Journal of Engineering and Applied Sciences 13 (Special Issue 12): 9461-9467, 2018
ISSN: 1816-949X

A Efficient Network Security Management Model in Industrial Control System

[1]Jun-Woo Lim, [1]Il-Yong Kim, [1]Kwang-Jik Kim and [2]Jae-Pyo Park
[1]Department of IT Policy Management,
[2]Department of Information Security, Soongsil University, 07027 Seoul, Republic of Korea

Abstract: The industrial control system constitutes an interdependent system through the cross-connection, so, the security policies for the maintenance of the closed network cannot be applied to the practical situations. Thus, the need for the development of the security management system applicable to various environments arises. In this study, we separated the industrial control network and suggested a security application model as an efficient security management system of the industrial control network. Also, in order to address the existing security problems, we proposed an efficient industrial control network security management system that was hierarchically defined in accordance with the domestic environment of the control network, under the application of hierarchical security model level 0-4 concept defined by the ISA-99. The proposed application security model of the industrial control network was systemized through the application of the separated industrial control network that is separated into the control network and the intranet or into the control network and the external network in accordance with the practical application environment. Also, the hierarchical security model is structured to direct the control system whichis the most important asset to be protected in the control network. Therefore, applying this model has an advantage that the security is strengthened in the process of converting the security system integrated into the internal control network into the multiple protection model. It is expected that if the physical one-way transmission device and the commercial security system provided through the one-way transmission device are developed, it could be flexibly applied to the proposed industrial control network security model.

Key words: Industrial control, cyber security, security management, network separation, model, intranet

INTRODUCTION

The control system is operated as a major national infrastructure and linked to the information communication network system, so, there is a possibility of disruption due to the cyber invasions. Hence, when an invasive action occurs, there might be a chain of impacts on various areas such as the electric grid, nuclear power, traffic, environment and water resources. Traditionally the control system was operated as a closed network, so, usually disruptions have been due to the physical attacks or operational mistakes. However, today the systems are linked to the information communication services such as the infectious flash drives, web publications and spam mails, so, they are exposed to cyber-attacks (Morris and Gao, 2013).

The expression ICS (Industrial Control System) is a common term embracing various control systems such as 0SCADA (Supervisory Control And Data Acquisition), DCS (Distributed Control System) and PLC (Programmable Logic Controllers), that are used in the industry or for the important infrastructure. The industrial control systems are used throughout the industry including electricity, water wastewater, oil and gas, chemicals, transportation, pharmaceuticals, pulp and paper, food and beverage and individual manufacturing. The control systems are operated as an important infrastructure and sometimes cross-linked to constitute an interdependent system (Reaves and Morris, 2012).

The recent industrial control systems are linked with many different institutions and are able to provide, receive and exchange the information. The exchange of information under the physically one-way policy means that there is a discrepancy between the administrative security management system and the practical security management system. There is a problem that the linkages other than the possibly one-way links lack the security management system, so, the security becomes more vulnerable (Cook *et al*., 2016).

In this study, we aimed to separate the intranet areas into the control network intranet and the external network to review the methods of data transmission between the previously suggested areas and to propose methods to efficiently establish the systems through the analysis of the characteristics of the existing data transmission products.

Corresponding Author: Jae-Pyo Park, Department of Information Security, Soongsil University, 07027 Seoul, Republic of Korea

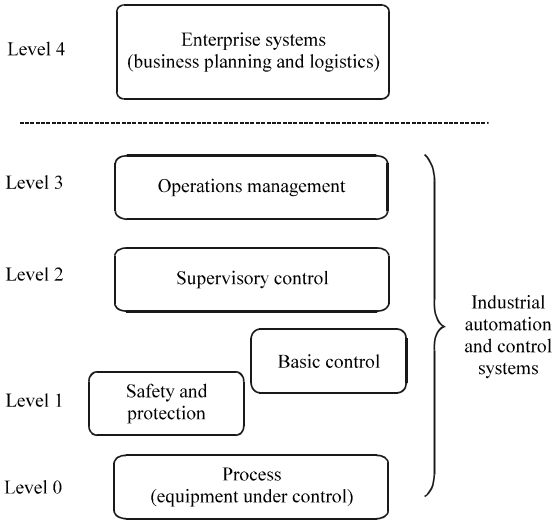

Fig. 1: The standard reference model of industrial control network (ISA99)

Literature review

Industrial automation and control system: The ANSI/ISA (American National Standards Institute) International Society of Automation)-99 series was developed as a cyber security program for the control system and is registered as IEC 62443 series.

