Development of A Prototype FPGA based Security Module to Control Data Communication Network Access

EL-AKRAT Mohamed Abdallah, JUNG Jae Cheon

1. Department Of NPP Engineering, KEPCO International Nuclear Graduate School, Ulsan, Korea
, Postal address, City post-code, Nationality (E-mail: maakrat@yahoo.com / jcjung@kings.ac.kr)

Abstract: In this paper, field programmable gate array (FPGA) based Security Module is presented, this module run an application of encryption using hardware. Using FPGA technology in industrial systems, especially in nuclear power plants, strongly present in I&C application, which considered as state-of-the-art in NPP I&C systems; although there are several challenging problems in the area of cybersecurity assurance for complex FPGA-based I&C systems consideration of all the possible vulnerabilities. In this work, a prototype FPGA based security module is developed to control network security for mitigating man in the middle (MITM) attacks, using commercial FPGA to verify and validate the designed hardwired security module to assure data confidentiality, and integrity of data communication system in APR 1400 nuclear power plant, model-based system engineering approach is applied to analysis system requirements, enhanced function flow block diagram (EFFBD) is created and simulated by using CORE9 university edition to compare between the current system and the developed module , HDL code is developed using ALDEC Design Suite as a programming tools and to run System synthesis and implementation for performance simulation and design .

Keyword: Cyber Security, I&C, FPGA

1 Introduction

Keeping data secure needs a strong cybersecurity countermeasure, One of the possible threats can happens during maintenance and test process in data communication system of APR1400 by outsider contractor is Man In The Middle (MITM) attacks, the adversary can insert himself in between the gateway and the workstations to in inject the malicious data , the way to make data secure against MITM is data encryption to prevent adversary make any modification or damaged for data to assure data confidentiality and integrity during transmission from sender to receiver, using Trusted Platform Module (TPM) to make data encryption and decryption process depending on software is not efficient enough in case of development new algorithms or vulnerabilities found because it is not reconfigurable device and need some techniques to accelerate the performance [1], using field programmable gate array FPGA is more efficient and has faster execution time compared with using TPM performance due to reconfigurable features and parallel execution for independent processes ,by using FPGA cybersecurity measurements improved ,it delivers a robust platform against MITM attack, also applying of FPGA in nuclear power plant subject to specific regulation has to meet in addition to codes and standards, In this paper, a discussion of development of prototype FPGA based security module is presented to shift from software to hardware encryption module by developing FPGA based AES-128 which is most popular and secure encryption algorithm, a comparison between functions execution performance in case of software-based system and the developed system is shown using CORE9 university edition which we use to create and simulate enhanced function flow block diagram (EFFBDs), ALDEC is chosen as a programming tool to develop and simulate HDL code to NEXYS video FPGA board, the developed system performance is verified by applied a pre-proven encryption block ciphers example using plaintext and key, the output of the developed module output is the same proven example by NTIS.

2 System Requirements

Referring to U.S NRC RG 73.54 highly assurance for digital networks and data communication system protection against cyber-attacks should be provided including all threats to assure that the data transfer securely and no impact on data integrity or confidentiality, also all assets functionally protected and not adversely impact due to any attacks also this work take in consideration the requirements of U.S NRC RG 1.152 and NIST SP 800-37 guidelines [2], [3], [4].

In accordance with security requirements, critical digital assets CDAs uses to implement cryptographic mechanisms should comply with security requirements for cryptographic modules and also protect the confidentiality of information rest, in addition, HDL coding rules are detailed in NUREG 7006 [5].

By using FPGA based security module, internal and external threats risk coming from the probability of malicious that can be inserted in HDL code can be prevented by independent V&V under highly controlled design and modification procedures and secure environment and by cybersecurity measures for programming device.

3 Design Theory

AES is the most important, secure, and widely used algorithm in cryptography, In this work AES-128 bit Algorithm is chosen to implement the FPGA based encryption module, AES-128 bits Algorithm is a block cipher, all plaintext bits are processed at the same time using encryption key which can be 128 or 192 or 256 bit key needs 10 or 12 or 14 round, respectively, according to the key length, a 128 bit length key is chosen for this design it need 10 rounds, As shown in figure (1) the encryption process need pre-round step by using XOR gate the inputs of this gate are plaintext and initial key, then there are two process iterate for 9 times, the first process is key expansion to generate the required key for each round according to figure (2), the second process deal with the output of the predecessor round to prepare data to the encryption round by running four operations before getting the round output ciphertext, these four steps are listed as flowing

1- bytes substitutions process using S-box which a constant 16*16 matrix

2- The output of substitution matrix is processed as 4*4 bytes matrix to run shift rows process by shifting the second row by one position and the third row by two positions and the fourth row by three positions.

