A Generic Approach for Capturing Reliability in Medical Cyber-Physical Systems

Argyro Mavrogiorgou[1], Athanasios Kiourtis[1], and Dimosthenis Kyriazis[1]

[1] University of Piraeus, Department of Digital Systems, Piraeus, Greece
{margy,kiourtis,dimos}@unipi.gr

Abstract. Cyber-physical systems (CPSs) are slowly emerging to dominate our world through their tight integration between the computational and physical components. While the reliability evaluation of physical systems is well-studied, the one referring to CPSs is difficult due to the fact that software systems do not degrade, as they follow a well-defined failure model like in physical systems. Henceforth, a great attention has been given to tackle the challenge of reliability in CPSs, especially in the field of Medical CPSs (MCPSs) that are being considered as a powerful candidate for healthcare applications. This paper proposes a generic approach for effectively measuring reliability in MCPSs, taking into consideration the multiple MCPSs' applications that exist. The proposed approach captures the MCPS's reliability by initially modelling its components, accompanied with the selection of the evaluation environment, which is finally being followed by the failure analysis, and the reliability estimation, which are necessary for deciding whether a MCPS is considered as reliable or not.

Keywords: Cyber-physical systems, Medical cyber-physical systems, Reliability.

1 Introduction

Cyber-Physical Systems (CPSs) are attracting a lot of attention in recent years and are being considered as an emerging key research area, where according to [1], CPS market is globally expected to drive growth through 2027, whilst it is listed as the number one research priority by the US President's Council of Advisors on Science and Technology [2]. A CPS is able to combine computation and communication capabilities with the physical world, meaning that it can control the physical world as well as the connections between objects. Therefore, a CPS is a concept that seeks to converge with the cyber world composed of various physical systems [3], while using a distributed software that implements smart algorithms in order to control these entities. CPSs are able to add smart mechanisms to fully automate manufacturing processes, manage and enhance the operations and safety of environments and infrastructures, enhance energy consumption in smart buildings, or improve healthcare for patients, among others [4][5].

However, the development of such complex systems that are composed of many distributed and heterogeneous components interacting in various ways and capabilities, is extremely difficult [4]. CPSs, 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. Due to device proliferation and large-scale connectivity, a variety of functionalities are now feasible in CPSs. Connectivity however, also means that CPSs function in unreliable open environments, where due to the fact that the software gets further coupled with hardware and users, reliability evaluation becomes a significant challenge [6]. Henceforth, a great attention has been given in particular to tackle this challenge, confronting system reliability as a fundamental requirement of CPSs.

This requirement becomes extremely important to the healthcare domain [7], where CPSs are being considered as a powerful candidate for healthcare applications including in-hospital and in-home patient care [8]. In fact, a separate class of CPSs, namely Medical Cyber Physical Systems (MCPSs) are recognized in the literature [9][10], as interconnected, intelligent systems of medical devices that support a holistic treatment of a patient. For example, in the context of a hospital, the ones that were previously used as stand-alone medical devices are now being designed with embedded software, and integrated with network interfaces [11][12]. These network interfaces are used to communicate with other devices during patient treatments as well as monitoring, and healthcare systems [13]. Hence, CPSs constitute a technological chance for new applications in healthcare assuring more advanced care and treatment of patients.

However, the development of a systematic reliability analysis of CPSs, especially in the healthcare domain, has not received an adequate consideration. To address this challenge, in this paper a generic approach is proposed that can be used to effectively measure the reliability in MCPSs. This approach captures a general MCPS's reliability following four (4) sequential steps. Initially, the modelling of the MCPS's components takes place, whilst afterwards, the selection of the evaluation environment occurs, followed by the failure analysis, and the reliability estimation that are necessary for finally deciding whether the MCPS is being considered as reliable or not.

The rest of this paper is organized as follows. Section 2 describes the study of the state of the art regarding MCPSs and their applications, while the challenges of the MCPSs are being analysed, citing a more detailed view of the reliability challenge. Section 3 describes the proposed approach for measuring reliability in MCPSs, while Section 4 is addressing the future challenges, analyzing our conclusions and plans.

