MJFAS
Malaysian Journal of Fundamental and Applied Sciences

RESEARCH ARTICLE

Models and Methods of Information and Control System Cyber–security for Smart Buildings

Hassan Falah Fakhruldeen[a,b*], Karrar A. Kadhim[a], Tahreer Abdulridha Shyaa[c], Heba Abdul-Jaleel Al-Asady[d]

[a]Computer Techniques Engineering Department, Faculty of Information Technology, Imam Ja'afar Al-Sadiq University, Baghdad, Iraq; [b]Department of Electrical Engineering, Faculty of Engineering, University of Kufa, Kufa, Najaf, Iraq; [c]Ministry of Higher Education and Scientific Research Supervision and Scientific Evaluation Apparatus; [d]Computer Technical Engineering Department, College of Technical Engineering, The Islamic University, Najaf, Iraq

Abstract Smart building management systems today employ the architectural multi-level creation of a system of unified components. Such a market is dynamic and always expanding, and sometimes the developers of such components stop maintaining their products or even collapse and vanish. It's not always possible to use professional-level components from proven developers when a building automation system (BAS) project budget is limited. The construction and analysis of models that consider the dependability and cyber security aspects of maintenance as well as ways of validating the selection of components, strategies, and service parameters are both necessary steps in finding compromises between the BAS architecture's value and quality. Use of information technology to determine maintenance parameters based on a model and model development approach.

Keywords*:* Building automation system, IoT, availability tree analysis, FPGA, VHDL.

Introduction

Cloud computing, the Internet of Things, and other forms of embedded intelligence are all contributing to the rise of new types of IT system design for smart buildings [1], such as apartments, office buildings, public buildings, and university campuses, for example [2]. A building automation system is a collection of subsystems that conduct information and control operations (BAS) [3]. It is difficult to evaluate the operational dependability and cyber security of software and infrastructure resources because of dynamic processes like information exchange between subsystems and BAS components, software modification to eliminate design flaws [4], and vulnerability patching used for attacks [5]. Development of a theoretical framework for assessing and ensuring dependability, as well as the availability of information systems and control systems, in the context of cyber security [6]. Various formal methods, like FMECA-analysis of the fault and attack tree and Markov models of availability, are used to evaluate the reliability of hardware and software (HW and SW) [7]. According to the characteristics of the BAS components and architecture, various service strategies concerning reliability and cyber security are not examined in detail [8-11]. As a result, the scientific challenge is to develop models and methods of information technology for the availability of Smart Building Information and Control System Cyber security, taking into account attacks on vulnerabilities and defects in software components, common and separate maintenance procedures by reliability, and security [12].

***For correspondence:**
hassan.falah@sadiq.edu.iq

Received: 13 Oct. 2022
Accepted: 11 April 2023

10.11113/mjfas.v19n3.2902

Method

By integrating mathematical models, engineering algorithms, and related software tools that form the applied information technology of evaluation and ensuring the availability of control systems [13], cyber-attacks on smart building control systems can be averted [14]. Building control systems for smart buildings can be simulated and analyzed using a computer program that considers both failures and attacks on the components of their architecture [15]. Set theory and reliability theory were utilized to build trees for the analysis of faults and attacks that take into account the impact of component inadequacies and weaknesses at various system levels, probability theory, Markov analysis, and mathematical statistics [16]. First, a method to select and define parameters for the maintenance of smart building systems has been developed that takes into account different maintenance procedures as well as the elimination of component defects and vulnerabilities [17], as well as restrictions on the reduction in the unsteady value of the availability factor that allows a certain amount of time for the system to be operational. And-or trees have been used to analyze faults and attacks in smart buildings, as well as parameters for recovery from system failure as well as attack blocking, to further improve the model's reliability and security. This helps determine the likelihood of system failure [18, 19].

The Architecture of the Building Automation System (BAS)

The approaches for developing, analyzing, and providing cyber security for smart buildings were examined [20]. There are three levels of architecture in the BAS of a smart building shown in Figure 1: automation, wireless communication, and database management [21]. The application of software at all three levels complicates the evaluation and prediction of system availability [22], particularly for corporate decisions. System failures due to physical and design defects of the BAS are also a problem (0.9999 ... 0.99999).

