DEVELOPMENT OF FPGA-BASED COMPUTER SECURITY CONTROLS FOR ADVANCED PWR REACTORS

A.S. IBRAHIM
Egyptian Nuclear Power Plants Authority (NPPA)
Cairo, Egypt
Email: a_salah9@rocketmail.com

Abstract

In advanced pressurized water reactors (PWR), instrumentation and control (I&C) systems comprise of different data processing and acquisition systems that utilize different network interconnections with different communication protocols. To provide data exchange between those several I&C systems, gateway (GW) devices play an important role in implementation of the I&C system of the plant. Currently, gateway devices are incorporating some type of software-based computer security functions to protect such data processing systems against potential cyberattacks or intrusions. In the paper, FPGA-based computer security controls are developed to perform computer security functions for gateway devices. Gateway devices provide a unidirectional data transmission from the safety side to the non-safety side of the plant main I&C system data network. Such unidirectional data transmission should be maintained so that there is no data reversely transmitted back to the safety-related I&C systems. Typical FPGA-based computer security controls should be placed between gateway devices and non-safety I&C system data network. FPGA-based computer security controls are intended to function as data packet filters and anti-malware scanners. Such controls should similarly be functioning like a next generation firewall (NGFW) technology. The intended FPGA-based computer security controls functionalities will be verified using HDL synthesis simulation tools. Further work is planned to develop a prototype of such computer security controls using an advanced Ethernet type FPGA kit.

1. INTRODUCTION

In advanced PWR, I&C system data networks are divided into safety data network and non-safety data network [1][2]. Both networks are separated and utilize different interconnections and different communication protocols. Redundant safety channels gateway devices are typically specific industrial computer systems that perform data processing of plant safety or normal operation parameters transmitted between different I&C system data networks with different communication protocols. Gateway devices are also functioning as interfaces between safety I&C systems of plant protection and non-safety I&C systems of plant normal operation. Unidirectional data transmission from safety data network to non-safety data network is accomplished via gateway devices and data diodes. Data diodes and gateway devices ensure that there is no data is reversely transmitted back from the non-safety I&C system data network to the safety data network. A bi-directional communication is only established between the gateway devices and non-safety data processing systems to acquire the processed plant parameters data. Such bi-directional communication is accomplished "automatically" where the processed data is continuously transmitted to the non-safety data systems in order to dynamically update the monitoring systems or "on-demand" the main control room (MCR) operators manually acquire the processed data from gateway devices via non-safety data acquisition systems. Although gateway devices are not safety-related systems, such devices are important to the availability of plant parameters data transmission. If a cyberattack or intrusion initiated from the non-safety side of the plant I&C system data network, it would maliciously affect the availability of gateway devices or integrity of its data. Such malicious act can lead to loss of communication between the safety and operation features of plant I&C system so that the plant parameters data cannot be dynamically updated for the purpose of control and monitoring of the plant operation.

In 2016, IAEA introduced the Application of Field Programmable Gate Arrays (FPGA) in Instrumentation and Control (I&C) Systems of Nuclear Power Plants (NPP) [3]. Being computer-based systems, gateway devices incorporate software-based computer security functions which if compromised or bypassed by an insider or cyber-attacker, a malicious act may cause the gateway devices unavailable resulting in a loss of view (LoV) event. In the paper, FPGA-based computer security controls are introduced to protect the redundant safety channel gateway devices and maintain its availability and its data integrity. Computer security controls are conceptually developed using FPGA technology. FPGAs are hardware description language (HDL)

programmable devices that have neither processors nor operating systems. FPGAs are being programmed by configuring its interconnections, which are typical digital logic circuits, so that the intended functions can be performed. The functionalities of such computer security controls are verified using an HDL synthesis simulation tool.

