

Assessment of control and monitoring system design security using the attack security tree analysis method

Mustafa Qahtan Alsudani^{1,2}, Israa Fayez Yousif³, Ahmed Nooruldeen Alsafi¹,
Hassan Falah Fakhruddin^{1,4,5}

¹Department of Computer Techniques Engineering, Faculty of Information Technology, Imam Ja'afar Al-Sadiq University, Baghdad, Iraq

²College of Medicine, Jabir Ibn Hayyan Medical University, Najaf, Iraq

³Department of Materials Engineering, Faculty of Engineering, University of Kufa, Kufa, Najaf, Iraq

⁴Department of Electrical Engineering, College of Engineering, University of Kufa, Kufa, Iraq

⁵Department of Computer Technical Engineering, College of Technical Engineering, The Islamic University, Najaf, Iraq

Article Info

Article history:

Received Oct 30, 2022

Revised Apr 4, 2023

Accepted Apr 16, 2023

Keywords:

Advanced persistent threat
Attack security tree analysis
Attack tree analysis
Controlling system and observation
Reliability block diagram

ABSTRACT

Because of the efficiency of the system and the fact that it successfully completed the tasks that were given to it under specific conditions, we are compelled to look for a way to measure these requirements according to the conditions and guidelines that were established by the people who make use of the system. Conduct an investigation into the many techniques that are available for use in analysis in light of the following conditions: i) sufficient time to detect the mistake, ii) time to maintenance, iii) the total number of constituents involved in the analytical process, and iv) an explanation of the level of complexity provided to the user. In this article, we will provide a concise overview of a number of different approaches, along with our recommendations for the most effective ones based on the issues raised earlier.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Mustafa Qahtan Alsudani
Department of Computer Techniques Engineering, Faculty of Information Technology
Imam Ja'afar Al-Sadiq University
Al-Wazireya Near the Ministry of Labour, and Social Affairs, Baghdad, Iraq
Email: alsudani.m.q@gmail.com

1. INTRODUCTION

Due to the interplay between technology and daily life, it is crucial to ensure the reliability and security of the methods employed. Course participants create a requirements map for the analytical procedure that takes these factors into account. We surveyed potential attacks on the system using three modern methods: the reliability block diagram (RBD) initial way, this system analysis technique, and attacks that affect the functioning of the system and refer to interstitial sections where their causes are discussed [1]. Attack tree analysis is the alternate strategy. The attack tree analysis (ATA) method assesses potential attacks on a system by creating a tree for attacks on all system components. When constructing the tree, the study considers the system's dependability and security [2]. The third approach Although the previous approach of forming the tree relies on physical components and software components, we now rely on the software components and attacks that may infect them, but the two methods are interconnected.

International standards [3] and the conditions that must be met to attain safety and availability can be used to evaluate the level of risk associated with a controlling system and observations. Ali and Gruska [4], the method is used to detect a failure or weak areas that enhance the likelihood of cyberattacks on the system, in addition to detecting a threat that will be used to carry out security vulnerability analysis and record the state

of the system while under attack. Information security risk assessment using hypothetical situations is demonstrated in [5]. This tactic was motivated by attacks of the advanced persistent threat (APT) variety. Chief security officer (CSO) security management at the management level can be aided by using risk scenarios to evaluate the security threat to an information system, and some sample attack scenarios are presented. Due to the findings of this study, security measures for network control systems have been significantly bolstered, and weaknesses in the system's design due to hardware and software defects have become the primary target of [6]. Examining the device, and highlighting potential weak spots in the system, is how [7], [8] demonstrate field-programmable gate arrays (FPGA's) security as a platform. It's possible that we'll see FPGA's advantages on other devices at the same time. Shulman and co-founder [9], we can see the most commonly attacked targets in the database, together with the number of attacks that have resulted from those assaults; this gives us the opportunity to look into every probable reason of system failure. Its primary function is to guarantee the security of both the controlling and observational systems. Al-Sudani *et al.* [10], IMECA/FMECA can be used to estimate the likelihood of a system failing. Also, it shows that the system can fix itself after malfunctions [11]. The key component of a controlling system and observation is the wireless units. It might be helpful to evaluate the unit in light of its vulnerable status during an attack [12].