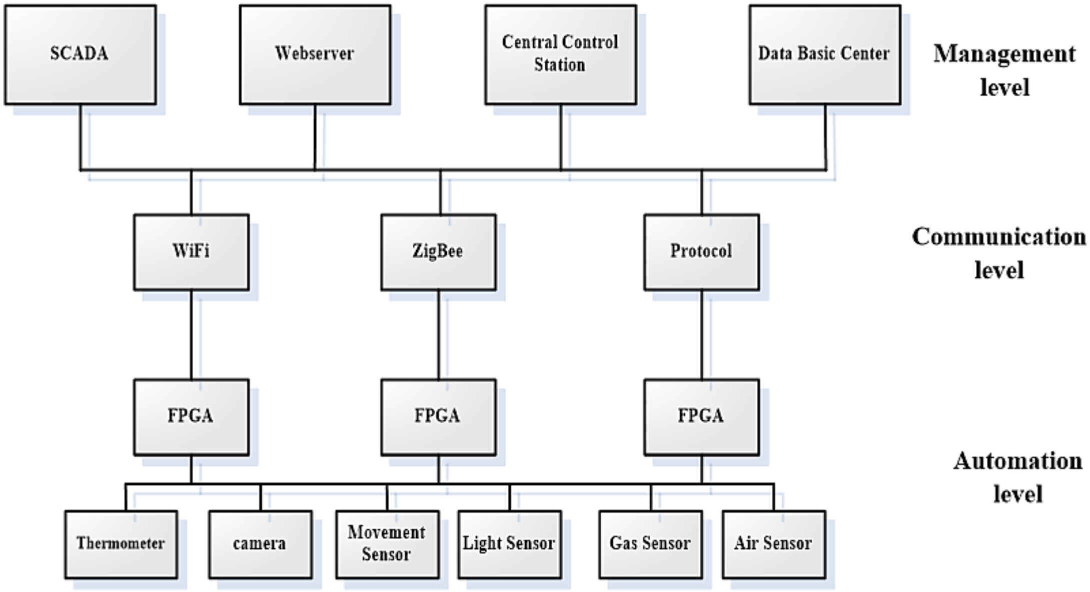

Figure1. Smart building information and control system architectural levels [23]

