Internet of Medical Things: A Review of Recent Contributions Dealing with Cyber-Physical Systems in Medicine

Arthur Gatouillat, Youakim Badr, Bertrand Massot, Ervin Sejdić

Internet of Medical Things: A Review of Recent Contributions Dealing with Cyber-Physical Systems in Medicine

Arthur Gatouillat, Youakim Badr, Bertrand Massot, and Ervin Sejdić, *Senior Member, IEEE*

***Abstract*—The Internet of Medical Things designates the interconnection of communication-enabled medical-grade devices and their integration to wider-scale health networks in order to improve patients' health. However, because of the critical nature of health-related systems, the Internet of Medical Things still faces numerous challenges, more particularly in terms of reliability, safety and security. In this paper, we present a comprehensive literature review of recent contributions focused on improving the Internet of Medical Things through the use of formal methodologies provided by the cyber-physical systems community. We describe the practical application of the democratization of medical devices for both patients and health-care providers. We also identify unexplored research directions and potential trends to solve uncharted research problems.**

***Index Terms*—cyber-physical systems, wearable devices, health informatics, Internet of medical things**

I. Introduction

The health industry is changing drastically in developed countries as the life expectancy has abruptly raised during the 20th century [1]. Chronic diseases are also increasingly pressuring these countries' healthcare systems [2]. Indeed, the life expectancy in developed countries has been raised by about 30 years during the 20th century. As a result, the population of older adults has rapidly increased [1]. Additionally, the escalation of chronic diseases have pressured healthcare systems around the world due to the lack of resources [2].

Major challenges arise from the increase of chronic diseases and aging population, as healthcare systems have to handle a wide variety of diseases and treatments, but also an increasing number of patients. In order to avoid overloads of healthcare infrastructures and to reduce healthcare-costs, in-home telemedicine systems have been proven to be efficient solutions [3].

However, telemedicine systems are extremely heterogeneous, and are also generally designed to answer a single therapeutic goal, such as remote cardiac monitoring, stroke rehabilitation [4], etc. This characteristic of telemedicine systems makes them efficient in reducing costs and healthcare infrastructure overload, but represents a drawback as the number of patients and variety of diseases increase. The need for better genericity and scalability can be tackled by the Internet of Medical Things (IoMT).

Indeed, the IoMT combines both the reliability and safety of traditional medical devices and dynamicity, genericity and scalability capabilities of traditional Internet of Things (IoT). It has the capability to solve the problem of ageing and chronic diseases by being able to manage numerous devices deployed for numerous patients, in addition to being generic enough to deal-with a variety of diseases calling for very heterogeneous monitoring and actuation requirements. Moreover, IoMT also provides a solution to additional challenges such as patients mobility (i.e. the pervasive monitoring of patients in their daily lives, in opposition to telemedicine systems, which are heavily focused on home-care).

Despite the challenging nature of these issues, new technological solutions for demanding healthcare systems in developed countries are changing the way we deliver healthcare. The proliferation of personal computing devices, along with gains in computational power in these devices, are enabling the development of the Internet of Medical Things (IoMT) and offering solutions to address the needs of both our aging population and patients with chronic diseases. The IoMT is the interconnection between not only numerous personal medical devices but also between devices and health care providers such as hospitals, medical researchers or private companies. The advent of the IoMT is mainly caused by increase in use and development of connected and distributed medical devices is bringing both promising potential applications and numerous challenges [5]. Because personal medical devices often come as wearable devices, we will focus on the integration of wearable medical devices to the IoMT. Due to the strict ethical requirements of the medical community, biomedical devices need to address the following concerns:

- *Reliability*: a reliable system must achieve its functional goals at all times, meaning it should not be prone to unexpected failure under normal operating conditions. The potential diagnostic nature of IoMT-based systems mandates reliability of every system component in order to guarantee the correctness of collected information.
- *Safety*: a safe system must not cause harm to its operating environment. In the context of IoMT, especially in the context of medical actuators, one must be able to prove that the system will not cause harm to its user.
- *Security*: medical systems must be robust to external threats and attacks because of the sensitive and personal information they collect.

A. Gatouillat and Y. Badr are with Univ Lyon, INSA Lyon, LIRIS, UMR5205, F-69621, France

B. Massot is with Univ Lyon, INSA Lyon, INL, UMR5270, F-69621, France

E. Sejdić is with the Department of Electrical and Computer Engineering, Swanson School of Engineering, University of Pittsburgh, Pittsburgh, PA, USA.

Corresponding author: Ervin Sejdić, esejdic@ieee.org

The definitive article was published in: A. Gatouillat, Y. Badr, B. Massot and E. Sejdić, "Internet of Medical Things: A Review of Recent Contributions Dealing With Cyber-Physical Systems in Medicine," in *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3810-3822, Oct. 2018, https://doi.org/10.1109/JIOT.2018.2849014

Because the IoMT is defined as the interconnection of medical-grade devices with broader healthcare infrastructures, requirements from lower layers of the IoMT (i.e., connected medical devices), must be transfered to higher layers of the IoMT (e.g. the communication and application layers). Additional requirements are also brought by the interconnectivity of medical devices, such as collected data processing and security, data access policy or data lifecycle management policy. As in the traditional IoT, devices of the IoMT are extremely heterogeneous in terms of computing capabilities, communication protocols or application fields. Devices of the IoMT are also numerous, and IoMT systems must be able to appropriately manage this mass of devices. The IoMT thus shares requirements with the traditional IoT, especially in terms of the management of a large amount of devices, reliable communication, or device heterogeneity and interoperability.

To achieve all these requirements for IoMT, they need to be considered from the beginning of the design process, and with the growing complexity of computing systems, this can be achieved using a set of methods and design philosophy typically used for cyber-physical systems (CPS). CPS are the combination of computational matters to physical processes through a theory designed to efficiently construct large scale computer controlled systems [6], [7]. Using this computing abstraction, various potential medical applications can be envisioned such as highly-reliable biomedical devices, assisted living or telemedicine [7].

In particular, medical CPS provide comprehensive modeling and design frameworks for the creation of reliable and safe medical devices. Reliability and safety can both be studied under physical and digital perspectives thanks to the combination of physical models and computational models. Medical CPS thus provide a comprehensive solution to the IoMT. Indeed, physical modeling is needed for the device layer of the IoMT, as IoMT devices are in constant interaction with the physical world. Communication and application layers of the IoMT can then make use of discrete models to ensure deterministic behavior under various operating conditions. Consequently, IoMT devices are seen as networked medical CPS making use of hybrid models to provide cross-layer reliability and safety guarantees.

Another critical aspect of IoMT devices are when they are used for physiological functions regulation. In such use-cases, physiological functions of patients are modified through actuators based on control inputs and a set of relevant physiological measurements. Typical examples of medical actuators are insulin pumps or chemotherapy infusion apparatuses, which modify levels of insulin or chemotherapy drug in the body. A comprehensive understanding of the underlying physiological processes are necessary in order to build optimal command laws of such devices. Medical CPS provide a good theoretical and modeling framework for such devices, as hybrid models can be used to represent the physiological process and the numerical control command. In addition, discrete networking models can be added to such devices in order to facilitate their integration into wider-scale IoMT systems.

This review is organized as follows. Section II introduces the challenges and design strategies of IoMT in addition to how CPS can address these issues. Section III then analyzes the IoMT under a CPS approach by adopting a layered strategy: the IoMT devices, the networking of devices, and eventually the use of a service oriented approach to build IoMT systems. Finally, section IV identifies key research directions to simultaneously achieve cross-layer safety, reliability and security.

II. IoMT Generalities

The IoMT is a complex field of study presenting various challenges. In this section, we will first introduce the main challenges of the IoMT. Then, design solutions providing partial solutions to improve the safety, reliability and security of the IoMT are discussed. Eventually, we introduce the CPS approach in an IoMT context, and demonstrate it is a solution of choice to challenges of the IoMT.

A. Challenges of the IoMT

Embedded systems are used in various environments to realize a variety of heterogeneous applications: telemedicine; traffic control; assisted living; or smart cities [8], [7]. In these applications, digital systems (also called cyber-systems) are controlling physical objects, resulting in a constant interaction between the digital and physical world [8].