- ANSI/ISA-99.01.01-2007 terminology, concept and models
- ANSI/ISA-TR99.01.02-2007 security technologies for industrial automation and control systems
- ANSI/ISA-99.02.01-2009 establish and industrial automation and control program

The ANSI/ISA-99 defines the concepts of zone and conduit for the security of the control network (Anonymous, 2007). The conduit refers to the logical communication asset group protecting the communication channels through the passage of information flow between two zones. The conduits provide security functions for a safe communication between different zones. The ANSI/ISA-99 suggests a reference model that can be used to design security programs for the industrial control network (Byres, 2012). The standard reference model of industrial control network consists of the hierarchical structure, from level 0-4 which is shown in Fig. 1.

In the reference model, level 4 shows the enterprise systems level, level 3 shows the operations management level, level 2 shows the supervisory control level, level 1 shows the local or basic control level and level 0 shows the process level.

MATERIALS AND METHODS

Types of application systems for network zone separation: The physically one-way transmission device consists of a pair of Transmitter (Tx) and Receiver (Rx). The system is designed to have a physical level that allows the data transmission only in one direction and prevents the data transmission in the reverse direction (Oh *et al*., 2015). The physically one-way transmission device can only transfer the data from the intranet to the external network, so, it is physically separated from the network connection. Thus, it has an advantage that the control system is completely protected against the attacks from the external network. However, it also has a shortage that the information about the control and production cannot be provided from the intranet to the control network.

The shared storage-based network connecting device is a multi-zone classification product that controls the real-time service connection data between the secured and unsecured zones and the information flow that exchanges information using the transmission storage. The shared storage-based network connecting device is the inter-server data transmission system suggested during the network separation of the central administrative agencies and most of them have adopted the data transmission method using shared storages (Anonymous, 2015).

In the shared storage-based network connecting device, the external system can only be connected through the proxy of the outer device. Therefore, the network-based attacks cannot reach the intranet, so, the networks can be protected. Also, since, the system uses shared storage, there is an advantage in sending large-sized files while the lack of real-time update could be disadvantageous that the data are stored in the stored in the shared storage before re-transmitted. In addition, the shared storage is constituted at the external proxy device, the internal proxy device and in between the two devices, so, it is easy to separate the internet and the intranet within the same zone but it is difficult to construct the remotely placed networks or the different networks connected through WAN.

The logical one-way transmission network connecting device is the multi-zone classification product that is installed on the physically separated networks or in the secured or unsecured zones separated by the intrusion blocking system to connect the data and services which exchanges the data stored in the internal and external storages to transmit the data (Qian *et al*., 2016; Kim and Yarlagadda, 2015). Like the shared

storage-based network connecting method in the logical one-way transmission network connecting method, the external system is only connected through the proxy of the outer device where the network-based attacks cannot reach the intranet, so, the intranet can be protected. However, the system does not use the shared storage, so, it is difficult to send and receive large-sized data.

The zone separation using the intrusion blocking system is most commonly used to separate the internet and the intranet. The NIST (National Institute of Standards and Technology) SP800-82 and ANSI/ISA99 also use this method to separate the work network and the control network or for the zone separation within the control network (Stouffer *et al*., 2011; Whilhoit, 2013). In the intrusion blocking system, the security policy can be accessed from the internal network to the external network but does not allow the access from the external network to the internal network. Therefore, it has improved security but the application and management of the security policy is difficult in practice. Also, as the connection occurs from the system of the internal network to the system of the external network, the direct influence of from the external system is possible.

