

A Study of Cyber Security Policy in Industrial Control System using Data Diodes

Boo-Sun Jeon, Jung-Chan Na

Cyber Security Research Division,

ETRI(Electronics and Telecommunications Research Institute), South Korea

bsjeon@etri.re.kr, njc@etri.re.kr

Abstract— The security of industrial control systems has been a big topic by the Stuxnet case in 2010. As a solution which can solve these requirements, data diode has emerged.

A data diode is a computer security device that restricts the communication along a network connection between two computers so that data can only be transmitted in one direction. This enables a more sensitive or highly classified computer network to receive data directly from a less secure source while prohibiting the transmission of data in the opposite direction. In this paper, we describe data diode applied into industrial control system, after reviewing the commercial product, we address the various ways to apply a data diode in ICS and future works

Keywords— ICS, Cyber Security, Data Diode, One-Way, Unidirectional Communication.

I. INTRODUCTION

Industrial control system (ICS) is a computer based system which are typically used in nation-wide critical infra-structure facilities such as electrical, gas, water, wastewater, oil and transportation. In addition, ICS is essentially used in industrial application domain to effectively monitor and control the remotely scattered systems. [1]

The security of industrial control systems has been a big topic by the Stuxnet case in 2010, for preventing Industrial Control System from cyber-attack threat, it is best way to air-gap(separate) internet line into control network and cooperative network. But, in this separated network environment, the need for network connection from safety zone to Unsafety Zone has been requested for monitoring systems

In the past, Firewall and SW based technologies were used for solving this problems. But these technologies have problems such as security vulnerability and low performance.

Then, One-way(unidirectional) Security Gateway recently emerged for preventing cyber-attack with high performance. One-way Security Gateway is connected only one-way, reverse direction is even physically blocked. It called Data Diode.

A data diode is a computer security device that restricts the communication along a network connection between two computers so that data can only be transmitted in one direction. This enables a more sensitive or highly classified computer

network to receive data directly from a less secure source while prohibiting the transmission of data in the opposite direction.[2]

In this paper, we describe data diode applied into industrial control system, after reviewing the commercial product, we address the various ways to apply a Data Diode in ICS and future works.

II. ONE-WAY COMMUNICATIONS

One-way Communication means that the transmission of data flows one direction. One-way communication consists of a Unidirectional Security Gateway for send and a Unidirectional Security Gateway for receive. The most common design of data diode relies on Ethernet optical fiber-based standard connectivity.

The send node only transfer the data through Unidirectional Security Gateway and the receive node only transfer the data through Unidirectional Security Gateway.

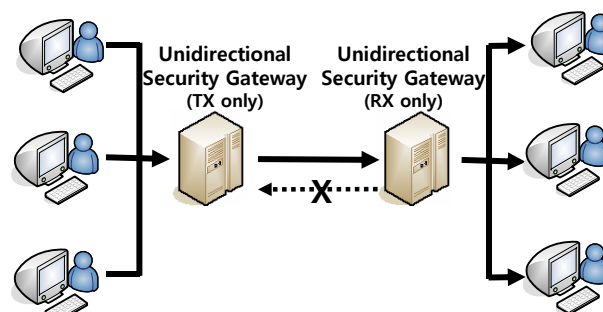


Figure 1. Unidirectional Security Gateway

For this, the end to end protocol such as TCP communication that use handshaking protocol can't be applied and UDP communication usually be used.

However, UDP communication doesn't guarantee that the date received safely, the reliability of the transmission can't be sure.

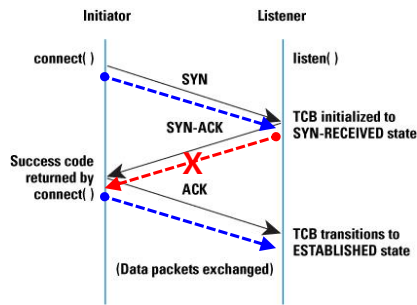


Figure 2. 3-way handshaking impossible

In response, various studies are being conducted to improve data reliability in one-way communication.

Among them, one-way communication gateway divided into two. The one is Data Pump that the data is transmitted in one-way but control signal such as acknowledgement, error information, resend request, and so on is transmitted in both-direction. And the other is Data Diode that is more strict one-way communication without allowing both-direction communication of control signal[3].