However, the critical aspects of these applications, especially when embedded systems are considered, raise challenges that can be classified into three categories [9]:

- These systems must comply to *reliability*, *robustness* and *security* requirements. Because of the unstable nature of the physical and physiological world, IoMT-based systems must not only be able to sustain acceptable performance under such changes, but also react correctly if deemed necessary. Such IoMT systems also raise security concerns because they often regulate situations where system failure could potentially be life threatening. Therefore, these systems must be able to resist various criminal attacks [10], [11].
- The IoMT must rely on *accurate models* of *hybrid systems*. They exist at the intersection of the digital and the physical world, thus needing both accurate physical models and precise computing abstractions. Moreover, relying on a model-based design enables the improvement of the testing procedures through simulation.
- There must be specific *verification* and *validation* mechanisms: the majority of the IoMT is bound to be widely distributed and in order to pass certifications, they must include verification and validation protocols on different levels of granularity.

These challenges are cross-disciplinary and are gathering scientists from diverse fields: from advanced control theory to computer science, along with electronics engineering, power electronics or signal processing. This mandates the development of models of *hybrid systems*, where both digital and physical components are represented along with their interactions. Finally, to facilitate the certification process and improve the system reliability, *verification* and *validation* procedures must be specified at different scales: from the narrowest level IoMT device scale to the widest level scale of the entire IoMT.

A virtual example of an IoMT-based system would be an Internet operated surgical robot, where surgeons can connect to tele-operate. For evident reasons, *reliability*, *robustness*, and *security* questions are immediately raised for such applications. Moreover, in order to improve the safety of the surgery, accurate models of both the human body and the robot characteristics must be developed. Modeling both of these aspects enables prompt detection and accurate correction of unexpected behaviors. In the case of developing a connected surgical robot, verification and validation procedures will greatly assist the strict certification procedure associated with the development and commercialization of medical devices.

Even though these problems are still both active research directions and partially unanswered, a design methodology for IoMT devices and IoMT-based systems has been developed and partially satisfies requirements in terms of safety, reliability, and security.

B. IoMT Design

In order to efficiently solve the reliability, robustness, security, modeling, verification and validation challenges of IoMT, design methods have been described in the literature. A synthesis of contributions dealing with each of the identified challenges of the IoMT is given in Table I.

TABLE I
FIELD-OF-INTEREST DRIVEN CATEGORIZATION OF REFERENCES

Subject		Reference Index
Modeling	Biological process	[12] [13] [14] [15] [16]
	Computing systems	[17] [18] [19] [20]
	Hybrid systems	[17] [21] [22] [23]
Robustness and security		[24] [25] [26] [27] [28] [29] [30] [31]
Verification and Validation		[32] [33] [34] [35] [36] [37]

1) Model-Based Development of the IoMT: The most explored IoMT-related challenge is the problem raised by the modeling of CPS [38]. As defined in the introduction, the IoMT can be seen at the interconnection of medical CPS. Moreover, tools introduced by the CPS community provide modeling frameworks for both the physical and digital characteristics of medical CPS [20], [6]. Because comprehensive models of systems provide better reliability and safety, we included contributions dealing with all aspects of medical CPS, and more particularly, physiological modeling. Indeed, physiological modeling in a medical CPS context can easily be extended with networking digital models in order to integrate devices in the IoMT.

Abundant literature on the subject can be found, and a wide range of potential applications for the developed models were experimented on. Modeling of hybrid systems starts with a good understanding of basic continuous systems modeling [17], where differential equations are used to describe the dynamics of an evolving system. Then, the modeling framework could be extended to discrete-time systems using a state-machine descriptive approach [17]. This is the basis of all further improved models of continuous time, discrete time or hybrid systems.

Continuous time models have been developed for a wide variety of fields. However, because of the focus of this review, an emphasis on the models developed for the medical field was chosen. Biological processes are hard to model because of their apparent randomness and their inherent physiological properties, which rely on physics, bio-chemistry and a wide variety of other fields. However, models have been developed for very specific applications: fractal models can be used to model glucose dynamics for artificial pancreas applications [12] (illustrated in Figure 1); fractal models of the heart rhythm for implantable pacemaker applications [13]; node based models and geometrical models of the heart for cardiac devices [14]; or even full multi-parametric patient models, accounting for several bio-medical data such as blood pressure of body temperature [15]. Another biomedical example using continuous time differential equations can be found in fluid-filled catheters, which measure the pressure in internal organs [16]. These models are complex and their parameters must be determined through clinical experimentation.

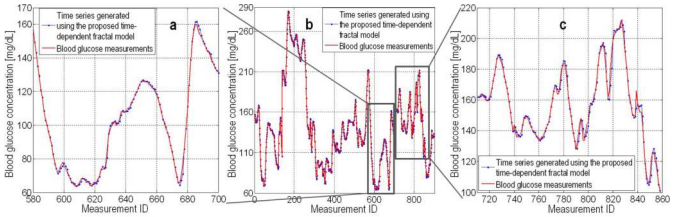

Fig. 1. Comparison of blood glucose measurements and blood glucose generated from a fractal model, from [12]. We thank IEEE for providing a permission to use this figure, which was originally published in M. Ghorbani and P. Bogdan, "A cyber-physical system approach to artificial pancreas design," *Proceedings of the 9th International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS)*, Montreal, QC, pp. 1–10, Nov. 2013.

The deep integration of computers in the IoMT mandates an accurate modeling of computing processes, enabling the improvement of IoMT predictability. Discrete time processes, thus computing processes, can be modeled using state machines [17]. Complementary to these state machine models, several modeling philosophies have been developed. For signal-processing oriented applications, one can use synchronous data flow to describe the computing processes of targeted applications [18]. This model uses directed graphs where nodes represent computing function and edges symbolize signal paths [18]. Rendezvous stochastic networks can be used for potential delays modeling in server-client architectures [19]. If the system is timed and presents discrete interactions between a set of actors, a discrete-event model can be used [20]. In these models, each interaction is represented as an event, and actors react to events in a temporal order [20]. Other modeling tools representing computer systems have been developed, but the true strength of CPS-based approaches to build the IoMT comes from the use of hybrid models, enabling the accurate modeling of both the computing world and the physical world.

Because of the strong relationship between the digital and physical world in the IoMT, one must rely on hybrid models that accurately represent both these worlds in order to achieve an efficient design process [39]. A possible way to describe

such models is the generalization of finite states machines with continuous inputs and outputs: the modal models [17], [21] (such models are illustrated in Figure 2).

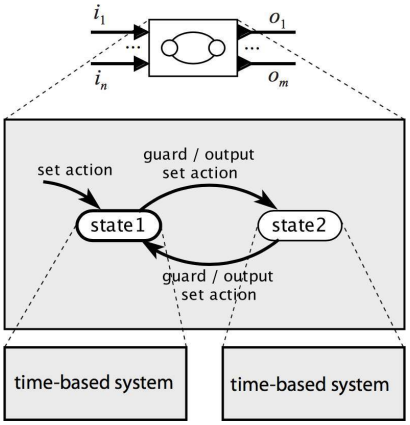

Fig. 2. Graphical representation of modal models, from [17]: *Introduction to Embedded Systems: A Cyber-Physical Approach, 1e*, by Edward Ashford Lee and Sanjit Arunkumar Seshia, published by The MIT Press. This figure has been reproduced with the kind permission of MIT Press.

Usually in these kinds of systems, the plant exists in a continuous state space, while the controller exists in a symbolic and discrete domain [23]. Other approaches, called complementary modeling, have also been studied [22]. This modeling philosophy is one of the roots of cyber-physical systems, but in order to be able to produce accurate hybrid models, one must understand both continuous time and computer system modeling.

2) Robustness and security design concerns: Because of the robustness, resilience (which refers to the capabilities of a system to resume its normal behavior after being subjected to abnormal circumstances) and security requirements of connected medical devices, such consideration must be considered as early as possible in the design process. In order to guarantee the robustness of the IoMT, several methods have been proposed in the literature. One of these methods is the inclusion of some control strategy during the system design process [26], where a stochastic approach to model both deterministic uncertainties and unexpected events is considered. Game-theoretical approaches or Markov processes modeling as described in [26] and in [24] can also be used in order to ensure the global robustness of the considered system. A more traditional controller switching approach was proposed in [25], where system metrics are used as indicators of its functional status, and where more robust but less precise controller can be deployed if the required functional properties are not verified.

Because of the abundance of literature dealing with IoMT security, we only selected papers with a focus on CPS security in a medical context. This problem is wide and covers several aspects: data privacy and aggregation [27], intrusion detection [28], alarm generation allowing non-interoperability detection [29], or integrity and authenticity [30]. To successfully assess all of these security attributes, different mechanisms have been used: cryptography (based on simple symmetric key [27] or a more evolved key system using physiological parameters of the human body [30]); a behavior rule based model, which can allow detecting intrusions when systems deviate from their expected behavior [28]; or the formulation of a set of requirements allowing the detection of interoperability problems [29]. All of these aspects can be combined to form general safety and security cyber-physical framework [31].

