Reliability of Cyber Physical Systems with Focus on Building Management Systems

Sanja Lazarova-Molnar[1], Hamid Reza Shaker[1], and Nader Mohamed[2]
[1]Center for Energy Informatics, University of Southern Denmark, Denmark
[2]Middleware Technologies Lab., Bahrain
slmo@mmmi.sdu.dk, hrsh@mmmi.sdu.dk, nader@middleware-tech.net

***Abstract*—Cyber-physical systems are slowly emerging to dominate our world. Cyber-physical systems (CPS) are systems that tightly integrates users, devices and software. Whereas many of these systems are obviously safety-critical systems, some of them become so under special circumstances. This is the case with our focus CPS, i.e. building management systems (BMS), which are not always safety critical per se, but under special circumstances they can become such. This certainly depends on the purpose of the building. We can easily imagine BMS of hospital buildings as safety-critical, but also BMS of buildings that store sensitive materials and equipment that could be of biological nature or encompassing sensitive technology that would need special temperature, humidity and light settings. For this reason, in this paper we would like to emphasize on the importance of reliability of CPS in general, with a special focus on BMS, as our area of interest. Furthermore, we also propose a classification of buildings with respect to the necessity of having their reliability evaluated.**

Keywords—cyber-physical systems; reliability; building management systems; challenge

I. INTRODUCTION

Cyber-physical systems (CPS) are increasingly reaching everywhere. A system is defined as cyber-physical if it tightly integrates users, devices and algorithms. Typically, CPS consist of a number of computing devices that communicate with each other and interact with the physical world through sensors and actuators in a feedback loop. Cyber physical systems encompass a large number of systems, from medical systems, automobiles, airport management systems, through to building management systems (BMS). The rise of Internet of Things as an enabling technology of cyber-physical systems can definitely further enhance their expansion [1].

CPS, compared to purely computational, or purely physical systems, exhibit quite a number of challenges, as the connection between the computational and the physical entities is far from smooth, and the integration of users only further aggravates this connection. Due to device proliferation and large-scale connectivity, a variety of functionalities are now feasible in cyber-physical systems. Connectivity, however, also means that CPS function in unreliable open environments, and consequently resiliency to faults (reliability), malfunctions (safety) and attacks (security) become imperative. Moreover, a significant number of cyber-physical systems are categorized as safety-critical systems, which means that their incorrect operation could imply loss of life, significant property damage or damage to the environment [2]. In the same source [2], which focused only on safety-critical *software* systems, Knight points out that "meeting the reliability goal seems unlikely for a system with this many computers, this number of lines of code, and this testing history" referring to a software system that was supposed to shut down a nuclear reactor when problems arose. Furthermore, in another report, the author Lee points out that "even the simplest C program is not predictable and reliable in the context of CPS because the program does not express aspects of the behavior that are essential to the system" [3]. When the software gets further coupled with hardware and users, as in CPS case, reliability evaluation becomes a significant challenge.

Henceforth, a great attention has been given in particular to tackling the following challenges of cyber-physical systems:

- Security, where a significant amount of ongoing research is focused on how to protect cyber-physical systems from security attacks [4, 5], and
- Safety, which is the system's resilience to hazards and malfunctions [6].

Certain highly safety-critical CPS have had tailored reliability analysis approaches developed [7, 8]. However, the development of a systematic reliability analysis of CPS has not received an adequate consideration, so in this paper we would like to summarize the calls for increased attention to the challenge [9], as well as provide an overview of the attempts to address the issue. Furthermore, we focus on BMS and demonstrate the importance of assessing reliability in relation to purpose of buildings. For this reason we also introduce classification of buildings with respect to the corresponding importance of their reliability evaluation.

The paper is structured as follows. We begin by providing preliminaries in Section II, where we describe the concepts of Reliability, CPS and the specificity of Reliability of CPS. In Section III, we focus on the reliability of building management systems, describing the state-of-the-art and pointing out the major challenges and directions. In Section IV we describe the implications of our research findings, and finally in Section V we conclude the paper.