10.11113/mjfas.v19n3.2902

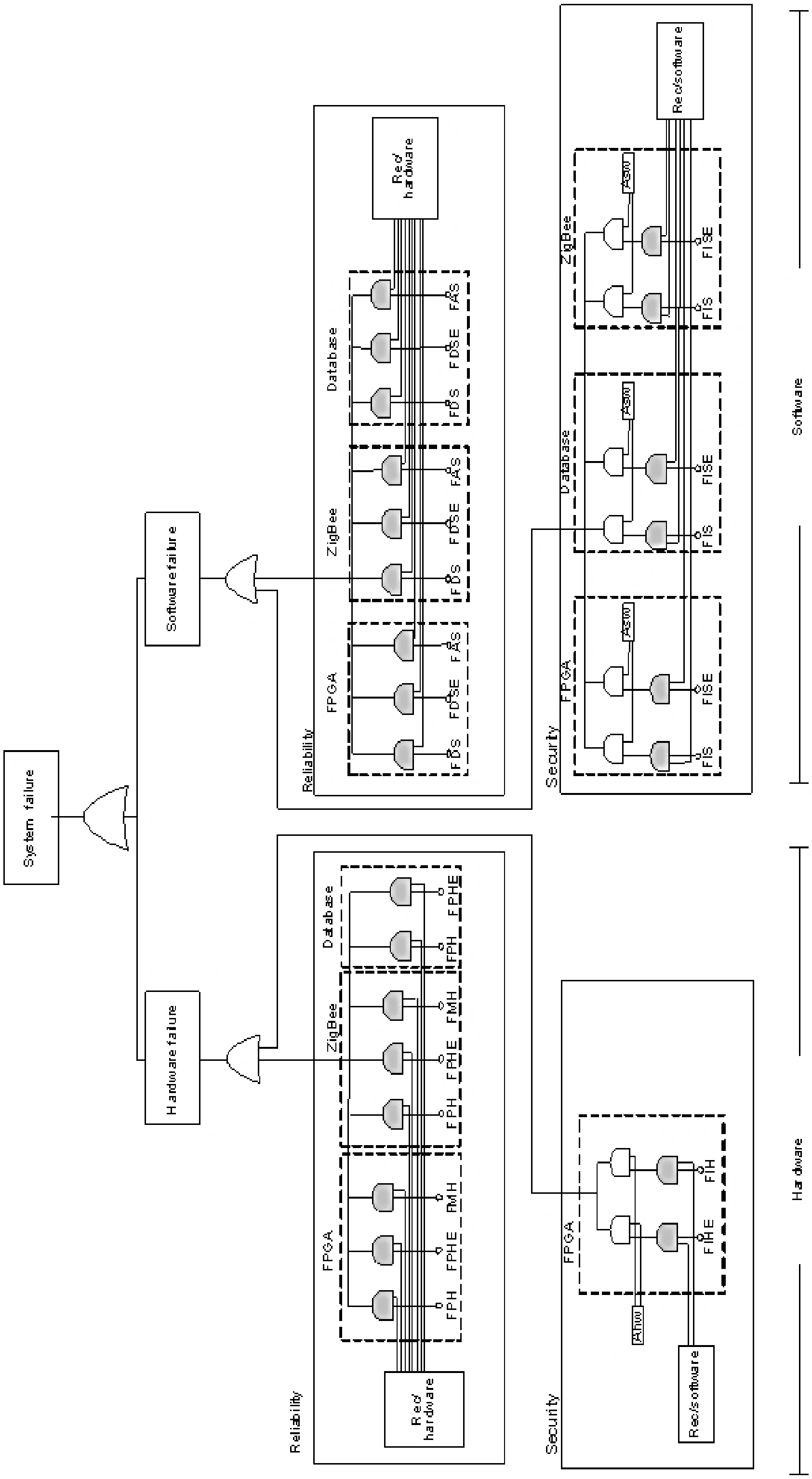

Figure 2. Model of the AvTA tree for information and control system of BAS

10.11113/mjfas.v19n3.2902

Table 1. The probability of (BAS) failure-free operation calculations

Level	Factor	Component	Parameter	Notation	Probability	
Hardware	Reliability	FPGA	operating error (hardware)	FPH	0.0012	Probability of system failure=0.001590089
			operating error (soft hardware error	FPHE	0.002	
			manufacture failure (hardware)	FMH	0.25	
		ZigBee	operating error (hardware)	FPH	0.0021	
			operating error (soft hardware error	FPHE	0.1265	
			manufacture failure (hardware)	FMH	0.15157	
		Database	operating error (hardware)	FPH	0.17664	
			operating error (soft hardware error	FPHE	0.20171	
		Rec/hardware	relies on the type of failure	REC	0.8	
	Cyber Securi	FPGA	interaction failure (severe hardware vulnerability)	FIH	0.25185	
			interaction failure (soft hardware vul	FIHE	0.27692	
		Ahw	attacks (hardware)	Ahw	0.30199	
		Rec/software	relies on the type of failure	REC	0.5	
Software	Reliability	FPGA	failure induced by a flaw in the desig (software)	FDS	0.0051	
			incompatibilities in software (softwa	FDSE	0.015	
			failure caused by ageing (software)	FAS	0.025	
		ZigBee	failure induced by a flaw in the desig (software)	FDS	0.035	
			Software faults are to blame for the (software error)	FDSE	0.045	
			failure caused by ageing (software)	FAS	0.055	
		Database	failure induced by a flaw in the desig (software)	FDS	0.065	
			Software faults are to blame for the (software error)	FDSE	0.075	
			failure caused by ageing (software)	FAS	0.085	
		Rec/hardware	recovery varies according to the typ	REC	0.8	
	Cyber Security	FPGA	interaction failure (severe software vulnerability)	FIS	0.0215	
			interaction failure (soft software vulr	FISE	0.078	
			attacks (software)	Asw	0.325	
		Database	interaction failure (severe software vulnerability)	FIS	0.445	
			interaction failure (soft software vulr	FISE	0.59675	
			attacks (software)	Asw	0.74845	
		ZigBee	lack of communication (severe softv vulnerability)	FIS	0.90025	
			interaction failure (soft software vulr	FISE	0.0252	
			attacks (software)	Asw	0.07851	
		(Rec/software)	recovery based on the type of failur	REC	0.5	

At the beginning of the operation, the system's availability drops to a minimum of AMBAS2.1min=0.9629, then steadily rises to its steady state. TMBAS2.1const=16225 hours characterize the timeframe of complete eradication of defects and vulnerabilities during the transition from the state of availability to the steady-state. The AMBASconst status of availability condition is at 0.9975% [24-26].