RESULTS AND DISCUSSION

Separation of safe industrial control network

Zone separation model of industrial control network: In this study, we defined as in Fig. 2 in accordance with the domestic control network environment, based on the SCADA reference model defined by ISA99 and separated the zones.

The enterprise zone (level 4) is the zone where the in-company tasks are performed using the information related to the control and production and the operations management zone (level 3) is where the integrated central operation and control occurs with respect to the local control network. In the supervisory control zone (level 2), the supervisory control tasks are performed regarding the local control devices and remote control devices. The basic control zone (level 1) is where the basic control tasks are performed with respect to the control devices. The process zone (level 0) is where the control devices are located.

In Korea, the control networks are operated separately from the intranet. The control networks are designed to have the central integrative control center that monitors the nationwide local control network status. Each local branch constitutes the control facilities and the local management system of the facilities as well as the remotely managed control facilities. Table 1 shows the classified zones of the domestic control network.

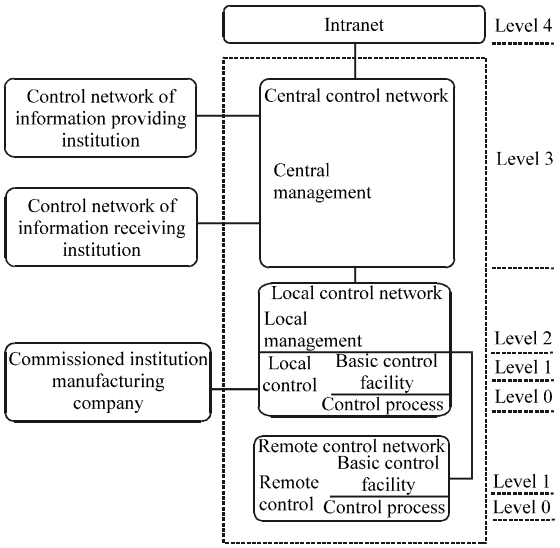

Fig. 2: The separation of the network zone for the control system

Table 1: The classified zones of the domestic control network

Networks	Zone	Level
Intranet	Enterprise zone	4
Central control network	Operations management zone	3
Local control network	Supervisory control zone	2
	Basic control zone	1
	Process zone	0
Remote control network	Basic control zone	1
	Process zone	0

Table 2: The related external institutions (networks) that are connected to the control network

Related institutions	Contents
Information providing institution	The institute that is supplied with the relevant information in case of transmitting the control or production information from the control network to the external network
Information receiving institution	The institute that provides the relevant information in case of receiving the control or production information from the external network and applying it to the control network
Commissioned institution	The institution that deputes the control facilities and relevant operation and receives the control and production information
Manufacturing company	The institution that supplies the control facilities and remotely controls or monitors the production information for the maintenance

The related external institutions (networks) that are connected to the control network can be classified as in Table 2.

The security application model of industrial control network: Regarding the network zone that is separated

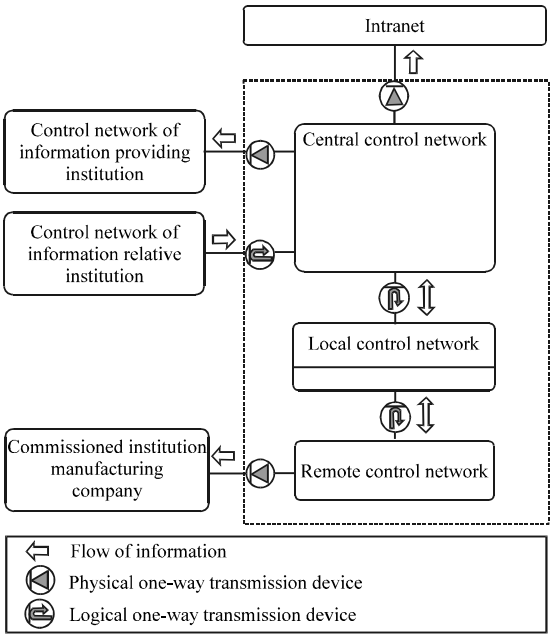

Fig. 3: The security application model of industrial control network

from the industrial control network, the network security application model is defined in accordance with the installation location as in Fig. 3.