2. METHODOLOGY

During performing the control and monitoring processes of plant operation, the MCR operators request information about monitoring status of the plant. Such on-demand data acquisition is accomplished via the non-safety data processing systems of I&C data network (the side where human-machine interfaces are located at the MCR). Ibrahim [4][5] developed a similar approach for the Korean APR-1400 Man-Machine Interface System (MMIS). The distributed control system (DCS) gateway servers are functioning as redundant safety channel gateway devices, while the information processing system (IPS) is functioning as a non-safety data acquisition system that retrieves the plant parameters data via the non-safety data network (Data Communication Network – Information, DCN-I). The computer security measures are to protect the availability and integrity of such gateway devices [6]. The principles of computer security levels and zones [7] are applied to ensure the security of gateway devices and maintain its availability and its data integrity. In the paper, the proposed FPGA-based computer security controls are to be implemented on advanced FPGA kit modules that support Ethernet data network communication. Such modules will be placed between the redundant safety channel gateway devices and the data processing and acquisition systems of non-safety data network side of plant I&C system as shown in FIG. 1.

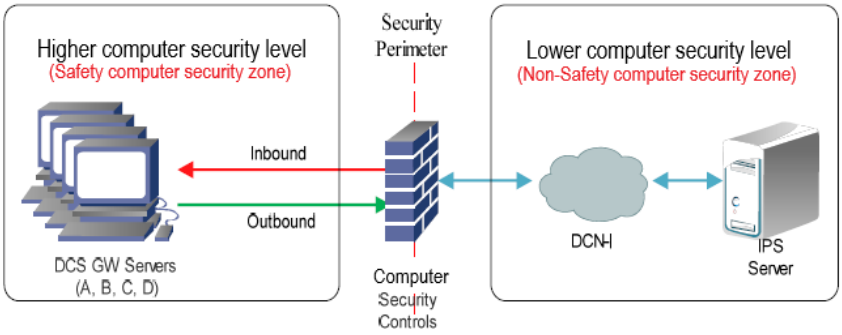

FIG. 1. Allocation of computer security levels, zones and controls

2.1. Design Concept

As illustrated in FIG. 2, the outbound data is transmitted from the safety computer security zone to the non-safety computer security zone. Such outbound data transmission is considered trusted by default because such data are essentially needed for dynamic update of control and monitoring processes of the plant operation status. On the other hand, the inbound data is transmitted from the non-safety computer security zone to the safety one. Such on-demand inbound data transmission may initiate a malicious act by an insider which if occurred, it may maliciously affect the availability and/or integrity of gateway devices and its data.

The FPGA-based computer security control modules will function similarly like next generation firewalls (NGFWs) where combination of traditional firewall functions together with other network security functionalities such as deep packet inspection (DPI) and in-line intrusion prevention system (IPS) will work together to protect the gateway devices.

When an on-demand inbound data transmission is initiated from the non-safety computer security zone via Ethernet-connected data network, the FPGA-based computer security controls modules intercept the inbound traffic *packet-by-packet* looking for unauthorized data transmission and/ or malicious contents. Firstly, the Ethernet packet header fields (i.e., source and destination internet protocol (IP) addresses and port numbers) are extracted for performing packet-filtering process. The extracted fields are compared with predefined static ruleset policy. The filtering process is permitting or denying a specific data traffic based on a specific filtering ruleset policy. The permitted data packet moves forward to perform the DPI matching for malicious content scanning process. Data packet payload is thoroughly scanned *byte-by-byte* looking for a known malicious

exploit pattern or a signature string for known cyberattacks, that are already detected and their source codes are included in the databases of computer security controls. If a DPI pattern string is matched with the input data payload, the whole data packet will be dropped, alerted and logged. The computer security controls functionalities only allow a legitimate data packet that does not contain any malicious contents. Once a gateway device receives an authorized legitimate data packet, the computer security controls modules will perform the same filtering and DPI processes for the next data packets until the end of data transmission session.