Characteristics of Classification the Models

Assumptions, a marked graph, and the associated differential Kolmogorov equations, input data, and modeling outcomes are all included in MBAS models [27]. In the MBAS1 base model, random events are used to describe the creation of software defects and vulnerabilities [28]. Within the time span of TMBAS 1const = 28117 hours, the availability function has a constant value of AMBAS 1min = 0.9964. Maintenance processes are taken into account in an unlimited number of ways in the MBAS2.1 availability model [29]. At the time of commissioning, there were two software faults and two vulnerabilities in the BAS architecture model depicted in Figure 4. A basic assumption is made that only one fault or vulnerability can be found and removed. Any time a bug or weakness is discovered, the system will go into a state of partial failure until the problem has been fixed. If a bug or vulnerability is never found, a program restart will restore everything to normal [29-32]. During the elimination process, no new defects or vulnerabilities are introduced.

Table 2. Models of I&CS availability classification for a smart building

	Characteristics	Model specification	Conventional notions
	A) Base model without maint	- No. of faults are (0 to Nd) - No. of sensitivity are (0 to Nv) - No. of maintenances is (0)	MBAS1
	B) Model with common main	- No. of faults are (0 to Nd) - No. of sensitivity are (0 to Nv) - No. of maintenances is infinite throughout the system's lifetime. - The type of maintenance is (common)	N
		- No. of faults are (0 to Nd) - No. of sensitivity are (0 to Nv) - No. of maintenances are (0 to Np) - The type of maintenance is (common)	MBAS2.2
	C) Model with separate main	- No. of faults are (0 to Nd) - No. of sensitivity are (0 to Nv) - No. of maintenances is infinite throughout the system's lifetime. - The type of the service is (separate)	MBAS3.1
		- No. of faults are (0 to Nd) - No. of sensitivity are (0 to Nv) - The No. of the maintenances by defects are (0 to Ndp) -The No. of the maintenances by vulnerabilities are (0 to Ndv) - the type of service: separate	MBAS3.2

On the graph, diagonal transitions with a downward shift show the development of software defects (with intensity λDi), and weaknesses - diagonal transitions with an upward shift (with intensity λIj). Following the development of vulnerability [33], its elimination is carried out with energy PS*μIj (for the defect - PR*μDi). When all faults and vulnerabilities have been eliminated, the system transitions to state F. (0,0).

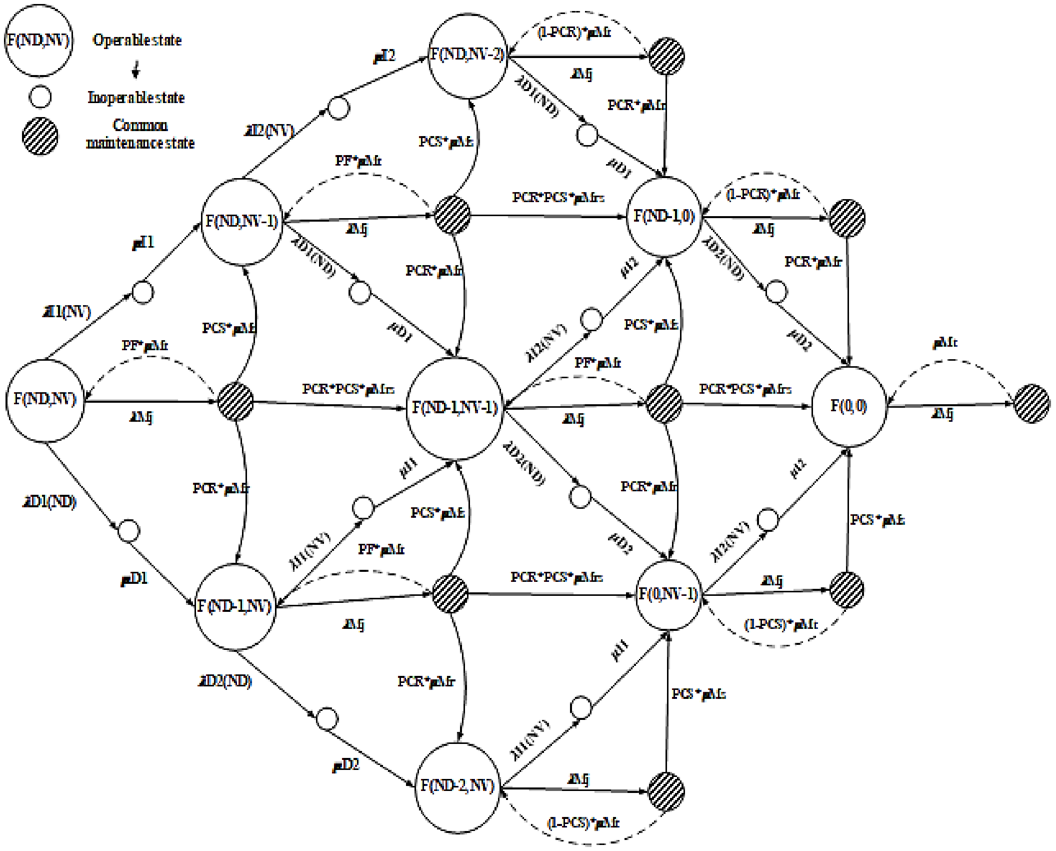

Figure 3. The BAS model is depicted as a marked graph, with the common maintenance