If the control network and the inter-company network are connected, the point of connection would be in between the intranet and the central control network and it is the most efficient method to use the physical one-way transmission device in terms of security. The connection between the central control network and the local control network or between the local control network and the remote control network occurs within the control network, so, often people overlook the importance of security. Although, it is within the control network, it is desirable to classify the network in consideration of the control tasks, aerial characteristics and control range and separate the network into subnets.

If the control network and the information provider are connected, the connecting point would in between the central control network and the information provider. Regarding the security, it is the most efficient to use the physical one-way transmission device. When the control network and the information provider are connected, the point of connection will be in between the central control network and the information provider but the access should be from the external institution to the control network, so, it is impossible to use the physical one-way transmission devices. It is more efficient to use the logical one-way transmission device to receive information without allowing the access from the external environment. If the connection is made between the control network and the commissioned institution/manufacturing company, the point of connection would be in between the local control network and the commissioned institution/manufacturing company. In this case, it is the most efficient to use the physical one-way transmission device.

Process for applying the proposed model: In the common cases of network separation, different information systems are mixed, so, it is necessary to identify the information system in accordance with the work zones and adequately locate the information systems in the separated network. On the other hand in the case of the industrial control network, the information systems for the intranet and control network are clearly separated. Therefore, the zone identification and separation should be preceded in terms of the control network intranet and external network. Figure 4 shows the network separation process of the industrial control network.

In the industrial control network, the internal, control and the external networks should be preferentially separated physically to constitute a closed network and consider the connection after the security review when there is a need for inter-network connection service.

The process of the establishment of security system when connecting intranet and external network: Figure 5 shows the process to establish the security system in case of linking the intranet and external network. First, review if the online connection is necessary when linking the intranet and the external network. If the task is unit-base and intermittent an online connection is not required, so, it is desirable to work offline. If the online connection with the control network is necessary, analyze if it is the one-way data transmission out of the control network or the bidirectional or the data supply from the external environment. If it is the one-way data transmission out of the control network, make the connection using the physical one-way transmitter. If it is the bidirectional communication as in the TCP service, review if it can be changed to the one-way data transmission, using UDP or others. If the change to one-way data transmission is possible, newly establish the information system to allow one-way data transmission service and connect using the physical one-way transmitter.

If the change to the one-way transmission is impossible, it is suggested to separately configure the connection between the linked device and the internal network, using the logical one-way transmitter. When the