2. PROPOSED METHOD

According to the system design and the division of parts that make up three levels, the first level processing unit and often crosses the CPU according to. The second part of the system design is telecommunication level and only sending and receiving information wireless according to [11] the use of wireless expensive and less complex than using wire, but security and privacy problems are discussed in this work in detail. Following secession analysis system levels according different scenario from attacks and vulnerability. In next section will describe the system according the levels and scenario of attack can be effect on system [13].

2.1. Analysis ending device

Which is responsible for feeding the system the information and data required to complete the tasks provided to the system parts that can cause hardware failure, which are regarded as failures. Which is responsible for feeding the system the information and data required to complete the tasks. The inability of the hardware to function at the third level RBD as designed does not have an impact on the functioning of the system; however, it is essential to think about the system in terms of its capacity to tolerate errors.

2.2. Analysis the vulnerability of wireless communication design

Communication it's the tools responsible of counted the system together, let's take a closer look at wireless networks. They are made up of four fundamental parts. Users, access points, and client devices (laptops and PDAs) all play a role in the transfer of data through radio frequencies. A breach of confidentiality, integrity, and availability may occur if the supplied components are attacked or have weaknesses. The following are examples of wireless network attacks: i) accidental association: this is an example of an intrusion into a company's wireless network without permission. Users may not be aware that they have connected to an access point on an adjacent network when they first switch on their computer. Information from one firm might be linked to information from another if a security breach occurs. Wired networks are the same as wireless networks when it comes to laptops. ii) Ad-hoc networks: networks connecting wireless computers that do not have access points are known as ad-hoc networks. These networks aren't often well-protected, although encryption techniques may be utilized to improve security. iii) Man-in-the-middle attacks (MITM): an attacker is created (access point). A second step is for him to have additional computers log in via this virtual access point (VAP). After that, the hacker uses a different wireless card to connect to a genuine access point, allowing traffic to pass through the transparent hacking machine and into the actual network. Because of this, the attacker is able to monitor the flow. iv) Denial of service (DoS): attacking an access point or a network with false DoS attacks are defined as requests, failure messages, premature connection messages, and/or other instructions [14]. These attacks may prevent genuine users from accessing the network, and they may even bring down the whole system. The extensible authentication protocol (EAP) is a common target of these attacks (EAP).

2.3. Vulnerability analysis of control level

We can call the head or the mind of the system which are responsible control the system by sending command analysis data and so on according to the system design, attacks on the control level have risen as data held at those levels has become more widely accessible. Information that is critical to the system and data from many levels are included at the control level of CSO design. The likelihood of data theft rises when several people have access to the stored information [15]. In the CSO system, the attacker is trying to get their hands on crucial information, which they may use to attack or monitor the system. This is why it is essential to manage

this sort of access. The following are examples of several sorts of risks that may compromise security at the control level: i) Privilege abuse: when a database user has greater rights than normal. Intentionally or inadvertently, these rights might be misused. ii) Vulnerabilities in operating systems like Windows, UNIX, Linux, and others, in addition to the products and services linked to databases, might provide an entry point for attackers. DoS attacks may result if operating system security updates are not updated (when they become available). Let's take a look at what a database rootkit is first. In order to get access to database data and disable intrusion prevention systems, an application or process is buried within the database that grants administrator-level rights (IPS). Only when the underlying operating system has been compromised can a rootkit be deployed [16]. Using frequent audit trails, this issue may be resolved such that the database rootkit is not noticed. If authentication measures are sufficiently wicked, attackers may resort to social engineering and brute force to get access to database credentials. The database may presume the attacker is using the identities of legal database users to commit his or her assault. Database servers that have insufficient audit trails may be at danger, particularly in businesses that need strict regulatory compliance. In the case of an accident, we should recreate the event at a later date. We use payment card industry (PCI), sarbanes oxley (SOX), and health insurance portability and accountability act (HIPAA), all of which need substantial recording, to do this. A database's sensitive or unusual transactions must be automatically logged in order to address any issues that may arise. The final line of defense for a database is an audit trail. They are capable of detecting an incursion, which aids in tracing the breach to a specific time and user [17].