2 Related Work

2.1 Medical CPS

The term "Cyber-Physical System" was created a few years ago. The concept had existed for several decades, as the Computer Science and Engineering community has been dealing with it by calling CPSs as "real-time computing systems" or "embedded computing systems" [14]. However, the last few years, those terms have been replaced by the official name of "Cyber-Physical Systems", suggesting that these systems

provide the people with much more properties and functionalities. In particular, the definition from Cyber-Physical Systems Week [15] refers to the CPSs as "complex engineering systems that rely on the integration of physical, computation, and communication processes to function". In more details, CPSs refer to the integration of computation with physical processes (i.e. they are about intersection, not the union of the physical and the cyber [16][17]). In that case, embedded computers and networks monitor and/or control the physical processes based upon local and remote computational models, usually with feedback loops, where physical processes affect computations and vice versa [18][19][20]. In other words, CPSs are specialized computing systems that interact with control or management objects, integrating computing, communication, and data storage with real world's objects and physical processes, in a real-time, safe, secure, as well as efficient manner [21][22].

CPSs are being applied in many domains [23][17][24], however those in the healthcare domain in particular, are among the most remarkable ones. More specifically, in this domain a separate class of CPSs exists, namely Medical Cyber Physical Systems (MCPSs) [10][17], that are being considered as interconnected, intelligent systems of medical devices that support a holistic treatment of a patient. The inherent feature of MCPSs is a conjunction of embedded software control of networked medical devices with complex safety that always have to match the needs of the patients [25]. Hence, MCPSs are context-aware, life-critical systems with patient safety as the main concern, demanding rigorous processes for validation to guarantee user requirement compliance and specification-oriented correctness [26]. For that reason, medical devices and systems must be dynamically reconfigured, distributed, and interact with patients and caregivers in complex environments. For example, devices such as infusion pumps for sedation, ventilators and oxygen delivery systems for respiration support, as well as a variety of sensors for monitoring patients' conditions are used in many operating rooms. Often, these devices must be assembled into a new system configuration to match specific patient or procedural needs. The challenge is to develop systems and control methodologies for designing and operating these systems that are certifiable, safe, secure, and reliable [27].

Consequently, CPSs' research is revealing numerous opportunities and challenges in the healthcare domain, aiming to transform the delivery of health care by enabling smart medical treatments and services [28]. Some examples of these include intelligent operating rooms and hospitals, image-guided surgery and therapy, fluid flow control for medicine and biological assays, sensors in home for detecting changing health conditions, new operating systems for making personalized medical devices interoperable, and the development of physical and neural prostheses [28][29]. Other opportunities of utilizing CPSs in healthcare include the introduction of coordinated interoperation of autonomous and adaptive devices, as well as new concepts for managing and operating medical physical systems using computation and control, miniaturized implantable smart devices, body area networks, programmable materials, and new fabrication approaches [30].

2.2 Applications of Medical CPS

The research on CPSs in healthcare is still in its early stages. Although many CPSs' architectures have been proposed in the literature, the number of CPSs' architectures

proposed for healthcare applications is very low. However, various research efforts have been conducted on developing CPSs for healthcare applications, based on integrating sensor and cyber infrastructures, and focusing mainly in the areas of the patients' daily living, monitoring, as well as medication intake.

Concerning the patients' daily living applications and their medication intake, the authors in [31] proposed the Ambient-Intelligence Compliant Objects (AICOs) that exist in a virtual layer overlaid by ordinary household objects integrated by various multimodal and unobtrusive wireless sensors, so as to represent one or more activities of a person. In the same concept, the authors in [32] presented the Wireless Identification and Sensing Platform (WISP) that utilizes the enhanced passive Radio Frequency Identification (RFID) tags with sensors so as to facilitate the data communication from sensor to receiver. The authors in [33] proposed the iCabiNET, a system that utilizes smart RFID packaging. Being capable of recording the removal of a pill by breaking an electric flow into the RFID circuit, using either residential network at home or smart appliances. In the same notion, the authors in [34] presented the iPackage, an intelligent packaging prototype that consists of remote medication intake and vital signs monitoring. Moreover, in [35] the LiveNet is presented, which is a real-time distributed mobile platform for monitoring the activities of Parkinson's disease and epilepsy patients. What is more, the authors in [36] proposed a system that detects fall by using an accelerometer on the head level and identify the fall via an algorithm. Finally, the authors in [37] proposed the HipGuard, which is a posture analysis application used for detecting the posture for the recovery period of eight to twelve weeks after hip replacement surgery, by integrating seven sensors positioned in specific locations near surgery.