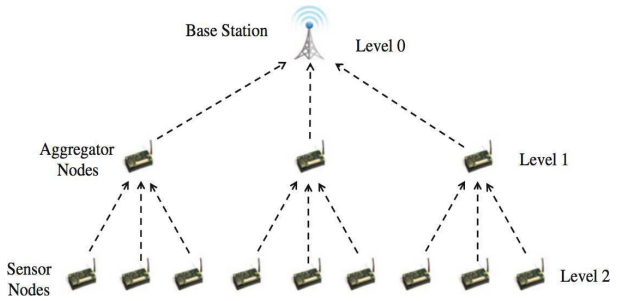

Fig. 3. Simple network model used in [27] to secure data transmission using cryptography. Reprinted by permission from Springer Customer Service Centre GmbH: Springer Nature and originally published in Parmar K., Jinwala D.C. (2015) Hybrid Secure Data Aggregation in Wireless Sensor Networks. In: Mousavi M., Berger C. (eds) *Cyber Physical Systems. Design, Modeling, and Evaluation. CyPhy 2015*. Lecture Notes in Computer Science, vol 9361. Springer, Cham, Copyright © 2015.

It is necessary to consider robustness and security requirements at the design time, because it allows designers of medical devices to provide guarantees related to these requirements. If such considerations are studied early in the design process, robustness and security testing can be deployed at each step of the design resulting in safe and robust medical devices.

3) Verification and Validation of IoMT: The last identified challenge when designing IoMT-based systems is the integration of a verification and validation process to the product development. Figure 4 describes the typical verification workflow using model checking techniques, where a set of system properties are checked against a formal system model in order to ensure correct global system behavior. The idea behind verification of the IoMT is the reachability analysis of the different states described in the hybrid model [32]. To perform verification of IoMT models, several tools and algorithms were developed for hybrid state machine models [32], [35] or for Petri net derived models [34]. Generic verification tools targeting distributed architecture were also developed [33]. However, when it comes to the validation part of the procedure, the literature is less developed. This also comes from the fact that while the verification process can be generalized to a wide range of IoMT-based systems aiming at very different fields of application, each of these fields has very specific validation requirements. Validation protocols and platforms have for instance, been developed for cardiac implantable devices [36] or industrial product lines [37].

Rigorous design methodologies allow the development of safe, secure, and robust CPS, which are compatible with the design of medical systems, where the same set of requirements are expected.

C. CPS as a comprehensive solution for IoMT requirements

Because of the intrinsic critical nature of medical systems, one must be particularly careful when designing them. Several

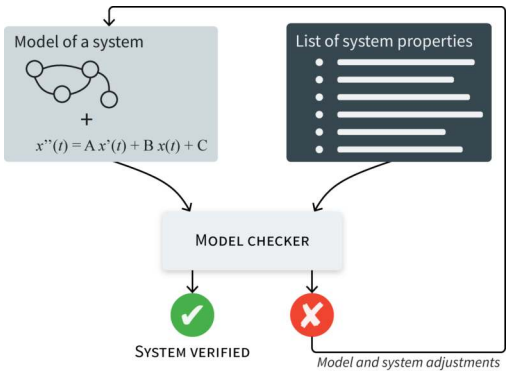

Fig. 4. Model checking based verification workflow

concerns regarding biomedical devices have been raised both by the medical and engineering communities. The main problem of medical systems, and of the IoMT, is the privacy and security of collected data [40], [41], [42]. The concern is greatly amplified when it comes to implantable medical devices because they usually assure vital function and any tampering could have disastrous consequences [43], [44]. Connectivity of devices composing the IoMT is also an issue, as exposure to the external world is a source of insecurity. On top of these security concerns comes robustness and reliability considerations: medical devices must present a deterministic behavior, even if placed under unanticipated conditions [40], [41]. This robustness must be both on the hardware side, where the system must be able to resist various hostile environments, and on the software side, where malfunctions should be minimized and handled appropriately [45]. Figure 5 gives a graphical representation of the degree of acceptability of potential device malfunction.

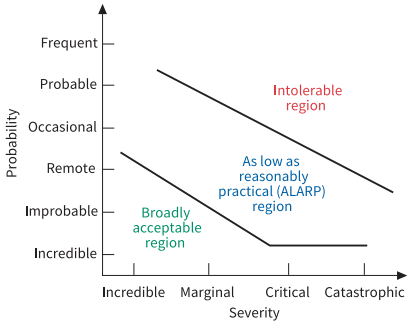

Fig. 5. Risk management policy graphical representation, from [45]. We thank IEEE for providing a permission to use this figure, which was originally published in R. Rakitin, "Coping with defective software in medical devices," in *Computer*, vol. 39, no. 4, pp. 40–45, April 2006.

Moreover, modern medical devices come with a lot of other requirements, such as performing real time data collection [40], [41]; improving networked infrastructures [41]; or accurately estimating computing processing required to analyze the collected data [40]. The extensive certification process associated with medical devices, such as the FDA [41], requires strong verification and validation procedures. It is also necessary to accurately capture user requirements of medical systems to ensure their adoption and correct use [46]. This can be realized through a careful validation process.

These difficult requirements can be fulfilled if the cyber-physical system design methodology is carefully followed. This methodology allows for the addressing of each medical system concern, from security to validation and verification through a careful modeling of the system and elaborate design procedures. Several examples of medical cyber-physical embedded systems will be detailed in the following section.

III. CPS as a Driver of the IoMT

In order to access the challenges and prospects of CPS in the context of IoMT, a layer-by-layer approach was preferred based on reviewed contributions. It was indeed noticed that papers in this area usually focus on either the device layer, the framework layer or the service layer. The device layer includes all the concerns regarding the design of IoMT devices. Because of strong hardware constraints of medical devices, such devices must be interconnected using low-energy protocols, and the global system behavior is delegated to other components. These components, which specify the global behavior of interconnected medical devices, are represented by the integration layer. Finally, another level of abstraction can be added, using a service oriented approach. A representation of the layers described herein above is given in Figure 6.

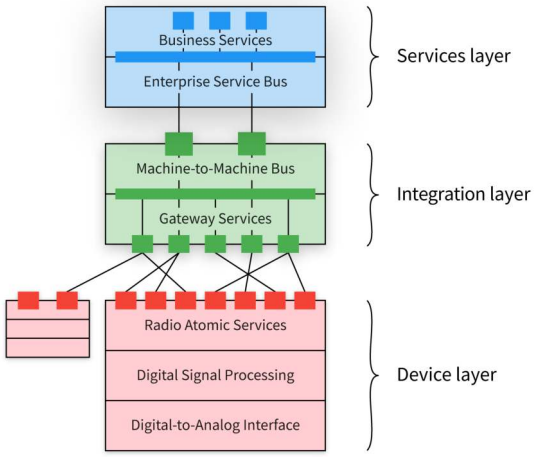

Fig. 6. Multi-layer representation of the IoMT

In addition to the layer representation of the IoMT, Figure 7 provides insights on the constraint and advantages of using a CPS approach for each of the layers of the IoMT.

A. A CPS Approach for IoMT Devices

The focus was first drawn to papers describing wearable IoMT device design that utilize a cyber-physical approach. The definition of wearable devices that was used to identify these papers was voluntarily kept wide: from implantable medical devices, which are by definition invasive, to simple non-invasive wearable sensors. After carefully selecting papers of interest in this area, a classification according to answered IoMT challenges was realized, and it is given in Table II.