2.4. Design of a control and observation system under assault by cyber-attacks

The purpose of a cyber-attack is to steal, change, or destroy a specific target in order to halt the operation of a target system. Individuals or whole businesses' computers, networks, and personal computing devices may be compromised to get access to sensitive data. Anonymity makes it difficult to track down the source of a danger, making it difficult to identify. An assault like this might be classified as cyber-warfare or terrorism. Installing spyware on a computer, trying to bring down a whole nation's infrastructure, and so on are all examples of cyber-attacks. It seems like every day, cyber-attacks become more sophisticated and lethal [18].

There are two types of cyber assaults: hardware attacks, which are designed to disrupt the functioning of physical components, and software attacks, which can read and modify all of the information included in the system design. Attackers may target any component of the system design in [10], according to system design. In hardware assaults, a virus or worm may be present in the chip and active throughout operation due to a manufacturer's mistake or flaw. Weaknesses in the system's design may be identified and exploited, for example, when wireless devices broadcast and receive data over a radio wave, software assaults might occur. In any of these cyber-attack situations, the hardware component may malfunction, and the software component may have an issue, resulting in the system failing. If we want to know how secure a building automation system (BAS) is, we need to think like an attacker attempting to get into the system, as stated in [10].

Cyberattacks on building automation systems may be broken down into three categories: i) the hacker gains access to the network by using a variety of tools to spy on it. If the attack's objective is to get entry inside, then that's a secondary goal. Attackers are looking for ways to spy on networks and read data across tiers in this initial stage of their assault strategy. System downtime is increased due to assaults like these that are difficult to detect during normal operations. As a result, recovery time is prolonged and resolution times increase. It is necessary to improve network security in order to prevent this issue and assaults of this kind. ii) If the attacker's purpose is to halt the system's performance, this is another situation. This may be done by either allowing the worm to operate for an extended period of time or terminating the system's performance right away. In terms of how long it takes to recover from this assault, it depends on the level of the game it occurred on, i.e. a) If the attacker intends to halt a component of the automation system at the level where it was attacked. We may be able to fix the problem by altering or upgrading the system within the time it takes for the system to recover. The system may be able to function again, but it won't be able to do so at its full capacity. b) In this instance, the recovery time would be more complicated since the management level controls all system tasks and the system's performance may be disrupted. Cyberattacks on the management level have made it difficult to recover and costly to implement new systems. iii) Error of design, it is possible to take advantage of errors in the design in favor of the cyber attack, which affects the performance of the system in general, with the possibility of the system not performing the tasks assigned to it as a result of this attack [19].

2.5. System performance according to RBD, ATA and AcTA methods

As a rule, the purpose of an attack is to cause the system as a whole to fail to work as designed. When we talk about failure, we're talking about the likelihood of real failures in operational systems, as well as the discovery and characterization of the processes that could cause them. Developers and consumers need to know the answers "How may the system fail?" and "What are the consequences?" What are the repercussions if we fail? Likewise, "How many system failures can we expect?" We'll go through two of the more successful

approaches in the following section. That were designed to provide a response to these concerns, and then will compare to the results with the attack security tree analysis (AcTA) method, which it helps us to understand the system performance. For our work we take case study the smart building, according to [20], it become part from system design of IoT, and it need to be insuring and security [21].

2.6. Reliability block diagram analysis of controlling and observation system

Analysis of systems may be done using the reliability block diagram. Graphics and formula are provided to aid in determining how reliable the system really is. Components of the system are represented by the blocks, which are collections of components that are not further subdivided. All of a system's components must be linked in series for it to fail if any one of them goes down. It is impossible for a system to function properly if its components are all linked in parallel.

In Figure 1 RBD deals with a system availability of subsystem design for case study (smart building) to understand all components work and the effects on the system we need to take more details to take a big picture for the system. In Figure 2 we focus on controlling and observation system as the first part of system design, according to (1) can understand the part relation and the effects of components on system availability, but if we try to go deep in details, as can see in (3), details and information will be a lot to explain and detect where the error and how it can fix it. This system with simple components, and if we deal with a complex system the operation will take a long time and many details. Our vision for this method to use for simple system (home) without complexity in design [22].

