UDC 004.056+681.518.5

**AL-SUDANI MUSTAFA QAHTAN ABDULMUNEM,**
**VYACHESLAV KHARCHENKO**

***National Aerospace University "KhAI" Kharkiv, Ukraine***

# CYBERSECURITY OF FPGA-BASED AUTOMATION SYSTEMS FOR SMART BUILDING

*Technology advancements such as programmable logic (FPGA) and mobile decisions have made the implementation of embedded intelligent systems within home and office appliances. This increased their capabilities and features. The given paper provides the properties of FPGA, and FPGA-based system of smart building in security field. The most important attacks (software and hardware) on FPGA and cyber-attacks on building automation systems are analyzed. Usage of FPGA as platform to protect the system of building automation system is described.*

***Key words:*** *Building Automation System, FPGA, Cybersecurity, WiFi, Smart Building*

## 1. Introduction

### 1.1. Motivation

With the development of new electronic technologies and their integration with older, traditional building technologies, building automation system is at last becoming a real possibility. It is not a new term for science society but is still far more away from people's vision and audition. This is because recent various works has been done in designing the general overview of the possible remote access approaches for controlling devices.

Building Automation System (BAS) comprises of electronic equipment that automatically performs specific facility functions. The commonly accepted definition of a BAS includes the comprehensive automatic control of one or more major building system functions required in a facility, such as:

- heating, ventilating, air conditioning (HVAC),
- lighting, power, lifts,
- security and others.

In short, BAS is to integrate the traditionally separate functions of Temperature Control, Energy Management, Fire and Security under one common operation (Fig. 1) [1].

BAS includes a collection of sensors that determine the condition or status of parameters to be controlled, such as temperature, relative humidity, and pressure. Similarly, output devices impart electronic signals or physical action to control the devices. Examples include electric relays or damper and valve actuators. Below there are some examples in which the BAS can lighten the loads as well as help to conserve energy.

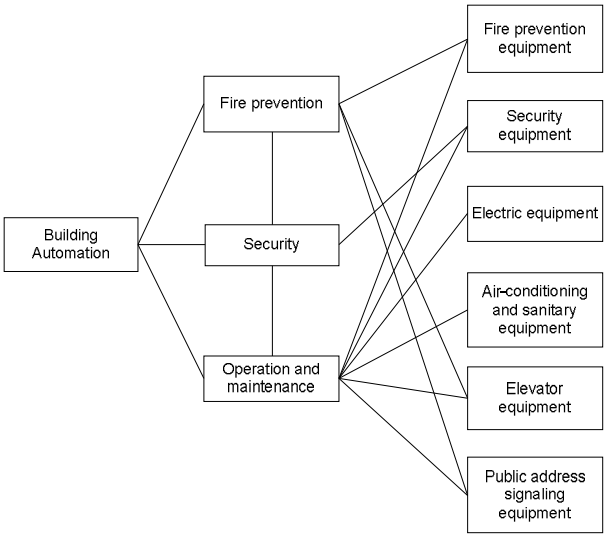


Fig. 1. BAS functions

### 1.2. Work Related Analysis

LAN communication technology [2] has been used in building automation system to control home appliances remotely and provide security when the user is away from the house. Internal communication in the building automation system between sensor and control unit is wireless, but not all communications are wireless. The paper [3] presents a Zigbee Wireless Network (ZWN) which consists of distributed devices that provide sensing features such as temperature, sound, vibration, pressure, motion. In [4] the IOT describes a system where digital world is connected to physical world via global network.

The major challenges with building automation system (smart building) are the reliability of the sensory

and surveillance system. FPGA platform is applied for building automation to increase security and reliability of system. To avoid system failure, we will present cybersecurity on FPGA and effect on it.

### 1.3. Goals and Structure

Analyzing attacks on building automation system we develop model of a platform on FPGA to protect system from failure with high reliability and efficiency and to choose the right application for model in building automation system structure. Structure of the paper is the following.

