implement the security patch of a control system that has been used for a long time, in that it can disrupt the currently operating control system. Therefore, the latest security patches must be applied by updating the control system after securing replacement equipment to ensure uninterrupted operation of the control system, and establishing a system maintenance strategy using this. In a system that is difficult to apply security patches to, the connection point with other systems should be removed or the external attack path should be blocked by one-way transmission.

3.3.3 Enhancement of security functions focusing on availability

It is essential to construct a control network to secure availability, which is important due to the specific nature of the control system. To reinforce the confidentiality necessary for security, it is necessary to predict the loss of network and system performance and to reflect it in the control system to be built. Through the identification/authentication of a system that is connected to the control system and communication encryption, it is necessary to fundamentally block the unauthorized systems from accessing the control system and stop the illegal inflow/outflow of information through the encryption of communication data.

3.4 Safe security network model in control system

The purpose of this study is to present a role-based security network as a safe network model in the control system. The components of the safe network model are classified as follows: It is shown in [Figure 4].

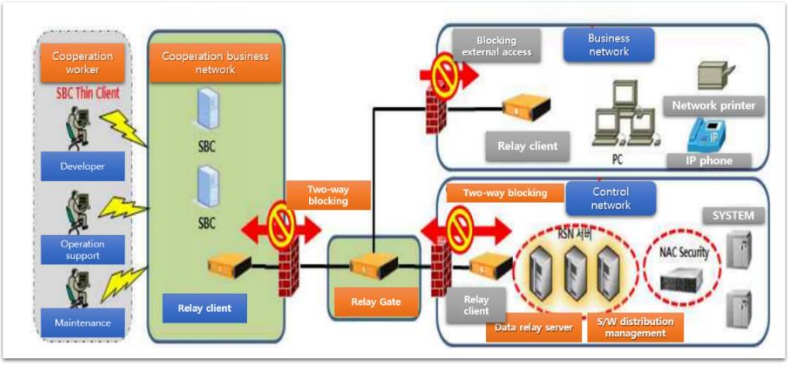


Figure 4 Network disconnection by relay system between control network and external network

It is composed of the external cooperator for operation and maintenance of the control network, the internal user on the internal network, and the cooperative business network which the cooperator uses for work performance. The network is divided into the control system network (control network), the internal user network (business network), the cooperative business network and the sections to secure closedness and relay between the control and business networks.

In addition, it aims to provide safe role-based security and network security, such as network separation at the level of a closed network, restriction of use of computing resources outside the scope of the job role, removal of paths for spreading attacks or reattacks between domains, prevention of vulnerabilities caused by the installation of illegal software, and blockage of the external leakage of accessed or generated information for business performance.

Networks constituting the control system should be divided into a cooperative business network, business network, and control network, each of which is formed as a closed network that blocks the access from outside

or from other individual networks by using an intrusion prevention system and relays the authorized data using a safe relay system. Thus, it is necessary to block movement and use outside the scope of the role of individual network users and configuration systems.

The cooperative business network shall be able to block data leakage as well as threats arising from cooperators, such as the installation of illegal software not designated by S/W distribution management.

The cooperator shall upload and download the work results or the data necessary for their work only through the data relay server, thus blocking the introduction of illegal data or leakage of data to outside the system.

The control network shall relay only the data guaranteed by the secure relay system in the closed area where bidirectional communication is blocked in order to intercept the attack threats from other domain networks.

In order to block attacks and the spreading of worms within the control network, a security system with an access control function shall be installed to block the attack or spreading of worms to other systems.

Inter-section security control shall be performed through the inter-section relay data license and control system in a closed network relay type system.

4. Conclusion

In this paper, the threat factors against industrial control systems were identified, which included the negative effects of informatization related to the spread of open networks and system utilization, and countermeasures that can be applied for security management were suggested. In particular, given that the actual operating system of an industrial control system can not be stopped to install a new security system, a new security management plan should be established and continuous efforts to improve the level of security through preventive activities and regular mock penetration checks or vulnerability consulting are required. In addition, it is necessary to strengthen the constant response to global cyber threats by maintaining information sharing with the related organizations operating the control system.

In reality, it is impossible to stop an industrial control system given that it must be operated almost 24 hours a day, and so it is important to verify the cyber threats against the control system itself. In this study, preventive security measures were suggested through virtual scenarios to predict threat factors in advance by applying the security vulnerabilities in the general system. On the other hand, to secure the cyber safety of the control system, the requirements of confidentiality, integrity, and availability should be met through cyber security activities for the entire lifetime of the system. To secure the safety of the control system and internal network from cyber threats, cyber security measures should be established for each network unit according to its use, as well as access security measures for the connected networks.

In the future, it seems necessary to analyze the security vulnerabilities of the industrial control system itself in order to apply standard information protection technology to the control system and verify the security vulnerabilities thereof from the initial stage of the control system's introduction.

5. Acknowledgements

This dissertation (or book) is a study conducted with funding for academic research grants at Yongin University in 2020

6. References

1. P. A. KHAND. ATTACK TREE BASED CYBER SECURITY ANALYSIS OF NUCLEAR DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS, Theoretical Plasma Physics Division, PINSTECH, P.O. Nilore Islamabad, Pakistan. 2009.09
2. GAO. Critical Infrastructure Protection : Challenge and Efforts to Secure Control Systems, http://www.gao.gov, 2004.3.
3. Moonsoo Jang, Shinkyu Kim, Min Byeong-gil, Seo Jeong-taek . Study on Technology Requirement using the Technological Trend of - Security Products concerning Industrial Control System. Journal of Security Engineering 2008.12.
4. Injoong Kim, Jeong Yoon-jung, Jaeyoung Ko, Dongho Won. The Journal of Korean Institute of Communications and Information Sciences. Journal of Communications and Networks, Vol.30 No.8C, 2005. 8.
5. Japan IPA(Independent Administrative Corporation Information Processing Promotion Organization). Critical Infrastructure Control System Security and IT Service Continuation", http://www.ipa.go.jp(website) 2009. 3.
6. Choi Yu-rak et al. IT-based nuclear power plant communication network cyber security technology development", Korea Nuclear Safety Research Institute, 2009.11.

7. Jeon-yonghui. Network design and structure for industrial control system security. Journal of the Society for Information Security vol19.05, pp. 68-72, 2009.10.
8. Han SeogGyo. A Study on Cyber Threats in Control System Linkage Section. [dissertation] Korea University, 2010.05
9. Hyun Jin Woo. DCS reliability evaluation and communication network design for the application of digital distributed control system in nuclear power plants", Chungnam National University, 2006.02.
10. Cheolwon Lee, Kim Hwi-gang, Lim Jong-in. Corporate private network bypass access analysis and control measures research. Journal of the Society for Information Security vol20. 06, 2010.12.
11. Young-Doo Kang. A study on the cybersecurity evaluation method of nuclear power plant measurement control system. [dissertation] Chonbuk National University, 2011.02.
12. Korea Nuclear Safety Technology Institute. Cybersecurity regulation guidelines for digital measurement and control systems. 2007.12. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE02432687(website)