UDC 004.056+681.518.5

Al-Sudani Mustafa Qahtan Abdulmunem, Ahmed Waleed Al-Khafaji, V.S. Kharchenko

National Aerospace University "KhAI", Kharkiv

THE METHOD OF IMECA-BASED SECURITY ASSESSMENT: CASE STUDY FOR BUILDING AUTOMATION SYSTEM

The information and control system of smart building is considered as a set of subsystems including building automation system (BAS), communication and controllers considering their failure rates. BAS security and system availability during life cycle are assessed using IMECA, FMECA, Markov's model. IMECA is applied to investigate any intrusions into BAS by analyze of vulnerabilities and effects of attacks using criticality matrix. FMECA is applied to assess criticality of BAS hardware failures. Markov's model is used to calculate BAS availability considering the possibility of recovery and different kinds of the faults.

***Keywords**: FMECA, IMECA, Building Automation System, criticality matrix, RBD, Markov's model*

1. Introduction

1.1. Motivation

The primary goal of system analysis is to give enough details of system work and the ability of this system to perform a task during a period of time without threats (errors, faults, failures). Analysis of the system is performed to determine its dependability and security. In this paper the investigation of the system for building automation also takes into account the analysis of availability and security of the system. In order to perform these types of analyses we can apply such techniques as the FMEA (Failure Mode and Effects Analysis and its modifications), FTA (Fault Tree Analysis), HAZOP (Hazard and Operability Analysis), RBD (Reliability Block Diagram), MM (Markov's models). They are designed for the analysis of the system, dependability and evaluation of system attributes as well as quantitative or qualitative assessment.

In this paper we analyze a scenario of cyber attacks on a building automation system as a case study and how they can affect the system performance using the IMECA - Intervention Mode Effects and Criticality Analysis, the FMEA – Failure Mode Effects and Analysis. The analysis of attacks effects and availability of the system measures the ability of system to end task under different scenarios of attacks. Building automation system (BAS) is one of the most popular systems in different areas of human life. It requires security, safety and probability. Analysis of BAS vulnerability using the Failure Mode Effects and Analysis (FMEA) is a common reliability analysis method; it is applied for determining the weakest parts of BAS design in hardware and software and connections between components in one fault.

Taking into account the majority of possible interventions into the system that will affect its security and availability, it is possible to build a criticality matrix of the system to show critical points during a period of time, and understand the critical state of the system and points where the system can be under the intervention or failure in component leading to shut down.

1.2. Work related analysis

The purpose of [1] is to show steps of facility managers through the Failure Mode, Effects and Criticality Analysis (FMECA) process, directing them how to apply this type of analysis to a command, control, communications, and it shows the practical examples that will illustrate how this can be accomplished by quantitative (with data) or qualitative means (without data), the FMECA process can be applied to any electrical or mechanical system, it helps to use and develop information in building automation design for future work.

SCADA is a one of the basic BASs. The analysis gives an idea of the degree of system availability, in [2] the analysis of the FMECA usage helps to develop the concept of availability and safety of the system in general.

The [3] describes modern technologies of Computer Network Reliability. Software tool is developed to estimate the CCN critical failure probability (construction of a criticality matrix) according to the results of the FME(C)A-technique which can be used to develop the building automation system design, and describe a technique and basic principles of dependable development and deployment of computer networks that are based on results of FMECA analysis and procedures of optimization choice of means for fault-tolerance ensuring.

In [4] the application of functional modeling to the automated production of FMEAs for mechanical systems is considered; it is also considered how a functional model can be generated algorithmically from the geometric and assembly data already presented for a device in a CAD/CAM system. There is a functional model used for representing the mechanical system, and

propose reasoning techniques that can be applied to the model in order to produce an FMEA.

Practical application, showing the benefits of the system, was analyzed using methods of analysis in [5]. There is an example of the application of the FMECA for the analysis of system components and brief analysis on the physical components of the system. The effect of this failure on system work is shown.

1.3. Goal

Building automation system design consists of two major elements (hardware and software) as any other system (surveillance, aviation and navigation systems, etc.). System analysis is generally aimed at showing the characteristics of the system (availability, security) through using two methods –the IMECA and FMECA. In this paper we take the case study of building automation system, showing availability of the system of (quality, quantity), and calculating security assessment according to attacks scenario. The process of analyzing BAS security and availability is divided into two parts.