## 2. Cybersecurity of FPGAs

### 2.1. Advantages of FPGA

FPGA-based technologies have specific beneficial properties regarding critical applications [5]:

1. Implementation of safety functions without the use of any operation software and operating system:

– reduction in the time necessary for software verification in the design phase;

– parallel processing of all control algorithms within one cycle, and proven deterministic timing characteristics due to parallel operation of control algorithms;

– flexibility of the I&C platform which can be configured for any type of functions and reactor designs;

– easy modification of control logic without any need for hardware modification;

– possibility of implementing all safety requirements in integrated safety I&C systems;

– resistance to internal failures and external environmental impacts;

– resilience to obsolescence due to the portability of the Hardware Description Language (HDL) code between various FPGA-chips produced by different manufacturers.

2. FPGAs also have specific beneficial properties regarding cyber security that are different from those of Programmable Logic Controller (PLC) based technologies [6]:

– use of HDL codes (usually in VHDL or Verilog)without the need for an operating system for FPGA programming. At the present time, there are no known viruses and malware for HDL;

– FPGA-based designs and operation do not rely on an operating system and therefore do not have hidden, unused capabilities that can be attacked;

– HDL code is located in flash memory (separated chip) without having a physical access for modification;

– FPGA programming and reprogramming can be done only through a special interface. It is impossible to connect common storage media or communication devices that could infect the control logic code, as it was in case with the w32.Stuxnet worm;

– FPGA-based devices have simpler and transparent designs (compared to conventional PLC-based solutions).

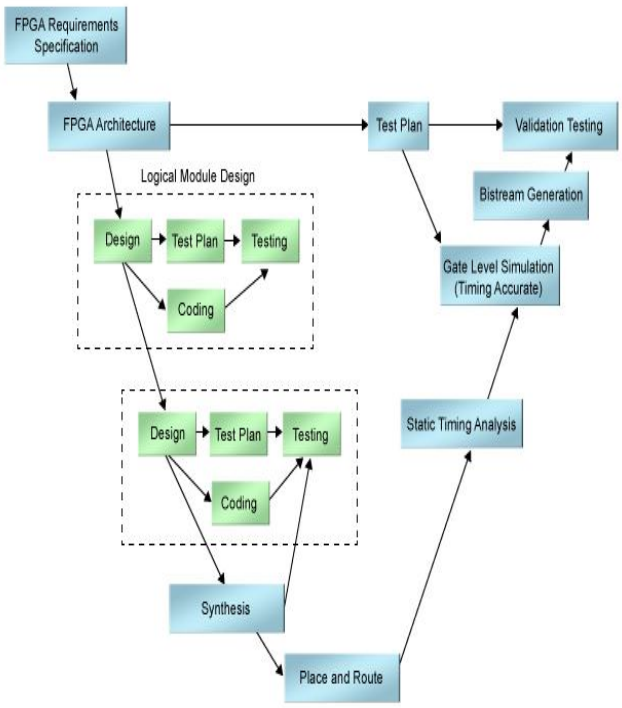


Fig 2. FPGA architecture design

### 2.2. FPGA Architectures

The architecture of FPGA can be explained as arrays of logic block, which can be interconnected using a programmable interconnect network along with input output block (IO Blocks).

The logic block in an FPGA can be as simple as a transistor or as complex as a microprocessor, which is capable of implementing various combinational and sequential logic functions [5, 7, 8].

The logic block in a commercial FPGA is basically multiplexer, Look-up-table or AND-OR array. The periphery of the FPGA consists of I/O blocks, which process signal to and from the FPGA.

The routing network in FPGA consists of wire segments of different lengths, which are interconnected using programmable switches. Wires for interconnection are laid in wiring channels or routing channels that run horizontally and vertically through the chip.

If long wire segments are used, only a fraction of

logic blocks can be used. If small wire segments are used to implement a logic function, more number of interconnections should be used resulting in an increased delay [8]. Different programming technologies are used to implement the programmable switches [9].