3- After that, a mix-column process is run by multiplying each column of the shifted matrix by constant matrix

4- The output of step 3 is XOR with the output of the key expansion process to create the ciphertext of the round,

These 4 processes iterate 9 times, Round 10 run as the same previous 9 iterations except mix-column step, the shifted matrix of round 10 XOR with the key expansion output of round 10 directly to create the ciphertext [6]. Cryptographic keys are managed by using automated mechanisms with supporting procedures when cryptography is required and employed within the critical digital assets CDAs [3]

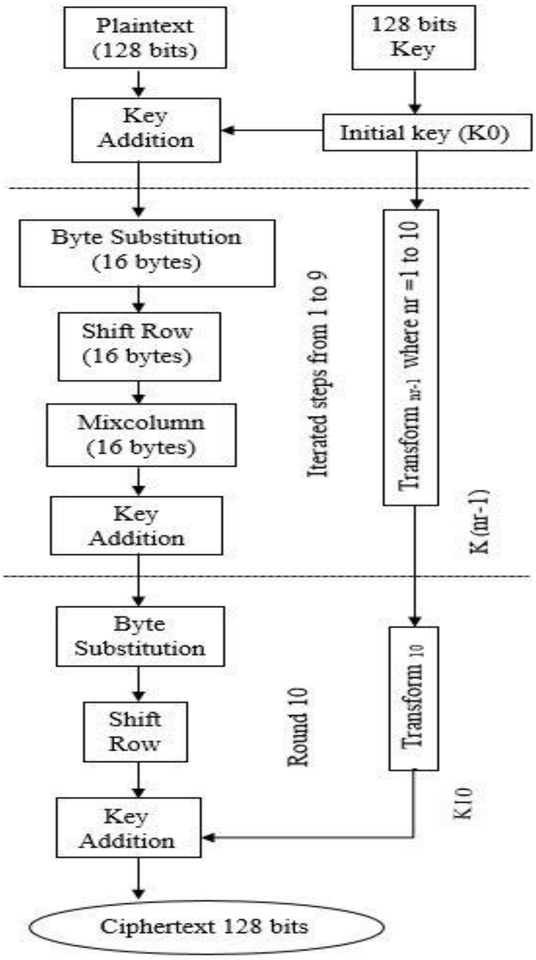


Fig .1.AES-128 Algorithm Flowchart

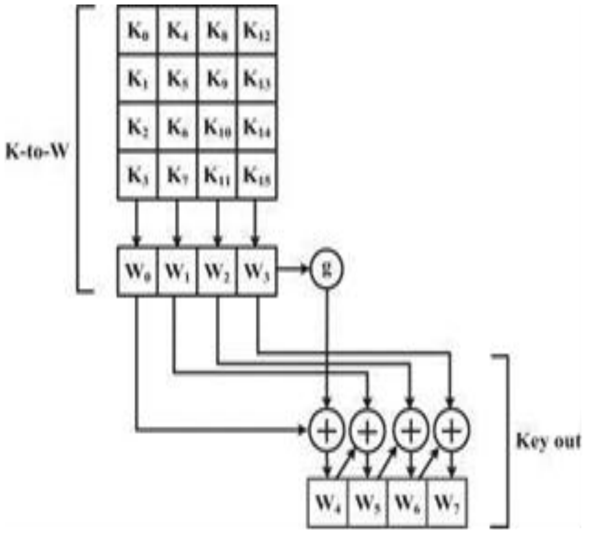


Fig .2 Key expansion

4 Function Flow Diagrams

The function flow of the Software based system depends on the serial execution of all function even they are independent functions, in AES key expansion process and data preparation process are independent functions, one of the most significant advantages of FPGA that it can run all independent functions in parallel that can reduce the execution time of whole system performance, as shown in figure (3) the serial execution of the function appears to function by function using software-based system, using FPGA the function flow enhanced as shown in figure (4) by run the independent function at the same time in parallel the natural of FPGA give this advantage and save execution time