Concerning the patients' monitoring, the authors in [38] proposed the MobiHealth, a system that gathers data from the wearable sensor devices that the patients carry all day, collecting audio and video signals to provide early response in case of accidents. Furthermore, in [39] the CyPhyS+ system is presented, a comprehensive, low-cost and standards' compliant CPS, based on the concept of Internet of Things (IoT) for remote health monitoring of elderly, while in [25] a dependable MCPS for telecare of pregnant women at home has been presented. Moreover, the authors in [40] presented the Mobile ECG system that uses smart phones as base station for electrocardiography (ECG) measurement and analysis, forwarding the received data to the medical professionals. The authors in [41] presented the CodeBlue, a platform that consists of biomedical sensors (e.g. pulse oximeter, motion sensor), aiming to manage the communication among these devices. Finally, in the same concept, the authors in [42] proposed the AlarmNet, a wireless biosensor network system prototype, consisting of heart rate, pulse rate, oxygen saturation, and ECG system, that is able to monitor all the patients' measurements, and provide a graphical user interface to assist healthcare professionals to monitor the vital signs of their patients.

2.3 Reliability in Medical CPS

Due to the importance of MCPSs' applications and the complexity of their development process, huge research efforts have been started on different CPSs' challenges [4][30][43]. However, a great attention has been given in particular to the reliability

challenge, confronting system reliability as a fundamental requirement of MCPS. More particularly, 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 the aggregation of the reliability of each of their components [6]. Reliability may be measured in different ways depending on the particular situation [44][45], and can be estimated using either a qualitative or a quantitative method. To accurately describe quantitatively the concept of reliability it is essential to define the notions of fault, failure and error, as all of them are highly related to the concept of reliability [20]. However, some systems' reliability cannot be estimated quantitatively due to various reasons (e.g. lack of failure data), and therefore qualitative methods may be applicable.

Reliability has been recognized as a critical requirement for CPSs. In [17] it is pointed out that CPSs will not be deployed into mission critical applications as traffic control, automotive safety, and health care without improved reliability. An unreliable system may lead to disruption of service, financial cost and even loss of human life [46][47][48]. For that reason, the demand for reliability in CPSs, and especially in MCPSs, has constantly been increased. If demands for reliability are not addressed effectively, further deployment of MCPSs will be slowed down in applications [17][18]. Therefore, the reliability analysis for MCPSs is very challenging, and for that reason a lot of effort has been put into the research area in order to cope with this challenge. More particularly, in [49] a hybrid method that uses fault-tolerant structures with formal verification is proposed. The presented architecture supports the design of reliable CPSs. Another example of such efforts is presented in [50] that describes a service-oriented CPS with a service-oriented architecture and a mobile Internet device [6]. What is more, the authors in [51] developed a reliability model where Markov models are constructed for each component, in order to estimate the reliability of an Integrated Modular Avionics (IMA) system. In the same concept, in [52] a Markov Imbedded System (MIS) is used in order to model dependence between components in a smart power grid. Additionally, in [53] a phased-mission system model, which consists of Markov models for individual components and a binary decision diagram is proposed, so as to analyze the reliability of a fuel management system in an aircraft. Furthermore, the authors in [54] developed a reliability framework through a weighted reliability metric, using individual components' reliabilities and the performance metric of the CPSs considering their services, cyber security, resilience, elasticity, as well as vulnerability. Moreover, the authors in [55] presented the Failure Analysis and Reliability Estimation (FARE), a data-driven approach for reliability evaluation using historical data, accelerated life testing data, and real-world data.

Therefore, it becomes clear that the reliability of CPSs has received great attention in different applications. However, all of the aforementioned researches, do not highlight the complete reliability of the existing systems, which is crucial for any CPS in the healthcare domain. Moreover, most of these approaches are giving specific solutions to problems of a particular domain, arising the need of a holistic approach. Especially in MCPSs a little work has been done, even though this field seems to be of extremely importance, taking into consideration that the MCPSs are expected to be safe and reliable even in changing environments and unforeseen conditions [56]. For that reason, in this paper an approach is being presented that constitutes a generic approach for effectively measuring the reliability in MCPSs. More specifically, this approach

provides a set of methods and metrics on failure analysis, as well as reliability estimation for capturing MCPSs' reliability. Therefore, the proposed approach includes a more general and accurate representation of MCPSs' reliability, measuring various metrics for estimating systems' reliability, as well as offering a holistic system representation that covers the different MCPSs' applications that exist. It is worth mentioning that the proposed approach is extensible for accommodating new reliability measurement techniques and metrics. It does not only provide a retrospect evaluation and estimation of the MCPSs' system reliability using past data, but also provides a mechanism for continuous monitoring and evaluation of MCPSs' reliability for runtime enhancement.