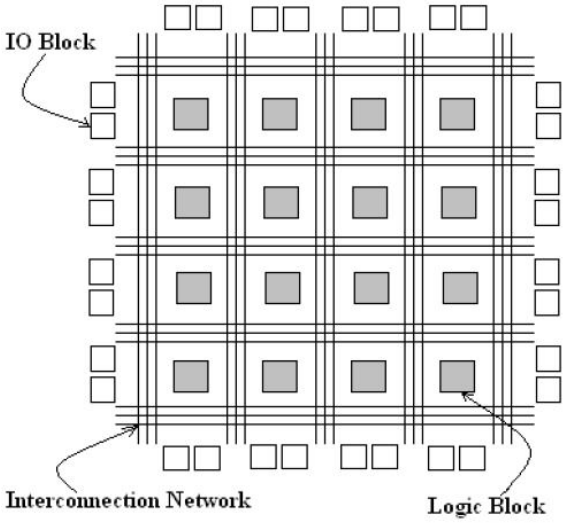


Fig. 3. General overview of FPGA

### 2.3. Criticality Matrix and Security Indicator

Building automation system is exposed to risks, risks that affect the functioning of the system and attack hardware or software. Attacks on communication, information, and sensors affect system performance and lead to its failure or shutdown.

Use of FPGA technology can reduce the risk of attacks. FPGA ability to avoid the failure of the system depends on IMECA analysis results by criticality matrix, which represents the percentage of the severe and probability of the failure similar FMECA table [10], Failure Modes and Effect (Criticality) Analysis (FMECA) is the most widely used reliability analysis technique at the initial stages of system development.

In this chapter we take an example of the work of the system at a time and determine risk of attacks on the system. The system worked in period from 9:00 am to 9.00 pm; with failure stage, retrieval system worked after the attack in a specific time periods is shown on Fig. 4.

Each of this state present system work, all this state has failure state when it goes down after attacks.

We can analyze attacks and the average of attacks is shown in criticality matrix which represents the building automation system S in four times during the day (S1, S2, S3, S4 as we divided) in the Table 1.

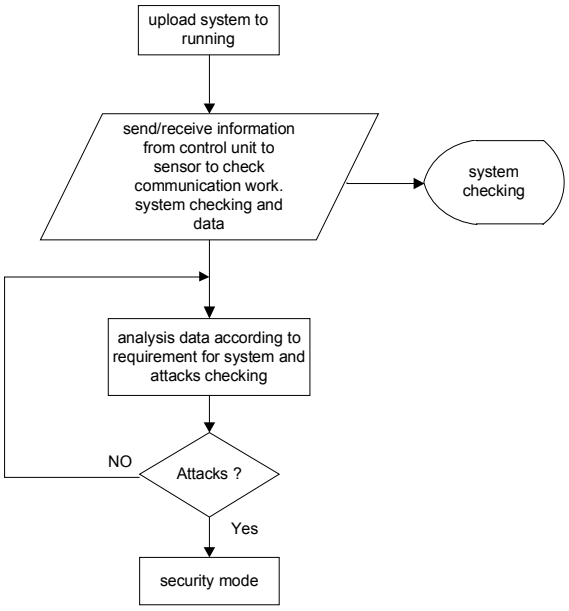


Fig. 4. System step

Table 1

Criticality matrix for system

| System | Severity of failure | | | |
|---|---|---|---|---|
| Probability | | H | M | L |
| | H | S1,S2 | | |
| | M | | S3 | S4 |
| | L | | | |

### 2.4. Countermeasures and Solutions

When a bit stream is sent from an external flash or is mote location to an FPGA, this stream can be intercepted and fraud can be committed. A solution to this problem is to encrypts the bit stream, and decrypts the stream internally in the FPGA.

To implement the encryption on an FPGA, we distinguish 3different approaches: one is purely hardware based, the other is software based, and the last one uses extra external components.

1. Hardware-based approach: First we have the built-in hardware decryption modules, as provided by the main FPGA vendors, such as Xilinx, Altera, Actel, etc.

Fig. 5 shows that the stream enters the decryption module and passes it to the in system programming when the HW decryption module is enabled, it can only be programmed with a bit stream using the same key and algorithm as the decryption module. Depending on the FPGA supplier, different methods to store the key

are applied. Xilinx, for example, stores the key in a special on-chip SRAM memory nested under a metal layer. This memory is powered by an external battery and should last for at least 20 years (theoretically up to 67 years) [11]. In order to program the key, one has to enter a key access mode. Accessing this mode automatically deletes the key in order to prevent read back.