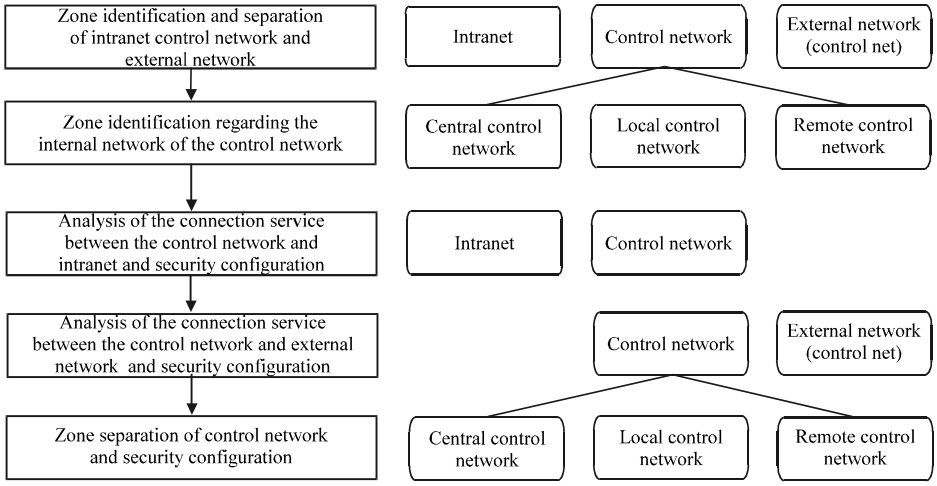

Fig. 4: The network separation process of the industrial control network

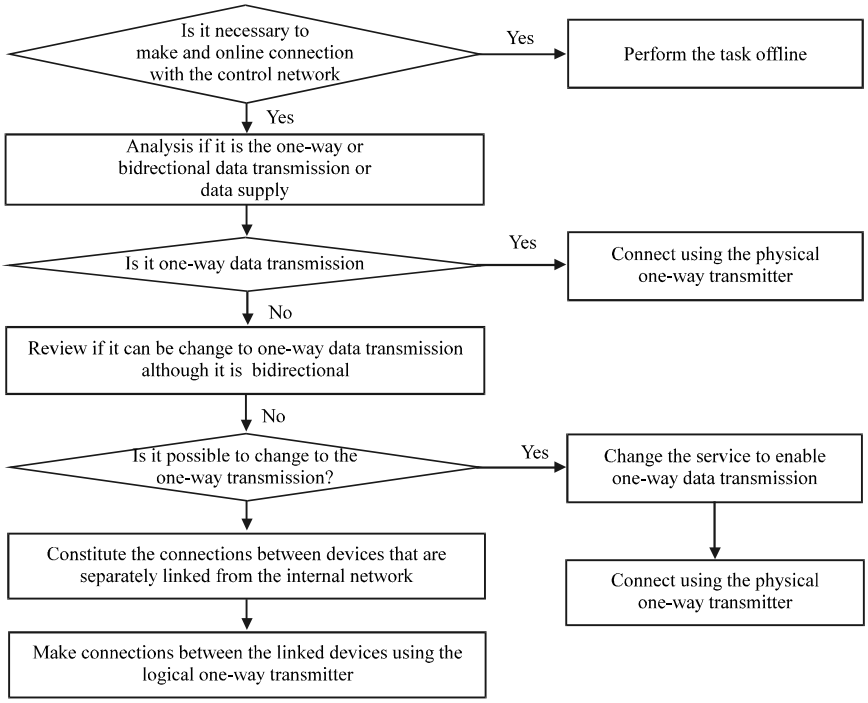

Fig. 5: The process to establish the security system in case of linking the intranet and external network

change to the one-way transmission is possible but if the cost is too high, it is suggested to initially connect using the logical one-way transmitter and for the long-term plan, change the service structure and make a connection using the physical one-way transmitter.

Comparison and analysis of control network separation system: We compared the industrial control network zone separation and security application model proposed in this study with the (Stouffer *et al*., 2011; Byres, 2012) and domestic security policy to verify the security and efficiency of the proposed model. Table 3 shows the overall characteristics of the proposed industrial control network zone separation and security application model and the domestic and overseas security policies in terms of the control network zone separation.

Previous studies or policies have been separating the network into the intranet and the control network or in accordance with the concept of the zone and conduit.

Table 3: The analysis and comparison of control network area separation

Types	Proposed model	NIST SP800-82	ASNI/ISA-99	Domestic policy
Zone classification properties	Zone classification using the zone concept of ISA-99	Classified into intranet and control network	Zone classification using the concept of zone and conduit	Classified into intranet and control network
Applied security model separation	Applied hierarchical security model directed towards the control system	Applied the model of classifying intranet and control network	Applied hierarchical security model directed towards the control system	Applied the model of classifying intranet and control network
Device of main zone	Mixed use of physical one-way transmitter and logical one-way transmitter	Intrusion blocking system	Intrusion blocking system	Physical one-way transmitter
System of connecting with the intranet	Provides the security system establishment process in accordance with the properties of the intranet linking service	Zone separation using the intrusion blocking system	Zone separation using the intrusion blocking system	Recommends one-way structure because the intranet is an external network from the control network
System of connecting with the external network	Provides security establishment process according to the linking properties of external network	Unifies as the external network and separates the zone with intrusion blocking system	Unifies as the external network and separates the zone with intrusion blocking system	Unifies as the external network and recommends only the one-way transmission
System of separating the intranet	Provides the internal network separation of the hierarchical security model	No internal network separation system	Provides the internal network separation of the hierarchical security model	Provides the internal network separation under the regular IT environment

