Journal of KOSSE. (2016. 12) Vol. 12, No. 2 pp. 101-114
DOI: https://doi.org/10.14248/JKOSSE.2016.12.2.101
www.kosse.or.kr

ISSN (print) : 1738-480X
ISSN (online) : 2288-3592

A Systems Engineering Approach to Implementing Hardware Cybersecurity Controls for Non-Safety Data Network

Ahmad Salah Ibrahim, Jaecheon Jung*

Department of NPP Engineering, KEPCO International Nuclear Graduate School

Abstract : A model-based systems engineering (MBSE) approach to implementing hardware-based network cybersecurity controls for APR1400 non-safety data network is presented in this work. The proposed design was developed by implementing packet filtering and deep packet inspection functions to control the unauthorized traffic and malicious contents. Denial-of-Service (DoS) attack was considered as a potential cybersecurity issue that may threaten the data availability and integrity of DCS gateway servers. Logical design architecture was developed to simulate the behavior of functions flow. HDL-based physical architecture was modelled and simulated using Xilinx ISE software to verify the design functionality. For effective modelling process, enhanced function flow block diagrams (EFFBDs) and schematic design based on FPGA technology were together developed and simulated to verify the performance and functional requirements of network security controls. Both logical and physical design architectures verified that hardware-based cybersecurity controls are capable to maintain the data availability and integrity. Further works focus on implementing the schematic design to an FPGA platform to accomplish the design verification and validation processes.

Key Words : APR1400; Data Communication Network, Cybersecurity, Denial-of-Service; Model-based Systems Engineering

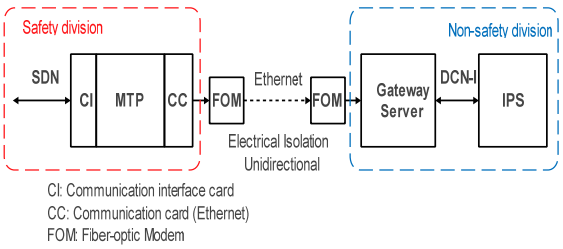
Received: October 28, 2016 / **Revised**: October 29, 2016 / **Accepted**: November 30, 2016

* Corresponding Author : Jaecheon Jung, jcjung@kings.ac.kr

1. Introduction

Data communication systems in APR1400 mainly encompass safety systems data network (SDN) and non-safety systems data communication and information network (DCN-I). Unidirectional gateways and data diodes (e.g., fiber-optic modems) are serving as network security zones allowing data transfer from the safety to the non-safety networks and block the reverse communication path. Figure 1 illustrates the concept of network isolation and separation using data diodes. [1]

Unidirectional gateway server is a non-safety related system. It protects the safety critical digital systems from unauthorized access. The gateway server is computer-based, its availability could be compromised if a potential cyberattack initiated from the non-safety side. The unavailability (i.e., system failure or malfunction) of gateway server does not prevent the safety systems from performing its intended functions. The failed gateway server could not supply the real-time status of plant performance which causing a Loss of View (LoV) event. Cyberattacks maliciously affect the availability, integrity, and confidentiality of data and systems. In this paper, hardware-based network security controls are implemented to maintain the availability and integrity of gateway server data transmission for monitoring and display processes.



[Figure 1] Safety to Non-safety Data Transfer

In this paper, the systems engineering (SE) approach focused on the reverse and re-engineering processes. The proposed design logical architecture was modelled and simulated by Vitech CORE9 software to develop a model-based systems engineering (MBSE) approach. MBSE model simulates the behavior of Security Controls functions flow. Enhanced function flow block diagrams (EFFBDs) were developed to verify that system design functions will be executed in the intended process.

PART I: Reverse Engineering Process

2. Stakeholders Needs Analysis

According to the 2015 ICS-CERT Year in Review Report, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) received and responded to 295 cyber incidents. The critical manufacturing sector accounted for 97 of these incidents, while the energy sector accounted for 46 and nuclear sector had 7 incidents. 22 of these incidents were observed as high-level intrusion that infected critical systems. (DHS, 2015) [2]

Recently, most of cyberattacks target the critical infrastructure, specifically the industrial control systems (ICS). Although the DCS gateway server is not a safety-related or important-to-safety system, but if compromised, by a malicious action, it would adversely prevent the MCR operators from monitoring the plant performance. Denial-of-service (DoS) is a potential cyberattack that could disrupt the gateway server availability. [3]

In this paper, the measure of effectiveness (MOE) is defined as the robustness of the

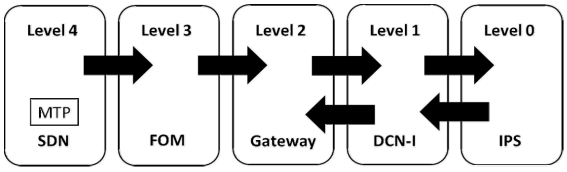
proposed design against cybersecurity issues. Robustness is defined as the ability of a system to cope with errors during operation and cope with erroneous input due to malicious action or cyberattack. In other words, a robust system is able to transfer data in a cyberattack-free environment. Robustness can be measured by the availability, integrity, and confidentiality of data and systems. In this paper, system availability and data integrity are the selected measures of performance (MOPs). System availability is defined as maintaining the system to perform its intended function and communicate over a network. Data integrity is defined as maintaining the consistency, accuracy and trustworthiness of data transmitted over a network.

A cybersecurity program, with strict policies, is required to protect the digital instrumentation and control (I&C) systems as a part of the site physical protection program. Developing, implementing or maintaining a cybersecurity plan is out of scope of this paper. Scope of this paper focuses on developing a physical hardware-based perimeter of security controls to protect the redundant channel DCS gateway servers and maintains its availability against cybersecurity issues.