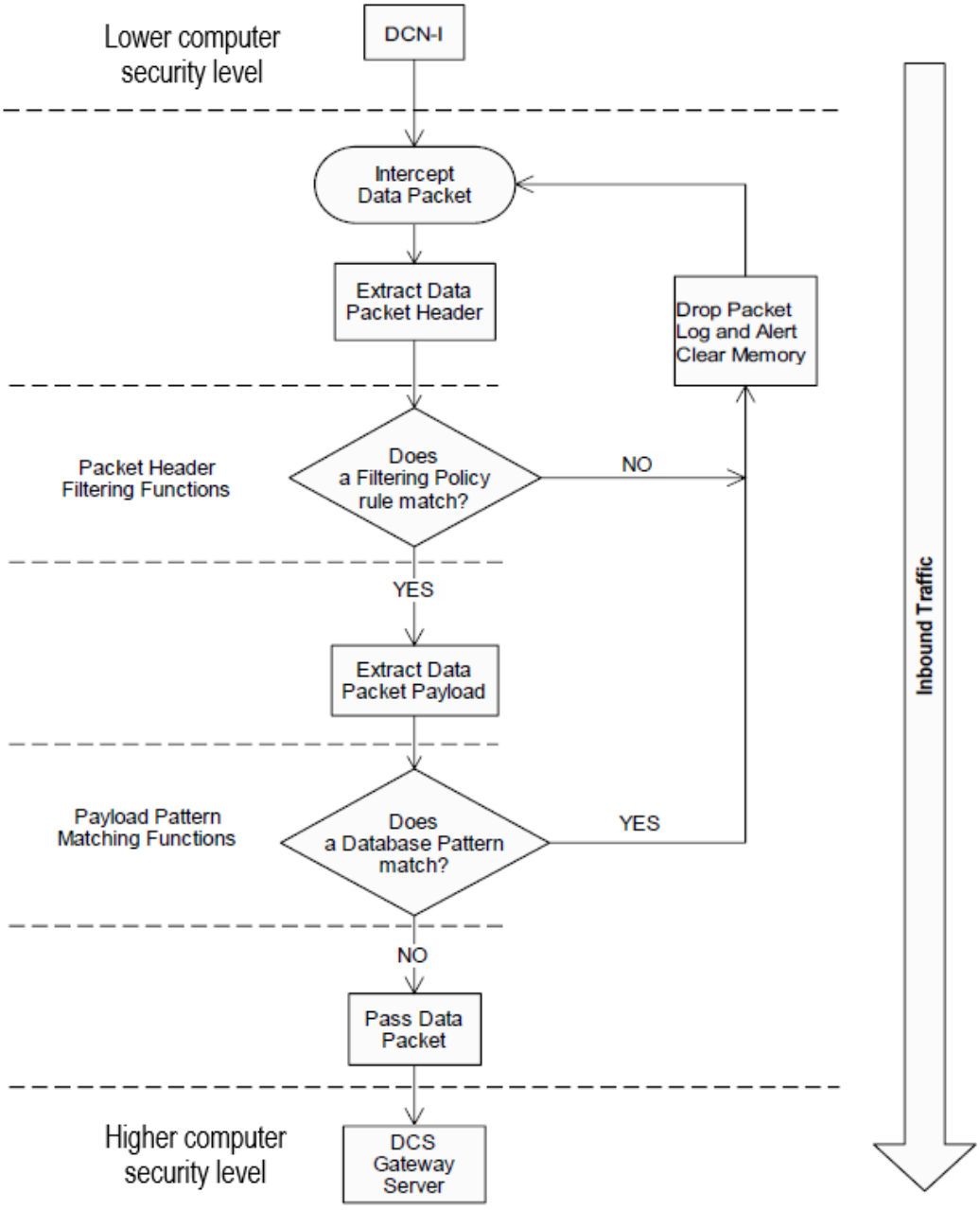

FIG. 2. Design functional flowchart (inbound data traffic)

As illustrated in FIG. 3, when an inbound data packet is transmitted from the non-safety computer security zone to the safety, the Ethernet Input/output (I/O) Unit intercepts the received packet at the Ethernet interface and writes to the memory control unit (MCU) buffer memory. 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.