A wide variety of sensors and devices have been designed using the CPS approach: from external sensors to implantable

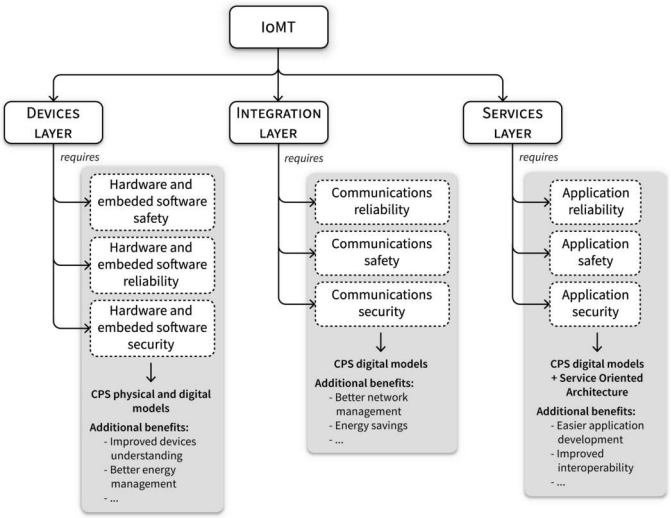

Fig. 7. Layer representation of constraints and advantages of the IoMT

devices controlling vital processes. For this variety of developed devices, all the key aspects of CPS were identified and dealt with: safety, security and robustness; the development of accurate models for both physiological processes and computing systems; and the implementation of some verification and validation procedures.

The first observation that can be drawn from the selected literature is that most of the papers deal with the development of models for IoMT devices. Our selection represents the whole range of modeling that has to be realized when designing cyber-physical systems. Indeed, papers focused on the development of models describing physiological (and thus continuous time) processes, such as the modeling of cardiac activity [13], [14]; models of the blood glucose rate for artificial pancreas design [12]; or the development of models describing the human body's absorption rate of a given medicine [47], [48]. Figure 8 exhibits a detailed example about how authors of [14] have used finite state automata to model the electrical behavior of the heart, intended for cardiac fault detection in implantable pacemakers.

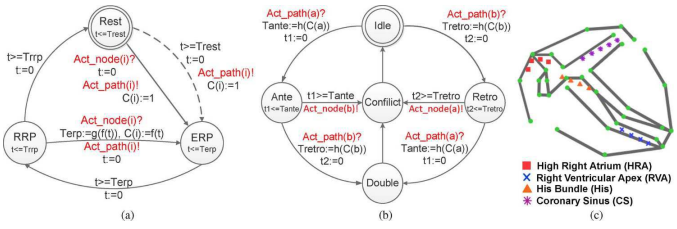

Fig. 8. Discrete models of continuous-time cardiac tissue electrical behavior, from [14]. We thank IEEE for providing a permission to use this figure, which was originally published in Z. Jiang, M. Pajic and R. Mangharam, "Cyber–Physical Modeling of Implantable Cardiac Medical Devices," in *Proceedings of the IEEE*, vol. 100, no. 1, pp. 122–137, Jan. 2012.

The particularity of these models is that they focus on a very specific physiological process, while keeping their practical implementation in consideration. More generic models have also been developed: a multiparametric fall detection model using electroencephalography and electromyography [49], an electromyography-based model of user intention for artificial legs [50]; general human body 3D model [51]; or even structured human interaction models to achieve better CPS reliability [52].

Models using the human body as a whole system have also been used to validate CPS [15], [53], i.e. to potentially detect sensor error based on elaborate models of the human physiology. Some papers make use of physiological modeling for computing-related purposes, such as electrocardiogram compression [54]. Computing system models have also been developed from CPS through the development of network on-chips [55]. Models of computing module temperature can ensure the safety of devices in contact with the skin [56], [30]. Such thermal model is displayed in Figure 9. Software architecture models in cyber-physical systems, where hardware abstractions are realized through the use of tasks, have also been developed [57]. Potential attack analysis models have also been described [58], along with model-based false alarm detection [59]. Verification and validation schemes through modeling were developed, with various targets: the validation of implantable medical devices [36], the verification of CPS using digital equivalents [60] and the generation of a model-based code and verification architecture [61]. Finally, models accounting for the CPS environment were investigated through the modeling of packet loss in a networked architecture dedicated to post-stroke gait rehabilitation [62]; through the modeling of the physical context in IoMT-based systems [63].

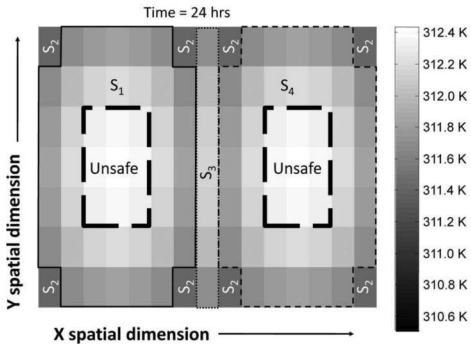

Fig. 9. Thermal map of skin temperature during sensor contact, from [30]. We thank IEEE for providing a permission to use this figure, which was originally published in A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee and S. K. S. Gupta, "Ensuring Safety, Security, and Sustainability of Mission-Critical Cyber-Physical Systems," in *Proceedings of the IEEE*, vol. 100, no. 1, pp. 283–299, Jan. 2012.

The robustness and security challenges have been described independently from the modeling perspective only once with the use of smart algorithm selection for biosignal acquisition robustness improvement [64]. Verification and validation have been considered separately from any modeling aspects in the very specific situation where an implementation already existed, with the real life testing of CPS devices such as an ECG sensor [65] or a general CPS hardware node [66].

The modeling part is the most frequently discussed challenge at the device-level in CPS literature (it is dealt with in 88 % of the selected papers). Following modeling, verification and validation is the next most problematic process, which is mentioned in 56 % of the selected literature. Finally comes

robustness and security, which is addressed in 16 % of the papers. This leaves potential improvement and points for research focused on the integration of the CPS security requirements at the device level.

In this section, we introduced a list of techniques and approaches that have been used to design safer, more reliable and more secure medical devices. Because such devices are the building blocks of the IoMT, and because IoMT applications tend to be highly critical (e.g., disease diagnosis, remote monitoring used to trigger urgent medical response), non-functional properties of such devices must be guaranteed and medical devices must be trustworthy. The predominant approach to improve devices non-functional characteristics is to use model-driven development to test the behavior of implemented devices against theoretical functional models. No clear modeling framework trend has been identified, partly because of the wide variety and heterogeneous nature of devices and biological processes that are modeled. The application of such methodologies to develop reliable, safe and secure medical devices is crucial, and is a required step before any higher level considerations.

B. IoMT Integration Frameworks for Wearable Devices

Our main topic of interest is medical wearable IoMT-based systems, and our review was focused on literature applying networked architectures for the integration of medical devices to the IoMT. To identify papers of interest in this section, the same methodology from the previous section was used, and results were displayed accordingly in Table III.

In the previous section, contributions mainly focused on the modeling strategies of IoMT-devices, while the robustness and validation concerns were clearly less developed. However, when it comes to the integration of IoMT devices, all the identified IoMT key research problems are studied more homogeneously.

The security and robustness of networked IoMT is the topic that is the most frequently dealt with independently of the two other challenges. Cyber-physical safety is critical because of the sensitive nature of IoMT-based devices and systems. In the medical case, because of the confidential nature of transmitted data over the network, one must ensure that adequate measures are taken to protect these data [30], [42]. Such security measures can include data encryption [31], user authentication [31], or resistance to denial-of-service attacks [31]. Detailed security frameworks to prevent attacks and to study the response of systems under these attacks have been developed [67], along with attack detection methods for networked IoMT [68]. The robustness of networks using several heterogeneous sensors has also been studied through the implementation of an interoperability analysis framework for IoMT [69]. Models have also been used for security purposes, allowing intrusion detection based on a derivation from the expected behavior [28].

Then, verification and validation of IoMT-based systems was also an independently considered subject. These papers mainly focused on the real life testing of networked IoMT devices, such as the field verification of a sensor networked using the 6LoWPAN protocol and aimed at the remote monitoring of elderly subjects [70], the experimental evaluation of the synchronization of two IoMT nodes [71], or the testing of Zigbee based networked sensor aiming to be integrated in a wider health structure for post-stroke rehabilitation [72].

Finally, the modeling of networked IoMT devices was considered in the following contexts: the development of a web-of-things (WoT) architecture for cyber-physical systems using widely used RESTful protocols [73], the study of a scenario and Internet-based CPS for assisted living with the minimization of response time [74], and finally the development of an event based model for networked IoMT devices [75]. Figure 10 illustrates how [73] networked cyber-physical systems can be architecturally modeled using a block-diagram syntax. This web-of-things approach uses popular Internet-based technologies, enabling better system interoperability.

