Nuclear Engineering and Technology xxx (2018) 1–8

Contents lists available at ScienceDirect

Nuclear Engineering and Technology

journal homepage: www.elsevier.com/locate/net

Technical Note

Development of field programmable gate array–based encryption module to mitigate man-in-the-middle attack for nuclear power plant data communication network

Mohamed Abdallah Elakrat, Jae Cheon Jung*

Department of Nuclear Engineering, KEPCO International Nuclear Graduate School, Ulsan, South Korea

ARTICLE INFO

Article history:
Received 12 September 2017
Received in revised form
17 January 2018
Accepted 30 January 2018
Available online xxx

Keywords:
AES-128
Cyber Security
Encryption
Field Programmable Gate Array
I&C

ABSTRACT

This article presents a security module based on a field programmable gate array (FPGA) to mitigate man-in-the-middle cyber attacks. Nowadays, the FPGA is considered to be the state of the art in nuclear power plants I&C systems due to its flexibility, reconfigurability, and maintainability of the FPGA technology; it also provides acceptable solutions for embedded computing applications that require cybersecurity. The proposed FPGA-based security module is developed to mitigate information-gathering attacks, which can be made by gaining physical access to the network, e.g., a man-in-the-middle attack, using a cryptographic process to ensure data confidentiality and integrity and prevent injecting malware or malicious data into the critical digital assets of a nuclear power plant data communication system. A model-based system engineering approach is applied. System requirements analysis and enhanced function flow block diagrams are created and simulated using CORE9 to compare the performance of the current and developed systems. Hardware description language code for encryption and serial communication is developed using Vivado Design Suite 2017.2 as a programming tool to run the system synthesis and implementation for performance simulation and design verification. Simple windows are developed using Java for physical testing and communication between a personal computer and the FPGA.

1. Introduction

One of the cybersecurity targets is keeping sensitive data secure. This target can be achieved by disclosing the sensitive data to authorized parties, preventing unauthorized modification, and guaranteeing that the data can be accessed by authorized parties when requested. To guarantee data the confidentiality, integrity, and availability triad, data need to be protected against man-in-the-middle (MITM) attacks. A MITM attack is defined as any attack in which the adversary devises a way to access the networks and inserts himself in between the server and client communication. MITM attacks are rare and difficult to execute, especially in a nuclear power plant, but they seriously impact data integrity and confidentiality. There is a low probability of occurrence of MITM attacks in data communication systems (DCSs) in nuclear power plants (NPPs) because the DCS is isolated from the internet and other off-site networks. In this article, we assumed that an MITM attack may occur when a portable device or media is connected to a DCS during maintenance and testing activities by contractors or suppliers; the consequence of this attack could be an unauthorized gathering of confidential data and modification of the traffic by injection of malware or malicious data, which could leave some persisting damaging effects. Use of cryptographic processes can offer an appropriate solution to mitigate MITM attacks [1,2]. In the current system, the cryptographic process is performed using software-based modules, e.g., Trusted Platform Modules. In these modules, the firmware can be updated. On the other hand, the Trusted Platform Module itself must be replaced when a new algorithm or higher hardware speed is implemented because of the nonreconfigurable properties of the system [3]. Using hardware-based encryption modules improves the information security. A variety of applications that are performed using software can be executed by developing hardware circuits such as a field programmable gate array (FPGA). The hardware is advantageous for various reasons: no required extra operating system, faster parallel execution of the independent functions, and greater security. FPGA-based encryption modules have more advantages than software-based modules, e.g., greater flexibility and better security. Using

* *Corresponding author.*
E-mail addresses: maakrat@yahoo.com (M.A. Elakrat), jcjung@kings.ac.kr (J.C. Jung).

https://doi.org/10.1016/j.net.2018.01.018

only software to protect a system is not enough. Using an FPGA improves cybersecurity by applying the model-based systems engineering (MBSE) approach to develop the FPGA-based encryption module. The proposed module provides a cybersecurity defensive architecture to combat malicious cybersecurity threats. By using the FPGA-based security module, the risk of internal and external threats can be reduced and achieved by independent V&V under highly controlled design and modification procedures, such as using a secure programming environment and with cybersecurity measures for programming the FPGA. By following these procedures, the probability of malware being inserted into the hardware description language (HDL) code can be prevented [4].

In this study, we used a model-based systems engineering approach to develop a hardware-based encryption module using an advanced encryption standard algorithm, the AES-128, for an NPP DCS. The V model was used as a system life cycle model to develop this FPGA-based advanced encryption module to ensure confidentiality and integrity of data transmission. We created both an enhanced function flow block diagram for a software-based encryption module and the FPGA-based encryption module and modeled them using the CORE9 university edition. HDL code was developed using Vivado Design Suite 2017.2. Code synthesis and implementation tests were run and analyzed. Design functions verification and validation were performed on the developed module. The designed hardware-based security platform performs data encryption using the Advanced Encryption Standard algorithm AES-128. The AES algorithm is considered to be the most popular and secure algorithm and is currently used worldwide. It is the first and only publicly accessible cipher that is approved by the US National Security Agency for high-level secret information [5].