3 Proposed Approach

Our approach proposes a generic way for effectively measuring the reliability in MCPSs. More specifically, the proposed approach consists of four (4) different stages: (i) the CPS modelling, (ii) the evaluation environment, (iii) the failure analysis, and (iv) the reliability estimation, as depicted in Fig. 1.

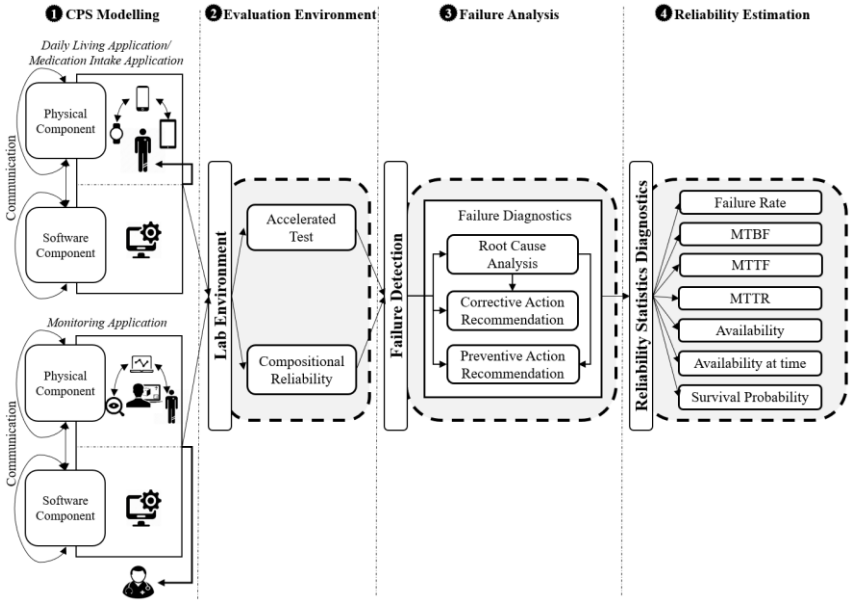

Fig. 1. Proposed approach architecture

CPS Modelling. In this stage of the proposed approach, the modelling of the MCPS's components takes place, using a specific domain modelling language [57] to capture the component-component interactions, whilst taking into consideration the different applications that the MCPSs may be implemented. In more details, the specific MCPS whose reliability is going to be examined, may have been used for daily living applications, or for patients' monitoring, or for medication intake of patients. As depicted in Fig. 1, the MCPS always consists of the physical or hardware components

(i.e. physical part), the cyber or software components (i.e. cyber part), and the communication between them. However, each one of them is differentiating according to the three (3) aforementioned situations of usage of the MCPS.

Regarding the patients' daily living applications and their medication intake, as for the physical part, in both situations this is comprised of a set of networked diverse medical devices (MDs) including biomedical sensors and actuators. The latter are used either for monitoring different patients' measurements (e.g. a smart watch for measuring patients' daily steps) or for capturing whether a patient has taken her medication or not (e.g. an electronic monitoring device for measuring medication adherence). Regarding the cyber part, this is responsible for the control and the management of these MDs, the processing of the acquired biosignals, as well as the invocation of the smart alarms that go back to the patient herself.

Regarding the patients' monitoring, as for the physical part, this is comprised of a set of MDs including biomedical sensors and actuators. The latter are being used, as in the previous scenario, for monitoring different patients' measurements (e.g. a smart watch for measuring patients' daily steps) as well as for in-home monitoring systems. Concerning the cyber part, this is responsible for the control and the management of these MDs, in combination with the monitoring system, the processing of the acquired biosignals, the invocation of smart alarms, and the communication with the surveillance center, whose outputs are finally sent back to the caregiver.

Henceforth, all of the aforementioned are considered as potential applications of MCPSs, being feasible to be modelled through a model-based analysis framework. In this framework, the MCPS that is being used is being modeled in a domain specific modelling language [57] in which each system-level function is associated to the corresponding component(s) through functional decomposition and component association. It should be noted, that in this stage, it is considered that there are used only MCPS of known nature (i.e. their architecture is known).

