Journal of KOSSE. (2018. 12) Vol. 14, No. 2 pp. 73-82
DOI: https://doi.org/10.14248/JKOSSE.2018.14.2.073
www.kosse.or.kr

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

Systems Engineering Approach to develop the FPGA based Cyber Security Equipment for Nuclear Power Plant

Jun Sung Kim, Jae Cheon Jung*

Department of NPP Engineering, KEPCO International Nuclear Graduate School

Abstract : In this work, a hardware based cryptographic module for the cyber security of nuclear power plant is developed using a system engineering approach. Nuclear power plants are isolated from the Internet, but as shown in the case of Iran, Man-in-the-middle attacks (MITM) could be a threat to the safety of the nuclear facilities. This FPGA-based module does not have an operating system and it provides protection as a firewall and mitigates the cyber threats. The encryption equipment consists of an encryption module, a decryption module, and interfaces for communication between modules and systems. The Advanced Encryption Standard (AES)-128, which is formally approved as top level by U.S. National Security Agency for cryptographic algorithms, is adopted. The development of the cyber security module is implemented in two main phases: reverse engineering and re-engineering. In the reverse engineering phase, the cyber security plan and system requirements are analyzed, and the AES algorithm is decomposed into functional units. In the re-engineering phase, we model the logical architecture using Vitech CORE9 software and simulate it with the Enhanced Functional Flow Block Diagram (EFFBD), which confirms the performance improvements of the hardware-based cryptographic module as compared to software based cryptography. Following this, the Hardware description language (HDL) code is developed and tested to verify the integrity of the code. Then, the developed code is implemented on the FPGA and connected to the personal computer through Recommended Standard (RS)-232 communication to perform validation of the developed component. For the future work, the developed FPGA based encryption equipment will be verified and validated in its expected operating environment by connecting it to the Advanced power reactor (APR)-1400 simulator.

Key Words : Cyber Security, Advanced Encryption Standard, Field Programmable Gate Array, Hardware Description Language, Man-in-the-middle Attack, System Engineering, Nuclear Power Plant, Advanced Power Reactor-1400

Received: November 15, 2018 / **Revised**: November 27, 2018 / **Accepted**: January 7, 2019

* Corresponding author : Jae Cheon Jung, jcjung@kings.ac.kr

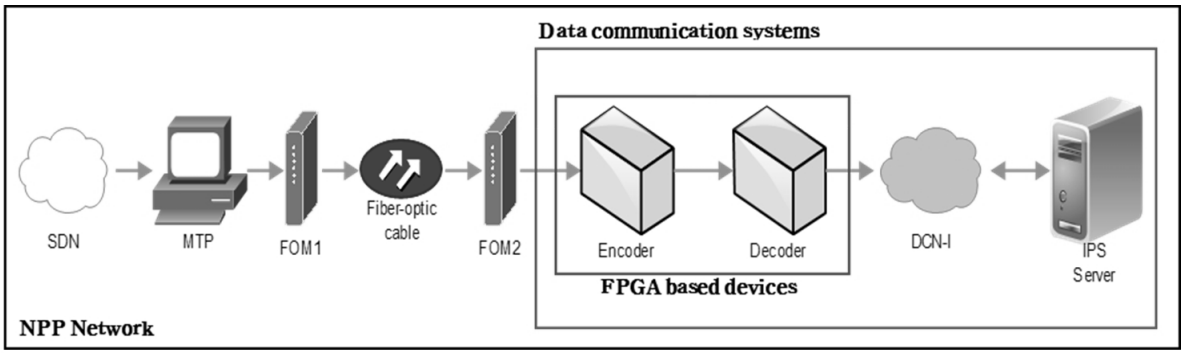
1. Introduction

1.1 Background and Purpose

Recently, Advanced Persistent Threats (APT), which targets Industrial Control System such as nuclear and process facilities, is a dominant type of cyber threat. A well-publicized case is the Stuxnet worm attack in Bushehr nuclear power plant in Iran in 2010 [1]. The purpose of this work is to develop Field Programmable Gate Array (FPGA) based cyber security equipment through a system engineering approach to enhance cyber security principles such as the CIA triads (Confidentiality, Integrity, and Availability). As shown in Figure 1, the module is developed for the Data Communication Systems (DCSs) of the Nuclear Power Plant (NPP). Requirements elicitation and the selection of an encryption algorithm for cyber security enhancement is done by reverse engineering and the results are applied to develop encryption module as well as to verify and validate the performance by re-engineering process. These processes are finally verified by checking out that the plain text (raw data) and the FPGA output value are matched.