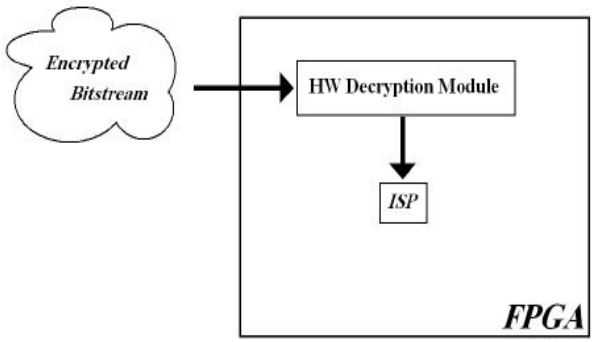


Fig. 5. HW built-in decryption

A mechanism used by Altera on the Stratix FPGA consists of choosing 2 keys, which are sent to the FPGA, where the two keys are encrypted using AES to produce another "real key". That real key is then transformed using a function before it is stored in a 256-bit nonvolatile memory. In order to decrypt a stream, the stored transformed key will be passed to the inverse function to reproduce the real key.

This feature protects the key to be simply read out, in case one should succeed to find the location and value of the key on the chip. Hardware based approach is less flexible since one can never change the encryption/decryption algorithm afterwards.

2. Software-based approach: Low cost FPGAs typically have no built-in decryption capabilities. But, when the FPGA has the ability to internally trigger a reconfiguration it is possible implement own decryption design.

In Fig. 6, the encrypted bit stream is first received by the embedded processor and stored in an external memory (this is especially needed when sending the bit stream by TCP/IP.

Once the stream is completely received, it is decrypted by the same processor and stored into the FLASH memory (externally or internally). The processors ends a signal to the ISP module and the FPGA starts to partially reconfigure itself with the required design.

The method for key storage is completely determined by the developer and will mostly be part of the implementation (part of the bit stream). Instead of using a simple variable or signal, one should define a function with spatially distributed bits. This is for the sake of hiding the key, instead of storing it on a logically and easily locatable place on the chip.

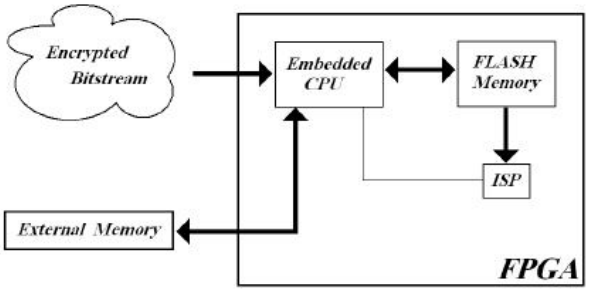


Fig. 6. A SW decryption design

When using a soft decryption implementation, we also have the possibility to use an IP core for the AES decryption. Using an IP core relieves the CPU from the decryption task, allowing more resources for other applications. Different IP cores are available, depending on the required throughput speed or available logic resources.

Unfortunately, a soft IP AES core will always be lost on each reboot. As a consequence, such an IP core cannot be used for secure uploading of a bit stream from an external FLASH (unless partial dynamic configuration is applied).

Besides the encryption of bit streams, there are currently there security features proposed on HW level: on-chip flash (for SRAM-based FPGAs), device authentication, tampering protection, key generation and multi boot capabilities.

## 3. FPGA-based Building Automation System

### 3.1. Building Automation System through a Central FPGA Controller

FPGA technology allows developing specific hardware architectures within a flexible programmable environment. This specific feature of the FPGAs gives designers a new degree of freedom comparing to microprocessor implementations. Describing FPGA applied for building automation system to control core of the system, for this task will Implantation communication device Bluetooth to connect between FPGA and user.

Bluetooth multiple topologies used to read sensory information to user through smart device or computer.

[12]. The architecture of system is shown on Fig.7.

