# Conceptual Design Approach to Implementing Hardware-based Security Controls in Data Communication Systems

Ahmad Salah Ibrahim, Jaecheon Jung*
*Department of NPP Engineering, KEPCO International Nuclear Graduate School*
*1456-1 Shinam-ri, Seosaeng-myeon, Ulju-gun,Ulsan, 689-882, KOREA*
**Corresponding Author: jcjung@kings.ac.kr*

## 1. Introduction

In the Korean Advanced Power Reactor (APR1400), safety control systems network is electrically isolated and physically separated from non-safety systems data network. Unidirectional gateways, include data diode fiber-optic cabling and computer-based servers, transmit the plant safety critical parameters to the main control room (MCR) for control and monitoring processes. The data transmission is only one-way from safety to non-safety. Reverse communication is blocked so that safety systems network is protected from potential cyberattacks or intrusions from non-safety side. [1, 2]

Most of commercials off-the-shelf (COTS) security devices are software-based solutions that require operating systems and processors to perform its functions. Field Programmable Gate Arrays (FPGAs) offer digital hardware solutions to implement security controls such as data packet filtering and deep data packet inspection. [3, 4]

If the gateway server failed, MCR operators could not monitor or display the plant performance. The availability of gateway server could be compromised by the act of potential cyberattack or intrusion. [5] This paper presents a conceptual design to implement hardware-based network security controls for maintaining the availability of gateway servers.

## 2. Methods and Results

Design approach is to implement a network security perimeter with hardware-based security functions to control and manage the data traffic between the redundant safety channel gateway servers and the non-safety data network (DCN-I). The proposed design utilized the static data packet filtering and deep inspection functions together to protect the gateway servers from unauthorized traffic and malicious contents. Fig. 1 illustrates the proposed security perimeter.

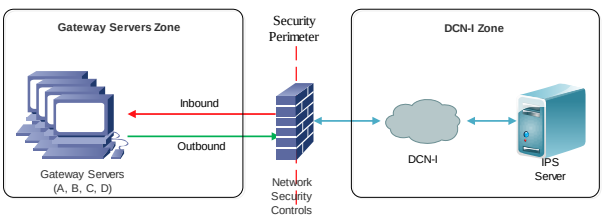


Fig. 1. Network Security Controls Perimeter.

### *2.1 Design Conception*

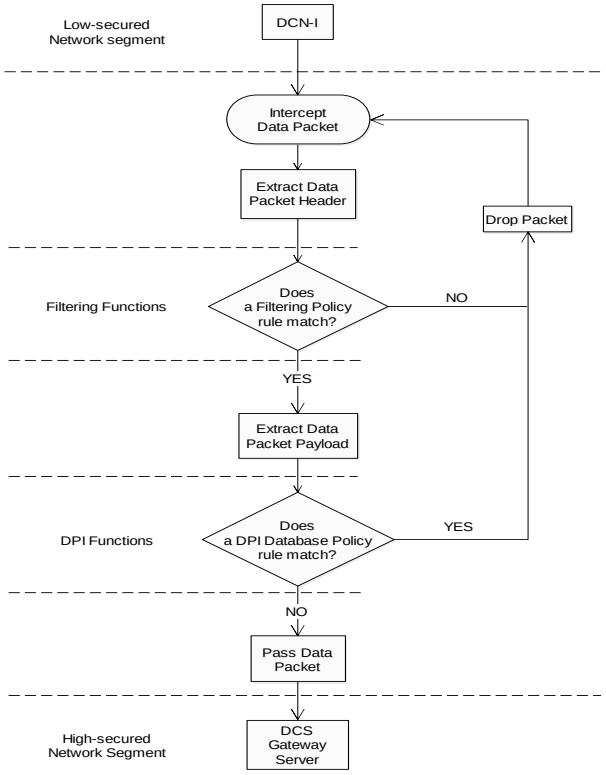


Fig. 2 Design Functional Flowchart

Fig. 2 shows the flowchart of proposed design functions. When the security perimeter control device receives a data packet, the filtering functions extract data packet header fields (e.g., source and destination IP addresses, and source and destination UDP port numbers). The extracted header fields are compared to a predefined static ruleset policy. The ruleset policy is configured as 'permit' rules to only allow the authorized traffic. If a rule is matched, the deep packet inspection (DPI) functions extract the data packet payload message looking for malicious contents. If all permit rules are not matched. The security control device will drop the whole packet and receives the next one.