$$RBD = COS * CU * EU \tag{1}$$

$$RBD = [H.c * S.c] + Tell \tag{2}$$

$$RBD = [(H.c * S.c) + Tell] * CU * EU. \tag{3}$$

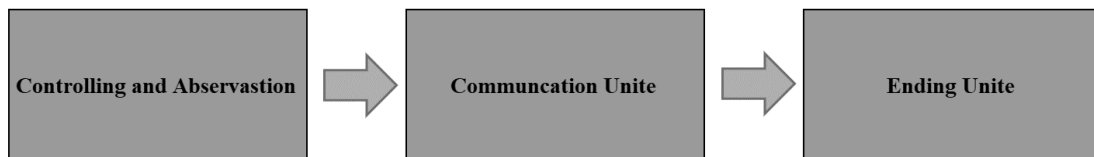


Figure 1. Architecture system design of smart building

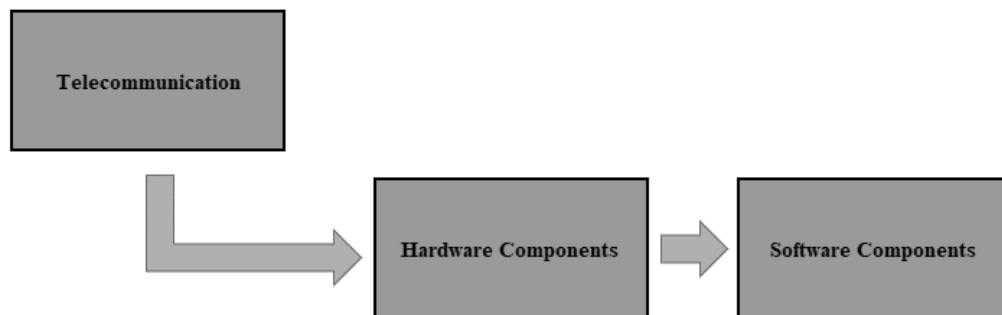


Figure 2. Architecture design of controlling and observation part from smart building

2.7. Attack tree analysis of controlling and observation system

Attack trees are a good example of this. It is a method for analyzing a system in an undesirable condition. After that, the system is examined in relation to its surroundings and functioning in order to uncover any potential points of failure. Both the OR-gate and the AND-gate will be examined in this section. The output event is shown by applying the OR-gate. Only if one or more of the input events occur will this output occur. All input assaults are required for an AND-gate attack to be triggered. It's required for us to identify the immediate, necessary, and sufficient causes of any event in the system in order to do a system analysis. These aren't the primary reasons of the event, but they are the proximate ones that led to it. Sub-goals are what we've come to refer to these days. Our investigation into what caused them may now go forward. In other words, we

work our way down the tree until we reach the node at the end of the attack tree's resolution limit, which is the leaf node (an atomic assault) [23]. According to Figure 3 the parameters of ATA depend on the inputs value of components, the probability of parameter depending on two issues (reliability and security) what it can't find in RBD, from this point we need to divided components to calculate the reliability and security in the same time.

$$pf(t)_2 = (COS * CU) \tag{4}$$

$$pf(t)_1 = 1 - (1 - pf(t)_2)(1 - pf(t)_4) \tag{5}$$

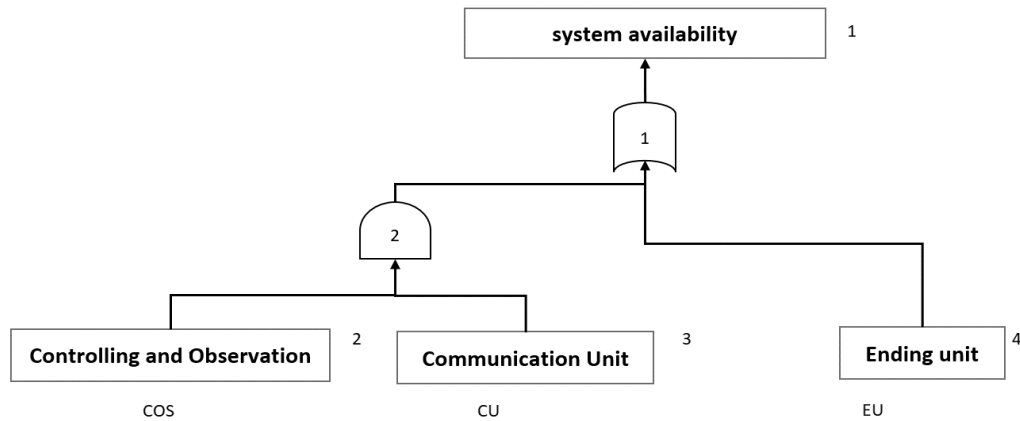


Figure 3. ATA analysis of smart building case study

Taking controlling and observation system as part of our case study (smart building) and apply ATA to analyze the availability of COS as shown in Figure 4 and analysis the result of the method with a number of components in the system. We can see the issues of reliability and security for components. The following equation depicts the likelihood of system failure, the relationship between components, and the ultimate goal in terms ATA analyzing, PF(t)=probability of failure, t=interval from (0,t) of system life.