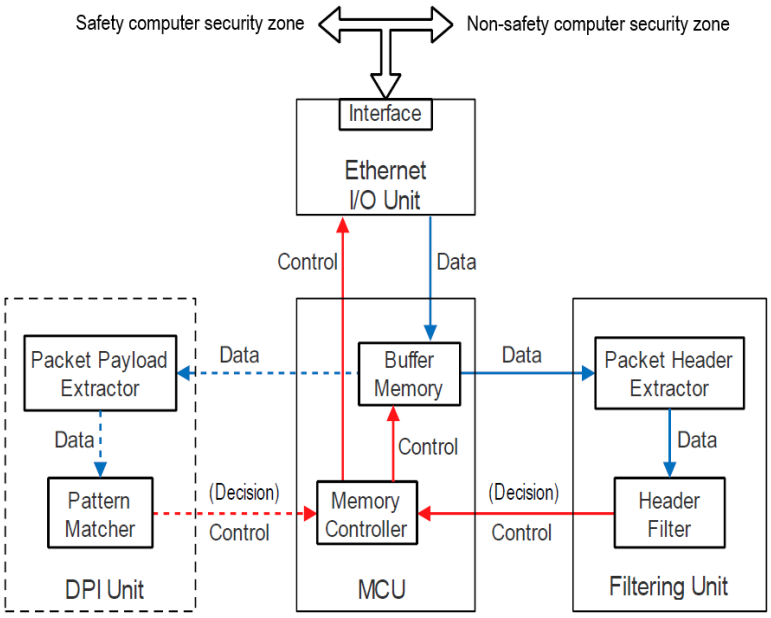

FIG. 3. Computer security controls module block diagram

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 remaining rules in the ruleset order and the decision is made only upon the matched rule. The MCU notifies the buffer memory to write its content to the DPI Unit for malicious content scanning. The data packet payload is extracted to be thoroughly scanned and inspected for malicious content (e.g., a predefined malware pattern or exploit string code). In a similar concept as that of filtering ruleset policy, DPI functions compare the payload content with the pattern database constraints that are applied to each pattern matcher of the DPI pattern database. In contrast to the filtering process 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 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.

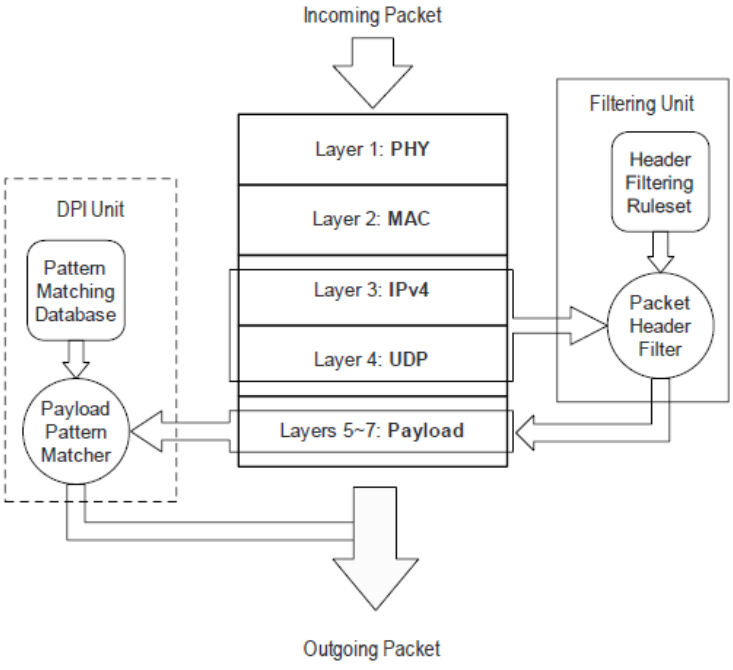

FIG. 4. OSI model layers

As shown in FIG. 4, if any one of ALLOW rules does not match Layers 3 and 4 information (Packet Header), then the packet is dropped (*marked as unauthorized traffic*); else the packet is deeply inspected. If any one of database patterns matches Layers 5 to 7 information (Packet Payload), then the packet is dropped (*marked as malicious content*); else the packet is allowed to pass.