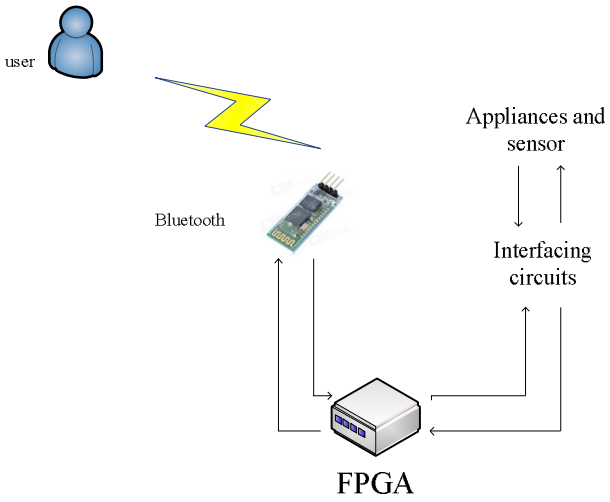


Fig. 7. A SW decryption design

The number of control and monitoring devices attached to the FPGA depend on the number of free input/output ports available on the FPGA. Furthermore, the system can be further expanded by cascading FPGAs or by multiplexing data coming from different sensors. This makes the system scalable. The devices connected to the FPGA can use either a wired connection or a wireless one, such as Zigbee or Infra-red. In this work wired solutions were used, the interface can be easily replaced by a wireless solution.

The modules interfaced were; a temperature sensor, a motion sensor, a light sensor, a relay switch, a Light Emitting Diode (LED) and a servo. These represent typical sensors used in the home which can allow the central controller to make decisions on whether to switch on or off various devices. Moreover, the circuits tested emulate low voltage switching, high voltage control via the relay, and motor control through the servo. The latter is useful for example to control light in a room by opening or closing shutters. Thus, the system covers most of the typical interfaces found in appliances in homes [13].

### 3.2. FPGA-based Solutions

After the analysis FPGA threats and solutions we can give the basic recommendations for reconfigurable systems. Solutions to reconfigurable security problems fall into two categories: life-cycle management and a secure architecture [14, 15].

1) Life-cycle management: In order to solve life-cycle management [15] offers to use software configuration management that covers operating system, security kernels, applications and computers. Configuration management stores software in a repository and assigns it a version number. The version shows the reputation of the tool, how it was calculated and tested, could it have any security flaw. That is why sometimes it is reasonable to wait until the new version will be fully tested before upgrading.

Hardware security should include control of development environment and tools, trusted delivery of chip etc. Cores and tools must be placed under configuration management system. Preferably it should be possible to verify faithful implementation of the design flow of each stage via formal methods, e.g. model checking.

The work [15] also offers an alternative – to build a custom set of trusted tools for security-critical hardware. The result will be less performance but more security. However the main goal of life-cycle management is ensuring that the output does not contain malicious artifacts or perform testing for fidelity to requirements and common failure modes. Management of life-cycle also includes delivery and maintenance (configuration updates, remote ones for some FPGAs).

2) Secure architecture: The ability to be programmed is the main advantage of FPGAs but it also introduces vulnerabilities. However FPGAs can provide the opportunity to incorporate self-protective security mechanisms at lower cost.

a) *Memory protection:* When considering memory protection it is possible to apply reference monitor. It is an access control mechanism that possesses three properties (self-protection, inability to bypass its enforcement mechanisms and subjection to analysis for ensuring its correctness and its correctness and completeness).

b) *Spatial distribution*: FPGAs possess powerful means of isolation. It is possible to isolate computation resources (e.g. cores) in space due to controlling the layout function because applications are mapped spatially to the device. Physical isolation of components more cleanly modularizes the system. It is easier to make checks for the design correctness because the parts of the chip which are not relevant to the component under test can be masked.

c) *Tags*: A tag is metadata that can be attached to individual pieces of system data. Tags can be used as security labels, and, thanks to their flexibility, they can tag data in an FPGA at different granularities. Once this data is tagged, static analysis can be used to test that tags are tightly bound to data and are immutable within a given program. Automatic methods of adding tags to other types of cores are needed for tags to be useful as a runtime protection mechanism.

d) *Secure communication:* Cores cannot be completely isolated because they must communicate with one another (e.g. via shared memory, direct connections, or a shared bus). When communication is done via shared memory, the reference monitor can

enforce the security policy as a function of its ability to control access to memory in general. Using communication via direct connections, static analysis can verify that only specified direct connections are permitted. Communication via a shared bus must address several threats (e.g. encryption of the bus). To address covert channels resulting from bus contention, every core can be given a fixed slice of time to use the bus [15].

## 4. Cybersecurity of FPGA-based BAS

The consequences of cyber-attacks in FPGA-based systems can lead to serious problems like misinformation, cripple tactical services, access sensitive information, espionage, data theft, financial losses, and other. The nature, complexity and severity of the cyber threats are increasing in time, which makes it difficult to build a good classification framework.