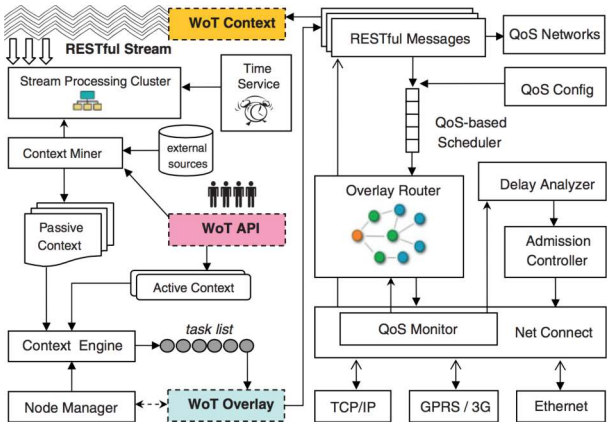

Fig. 10. Architecure of networked cyber-physical systems based on a web-of-things approach, from [73]. We thank John Wiley and Sons for providing a permission to use this figure, which was originally published in T. S. Dillon, H. Zhuge, C. Wu, J. Singh, and E. Chang, "Web-of-things framework for cyber–physical systems," *Concurrency and Computation: Practice and Experience*, vol. 23, no. 9, pp. 905–923, 2011.

The verification and validation of networked IoMT devices is the main point of focus in papers dealing with several research directions for the IoMT. The verification and validation process is most often coupled with a modeling problematic: models are used as a reference behavior and the real-life experimentation is then compared to this reference. Such approaches have been used to analyze cloud-based IoMT systems: it was explored for remote patient monitoring [76]; quality of data evaluation [77]; or even large scale health data collection [78]. This model-verification approach was used to build a test platform for body area networks (BAN) [79], but also for more general network topology. Indeed, fault models for binary sensor based networked IoMT were studied [80]. Special-need adults targeted IoMT-based systems [81] or pregnancy monitoring platforms [82] were also developed. Such methods have also been used to enable the successful operation of computer intensive tasks on resource limited networked node [83].

Verification and validation were also discussed in combination with robustness and security concerns. The robustness of IoMT systems has been explored for numerous applications, such as power optimization and packet scheduling mechanisms for BANs [84], the development of an analysis framework allowing the improvement of IoMT interoperability [29], and

TABLE II
SUMMARY OF THE DEVICES DESIGNED USING A CPS APPROACH

Reference	Rob. & Sec.	Modeling	V & V	Comments
[49]		★		Electroencephalography and electromyography fall risk model
[51]		★		3D human body model
[48]	★	★		Hybrid model & safety analysis for infusion pump
[47]		★		Insulin & chemotherapeutic infusion pump model
[55]		★	★	Designing and modeling NoC core for IoMT devices
[61]		★	★	Model based code generator & verification
[56]		★	★	Temperature of skin touching IoMT device modeling & ver.
[13]		★		Implantable cardiac device model
[52]	★	★		Robustness impr. w/ human interaction model
[12]		★		Artificial pancreas modeling
[59]		★		False alarm detection using modeling
[50]		★	★	User intention model and verification for artificial legs
[66]			★	Design, testing & validation of a IoMT hardware node
[60]		★	★	Modeling for IoMT verification
[54]		★		Embedded electrocardiogram compression using generative models
[36]		★	★	Platform to validate IoMT devices models
[64]	★			Biosignals acquisition using smart algorithm selection
[15]		★	★	The use of models to validate medical IoMT devices
[53]		★	★	— *Same as previous paper* —
[65]			★	Testing of an energy consumption adaptive electrocardiogram
[62]		★	★	Gait Rehabilitation IoMT platform modeling packet losses
[63]		★	★	Design framework for IoMT devices
[58]	★	★	★	Modeling and testing of IoMT devices security
[57]		★		Task model for IoMT devices
[14]		★	★	Cardiac implantable IoMT device modeling and verification

analysis of the robustness of a MAC protocol for networked devices [85]. Some global reliability and safety framework have also been developed [56]. Finally, a verification of a physiological parameter based key generation for encryption and data protection purposes has been discussed [86].

In summary, the integration of devices is largely studied from a networking perspective. Since the IoMT consists of networked connected medical devices, reliability, safety and security of networked connected devices must be carefully studied both at design time and at runtime. This is achieved once again through the wide use of model driven design and the use of formal validation and verification tools. Being able to provide a reliable networking framework for connected medical devices is important, as network failure or malicious intrusions could cause severe consequences. If the example of remote monitoring is considered, network failure could imply missing critical health events and cause serious problems for the monitored patient. However, the reliability of the target networks can be estimated using models and formal verification tools. The development of reliable and resilient networks is still an active research direction, and is enabling a more trustworthy IoMT.

C. IoMT Service Layer: an Unexplored Approach

The last layer considered in this survey is the service layer, where the IoMT is considered from a service oriented perspective. Similar research methodology that is used in the previous sections was applied to this case, and it was observed that the service oriented approach has been less studied than the devices and framework design using a CPS perspective. While 26 papers of interest were selected to illustrate both device and framework design using CPS, only 19 papers considered a service based approach of the IoMT.

The main concern of the literature using the service oriented approach to design the IoMT is the quality-of-service (QoS) requirements, techniques and models for such systems. The use of appropriate network controllers was described to guarantee the expected QoS in a wide scale IoMT, integrating both patient and clinician services [87]. For general cases, the QoS requirements of CPS was well-developed from different perspective: network QoS requirement for CPS [88]; QoS management architecture at both the CPS device and the CPS framework [89]; UML (unified modeling language) based QoS modeling for CPS [90]. Still on the question of quality-of-service management, middleware improving QoS by considering resource managers and network properties has been developed [91]; and a framework to guarantee appropriate QoS through radio resource management has been built [92].

Another important aspect of the service oriented approach is composition. This matter has been developed in the service oriented IoMT and solutions have been offered: a framework derived from the OWL-S (web ontology language for web services) ontology model was adapted to the IoMT, allowing efficient IoMT services composition [93]; traditional Java-based composition techniques were also adapted to CPS [94]; and finally framework allowing the self architectures of service oriented IoMT has been developed [95].

Some contributions have proposed a model based design process to successfully achieve the execution of service oriented cyber-physical systems: architecture analysis and design languages were used to model architectures in [96], along with an extension of the OWL-S allowing the enhancement of service based CPS models [97]. A three step service oriented cyber-

TABLE III
SUMMARY OF IOMT INTEGRATION FRAMEWORKS

Reference	Rob. & Sec.	Modeling	V & V	Comments
[56]	★		★	Analysis of BAN framework
[30]	★			Security requirements for networked IoMT devices
[70]			★	IoMT network field testing
[73]		★		WoT architecture and model for networked CPS
[31]	★			Security and Robustness framework for networked CPS
[84]	★		★	Robustness and verification framework for BAN
[71]			★	Verification of networked IoMT devices
[76]		★	★	Integration of cloud technology in the IoMT
[69]	★			Interoperability framework for the IoMT
[74]		★		Scenario based networked IoMT devices for assisted living
[72]			★	IoMT framework for post-stroke rehabilitation
[28]	★	★		Networked IoMT devices intrusion detection
[82]		★	★	IoMT requirements for pregnancy monitoring
[77]		★	★	Cloud based IoMT models and simulation
[67]	★			Security requirements of networked IoMT devices
[68]	★			Security requirements of networked sensors
[42]	★			Privacy and security requirements for the IoMT
[83]		★	★	Model based framework and simu. for networked CPS
[75]		★		Event based model for networked CPS
[29]	★		★	Interoperability of IoMT analysis and testing
[81]		★	★	Designing and testing of a networked CPS
[85]	★		★	Robustness verification of an IoMT MAC protocol
[86]	★		★	Physiological key agreement, verification
[79]		★	★	Packet loss models and test environment for BAN
[80]		★	★	Verification through simulation of sensor network
[78]		★	★	Big data and cloud based IoMT modeling and testing

physical system design process was also defined, along with a case study of the proposed design method [98]. This design method is introduced in Figure 11, and defines 6 methodological steps to enable service-oriented CPS.

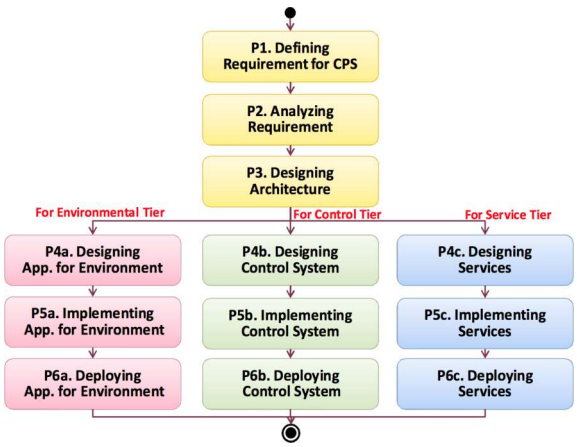

Fig. 11. Service-oriented design method for cyber-physical systems, from [98]. We thank IEEE for providing a permission to use this figure, which was originally published in H. J. La and S. D. Kim, "A Service-Based Approach to Designing Cyber Physical Systems," in *Proceedings of the IEEE/ACIS 9th International Conference on Computer and Information Science*, Yamagata, Japan, pp. 895–900, Sept. 2010.

