UDC 005.93:004.056

AL-SUDANI MUSTAFA QAHTAN ABDULMUNEM,
AHMED WALEED AL-KHAFAJI, V. S. KHARCHENKO

National Aerospace University "KhAI" Kharkiv, Ukraine

ATA-BASED SECURITY ASSESSMENT OF SMART BUILDING AUTOMATION SYSTEMS

The information and control system of smart building is considered as a set of subsystems including building automation system (BAS). BAS security and availability during its life cycle are assessed using the technique Attack Tree Analysis (ATA), and Failure Modes and Effects Analysis (FMECA). The FMECA is applied at the initial stage of analysis to assess criticality of BAS hardware/software failures and failed connections between components on the different levels of system design. Modification of FMECA is IMECA allowing to analyze modes and effects of attacks/intrusions. The ATA is applied to investigate any intrusions into the BAS by analyzing system probability of a failure caused by faults and vulnerabilities during operation time. The ATA is applied for different BAS subsystems and results of analysis are combined.

Keywords*: Smart building, Building Automation System, security, FMECA,IMECA, ATA*

1. Introduction

1.1. Motivation

Technological development and the development of modern devices used in human life offer services to people for controlling of many events of their lives, made it necessary to analyze these techniques and to measure the availability according to safety and security standards, information security analysing is our main task. In this paper, we analyze the information security for building automation system design which is the most commonly used in human life.

In this paper, we develop an ATA (Attack Tree Analysis) model to simulate security in BAS depending on measuring the probability of fault for the system under a scenario of cyber attacks, and analyzing the vulnerability of the primary elements in system design (BAS) according to [1] (FPGA, Database, Wireless unite) using FMECA tools to understand the connection between components in one level and describe the effect of the fault on the system and other components, this investigation will help a user (developer, programming) to increase the knowledge about the fault probability of the system for successful security during attacks period time and show the main threats in its design, and give the ability to manage design and avoid failures in future design

1.2. Work-related analysis

According to the international standards in [2], we can assess the level of risk for a building automation system and give the requirements that must be met to achieve the desired goal of safety and availability.

In [3] apart from performing security vulnerability analysis for the system design and identifying a threat which will be used to conduct security vulnerability analysis and describing system state under attacks, the technique can also be used to identify a failure or weakness, due to which the system is exposed to cyber-attacks.

In [4] the scenario-based information security risk evaluation method is shown. It is based on the thought of Advanced Persistent Threat (APT) attack by constructing risk scenario information system, the security risk stat us is evaluated and the example of the scenario attacks, which can help to manage security in BAS for the management level is given.

The primary goals of the work in [5] are security issues for system design and the integration of security subsystems, which significantly tightens security requirements to the protocol of a network control system, and weaknesses in the system design according to hardware and software components.

In [6, 7] during the analysis of FPGA the security of device was shown as a platform and vulnerability points were presented during the system development, at the same time, we can see the advantages of FPGA on other devices.

The most attacked targets in the database can be listed in [8] with number of attacks due to which we can analyze all possibilities of system fault according to this work, its primary task is to ensure security of a building automation system.

In [1] the system vulnerability is given based on

IMECA and FMECA and it shows the possibility of system fault during period of time, at the same time it shows there recovery state of system and the possibility to fix the problems. The main element in a building automation system is wireless unit in [9], the analysis of the unit according to a scenario of attacks can be done by taking into account the critical state of system during the period time of attacks.

1.3. Goal

In general, we calculate system dependability (reliability and security) taking into account the reliability issue, which depends on number of causes:

1) operation failure during system life;

2) manufacturing failure in components during system design;

3) software error.

As for the security side, we focus on the elements, which can lead system to be attacked by e.g. hardware Trojan and software vulnerability; we use FMECA to analyze the degree of fault on components and the relation between the components at one level, we use ATA tools to develop the model to measure the system probability to fail during time, we describe practical example and take different values of probability of components in system design and analyze the effect of these components for final result of top event in ATA design.

2. Vulnerability analysis of building automation system

According to [9, 1, and 10] design of BAS has three levels and that is why the analysis of vulnerabilities should be conducted on these three levels, measuring the vulnerability of these levels helps a designer to manage the risk and understand the degree of threat to system design, according to the previous analysis in [10], the main elements in system design that have high level of threat are FPGA, database, wireless unite). In this section, we will analyze these components and the received information will be used to update IMECA table and to support the root in ATA design.

2.1. Vulnerability analysis of FPGA architecture

Field programmable Gate Arrays (FPGAs) are silicon devices, which are ready to be used. They can be electrically programmed and then can be used as a kind of system or digital circuit.

One of the features of FPGAs is easiness of configuration and cost-effectiveness. It is also possible to make any updates and upgrade it. To do this it is necessary just to download a new application bit stream. FPGAs have numerous advantages but nevertheless, design flexibility remains their main advantage, when we consider cyber-security of FPGA we must take into account all parts involved in the life cycle of the FPGA chips and FPGA-based I&C systems.

These are an FPGA chip vendor, a developer of the I&C system as well as a user of FPGA-based I&C system. The analysis of cyber-security for FPGA technology includes the development process as well as the operation of the integrated I&C system. It must be noted that cyber-security vulnerabilities can be introduced by:

– the FPGA-chip vendor, during designing, manufacturing, packing and testing of FPGA chips;

– the I&C system developer, i.e. when FPGA electronic design is developed, implemented or tested;

– the operator of the I&C system, i.e. it is possible to make changes in the operating I&C system during operation or maintenance.

2.2. Vulnerability analysis of database architecture

Database attacks have increased because of the increased availability of access to data stored in those databases, database in BAS design contents the information, which is important for the system and data from different levels for management and storage, when the access to the stored information will be available for several users, it will increase the possibility of data theft, that is why it is necessary to control this kind of access because in the BAS system the attacker aims to access the important information, which he can use for attacks or monitoring the system.