3. System Requirements Analysis

3.1 Regulatory Requirements

Based on U.S.NRC 10 CFR 73.54 and RG-5.71 regulations [4, 5], a cybersecurity program must be implemented into the site physical protection program to protect the critical digital assets (CDAs), including digital computers, communication systems and networks, against



[Figure 2] APR1400 MMIS cybersecurity defensive architecture

cyberattacks that adversely compromise the CDA availability, data integrity or data confidentiality. A cybersecurity plan should comply the regulatory requirements to achieve high assurance for digital systems, which are related-to-safety, security and emergency preparedness (SSEP) functions, are protected against cyber-attacks that would act to modify, sabotage, or compromise the integrity or confidentiality of data or software as well as the availability of system itself.

Defense-in-depth protective strategies must be implemented with various levels of security to guarantee the diversity of security functions, protect, detect, respond to, and recover from cyberattacks. Figure 2 shows APR1400 MMIS cybersecurity defensive architecture that conformed to RG-5.71

Regarding the RG-5.71, the defensive architecture shows that CDAs associated with safety-related and important-to-safety systems that, if compromised, would adversely impact the safety functions, are allocated at levels 4 and 3. Only one-way communication is allowed from level 4 to level 3 and from level 3 to level 2, so that the digital I&C safety systems are physically protected from a cyberattack that would be initiated from the non-safety network. It is impossible to initiate a communication from the non-safety network because the safety network is physically separated and

electrically isolated by a unidirectional fiber-optic cabling systems (i.e., fiber-optic modems) where high-side (at the safety network) is transmit-only and its low-side (at the non-safety network) is receive-only.

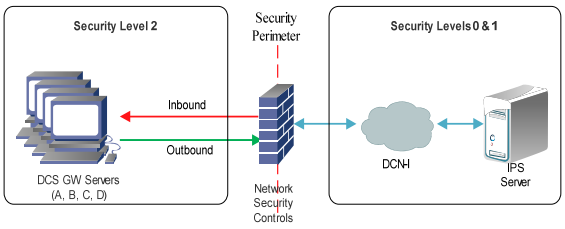
Data is transferred from one level to another through security control functions that enforce predefined polices and rules to monitor the data transfer between each security level (i.e., security zone, network perimeter or conduit). Those security devices (e.g., firewalls, intrusion detection and preventions systems, etc.) maintain the capability of detecting, preventing, delaying, mitigating, and recovering from cyberattacks. The security level (or criticality) of the security zone dictates the degree of security that is required, consequently, it determines which security device that shall be implemented to monitor, detect, and block malicious packets of data that could be initiated from unauthorized access (i.e., a cyberattack).

The current data network architecture does not implement a security perimeter between the DCN-I network and the redundant safety channels gateway servers which make the gateway servers as potential targets for a cyberattack or intrusion if initiated from the DCN-I. Network segmentation allows implementing a security perimeter between two security zones (i.e., subnetworks). One security zone includes servers and computers and is categorized as low-secured zone, while the other includes the redundant safety channels gateway servers as a high-secured or trusted zone.

3.2 Performance and Functional Requirements

The data traffic of current gateway server depends on cyclic redundancy check (CRC) algorithm for data error detection and correction. Nowadays cyberattacks are developed using much more advanced and sophisticated pieces of malicious software and codes that the current level of security is not robust enough to prevent them. It is required that the implemented security device shall maintain the DCS gateway server availability as well as data integrity.

According to NERC CIP 005 standard [3], both firewall filtering functions and network intrusion detection and prevention system (NIDS/NIPS) functions are used to implement security devices between zones. Data packet filtering manages and controls what type of data packets are allowed to pass through the security zone. The data packet headers are filtered by enforcing its ruleset policy. Only legitimate traffic can pass through, while the unauthorized traffic will be blocked based on static filtering ruleset policy. The NIDS/NIPS, on the other hand, perform deep packet inspection (DPI) by deeply check and inspect the payload contents (and possibly the header also) of allowed traffic packets in order to detect malicious content based on known attack signatures (or patterns) database. Use of both inspection methods (i.e., header filtering and payload DPI) achieves the principle of defense-in-depth. The DPI functions focus only on inspecting the contents of allowed traffic



[Figure 3] Network Security Controls Perimeter

through the filtering functions. Figure 3 illus-trates the proposed security controls perimeter.

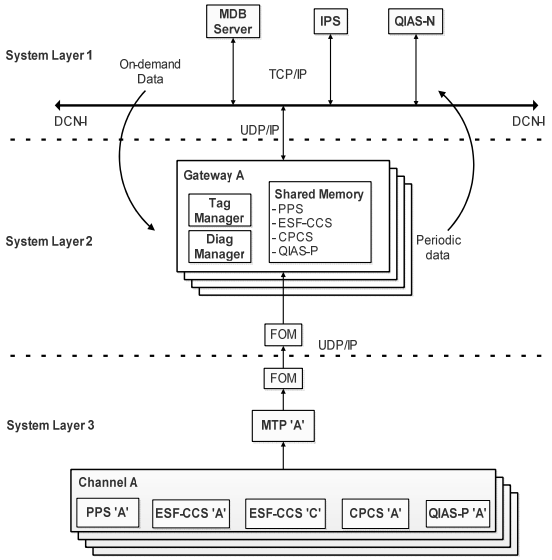
4. DCS Gateway Server Description

The safety data network (SDN) interconnects the plant safety critical digital control systems. Safety control systems are to maintain the reactor in a safe and reliable operation mode. MMIS is to monitor and control the plant operating performance.