However, in this study, we classified the zones using the zone concept from ISA-99. Also, for the main zone separation devices, previous studies could only apply the intrusion blocking system or the physical one-way transmitters. However, this study separated the zones using the physical one-way transmitter and the logical one-way transmitter together. Therefore, in terms of the linkage system with the intranet, previous studies separated the zones using the intrusion blocking system or recommended the one-way system with the concept of considering the intranet as an external network but in this study, we could provide the security system establishment process according to the service properties with the linkage with the intranet.

CONCLUSION

This study separated the zones of industrial control networks and proposed a security application model as an efficient system for managing the security of the industrial control network. In terms of the zone separation of the industrial control network, the concept of level 0-4 whichwas defined in ISA-99 was applied and it was hierarchically defined as the intranet, central control network, local control network and remote control network. Also, in terms of the external connection network, the information providing institution network and information receiving institution network were defined as the external networks that are linked to the control network and the commissioned institutional network and the manufacturing company network as the external networks that are linked to the local control network, according to the properties of each network. As the security application model in terms of the industrial control network, we proposed the security systems for the following connection points: between the intranet and central control network between the central control network and local control network, between the local control network and remote control network between the central control network and the information providing institution between the central control network and the information receiving institution network and between the local control network and the commissioned institution/manufacturing company network.

If the commercial security systems provided in the form of physical one-way transmitters and logical one-way transmitters are further developed, it is expected that they could be more flexibly applied to the industrial control security model proposed in this study.

REFERENCES

Anonymous, 2007. Security for industrial automation and control systems part 1: Terminology, concepts and models. Scribd Inc, San Francisco, California, USA.

Anonymous, 2015. Recommended practice: Improving industrial control system cybersecurity with defense-in-depth strategies, industrial control systems cyber emergency response team. Department of Homeland Security, Southwest, Washington, USA.

Byres, E., 2012. Using ANSI/ISA-99 standards to improve control system security. Tofino Security, Lantzville, British Columbia.

Cook, A., R.G. Smith, L. Maglaras and H. Janicke, 2016. Measuring the risk of cyber attack in industrial control systems. Proceedings of the 4th International Symposium on ICS & SCADA Cyber Security Research (ICS-CSR 2016), August 23-25, 2016, BCS Publishing, Belfast, Northern Ireland, BCS Publishing, Belfast, Northern Ireland, UK.,-pp: 23.

Kim, Y.H. and P. Yarlagadda, 2015. Design considerations for reliable data transmission and network separation. J. Appl. Mech. Mater., 738: 1146-1149.

Morris, T.H. and W. Gao, 2013. Industrial control system cyber attacks. Proceedings of the 1st International Symposium on ICS & SCADA, Cyber Security Research, September 16-17, 2013, University of Leicester, Leicester, England, UK., pp: 22-29.

Oh, Y.C., M.R. Han, Y. Shin and J.B. Kim, 2015. A study on the communication agent model for one-way data transfer system. Intl. J. Smart Home, 9: 161-168.

Qian, S., V. Tervo, J. He, M. Juntti and T. Matsumoto, 2016. A comparative study of different relaying strategies over one-way relay networks. Proceedings of the 22th European Wireless Conference on European Wireless, May 18-20, 2016, VDE, Oulu, Finland, ISBN:978-3-8007-4221-9, pp: 1-6.

Reaves, B. and T. Morris, 2012. An open virtual test bed for industrial control system security research. Intl. J. Inf. Secur., 11: 215-229.

Stouffer, K., J. Falco and K. Scarfone, 2011. Guide to Industrial Control Systems (ICS) security. MBA Thesis, US Department of Commerce, National Institute of Standards and Technology, Gaithersburg, Maryland, USA.

Whilhoit, K., 2013. Who's really attacking your ICS equipment?. Trend Micro, Shibuya, Tokyo, Japan.