Various types of threats that affect database security are shown below:

1. Privilege abuse: When database users have more privileges than usual. These privileges can be abused intentionally or unintentionally.

2. Operating System vulnerabilities: Vulnerabilities of operating systems such as Windows, UNIX, Linux, etc., as well as the services related to the databases could act as a way for unauthorized access. This can cause the Denial of Service (DoS) attack but it could be prevented due to updating the operating system security patches (when they become available).

3. Database rootkits: Let us consider what a database rootkit is. It is a program or a procedure that is hidden inside the database, which provides administrator-level privileges in order to obtain access to the data in the database and turn off Intrusion Prevention Systems (IPS), a rootkit is possible to be installed only after compromising the underlying operating system, this problem can be solved using periodical audit trails; otherwise, the presence of the database rootkit may remain undetected, weak

authentication: attackers can implement strategies such as social engineering and brute force to obtain database login credentials if authentication models are weak, the database may assume that the attacker has the identity of legitimate database users.

4. Weak audit trails: Having a weak audit logging mechanism in a database server may put the system under a critical risk, especially in industries with stringent regulatory compliance, if any incident happens, we should reproduce an event at a later point of time, to do this we apply PCI, SOX, and HIPAA, which need extensive logging actions, it should be noted that logging of sensitive or unusual transactions in a database must be done automatically to fix the problems. Audit trails are considered to be the last line of security in a database; they can detect an intrusion what in its turn will help trace back the violation to a particular point of time and a certain user.

2.3. Vulnerability analysis of wirelesses communication architecture

Let us consider what wirelesses networks consist of they have four basic components. These are: the transmission of data via radio frequencies; access points providing a connection to the organizational network and/or the client devices (laptops, PDAs, etc.); and Users, the given components may have vulnerabilities and be attacked and this will result in the compromise of confidentiality, integrity, and availability.

Wireless Network Attacks are as follows:

1. Accidental association: It is a type of an unauthorized access to wireless networks of a company. This means that when a user turns on a computer and connects to a wireless access point from an overlapping network, he might not even know that this has happened, such a security breach can expose valuable company information and create a link from one company to the other, it is the same when a laptop is connected to a wired network.

2. Ad-hoc networks: Ad-hoc networks are peer-to peer networks between wireless computers without an access point between them, such networks usually not very protected but in order to advance security encryption methods can be used.

3. Man-in-the-middle attacks: An attacker or man-in-the-middle creates computer, which is set up as a soft AP (Access Point), then he makes other computers to log into this soft AP; after that the attacker connects to a real access point using another wireless card, which offers a steady flow of traffic through the transparent hacking computer to the real network. Therefore, the attacker can sniff the traffic.

4. Denial of service: A Denial-of-Service attack (DoS) means continually attacking a targeted AP or a network using bogus requests, failure messages, premature successful connection messages, and/or other commands, due to this kind of attack legitimate users are not able to get on the network and it can even cause the network to crash, these attacks are based on the abuse of protocols such as the Extensible Authentication Protocol (EAP).

2.4. Scenario of cyber-attacks on BAS system design

The goal of a cyber-attack is to stop the performance of a target system by stealing, altering or destroying a specified target. It can be done by hacking individuals' or whole organizations' computer information systems stored at infrastructures, computer networks, and/or personal computer devices. It is usually hard to detect the source of the threat because it is usually anonymous; such attacks can be a cyber-campaign, cyber warfare or cyber terrorism, the ways of implementation of cyber-attacks include installing spyware on a PC, attempts to destroy the infrastructure of an organization or even entire nations, every day cyber-attacks become much more developed and dangerous.

Cyber-attacks are divided into two parts: hardware attacks aimed to stop operation of hardware components, and software, which have access to the system design and have an ability to read and change all the information inside the system design.

According to system design in [1], each component in the system design can get under attacks and be affected by attackers.

Hardware attacks can be an error or fault of manufacturer, which means there is a virus or a worm inside a chip and it can be active during some time of operation, we can measure system vulnerability, find weakness points in system design, and use them. Software attacks can appear using different tools for monitoring and reading data, e.g. when wireless units send and receive data through a radio wave.

All these scenarios of cyber-attacks on hardware or software can lead the system to failure by causing a fault in the hardware component and an error in the software component.

To analyze the security of a BAS we need to analyze and study all the possible attacks on the system and we need to think as attacker trying to access the system from inside, according to [1].We can divide the scenarios of cyber-attacks on design of the building automation system into three parts:

1. The attacker accesses the network using specific tools to monitor the network, getting the access inside has another goal; it depends on the purpose of the attack, in the first state the goal of the attacker is to monitor the network and to read the data between levels.

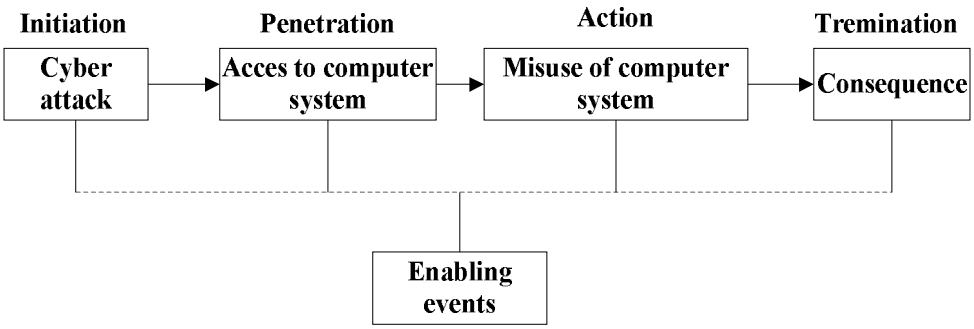

Fig. 1. Elements of a cyber threat scenario

This kind of attacks has longer effect on the system because it is not easy to detect hem during the system performance, which gives the system sometime to recover and takes longer time to solve the problem. To avoid such a problem and kind of attacks it is needed to increase network security.