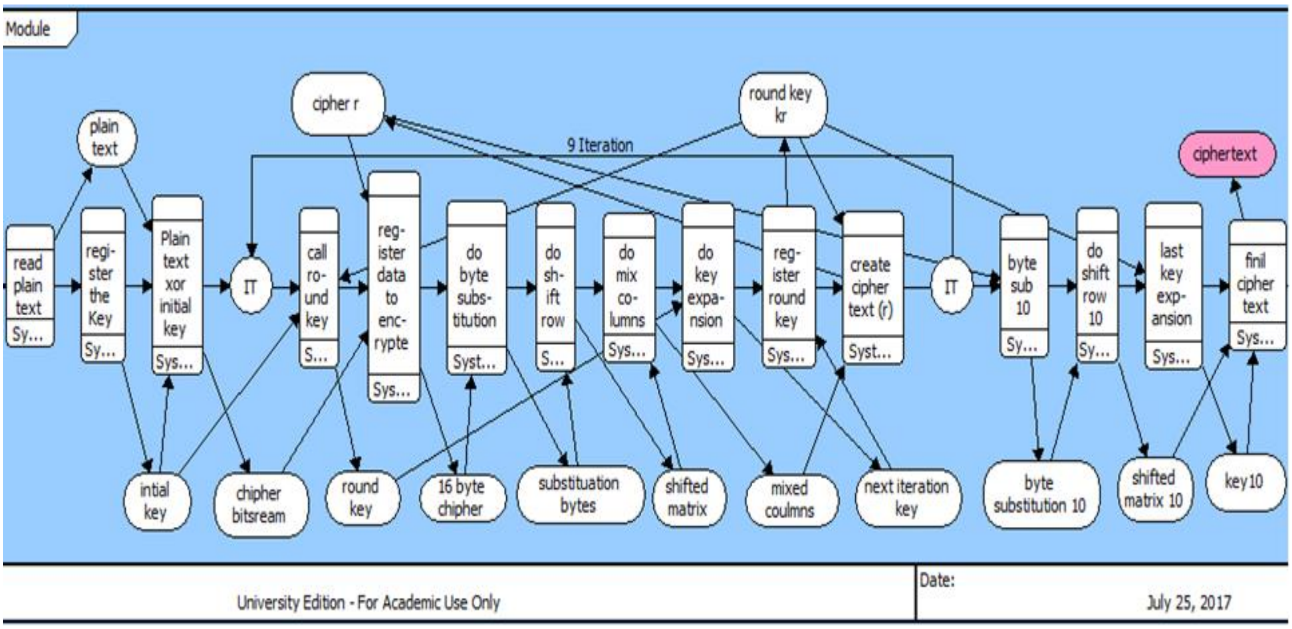


Fig. 3.Software and Microprocessor based system Enhanced Function Flow Bloc

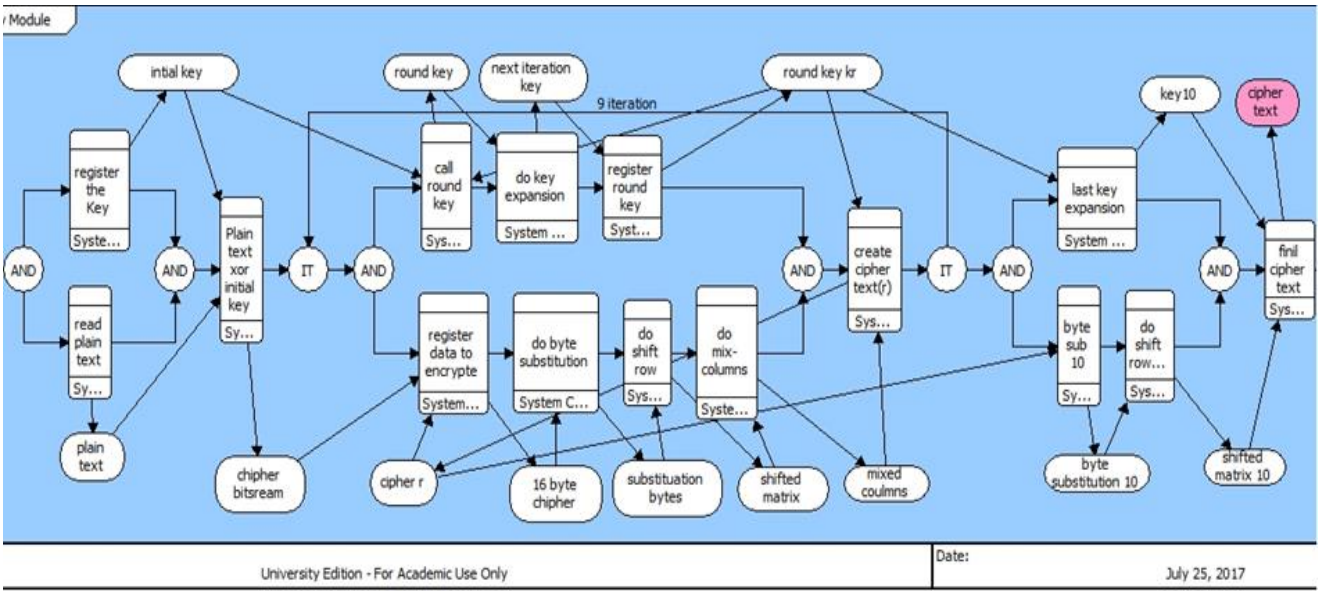


Fig. 4 FPGA based system Enhanced Function Flow Block

5 Modeling

Using Vitech CORE9 [7] MBSE tools, the logical architecture for the current and modified developed system was created as shown in figure (3), and figure (4) enhanced function flow block diagrams (EFFBDs), figure (3) illustrates software functions at the same time that improve the execution time for the same operation, as shown in figure (4) and flowchart in figure (1) key expansion and the three layers for data preparation process are independent processes, logic gates for each process can work in parallel. A dimensionless and non-real-time simulation is run to compare between FPGA based AES-128 bits encryption system and software-based AES-128 encryption system, it shows how the new design FPGA-based is faster than the other design, the new design is timely manner as shown in figure (5) and figure (6), it describes total execution performance time for the both systems