Cyber threats can be classified in several directions.

1. According to the intention: unintentional and intentional. The cause of the former is due to lack of training, software upgrade, equipment failures or software upgrades that unintentionally disturb the functioning of computers or corrupt data. The latter can be either targeted or no targeted.

a) Targeted attack aims at harming a person, institution or critical infrastructure system. Such may include the energy, finance, telecommunication, military, transportation or water sectors. They originate from spies, criminals, hackers, virus and malware programmers, or employees ("insiders") within an organization.

b) Non-targeted attack has no particular aim but is intended to do harm to as many digital systems as possible. Example of non-targeted attacks is viruses, worms, malware released on the Internet.

2. According to the effect of the attack: critical, non-critical and non-critical but dangerous.

c) Critical attacks can block or phase out entire systems, including infrastructural or certain modules, leaving them in limited or fully non-functional state.

d) Non-critical attacks do not harm or modify the system or its elements. For example – classified information may be fetched; information to be used for marketing or advertisement purposes may be gathered.

e) Non-critical but dangerous are such that do not cause immediate harm (no effect on the system or its elements) but may have critical effect at a later moment. For example – stealing passwords, identity theft, misuse of personal or confidential information, etc.

3. According to utilization: syntactic and semantic.

a) Syntactic attacks are direct – insert viruses, worms, malware, etc.

b) Semantic attacks modify and/or disseminate information. Modified information can be used for covering tracks of crime, or setting somebody to a wrong track.

Basic vulnerabilities in software systems of building automation system which can be used by intruders to insert malware:

a) inability to block connections from unauthorized devices;

b) lack of control over data gram broad casting in the smart home network;

c) Absence of authentication for control program that transmits the packet to the network of the building automation system;

Let us consider the main channels of the attack:

a) Bluetooth channel. Bluetooth networks are notoriously unreliable and can easily take the file with a virus from an attacker without requesting authorization [6];

b) Wi-Fi channel. Wi-Fi network can be easily broken by an attacker who can transmit the virus to the server bypassing authentication system;

c) HTTP-channel for remote access. HTTP-sharing with the Internet can be one of the ways of the attack penetration into the automatic control system of the building;

d) GSM channel. It is also possible to carry out unauthorized system control via GSM channel. It can be done, for example, by transmitting a SMS-message with a spoofed sender's number;

e) Conjugate channels. If the server of building automation system is also connected to the local network of the building, the malware may well penetrate from the local network. [7];

f) Preinstalled software and logic bombs.

Building automation system based on FPGA have the same specifications but they differ from other systems without FPGA, therefore, that the specification of the FPGA includes encryption, speed of reprogramming and performance of operations in parallel. The system depends on FPGA in two levels (Fig.8):

1. First - software level:

a) In the field of internal communications and external communication related to the Internet;

b) In internal communications and external communication related to the Internet. Security information in the control unit in the system of building automation system, which encrypts data sent and received between the control unit and sensors on system.