2. Another scenario is if the goal of the attacker is to stop the system performance, it can be done by adding a worm (a virus) to the system and let the system work after some period of time or stop the performance directly.

The recovery time for this attack is different, it depends on which level had attack, i.e.:

a) if the attacker aims to attack the automation level and stop one of its components, in this case, we can detect the system error and there is a possibility to recover by changing or updating the system during recovery time, the system may recover but it will not have the full ability to work.

b) if the goal of attacker is the management level, the recovery time in this case will be complex because this level controls all system tasks and the system performance may be stopped, due to cyber-attacks on the management level, the recovery time will be long and also it will be expensive to update;

3. Error of design is also kind of cyber-attacks, which affects the system performance and puts the design at risk. Figure 1 shows the steps of cyber security attacks based on system attacks, it can be used to understand the strategy of attacker when he tries to access and attack BAS.

3. System analysis using FMECA and ATA

In general, the goal of attacks is to make the system have a failure to perform its tasks according to system architecture design, a failure means the identification and characterization its potential mechanisms in systems and the possibility of actual failure occurrences in operational systems, in order to protect the system developers and users must find the answers on the following three questions: "How can the system fail?", "What effects will a failure have?", and "How many failures will the system experience?", the following chapter will present two most useful techniques that have been created to answer these questions, the next step is to describe system cyber-attacks according to these two methods.

3.1. FMECA and IMECA

Failure Modes and Effects Analysis (FMEA) is an engineering process, which is used to study the potential effects of failures on a system as well as its environment, in certain cases the criticality of the effects is also considered, that is why the technique is called a Failure Modes, Effects and Criticality Analysis (FMECA).

FMEA and FMECA are the most popular tools to find design defects during development of a system. They also facilitate troubleshooting problems during system operation; in this paper we use the same processes of these methods but taking in account added intrusion possibility of system failure IMECA, it is the same technique but it deals with the system fault according to the intrusion, it can be from software design or in our case– vulnerability of system according to cyber-attacks.

According to the scenario of attacks, which is analyzed in Section 2, we can apply IMECA to analyze BAS security within this scenario and measure level of failure degrees, which can be done on system, according to security analysis, we can divide security to elements (hardware, software).

In this paper, we use FMEA to show attacks result in the hardware part of the system design as in the Table 2. IMECA is used to analyze the software part of the system design as shown in the Table 1. Both of these analyses in two tables depend on the scenarios in Section 2.

3.2. Attack Tree Analysis

Let us consider an attack tree. It is an analytical

ISSN 1814-4225. РАДІОЕЛЕКТРОННІ І КОМП'ЮТЕРНІ СИСТЕМИ, 2016, № 3 (77)

Table 1

System analysis according to cyber-attack scenario using IMECA

No	Intrusion attack mode	Component	Attack nature	Case of attack	Influence on operability	Attack results	
						Security	Availability
1	Communication level	Wi-Fi	passive	Attacker has availability to access to wireless local area and to monitor all the transmission data.	Interruption	All the data will be monitoring by attacker in the communication level or another level in the system.	There will be no effect on system availability; the goal of the attack is to monitor transmission data.
			active	After attacks he has the possibility to enter network, starts to break the connection between levels using different tools by creating virus and injection in the system.	Termination	According with attack the goal is to stop system work, in result there will be no security in all system levels.	System going to shut down state; in the next step the system will try to recover and back to up state; this process takes time and depends on the error detection in the system performance.
2	Management level	Database	passive	According to cyber-attacks, attacker has possibility to access the system database, read, and write the information.	Interruption	In this case, security will be at the minimum level, because attacker has the possibility to freely control all data inside the BAS.	Availability will depend on the goal of attacker; in this case the goal is to change data and system availability will be less than before, but if the goal is to stop system, then the system goes to shut down state.

Table 2

System analysis according to cyber-attack scenario using FMECA

No.	Component	Failure mode	Failure case	Failure effect
1	Management level	Hardware	Human error or design fault	This level is presented as control unite of the system, failure will lead to the system shutdown
2	Management level	Hardware	Error in design or interruption of a component	System performance interruption and recovery time will be long and costly because it is needed to change a component
3	Automation level	Hardware	End devices activity interruption in time	The system works normally, just with some missing of information. Recovery time will be short because it can be changed during short period of time

technique with a specified undesired state of the system, then the system is analyzed in the context of its environment and operation to find all possible ways of the occurrence of a failure, we will consider two basic types of attack tree gates.

The OR-gate and the AND-gate, the OR-gate is applied to show the output event; this output event can only occur if one or more of the input events happen, the AND-gate shows that the output attack occurs only when all the input attacks occur.

When we need to analyze the system, we select a particular event of the system as a target of an attacker, and then determine the immediate, necessary, and sufficient causes for the occurrence of this target. note that these causes are not the basic of the goal but they are immediate causes for the event, these kinds of goals we now call sub-goals, now we can proceed to determine their immediate, necessary, and sufficient causes. Therefore, we go down the tree step by step until we reach the limit of resolution of our tree, i.e. a leaf node (atomic attack) of an attack tree.