$$pf(t)_4 = 1 - (1 - pf(t)_{10})(1 - pf(t)_9) \tag{6}$$

$$pf(t)_3 = 1 - (1 - pf(t)_8)(1 - pf(t)_7) \tag{7}$$

$$pf(t)_2 = 1 - (1 - pf(t)_3)(1 - pf(t)_2) \tag{8}$$

$$pf(t)_{gate 2} = 1 - (1 - pf(t)_3)(1 - pf(t)_2) \tag{9}$$

$$pf(t)_1 = pf(t)_4 * pf(t)_{gate 2} \tag{10}$$

For the ATA analysis's top event (PF(t)), the overall probability of failure (PF(t)) changes based on the probability of failure for each component. Naoual *et al.* [24] system availability depending if system will pass the failure period and the result will be the same before failure, in the Table 1 the system availability using ATA, and measuring the degree of possibility system will be failure. All value of parameters applied (6)-(10) to get the final result [25].

no	The issues	Components	Number of gates	Probability	System probability to fault
1	Security	Cybersecurity	5	0.009	
2	Security	Software vulnerability	3	0.0123	
3	Reliability	Hardware trojan (design fault)	5	0.0321	0.001365671
4	Reliability	Manufacturing fault/back attack	4	0.0391	
5	Reliability	Physical failure during operation	4	0.01	
6	Reliability	Manufacturing hardware/trojan/back attack	16	0.0312	

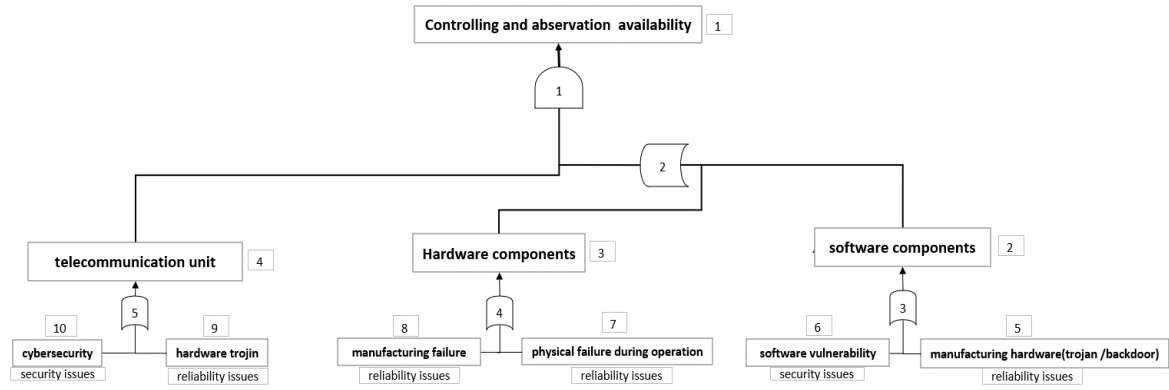


Figure 4. ATA analysis of controlling and observation part of case study (smart building)

3. RESULTS AND DESCATION

In general, we have calculated the reliability of the system (safety and availability) by considering reliability issues, which depend on a range of factors:

- a) The total time to fiend error in system.
- b) Diagnostic speed to find fault and direct the result.
- c) Number of components included in analysis, if number be less better to track fault and find the reason.
- d) Level of complexity explained to the user.