2.2. Design modelling using Xilinx ISE software tools

FIG. 5 and FIG. 6 illustrate the block diagrams of Filtering Unit and DPI Unit respectively. Using Xilinx ISE software tools [8], eight-bit (one-byte) X-NOR digital comparators are incorporated to build the hardware block schema.

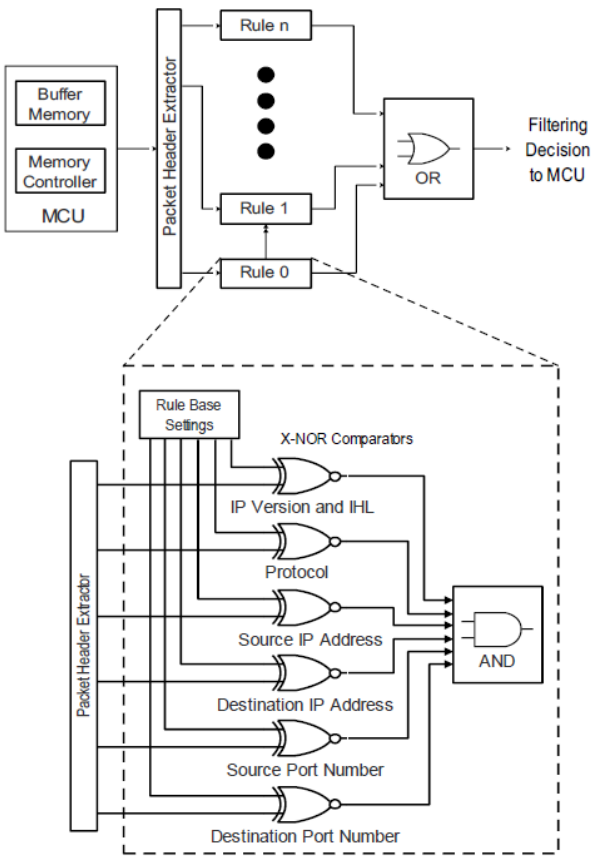

FIG. 5. Filtering unit block diagram

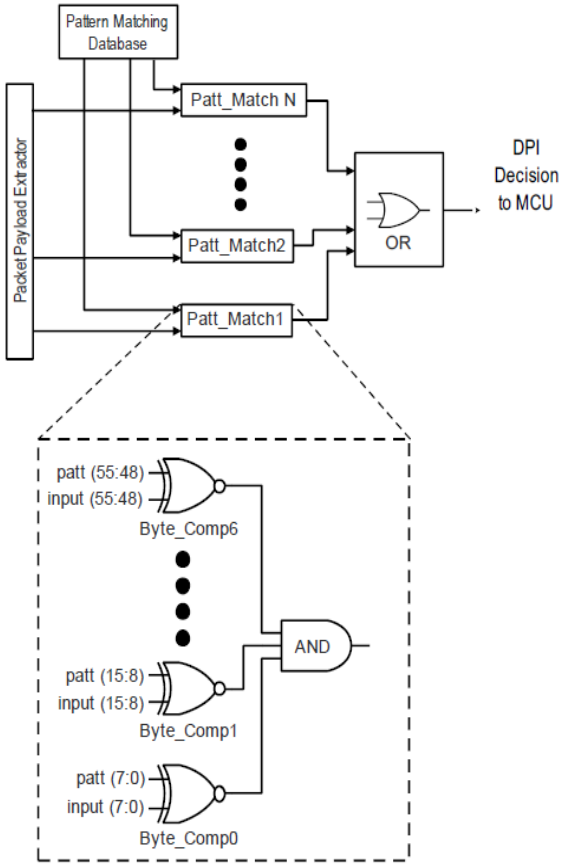

FIG. 6. DPI unit block diagram

3. RESULTS

The hardware block schema of proposed FPGA-based computer security controls is simulated using Xilinx ISE synthesis simulation tools (ISim). FIG. 7 shows a simulation timeline for a valid data packet of size 1500 bytes. As shown, such data packet is authorized to pass from the non-safety computer security zone to the safety one (in_fltr_flag = 1). The packet is also legitimate and has no malicious content (vld_pkt = 1). Moreover, it is obvious that the execution running time of processing such data packet through the computer security controls module is about 7145 nanoseconds (approximately seven microseconds). Such execution time is considered negligible if compared with the maximum transmission time of a data packet initiated from the non-safety computer security zone transmitted through the computer security controls module and arrived at its destination in the safety computer security zone. Consequently, implementing the FPGA-based computer security control functions are not *significantly* affecting the data transmission time or delay time of the whole I&C system.