Figure 4 shows that the safety operating parameters are transferred from the shared Maintenance and Test Panel (MTP) of each safety channel to the non-safety Information Processing System (IPS), Qualified Indication and Alarm System-Non safety (QIAS-N), and the main database (MDB) server via unidi-rectional data diodes. IPS and QIAS-N are to monitor critical safety and non-safety parameters; QIAS-N satisfies principle of diversity when the IPS fails.

DCS gateway server receives, processes, and forwards safety parameters data from MTP to IPS and QIAS-N periodically via UDP/IP Ethernet communication. On-demand UDP/IP Ethernet communication is initiated in case of requesting monitoring or status data from the gateway server by the main control room (MCR) operators. The size of periodic data packet, sent by DCS gateway server, depends on data type (e.g., monitoring, status, etc.). [6]

DCS gateway server is a computer-based system. It works in Microsoft Windows operating system environment. There are no cybersecurity controls to maintain the availability of gateway servers in case of a cyberattack initiated from



[Figure 4] Channel-A Gateway Server functional block diagram

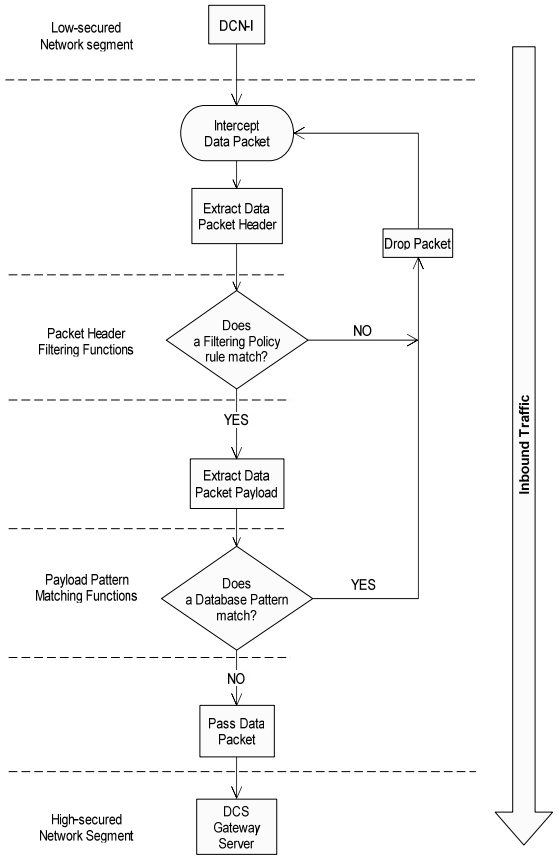
the non-safety network. Even though DCS gateway server is non-safety system, it is crucial to transmit the plant performance to the MCR operators.

PART II: Re-Engineering Process

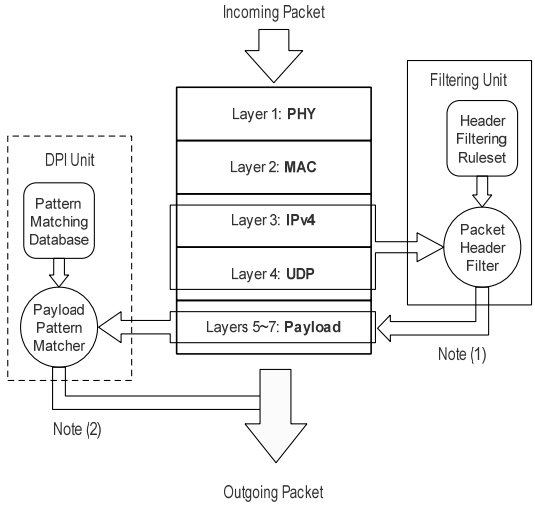
5. Design Methodology

5.1 Design Concept

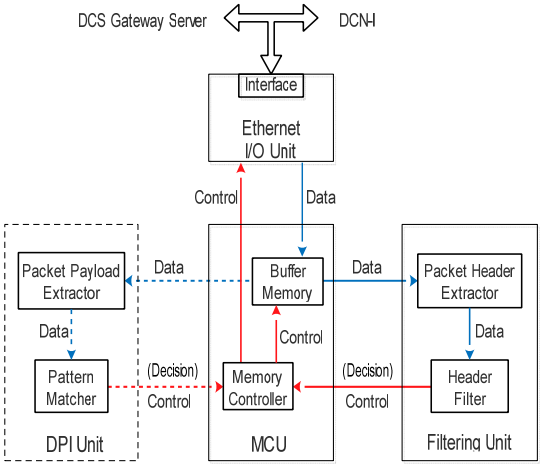
As shown in Figure 5, when the MCR operators request data for monitoring the status of safety functions, an on-demand UDP/IP connection is established from the DCN-I originating from IPS, QIAS-N, or MDB. The Security Controls intercept the inbound data traffic packet by packet looking for unauthorized traffic and/or malicious contents. First of all, the data packet header fields (i.e., source and destination IP addresses, and source and destination UDP port numbers) are extracted for performing filtering functions. The extracted fields are compared to the predefined ruleset policy to



[Figure 5] Security Controls Functional Flowchart (Inbound traffic)



[Figure 6] OSI Model Layers to be controlled



[Figure 7] Security Controls Block Diagram

permit or deny specific traffic based on a static filtering policy. If a filtering policy permitting rule (e.g., ALLOW rule) is matched, the filtering task will be accomplished and the allowed data packet will be forwarded to perform the DPI functions. But if the filtered data packet does not match any of the permitting rules, the default policy rule (i.e., DENY rule) takes place, the filtering functions will drop the whole data packet, log this event, and alert it. [7, 8, 9, 10]

The allowed data packet moves forward to perform the DPI functions. Data packet payload message is thoroughly scanned byte by byte looking for known malicious exploit pattern or signature string. A predefined database of patterns or signature strings for known cyber-attacks or intrusions that already have been detected. If a DPI policy pattern or signature is matched, the whole data packet will be dropped, logged, and alerted. The Security Controls functions only allow the legitimate data packet that does not match any attack pattern or signature. Once the DCS gateway server receives that data packet, Security Controls will perform the same procedures to authorize and/or deeply inspect the next data packet.