1.2 The Hypothesis

Nuclear facilities are less likely to be cyber threats because the Internet and the network are separate and independent networks are built on the site. This paper assumes the possibility of cyber threats by Man-in-the-middle attacks (MITM) at nuclear facilities [2]. This is done through the maintenance and testing activities of staff working with portable devices during the outage period. The impact of this attack can be the unauthorized collection of confidential data or the modification of traffic by injecting malware or malicious data into the systems. The use of cryptographic equipment provides one solution for the mitigation of MITM. In terms of cyber security, the operating system (OS) and patches are so complex that it is difficult to grasp all the interactions that can be hacked. Therefore, there may be many weak points in the system. That's why hackers are constantly targeting software security tools and network vulnerabilities. Hardware based security is more robust than software based security because it is difficult to change the physical layer during cyber-attacks. The physical layer also blocks the possibility of malware penetrating the operating system and penetrating the virtual layer [3]. Hardware based encryption



[Figure 1] Cyber Security Equipment Configuration of NPP

devices therefore improve the security of information. FPGA based encryption has extra advantage and higher security since it does not need an operating system [4]. It can provide a cyber security defense architecture that can cope with greater flexibility and malicious cyber security threats as well. FPGA based security modules enable independent V&V (Verification and Validation) through highly controlled designs and modification processes. By following these procedures, it is possible to prevent the possibility of malware being inserted into the HDL code [5].

2. Reverse Engineering Process

2.1 Regulatory Requirements

According to 10 CFR 73.54 (Title 10, of the Code of Federal Regulations, Section 73.54) (a) (1), requires licensees to protect Critical Digital Assets (CDAs) with the following categories of functions:

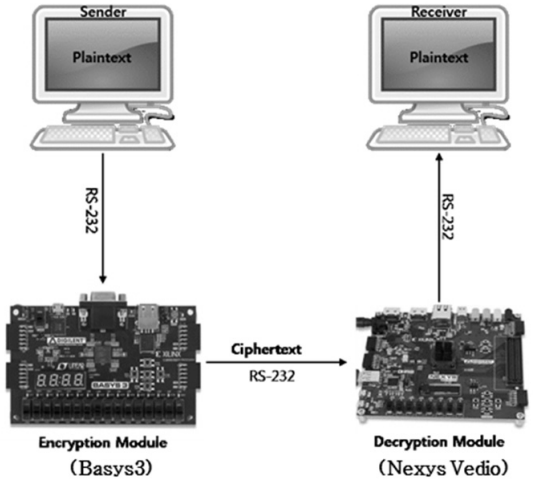
- Safety-related and important-to-safety functions,
- Security functions,
- Emergency preparedness functions, including offsite communications, and
- Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions [6].

2.2 System Requirement Analysis

Cyber security is technology and process that are designed to protect systems and networks from cyber-attacks. In nuclear power plants, cyber security is the protection of digital assets including digital instrumentation and control systems or equipment. Cyber security at nuclear power plants promotes performance-based programmatic approaches supported by defense-in-depth strategies, including efforts to detect, prevent, delay, mitigate, and recover from cyber-attacks [7].