Evaluation Environment. In this stage, after the MCPS's modelling, the selection of the evaluation environment takes place. As it can be observed in Fig. 1, there exist various different evaluation environments where the failure data (i.e. either MCPS does not provide correct solutions or MCPS provides correct solution, but not within the expected time) will be collected, and the reliability tests will be implemented. This collection is being implemented regardless of the situation that the MCPS has been used for, as all of the possible existing situations are being constituted of the general concept that covers the MCPSs. In more details, the MCPS's model is sent to the lab environment, as medical systems need to be properly tested for reliability prior to their use in the medical operations. To this end, two (2) different types of tests may occur in the lab environment. In the first case, accelerated tests [58] can be applied based on a life test that simulates the actual running environment. More specifically, these tests include the Highly Accelerated Life Test (HALT) in a normal pace, which is similar to the stress test that creates a situation such that failure is more likely to happen. It is a method based on physics of failure, an approach for reliability assessment based on modelling and simulation that relies on understanding the physical processes contributing to the appearance of the failures [59]. However, in some cases the accelerated tests are not applicable in a lab environment, thus the second type of test can be applied. This type, is being based upon the components' reliability data (i.e.

compositional reliability) that can be used to construct the whole MCPS's reliability. Although there are many ways to do the compositional reliability [60], it should be noted that these estimates are not often indicative or accurate for representing the whole system reliability, mainly due to the communication failure that is often not easy to be incorporated in these models [61].

Failure Analysis. After the selection of the most suitable case for the lab environment in order to perform the evaluation, the failure analysis stage occurs, which includes the failure detection and diagnostics, along with domain knowledge and heuristics. In general, the operation of a CPS can be divided into three (3) possible scenarios: (i) the CPS provides the correct solution, within the expected time, (ii) the CPS does not provide correct solution (i.e. incorrect solution or no solution at all), and (iii) the CPS provides the correct solution, but not within the expected time. The last two cases are considered as system-level failure cases of a CPS and are being taken into consideration in our proposed approach. In more details, regarding the failure detection, this can be used as a proxy to a system's failure (e.g. an out of range measurement), whilst it might be induced by the external environment, a human mistake or an internal system fault [62][63].

As for the failure diagnostics, these are responsible for processing the detected failure data using [64]:

(i) the root cause analysis that is used to classify the failure type, analyze its nature and mechanism,
(ii) the corrective action recommendation that is used to correct the current failure and avoid future recurrence of the same type of failure,
(iii) the preventive action recommendation that is used to prevent occurrence of a certain potential failure before it happens.

Reliability Estimation. In the final stage of the proposed approach, after ingesting the failure detection and diagnostics data, the estimation of the MCPS's reliability takes place. More particularly, as mentioned in Section 2.3, reliability can be estimated using either a qualitative or a quantitative method. In our approach, we primarily examined and used quantitative methods for MCPSs' reliability estimation, implementing some commonly used reliability metrics [55]:

- *Failure Rate*: It is defined as the total number of failures within an item population, divided by the total time expended by that population, during a particular measurement interval under stated conditions
- *Mean Time Between Failures (MTBF)*: It is the mean expected time between system failures, in terms of the predicted elapsed time between inherent failures of a system during operation.
- *Mean Time To Failure (MTTF)*: It is sometimes used instead of MTBF in cases where a system is replaced after a failure.
- *Mean Time To Repair (MTTR)*: It is the mean time required to repair a failed component or device.
- *Availability* or *Mission Capable Rate*: It is the proportion of time that a system is in a functioning condition.
- *Power-on hours (POH)*: It is the length of time (in hours), during which electrical

power is applied to a device.

- *Availability at time*: It is the probability that the system is able to function on a specific pre-defined time.
- *Survival Probability*: It is the probability that the system does not fail in a time interval (0; t].

Consequently, in order to calculate the reliability of the chosen MCPS in terms of whether it is considered as reliable or not, a pre-defined threshold level is being set for each different reliability metric. Afterwards, the results of each metric are being aggregated, calculating the average value of the pre-defined metrics, and finally deciding whether the MCPS is considered as reliable or not.

4 Conclusions

In this paper, we have raised the importance of addressing reliability of CPSs, by deeply studying the challenging topic of MCPSs' reliability. We have considered all the possible existing applications of MCPSs whose architecture is known in advance, and proposed a generic approach for effectively capturing the reliability metrics of MCPSs so as to calculate the degree of the MCPSs' reliability. In this approach four (4) sequential steps were implemented, beginning from the modelling of the MCPS's components, followed by the selection of the evaluation environment, the failure analysis, and finally, the reliability estimation.