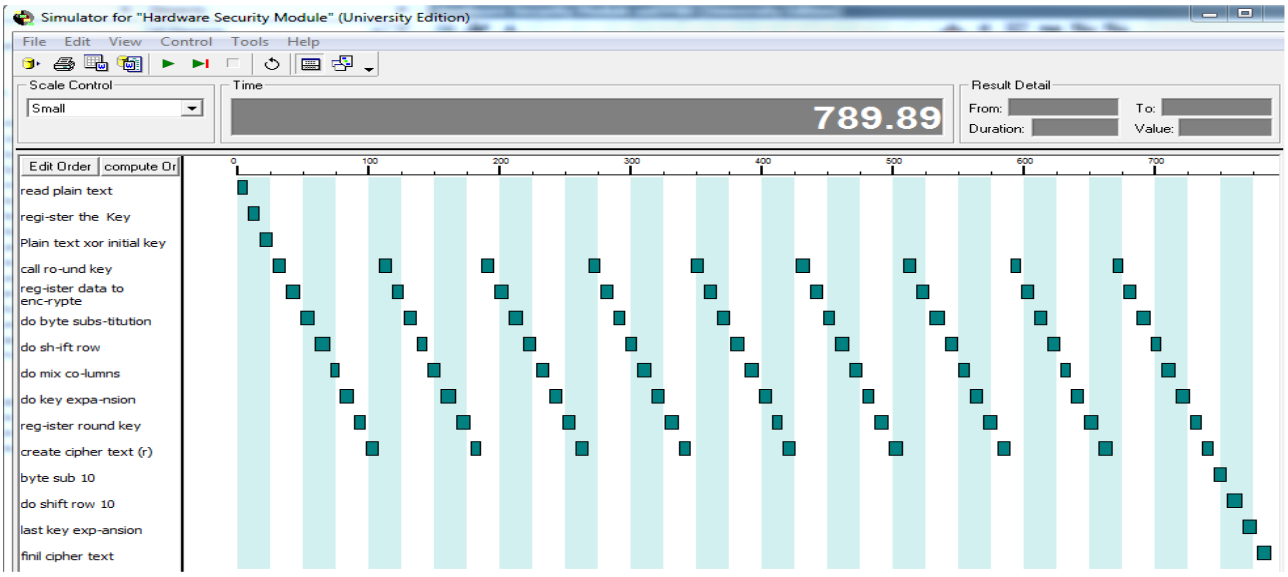


Fig. 5 Simulation of Software-based system

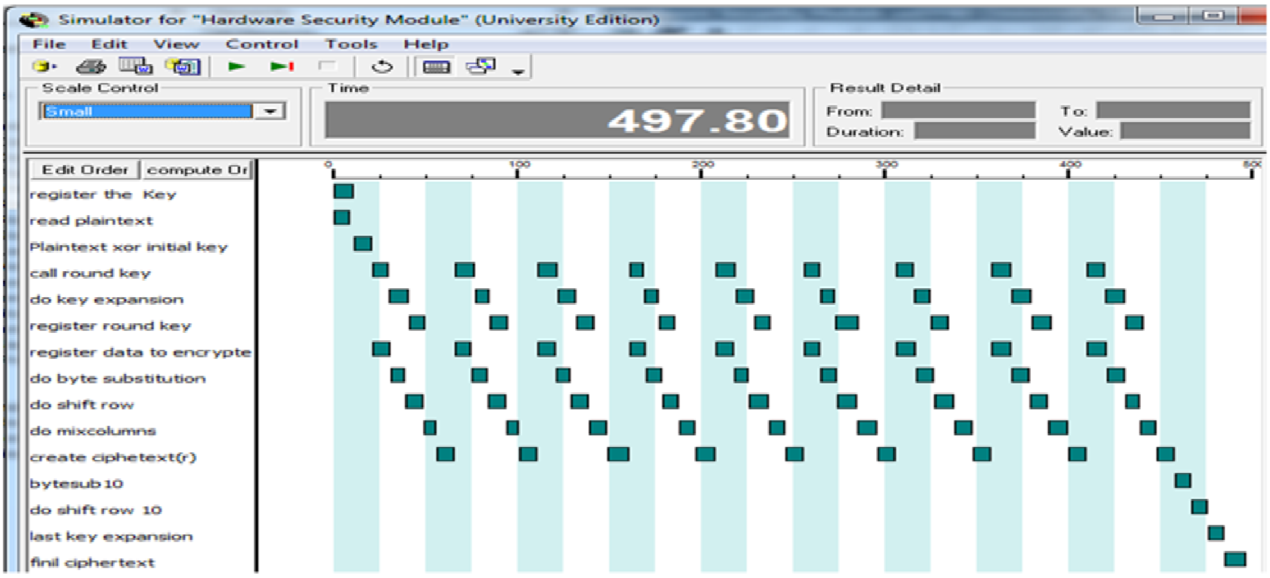


Fig. 6 Simulation FPGA based system

5 Coding and Testing

By using ALDEC as a programming and testing tool for creating and verify the integrity of HDL code structure and functions; three HDL code sources are creating, the first source to perform encryption process layers and rounds the second source code for key expansion process each round, the third source code is developed to control serial communication between PC and FPGA to implement and test physical simulation and data transmission from PC to FPGA and vice versa, after code developing, there are many verification steps run to check the effectiveness of performance of the developed code to generate the ciphertext by applying AES-128 algorithm on a plaintext and using specific key, the output of the developed module is compared with a proven plaintext and key vectors listed in NIST SP 800-38A, Recommendation for Block Cipher Mode of Operation, a plaintext, and initial key test vectors are chosen to feed to the simulation process, By running simulator the generated cipher is equal to that one listed in NIST SP 800-38A Appendix (F) [8],the simulation run to deploy to NEXYS video FPGA board[9] , as shown in figure (7), this code shows the integrity of the code and hardware for implementation process and represents the components needed to perform this function ,it needs 1113 lookup table (LUT) and 939 flip flop (FF) which is to small number that makes deployment to large numbers and cheap FPGAs, this code uses a constant key it is reduce the number of input/output (I/O) resources needs in FPGA ,also it is suitable for limited area application like nuclear power plant site ,it is easy to distribute the key securely and no need to encrypt it, by running the simulation test in ALDEC using the pre-proven vectors of key and plaintext we get the same value of cipher text as shown in figure (7) in this simulation we feed the plaintext input by the following vector:

