Transactions of the Korean Nuclear Society Virtual Spring Meeting
July 9-10, 2020

Data Packet Backtracking in Digital System Network

Dongil Lee [a*], Kwang-Hyun Lee [a], Wonwoong Ko [a]
[a]*KHNP, Central Research Institute, 70, 1312-gil, Yuseong-daero, Yuseong-gu, Daejeon, 34101, South Korea*
[*]*Corresponding author: diturtle@khnp.co.kr*

1. Introduction

Most power plant systems are undergoing a transition from analog to digital.

Unlike analog systems, digital equipment delivers most of the control, measurement, and information signals using networks.

In the control system, the soundness and response time of information and measurement signals are very important. Therefore, it is considered very important when designing a system.

In the Operation & Maintenance (O&M) phase, network delays occur due to signal delays and process delays, despite being perfectly designed.

Data packet backtracking is needed to identify the cause of network delays and to find vulnerabilities to improve the system and analyze the cause.

In this paper, I will describe the experiences of backtracking of digital systems excluding safety class.

2. Network Environment and Backtracking of Data Packets

This chapter describes the power plant's non-safety network environment, and describes the environment configuration for data packet backtracking.

2.1 Network Configuration

In digital system, embedded systems or programmable logic controllers (PLCs) are responsible for measuring and controlling field signals, and servers and switches arbitrate network data. The following figure is a simplified diagram of the information network and control network of the Korean-type APR1400. [1]

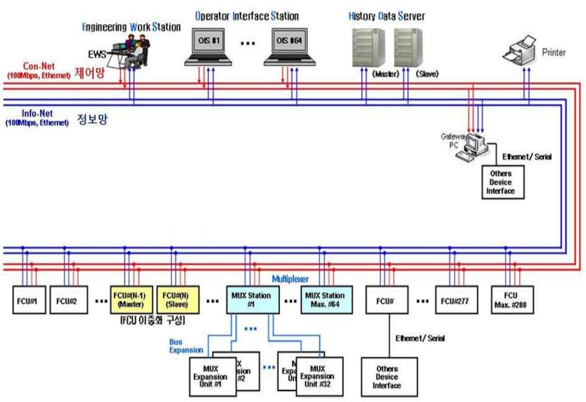

Fig. 1. Non-Safety network structure

The foreign-type APR1400 consists of a control network and an information network.

2.2 Data Packet Data and Environment in Networks

The more data you have, the better. In particular, it is good to have information about the packet. And it's even better if you have network routing information.

However, it is difficult to find this information in the field. This is because a lot of information is not disclosed due to the intellectual property rights of the design / production company.

To trace a packet back, you need to figure out the specific pattern of the packet. If there is a lot of encryption in the packet, it will not be possible to trace it.

Fortunately, the power plant is made up of closed networks, so it is highly unlikely that data packets will be encrypted.

In addition, there is a high possibility of not encrypting raw data that can place a load on the CPU (Central Processing Unit) due to restrictions such as response time, which are very sensitive to signal delay.

2.3 Analysis Devices Composition

Network data is divided into transmission / reception (TX / RX), but half-duplex is used instead of full-duplex. Therefore, it is necessary to utilize equipment that can acquire data separately by transmitting/receiving or mirroring data. In addition, computers must be used to acquire and analyze data packets.

2.3.1 Data Packet Acquisition Device

1) TAP device : Continuously monitors packets transmitted on the network
2) Intelligent Hub: Analyzes and controls all data in the network management system (for packet aggregation and synchronization of switch and TAP device)
3) Two (2) computers for packet acquisition and analysis with wireshark (open source packet analysis program) installed

2.3.2 Configuration for data packet acquisition

As shown in the following figure, TAP and Intelligent HUB are installed in an existing system. In addition, the Switch mirrors a specific port for data packet acquisition.