Another topic of interest of the service based IoMT is the deployment of adequate middleware, which adds a level of abstraction to the control of devices by proposing a generic interface for the connected objects. Service oriented middleware architecture has been detailed, either using low level C structures [99] or higher level XML description targeted at objects integration to large scale IPv6 networks [100].

Papers also focused on less general aspects of service oriented computing, with a more application-targeted approach, such as the implementation of real time data collection services for networked sensors (with some focus on security and robustness aspects of the described system) [101], or the case study of the use of IEEE 802.15.4 protocol in CPS, and its impact on the systems' QoS [102].

Finally, cloud computing was also considered in an IoMT context, with the development of cloud and big-data services for telehealth applications [103], [78]. Data collection services aiming to be integrated into a cyber-physical cloud based system were also proposed [104].

For medical applications, a lack of contributions describing service oriented IoMT was observed. However, the concepts defined in service-oriented architectures, where modular, self-contained software components are combined to build bigger systems, are quite similar to the IoMT concerns. Indeed, in the IoMT, heterogeneous and self-contained medical devices must collaborate to achieve health-oriented functional goals. The similarities between the service-oriented computing characteristics and the IoMT architectural implementations makes the study of service oriented medical devices an interesting research direction. One of the main challenges of this direction is the integration of strong hardware constraints to services oriented architectures where contributions exclusively consider research problems from a pure software point of view.

IV. RESEARCH PERSPECTIVES AND DIRECTIONS

CPS covers a wide variety of fields of expertise, they are gathering researchers coming from various backgrounds.

Thanks to the literature gathered in this review paper, potential research directions and topics of interest have been identified.

First, an extension of service oriented computing applied to IoMT-based systems could lead to interesting medially oriented applications. Indeed, the service abstraction enables great modularity, interoperability and ease of use by third parties. The modularity of this approach is granted by service composition mechanisms, where several services are combined to form new composite services, and the interoperability is allowed by the use of service ontology and specification, where services are extensively described. Improving the high level abstraction for IoMT devices and systems could improve the reliability of devices integration, but also to build comprehensive and personalized medical solutions through services compositions.

Networked architectures, as described in the previous section, raise the question of machine-to-machine communication and standardization. To allow seamless communications between CPS devices, one must carefully study how these devices communicate using standard communication protocol such as 6LoWPAN [70], MAC [85] or IEEE 802.15.4 [102] in strict IoMT contexts and more generic CPS contexts. However, the machine-to-machine communication concern is wider than simple protocol matters. Indeed, machine-to-machine communications require the investigation of network architectures, heterogeneity, QoS or energy and resources management [105]. This approach has the potential to drastically improve the IoMT through a better understanding of networked systems' properties, behavior and handling. Moreover, standardization initiatives for machine-to-machine communications through organizations such as oneM2M [106] are emerging, and the use of the developed standards for the IoMT might help the improvement on the interoperability and ease of use of such systems. The oneM2M standardization initiative tackles the interoperability issue by providing a global application programming interface (API) with bindings to several traditional Internet protocols (namely HTTP, CoAP and MQTT protocols). This approach only focuses on providing interoperability at the application level, and acts as a generic middleware providing common device representation and access mechanisms.

While oneM2M provides a generic solution of connected object interoperability, other initiatives such as the MD PnP[1] [107] program or the MDCF[2] [108] framework target interoperability of medical systems, and can be potential fundamental building blocks of the IoMT. The MD PnP program aims at full medical devices interoperability by providing standard, open-source software and various use-cases: it was at the origin of the integrated clinical environment (ICE) standard and maintains OpenICE [109], an open-source implementation of this standard. This software provides bindings for medical devices based on the data distribution service (DDS) middleware, and a variety of typical clinical use-cases to facilitate real-world deployment. Devices interoperability in the MD PnP is based on an ad hoc approach where devices are integrated manually to the framework through software bindings. A different and complementary approach based on model-driven development is offered by the MDCF framework, where medical devices are modeled as communicating components. This framework is heavily software oriented and can be used to verify particular clinical scenarios based on medical devices communicating using a publish/subscribe approach. The interoperability issue is dealt with by the use of the Java messaging service (JMS) protocol for all system communications. While both initiatives provide encouraging insights on communicating medical devices interoperability, their scalability seems limited as they rely on the use of a specific protocol for cross-device communication. This limited scalability is hindering in an IoMT context where multiple application-specific protocols coexist because of hardware constraint (for instance, the use of energy-saving protocols might be preferred in order to extend the battery-life of constrained wearable medical devices). In conclusion, interoperability of the IoMT is still an ongoing research area, and IoMT systems designer must compromise between the use of unified and system-wide protocols and protocols heterogeneity brought by medical devices hardware constraints.

Finally, a wide range of medical monitoring devices have been developed, from gait multiparametric monitoring devices [110] to multi-purpose body sensor networks [111] and the review herein above leads to believe that such systems' reliability, safety, security of testing could be drastically improved with a cyber-physical approach. Indeed, using such an approach early in the system development process would ensure the quality, completeness and security of the gathered data, which is a capital requirement for medical devices.

It is however worth noticing that holistic full-stack approaches are lacking. Contributions often consider only one layer of the stacked architecture described in this review. Future research should focus on more transversal approaches, where all the layers are considered simultaneously to enable better cross-layer reliability. Indeed, since the goal of the IoMT is to enable better healthcare thanks to device interconnectivity and the use of Internet-based technologies, it is crucial that the robustness, safety and security requirements, which have been studied for each layer of the IoMT is preserved when the system is considered on a global perspective.

From a medical point of view, the birth of the IoMT represent an incredible field of opportunities for a wide variety of applications: from the early diagnosis of chronic diseases [112] to the remote monitoring of at risk patients to trigger urgent medical response if deemed necessary. However, to enable true pervasive healthcare applications through the IoMT, some research challenges must still be investigated. One particularly interesting research direction is the use of service oriented architectures to enable better modularity and interoperability of the IoMT.

From a patient perspective, pervasive healthcare has numerous advantages: comfort improvements thanks to remote monitoring and smaller devices, better self awareness of health status thanks to realtime feedback, or health improvements enabled by tailored recommendations based on patient history. The improvement of self health status awareness in patient with chronic and environment-influenced conditions has the potential to lead to better disease management thanks to

[1]MD PnP: Medical Devices Plug-and-Play

[2]Medical Devices Coordination Framework

lifestyle modification improved by the IoMT.

Yet another interesting research direction is the experimental medical validation of devices and infrastructures composing the IoMT. Indeed, if technologies developed for the IoMT are to be used in a medical context, it is necessary to be able to prove the reliability of the data collected by the system and the stability of the long term system behavior. In order to successfully explore this research direction, a multidisciplinary approach must be considered because of the intrinsic nature of the Internet of medical things. There is a clear lack of wide-scale studies concerned with the medical validation of medical devices. The modest accuracy in terms of heart rate measurements [113] or in terms of physical activity measurements [114] of popular wearable medical devices calls for further accuracy investigations of consumer oriented medical devices. In order to be clinically accepted, components of the IoMT must be studied considering a result accuracy perspective with wide scale and real life data collection and experiments.

In conclusion, Figure 12 gives a qualitative representation of how IoMT efforts evolved over time. Previous efforts were mainly focused on the development of reliable IoMT devices, while recent efforts focused on IoMT integration frameworks. Research in terms of IoMT frameworks is extremely active as new protocols and architectural styles are developed. Finally, service-oriented IoMT initiatives are only recent, but they provide encouraging insights in terms of interoperability, scalability and ease of development of IoMT systems.