AcTA procedures focus the total solution and tree building on relying on security issue and neglecting or leaving the data sheet unlike the ATA that uses all data (security and reliability) as stated in [26], but in the use of RBD cannot identify elements that are under the influence of security, but the calculation is generally for the work of the system within a specified period of time. ATA to develop model that determines a reasonable chance of failure throughout the course of time RBD solves the possible failure of the system's work. With the same architecture of design of ATA, the AcTA deal with all security issues and isolate other issues. The new technology in the world and competition between companies to produce components, make the produce almost meet the market requirements without issues of failure (hardware and software). But the question what about security? As seen in Figure 5 the methods deal with security and isolate other issues.

$$pf(t)_1 = pf(t)_2 * pf(t)_3 \tag{11}$$

For the same values of the input, we can find the probability of system failure which affects the availability will approximate around (0.00125511), and if we compare the value with ATA reading will see there are little differences between reading. From this point, our analysis to comparison between these three methods and as shown in Figure 6. we can collect and analyze the information for methods depending on time and number of components. All these results and information are collected depending on the case studded (smart building) [27].

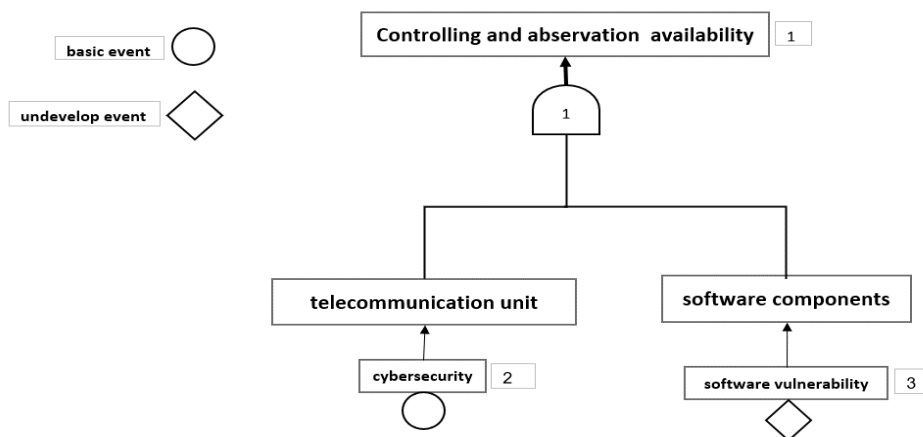


Figure 5. AcTA analysis of controlling and observation part of case study (smart building)

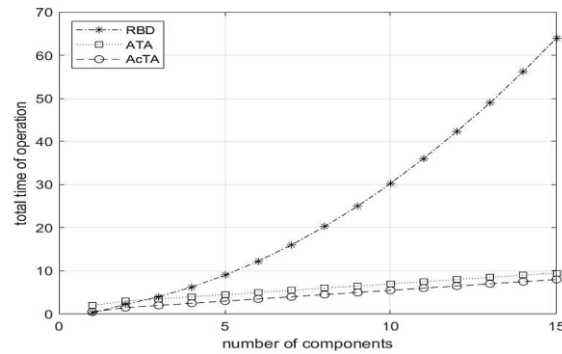


Figure 6. Results of three methods analysis

4. CONCLUSION

According to our analysis of the system design, we evaluated the system's chance of failure based on real-world data, and we identified weaknesses in the system's design. This analysis was done using a number of methods. These methods help to understand the point that needs to be secure and focused during design, AcTA give the minimum level of analysis with only the important component. The next step is to apply AcTA method with a complex system and union the components as one system to easily input data and calculate the result of system availability, taking into account the possibility a system recovery through a short time without effect on system work.

ACKNOWLEDGMENT

The authors are grateful for the financial and technical support from Imam Jaffar Al-Sadiq University, Al-Mustaqbal University College, and The Islamic University, Najaf.