Figures 6 and 7 show the specified OSI model layers to be controlled and Security Controls

block diagram respectively. When an inbound traffic is transmitted from DCN-I to the DCS gateway server (e.g., the on-demand data traffic), the Ethernet I/O Unit intercepts the received data packet at the Ethernet interface and writes to the Memory Control Unit (MCU) buffer. The packet header fields are extracted by the Filtering Unit to be scanned and inspected for unauthorized traffic. Filtering functions compare the incoming packet header fields to the constraints that applied to each rule. The ruleset policy hardware blocks are cascaded to the order of its intended execution. The static filtering ruleset policy is arranged at the order of executing all the ALLOW rules first, and if a match does not exist, the DENY rule will be enforced as the last and default rule.

Note (1): If any one of ALLOW rules does not match Layers 3~4 information (Packet Header), then the packet is dropped (Unauthorized Traffic); else the packet is deeply inspected.

Note (2): If any one of database patterns matches Layers 5~7 information (Packet Payload), then the packet is dropped; else the packet is allowed to pass.

If the packet header does not match any ALLOW rule and the DENY rule is matched, the MCU will instruct the Ethernet I/O Unit to drop the data packet, log and alert the event. MCU will clear the buffer memory to receive the next data packet. In case of an ALLOW rule is matched, the Filtering Unit will not execute the following rules and the decision is made upon the matched rule. The MCU notify the buffer to write its content to the DPI Unit. The data packet payload message is extracted to be thoroughly scanned and inspected for malicious content (e.g., attack pattern or exploit string). In a similar concept as that of filtering ruleset policy, DPI functions compare the payload message to the pattern database constraints that are applied to each rule of the DPI policy. In contrast to the filtering actions, the DPI database policy rules are set to drop the whole data packet if a match exists. If a pattern rule is matched, the DPI Unit will notify the MCU which in turn will instruct the Ethernet I/O Unit to drop the data packet, log and alert the event, and clear the buffer to receive the next data packet. If the payload message does not match any rule of the DPI policy, the MCU will instruct the Ethernet I/O Unit to pass the data packet to its destination (i.e., the DCS gateway server).

The Security Controls serves as a security perimeter that divides the non-safety network to two segments, the trusted network which includes the four redundant safety channels gateway servers, and the low-secured network which includes the remaining interconnected servers and workstations of DCN-I (e.g., IPS, QIAS-N, and MDB). As a trusted security zone, the outbound traffic originates from the DCS gateway server to the DCN-I network (i.e., the periodic data traffic) is not subjected to be thoroughly inspected by the DPI Unit and directly reaches its destination providing the periodic traffic of safety parameters data for monitoring and display processes.

As soon as the Security Controls Ethernet I/O Unit intercepts the outbound data packet and writes to the buffer. The packet header fields are extracted and match that assigned ALLOW rules of the filtering ruleset policy. The inbound and outbound traffics are subjected

<Table 1> Given Network Socket Number

For DCN-I interconnected systems and servers			
System	IP address	Port number	Protocol
IPS	192.168.1.10	50001	UDP
QIAS-N	192.168.1.20	50002	UDP
MDB	192.168.1.30	50003	UDP
For redundant channel DCS gateway servers			
Ch. A GW	10.0.1.10	50000	UDP
Ch. B GW	10.0.1.20	50000	UDP
Ch. C GW	10.0.1.30	50000	UDP
Ch. D GW	10.0.1.40	50000	UDP

to the same static ruleset, so that it is strongly recommended to arrange the ALLOW rules for outbound traffic as the top of filtering ruleset policy. The Filtering Unit notifies the MCU which in turn instructs the Ethernet I/O Unit to pass the data packet to its destination (i.e., the DCN-I), as well as it clears the buffer to receive the next data packet.

As shown, DPI Unit block and connections are dashed lines to illustrate that the DPI functions will be executed only if the packet is allowed by the Filtering Unit.

For more explanation, the following tables illustrate how the data traffic is exchanged between the DCN-I and DCS gateway servers security zones. Upon the assumed inputs given by table 1, the static filtering policy ruleset is given by table 2.

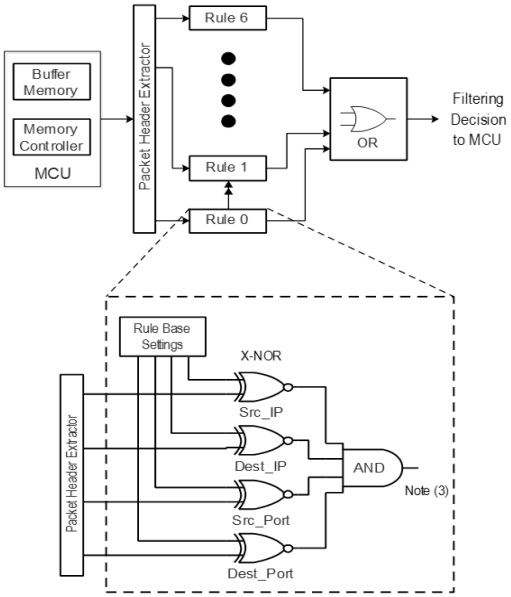
As shown above, the static filtering ruleset policy is a fixed configuration that is not changed or modified from session to another. In table 2, the first four ALLOW rules show that periodic data traffic originating from the gateway servers subnetwork is directly forwarded to its destination. Rules 4, 5, and 6 are the ALLOW rules for inbound traffic (i.e., on-demand) where only allowed to be deeply