II. RELIABILITY AND CYBER-PHYSICAL SYSTEMS

In the following we provide a background on the concept of reliability and its importance with respect to cyber-physical systems.

978-1-5090-5252-3/16/$31.00 ©2016 IEEE

A. Reliability

Reliability is a measure of the ability that the system operates as expected under predefined conditions for a predefined duration of time. As systems are composed of a number of components, reliability of systems is expressed through reliabilities of each of their components. To accurately describe the concept of reliability it is essential to define the notions of fault, failure and error, as both are highly related to the concept of reliability:

- Fault is an incorrect step, process, or data definition in a program [3]. It is a programming error that leads to an erroneous result in some programs during execution. A software bug is the common term used to describe a fault in a program that produces an incorrect or unexpected result, or causes it to behave in unintended ways. Fault density is the number of software faults, usually expressed as faults per thousand lines of code. It is a common software reliability metric.
- Failure is the inability of a system or component to perform its required function within the specified performance requirement [3].
- Error is the difference between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition. It is also known as the manifestation of a fault.

The main reliability measures are defined through the concepts of faults and failures, such as "mean time to failure" or MTTF or "mean time to repair" or MTTR. The assumption for using these two measures is that both the repair time and inter-failure time are exponentially distributed. These are also the most common reliability features for describing components. In the case of non-exponentially distributed failures and repairs, one speaks of failure distributions and repair distributions.

The convenience of assuming exponentially distributed failures and repairs is in the significant number of analytical methods available to tackle this class of problems. One of the most popular reliability modeling methods that utilizes this assumption are Fault Trees [7, 8]. The assumption for exponentially distributed failures and repair times, however, has often been proven to be an inadequate and over-simplifying assumption [10, 11], and thus, as misleading for evaluating reliability. The releasing of the assumption of memoryless-ness has further yielded development of a number of more sophisticated methods [12], such as Dynamic Fault Trees [13] and the Proxel-Based Method [14]. Standard discrete-event simulation is also one of the methods that can manage non-exponentially distributed failures, the disadvantage being the typical stiffness of reliability models, as failures are typically rare events.

B. Cyber-Physical Systems

Cyber-physical systems are distributed embedded systems developed to support smart and context-aware mission-critical applications that provide interactions between physical and cyber worlds. There are many important CPS applications that add many enhancements and smart features to several types of physical systems and environments. CPS can add smart mechanisms to fully automate manufacturing processes, manage and enhance the operations and safety of environments and infrastructures, and enable unmanned vehicles operations and applications. They can also enhance the safety of transportation systems and improve healthcare for patients. CPS combine various concepts and technologies from embedded systems, distributed systems, networks, software, and hardware; as well as other engineering disciplines such as systems, civil, mechanical, electrical, electronic, and control engineering to provide added features to the physical world [15]. CPS provide monitoring and control functions that help achieve specified goals to benefit the application domain. Unlike traditional embedded systems, CPS are distributed embedded systems with distributed components and processing capabilities. Embedded computing devices of CPS can be in sensors, actuators, microcontrollers, and other devices that are usually connected with a wired or wireless network and tightly coupled with their physical environment.

As CPS are embedded in physical environments, they provide useful interactions between the computational and physical elements through intelligent mechanisms. These intelligent mechanisms can be organized in four main steps:

1- Observing the current status of the physical system or environment using different type of sensors that are attached to the elements of the physical system or environment.

2- Building a knowledge base about the physical system environment from the collected sensed information using software functions and storage systems.

3- Making decisions to enhance or control the physical system or environment to meet specific objectives defined for the application. This is done using the knowledgebase and some current status information of the physical system or environment with the help of smart algorithms that run on some integrated computing components.

4- Applying the enhancement or control actions through the use of actuators that are attached to the elements of the physical system or environment.

These four steps are linked in a closed loop to allow the CPS to provide full monitoring and control functions to achieve the needed objectives. These objectives can be to provide the adaptability, autonomy, efficiency, functionality, reliability, safety, and usability of the system or environment.