Currently, we are working on the evaluation of the developed approach, by testing it with multiple existing MCPSs in the lab environment. Our future work includes the development of a mechanism that does not require prior knowledge of the used MCPS's architecture. Furthermore, one of our main goals is to extend the existing approach by including more measuring metrics concerning the failure analysis, as well as the reliability estimation. Finally, we are willing to implement a visualization module providing the final results of the approach, enabling the users to observe the reliability results of each MCPS.

Acknowledgements. The authors would like to acknowledge the financial support from the "Hellenic Foundation for Research & Innovations (HFRI)".

References

1. Cyber-physical Systems Market Globally Expected to Drive Growth through 2027, http://www.findmarketresearch.org/2018/02/cyber-physical-systems-market-globally-expected-to-drive-growth-through-2027/
2. J. Wang, H. Abid, S. Lee, L. Shu, and F. Xia, "A secured health care application architecture for cyber-physical systems," Control Engineering and Applied Informatics, vol. 13, no. 3, pp. 101–108, 2011.
3. Seo, A., Jeong, J., & Kim, Y. (2017). Cyber Physical Systems for User Reliability Measurements in a Sharing Economy Environment. Sensors, 17(8), 1868.

4. Mohamed, N., Al-Jaroodi, J., Lazarova-Molnar, S., & Jawhar, I. (2016, December). Middleware to support cyber-physical systems. In Performance Computing and Communications Conference (IPCCC), 2016 IEEE 35th International (pp. 1-3). IEEE.
5. J. Al-Jaroodi et al., "Software Engineering Issues for Cyber-Physical Systems", IEEE SMARTCOMP, 2016.
6. Lazarova-Molnar, S., Shaker, H. R., & Mohamed, N. (2016, December). Reliability of cyber physical systems with focus on building management systems. In Performance Computing and Communications Conference (IPCCC), 2016 IEEE 35th International (pp. 1-6). IEEE.
7. Fda approves world's smallest pacemaker that attaches directly to heart, http://www.foxnews.com/health/2016/04/07/fda-approves-worldssmallest-pacemaker-that-attaches-directly-to-heart.html
8. A. Milenkovi´c, C. Otto, and E. Jovanov, "Wireless sensor networks for personal health monitoring: issues and an implementation," Computer Communications, vol. 29, no. 13-14, pp. 2521–2533, 2006.
9. Lee, I., & Sokolsky, O. (2010, June). Medical cyber physical systems. In Design Automation Conference (DAC), 2010 47th ACM/IEEE (pp. 743-748). IEEE.
10. I. Lee, O. Sokolsky, et al. (2012), Challenges and Research Directions in Medical Cyber-Physical Systems, Proc. of the IEEE, vol 100, no1.
11. King, A. L., Feng, L., Sokolsky, O., & Lee, I. (2013, August). Assuring the safety of on-demand medical cyber-physical systems. In Cyber-Physical Systems, Networks, and Applications (CPSNA), 2013 IEEE 1st International Conference on (pp. 1-6). IEEE.
12. Sokolsky, O., Lee, I., & Heimdahl, M. (2011, October). Challenges in the regulatory approval of medical cyber-physical systems. In Proceedings of the ninth ACM international conference on Embedded software (pp. 227-232). ACM.
13. Grispos, G., Glisson, W. B., & Choo, K. K. R. (2017, July). Medical Cyber-Physical Systems Development: A Forensics-Driven Approach. In Connected Health: Applications, Systems and Engineering Technologies (CHASE), 2017 IEEE/ACM International Conference on (pp. 108-113). IEEE.
14. Kim, K. H. (2010, July). Challenges and future directions of cyber-physical system software. In Computer Software and Applications Conference (COMPSAC), 2010 IEEE 34th Annual (pp. 10-13). IEEE.
15. Cyber-Physical Systems Week, http://www.cpsweek.org/
16. Lee, E.A. and Seshia, S.A. (2011). Introduction to embedded systems - a cyber-physical systems approach
17. Lee, E. A. (2008, May). Cyber physical systems: Design challenges. In Object oriented real-time distributed computing (isorc), 2008 11th IEEE international symposium on (pp. 363-369). IEEE.
18. C. S. Group, "Cyber-physical systems executive summary", CPS Summit, 2008.
19. Cyber-Physical Systems, http://cyberphysicalsystems.org/
20. Lee, E. A. (2007). Computing foundations and practice for cyber-physical systems: A preliminary report. University of California, Berkeley, Tech. Rep. UCB/EECS-2007-72.
21. Rajkumar, R. (2012). A cyber–physical future. Proceedings of the IEEE, 100(Special Centennial Issue), 1309-1312.
22. Skorobogatjko, A., Romanovs, A., & Kunicina, N. (2014). State of the Art in the Healthcare Cyber-physical Systems. Information Technology and Management Science, 17(1), 126-131.
23. NIST, Strategic R&D Opportunities for 21st Century Cyber-Physical Systems (2012), Foundations for Innovation in Cyber-Physical Systems Workshop, US.