<Table 2> Static Filtering Ruleset Policy Upon Given Inputs

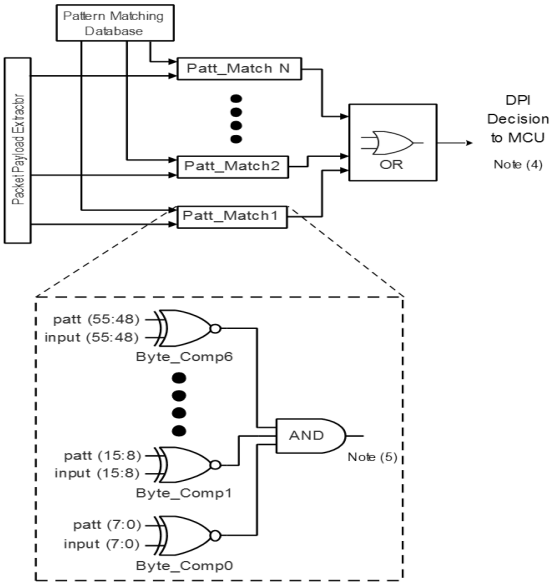
Comment	GW_A	GW_B	GW_C	GW_D	IPS	QIAS-N	MDB	Default Rule
Action	ALLOW	ALLOW	ALLOW	ALLOW	ALLOW	ALLOW	ALLOW	DENY
Direction	OUT	OUT	OUT	OUT	IN	IN	IN	Any
Service	UDP	UDP	UDP	UDP	UDP	UDP	UDP	Any
Destination	Any	Any	Any	Any	Any	Any	Any	Any
Source	10.0.1.10:50000	10.0.1.20:50000	10.0.1.30:50000	10.0.1.40:50000	192.168.1.10:50001	192.168.1.20:50002	192.168.1.30:50003	Any
No	0	1	2	3	4	5	6	7

inspected for malicious content by DPI Unit. Being allowed or authorized traffic does not make the incoming inbound data packet valid to pass through the subnetwork of gateways. In this case, the DPI Unit decides if that packet is malicious or not. A database of known DoS attack signatures is compared to the packet payload data, if a pattern or exploit string is matched, the Security Controls drops the data packet and log it. The DENY rule is executed as the last and default policy rule as the incoming data packet is definitely un-authorized.

Figure 8 shows that how packet headers are filtered. Each filtering policy rule is implemented in a single hardware block, so we have 7 hardware blocks for the rules 0 ~ 6, while the default rule (performed as the last rule if any ALLOW rule was not matched), is executed as a control signal from MCU to Ethernet I/O Unit for dropping the packet. A rule hardware block



[Figure 8] Filtering Unit Block Diagram



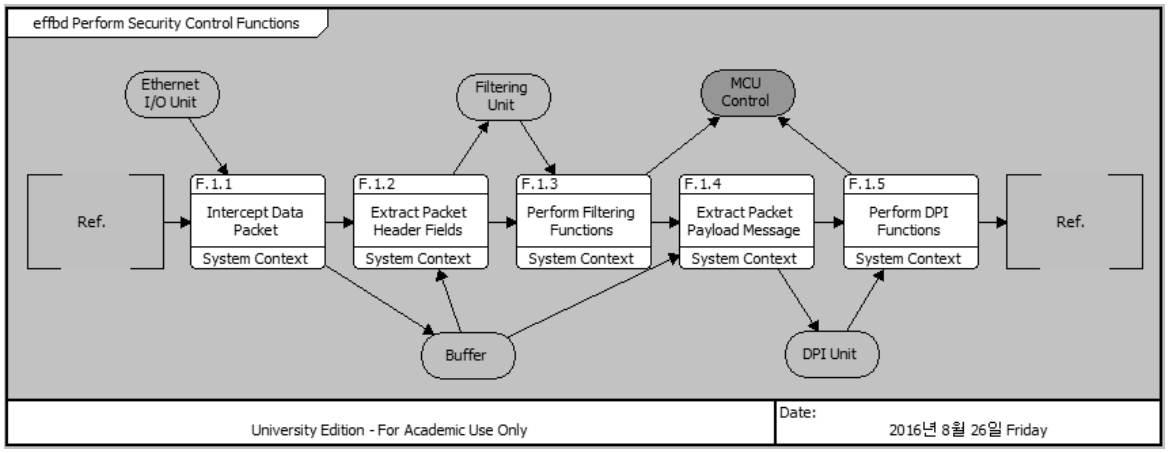
[Figure 9] DPI Unit Block Diagram

is basically consisted of X-NOR logic comparators to fulfil the ALLOW rules. The rules are implemented to be performed in the order as in table 2. Once a rule is matched, the filtering unit does not perform the next rules and builds its decision upon the matched rule. If any rule is not matched, the default decision is made by the MCU to drop the packet.

The Filtering Unit executes the first rule 'Rule 0', if it is not matched, the next rule 'Rule 1' is executed and so on till a rule match exists (transition from one rule to the next rule is indicated with the double-headed arrow). Packet header extractor is to write the header fields from the buffer memory to specified comparator inputs in order to compare them with the rule base settings, each rule block has 4 comparators (source IP address, destination IP address, source port number, and destination port number). The outputs of all comparators are ANDed to create the rule match flag (matched = logic '1', unmatched = logic '0').

Figure 9 shows the pattern matching process for payload inspection. Each pattern matcher inspects the payload contents by comparing to predefined database of well-known detected attacks. Each pattern matcher is specified for specific pattern or signature string code, there are hundreds of detected attacks patterns with different sizes of string data. Each pattern matcher consists of number of byte comparators equal to the size of pattern string. The packet payload extractor to write the payload contents from the buffer memory to the input of byte comparators. All pattern matchers process the payload contents simultaneously and once a pattern match exists, the DPI Unit instruct the MCU to drop the packet (Figure 9, note 4).