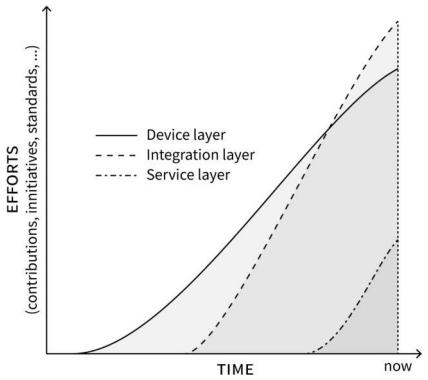

Fig. 12. Qualitative time and effort diagram

V. Conclusion

In this review, the field of IoMT-based systems and IoMT devices were studied from a multi-layer perspective. We demonstrated that the CPS approach enables a better control of not only system robustness, security, reliability, but also the verification and validation. Because these questions are crucial when designing biomedical systems, CPS is an appropriate design process for designing, implementing, testing and deploying such systems. A comprehensive list of the use of CPS approaches in the IoMT was given and discussed, and potential research directions for the IoMT were given.

Acknowledgments— This work was generously supported by a research grant from Région Auvergne-Rhône-Alpes.

References

[1] K. Christensen, G. Doblhammer, R. Rau, and J. W. Vaupel, "Ageing populations: the challenges ahead," *The Lancet*, vol. 374, no. 9696, pp. 1196–1208, 2009.

[2] D. Yach, C. Hawkes, C. L. Gould, and K. J. Hofman, "The global burden of chronic diseases: overcoming impediments to prevention and control," *Journal of the American Medical Association*, vol. 291, no. 21, pp. 2616–2622, 2004.

[3] A. Darkins, P. Ryan, R. Kobb, L. Foster, E. Edmonson, B. Wakefield, and A. E. Lancaster, "Care coordination/home telehealth: The systematic implementation of health informatics, home telehealth, and disease management to support the care of veteran patients with chronic conditions," *Telemedicine and e-Health*, vol. 14, no. 10, pp. 1118–1126, 2008.

[4] A. G. Ekeland, A. Bowes, and S. Flottorp, "Effectiveness of telemedicine: A systematic review of reviews," *International Journal of Medical Informatics*, vol. 79, no. 11, pp. 736–771, 2010.

[5] I. Lee and O. Sokolsky, "Medical cyber physical systems," in *Proceedings of the 47th Design Automation Conference*. ACM, 2010, pp. 743–748.

[6] W. Wolf, "Cyber-physical systems," *Computer*, no. 3, pp. 88–89, 2009.

[7] E. Lee *et al.*, "Cyber physical systems: Design challenges," in *11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing*. IEEE, 2008, pp. 363–369.

[8] E. A. Lee, "CPS foundations," in *Proceedings of the 47th Design Automation Conference*. ACM, 2010, pp. 737–742.

[9] 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*. ACM, 2010, pp. 731–736.

[10] 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.

[11] C. Neuman, "Challenges in security for cyber-physical systems," in *DHS: S&T workshop on future directions in cyber-physical systems security*, vol. 7, 2009.

[12] M. Ghorbani and P. Bogdan, "A cyber-physical system approach to artificial pancreas design," in *Proceedings of the 9th IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis*. IEEE Press, 2013, pp. 1–10.

[13] P. Bogdan, S. Jain, K. Goyal, and R. Marculescu, "Implantable pacemakers control and optimization via fractional calculus approaches: a cyber-physical systems perspective," in *Proceedings of the 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems*. IEEE Computer Society, 2012, pp. 23–32.

[14] Z. Jiang, M. Pajic, and R. Mangharam, "Cyber–physical modeling of implantable cardiac medical devices," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 122–137, 2012.

[15] L. C. Silva, M. Perkusich, F. M. Bublitz, H. O. Almeida, and A. Perkusich, "A model-based architecture for testing medical cyber-physical systems," in *Proceedings of the 29th Annual ACM Symposium on Applied Computing*. ACM, 2014, pp. 25–30.

[16] M. U. Sanwal and O. Hasan, "Formally analyzing continuous aspects of cyber-physical systems modeled by homogeneous linear differential equations," in *Cyber Physical Systems. Design, Modeling, and Evaluation*. Springer, 2015, pp. 132–146.

[17] E. A. Lee and S. A. Seshia, *Introduction to embedded systems: A cyber-physical systems approach*. Lee & Seshia, 2011.

[18] E. Lee and D. G. Messerschmitt, "Synchronous data flow," *Proceedings of the IEEE*, vol. 75, no. 9, pp. 1235–1245, 1987.

[19] C. M. Woodside, J. E. Neilson, D. C. Petriu, and S. Majumdar, "The stochastic rendezvous network model for performance of synchronous client-server-like distributed software," *IEEE Transactions on Computers*, vol. 44, no. 1, pp. 20–34, 1995.

[20] P. J. Ramadge and W. M. Wonham, "The control of discrete event systems," *Proceedings of the IEEE*, vol. 77, no. 1, pp. 81–98, 1989.

[21] E. A. Lee and H. Zheng, "Operational semantics of hybrid systems," in *Hybrid Systems: Computation and Control*. Springer, 2005, pp. 25–53.

[22] A. J. Van der Schaft and J. M. Schumacher, "Complementarity modeling of hybrid systems," *IEEE Transactions on Automatic Control*, vol. 43, no. 4, pp. 483–490, 1998.

[23] P. J. Antsaklis, J. A. Stiver, and M. Lemmon, "Hybrid system modeling and autonomous control systems," in *Hybrid Systems*. Springer, 1993, pp. 366–392.

[24] M. L. Bujorianu and N. Piterman, "A modelling framework for cyber-physical system resilience," in *Cyber Physical Systems. Design, Modeling, and Evaluation*. Springer, 2015, pp. 67–82.

[25] N. Kottenstette, G. Karsai, and J. Sztipanovits, "A passivity-based framework for resilient cyber physical systems," in *Proceedings of the 2nd International Symposium on Resilient Control Systems*. IEEE, 2009, pp. 43–50.

[26] Q. Zhu and T. Başar, "Robust and resilient control design for cyber-physical systems with an application to power systems," in *Proceedings of the 50th IEEE Conference on Decision and Control and European Control Conference*. IEEE, 2011, pp. 4066–4071.

[27] K. Parmar and D. C. Jinwala, "Hybrid secure data aggregation in wireless sensor networks," in *Cyber Physical Systems. Design, Modeling, and Evaluation*. Springer, 2015, pp. 116–131.

[28] R. Mitchell and I.-R. Chen, "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 16–30, 2015.

[29] K. K. Venkatasubramanian, E. Y. Vasserman, V. Sfyrla, O. Sokolsky, and I. Lee, "Requirement engineering for functional alarm system for interoperable medical devices," in *Computer Safety, Reliability, and Security*. Springer, 2015, pp. 252–266.

[30] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, "Ensuring safety, security, and sustainability of mission-critical cyber–physical systems," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 283–299, 2012.

[31] P. Dong, Y. Han, X. Guo, and F. Xie, "A security and safety framework for cyber physical system," in *7th Conference on Control and Automation*. IEEE, 2014, pp. 49–51.

[32] S. Schupp, E. Ábrahám, X. Chen, I. B. Makhlouf, G. Frehse, S. Sankaranarayanan, and S. Kowalewski, "Current challenges in the verification of hybrid systems," in *Cyber Physical Systems. Design, Modeling, and Evaluation*. Springer, 2015, pp. 8–24.

[33] P. Kumar, D. Goswami, S. Chakraborty, A. Annaswamy, K. Lampka, and L. Thiele, "A hybrid approach to cyber-physical systems verification," in *Proceedings of the 49th Annual Design Automation Conference*. ACM, 2012, pp. 688–696.

[34] R. A. Thacker, K. R. Jones, C. J. Myers, and H. Zheng, "Automatic abstraction for verification of cyber-physical systems," in *Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems*. ACM, 2010, pp. 12–21.

[35] G. Frehse, "PHAVer: Algorithmic verification of hybrid systems past HyTech," *International Journal on Software Tools for Technology Transfer*, vol. 10, no. 3, pp. 263–279, 2008.

[36] M. Pajic, Z. Jiang, A. Connolly, S. Dixit, and R. Mangharam, "A platform for implantable medical device validation," in *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks*. ACM, 2010, pp. 418–419.

[37] A. Arrieta, G. Sagardui, and L. Etxeberria, "Test control algorithms for the validation of cyber-physical systems product lines," in *Proceedings of the 19th International Conference on Software Product Line*. ACM, 2015, pp. 273–282.

[38] J. C. Jensen, D. H. Chang, E. Lee *et al.*, "A model-based design methodology for cyber-physical systems," in *7th International on Wireless Communications and Mobile Computing Conference*. IEEE, 2011, pp. 1666–1671.