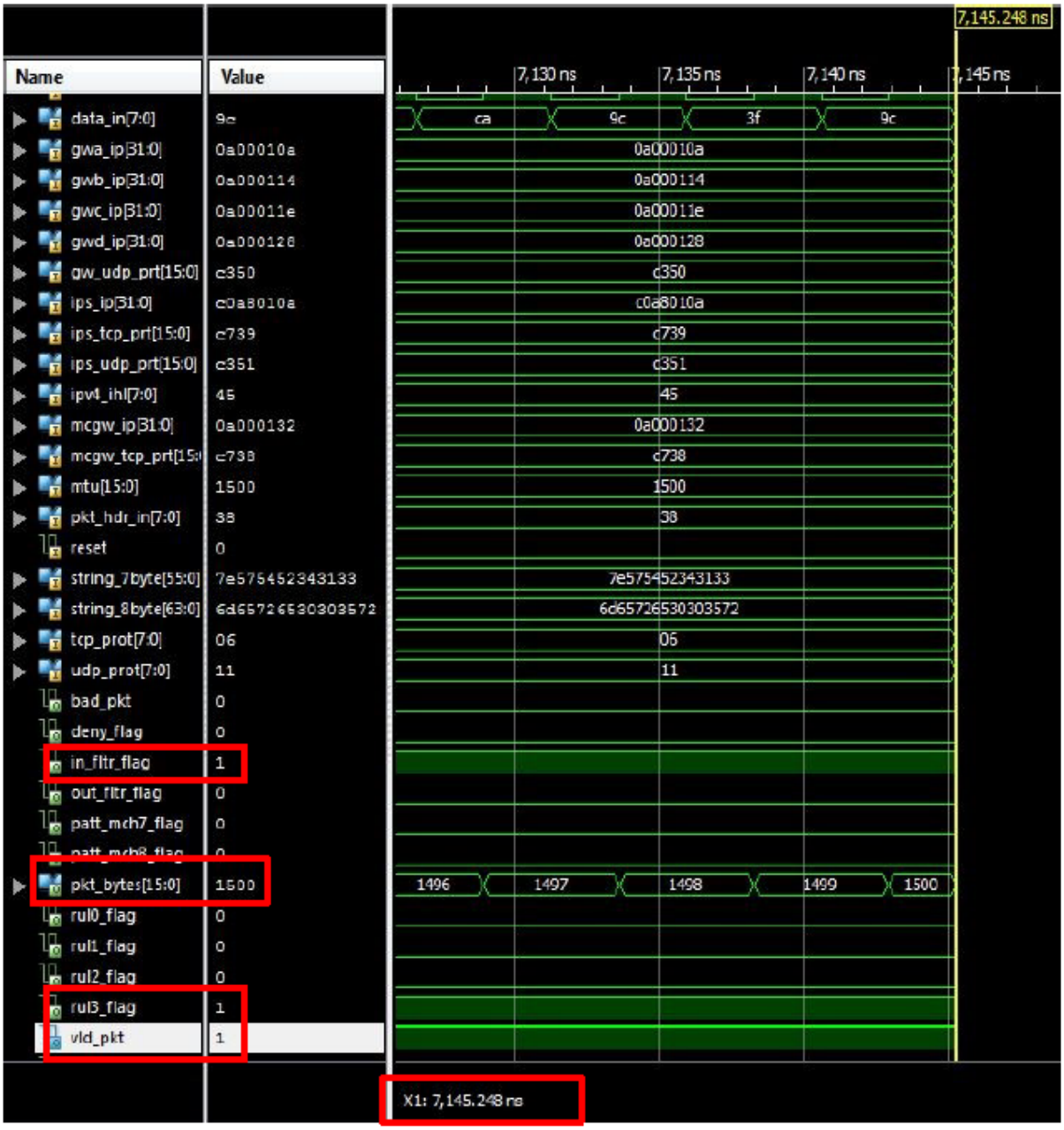

FIG. 7. Authorized and legitimate data packet simulation using ISim

4. CONCLUSION AND FURTHER WORK

FPGA-based computer security control functions were developed in this paper using FPGA technology and HDL synthesis simulation tools. The computer security controls modules were implemented as redundant network security perimeters between the redundant safety channel gateway devices and the non-safety data acquisition systems of I&C data network to maintain the availability and integrity of data transmission for the purpose of control and monitoring of the plant operation.

Computer security control functions design included NGFW functionalities such as filtering and deep data packet inspection functions in order to control and block the unauthorized and malicious data transfer. The developed design was of FPGA-based to ensure the computer security of gateway devices as well as not affect the whole I&C system data networks performance. Static filtering ruleset policy and database of known cyberattack signatures were together used to control the inbound data traffic initiated at the non-safety computer security zone so that a potential intrusion could be prevented. Denial-of-service (DoS) attack was considered the potential intrusion that if occurred it may disrupt the data availability and integrity.