As shown in Figure 9, the selected pattern matcher (Patt_Match1) insists of byte 7 comparators (numbered from 0 to 6) to inspect the packet payload byte-by-byte against the 7-byte pattern string. The payload extractor is type of First-In-First-Out (FIFO) memory



[Figure 10] Security Controls EFFBD by Vitech CORE9 (1st level)

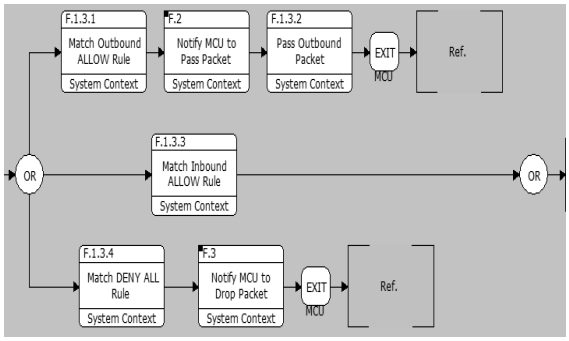
so that the pattern matching logic is repeated in such a way that all possible byte alignments are scanned. The outputs of all byte comparators are ANDed so that if a match is detected, the pattern matcher create the pattern match flag (matched = logic '1', unmatched = logic '0') as shown in figure 9 (Note 5)

The Security Controls design was verified by developing the logical architecture. Next section discusses the results of modelling and simulating the MBSE approach.

5.2 Design Modelling Using CORE9

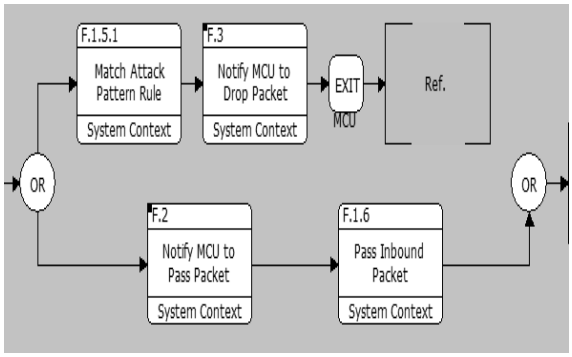
Using Vitech CORE9 [11] MBSE tools, the behavioural logical architecture of Security Controls functions was represented by enhanced function flow block diagrams (EFFBDs). Figure 10 illustrates the Security Controls EFFBD diagram based on the design flowchart and block diagram illustrated in figures 5, 6 and 7 respectively.

The behaviour of functions flow was executed based on the Select construct branch probability. It means that the branch with highest selection probability will be executed irrespective the



[Figure 11] Filtering Functions EFFBD (2nd level)

remaining branches with lower selection probabilities. As shown in figure 10, the selection probabilities for both Filtering and DPI Select constructs are set to represent the behavioural flow of Security Controls functions if only a legitimate data packet received at the Ethernet I/O Unit. It means that the selection probabilities are set higher for executing function branches of the Security Controls to pass the allowed packet considering its direction (i.e., inbound or outbound). Figure 10 shows first level of depth while second level of depth for performing filtering and DPI actions are illustrated in figures 11 and 12 respectively.



[Figure 12] DPI Functions EFFBD (2nd level)

5.2 DPI Modelling Using Xilinx ISE

Using Xilinx ISE software [12], a 7-byte string pattern matcher was modelled using 7 byte comparators. Based on figure 9, each byte of data packet payload is scanned for finding a match with the pattern string, the data payload bytes are retrieved byte*by-byte from an output of a First-In-First-Out (FIFO) memory so that all byte alignments are scanned and inspected against the pattern string.

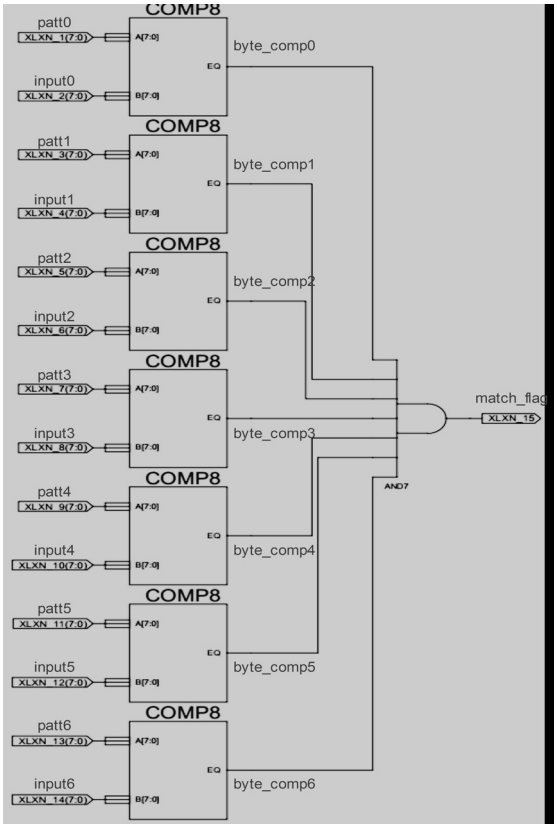
Figure 13 shows a DPI pattern matcher based on X-NOR logic gates comparators.