Four transitions are conceivable from the condition of maintenance: a) in the case of vulnerability detection, the transition is vertically upward with the intensity of PCS*Ms, b) in the case of defect detection [34], the transition is vertically downward with the intensity of PCR*Mr, c) in the case of the defect and vulnerability detection, the transition is to the right weighted by the intensity of PCS*PCR*Mrs, d) in the case of non-identification of the defect and vulnerability, the transition is to the predefined state [35]. At the same time, the ratio defining the complete group of events is important: (PF+PCS+PCR+PCS*PCR=1). The (MBAS 2.2) model, in contrast to the MBAS2.1 model, restricts the total number of measures that can be taken throughout the system's lifespan [36]. Using the simulation, developers can only assume that there are no problems or vulnerabilities that have not yet been discovered. Consequently, it is designed to conduct a predetermined number of Np service procedures. The simulation results indicated that the (MBAS 2.2) maintenance limitations allow for perfect availability (AMBAS 2.2const = 1) in a stable condition. Simultaneously [36,37], the value of the minimal availability changes insignificantly between models with limited and unlimited maintenance (at 8.831e-4). The transition period of the steady mode availability in the (MBAS 2.2) model is (9.481) times longer than in the model with limitless (MBAS 2.1) maintenance; yet, defect and vulnerability eradication in the maintenance model is faster than in the (MBAS 1) model (1.271 times) as shown in Figure 4.

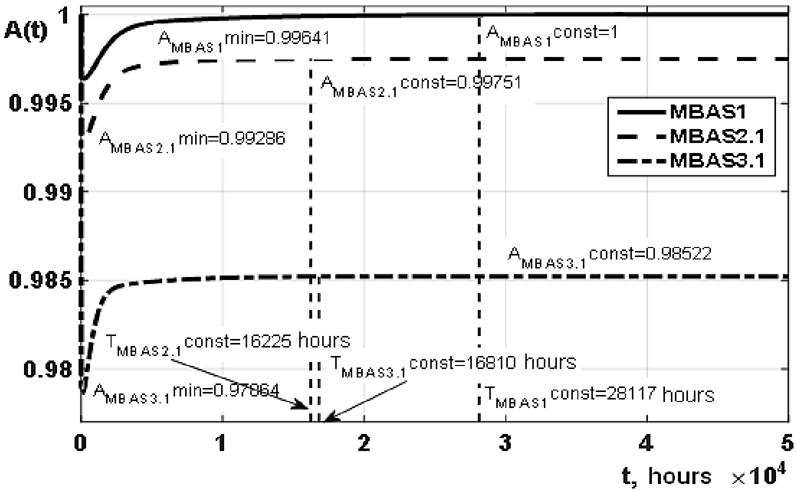

Figure 4. Graphs of alterations to the BAS architecture's availability function with no maintenance (MBAS 1), shared maintenance (MBAS 2.1), and with separate maintenance (MBAS 3.1)

Results and Discussion

When conducting separate and common maintenance operations, this method was used to determine the parameters that should be used to define strategies for maintenance information and control systems in smart buildings. Simulation models in the Matlab (Figure 6) environment were constructed to validate the results' robustness and overcome the constraints of analytical models, particularly the exponential distribution of attack flow parameters. Comparison of analytical and simulation models of BAS showed a satisfactory convergence of values of availability coefficients in the steady-state (Figure 6).