REFERENCE

- [1] T. Alam, "Internet of things: A secure cloud-based manet mobility model," *International Journal of Network Security*, vol. 22, no. 3, 2020, doi: 10.6633/IJNS.202005_22(3).17.
- [2] S. Du and H. Zhu, "Security assessment via attack tree model," *Security Assessment in Vehicular Networks*, pp. 9-16, 2013, doi: 10.1007/978-1-4614-9357-0_2.
- [3] A. E. M. AL-Dahasi and B. N. A. Saqib, "Attack tree model for potential attacks against the scada system," in *2019 27th Telecommunications Forum (TELFOR)*, 2019, pp. 1-4, doi: 10.1109/TELFOR48224.2019.8971181.
- [4] A. T. Ali and D. Gruska, "Dynamic attack trees," in *OVERLAY*, pp. 25-29, 2021.
- [5] B. Bhargava, "International journal of security and its applications foreword," *International Journal of Security and its Applications*, vol. 12, no. 5, pp. V-VI, 2018.
- [6] M. Q. Alsudani, H. F. Fakhruideen, H. A.-J. Al-Asady, and F. I. Jabbar, "Storage and encryption file authentication for cloud-based data retrieval," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 2, pp. 1110-1116, 2022, doi: 10.11591/eei.v11i2.3344.
- [7] V. A. Torres *et al.*, "Combined weightless neural network FPGA architecture for deforestation surveillance and visual navigation of UAVs," *Engineering Applications of Artificial Intelligence*, vol. 87, p. 103227, 2020, doi: 10.1016/j.engappai.2019.08.021.
- [8] M. Q. A. Al-Sudani and K. Vyacheslav, "Cybersecurity of FPGA-based automation systems for smart building," no. 1, pp. 39-46, 2015.
- [9] A. Shulman and C. Co-founder, "Top ten database security threats," *How to Mitigate the Most Significant Database Vulnerabilities*, 2006.
- [10] M. Q. A. Al-Sudani, W. A.-K. Ahmed, and V. Kharchenko, "The method of IMECA-based security assessment: case study for building automation system," *Системи обробки інформації*, no. 1, pp. 138-144, 2016.
- [11] M. Q. A. Al-Sudani, V. Kharchenko, and D. Uzun, "Vulnerability analysis of wireless networks: case for smart building automation system," *Радіоелектронні і комп'ютерні системи*, no. 2, pp. 69-76, 2015.
- [12] A. T. Ali, "Simplified timed attack trees," in *International Conference on Research Challenges in Information Science*, 2021, pp. 653-660, doi: 10.1007/978-3-030-75018-3_49.
- [13] A. Altaf, S. Faily, H. Dogan, E. Thron, and A. Mylonas, "Integrated design framework for facilitating systems-theoretic process analysis," in *European Symposium on Research in Computer Security*, 2021, pp. 58-73, doi: 10.1007/978-3-030-95484-0_4.
- [14] R. Maciel, J. Araujo, J. Dantas, C. Melo, E. Guedes, and P. Maciel, "Impact of a DDoS attack on computer systems: An approach based on an attack tree model," in *2018 Annual IEEE International Systems Conference*, 2018, pp. 1-8, doi: 10.1109/SYSCON.2018.8369611.
- [15] V. de Vasconcelos, W. A. Soares, A. C. L. da Costa, and A. L. Raso, "Use of reliability block diagram and fault tree techniques in reliability analysis of emergency diesel generators of nuclear power plants," *International Journal of Mathematical, Engineering and Management Sciences*, vol. 4, no. 4, p. 814, 2019, doi: 10.33889/IJMEMS.2019.4.4-064.
- [16] B. Gunes, G. Kayisoglu, and P. Bolat, "Cyber security risk assessment for seaports: A case study of a container port," *Computers and Security*, vol. 103, p. 102196, 2021, doi: 10.1016/j.cose.2021.102196.
- [17] K. Dussarlapudi, K. N. Raju, K. K. Kumar, K. Sudhakar, and C. S. Tiruvuri, "Design and prototyping of an accelerometer based parallel manipulator for endoscope position control," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 27, no. 3, pp. 1320-1329, 2022.
- [18] N. Hossain, T. Das, T. Islam, and M. A. Hossain, "Cyber security risk assessment method for SCADA system," *Information Security Journal: A Global Perspective*, pp. 1-12, 2021, doi: 10.1080/19393555.2021.1934196.