1. Analysis of components depending on the type failure (hardware or design failure) by using the FMECA method, which shows the degree of failure in components, and the vulnerability of component, and effect on the system performance.

2. Interventions aiming at penetrating the system and disabling the system performance are analyzed by the IMECA, which allows studying the parts exposed to the intervention and calculating the impact and degree of the intervention on the system work. We can use this information to calculate the impact of intervention on information and the system security.

In section 2 the general review of the IMECA and FMECA is given and a block diagram of model used for system analysis and testing is presented. Section 3 presents the case of study, using building automation system as input system, data reading, and system analysis as well as monitoring the output of diagram. Section 4 gives the results and necessary steps to get the best results avoiding problem in future work.

2. General approach to analysis

Fig. 1 contains an illustration of system analysis steps and how to deal with the input, and handle the conditions set by the user to check the system. System analysis of the work depends on the analysis of the degree of security and the extent of the system; it provides the completion of the tasks entrusted to it by the terms of the user during a certain period of time. This analysis can be applied to different systems to measure the safety and other requirements. Analysis is divided into following steps.

1. System Information is input into the form that contains the basic information such as the number of system components, the number of levels. The nature of system work and information (control, protection, etc.) are given on the physical components during manufacturing (date of components and degree of failure), as well as information on the software used in the system (software components). Methods of analysis will be the FMECA and IMECA.

2. System requirements: the requirements set by the user are used to ensure system scalability for the full task under different conditions of failure and violation according to requirements set by the user.

3. Data analysis by classification (hardware, software, and interventions) in this step divides the information entering the form and distributes it by the division between (FMECA) for the analysis of hardware and software, and (IMECA) for the analysis of interventions. The reliability of system can be calculated using Reliability Block Diagram (RBD) method, in some cases we have complex system with a large number of components, in this case using Markov's model to analyze the system.

4. After dividing the input taking into account the number of levels in the system and the number of hardware components at every level of the system, the process of analysis by the data (hardware, software, and interventions) starts, and calculates availability (quantitative, quality) of data during period of time. In this paper our case study building automation system, the main requirement of system it (security and availability). According to the analysis of the building automation system, the communication system has higher level of intervention in building automation system design according to [6].

5. According to system analysis in step 4, the analysis is divided into three parts (hardware, software, and interventions), the FMECA method is used for analyzing the components of system according hardware fault or design fault. The IMECA methods specialize in the analysis of interventions in the system and calculate the impact of interference to the system. Results can be analyze and showed through use of critical matrix

6. The calculation of system availability helps to project an image about the possibility of meeting the requirements that have been set by the user. The system will proceed to the next stage, if it matched with the terms set by user; if the results do not match, the requirements set by the user, and then we must re-analyze using a lower requirement than those set at first.

Any failure in a system component can affect system security, i.e. hardware security for building a system. The RBD is used to define a failure component in the system and Markov's Modelanalysis helps to give picture for system recovery and possibility to restore all the information and it can be used to calculate hardware security for BAS. Analysis of the failure for each levels of BAS design shows system availability during a period of time. The FMEA can calculate availability of system A(t).

Analysis of interventions on system using IMECA gives the details about system state as shown in table 3, and what impact these interventions can have on system performance. The Markov's model gives the opportunity to calculate the probability to recover.