Security is primary goal of our work; it depends on analyzing the threat of the system and its vulnerabilities to understand the way, which an attacker can choose to attacks the system. Figure 2 shows system levels and the priority of each level according our analysis. It can be seen that the communication level has the priority and direct connection, which can lead to the system failure state, these two levels can be connected together and they cannot bring the system to the failure state because it depends on whether they both have faults at the same time but there is a low possibility of a fault to appear, in general a system failure can be when there is a fault in the communication unites or one of other levels.

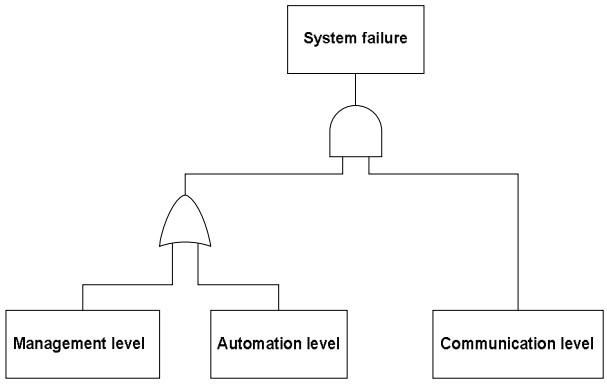

Fig. 2. ATA analysis of BAS levels

Taking into account the all possibilities of attacks, which can be aimed at the system and on the components in each level and according to cyber-attacks scenarios in Section 2.

The aim of the ATA analysis is to calculate system dependability (availability, security), the dependability helps a user (developer, designer) to understand how the system works according to the weakness in design, which can be used by an attacker. For security and for reliability area the ATA analysis shows what requirements are needed to increase the system availability during the system life.

In Figure 3 we apply the ATA to analyze ZigBee dependability and show the possibility to build a tree that contains availability and security.

According to the analysis we can see the following reliability issues: operational physical failures, manufacture (physical) failures, software errors; and security issues: hardware (Trojan/backdoors, Software vulnerabilities).

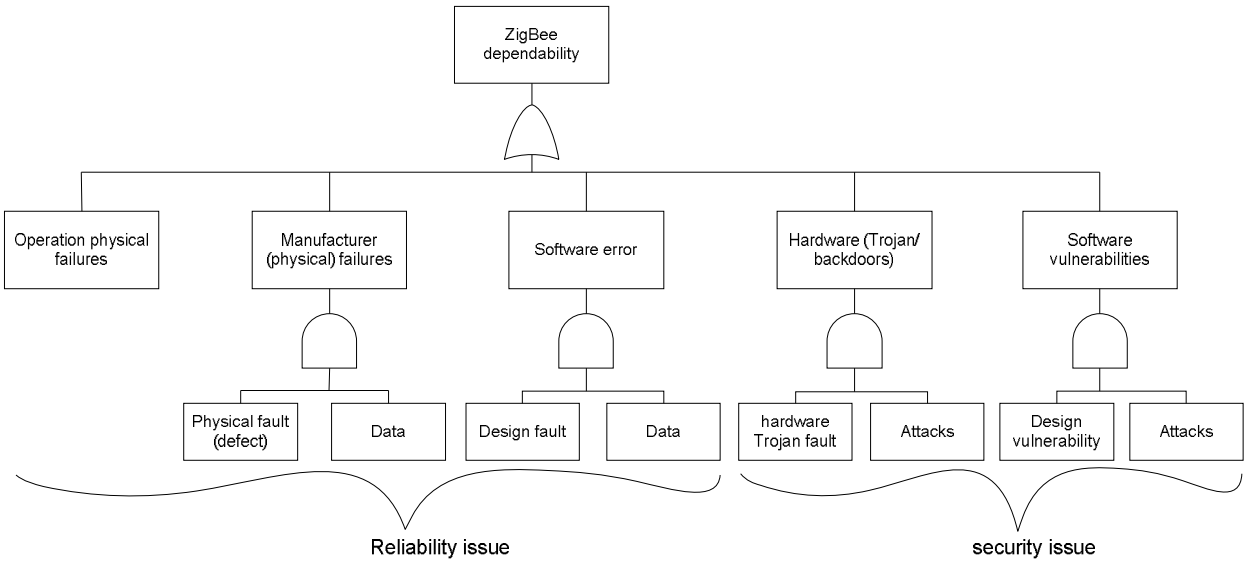

Fig. 3. Dependability analysis of ZigBee according to ATA

We analyze the security of the system component as shown in Figure 4. There is a big tree for system analysis, which considers all possibilities of faults in the two sides: hardware and software; our analysis is based on the basic design and it has remained similar to other designs, we can say that all the BAS are involved in this design. In this section, the analysis will be divided into two parts, to begin with we analyze the system components and the probability of fault according to the scenario of attacks and threats, then we use practical results for system components to show the final result for the system probability of fault and how it will affect the security, our probability analysis can start with the communicati1on divided into three components.

ZigBee used in the end device to send and receive signals from/to other components. ZigBee can have two kinds of fa1ults: one is introduced by a manufacturer (inside a device) and it can be activated during the life cycle of the device; and second fault is in software and it can be done when an error appears in code design and it can be from outside, i.e. like a hacker or designer error.

Wireless network unite which is responsible for data transfer between levels can have a fault in two ways: first in the software, which it can be done when there is an error from manufacturer or design user, and second is in hardware when there is error in updating data, which can affect unit components.

Automation level has two components:

1. FPGA. This unit can have a fault according to three scenarios of faults:

1) hardware fault means chip damage;

2) software fault depends on VHDL language program, which can have a fault from a user during design or form attacker;

3) the last can be attacks directly from hacker by using radio wave to affect a chip according to [9].

2. End device can be affected just when there is any hardware damage.

Management level depends on four components as show in Figure 3, and we analyze two components:

1. Database because it is our primary task of system analysis. It can have two parts of fault (software, hardware). Software faults depend on degree of fault because in general software fault can be affected by a human error during designing data for the system or by an attacker, which aims to steal or destroy the information inside the system. In the hardware part, a fault can be in manufacture design (chip).