6. Results and Discussion

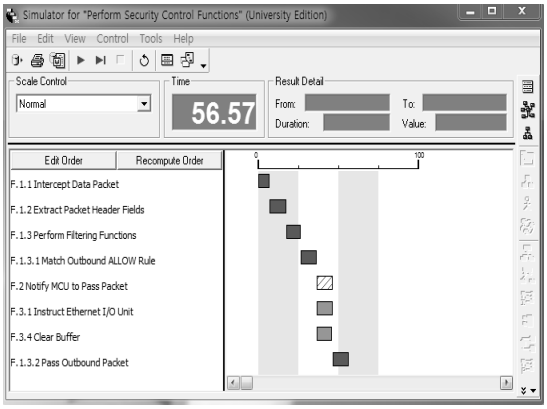
6.1 CORE9 Simulation Results

Using COREsim, simulation timelines were generated based on the intended function to be performed by Security Controls with specific selection probabilities. The behavioural function flow of Security Controls in cases of passing outbound traffic, passing legitimate inbound traffic, blocking unauthorized inbound traffic, and blocking malicious inbound traffic are illustrated in Figures 14, 15, 16, and 17 respectively.

As shown above, the simulation timelines verified that the design logical architecture

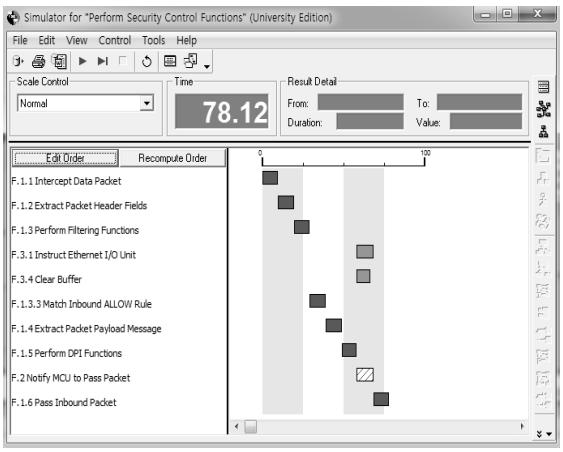


[Figure 13] DPI Pattern Matcher using Xilinx ISE

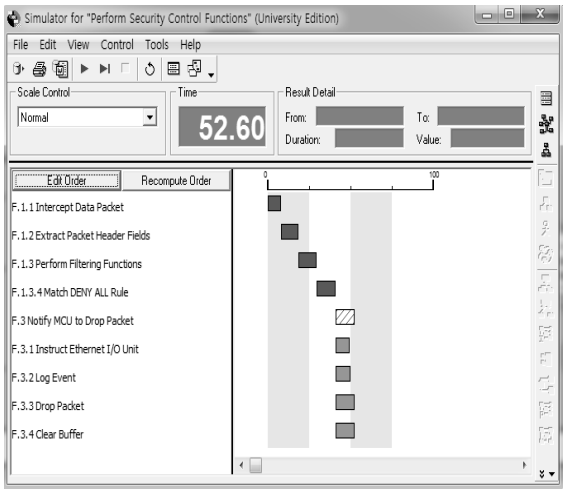


[Figure 14] Simulation Timeline of Passing Outbound Packet

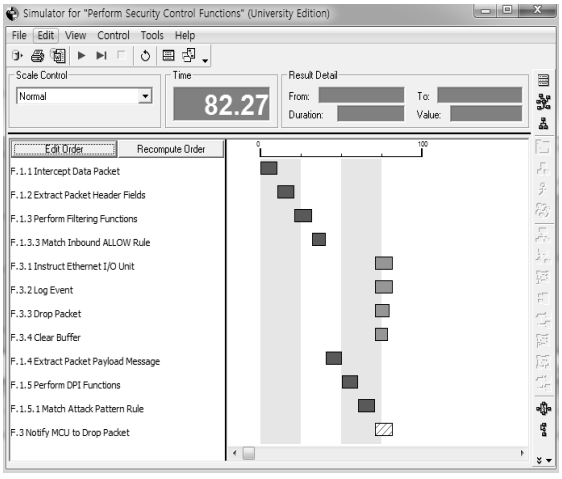
introduced the intended behaviour of Security Controls design. In timeline, the teal-coloured events represent the flow of data packet when executing the specified functions depending on assigned Security Controls policies. While the bright green-coloured events represent control



[Figure 15] Simulation Timeline of Passing Inbound Packet



[Figure 16] Simulation Timeline of Blocking Unauthorized Packet



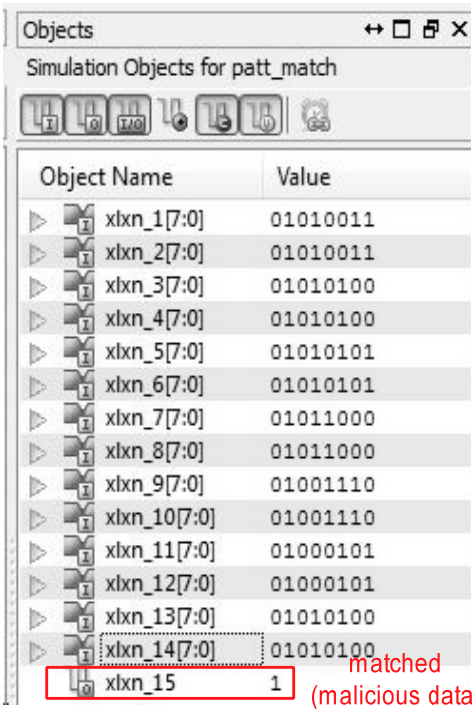
[Figure 17] Simulation Timeline of Blocking Malicious Packet

signals originating from Filtering or DPI units to MCU in order to instruct the Ethernet I/O Unit about passing or dropping the data packet, and clearing the buffer to receive the next data packet.