2. Second - hardware level: control sensors and work as platform for all system.

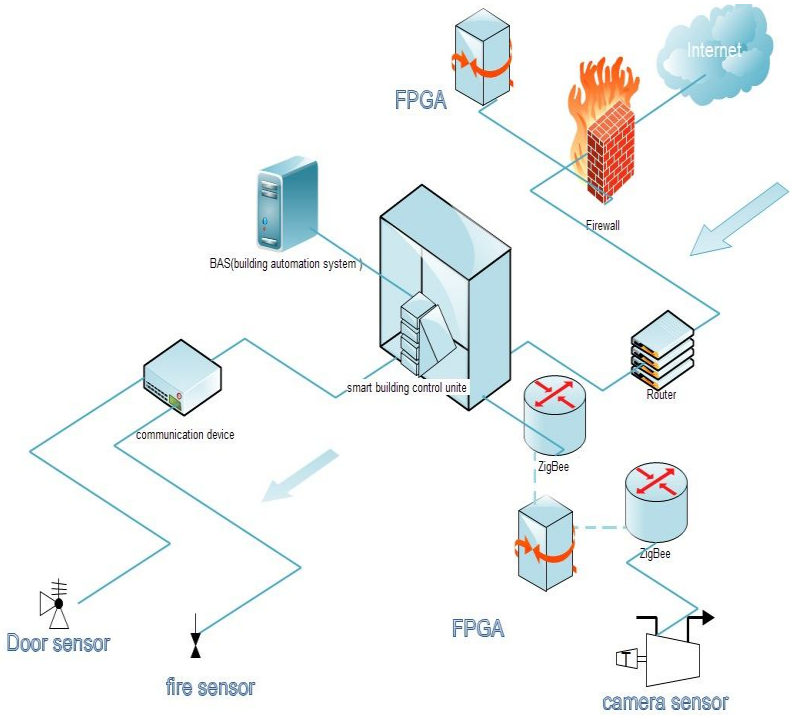


Fig. 8. FPGA-based BAS

## 5. Conclusion

Modern FPGAs have high computational efficiency, broad band for simultaneous memory access and flexible structure for interconnections. Configuration can be performed in software and hardware. Due to the obvious advantages FPGA expanding its application area, affecting even the most sophisticated computer systems that impose stringent requirements to the computing speed and quality of signal or data packets processing. Fig.8 shows the building automation system design, with FPGA applied in security inside building automation system field, and it will increase security for building automation circuit design.

Future work is to apply FPGA for WIFI technology, and attempt to build a safe system for computation using FPGA characteristic and introduce encryption on the FPGA platform.

## References

*1. Ler, Eng Loo. Intelligent Building Automation System [Electronic resource] / Eng Loo Ler. – Faculty of Engineering and Surveying, University of Southern Queensland, November, 2006. – Access mode: http://core.ac.uk/download/pdf/11036310.pdf. – 16.02.2015.*

*2. Int. Building Automation Using Wired Communication [Text] / A. Joseph et al. // Journal of Engineering Research and Applications. – April 2014. – Vol. 4, Issue 4( Version 9). – P. 63-68.*

*3. Mahendran, N. Multiple Sensor Feeding Supported Building Automation System Using Arduino Platform With Exposure of 802.15.4 Functionalities [Electronic resource] / N. Mahendran, G. J. Mathai, M. U. Veenesh // International Journal of Engineering Trends and Technology. . – 2013. – Vol. 4, Issue 2. – P. 77–80. – Access mode: http://www.ijettjournal.org/volume-4/issue-2/IJETT-V4I2P201.pdf. – 16.02.2015.*

*4. Brad, B. S. Smart Buildings Using IoT Technologies [Electronic resource] / B. S. Brad, M. Murar // Construction of Unique Buildings and Structures. – 2014. – № 5 (20). – P. 15–27. – Access mode: http://www.unistroy.spb.ru/index_2014_20/2_brad_20.pdf. – 16.02.2015.*

*5. Park, J. Hardware Security of FPGAs [Electronic resource] / J. Park. – Computer Engineering Iowa State University. – 5 p. – Access mode: http://class.ece.iastate.edu/cpre583/HW/mini_survey/FPGA_security.pdf. – 16.02.2015.*

*6. Secure FPGA Technologies and Techniques [Electronic resource] / A. Braeken, S. Kubera, F. Trouillez, A.Touhafi, J. Vliegen, N. Menten. – Access mode: http://ontwerpen1.khlim.be/~jvliegen/STRES/paper_FPL.pdf. – 16.02.2015.*

*7. Boyanov, L. Cyber security Challenges in Smart Homes [Text] / L. Boyanov, Z. Minchev. // In Proceedings of NATO ARW "Best Practices and Innovative Approaches to Develop Cyber Security and Resiliency Policy Framework", Ohrid, Macedonia, June 10-12, 2013, Published by IOS Press, NATO Science for Peace and Security Series - D: Information and Communication Security. – 2014. – Vol. 38. – P. 99-114 ; ISBN 978-1-61499-445-9 ; DOI 10.3233/978-1-61499-446-6-99.*

*8. Majzoobi, M. FPGA-oriented Security. Chapter 1 [Electronic resource] / M. Majzoobi, F. Koushanfar, M. Potkonjak. – 38 p. – Access mode: http://www.aceslab.org/sites/default/files/fpga_security_chapter_fk3.pdf. – 16.02.2015.*