Due to the importance of CPS applications and the complexity of their development process, huge research efforts started on different CPS challenges. These include security, reliability, performance, quality, validation, and development methodologies and tools [16, 17]. This includes some efforts in efficient utilizations of CPS to enhance energy consumption in smart buildings.

C. Reliability of Cyber-Physical Systems

System reliability is an important requirement of CPS since examples of such systems range from safety critical complex infrastructures to simple but important medical devices [18-

20]. The demand for reliability in cyber-physical systems has constantly been increased. If demands for reliability are not addressed effectively, further deployment of cyber-physical systems will be slowed down in applications [16, 21]. Reliability of cyber-physical systems has therefore received attention in different applications [22-24].

Reliability analysis for CPS is challenging due to their nature and structure [25]. While reliability analysis for the hardware part of CPS is well-explored, it is certainly not sufficient for reliability evaluation of the overall cyber-physical systems. Hardware and physical components in cyber-physical systems are tightly combined with software and computational elements. In contrast to the performance degradation in hardware and physical elements, which can be described by failure models, software and computational elements do not deteriorate and do not follow a failure model similar to physical components. To design architecture of a reliable cyber-physical system one has to take into account the integrated nature of the systems. In [26], a hybrid method that uses fault-tolerant structures with formal verification is proposed. The presented architecture supports the design of reliable cyber-physical systems. Another example of such efforts is presented in [27], which describes a service-oriented cyber-physical system with a service-oriented architecture and mobile Internet device.

Security of CPS is a related research field, which has received a lot of attention recently [28-31]. While security is different than reliability, they are highly related. It is well-known that non-secure system is not reliable, and a non-reliable system cannot be secure [32].

III. Reliability of Builidng Management Systems

Building management systems represent a special type of cyber-physical systems. BMS are systems that control and monitor mechanical, electrical and electromechanical services in buildings. Such services can include power, heating, ventilation, air-conditioning, physical access control, pumping stations, elevators and lights. With the emergence of new sensing technologies and other building intelligence solutions, BMS have grown to be very sophisticated and complex systems [33, 34]. They are specific in that they carry a large burden in the global struggle for lower energy consumption (ca. 40% of total energy consumption is attributed to buildings) and they can serve various purposes, including highly critical ones. At the same time, BMS are also highly multifaceted as they interconnect entities of different natures, such as occupants, weather conditions, building materials, software, etc., many of which exhibit high uncertainties in their behaviors.

Currently, the majority of BMS are assessed according to two significant performance metrics, energy savings and occupants comfort [35]. Reliability is still a grey zone, as illustrated in Figure 1. Reliability, however, can significantly affect and enhance both of the other two measures and it should not be ignored. In the following we provide an insight into the state of the art in reliability approaches for BMS, as well as the challenges associated with it.

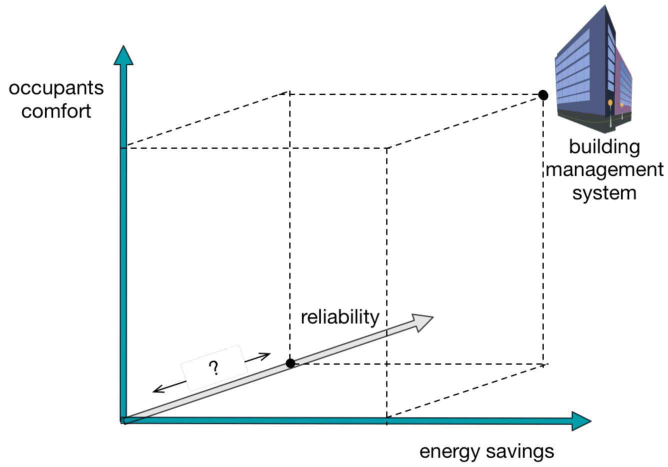

Figure 1. Performance goals of a building, energy savings and occupants comfort typically predefined, reliability typically neglected

A. *State of the Art*

Reliability of BMS is a critical measure, and derived from the definition of the concept of reliability, it represents the ability of a building management system to perform its predefined functions for a given period of time. This implies proper functioning of a building, demonstrated by supporting all hosted entities in achieving their corresponding performance goals.