2. SCADA system has different results of fault in a part of system performance control.

First is hardware failure:

a) computer components failure at central office;

b) network components failure between central office and intersection, and components on traffic pole failure.

Second is a software failure:

a) central Traffic Control System is unavailable (crashed);

b) operating system failed. Real-time application failed.

According to Figure 4 the top event for the ATA method is the probability of failure of system, in our model design we consider the connection between basic events as a serial connection, this means that a failure can be made when one basic event fails. This can be applied for all tree except the connection between the management level and automation level, the connection between them is parallel, because failure can happen when both levels have a fault at the same time. We simulate a practical case study of Building Automation System design according to [1] analysis.

This simulation aims to find the system probability of failure depending on the Initial elements.

The following equation describes the probability of failure to system and the relation between components as well as the final target according to ATA analyzing, P(t)=probability of failure, t=interval from (0,t) of system life:

$$P(t)_5 = 1-(1-P(t)_{14})(1-P(t)_{15}), \quad (1)$$

$$P(t)_7 = 1-(1-P(t)_{20})(1-P(t)_{21}), \quad (2)$$

$$P(t)_2 = 1-(1-P(t)_7)(1-P(t)_8)(1-P(t)_5)(1-P(t)_6), \quad (3)$$

$$P(t)_{10} = 1-(1-P(t)_{24})(1-P(t)_{22})(1-P(t)_{23}), \quad (4)$$

$$P(t)_9 = 1-(1-P(t)_{16})(1-P(t)_{17}), \quad (5)$$

$$P(t)_3 = 1-(1-P(t)_{10})(1-P(t)_9), \quad (6)$$

$$P(t)_{12} = 1-(1-P(t)_{25})(1-P(t)_{26}), \quad (7)$$

$$P(t)_{11} = 1-(1-P(t)_{18})(1-P(t)_{19}), \quad (8)$$

$$P(t)_4 = 1-(1-P(t)_{11})(1-P(t)_{12})(1-P(t)_{13}), \quad (9)$$

$$P(t)_x = P(t)_2 P(t)_3, \quad (10)$$

$$P(t)_l = 1-(1-P(t)_x)(1-P(t)_4). \quad (11)$$

Table 3 shows the system probability of failure during period of time from the system life cycle, these probabilities were calculated according to the typical values of failure rate of system components. Also we can see the result of the system probability of failure for top event of ATA analysis, total probability of failure (P(t)) it change depending on components probability of failure.

Conclusion

The article considers the case study- Building Automation System with its requirements to high level of security and safety during work. We analyze the