2.3 System performance Criteria

In this study, the FPGA-based Advanced Encryption Standard (AES)-128 encryption module must meet stakeholder needs and system requirements as well as high performance. In all the processes, unidirectional communication of information was taken as a basic requirement, not bi-directional communication, considering the security aspect of nuclear power plant. We assume that the AES algorithm itself is a trusted algorithm that is published as a top - level security step U.S. National Security Agency. The Measure of effectiveness (MOE) is the completeness of the CIA (confidentiality, integrity, availability) by the security definition criteria [8]. The first factor, Confidentiality, is excluded because the AES algorithm itself is a guaranteed program, and the third one, Availability, will be objective as the comprehensive testing after cryptographic module and system integration in the future work. As shown in Figure 2, the confirmation of the integrity of the data is obtained by encrypting the Plain text as an input from the sender with the FPGA based encryption module and generating the original data to the receiver through the decryption module. Measure of performance (MOP) is based on data processing speed. This study compares the processing speed of hardware based cryptosystem with the software based method of serial



[Figure 2] Cyber Security Equipment Configuration

processing of data. In this process, the speed of the interface is excluded and only hardware-based cryptographic processing time is computed. This is because it depends on the developer's choice such as RS-232 (Recommended Standard 232) and TCP/IP (Transmission Control Protocol/ Internet Protocol). Acceptance criterion of MOP is 20% faster than software based encryption system.

2.4 AES Theory: Design Guide

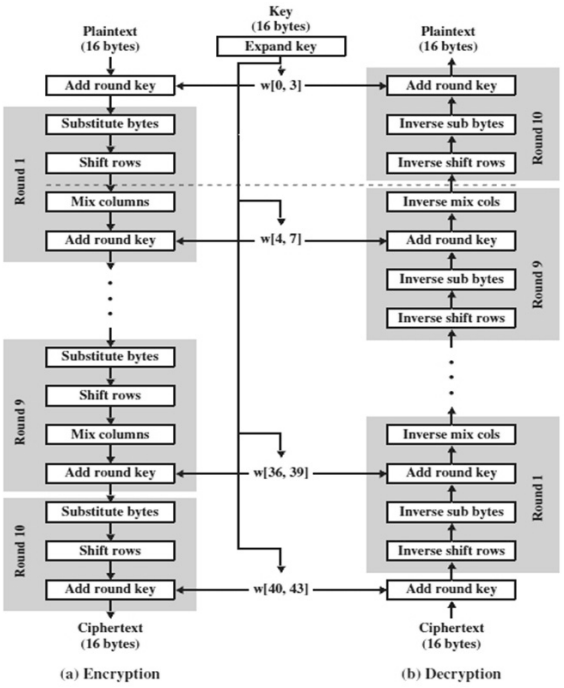
2.4.1 AES Introduction

This algorithm was developed by the National Institute of Standards and Technology (NIST) in 2001 and has been widely used since it is the first of the algorithms officially approved by the National Security Agency (NSA) for use in the Top Secret. It has a symmetric key algorithm structure that uses the same key in the encryption and decryption process and has a plaintext block size of 128 bits. And the cipher key length can be either 128, 192, or 256 bits. The algorithm is referred to as AES-128, AES-192, or AES-256, depending

<Table 1> AES types and parameter

(Units : words/bytes/bits)

Parameters	Round Key Size	Plaintext Block Size	Number of Rounds
AES-128	4/16/128	4/16/128	10
AES-192	6/24/192	4/16/128	12
AES-256	8/32/256	4/16/128	14



[Figure 3] AES-128 Encryption and Decryption

on the key length as shown in Table 1. The longer the encryption key length, the more the number of round iterations and the greater the security.

2.4.2 AES-128 Algorithm

AES is divided into two categories: encryption and decryption. During both two processes, AES-128 goes through 10 rounds with 128-bit cipher key. For both encryption and decryption, the first process is an Add round key stage followed by 9 rounds that each includes all four stages. The last 10^{th} round is consists of three stages as shown in Figure 3. To understand the algorithm of

AES-128, the only encryption process is described here [9]. This is because the decryption process is the reverse of the encryption process.

1) Substitute bytes: each byte in the state is replaced with its entry in a fixed 8 bits lookup table named s-box
2) Shift rows: operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset
3) Mix columns: All bytes belonging to a column are transformed using a particular matrix, replacing each byte in the column with a function.
4) Add round key: A simple bitwise XOR of the current block with a portion of the expanded key.