Hospitals are examples of buildings where proper functioning of a BMS is critical. Think of lighting failing during a surgery to comprehend its criticality. Therefore, besides comfort and energy savings, reliability evaluation should play an essential role in assessing the performance of hospital's building management system. One attempt to tackle reliability for hospital buildings, although not as explicit, is presented in [36], where the authors describe a methodology of how to set maintenance priorities in hospital buildings based on performance indicators for building components and systems. The solution was successfully tested on 17 public health care facilities in Israel.

Reliability of BMS has not received an adequate span of attention, despite the frequent calls for its importance [37, 38]. BMS' reliability, however, is a highly critical measure and goes hand in hand with its maintenance cost. In other words, having an accurate reliability measure would enhance the potential for designing optimal preventive maintenance schedules and influence components purchasing decisions. This, in turn, would both minimize maintenance cost, as well as improve the performance of the building, thus enhancing both comfort and energy savings.

In one recent work on the topic of reliability [39], authors state that "reliability, maintainability and availability are essential features if we want to define the quality, that is the ability, of the plant to fulfill a specific requirement". This is one of the rare works that emphasizes on the importance of reliability in buildings, focusing on residential buildings.

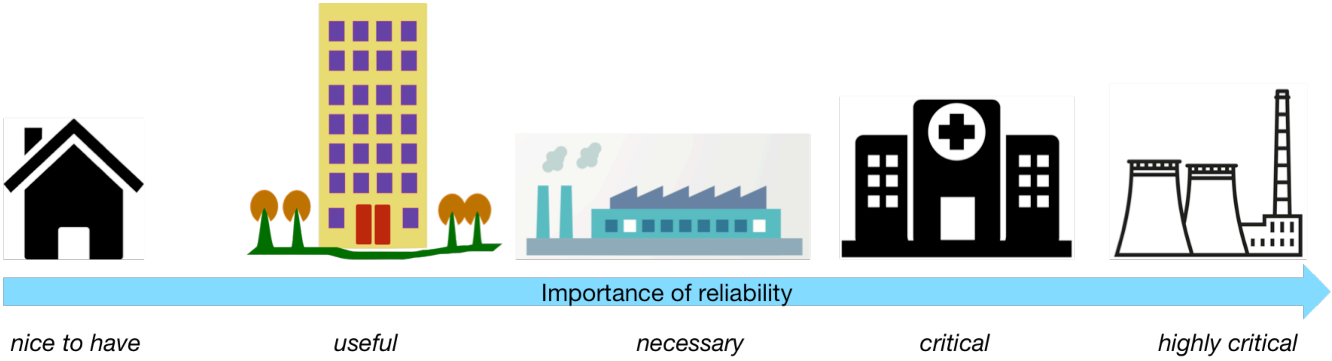

Figure 2. Illustration of the concept of importance of reliability with respect to the purpose of the building

In another work focused on lighting systems [40], Salata et al. investigate the impact of reliability of lighting systems on the economy of a building. The authors of the paper further conclude that "the fact of choosing a system, consisting of LED sources only, can represent a convenient choice only under certain circumstances, that is as long as we talk about reliability and service life". Thus, having an accurate reliability measure is of paramount importance to estimating cost. We are confident that this conclusion can be extended to other types of systems that comprise BMS, besides lighting.

Through a comprehensive modeling of BMS' fault dependency, and tracking of relevant data, which is now easier than ever before, reliability of a BMS can be estimated at any given point in time. These reliability models and estimates can be further used to provide decision support in purchasing components for BMS. Furthermore, they can also be utilized to support configuring BMS.

In the following we observe the different purposes of buildings and relate them to the importance of providing reliability analysis correspondingly.