24. Nannapaneni, S., Mahadevan, S., Pradhan, S., & Dubey, A. (2016, May). Towards reliability-based decision making in cyber-physical systems. In Smart Computing (SMARTCOMP), 2016 IEEE International Conference on (pp. 1-6). IEEE.
25. Pawlak, A., Jezewski, J., & Horoba, K. (2015). Dependable Medical Cyber-Physical System for Home Telecare of High-Risk Pregnancy. ADA USER, 36(4), 254.
26. Silva, L. C., Almeida, H. O., Perkusich, A., & Perkusich, M. (2015). A model-based approach to support validation of medical cyber-physical systems. Sensors, 15(11), 27625-27670.
27. National Aeronautics Research and Development Plan, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/aero-rdplan-2010.pdf
28. Cyber-Physical Systems: Enabling a Smart and Connective World, http://www.nsf.gov/news/special_reports/cyber-physical/
29. Nasser Al-Mhiqani, Mohammed & Ahmad, Rabiah & Hameed, Karrar & Salih Ali, Nabeel. (2017). Investigation study of Cyber-Physical Systems: Characteristics, application domains, and security challenges. Journal of Engineering and Applied Sciences. 12.
30. Haque, S. A., Aziz, S. M., & Rahman, M. (2014). Review of cyber-physical system in healthcare. International Journal of Distributed Sensor Networks, 10(4), 217415.
31. Lu, C. H., & Fu, L. C. (2009). Robust location-aware activity recognition using wireless sensor network in an attentive home. IEEE Transactions on Automation Science and Engineering, 6(4), 598-609.
32. Philipose, M., Smith, J. R., Jiang, B., Mamishev, A., Roy, S., & Sundara-Rajan, K. (2005). Battery-free wireless identification and sensing. IEEE Pervasive computing, 4(1), 37-45.
33. Lopez-Nores, M., Pazos-Arias, J. J., Garcia-Duque, J., & Blanco-Fernandez, Y. (2008, January). Monitoring medicine intake in the networked home: The iCabiNET solution. In Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008. Second International Conference on (pp. 116-117). IEEE.
34. Pang, Z., Chen, Q., & Zheng, L. (2009, November). A pervasive and preventive healthcare solution for medication noncompliance and daily monitoring. In Applied Sciences in Biomedical and Communication Technologies, 2009. ISABEL 2009. 2nd International Symposium on (pp. 1-6). IEEE.
35. Sung, M., Marci, C., & Pentland, A. (2005). Wearable feedback systems for rehabilitation. Journal of neuroengineering and rehabilitation, 2(1), 17.
36. Wang, C. C., Chiang, C. Y., Lin, P. Y., Chou, Y. C., Kuo, I. T., Huang, C. N., & Chan, C. T. (2008, May). Development of a fall detecting system for the elderly residents. In Bioinformatics and Biomedical Engineering, 2008. ICBBE 2008. The 2nd International Conference on (pp. 1359-1362). IEEE.
37. Iso-Ketola, P., Karinsalo, T., & Vanhala, J. (2008, January). HipGuard: A wearable measurement system for patients recovering from a hip operation. In Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008. Second International Conference on (pp. 196-199). IEEE.
38. Konstantas, D., & Herzog, R. (2003, September). Continuous monitoring of vital constants for mobile users: the MobiHealth approach. In Engineering in Medicine and Biology Society, 2003. Proceedings of the 25th Annual International Conference of the IEEE (Vol. 4, pp. 3728-3731). IEEE.
39. Dagale, H., Anand, S. V. R., Hegde, M., Purohit, N., Supreeth, M. K., Gill, G. S., ... & Surya, P. (2015, June). Cyphys+: A reliable and managed cyber-physical system for old-age home healthcare over a 6lowpan using wearable motes. In Services Computing (SCC), 2015 IEEE International Conference on (pp. 309-316). IEEE.