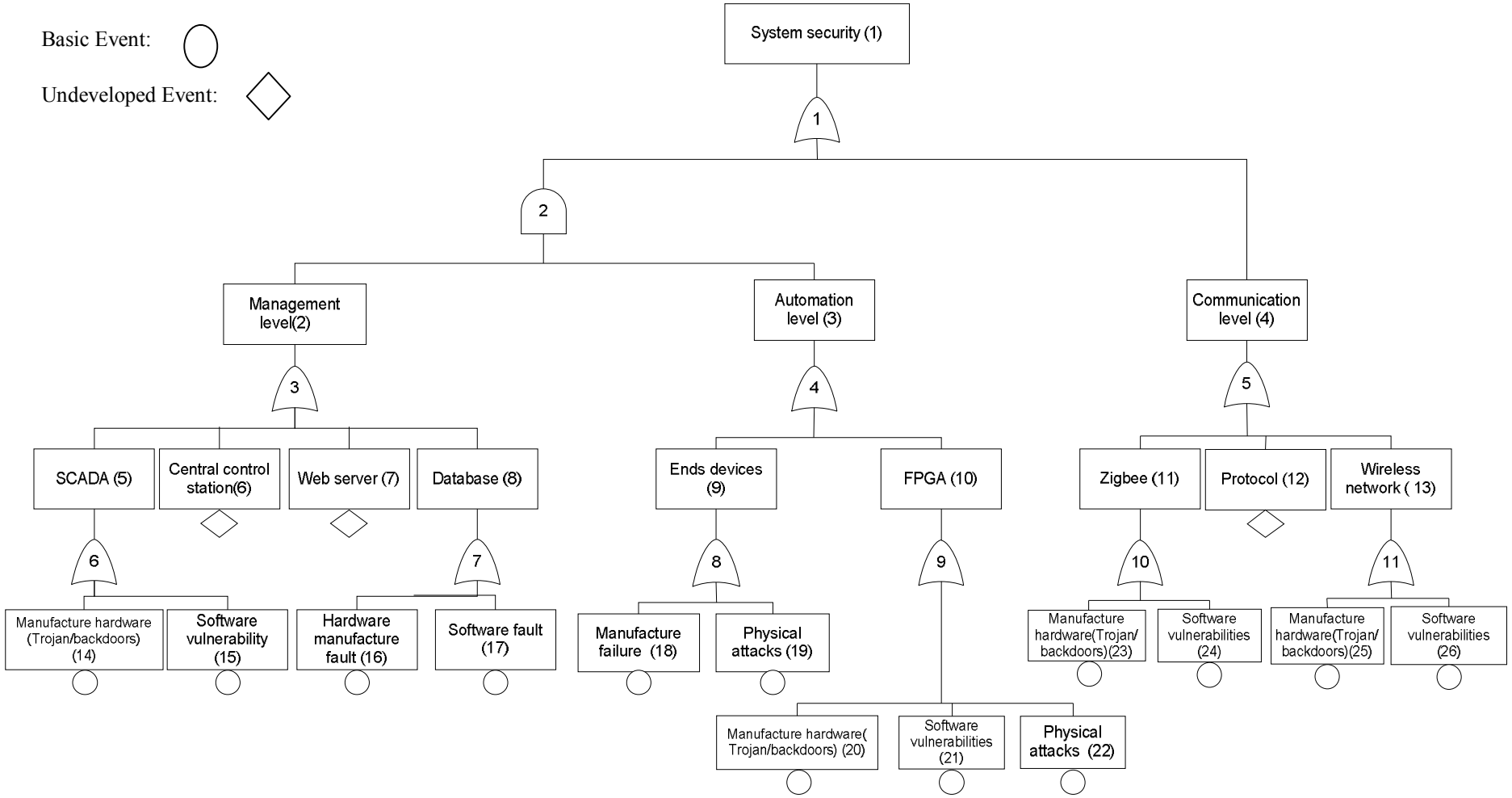

Fig. 4. ATA tree analysis of cyber-attacks on BAS components design

Table 3

Probability of system fault during period of time

Level of components	Number of components	Components	Probability	
Management level	1	Manufacture hardware (Trojan/backdoors) (14)	0.0000842	System probability to fault = 0.000281468
	2	Software vulnerability (15)	0.0000458	
	3	Hardware manufacture (20)	0.0000789	
	4	Software fault (21)	0.0000523	
	5	Central control station (6)	0.0000157	
	6	Web server (7)	0.0000791	
Automation level	7	Manufacture failure (16)	0.0000825	
	8	Physical attacks (17)	0.0000423	
	9	Manufacture hardware (Trojan/backdoors) (22)	0.0000373	
	10	Software vulnerability (23)	0.0000656	
	11	Physical attacks (24)	0.0000474	
Communication level	12	Manufacture hardware (Trojan/backdoors) (18)	0.0000063	
	13	Software vulnerability (19)	0.0000888	
	14	Manufacture hardware (Trojan/backdoors) (25)	0.0000764	
	15	Software vulnerability (26)	0.0000678	
	16	Protocol (13)	0.0000421	

system security using different tools: ATA tools and developments of these tools to match with system design and analyze the system probability of failure during a period of time of the system life. We use FMEA to analyze the vulnerability of system design (FPGA, Database, Wireless units).

In this paper, we calculated system probability of failure with practical data and analyze weakness points in the system design according to our vision of analyzing the system levels [1]. The technique presented in this paper can be used not just for the BAS but also to measure security in different system design.

The next step of our work will be to develop a Markov model to show all possibilities of system recovery and states of system under different types of system faults and the compare the recovery paths with cost and requirements of the user.

References (GOST 7.1:2006)

1. Al-Sudani, Mustafa Qahtan Abdulmunem. The method of IMECA-based security assessment case study for building automation system [Electronic resource] / Mustafa Qahtan Abdulmunem Al-Sudani, Ahmed Waleed Al-Khafaji, V. S. Kharchenko // Information processing systems. – 2016. – № 1 (138). – P. 138-144. - Available to: http://www.hups.mil.gov.ua/periodic-app/article/15263/soi_2016_1_31.pdf. – 15.05.2016.

2. International standard ISO/IEC 15408-2 [Electronic resource] / Third edition 2008-08-15 Corrected version 2011-06-01 // Information technology – Security techniques. – Evaluation criteria for IT security. – Part 2: Security functional components. – Available to: https://webstore.iec.ch/preview/info_isoiec15408-2%7Bed3.0%7Den.pdf. – 01.06.2016.

3. Baybutt, P. Scenario based approach for industrial cyber security vulnerability analysis [Electronic resource] / P. Baybutt, P. A. Baybutt // In: Hydrocarbon processing. – March 2004. – Vol. 83, No. 3. – 49 p. – Available to: https://www.researchgate.net/publication/228734434_A_SCENARIO-BASED_APPROACH_FOR_INDUSTRIAL_CYBER_SECURITY_VULNERABILITY_ANALYSIS. – 05.06.2016.

4. Ban, X. A Scenario-Based Information Security Risk Evaluation Method [Electronic resource] / X. Ban, Tong Xin // International Journal of Security and Its Applications. – 2014 – Vol. 8, No. 5. – P. 21-30. – Available to: http://www.sersc.org/journals/IJSIA/vol8_no5_2014/3.pdf. – 15.06.2016.

5. Granzer, W. Security in Networked Building Automation Systems [Electronic resource] / W. Granzer, W. Kastner, N. Georg // Vienna University of Technology Inst. of Computer Aided Automation, Automation Systems Group Treitlstraße 1-3, A-1040 Vienna, Austria. – Available to: http://osgug.ucaiug.org/utilisec/embedded/Shared%20Documents/Device%20Security/EpochInputs/BAS%20Security.pdf. – 20.06.2016.

6. Anonymous. FPGA Architectures: An Overview, Chapter 2 [Electronic resource]. – Available to: http://www.springer.com/cda/content/document/cda_downloaddocument/9781461435938-c2.pdf?SGWID=0-0-45-1333135-p174308376. – 29.06.2016.

7. Majzoobi, M. FPGA-oriented Security [Electronic resource] / M. Majzoobi, F. Koushanfar, M. Potkonjak // Hand book, chapter 1. – Avalable to: http://web.cs.ucla.edu/~miodrag/papers/Majzoobi_2011.pdf. – 04.07.2016.

8. Shulman, A. Top Ten Database Security Threats [Electronic resource] / A. Shulman. – Available to: http://www.schell.com/Top_Ten_Database_Threats.pdf. – 04.07.2016.