B. *Challenges and Importance of Reliability of Building Management Systems*

BMS are multi-objective cyber-physical systems that are very domain specific and these domains also dictate their objective and performance metrics definition. We define reliability to range from "nice to have" to "extremely important" metric based on the purpose of a building. Buildings have been classified based on various properties [41], such as airtightness [42], or acoustics [43]. However, up to now, there has not been a classification proposed to target importance of reliability to buildings. This has motivated us to investigate buildings specifications and purpose with respect to reliability and provide their classification with respect to their reliability importance. To start with, we have identified several different types of buildings, as follows:

- Single Residential Buildings,
- Communal Residential Buildings,
- Commercial Office Buildings,
- Commercial Retail Buildings (e.g. shopping centers, etc.),
- Hospitals and Emergency Centers (Fire Department or Police),
- Educational Buildings, and
- Sensitive Materials Buildings.

Note that this classification is in no way exhaustive and it is more thought of as a call for attention to assess the importance of reliability evaluation to buildings. We have further utilized and generalized these different types of buildings to assess the importance of their reliability evaluation. Reliability evaluation, however, always comes at a cost, and in some cases this cost is not justified. In other cases, however, the cost is in human lives, and that definitely justifies the expenses. With respect to this, in Figure 2 we illustrate the concept of importance of reliability with respect to the various types of buildings. Furthermore, in Table 1 we provide the meanings of each of the reliability importance levels in terms of its cost with respect to the benefits.

Table 1. Explanation of the levels of importance of reliability evaluation

Reliability Importance	Meaning
nice to have	benefits do not justify the cost of reliability assessment
useful	benefits could exceed the cost of reliability assessment
necessary	benefits largely exceed the cost of reliability assessment
critical	benefits of reliability assessment concern human lives
highly critical	benefits of reliability assessment concern a large number of human lives

We define the first level of reliability importance to BMS as "nice to have". This level encompasses BMS of smaller buildings, such as one-family houses, where reliability assessment would be typically seen as an unnecessary luxury. Note that currently it is very rare that small residential buildings are controlled by BMS. This, however, has likelihood to change in future. In communal residential buildings, nevertheless, assessment of reliability of their BMS can be seen be "useful", as certain faults have the potential to affect a large number of occupants, and their repairs can also turn out to be quite costly. Even though these two categories of buildings ("nice to have" and "useful") are still currently less important in terms of reliability evaluation, we can imagine this changing in the future. This is mostly due to the emergence of many new building intelligence technologies, which in general decrease reliability of a building as new devices exhibit new types of faults, but also increase the possibilities of collecting data that is essential for reliability evaluation [44-46].

The third category of buildings, termed as "necessary" with respect to the importance of reliability evaluation of their BMS, encompasses buildings where benefits from reliability evaluation have the potential to largely exceed the cost of performing it. These are mostly commercial buildings, where the correct operation of a building largely influences the productivity of the hosted businesses. Examples of these types of buildings are shopping centers or factories.

The last two categories, "critical" and "highly critical" encompass buildings where the lack of reliability could cost human lives, at two different scales. An example of a "critical" building is a hospital, where the correct operation of the building management system is crucial for the well-being of patients. An example of a "highly critical" system is a nuclear power plant, where the inability of the building to operate as expected could have devastating consequences for both the environment and a large number of humans.

As of now, only reliability in highly critical BMS has been tackled more thoroughly, and it is usually improved through heavy redundancy [47]. Generally, this could mean that the system incorporates redundant components having multi state systems with different maintenance policies. Among the significant work on this topic, although quite dated, Arueti [48] presents a tool to assist scheduling and decision-making for performance of preventive maintenance for a nuclear power plant. The tool is based on data on failure rates, repair times, repair costs and indirect economic costs and utilizes probabilistic judgement and inference rules.

The category of buildings, for which reliability evaluation is of "critical" importance, such as hospitals, have had various isolated reliability approaches targeted at different parts/aspects of BMS [36]. However, we have not discovered an integral solution that targets the reliability of BMS as a whole.