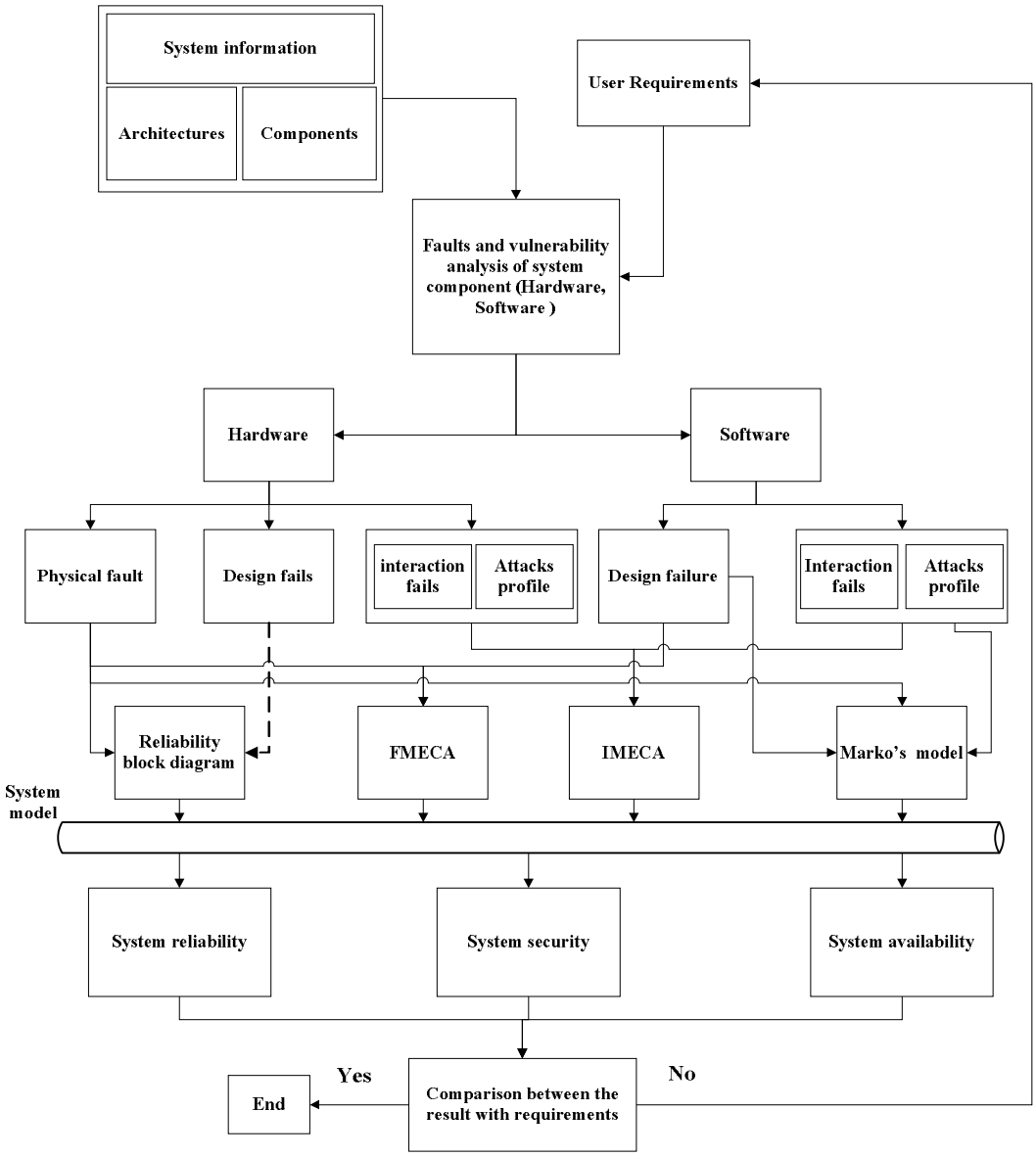

Fig. 1. Architecture of analysis steps for general system design

3. FMECA/IMECA-based assessment

When performing the FMEA we should remember that it must be scheduled and completed concurrently as an integral part of the design process. In a perfect case, the analysis is better to begin at the early stage of design in its conceptual phase during the development of the design criteria, mission requirements and performance parameters. In order to make the final design effective we should reflect and incorporate the analysis results and recommendations in it. Therefore, it is not reasonable to initiate the FMEA for estimation of existing risks using this systematic approach after the system is built.

In fig. 2, there is the analysis phase of the system work using mathematical modeling. Depending on the input information about the system, as shown in fig. 1:

V(t) - vulnerability analysis and fails types, P(t) - choosing analysis method (IMECA, FMECA, Markov's model , reliability block diagram), M(t) - comparing the results of the analysis with user requirement, Z(t) –the result of system analysis >= user requirement, W(t) –the result of system analysis < user requirement, send information about analysis result and advise user to change requirement to matching with system A(t) - system availability (quantitative and qualitative), R(t) - system reliability.