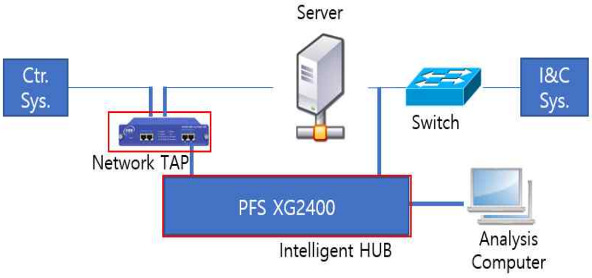

Fig. 2. Data packet measurement devices composition

2.4 Data pattern analysis method

2.4.1 Wireshark data acquisition

Data acquired through mirroring of the switch and data acquired with the TAP device are synchronized through the Intelligent Hub to generate a log file pcap file with Wireshark and converted to a cvs file for analysis.

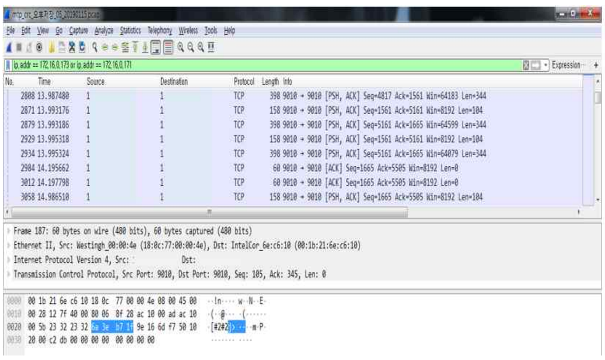

Fig. 3. Wireshark acquisition data

2.4.2 Search for a specific pattern

Extract specific patterns from manual or system

2.4.3 Packet time comparison in a specific section

Time delay interval estimation and cause analysis through comparison of the log time of data packets for the control system, server, and specific point of the field systems

2.4.4 Packet Acquisition Constraints

1) Although there is no time delay for TAP device, Switch, and Intelligent Hub in theory, it is difficult to completely exclude them (almost no effect)
2) In order to record and synchronize a specific control signal (operator's operation or automatic operation), it is necessary to review by adding an offset to the time record

3. The Data Packet Traceback Results

As a result of tracking a specific pattern, the data packet satisfies within the response time requirement, and a slight difference occurs due to wire delay or delays such as TAP, HUB, and Switch.

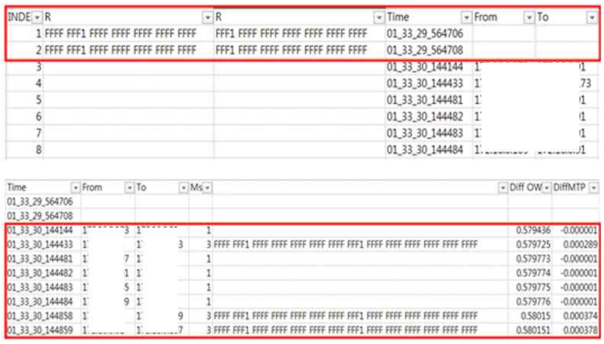

Fig. 4. Comparison result of standard input/output time of data pattern

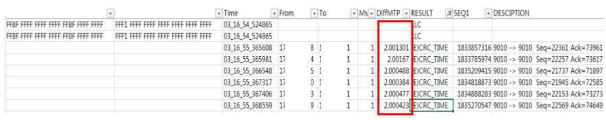

Fig. 5. Time Error due to measurement devices and wire delay (within 0.1 μs)

4. Conclusions

Backtracking data packets in a network requires a lot of time and effort, especially when not knowing the packet information.

During the O&M phase, many errors and unexpected situations occur. In digital power plants, it is very difficult to determine the cause.

Backtracking of network data packets will be a very important method for analyzing the unexpected causes of power plants.

The method proposed in this paper is expected to be very helpful in proving the integrity of networks and systems and analyzing the cause of unexpected malfunctions.

REFERENCES

[1] M. G. Min, Verification of failover effects from distributed control system communication networks in digitalized nuclear power plants, NET-49-5-11, 2017