As a further requirement, future reliability solutions for BMS have to be scalable and flexible, as the speed with which new technologies are emerging simply demands this as a basic condition for any reliability approach to be sustainable. If this condition is not fulfilled, reliability approaches would quickly become obsolete as BMS get updated, or they will be tightly linked to specific buildings. Therefore, a robust and scalable framework for reliability assessment of BMS is paramount.

IV. IMPLICATIONS

As of currently, there is no such thing as a general "design for reliability" approach to building management systems. This, however, will need to change, as the pressure towards energy performance will come at a price for reliability if reliability is not assessed timely and accurately, and included among the objectives while designing building management systems. Therefore, we can foresee a new trend emerging along the lines of "design for reliability" for BMS. It will definitely inject balance in addressing the energy consumption concerns, as well as have an impact on the occupant comfort metrics.

The accurate evaluation of reliability of BMS on its own would provide extra benefits for different purposes, such as:

- assisting component purchase decisions, or
- generation of optimal preventive maintenance schedules,

Both of these actions can actually further help in both cutting down maintenance cost, increasing occupant comfort and decreasing energy consumption.

The availability and growth of the Internet of Things platform invites for and enables development of a systematic approach towards reliability. This can be especially enhanced with new and advanced data-based approaches that could streamline reliability evaluation processes and provide less dependence on expert knowledge and higher accuracy. The convenience of the availability of data has to be utilized to enhance reliability of BMS, and CPS, in a more general view.

V. SUMMARY AND CONCLUSIONS

The goal of this paper is to raise the importance of addressing reliability of CPS. Due to our research focus being smart buildings, we have paid special attention to BMS. Reliability needs to be one of the objectives when BMS are being designed, and this is not the case now, as it is seen as a very complex/less-relevant issue. Nonetheless, a systematic approach to assessing reliability is more than necessary, and we would like to call for "design for reliability" in smart buildings, especially for the two categories that have not yet received adequate attention, i.e. "necessary" and "critical" buildings, as previously defined. We believe that all categories of buildings can utilize and benefit from the methods and findings that have already been developed for the "highly critical" BMS, generalized and further matched to satisfy reliability goals for corresponding buildings' category.

Conclusively, a systematic approach for reliability evaluation of BMS is the way to go, especially with the emergence of new data infrastructure technologies, such as the Internet of Things, to support and enable it. Therefore, we see this systematic reliability approach to BMS as both a necessity and a convenience.

ACKNOWLEDGMENT

This work is supported by the Innovation Fund Denmark for the project COORDICY.

REFERENCES

[1] X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin, "Smart community: an internet of things application," *IEEE Communications Magazine,* vol. 49, pp. 68-75, 2011.

[2] J. C. Knight, "Safety critical systems: challenges and directions," in *Software Engineering, 2002. ICSE 2002. Proceedings of the 24rd International Conference on*, 2002, pp. 547-550.

[3] E. A. Lee, "Computing foundations and practice for cyber-physical systems: A preliminary report," *University of California, Berkeley, Tech. Rep. UCB/EECS-2007-72,* 2007.