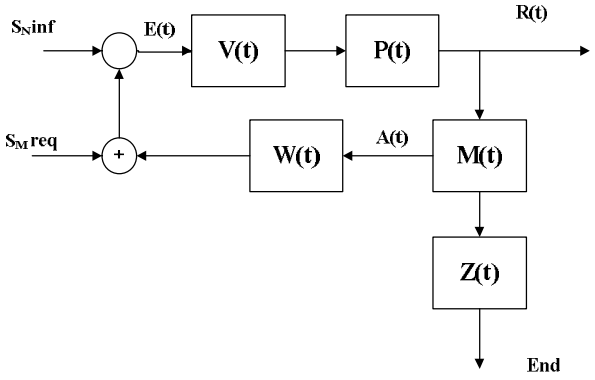

Fig. 2. Mathematical modeling of Systems analysis

The representation of the work of the system using mathematical ratios is shown below:

Sinf: system information,

Sreq: system requirements,

N: number of components in system design,

M: number of requirements.

Fig. 3 shows how FMEA process should be implemented within the process of facility development.

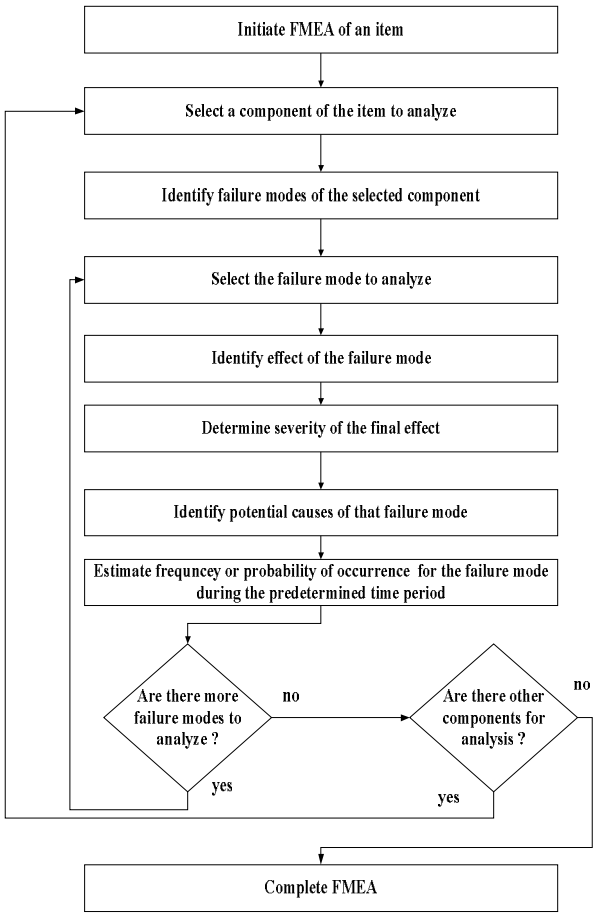

Fig. 3. Typical FMEA flow

We use the FMEA for maintainability, safety and logistics analyses; however, there is a risk duplication of effort within the same program. Thus, it is important to coordinate the analysis in order to prevent duplication. Being an iterative process, the FMEA must reflect the additional details with the design development. After the changes are implemented into the design, the FMEA must be performed on those redesigned sections. Such a performance ensures that the potential failure modes of the components of interest will be addressed. Thus, the FMEA turns out to be an important continuous improvement tool that makes program decisions take into account trade-offs affecting integrity of the design.

The difference between the IMECA and FMEA is in input and system analysis data. The IMECA requires more information about intervention in system software and a type of cyber attacks, which can affect the system work. The IMECA analyzes the system according to the given information and connection between components to investigate the impact of attacks on system, and give a picture of system criticality.

3.1. Structure and stages

Fig. 3 gives the description of the major approach to perform the FMEA. It includes the following steps depicted in the flow chart. We divide the system into components; then we identify failure modes for each component. The examination of the severity of the final effect on the system and its potential causes is performed for each failure mode and then the estimation of the failure modes probability is made. Fig. 3 presents the analysis of the cause-effect chain investigated using the FMEA. There is a failure cause for each failure mode that is why any failure effect is connected to a failure mode leading to a certain effect. A certain failure effect can cause an unintended scenario. The significance of the scenarios described by severity, in order to understand how likely an event can emerge we use frequency, which is associated with failure cause and effect.

It is necessary to include security in the analysis that is why we need a comparable cause-effect chain. The security-critical events are divided into similar steps. The given elements are offered parts of the security cause-effect chain. Threat Agents are considered to be some active elements trying to use vulnerabilities, e.g. insiders, hackers, computer criminals or even terrorists and industrial espionage.