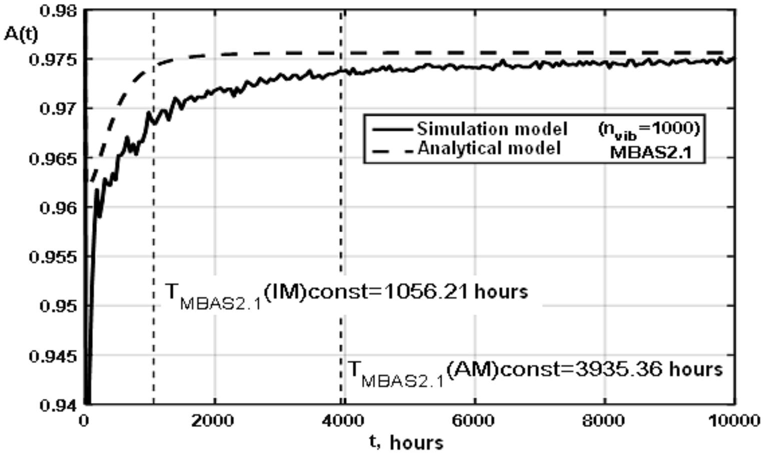

Figure 6. Results of simulation and analytical modeling of BAS availability

The tconst result indicator has a distribution with a shifted left maximum, as demonstrated by calculations for (MBAS 1) and (MBAS 2.1) models. Mean (tconst) and max (tconst) are both consistent with the analytical model with an error of (10^{-4} and 10^{-7}) respectively. The smallest mistakes in the AMBASmin (analytical model) are found in (MBAS 1) systems that do not require common maintenance; the largest errors are found in systems that do require common maintenance. In general, AMBASmin's mean (Amin) and max (Amin) errors do not surpass (9.8% and 4.7%) respectively (Amin). Using the mean (tconst) average and maximum max (tconst) estimate, the transition time to steady-state is computed with an error of no more than $4.7*10^{-4}$ and $5.1*10^{-7}$, respectively.

10.11113/mjfas.v19n3.2902

Analyze all relevant documentation on the researched system (technical specification, technical conditions, operational instructions, and normative documents, for example) in this situation, all of the system's needs are exposed (cost limitation: тmax, reliability and cybersecurity limitation: Pmin, Aminmin, Tconstmin), and the explanation for the possibility of endless maintenances is conducted. There are several combinations of options for limitless and limited maintenance, as well as common and separate maintenances by dependability and cyber security, as a result of evaluating input parameters for Markov behavior. Making proper (MBAS) models is one of these choices. Figure 7 depicts the block's outcomes.

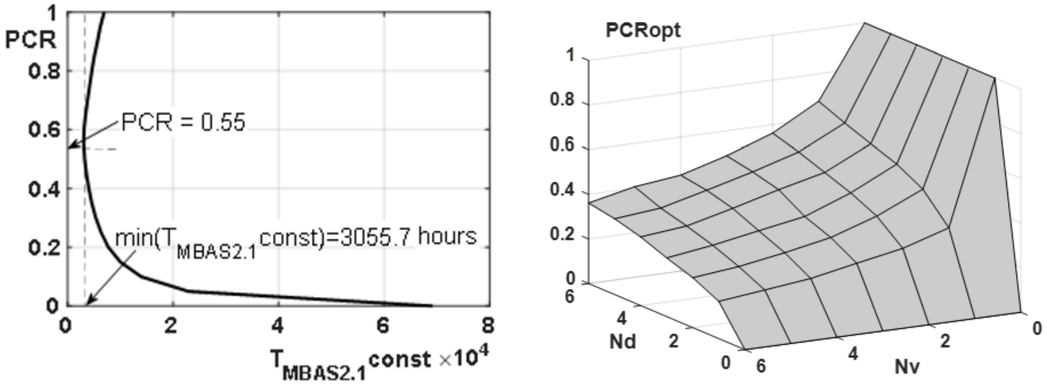

Figure 7. Results of studying the dependence of Tconst (PCR), and the determination of the optimal Tconst→min criterion for the input parameter PCRopt using the MBAS2.1 model

Conclusion

Information technology (IT) evaluation and choice of choices for its provision are based on the proposed models and procedures, which take into consideration various forms of maintenance strategies by dependability and cyber security. A method for defining parameters for maintenance and information technology for providing availability and cyber security of smart building information systems has been developed in this study, thereby completing this paper's scientific task. Smart building information and control systems are protected by this information technology strategy, which takes into account attacks on software vulnerabilities and faults, as well as common and distinct maintenance methods. These faults and vulnerabilities may be taken into account, as could the parameters of the performance recovery and attack blocking processes, in their architecture as a whole.

Conflicts of Interest

The author(s) declare(s) that there is no conflict of interest regarding the publication of this paper.

Acknowledgement

This work is part of a research project, supported by the Ministry of Higher Education, Malaysia, and the University of Technology Malaysia. Also supported by Imam Ja'afar Al-Sadiq University, Baghdad, Iraq.

References

[1] Gong, K., Yang, J., Wang, X., Jiang, C., Xiong, Z., Zhang, M., & Zhang, S. (2022). Comprehensive review of modeling, structure, and integration techniques of smart buildings in the cyber-physical-social system. *Frontiers in Energy*, 1-21.