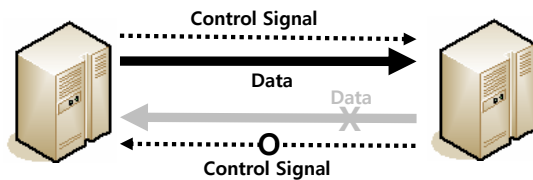


Figure 3. Data Pump

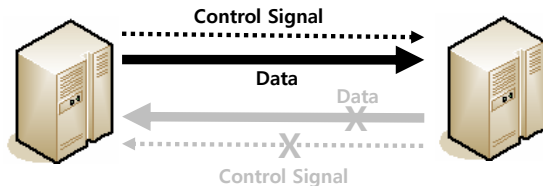


Figure 4. Data Diode

The big difference of Data Pump and Data Diode is whether control signal can be transmitted in reverse direction. Data Diode that can't transmit control signal is more safe in intrusion prevention from the outside, but has disadvantage in the data reliability[4]. In this paper, we call both of Data Pump and Data Diode to Data Diode.

Data Diode provides Application Proxy because application using in ICS usually use two-way communication such as TCP. The role of Proxy is internally transmitting function for one-way communication, externally emulating two-way communication. There are various proxy such as TCP Proxy, UDP Proxy, FTP Proxy, Modbus Proxy, the application area is determined depending on which proxy is provided for each product.

III.COMMERCIAL PRODUCTS OF DATA DIODE

Presently, the market has been released various Data Diode product.

A. Owl Dual Diode

Owl Computing in USA uses Dual Diode Technology® for hardware-enforced one-way data transfer. All data application types are supported including Historian Replication, Streaming Full Motion Video, Scanned File, and SMTP email systems.

Dual Diode supports up to 10Gbps, Industry protocol such as Modbus, file delivery, TCP/UDP packet delivery service etc. and CC certification is received EAL4[5].

B. Waterfall Unidirectional Security Gateway

Waterfall Unidirectional Security Gateways of Waterfall Security Solutions Ltd. in Israel provide reliable two-way communication agent technology through content filtering, data verification mechanism using unique one-way protocol. This gateway provides standard SCADA protocols such as ICCP, Modbus, NDP3, FTP, up to 1Gbps. CC certification is received EAL4+[6]

C. Interactive Link Data Diode Device

Interactive Link Data Diode Device(IL-DDD) of BAE Systems Inc. in the UK supports unidirectional transfer of files, streaming data, and email including attachments. The solution converts data into sequenced UDP packets that are then transferred across the Data Diode device. Once received, the UDP broadcast is reconverted back to its original format. The solution includes TCP support as well.

In each version ensures service performance of 100Mbps to 1Gbps. The IL-DDD is to the highest levels of assurance in each of the following schemes: CC EAL7+, UCDMO(Unified Cross Domain Management Office) Baseline, DSD(Australian Defence Signals Directorate) High Assurance, ITSEC(Information Technology Security Evaluation Criteria) E6.[7]

D. Fox Data Diode

The Fox DataDiode of Fox-IT Inc. in Netherlands is a turn-key solution that enables transfer and sharing of files/folders, UDP streaming, transfer of e-mail, time synchronization using NTP and transfer of monitoring data. Transfer of files or replication/mirroring of folders works via standard protocols: FTP, sFTP, FTPs, CIFS/SMB, and SCP. By supporting a variety of protocols, customer's needs and interoperability of systems can be ensured.

Also, Modbus, DNP3, IEC or OPC data is received by the proxy on the ICS-network, transmitted to the proxy on the corporate network where it is propagated or made available. It ensures the file transfer performance of 100Mbps and the UDP data transfer performance of 800Mbps.

The Fox DataDiode has a CC EAL 7+ certificate and it is listed in the NIAPC(NATO Information Assurance Product Catalogue) and is approved for use up to and including Nato Secret (NS).[8]

TABLE 1. COMMERCIAL PRODUCTS

Company	OWL (US)	Waterfall (Israel)	BAE Systems (UK)	Fox-IT (Netherlands)
Product Name	DualDiode	Unidirectional Security Gateways	Interactive Link Data Diode Device (IL-DDD)	Fox Data Diode
Bandwidth	10Gbps	100Mbps	1Gbps	800Mbps
Supported Service	File Transfer, Modbus, TCP, UDP, Historian, PI, OPC	File Transfer, OPC, ICCP, Modbus, DNP3, Historian, DB Replication.	File Transfer, SMTP, UDP, TCP, Streaming Data	File Transfer, SMTP, CIFS, UDP, NTP, Modbus, DNP3, OPC, ICCP
Certification	CC EAL4	CC EAL4+	CC EAL7+, DSD, ITSEC E6	CC EAL7+, NATO SECRET

In addition, there are various products such as Cyber-Diode of Genua in Germany, NEXOR Data Diode of NEXOR in the UK, SINA One Way Gateway of Secunet in Germany, and so on.