2. System development cycle

We used the MBSE approach to develop the FPGA-based encryption module. The traditional "V cycle" is recommended in IAEA SSG-39 as model system life cycle for developing headwear programmable devices such as an FPGA. Fig. 1 describes the development process of the FPGA-based encryption module. A necessary adjustment is allowed on the V model due to the ability of the programming tool to perform and verify some phases automatically [6,7].

In developing an FPGA-based system, especially for large software, synthesis and place and route steps are run to check code-hardware integration. These steps may fail for various reasons, such as errors in the code, or some additional functions or requirements may need to be added for a debugging process and safe operation. It is essential to run the simulation and debugging processes to ensure code-hardware integration. After the compatibility of the software and hardware is satisfied, it must then be ensured that both will perform the required functions. Then, the code is ready to deploy without errors or damage to the FPGA board [8].

3. System analysis

3.1. Requirement analysis

According to NRC RG 73.54, the design needs to provide high assurance that digital networks and communication systems' equipment are adequately protected against cyber attacks, up to and including the design basis threat. All systems and networks need to be protected against any probable cyber attacks that would adversely impact the integrity or confidentiality of data and/or software, such as MITM attacks, by using cryptographic mechanisms. These mechanisms need to be able to recognize changes to information during transmission and on receipt. All systems and networks must deny unauthorized access to systems, services, and/or data. The cybersecurity plan must be established, implemented, and maintained to satisfy the cybersecurity program requirements of the regulation guide. This plan must describe how to control and protect the assets and maintain defense-in-depth protective strategies to ensure the capability to detect, respond, and recover from cyber attacks, to mitigate the adverse effects of cyber attacks, and to ensure that the functions of protected assets are not adversely impacted due to cyber attacks. In addition, the system needs to be capable of timely detection and response to cyber attacks. Referring to RG 5.71, Appendix A, cybersecurity must comply with the licensing requirements of 10 CFR 73.54; Appendices B and C give an acceptable set of security controls which are developed using the NIST cybersecurity standards and security controls. These controls depend on well-defined and well-understood vulnerabilities, threats, and attacks, in addition to well-understood and vetted countermeasures and protective techniques [9,10].

Acceptable security controls are transmission integrity and transmission confidentiality and should be achieved by using cryptographic mechanisms. When security requirements are considered as an integral subset of other information system requirements, the resulting system has fewer weaknesses and deficiencies, and therefore, fewer vulnerabilities can be exploited in the future [11,12].

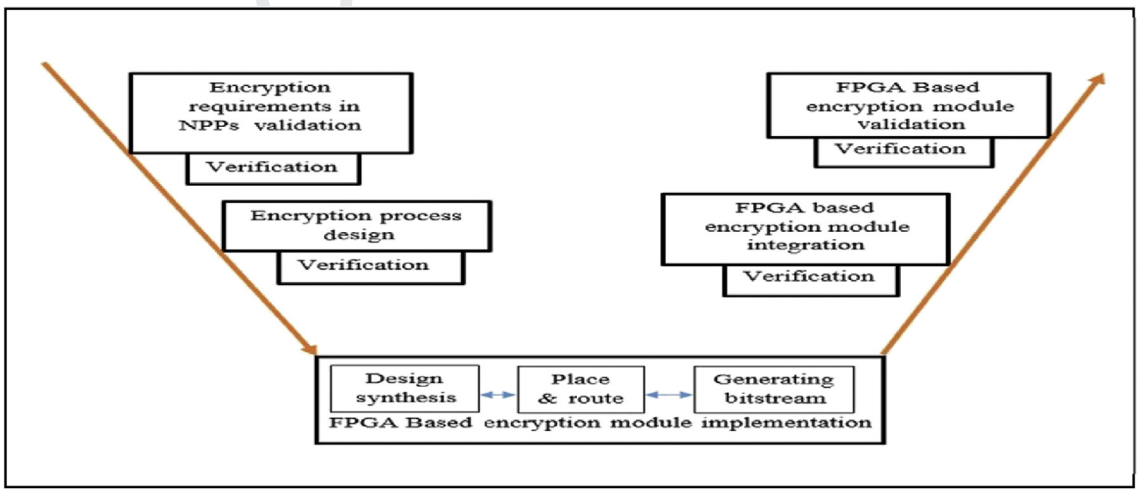

Fig. 1. V model system life cycle for FPGA-based encryption module.
FPGA, field programmable gate array; NPP, nuclear power plant.

Please cite this article in press as: M.A. Elakrat, J.C. Jung, 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 (2018), https://doi.org/10.1016/j.net.2018.01.018