*9. Binu, K. Mathew. New techniques to enhance FPGA based system security [Electronic resource]/ Mathew K. Binu, K. P. Zachariah // International Journal of Advanced Research in Computer Engineering & Technology. – July 2012. – Volume 1, Issue 5. – P. 91-94. – Access mode: http://ijarcet.org/wp-content/uploads/IJARCET-VOL-1-ISSUE-5-91-94.pdf. – 16.02.2015.*

*10. Yastrebenetsky, M. Nuclear Power Plant Instrumentation and Control Systems for Safety and Security [Text] / M. Yastrebenetsky, V. Kharchenko. – IGI Global, 2014. – 470 p. ; DOI: 10.4018/978-1-4666-5133-3.*

*11. An FPGA Design Security Solution Using a Secure Memory Device [Electronic resource] // Altera WP-01033-1.0, October 2007, ver. 1.0. – Access mode: https://www.altera.com/en_US/pdfs/literature/wp/wp-01033.pdf. – 16.02.2015.*

*12. Sriskanthan, N. Bluetooth based home automation system [Text] / N. Sriskanthan,. F. Tan, A. Karande // Microprocessors and Microsystems. – 2002. – № 26. – P. 281 – 289.*

*13. Andraka, R. A survey of CORDIC algorithms for FPGAs [Text] / R. Andraka // Proc. ACM/SIGDA Conf., 1998. – P. 191-200.*

*14. Illiashenko, O. Security Assessment and Green Issues of FPGA-Based Information & Control Systems [Electronic resource] / O. Illiashenko, V. Kharchenko, M. Ahtyamov // Critical Computing, KriKtech, November 30, 2012 ; DOI: 10.1109/DT.2013.6566309. – Access mode: http://www.researchgate.net/publication/261243319_Security_assessment_and_green_issues_of_FPGA-based_information__control_systems. – 16.02.2015.*

*15. Managing Security in FPGA-Based Embedded Systems [Electronic resource] / T. Huffmire, T. Sherwood, B. Brotherton, R. Kastneretet et al. – Access mode: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA516512. – 16.02.2015.*

*Поступила в редакцию 16.02.2015, рассмотрена на редколлегии 20.03.2015*

## КІБЕРБЕЗПЕКА ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ НА FPGA РОЗУМНОГО БУДИНКУ

***Аль-Судані Мустафа Кахтан Абдулмунем, В. С. Харченко***

Технологічні досягнення, такі як програмовна логіка (FPGA) і мобільні рішення, зробили можливим впровадження вбудованих інтелектуальних систем у різних пристроях будинків та офісів. Це збільшило їхні можливості та обсяг виконуваних функцій. Дана стаття досліджує властивості та можливості FPGA і систем на їхній основі для розумних будинків у контексті кібербезпеки. Аналізуються найбільш небезпечні типи атак на такі системи. Описується застосування FPGA як платформи для інформаційного захисту систем розумних будинків.

**Ключевые слова**: информационно-управляющие системы, умные дома, FPGA, беспроводные системы, кибербезопасность

## КИБЕРБЕЗОПАСНОСТЬ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ НА FPGA УМНОГО ДОМА

***Аль-Судани Мустафа Кахтан Абдулмунем, В. С. Харченко***

Технологические достижения, такие как программируемая логика (FPGA) и мобильные решения, сделали возможным внедрение встроенных интеллектуальных систем в различных устройствах домов и офисов. Это увеличило их возможности и объем выполняемых функций. Данная статья обсуждает свойства и возможности FPGA и систем на их основе для умных домов в контексте кибербезопасности. Анализируются наиболее опасные типы атак на такие системы. Описывается применение FPGA как платформы для информационной защиты систем умных домов.

**Ключевые слова**: информационно-управляющие системы, умные дома, FPGA, беспроводные системы, кибербезопасность

**Аль-Судани Мустафа Кахтан Абдулмунем** – аспирант каф. компьютерных систем и сетей, Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», г. Харьков**,** Украина.

**Харченко Вячеслав Сергеевич**– д-р техн. наук, профессор, зав. каф. компьютерных систем и сетей, Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт», г. Харьков, Украина, e-mail: v_s_kharchenko@ukr.net.