IV. APPLY POLICY DATA DIODE

Data Diode is usually used for transferring data between two network that each network has different security level. Data Diode needs to prevent system from outside's intrusion and improve reliability of data transmission.

In traditional TCP communication, when some packet was lost, TCP guarantee data integrity by resending lost packet. Though Data Diode can't resend data directly, there are various research for solving this issues. We will introduce some of them as follows.

A. Simple One-way Communication

First is the case of simple one-way communication. It generally use UDP communication for data transfer and it is applicable when application doesn't need high data reliability or integrity.

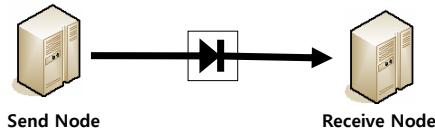


Figure 5. Simple One-way Communication

B. Bilateral Communication using Multiple Data Diodes

This policy relates to a bilateral data transfer system comprising a first node, a second node, a first one-Way link for unidirectional transfer of first data from the first node to the second node, a second one-Way link for unidirectional transfer of second data from the second node to the first node, a first data transfer application for administering the unidirectional transfer of the first data from the first node to the second node via the first one Way link, and a second data transfer application for administering the unidirectional transfer of the second data from the second node to the first node via the second one-Way link.[9]

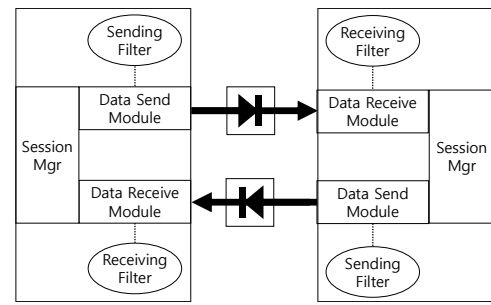


Figure 6. Bilateral Communication using Multiple Data Diodes

This method provides two-way communication with two of one-way transmission module. In the one-way transmit module and receive module, they have Filter for transferring only pre-defined data.

C. Control Signal transmission by Feedback Node

The three nodes are interconnected with each other by a one-way data link, and the Feedback Node is designed solely for processing and relaying data verification information from the Receive Node to the Send Node.

Receive Node verify data integrity by comparing hash information of received data. When error occurs, send this information to Feedback Node, Feedback Node send this information to Send Node. Then Send node detect data transmission error and re-send the data.[10]

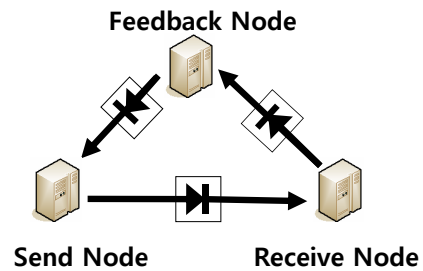


Figure 7. Control Signal transmission by Feedback Node

This method has a big advantage actively to resend the data that was error by receiving control signal such as transmission error information.

D. Using the Control Signal Memory

This policy uses separate one-way control link for sending control signal such as transmission success or fail.

This control link send only small size of control signal.

The send node save received control signal into separate Control Signal Memory. Control Signal Memory can be written in Data Receive Module of receive node and Control Signal Send Module of send node. Also, Control Signal Memory can only be read in Control Signal Send module of receive node and Data Send Module of send node.[11]

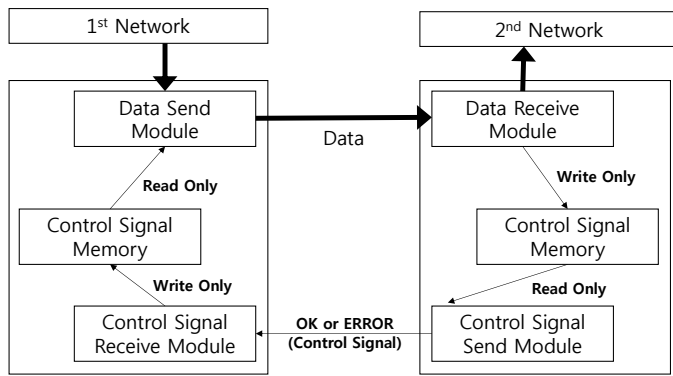


Figure 8. Using Control Signal Memory

E. Policy for applying the Forward Error Correction(FEC)

In the one-way transmission, it is not possible retransmission about transmission error basically, it is the policy to correct transmission error at the receiving node.

Forward error correction (FEC) is a technique used for controlling errors in data transmission over unreliable or noisy communication channels. The central idea is the sender encodes the message in a redundant way by using an error-correcting code.[12]

There are various algorithms of FEC such as Hamming Code, Turbo Code, Reed-Solomon, LDPC, RaptorQ, and so on.