[2] Jain, S., & Chandrasekaran, K. (2022). Industrial automation using internet of things. *Research Anthology on Cross-Disciplinary Designs and Applications of Automation* (pp. 355-383). IGI Global.

[3] Xiao, F., & Fan, C. (2022). Building information modeling and building automation systems data integration and big data analytics for building energy management. *Research Companion to Building Information Modeling* (pp. 525-549). Edward Elgar Publishing.

10.11113/mjfas.v19n3.2902

[4] Camachi, B. E., Ichim, L., & Popescu, D. (2018, May). Cyber security of smart grid infrastructure. *2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI)* (pp. 000303-000308). IEEE.

[5] Akram, J., & Ping, L. (2020). How to build a vulnerability benchmark to overcome cyber security attacks. *IET Information Security*, *14*(1), 60-71.

[6] Dhillon, G., Oliveira, T., Susarapu, S., & Caldeira, M. (2016). Deciding between information security and usability: Developing value based objectives. *Computers in Human Behavior*, *61*, 656-666.

[7] Alsudani, M. Q., Fakhruldeen, H. F., Al-Asady, H. A. J., & Jabbar, F. I. (2022). Storage and encryption file authentication for cloud-based data retrieval. *Bulletin of Electrical Engineering and Informatics*, *11*(2), 1110-1116.

[8] Kharchenko, V., Ponochovniy, Y., Abdulmunem, A. S. M. Q., & Shulga, I. (2019, September). AvTA based assessment of dependability considering recovery after failures and attacks on vulnerabilities. *2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (Vol. 2, pp. 1036-1040). IEEE.

[9] Waheed, S. R., Rahim, M. S. M., Suaib, N. M., & Salim, A. A. (2023). CNN deep learning-based image to vector depiction. *Multimedia Tools and Applications*, 1-20.

[10] Salim, A. A., Ghoshal, S. K., Suan, L. P., Bidin, N., Hamzah, K., Duralim, M., & Bakhtiar, H. (2018). Liquid media regulated growth of cinnamon nanoparticles: Absorption and emission traits. *Malaysian Journal of Fundamental and Applied Sciences*, *14*(3-1), 447-449.

[11] Amana, M. S., Aldhuhaibat, M. J. R., & Salim, A. A. (2021). Evaluation of the absorption, scattering and overall probability of gamma rays in lead and concrete interactions. *SCIOL Biomed*, *4*, 191-199.

[12] Alguliyev, R., Imamverdiyev, Y., & Sukhostat, L. (2018). Cyber-physical systems and their security issues. *Computers in Industry*, *100*, 212-223.

[13] Waheed, S. R., Adnan, M. M., Suaib, N. M., & Rahim, M. S. M. (2020, April). Fuzzy logic controller for classroom air conditioner. *Journal of Physics: Conference Series*. *1484*(1), 012018. IOP Publishing.

[14] Kim, D., Choi, S., Kim, S., & Choi, B. (2011, May). MATLAB-based digital design of current mode control for multi-module bidirectional battery charging/discharging converters. *8th International Conference on Power Electronics-ECCE Asia* (pp. 2256-2260). IEEE.

[15] Al-Asady, H. A. J., Fakhruldeen, H. F., & Alsudani, M. Q. (2021). Channel estimation of OFDM in c-band communication systems under different distribution conditions. *Indonesian Journal of Electrical Engineering and Computer Science*, *23*(3), 1778-1782.

[16] Wen, J. T., & Mishra, S. (2018). Intelligent building control systems. *A Survey of Modern Building Control and Sensing Strategies (Advances in Industrial Control)*.

[17] Elnour, M., Meskin, N., Khan, K., & Jain, R. (2021). Application of data-driven attack detection framework for secure operation in smart buildings. *Sustainable Cities and Society*, *69*, 102816.

[18] Hachem, J. E., Chiprianov, V., Babar, M. A., Khalil, T. A., & Aniorte, P. (2020). Modeling, analyzing and predicting security cascading attacks in smart buildings systems-of-systems. *Journal of Systems and Software*, *162*, 110484.

[19] Boarin, P., Martinez-Molina, A., & Juan-Ferruses, I. (2020). Understanding students' perception of sustainability in architecture education: A comparison among universities in three different continents. *Journal of Cleaner Production*, *248*, 119237.