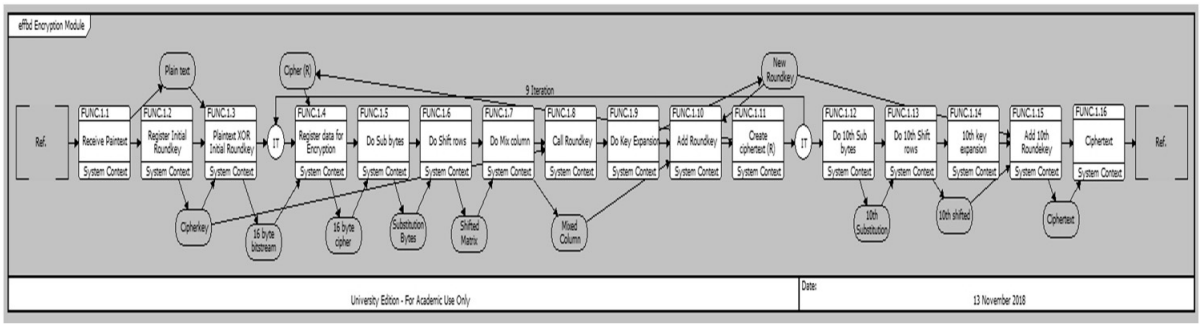
3. Re-Engineering Process

3.1 Design Concept and Modeling

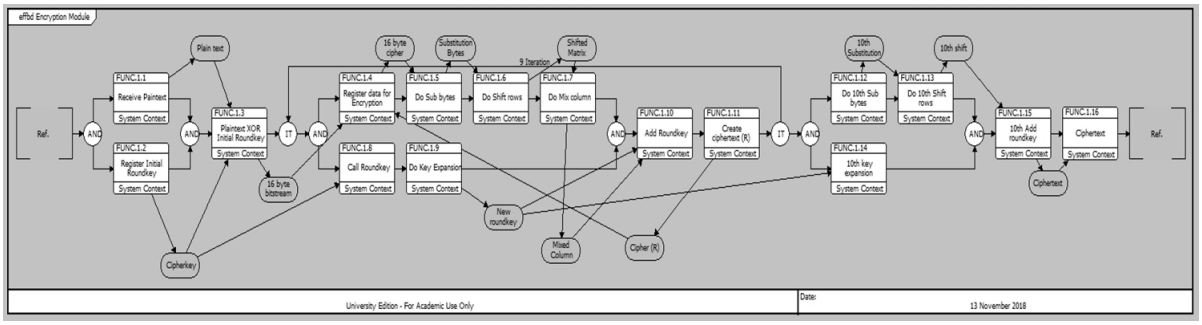
In this design, Vitech CORE 9 software is used as a tool for model-based systems engineering (MBSE) and corresponds to the preliminary design process. The results of this process give validity to the development of HDL code in the AES-128 algorithm. The results of the decomposition into functional units through reverse engineering were modeled: one is a logical sequential structure of the software based design currently used; the other is parallel structure of the proposed FPGA based design [10]. This modelling was performed using Enhanced Function Flow Block Diagrams (EFFBD) using CORE9 [11]. In order to confirm the MOP, we constructed a basic framework for code development and confirmed the prediction of the processing speed for the model implementation through simulation. There are the same encryption and decryption processes that are repeated nine times in the AES algorithm. The key point is that the process of generating cryptographic keys used in this process can be sped up if it is changed to a parallel structure instead of serial processing. The result is confirmed through the simulation.