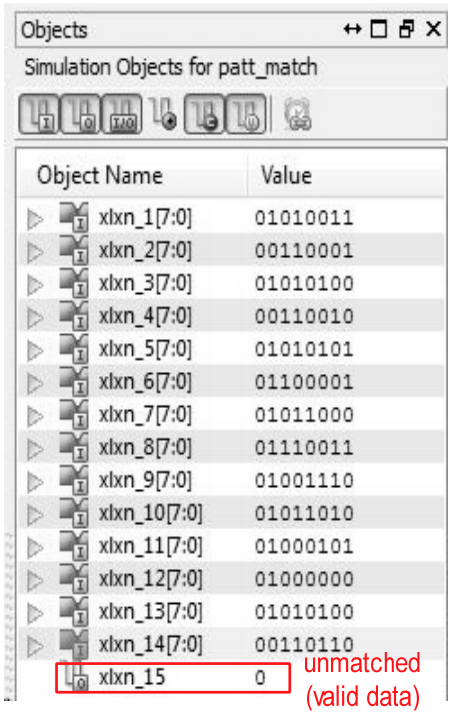
The simulation time is non real-time and dimensionless, it represents the relative time units established by each function specification settings. In this paper, the simulation time was maintained as the COREsim default settings. In the real physical design, FPGAs are capable to handle and process large data traffic at timely manner.

6.2 Xilinx ISE Schematic Simulation

If the data input is matched with the pattern string, then the *match_flag* output is '1' which mean that a match exists and the packet will be dropped because it is malicious; else the



[Figure 18] Malicious Data Matched with the Pattern



[Figure 19] Valid Data Unmatched with the Pattern

data packet will be passed is the *match_flag* output is '0' where there is no match and data is valid.

Figures 18 and 19 shows the simulation results from Xilinx ISE showing matched status and unmatched status respectively.

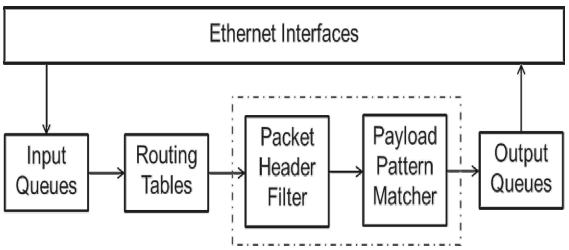
7. Conclusion and Further Work

Hardware-based network security controls were developed in this paper using the systems engineering approach. Reverse and re-engineering processes have been performed. Stakeholders needs and system requirements analyses were conducted to determine the measures of effectiveness and performance of the proposed design. In this work, a network security perimeter was implemented between the non-safety network and the redundant safety channel DCS gateway servers to maintain the availability and integrity of data transmission for monitoring and display processes. Security Controls design included filtering and deep data packet inspection functions to control and block the unauthorized and malicious data transfer. The developed design is hardware-based to ensure the cyber-security of DCS gateway servers as well as not affect the network performance. Static filtering ruleset policy and database of known cyberattack signatures were together used to control the inbound data traffic coming from DCN-I so that a potential intrusion could be prevented. Denial-of-service attack was considered the potential intrusion to disrupt the data availability and integrity.

The design logical architecture was modelled and simulated by Vitech CORE9 software. The behavioural function flow of Security Controls was simulated using EFFBD diagrams. Simulations timelines verified the behaviour of logical architecture to perform the intended functions. The hardware-based DPI function (i.e., pattern matching) was developed and modelled using Xilinx ISE software. Simulation results verified the DPI matching functions.

Further works focus on building an FPGA-based prototype to validate the functionality of network cybersecurity access controls. The validation phase includes developing a hardware description language (HDL) code using VHDL programming language, implementing the code to FPGA board, and testing in an IPv4 Ethernet network-based environment. Mitigation of the denial-of-service attack (DoS and DDoS) is the limitation for this work as considered as one of the major cyber intrusions to affect data systems availability and integrity.

NetFPGA project [13] provides an open source



[Figure 20] Placement of Cybersecurity Controls Modules in NetFPGA Platform

hardware and software platform designed for research. The platform encompasses a Virtex II Pro FPGA development system providing IPv4 router and Ethernet switch with four RJ45 Ethernet network ports. The reference HDL code can be reconfigured so that the two sub-networks (i.e., DCN-I and redundant channel gateway servers) can be configured in the routing table. Filtering and DPI functional modules can be inserted between the routing table outputs and output queues as shown in figure 20.

Acknowledgement

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. US Department of Homeland Security, NCCIC/ICS-CERT. Year in Review FY 2015. [Cited 2016 July 20] Available from: https://ics-cert.us-cert.gov/
3. E. Knapp et al., "Industrial Network Security", Second Edition, Elsevier Inc., 2015.
4. U.S.NRC 10 CFR 73.54, "Protection of digital computer and communication systems and networks" [Last update: 2015, December 2] available from: http://www.nrc.gov/
5. U.S.NRC Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities", January 2010.
6. J. C. Jung and I. S. Choi, "Lecture on DCS Gateway Server: Design and Function", KEPCO International Nuclear Graduate School, July 2016.
7. A. Kayssi et al., "FPGA-based Internet protocol firewall chip", The 7th IEEE International Conference on Electronics, Circuits and Systems, 2000.
8. A. Goodney et al., Pattern based packet filtering using NetFPGA in DETER infrastructure. 1st Asia NetFPGA developers workshop. Daejeon, Korea. 2010.
9. Y. H Cho, and William H. Mangione-Smith, Deep network packet filter design for reconfigurable devices, 2004. FCCM 2004. 12th Annual IEEE Symposium on. IEEE, 2004.
10. T. Holland, Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth, SANS Institute, 2004.
11. Vitech CORE sim User Guide, CORE 9 Version. [Cited 2016 August 16] Available from: http://www.vitechcorp.com/
12. Xilinx ISE Design Suite, software manuals, and tutorials, http://www.xilinx.com/
13. NetFPGA Project, http://netfpga.org/