[20] Sun, Y., Zhang, J., Li, G., Wang, Y., Sun, J., & Jiang, C. (2019). Optimized neural network using beetle antennae search for predicting the unconfined compressive strength of jet grouting coalcretes. *International Journal for Numerical and Analytical Methods in Geomechanics*, *43*(4), 801-813.

[21] Peeters, J. F. W., Basten, R. J., & Tinga, T. (2018). Improving failure analysis efficiency by combining FTA and FMEA in a recursive manner. *Reliability engineering & system safety*, *172*, 36-44.

[22] Smith, M. D., & Paté-Cornell, M. E. (2018). Cyber risk analysis for a smart grid: How smart is smart enough? A multiarmed bandit approach to cyber security investment. *IEEE Transactions on Engineering Management*, *65*(3), 434-447.

[23] Kharchenko, V., Ponochovnyi, Y., Boyarchuk, A., Brezhnev, E., & Andrashov, A. (2018, May). Monte-Carlo simulation and availability assessment of the smart building automation systems considering component failures and attacks on vulnerabilities. *Contemporary Complex Systems and Their Dependability: Proceedings of the Thirteenth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX, July 2-6, 2018, Brunów, Poland* (pp. 270-280). Cham: Springer International Publishing.

[24] Hyman, B. T., Alisha, Z., & Gordon, S. (2019). Secure controls for smart cities; applications in intelligent transportation systems and smart buildings. *International Journal of Science and Engineering Applications*, *8*(6), 167-171.

[25] Waheed, S. R., Suaib, N. M., Rahim, M. S. M., Adnan, M. M., & Salim, A. A. (2021, April). Deep learning algorithms-based object detection and localization revisited. *Journal of Physics: Conference Series*. *1892*(1), 012001. IOP Publishing.

[26] Ciholas, P., Lennie, A., Sadigova, P., & Such, J. M. (2019). The security of smart buildings: a systematic literature review. *arXiv preprint arXiv:1901.05837*.

[27] Eini, R., Linkous, L., Zohrabi, N., & Abdelwahed, S. (2021). Smart building management system: Performance specifications and design requirements. *Journal of Building Engineering*, *39*, 102222.

[28] Sinopoli, J. (2016). *Advanced technology for smart buildings*. Artech House.

[29] Verma, A., Prakash, S., Srivastava, V., Kumar, A., & Mukhopadhyay, S. C. (2019). Sensing, controlling, and IoT infrastructure in smart building: a review. *IEEE Sensors Journal*, *19*(20), 9036-9046.

[30] Salim, A. A., Mahraz, Z. A. S., Anigrahawati, P., Jan, N. A. M., Ghoshal, S. K., Sahar, M. R., ... & Sazali, E. S. (2021). Structural, chemical and magnetic features of gold nanoshapes integrated-Er2O3-doped tellurite glass system prepared by a conventional melt-quenching technique. *Applied Physics A*, *127*(9), 673.

[31] Salim, A. A., Bakhtiar, H., Ghoshal, S. K., & Huyop, F. (2020). Customised structural, optical and antibacterial characteristics of cinnamon nanoclusters produced inside organic solvent using 532 nm Q-switched Nd: YAG-pulse laser ablation. *Optics & Laser Technology*, *130*, 106331.

[32] Salim, A. A., Ghoshal, S. K., & Bakhtiar, H. (2021). Tailored morphology, absorption and bactericidal traits of cinnamon nanocrystallites made via PLAL method: Role of altering laser fluence and solvent. *Optik*, *226*, 165879.

[33] Mylrea, M., & Gourisetti, S. N. G. (2017). Cybersecurity and optimization in smart "autonomous" buildings. *Autonomy and Artificial Intelligence: A Threat or Savior?* 263-294.

[34] Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015, November). An investigation on cyber security threats and security models. In *2015 IEEE 2nd international conference on cyber security and cloud computing* (pp. 307-311). IEEE.

[35] Xu, W., Zhang, J., Kim, J. Y., Huang, W., Kanhere, S. S., Jha, S. K., & Hu, W. (2019). The design, implementation, and deployment of a smart lighting system for smart buildings. *IEEE Internet of Things Journal*, *6*(4), 7266-7281.

[36] Andri, C., Alkawaz, M. H., & Waheed, S. R. (2019, June). Examining effectiveness and user experiences in 3d mobile based augmented reality for msu virtual tour. In *2019 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)* (pp. 161-167). IEEE.

[37] Salim, A. A., Bidin, N., & Islam, S. (2017). Low power CO2 laser modified iron/nickel alloyed pure aluminum surface: Evaluation of structural and mechanical properties. *Surface and Coatings Technology*, *315*, 24-31.