3.2 EFFBD simulation

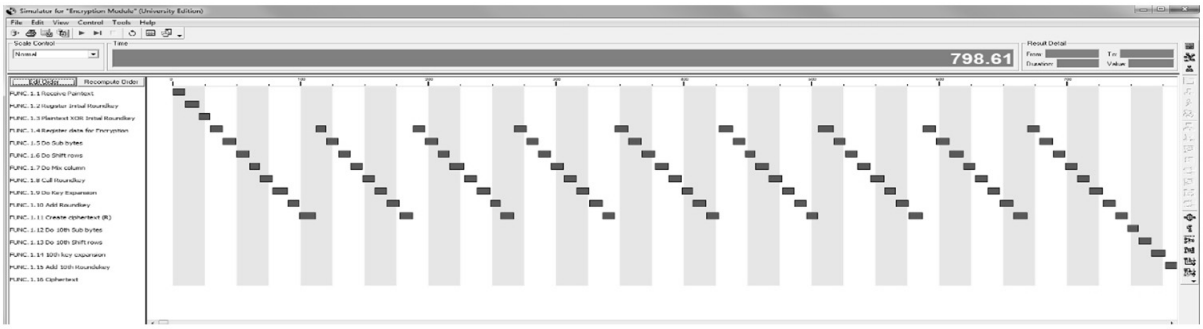
The main goal of EFFBD simulation is to compare the development of encryption and decryption with software that can only process sequential processes, and the development of parallel and independent hardware that can be simultaneously processed. Fundamentally, encryption and decryption processes are symmetric, but as shown in Figure 4, 5, 8 and 9, EEFBD has a slightly different structure, especially in processing order in the repeated round. As



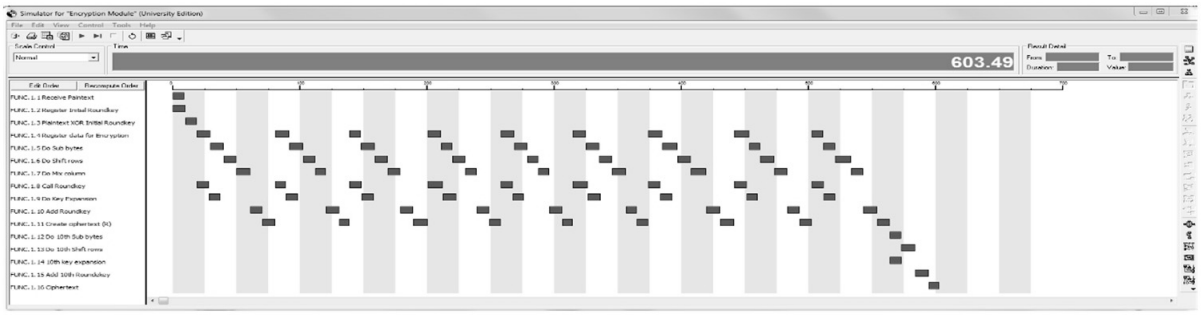
[Figure 4] EFFBD of software based Encryption