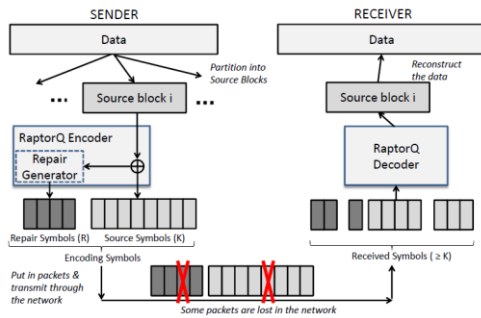


Figure 9. Sample of FEC : RaptorQ FEC[13]

The send node creates Repair Symbols to correct errors and transmits them. When the error occurs, the receive node can corrects the error by FEC decoding using additional information such as Repair Symbol and Source Symbol.

V. CONCLUSIONS

Through Stuxnet in 2010, the security of the industrial control system has become a big issue. Data Diode has been emerged from the need for solving such a security problem.

In this paper, we described Data Diode that provide a one-way communication physically. We also analyse the commercial products that are currently available on the market and the various techniques that can be applied to the actual ICS.

In the future, we will carry out our research on the retransmission mechanism to ensure reliability of the one-way data transmission by minimizing impact on transmission performance.

ACKNOWLEDGMENT

This work was supported by the ICT R&D program of MSIP/IITP. [R0126-15-1095, Unidirectional Security Gateways developments in cyber-physical systems]

REFERENCES

- [1] Do-yeon Kim, "Vulnerability Analysis for Industrial Control System Cyber Security", *The Korea Institute of Electronic Communication Sciences* 9(1), p137-142, Jan, 2014.
- [2] STEVENS, Malcolm W.; POPE, M. "An Implementation of an Optical Data Diode". *DSTO*, 1999.
- [3] L. Pietre-Cambacedes and P. Sitbon, "An analysis of two new directions in control system perimeter security" [Data diodes and Layer 8 security] *Proceedings of the 3rd SCADA Security Scientific Symposium (S4)*, pp. 4.1–4.30, January 2009.
- [4] R.T. Barker and C.J. Cheese, "The application of data diodes for securely connecting nuclear power plant safety systems to the corporate it network", *7th IET International Conference on System Safety, Incorporating the Cyber Security Conference*, Issue 607 CP, October 2012
- [5] Dual Diode, Owl Computing Technologies, Inc. http://www.owlcti.com/products/products_applications.html
- [6] Waterfall's® Unidirectional Security Gateways, <http://www.waterfall-security.com/technology/>
- [7] Data Diode Solution, BAE Systems Inc., <http://www.baesystems.com/en/product/data-diode-solutiontrade>
- [8] Fox Data Diode, Fot-IT Inc., <https://www.fox-it.com/datadiode/>
- [9] Owl Computing Technologies, Inc., "Bilateral Communication using Multiple One-way Data Links", *United States Patent, Patent No.:US2013/0097283 A1*, Apr. 2013.
- [10] Owl Computing Technologies, Inc., "One-Way Data Transfer System with Built-In Data Verification Mechanism", *United States Patent, Patent No.:US7675867*, Mar.2010
- [11] Korean electric power corporation (KEPCO), "One-way Data Transmission System", *Republic of Korea Patent, Patent No.: 10-1334240*, Nov.2013.
- [12] Forward Error Correction from Wikipedia, https://en.wikipedia.org/wiki/Forward_error_correction
- [13] Jos'e Lopes and Nuno Neves, "Stopping a Rapid Tornado with a Puff", *35th IEEE Symposium on Security & Privacy*, 2014.



BooSun Jeon was born in South Korea in 1975. She received the B.E., M.E. degree in Computer Science from Chungnam National University, Seoul, Korea, in 1998, 2000, respectively. She joined Electronics and Telecommunications Research Institute(ETRI), Daejeon, Korea, in 2000. She is currently a senior researcher of Cyber Security Research Division. Her main areas of research interest are Network Security and ICS Security.



JungChan Na was born in South Korea in 1962. He received B.S. degrees in Calculation of Statistics from Chungnam National University in 1986, and He received M.S. degrees in computer engineering from Soongsil University in 1989, respectively. He also received Ph.D degree in Computer Science from Changnam National University in 2004. He joined Electronics and Telecommunications Research Institute(ETRI), Daejeon, Korea, in 1989. He is the leader of the Industrial Control System(ICS) Security Research Section. Currently, his main areas of research interest are Network Security and ICS Security.