[4] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for securing cyber physical systems," in *Workshop on future directions in cyber-physical systems security*, 2009, p. 5.
[5] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control,* vol. 58, pp. 2715-2729, 2013.
[6] M. Trapp, D. Schneider, and P. Liggesmeyer, "A safety roadmap to cyber-physical systems," in *Perspectives on the future of software engineering*, ed: Springer, 2013, pp. 81-94.
[7] R. Yan, S. J. Dunnett, and L. M. Jackson, "Reliability modelling of automated guided vehicles by fault tree analysis," 2016.
[8] E. Ruijters and M. Stoelinga, "Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools," *Computer science review,* vol. 15, pp. 29-62, 2015.
[9] (2015, January 5). *Diagnostic Tool to Identify Building Issues*. Available: http://www.buildings.com/news/industry-news/articleid/19435/title/diagnostic-tool-to-identify-building-issues.aspx
[10] B. Schroeder and G. A. Gibson, "Disk failures in the real world: What does an mttf of 1, 000, 000 hours mean to you?," in *FAST*, 2007, pp. 1-16.
[11] H. Sun and J. J. Han, "The failure of MTTF in availability evaluation," in *Reliability and Maintainability Symposium, 2002. Proceedings. Annual*, 2002, pp. 279-284.
[12] S. Distefano and K. S. Trivedi, "Non-Markovian State-Space Models in Dependability Evaluation," *Quality and Reliability Engineering International,* vol. 29, pp. 225-239, 2013.
[13] D. Ge and Y. Yang, "Reliability analysis of non-repairable systems modeled by dynamic fault trees with priority AND gates," *Applied Stochastic Models in Business and Industry,* vol. 31, pp. 809-822, 2015.
[14] S. Lazarova-Molnar and G. Horton, "Proxel-based simulation for fault tree analysis," in *17. Symposium Simulationstechnik (ASIM 2003)*, Erlangen, Germany, 2003.
[15] R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: the next computing revolution," in *Proceedings of the 47th Design Automation Conference*, 2010, pp. 731-736.
[16] E. A. Lee, "Cyber physical systems: Design challenges," in *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, 2008, pp. 363-369.
[17] J. Al-Jaroodi, N. Mohamed, I. Jawhar, and S. Lazarova-Molnar, "Software Engineering Issues for Cyber-Physical Systems," in *Smart Computing (SMARTCOMP), 2016 IEEE International Conference on*, 2016, pp. 1-6.
[18] S. Nannapaneni, S. Mahadevan, S. Pradhan, and A. Dubey, "Towards Reliability-based decision making in Cyber-Physical Systems," presented at the IEEE International Conference on Smart Computing (SMARTCOMP), .
[19] L. L. Wu. (2011). *Improving system reliability for cyber-physical systems*. Available: http://academiccommons.columbia.edu/catalog/ac:146625
[20] R. Baheti and H. Gill, "Cyber-physical systems," *The impact of control technology,* vol. 12, pp. 161-166, 2011.
[21] C. S. Group, "Cyber-physical systems executive summary," *CPS Summit,* 2008.
[22] E. M. Clarke, B. Krogh, A. Platzer, and R. Rajkumar, "Analysis and verification challenges for cyber-physical transportation systems," 2008.
[23] A. Faza, S. Sedigh, and B. McMillin, "Integrated cyber-physical fault injection for reliability analysis of the smart grid," in *International Conference on Computer Safety, Reliability, and Security*, 2010, pp. 277-290.
[24] C. Singh and A. Sprintson, "Reliability assurance of cyber-physical power systems," in *IEEE PES General Meeting*, 2010, pp. 1-6.
[25] J. VOAS and R. Chillarege, "Reliability of Embedded and Cyber-Physical Systems," *IEEE Security and Privacy,* pp. 12-13, 2012.
[26] L. Sha and J. Meseguer, "Design of complex cyber physical systems with formalized architectural patterns," in *Software-Intensive Systems and New Computing Paradigms*, ed: Springer, 2008, pp. 92-100.
[27] H. J. La and S. D. Kim, "A service-based approach to designing cyber physical systems," in *Computer and Information Science (ICIS), 2010 IEEE/ACIS 9th International Conference on*, 2010, pp. 895-900.
[28] A. Rashid, W. Joosen, and S. Foley, "Security and resilience of cyber-physical infrastructures: Proceedings of the First International Workshop held on 06 April 2016 in conjunction with the International Symposium on Engineering Secure Software and Systems, London, UK," 2016.