Threat Mode is needed to classify ways of vulnerabilities exploitation. An attacker can exploit vulnerabilities in different ways with various different effects. Threat modes are in dependence with the capabilities of a system and a threat agent. Threat Effect is an aftermath of attack in operation, function and status and it is similar to the failure effect. Attack Probability is needed to evaluate the criticality of a security attack along with the severity of the attack. Attack probability is defined in different way in comparison to safety and security and the severity can be estimated by domain experts.

3.2. Design steps of IMECA, FMEA

All methods depending on sequential steps facilitate the analysis and describe the system as a whole; flow steps describe types of data needed to deign IMECA and FMEA.

1. Identification of all components and associated functions with their proceed evaluation. Such process can include all of the parts that the product is constituted of. Although, if there is only one part of interest, the parts that make up the applicable sub-assemblies are needed. The description of function(s) of each part within in the product is given.

2. Identification of failure mode i.e. the potential failure mode(s) for each part should be identified (table 1). These failure modes can include but are not limited to.

3. Identification of intervention modes, different effects of attacks on system performance needed to recognize a type of these attacks and their ability to shut down the system.

Table 1

Failure level

Complete failure	Intermittent failure
Partial failure	Failure over time
Incorrect operation	Premature operation
Incorrect operation	Premature operation
Failure to cease function at allotted time	Failure to function at allotted time

4. Identification of the failure modes effects giving the list of the consequences or effects on product, property and people for each failure mode identified. Such description is better to make from the customer point of view.

5. Defining the severity of the failure mode; the level of severity or criticality indicates how significant an effect on the user is. Severity can vary from insignificant to risk of fatality. It is usually given either a code or numeric rating (in dependence on the FMEA method).

6. Identification of the failure mode causes and intervention mode; we identify causes for each mode of failure. The causes are: design deficiencies resulting in performance failures; induced manufacturing errors; accounts of intervention damage and the effect on system.

7. Defining the probability of occurrence i.e. determining and assessing the probability that a certain cause or failure mode will occur. It is possible to determine the probability of occurrence from field data or history of previous products. When the necessary information is not available, the rating can be made on the basis of the experience and knowledge of the cross-functional experts.

8. Identification of controls, i.e. the controls that are currently in place that either prevent or detect the cause of the failure mode.

9. Defining the effectiveness of current controls, i.e. estimation of how well the cause or failure mode can be prevented or detected.

10. Calculation of the Risk Priority Number (RPN); being an optional step RPN can be used to facilitate prioritization of failure modes for action. We calculate RPN for each failure mode by multiplying the numerical ratings of the severity, probability of occurrence and the probability of detection (effectiveness of detection controls) i.e. RPN = S x O x D.

4. Markov's model-based assessment

Types of threats on the system work are divided into three levels (hardware, software, and interventions). In this paper we consider that the risk of interventions is only the process of successfully penetrating the programmatic area. We use Markov's model to demonstrate the system work during a limited period of the system life. Markov's model is based on the analysis of the current state of the system, regardless its previous state as shown in fig. 4. Any failure in one of the levels means the stop of work order (shut down).Marko's Model process is aimed to describe the system. Any change can be done on system during a period of time. In general Markov's model describes the system with two states: 1) down state which measures failures of the system and change it to another one (in this case we can calculate the mean time to failure (MTTF) of system which can be applied to find availability of system; 2) up state when system recovers and gets back to original state or sometimes to another state depending on the system type (here we can calculate the mean time to repair (MTTR).

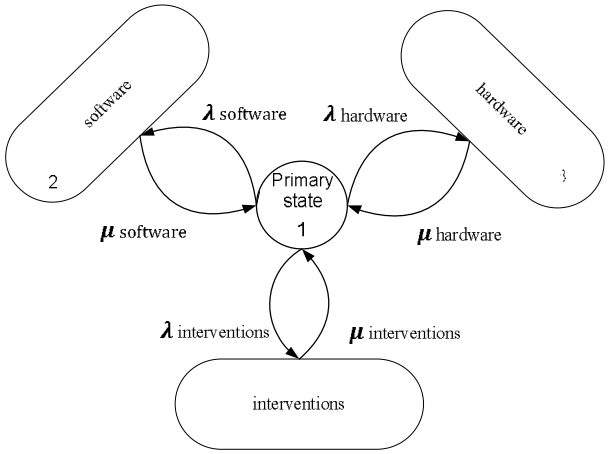

Fig. 4. System arability
based on Markov's model presented

5. Case study: building automation system architecture

As shown in Fig. 5, BAS designs vary depending on the area of application (military, medical, security, etc.) but they share the same principles of public design. The BAS is divided into three levels (management level, communication level and automation level). The analysis of levels helps to understand the process of work under any system failure or attack according to the scenario applied to the system to show its ability to test this scenario. Application of the FMECA system analysis mode is needed to see the failure of components of the level and its impact on the work of the system and its impact on other components of the same level. This method is concerned with the failure and deals with hardware and design.