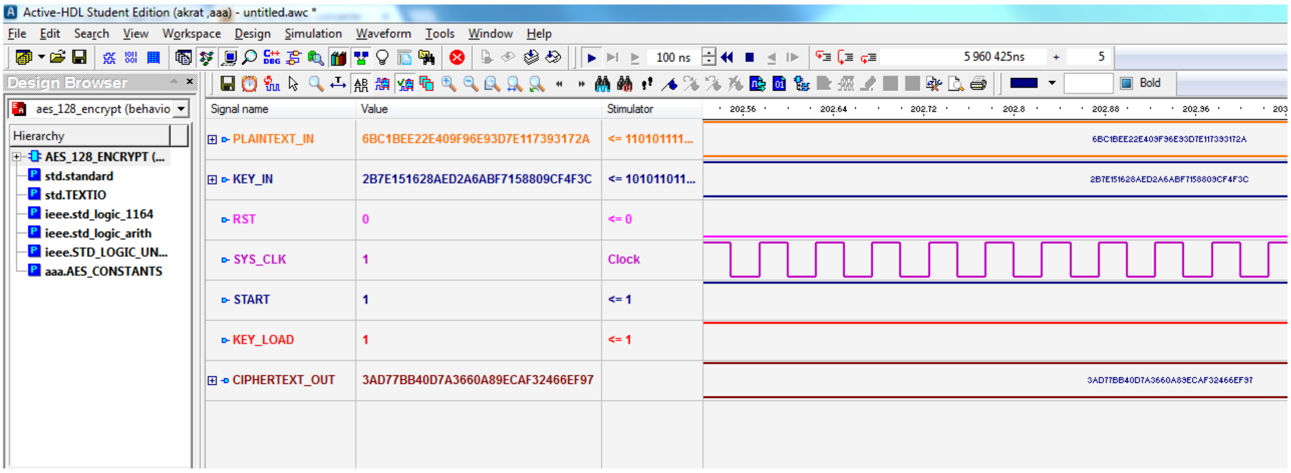
- Plaintext

(6BC1BEE22E409F96E93D7E117393172A)

- Constant initial key (2B7E151628AED2A6ABF7158809CF4F3C)

- Ciphertext

(3AD77BB40D7A3660A89ECAF32466EF97)


Active-HDL Student Edition (akrat ,aaa) - untitled.awc *
File Edit Search View Workspace Design Simulation Waveform Tools Window Help
100 ns
5 960 425ns
+ 5
Bold
Design Browser
aes_128_encrypt (behavio
Hierarchy
AES_128_ENCRYPT (...
std.standard
std.TEXTIO
ieee.std_logic_1164
ieee.std_logic_arith
ieee.STD_LOGIC_UN...
aaa.AES_CONSTANTS
202.56
202.64
202.72
202.8
202.88
202.96
203
6BC1BEE22E409F96E93D7E117393172A
2B7E151628AED2A6ABF7158809CF4F3C
3AD77BB40D7A3660A89ECAF32466EF97

Signal name	Value	Stimulator
PLAINTEXT_IN	6BC1BEE22E409F96E93D7E117393172A	<= 110101111...
KEY_IN	2B7E151628AED2A6ABF7158809CF4F3C	<= 101011011...
RST	0	<= 0
SYS_CLK	1	Clock
START	1	<= 1
KEY_LOAD	1	<= 1
CIPHERTEXT_OUT	3AD77BB40D7A3660A89ECAF32466EF97	

Fig .7 Code simulation using ALDEC

6 Conclusion:

Hardware-based security was developed in this paper using NEXYS video FPGA board to encrypt data using AES-128 and constant 128 bits key it is designed to control data transfer and mitigate MITM attacks for APR 1400 nuclear power DCS, system performance by using FPGA is improved ,FPGA based encryption module delivers many advantages than using software-based encryption system such as complexity in security regarding cybersecurity because no viruses for FPGA, System flexibility in case of upgrading or modification according to applying new algorithm FPGA is fit to apply reverse engineering no software or operating system needed for FPGAs operation, parallel processes execution ensures high response time compared to the other system, For development, CORE 9 is using to create and simulate EFFBD, ALDEC was used as a HDL code programming and testing tool to simulate and verify the performance of the developed module.

7 Further work

Further works focus on improvement of the designed FPGA-based prototype to perform full function of network cards, tradeoff analysis and technological risk are needed to assess the technologies readiness level of the designed module and cost, the interface between the designed module and other system is required to verify the computability and integrity of the whole system.

Acknowledgement

This work was supported by the 2017 Research fund of the KEPCO International Nuclear Graduate School (KINGS), Republic of Korea.

REFERENCES

[1] TCG Specifications Architecture Overview, August 2007, version 1.4

[2] 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/.

[3] U.S.NRC Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities”, January 2010.

[4] Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, National Institute of Standards and Technology NIST, Special Publication 800-37 Revision 1

[5]U.S.NRC, NUREG/CR-7006, Review Guidelines for Field- Programmable Gate Arrays in Nuclear Power Plant Safety Systems. 2009.

[6] C. Paar, J. Pelzl Understanding Cryptography Textbook, Springer, 2010

[7] Vitech COREsim User Guide, CORE 9 Version. [Cited 2016 August 16] Available from http://www.vitechcorp.com/.

[8] Block Cipher Modes of. Operation, National Institute of Standards and Technology NIST October 2011

[9] Nexys Video™ FPGA Board Reference Manual, May 2017 https://reference.digilentinc.com/reference/...logic/nexys video