[Figure 5] EFFBD of FPGA based Encryption

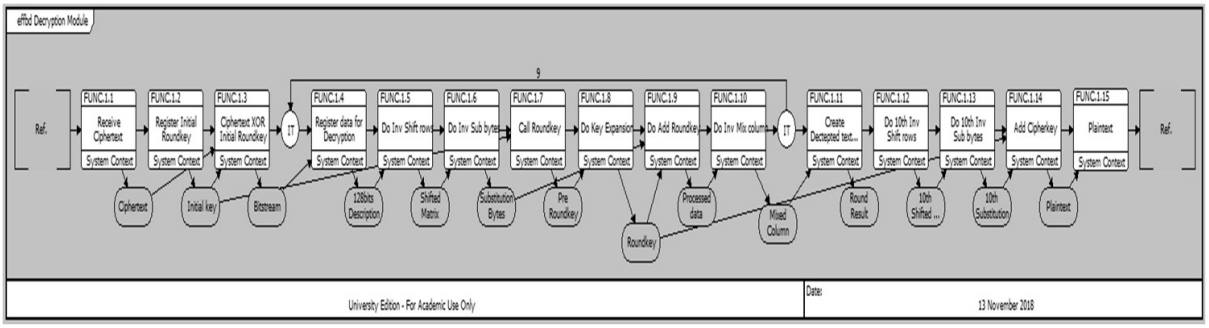


[Figure 6] Simulation of EFFBD of software based Encryption

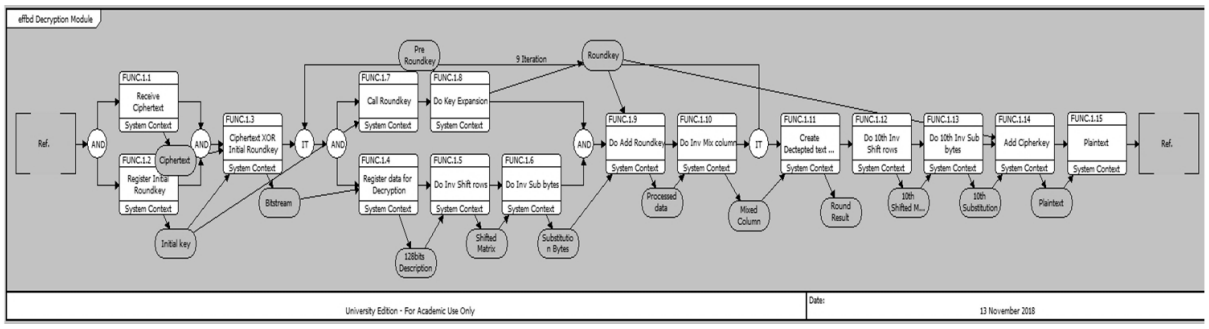


[Figure 7] Simulation of EFFBD of FPGA based Encryption

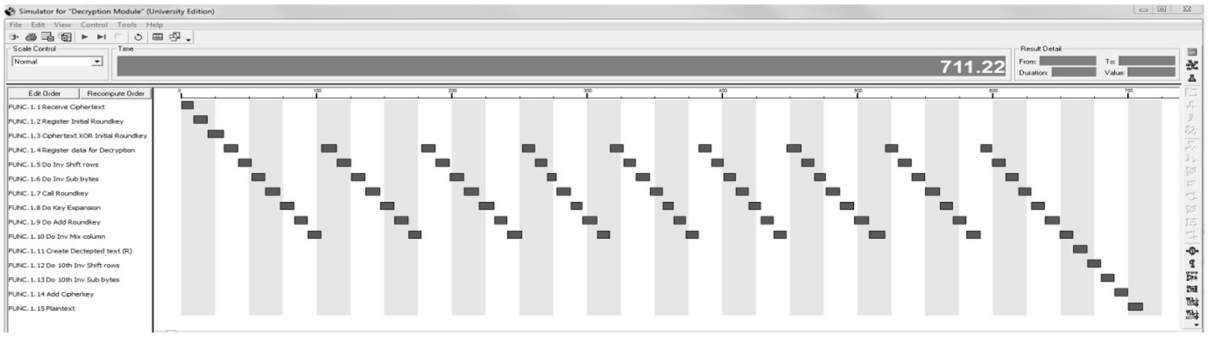
shown in Figure 4, 5, 8 and 9 the EFFBD simulation, there are differences in the order of operations for generating encryption keys processes and receiving first input process for both encryption and decryption. FPGA based configuration results are in parallel execution of all logically independent operations, rather than a typically serial process, as in the case of conventional microprocessor based platforms [4]. Therefore the results of simulation of FPGA based EFFBD shows faster processing time rather than software based systems such a programmable logic controller. Here, an important thing is that the same simulation results are checked and verified. The FPGA-based cryptographic modules perform better than the software-based cryptographic module. For encryption, the software based encryption module simulation results is 798.61 time unit. On the other hand, the FPGA based encryption module simulation result is 603.49 time unit. We confirmed that improved performance ratio