The application of the IMECA lies in the analysis of interventions into the work of the system and shows the possible impact on the system and work of other components. Interventions are generally divided into two types: effective and not effective interventions. Failure levels are divided into four levels as show in table 1. The table 2 represents the application of the FMEA method for the analysis of the three levels with an explanation of the impact of the failure on the work of other levels, and its impact on the system work with determining the failure rate. In the Table 3 the application of the IMECA method is shown for the communication level because it is more vulnerable to interference levels, and the impact of failure at this level on the work of the rest of the levels, indicating the intervention and its impact on the type of system work.

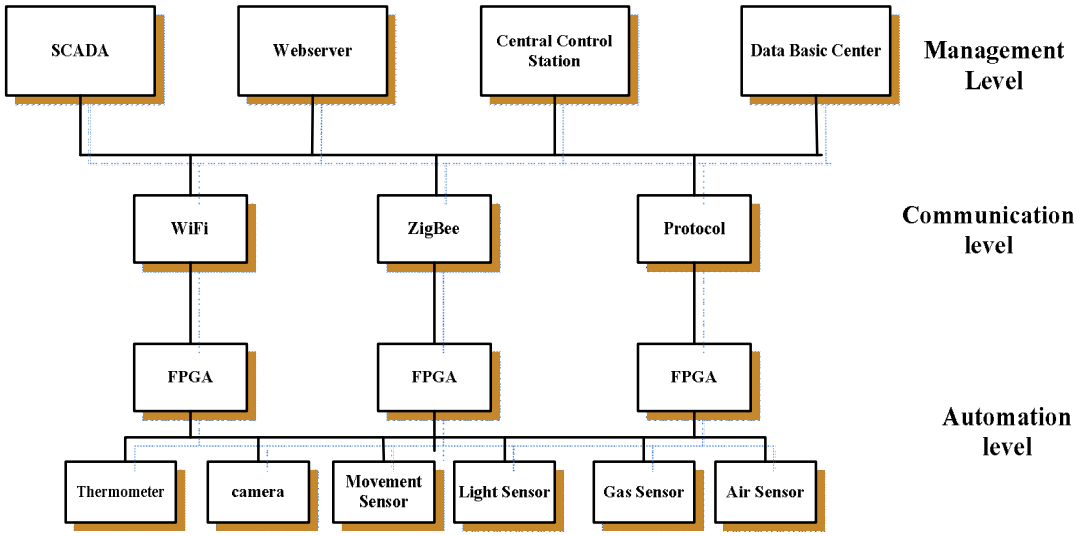

Fig. 5. Principal architecture of a building automation system [6]

Table 2

FMEA of Building automation system

No.	Component	Failure mode	Failure case	Failure effect	Failure level
1	Management level	Software	Human error or design fault	This level is presented as control unite of the system, failure will lead to the system shutdown	II
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	III
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	I

Table 3

IMECA of Building automation system [2]

Intrusion/Attack mode	Attack nature	Attack cause	Influence on operability	Intervention evidence	Intervention effect		
					Security	Availability	User
Communication level	Passive	Access to all information and monitoring of traffic inside system	Interruption	Non-evident	Data will be shown to attacker	The system is available but with risk for data	Lack of security of sensitive data
	Active	Breaking connection between levels, making the system lose control over a building	Termination	Evident	-	-	Long recovery time and loss of material

Conclusion

In the given article the FMEA method is applied to analyze two levels with a high failure rate using statistical analysis of defective components within the communication system. To analyze attacks and interventions the IMECA method is applied. Determining failures of communication function at BAS weak points improves communication security and can help to reduce risk to BAS. Although it should be noted that raising the security means rising of cost and system complexity.