- [19] H. Kanamaru, "The extended risk assessment form for IT/OT convergence in IACS security," in *2021 60th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*, 2021, pp. 1365-1370.
- [20] Y. Aoudni *et al.*, "Cloud security based attack detection using transductive learning integrated with hidden markov model," *Pattern Recognition Letters*, vol. 157, pp. 16-26, 2022, doi: 10.1016/j.patrec.2022.02.012.
- [21] V. Kharchenko, Y. Ponochovniy, A.-S. M. Q. Abdulmunem, and I. Shulga, "AvTA based assessment of dependability considering recovery after failures and attacks on vulnerabilities," in *2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, 2019, vol. 2, pp. 1036-1040, doi: 10.1109/IDAACS.2019.8924251.
- [22] H. A.-J. Al-Asady, H. F. Fakhruideen, and M. Q. Alsudani, "Channel estimation of OFDM in c-band communication systems under different distribution conditions," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 23, no. 3, pp. 1778-1782, 2021, doi: 10.11591/ijeecs.v26.i2.pp808-818.
- [23] B. N. Alsunbuli, H. F. Fakhruideen, W. Ismail, and N. M. Mahyuddin, "Hybrid beamforming with relay and dual-base stations blockage mitigation in millimetre-wave 5G communication applied in (VIOT)," *Computers and Electrical Engineering*, vol. 100, p. 107953, 2022, doi: 10.1016/j.compeleceng.2022.107953.
- [24] T. Naoual, O. Djamel, G. Abderrezak, and R. Messaoud, "Advanced control with extended Kalman filter and disturbance observer," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 28, no. 1, pp. 124-136, 2022, doi: 10.11591/ijeecs.v28.i1.pp124-136.
- [25] R. Jalil, A. Sabbar, H. F. Fakhruideen, and F. I. Jabbar, "Design and implementation of PC to PC data transmission using wireless visible light communication system," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 26, no. 3, pp. 1423-1428, 2022, doi: 10.11591/ijeecs.v26.i3.pp1423-1428.
- [26] C. E. Budde, C. Kolb, and M. Stoelinga, "Attack trees vs. fault trees: two sides of the same coin from different currencies," in *International Conference on Quantitative Evaluation of Systems*, 2021, pp. 457-467, doi: 10.1007/978-3-030-85172-9_24.
- [27] H. F. Fakhruideen, T. S. A. Mansour, F. I. Jabbar, and A. Alkhayyat, "Multiple inputs all-optical logic gates based on nanoring insulator-metal-insulator plasmonic waveguides," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, pp. 6836-6846, 2022, doi: 10.11591/ijece.v12i6.pp6836-6846.

BIOGRAPHIES OF AUTHORS






Mustafa Qahtan Alsudani    received the B.Eng. degree in technical computer engineering from Al-Rafidain University College, Iraq, in 2010 and the M.S. and Ph.D. degrees in computer engineering techniques from National Aerospace University "KhAI," Kharkiv, Ukraine, in 2013 and 2018, respectively. Currently, he is an Associate Professor and Head of the department of computer engineering teachings, imam Jaafar Al-Sadiq University. His research interests include computer vision, system vulnerability, system security, cyber-attacks, wireless networks, and wireless communications. He can be contacted at email: alsudani.m.q@mail.com.






Israa Fayeze Yousif    received the B.Eng. degree in materials engineering from the University of Kufa-Engineering College, Iraq, in 2014 and the M.S. degree in materials engineering from University of Kufa-Engineering College in 2013 and 2018, respectively. She can be contacted at email: israa.fayez@sadiq.edu.iq.



Ahmed Nooruldeen Alsafi    received the B.Sc. degree in computer science from University of Kufa, Iraq, in 2011 and the M.S. in computer science from Kharkiv National University of Radio Electronics, Ukraine, in 2013. Currently, he is Ph.D. candidate in University of Qom. Currently, he is an assist. lecturer at the department of computer engineering, Imam Jaafar Al-Sadiq University. His research interests include deep learning, programming, machine learning. He can be contacted at email: ahmed.alsafi90@gmail.com.



Hassan Falah Fakhruideen    received the B.Eng. degree in communications engineering from Al-Furat Al-Awsat Technical University, Iraq, in 2010 and the M.S. and Ph.D. degrees in electronics and communications engineering from Baghdad University, Iraq, in 2013 and 2020, respectively. Currently, he is an Associate Professor at the Department of Electrical Engineering, University of Kufa. His research interests include photonics, optics, optical fiber communications, nano-photonic devices, plasmonics devices, optical communications, optical fiber networks, plasmonic sensors, all-optical signal processing, 5G communications, communications transmission lines, signal transmission planning, wireless networks, wireless communications, radio over fiber communications. He can be contacted at email: hassan.fakhruideen@gmail.com.