[Figure 8] Simulation of EFFBD of software based Decryption



[Figure 9] Simulation of EFFBD of FPGA based Decryption

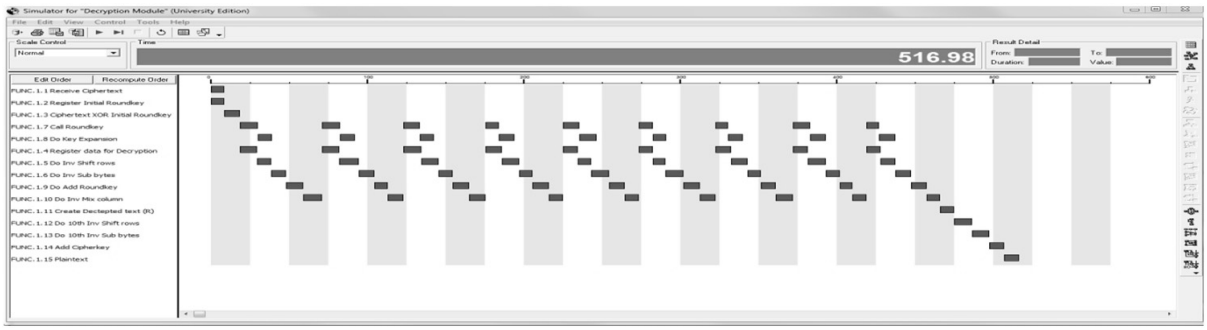


[Figure 10] Simulation of EFFBD of software based Decryption

is calculated at 24.43%. For decryption, FPGA based encryption module simulation result is 516.98 time unit and software based encryption module simulation results is 711.22 time unit. Improved performance ratio is 27.31%. This satisfies mop and shows that the FPGA is efficient for encrypting large amounts of data.

3.3 HDL code development

The VIVADO design suite was used as a programming tool for code development, as well as for the development of test bench and verification of the generated cryptographic code [12]. Code development consists of two structures. The first is the core function AES encryption algorithm, and the other is the interface that transmits data between the FPGA module and the computer terminal. The AES-128 is divided into two HDL codes: encryption and decryption. The interface is divided into three structures for the commu-nication between the sender, the receiver



[Figure 11] Simulation of EFFBD of FPGA based Decryption

[Figure 12] Test Bench Simulation

terminal, and the encryption and decryption module, and RS232 is selected. The initial ciphertext and plaintext used in the cryptographic HDL development are cited in NIST SP 800-38A Appendix (F) to verify the results at the intermediate stages of development. Initial cipher key is directly inserted into the code in the cryptographic coding, so that the cryptographic key management need not be separately performed [13].

3.4 Code Verification

After completing the synthesis of the developed HDL, the developed AES-128 code is verified through the use of a test bench. As shown in Figure 12, six sample plain texts and a cipher key are utilized from NIST SP 800-38A Appendix (F) [14] and the results are exactly matched with result of simulation using VIVADO software.

3.5 Testing Result

For the integration test, the system is configured as shown in Figure 2. Basys3 and Nexys video FPGA board are used for Encryption and Decryption module to apply the verified AES-128 HDL code to the hardware platform. RS-232C is used as an interface of this systems. In the FPGA, the plaintext is used as an initial input with a cipher key. The input is converted to the cipher text. It goes through the encryption module and then this cipher text goes to decryption module as an input to make final output. As shown in Table 2, the final output, the result of the FPGA based decryption module, produces the same plain text as the initial input. In addition, the intermediate output of processing, encryption module output, also has the same result comparing with the expected encryption data. This means

<Table 2> System Integration Test Results

Plain Text: Initial Input	Expected Encryption data	Encryption Module Output	Expected Decryption data	Decryption Module Output: Final output
AE2D8A571E03AC9C 9EB76FAC45AF8E51	F5D3D58503B9699D E785895A96FDBAAF	F5D3D58503B9699D E785895A96FDBAAF	AE2D8A571E03AC99 EB76FAC45AF8E51	AE2D8A571E03AC9C 9EB76FAC45AF8E51
30C81C46A35CE411 E5FBC1191A0A52EF	43B1CD7F598ECE23 881B00E3ED030688	43B1CD7F598ECE23 881B00E3ED030688	30C81C46A35CE411 E5FBC1191A0A52E	30C81C46A35CE411 E5FBC1191A0A52EF
F69F2445DF4F9B17 AD2B417BE66C3710	7B0C785E27E8AD3F 8223207104725DD4	7B0C785E27E8AD3F 8223207104725DD4	F69F2445DF4F9B17 AD2B417BE66C3710	F69F2445DF4F9B17 AD2B417BE66C3710

that the test results meet the performance of HDL code and FPGA logic gates. It also means that MOE ensures data integrity and confi-dentiality.