The DPI functions inspect the packet payload message thoroughly looking for a malicious pattern or intrusion code string. DPI policy functions are based on database of known attack patterns or signatures that have been already detected. Denial-of-service (DoS) attacks including distributed DoS (DDoS) attacks are to

affect the gateway server availability where periodic safety critical data transmission to MCR could be disrupted. The security perimeter device differentiates between normal data traffic and DoS traffic by looking for known attack patterns. If a pattern is matched, the security control device will drop the malicious packet and alert the event.

As shown in Fig. 2, the security control device only perform filtering and DPI functions for the inbound traffic (i.e., from DCN-I to gateway servers which is the on-demand traffic). The DCN-I is considered low-secured network zone while the gateway servers subnetwork is considered high-secured trusted zone. The outbound traffic (i.e., periodic traffic) originates from the trusted zone, so that there is no need to deeply inspect its packet payloads. When the security device receives an outbound data packet, the filtering unit will permit it to pass without performing the DPI functions. It is strongly recommended to configure the static filtering ruleset so that all permit rules for all outbound traffic are executed first, then followed by all permit rules of inbound traffic.

### *2.2 Results*

The proposed design concept of security perimeter controls has been modelled and simulated using model-based systems engineering (MBSE) software tools. The logical architecture was developed using enhanced function flow block diagrams (EFFBDs) to simulate the behavior of functions flow. The simulation results showed that the logical architecture performed intended design functions. Fig. 3 shows the EFFBD of proposed design.

## 3. Conclusions

A conceptual design of hardware-based network security controls was discussed in this paper. The proposed design is aiming at utilizing the hardware-based capabilities of FPGAs together with filtering and DPI functions of COTS software-based firewalls and intrusion detection and prevention systems (IDPS). The proposed design implemented a network security perimeter between the DCN-I zone and gateway servers zone. Security control functions are to protect the gateway servers from potential DoS attacks that could affect the data availability and integrity.

Future work will focus on verification and validation of proposed design by developing FPGA prototype to emulate the security controls. Emulation will be accomplished using VHDL programming software and Digilent Basys 2 Xilinx Spartan-3E board.

## Acknowledgment

This work was supported by the 2016 Research fund of the KEPCO International Nuclear Graduate School (KINGS), Republic of Korea.

## REFERENCES

[1] KEPCO and KHNP, APR1400 Design Control Document Tier 2, “Chapter 7 Instrumentation and Controls”, Revision 0, December 2014.
[2] E. Knapp et al., “Industrial Network Security”. Second Edition, Elsevier Inc., 2015.
[3] A. Kayssi et al., “FPGA-based Internet protocol firewall chip”, The 7th IEEE International Conference on Electronics, Circuits and Systems, 2000.
[4] Tran et al., “A FPGA-based deep packet inspection engine for Network Intrusion Detection System”, 9th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2012.
[5] J. C. Jung and I. S. Choi, “Lecture on DCS Gateway Server Design and Function”, I&C Design Project Lab., KEPCO International Nuclear Graduate School, July 2016.

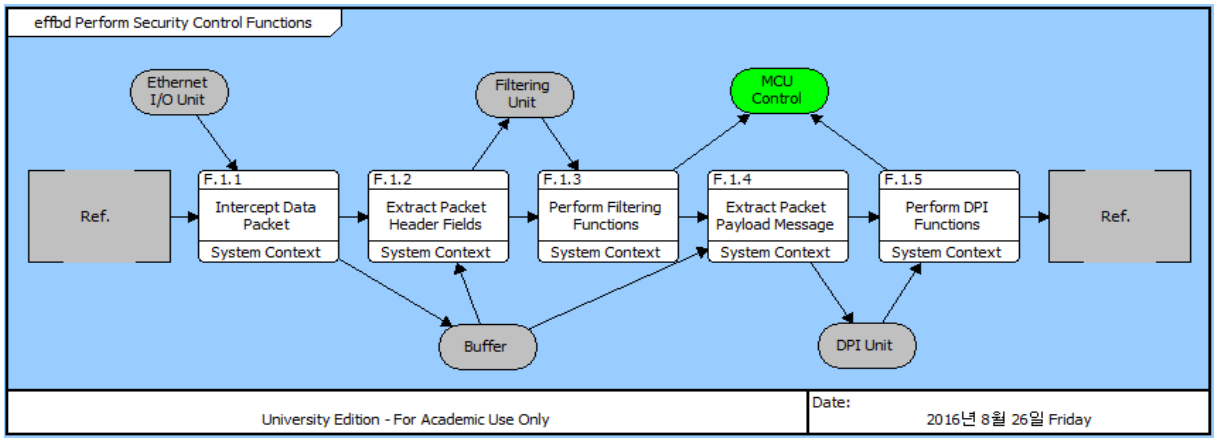


Fig. 3. EFFBD of Proposed Security Control Functions