The represented diagram can be applied to different kinds of system which has different requirements, as well as to a system to be tested. The scheme is used for static time and it analyzes different types of system, e.g. BAS system.

The article also describes the IMECA method giving the results in a certain period of time. There presented the Table which shows the intervention impact on the system and the possible damage it can make.The next step in future work will be focusing on components in levels (Wi-Fi, FPGA , database). The analysis will be conducted for these three components and will show the availability of these components under different attack scenarios. It will advise how to avoid threats in future building automation design.

References

1. Anonymous. Failure modes, effects and criticality analyses (FMECA) for command, control, communications, computer, intelligence, surveillance, and reconnaissance (c4isr) facilities. Headquarters Department of the Army, Washington, DC.2006; 9:29 (5-698-4): 4. Available: https://www.wbdg.org/ccb/ARMYCOE/COETM/tm_5_698_4.pdf.

2. Babeshko Eu, Kharchenko V, GorbenkoA. 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: 315-309. Available: http://www.scirp.org/journal/PaperDownload.aspx?paperID=8252.

3. Elyasi-KomariI, Gorbenko A, Kharchenko V, Mamalis A. Analysis of Computer Network Reliability and Criticality: Technique and Features", Int. J. Communications, Network and System Sciences. 2011: 11 (4): 726-720. Available: http:// www.scirp.org/journal/PaperDownload.aspx? paperID=8252.

4. Hughes N, Chou E, Price Ch, Lee M. Automating Mechanical FMEA Using Functional Models.Proceedings of the Twelfth International FLAIRS Conference.1999: 5. Available:https://www.aaai.org/Papers/FLAIRS/1999/FLAIRS99-071.pdf.

5. Anonymous. Reliability Analysis of Metro Door System Based on FMECA. Journal of Intelligent Learning Systems and Applications.2013; 11(5): 220-216. Available: http://www.scirp.org/journal/PaperDownload.aspx?paperID=39442.

6. Al-sudani Mustafa Qahtan Abdulmunem, Kharchenko V.S., Uzun D. Vulnerability analysis of wireless networks.Radioelectronni I kompyuternisystemy.2015; 2 (72):76-69. Available: http://www.khai.edu/csp/nauchportal/Arhiv/REKS/2015/REKS215/AlSudani.pdf.

Надійшла до редколегії 15.12.2015

Рецензент*:* д-р техн. наук, проф. А.В. Горбенко, Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», Харків.

МЕТОД IMECA ДЛЯ ОЦЕНИВАНИЯ КИБЕРБЕЗОПАСНОСТИ: ПРИМЕР ДЛЯ ИНФОРМАЦИОННО-УПРАВЛЯЮЩЕЙ СИСТЕМЫ УМНОГО ДОМА

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

Анализируется коммуникационная система как часть ИУС умного дома (УД) с высокой интенсивностью отказов. Исследуются вопросы оценивания кибербезопасности и готовности ИУС УД на этапах жизненного цикла с использованием методов IMECA, FMECA, а также марковских моделей. IMECA применяется, чтобы проанализировать влияние любых вторжений в систему и ее различные компоненты подобно тому, как FMECA показывает влияние отказов аппаратных средств. Марковские модели используются для получения аналитических оценок готовности ИУС УД с учетом возможности восстановления и всех видов отказов.

Ключевые слова: *FMECA, IMECA, ИУС умного дома, матрица критичности, марковские модели.*

МЕТОД IMECA ДЛЯ ОЦІНЮВАННЯ КІБЕРБЕЗПЕКИ: ПРИКЛАД ДЛЯ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧОЇ СИСТЕМИ РОЗУМНОГО БУДИНКУ

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

Аналізується комунікаційна система як частина ІУС розумного будинку (РБ) з високою інтенсивністю відмов. Досліджуються питання оцінювання кібербезпеки й готовності ІУС РБ на етапах життєвого циклу з використанням методів IMECA, FMECA, а також марківських моделей. IMECA застосовується щоб проаналізувати вплив будь-яких вторгнень у систему, її різні компоненти подібно тому, як FMECA показує вплив відмов апаратних засобів. Марківські моделі використовуються для отримання аналітичних оцінок готовності ІУС РБ з урахуванням можливості відновлення і різних видів відмов.

Ключові слова: *FMECA, IMECA, ІУС розумного будинку, матриця критичності, марковські моделі.*