4. Conclusion

In this work, FPGA based cyber security equipment for nuclear power plants was developed using a systems engineering approach. It consists of an encryption module, a decryption module and an interface for communication. Hardware-based security modules have no operating system and are free of malicious viruses based on Windows, such as Stuxnet worm attacks, and provide faster data processing speed than software-based encryption systems.

In the reverse engineering stage, Cyber security-related stakeholder requirements and system requirements were analyzed and AES-128 algorithm that is officially approved by NSA for use in the Top Secret was reviewed as a design guide

In re-engineering, and AES -128 HDL codes were developed and verified through test benches with VIVADO simulator. EFFBD is developed using MBSE approach at the pre-liminary design stage, confirmed that it could process more information by improving processing speed. This provides a feasibility to proceeding with development. The developed HDL code is synthesized and placed on the two FPGA boards. And system integration test were conducted to confirm that the requirements of this paper, MOEs and MOPs, were met.

The efficiency of the data processing speed and the integrity of the data have been verified while developing the hardware based encryption equipment. The development of a cyber security module using FPGA is not yet applied to the field of nuclear power, therefore the attempt itself is significant. In the future, additional interfaces such as TCP / IP must be developed and connected to the APR-1400 simulator to reflect and evaluate complex and diverse nuclear power plant requirements. It also offers the possibility to apply more complex and secure AES-192, 256-bit encryption to the FPGA. Successful connection between the APR-1400 simulator and the developed cyber security equipment enables data collection through many tests. The system is worth applying to a nuclear power plant.

References

1. N. Falliere, “W32.Stuxnet Dossier,” symantec, Feb 2011. [Online]. Available: http://www.

symantec.com/content/en/us/enterprise/media/security_resp onse/whitepapers/w32_stuxnet_dossier.pdf.

2. M. A. Elakrat, "Development of field programmable gate array-based encryption module to mitigate man-in-the-middle attack for nuclear power plant data communication network," Nuclear Engineering and Technology, vol. Volume 50, no. Issue 5, p. 780~787, June 2018.
3. D. Brecht, "Tales from the Crypt: Hardware vs Software," Infosecurity, [Online]. Available: https://www.infosecurity-magazine.com/magazine-features/tales-crypt-hardware-software/.
4. International Atomic Energy Agency, "Application of Field Programmable Gate Arrays in Instrumentation and Control Systems of Nuclear Power Plants," IAEA, p 4, 2016.
5. E. Phneah, "ZDNet," 13 Februrary 2013. [Online]. Available: https://www.zdnet.com/article/hardware-based-security-more-effective-against-new-threats/.
6. Protection of Digital Computer and Communication Systems and Networks Available, vol. 10 CFR 73.54, U.S. NRC, 2009.
7. "Cyber Security Programs for Nuclear Facilities," January 2010. [Online]. Available: http://www.nrc.gov/reading-rm/doc-collections/.
8. FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, "Standards for Security Categorization of Federal Information and Information Systems: FIPF PUB 199," U.S. DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2004.
9. William Stallings, CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE, FIFTH EDITION, NY 07458: PERASON, 2011.
10. Vitech Corporation, "COREsim User Guide," June 2015. [Online]. Available: http://www.vitechcorp.com/support/documentation/core/900/COREsimuserguide.pdf.
11. M. Nagendra and M. Chandra Sekhar, "Performance Improvement of Advanced Encryption Algorithm using Parallel Computation," International Journal of Software Engineering and Its Applications, vol. 8, no. 2, pp. 287-296, 2014.
12. XILINX, "Vivado Design Suite Tutorial: Using Constraints," April 2018. [Online]. Available: https://www.xilinx.com/support/documentation/sw_manuals/xilinx2018_1/ug945-vivado-using-constraints-tutorial.pdf.
13. Elaine Barker, William Barker and William Burr,, "NIST Special Publication 800-57: Recommendation for Key Management - Part 1: General(Revision 3)," July 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-57p1r3.pdf.
14. National Institute of Standards and Technology, "NIST Speacial Publication 800-38A," December 2001. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-38a.pdf.