9. Al-sudani, Mustafa Qahtan Abdulmunem. Vulnerability analysis of wireless networks [Electronic resource] / Mustafa Qahtan Abdulmunem Al-sudani, V S. Kharchenko, D. Uzun // Radioelectronic and computer systems. – 2015. – № 2 (72). – P. 76-69. Available to: http://www.khai.edu/csp/nauchportal/Arhiv/REKS/2015/REKS215/AlSudani.pdf. – 15.07.2016.

10. Al-sudani, Mustafa Qahtan Abdulmunem. Cyber security of FPGA-based System for Building Automation System: Problem and Solution, [Electronic resource] / Mustafa Qahtan Abdulmunem Al-sudani, V S. Kharchenko // Radioelectronic and computer systems. – 2015. – № 1 (71). – P. 39-46. – Available to: http://www.khai.edu/csp/nauchportal/Arhiv/REKS/2015/REKS115/SudaniKHarch.pdf. – 15.07.2016.

11. Moore, A. Attack Modeling for Information Security and Survivability [Electronic resource] / A. Moore, R. Ellison, R. Linger // Technical Note CMU/SEI-2001-TN-001. – Avalaible to: http://www.sei.cmu.edu/reports/01tn001.pdf. – 20.07.2016.

12. Anonymous. Security Assessment via Attack Tree Model, Chapter 2 [Electronic resource]. – Available to: www.springer.com/.../9781461493563-c1.pdf/. – 25.07.2016.

13. Terrance, R. Attack Tree-based Threat Risk Analysis [Electronic resource] / R. Terrance // Amenaza Technologies Limited406 – 917 85th St SW, m/s 125Calgary, Alberta T3H 5Z9Canada. – Available to: https://www.amenaza.com/downloads/docs/AttackTreeThreatRiskAnalysis.pdf. – 28.07.2016.

14. Ghahramain, Z. An Introduction to Hidden Markov Model and Bayeusain Network [Electronic resource] / Z. Ghahramain // International journal of pattern recognition and artificial intelligence. – 2001. – № 15(1). – P. 9-42. – Available to: http://mlg.eng.cam.ac.uk/zoubin/papers/ijprai.pdf. – 01.08.2016.

15. Babeshko, Eu. Applying F(I)MEA-technique for SCADA-based Industrial Control Systems Dependability Assessment and Ensuring [Electronic resource] / Eu. Babeshko, V. Kharchenko, A. Gorbenko // Third International Conference on Dependability of Computer Systems DEPCOS-RELCOMEX. – 2008. – P. 315-309. – Available to: http://www.scirp.org/journal/PaperDownload.aspx?paperID=8252. – 01.08.2016.

References (BSI)

1. Al-Sudani, Mustafa Qahtan Abdulmunem, Al-Khafaji, Ahmed Waleed, Kharchenko, V. S. The method of IMECA-based security assessment case study for building automation system. *Information processing systems,* 2016. no. 1 (138), pp. 138-144. Available at: http://www.hups.mil.gov.ua/periodic-app/article/15263/soi_2016_1_31.pdf (accessed at 15.05.2016).

2. International standard ISO/IEC 15408-2. *Third edition 2008-08-15 Corrected version 2011-06-01. Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components.* Available at: https://webstore.iec.ch/preview/info_isoiec15408-2%7Bed3.0%7Den.pdf (accessed at 01.06.2016).

3. Baybutt, P. Scenario based approach for industrial cyber security vulnerability analysis. *In: Hydrocarbon processing,* March 2004, vol. 83, no. 3, 49 pp. Available at: http://www.primatech.com/images/docs/paper_cyber_security_risk_analysis_for_process_control_systems_using_rings_of_protection_analysis_ropa.pdf (accessed at 05.06.2016).

4. Ban, X. A., Tong, Xin. Scenario-Based Information Security Risk Evaluation Method. *International Journal of Security and Its Applications. China Information Technology Security Evaluation Center Beijing,* 2014, vol. 8, no 5, pp. 21-30. Available at: http://www.sersc.org/journals/IJSIA/vol8_no5_2014/3.pdf (accessed at 15.06.2016).

5. Granzer, W., Kastner, W., Georg, N., Praus, F. Security in Networked Building Automation Systems. *ViennaUniversity of Technology Inst. of Computer Aided Automation, Automation Systems Group,* Treitlstraße 1-3, A-1040 Vienna, Austria. Available at: http://osgug.ucaiug.org/utilisec/embedded/Shared%20Documents/Device%20Security/EpochInputs/BAS%20Security.pdf (accessed at 20.06.2016).

6. *Anonymous. FPGA Architectures: An Overview, Chapter 2*. Available at: http://www.springer.com/cda/content/document/cda_downloaddocument/9781461435938-c2.pdf?SGWID=0-0-45-1333135-p174308376/ (accessed at 29.06.2016).

7. Majzoobi, M., Koushanfar F., Potkonjak, M. FPGA-oriented Security. *Handbook, chapter 1.* Available at: http://web.cs.ucla.edu/~miodrag/papers/Majzoobi_2011.pdf (accessed at 04.07.2016).

8. Shulman, A. *Top Ten Database Security Threats.* Available at: http://www.schell.com/Top_Ten_Database_Threats.pdf (accessed at 04.08.2016).

9. Al-sudani, Mustafa Qahtan Abdulmunem, Kharchenko, V. S., Uzun, D. Vulnerability analysis of wireless networks. *Radioelectronic and computer system,* 2015, no. 2 (72), pp. 76-69. Available at: http://www.khai.edu/csp/nauchportal/Arhiv/REKS/2015/REKS215/AlSudani.pdf (accessed at 15.07.2016).

10. Al-sudani, Mustafa Qahtan Abdulmunem, Kharchenko, V. S. Cyber security of FPGA-based System for Building Automation System: Problem and Solutions. *Radioelectronic and computer systems,* 2015, no. 1 (71), pp. 39-46. Avalable at: http://www.khai.edu/csp/nauchportal/Arhiv/REKS/2015/REKS115/SudaniKHarch.pdf (accessed at 15.07.2016).