Further work will focus on building an FPGA-based prototype to validate the functionality of computer security controls. The validation phase will include developing an HDL code using VHDL programming language, implementing the code to an advanced Ethernet-type FPGA kit, and testing in an IPv4 Ethernet network-based environment. Mitigation of DoS attack is the limitation for this work as considered as one of the major cyberattacks to affect data systems availability and integrity.

REFERENCES

[1] KEPCO and KHNP, APR1400 Design Control Document Tier 2, "Chapter 7 Instrumentation and Controls", Revision 0 (2014).

[2] Professional Solutions on Automation, JSC RASU Products and Services Catalog, (Cited on 10 May 2019) available at: https://rasu.ru/en/catalog_rasu.pdf.

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of Field Programmable Gate Arrays in Instrumentation and Control Systems of Nuclear Power Plants, Nuclear Energy Series No. NP-T-3.17, IAEA, Vienna (2016).

[4] Ibrahim, A.S., Jung, J.C., A Systems Engineering Approach to Implementing Hardware Cybersecurity Controls for Non-Safety Data Network. System Engineering Journal, 12 (2), 101-114. (2016) https://doi.org/10.14248/JKOSSE.2016.12.2.101.

[5] Ibrahim, A.S., A Systems Engineering Approach to Implementing Hardware Cybersecurity Controls for Non-Safety Data Network. Project Report of Master Degree, KEPCO International Nuclear Graduate School (KINGS), Ulsan, Republic of Korea (2016).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).

[8] ISE In-Depth Tutorial, UG695 (v13.1) March 1, 2011, Xilinx ISE Design Suite, software manuals and tutorials, (Cited on 31 March 2019) available at: http://www.xilinx.com/.