40. Kailanto, H., Hyvarinen, E., & Hyttinen, J. (2008, January). Mobile ECG measurement and analysis system using mobile phone as the base station. In Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008. Second International Conference on (pp. 12-14). IEEE.
41. Shnayder, V., Chen, B. R., Lorincz, K., Fulford-Jones, T. R., & Welsh, M. (2005). Sensor networks for medical care.
42. Wood, A. D., Stankovic, J. A., Virone, G., Selavo, L., He, Z., Cao, Q., ... & Stoleru, R. (2008). Context-aware wireless sensor networks for assisted living and residential monitoring. IEEE network, 22(4).
43. Key Design Drivers and Quality Attributes, http://www.informit.com/articles/article.aspx?p=2756464&seqNum=3
44. Thomas, M. O., & Rad, B. B. (2017). Reliability Evaluation Metrics for Internet of Things, Car Tracking System: A Review.
45. M. Rausand and A. Høyland. System Reliability Theory: Models, Statistical Methods, and Applications. Wiley, 2nd edition, December 2003.
46. Wu, L. L. (2011). Improving system reliability for cyber-physical systems. Technical reports. http://hdl. handle. net/10022/AC: P: 13134.
47. Baheti, R., & Gill, H. (2011). Cyber-physical systems. The impact of control technology, 12, 161-166.
48. VOAS, J., & Chillarege, R. (2012). Reliability of Embedded and Cyber-Physical Systems. IEEE Security and Privacy, 12-13.
49. Sha, L., & Meseguer, J. (2008). Design of complex cyber physical systems with formalized architectural patterns. In Software-Intensive Systems and New Computing Paradigms (pp. 92-100). Springer, Berlin, Heidelberg.
50. La, H. J., & Kim, S. D. (2010, August). A service-based approach to designing cyber physical systems. In Computer and Information Science (ICIS), 2010 IEEE/ACIS 9th International Conference on (pp. 895-900). IEEE.
51. Wu, Z., Huang, N., Zheng, X., & Li, X. (2014, June). Cyber-physical avionics systems and its reliability evaluation. In Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2014 IEEE 4th Annual International Conference on (pp. 429-433). IEEE.
52. Marashi, K., & Sarvestani, S. S. (2014, January). Towards comprehensive modeling of reliability for smart grids: Requirements and challenges. In High-Assurance Systems Engineering (HASE), 2014 IEEE 15th International Symposium on (pp. 105-112). IEEE.
53. Sun, X., Huang, N., Wang, B., & Zhou, J. (2014, June). Reliability of cyber physical systems assessment of the aircraft fuel management system. In Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2014 IEEE 4th Annual International Conference on (pp. 424-428). IEEE.
54. Li, Z., & Kang, R. (2015, December). Strategy for reliability testing and evaluation of cyber physical systems. In Industrial Engineering and Engineering Management (IEEM), 2015 IEEE International Conference on (pp. 1001-1006). IEEE.
55. L. Wu, G. Kaiser, "FARE: A framework for benchmarking reliability of cyber-physical systems", IEEE Conference on Systems Applications and Technology Conference(LISAT), pp. 1-6, 2013.
56. N. H. C. Software and S. C. Group. High-confidence medical devices: Cyber-physical systems for 21st century health care. technical report. http://www.nitrd.gov/about/meddevice-final1- web.pdf.

57. Pradhan, S. M., Dubey, A., Gokhale, A., & Lehofer, M. (2015, October). Chariot: A domain specific language for extensible cyber-physical systems. In Proceedings of the workshop on domain-specific modeling (pp. 9-16). ACM.
58. Meeker, W. Q., & Escobar, L. A. (2014). Statistical methods for reliability data. John Wiley & Sons.
59. Matic, Z., & Sruk, V. (2008, June). The physics-of-failure approach in reliability engineering. In Information Technology Interfaces, 2008. ITI 2008. 30th International Conference on (pp. 745-750). IEEE.
60. Glaß, M., Yu, H., Reimann, F., & Teich, J. (2012, September). Cross-Level compositional reliability analysis for embedded systems. In International Conference on Computer Safety, Reliability, and Security (pp. 111-124). Springer, Berlin, Heidelberg.
61. He, W., Liu, X., Zheng, L., & Yang, H. (2010, June). Reliability calculus: A theoretical framework to analyze communication reliability. In Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on (pp. 159-168). IEEE.
62. American Society for Quality, http://asq.org/learn-about-quality/process-analysis-tools/overview/fmea.html
63. Phan-Ba, M. D. N. (2015). A literature review of failure detection (Doctoral dissertation, UNIVERSITY OF BRITISH COLUMBIA (Vancouver).
64. Croskerry, P. (2005). Diagnostic failure: a cognitive and affective approach.