11. Moore, A., Ellison, R., Linger, R. Attack Modeling for Information Security and Survivability. *Technical Note CMU/SEI-2001-TN-001.* Available at: http://www.sei.cmu.edu/reports/01tn001.pdf (accessed at 20.07.2016).

12. *Anonymous. Security Assessment via Attack Tree Model, Chapter 2.* Available at: http://www.springer.com/.../9781461493563-c1.pdf (accessed at 25.07.2016).

13. Terrance, R. Attack Tree-based Threat Risk Analysis. *Amenaza Technologies Limited406 – 917 85th St SW, m/s 125 Calgary, Alberta T3H 5Z9 Canada.* Available at: https://www.amenaza.com/downloads/

docs/AttackTreeThreatRiskAnalysis.pdf/ (accessed at 28.07.2016).

14. Ghahramain, Z. An Introduction to Hidden Markov Model and Bayeusain Network. *International journal of pattern recognition and artificial intelligence*. 2001, 15(1), pp. 9-42. Available at: http://mlg.eng.cam.ac.uk/zoubin/papers/ijprai.pdf (accessed at 01.08.2016).

15. Babeshko, Eu. Kharchenko, V. S., Gorbenko, A. Applying F(I)MEA-technique for SCADA-based Industrial Control Systems Dependability Assessment and Ensuring. *Third International Conference on Dependability of Computer Systems DEPCOS-RELCOMEX*. 2008, pp. 315-309. Available at: http://www.scirp.org/journal/PaperDownload.aspx?paperID=8252/(accessed at 01.08.2016).

Поступила в редакцию 8.08.2016, рассмотрена на редколлегии 16.09.2016

ОЦІНЮВАННЯ БЕЗПЕКИ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ РОЗУМНИХ БУДИНКІВ З ВИКОРИСТАННЯМ ДЕРЕВ АНАЛІЗУ АТАК

Аль-Судані Мустафа Кахтан Абдулмунем, Аль-Хафаджі Ахмед Валід, В. С. Харченко

Інформаційно-керуючі системи розумних будинків розглядаються як множина підсистем, включаючи підсистему BAS (building automation system). Безпека і готовність BAS впродовж життєвого циклу оцінюються з використанням аналізу дерев атак ATA(Attack Tree Analysis) та аналізу видів і критичності наслідків відмов FMECA (Failure Modes and Effects Criticality Analysis). FMECA застосовується на початковій стадії аналізу для оцінювання критичності відмов, обумовлених дефектами програмних і апаратних засобів, комунікацій на різних рівнях BAS, а також атаками на вразливості. Модифікація FMECA – IMECA (Intrusion Modes and Effects Criticality Analysis) дозволяє аналізувати види і наслідки відмов внаслідок атак на вразливості. ATA аналіз використовується для дослідження втручань у BAS і визначення ймовірності відмов з їх урахуванням. Аналіз базується на комбінуванні результатів для різних компонент і рівнів системи.

Ключові слова: розумний будинок, система автоматизації, кібербезпека, FMECA, IMECA, ATA

ОЦЕНИВАНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ УМНЫХ ДОМОВ С ИСПОЛЬЗОВАНИЕМ ДЕРЕВЬЕВ АНАЛИЗА АТАК

Аль-Судани Мустафа Кахтан Абдулмунем, Аль-Хафаджи Ахмед Валид, В. С. Харченко

Информационно-управляющие системы умных домов рассматриваются как множество подсистем, включая подсистему BAS (building automation system). Безопасность и готовность BAS на протяжении жизненного цикла оцениваются с использованием анализа деревьев атак ATA (Attack Tree Analysis) и анализа видов и критичности последствий отказов FMECA (Failure Modes and Effects Criticality Analysis). FMECA используется на начальной стадии анализа оценивания критичности отказов, обусловленных дефектами программных и аппаратных средств и коммуникаций на разных уровнях BAS, а также атаками на уязвимости. Модификация FMECA – IMECA (Intrusion Modes and Effects Criticality Analysis) позволяет анализировать виды и критичность отказов вследствие атак на уязвимости. ATA анализ используется для определения вероятности отказов BAS с учетом этих атак. Анализ базируется на комбинировании результатов для разных компонент и уровней системы.

Ключевые слова: умный дом, система автоматизации, кибербезопасность, FMECA, IMECA, ATA

Аль-Судани Мустафа Кахтан Абдулмунем – аспирант каф. компьютерных систем и сетей, Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», г. Харьков, Украина, e-mail: mostafahkahtan1@gmail.com

Аль-Хафаджи Ахмед Валид – аспирант каф. компьютерных систем и сетей, Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», г. Харьков, Украина, e-mail: eng_ahmed.waleed@yahoo.com

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.kharchenko@csn.khai.edu

Al-Sudani Mustafa Qahtan Abdulmunem – postgraduate student of the Department of Computer Systems and Networks, National Aerospace University "Kharkiv Aerospace Institute" Kharkiv, Ukraine, e-mail: mostafahkahtan1@gmail.com

Al-Khafaji Ahmed Waleed – postgraduate student of the Department of Computer Systems and Networks, National Aerospace University "Kharkiv Aerospace Institute" Kharkiv, Ukraine, e-mail: eng_ahmed.waleed@yahoo.com

Kharchenko Vyacheslav S. – Doctor of Technical Sciences, professor, Head of the Department of Computer Systems and Networks, National Aerospace University "Kharkiv Aerospace Institute", Kharkiv, Ukraine, e-mail: v.kharchenko@csn.khai.edu.