[29] M. Steger, M. Karner, J. Hillebrand, W. Rom, and K. Rýmer, "A security metric for structured security analysis of cyber-physical systems supporting SAE J3061," in *Modelling, Analysis, and Control of Complex CPS (CPS Data), 2016 2nd International Workshop on*, 2016, pp. 1-6.
[30] V. Izosimov, A. Asvestopoulos, and O. Blomkvist, "Security-aware development of cyber-physical systems illustrated with automotive case study," in *2016 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2016, pp. 818-821.
[31] A. Bécue, N. Cuppens-Boulahia, F. Cuppens, S. Katsikas, and C. Lambrinoudakis, *Security of Industrial Control Systems and Cyber Physical Systems: First Workshop, CyberICS 2015 and First Workshop, WOS-CPS 2015 Vienna, Austria, September 21–22, 2015 Revised Selected Papers* vol. 9588: Springer, 2016.
[32] S. Barnum, S. Sastry, and J. A. Stankovic, "Roundtable: Reliability of embedded and cyber-physical systems," *IEEE Security & Privacy,* vol. 5, pp. 27-32, 2010.
[33] P. Zhao, S. Suryanarayanan, and M. G. Simoes, "An energy management system for building structures using a multi-agent decision-making control methodology," *IEEE Transactions on Industry Applications,* vol. 49, pp. 322-330, 2013.
[34] P. V. Paulo, F. Branco, and J. de Brito, "BuildingsLife: a building management system," *Structure and Infrastructure Engineering,* vol. 10, pp. 388-397, 2014.
[35] S. Lazarova-Molnar, M. B. Kjærgaard, H. R. Shaker, and B. N. Jørgensen, "Commercial Buildings Energy Performance within Context - Occupants in Spotlight," in *SMARTGREENS*, 2015, pp. 306-312.
[36] I. M. Shohet, "Building evaluation methodology for setting maintenance priorities in hospital buildings," *Construction Management and Economics,* vol. 21, pp. 681-692, 2003.
[37] H. Doukas, K. D. Patlitzianas, K. Iatropoulos, and J. Psarras, "Intelligent building energy management system using rule sets," *Building and environment,* vol. 42, pp. 3562-3569, 2007.
[38] E. M. Smith, D. R. Sewell, and P. T. Golden, "System and method for energy management," ed: Google Patents, 2004.
[39] L. Peruzzi, F. Salata, A. de Lieto Vollaro, and R. de Lieto Vollaro, "The reliability of technological systems with high energy efficiency in residential buildings," *Energy and Buildings,* vol. 68, pp. 19-24, 2014.
[40] F. Salata, A. de Lieto Vollaro, and A. Ferraro, "An economic perspective on the reliability of lighting systems in building with highly efficient energy: A case study," *Energy Conversion and Management,* vol. 84, pp. 623-632, 2014.
[41] T. Nikolaou, D. Kolokotsa, and G. Stavrakakis, "Review on methodologies for energy benchmarking, rating and classification of buildings," *Advances in Building Energy Research,* vol. 5, pp. 53-70, 2011.
[42] Y. Zou, "Classification of buildings with regard to airtightness," 2010.
[43] A. Di Bella, P. Fausti, F. Scamoni, and S. Secchi, "Italian experiences on acoustic classification of buildings," in *Proceedings of Inter Noise*, 2012, pp. 19-22.
[44] S. Lazarova-Molnar and N. Mohamed, "Challenges in the Data Collection for Diagnostics of Smart Buildings," in *Information Science and Applications (ICISA) 2016*, Ho Chi Minh City, Vietnam, 2016, pp. 941-951.
[45] S. Lazarova-Molnar, H. R. Shaker, and N. Mohamed, "Fault detection and diagnosis for smart buildings: State of the art, trends and challenges," in *2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*, Muscat, Oman, 2016, pp. 1-7.
[46] N. Mohamed, S. Lazarova-Molnar, and J. Al-Jaroodi, "CE-BEMS: A cloud-enabled building energy management system," in *2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*, 2016, pp. 1-6.
[47] A. K. Verma, S. Ajit, and D. R. Karanki, "Reliability of Complex Systems," in *Reliability and Safety Engineering*, ed: Springer, 2016, pp. 123-159.
[48] S. Arueti and D. Okrent, "A knowledge-based prototype for optimization of preventive maintenance scheduling," *Reliability Engineering & System Safety,* vol. 30, pp. 93-114, 1990.