[39] J. Eker, J. W. Janneck, E. Lee, J. Liu, X. Liu, J. Ludvig, S. Neuendorffer, S. Sachs, Y. Xiong *et al.*, "Taming heterogeneity-the ptolemy approach," *Proceedings of the IEEE*, vol. 91, no. 1, pp. 127–144, 2003.

[40] P. Kulkarni and Y. Öztürk, "Requirements and design spaces of mobile medical care," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 11, no. 3, pp. 12–30, 2007.

[41] I. Lee, G. J. Pappas, R. Cleaveland, J. Hatcliff, B. H. Krogh, P. Lee, H. Rubin, and L. Sha, "High-confidence medical device software and systems," *Computer*, vol. 39, no. 4, pp. 33–38, 2006.

[42] A. Sawand, S. Djahel, Z. Zhang, and F. Nait-Abdesselam, "Multidisciplinary approaches to achieving efficient and trustworthy eHealth monitoring systems," in *IEEE/CIC International Conference on Communications in China*. IEEE, 2014, pp. 187–192.

[43] D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, and W. H. Maisel, "Security and privacy for implantable medical devices," *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 30–39, 2008.

[44] W. H. Maisel and T. Kohno, "Improving the security and privacy of implantable medical devices," *New England Journal of Medicine*, vol. 362, no. 13, p. 1164, 2010.

[45] S. R. Rakitin, "Coping with defective software in medical devices," *Computer*, vol. 39, no. 4, pp. 40–45, 2006.

[46] J. L. Martin, E. Murphy, J. A. Crowe, and B. J. Norris, "Capturing user requirements in medical device development: the role of ergonomics," *Physiological measurement*, vol. 27, no. 8, p. R49, 2006.

[47] A. Banerjee, S. K. Gupta, G. Fainekos, and G. Varsamopoulos, "Towards modeling and analysis of cyber-physical medical systems," in *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies*. ACM, 2011, pp. 1–5.

[48] A. Banerjee and S. K. Gupta, "Spatio-temporal hybrid automata for safe cyber-physical systems: A medical case study," in *ACM/IEEE International Conference on Cyber-Physical Systems*. IEEE, 2013, pp. 71–80.

[49] V. Annese and D. De Venuto, "FPGA based architecture for fall-risk assessment during gait monitoring by synchronous EEG/EMG," in *6th IEEE International Workshop on Advances in Sensors and Interfaces*. IEEE, 2015, pp. 116–121.

[50] H. Huang, Y. L. Sun, Q. Yang, F. Zhang, X. Zhang, Y. Liu, J. Ren, and F. Sierra, "Integrating neuromuscular and cyber systems for neural control of artificial legs," in *Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems*. ACM, 2010, pp. 129–138.

[51] P. Asare, R. F. Dickerson, X. Wu, J. Lach, and J. A. Stankovic, "Bodysim: A multi-domain modeling and simulation framework for body sensor networks research and design," in *Proceedings of the 8th International Conference on Body Area Networks*. ICST, 2013, pp. 177–180.

[52] Y. Gao, S. Hu, R. Mancuso, H. Wang, M. Kim, P. Wu, L. Su, L. Sha, and T. Abdelzaher, "Exploiting structured human interactions to enhance estimation accuracy in cyber-physical systems," in *Proceedings of the ACM/IEEE Sixth International Conference on Cyber-Physical Systems*. ACM, 2015, pp. 60–69.

[53] L. C. Silva, H. O. Almeida, A. Perkusich, and M. Perkusich, "A model-based approach to support validation of medical cyber-physical systems," *Sensors*, vol. 15, no. 11, pp. 27 625–27 670, 2015.

[54] S. Nabar, A. Banerjee, S. K. Gupta, and R. Poovendran, "GeM-REM: Generative model-driven resource efficient ecg monitoring in body sensor networks," in *International Conference on Body Sensor Networks*. IEEE, 2011, pp. 1–6.

[55] P. Bogdan, "A cyber-physical systems approach to personalized medicine: challenges and opportunities for noc-based multicore platforms," in *Proceedings of the 2015 Design, Automation and Test in Europe Conference and Exhibition*. EDA Consortium, 2015, pp. 253–258.

[56] A. Banerjee, S. Kandula, T. Mukherjee, and S. K. Gupta, "BAND-AiDe: A tool for cyber-physical oriented analysis and design of body area networks and devices," *ACM Transactions on Embedded Computing Systems*, vol. 11, no. S2, p. 49, 2012.

[57] P. Troger, M. Werner, and J. Richling, "Cyber-physical operating systems—what are the right abstractions?" in *4th Mediterranean Conference on Embedded Computing*. IEEE, 2015, pp. 13–16.

[58] A. Hahn, R. K. Thomas, I. Lozano, and A. Cardenas, "A multi-layered and kill-chain based security analysis framework for cyber-physical systems," *International Journal of Critical Infrastructure Protection*, vol. 11, pp. 39–50, 2015.

[59] S. A. Haque and S. M. Aziz, "False alarm detection in cyber-physical systems for healthcare applications," *AASRI Procedia*, vol. 5, pp. 54–61, 2013.

[60] B. Miller, F. Vahid, and T. Givargis, "MEDS: Mockup electronic data sheets for automated testing of cyber-physical systems using digital mockups," in *Design, Automation and Test in Europe Conference and Exhibition*. IEEE, 2012, pp. 1417–1420.

[61] A. Banerjee and S. K. Gupta, "Model based code generation for medical cyber physical systems," in *Proceedings of the 1st Workshop on Mobile Medical Applications*. ACM, 2014, pp. 22–27.

[62] W. Zhang, Y.-H. Wei, Q. Leng, and S. Han, "A high-speed, real-time mobile gait rehabilitation system," *XRDS: Crossroads, The ACM Magazine for Students*, vol. 20, no. 3, pp. 46–51, 2014.

[63] T. Li, J. Cao, J. Liang, and J. Zheng, "Towards context-aware medical cyber-physical systems: design methodology and a case study," *Cyber-Physical Systems*, no. ahead-of-print, pp. 1–19, 2014.

[64] A. Pawlak, K. Horoba, J. Jezewski, J. Wrobel, and A. Matonia, "Telemonitoring of pregnant women at home — biosignals acquisition and measurement," in *22nd International Conference Mixed Design of Integrated Circuits and Systems*. IEEE, 2015, pp. 83–87.

[65] A. Tobola, C. Espig, F. J. Streit, O. Korpok, B. Schmitz, C. Hofmann, M. Struck, C. Weigand, H. Leutheuser, B. M. Eskofier *et al.*, "Scalable ECG hardware and algorithms for extended runtime of wearable sensors," in *IEEE International Symposium on Medical Measurements and Applications*. IEEE, 2015, pp. 255–260.

[66] M. Kane, D. Zhu, M. Hirose, X. Dong, B. Winter, M. Häckell, J. P. Lynch, Y. Wang, and R. A. Swartz, "Development of an extensible

dual-core wireless sensing node for cyber-physical systems," in *SPIE Smart Structures and Materials+ Nondestructive Evaluation and Health Monitoring*. International Society for Optics and Photonics, 2014, pp. 90 611U–90 611U.

[67] A. Ray and R. Cleaveland, "Security assurance cases for medical cyber–physical systems," *IEEE Design and Test*, vol. 32, no. 5, pp. 56–65, 2015.

[68] Y. B. Reddy, "Security and design challenges in cyber-physical systems," in *12th International Conference on Information Technology-New Generations*. IEEE, 2015, pp. 200–205.

[69] B. R. Larson, Y. Zhang, S. C. Barrett, J. Hatcliff, and P. L. Jones, "Enabling safe interoperation by medical device virtual integration," *IEEE Design and Test*, vol. 32, no. 5, pp. 74–88, 2015.

[70] H. Dagale, S. Anand, M. Hegde, N. Purohit, M. Supreeth, G. S. Gill, V. Ramya, A. Shastry, S. Narasimman, Y. Lohith *et al.*, "CyPhyS+: A reliable and managed cyber-physical system for old-age home healthcare over a 6LoWPAN using wearable motes," in *IEEE International Conference on Services Computing*. IEEE, 2015, pp. 309–316.

[71] U. Ghoshdastider, R. Viga, and M. Kraft, "Experimental evaluation of a pairwise broadcast synchronization in a low-power cyber-physical system," in *IEEE Topical Conference on Wireless Sensors and Sensor Networks*. IEEE, 2015, pp. 50–52.

[72] X. Ma, X. Tu, J. Huang, and J. He, "A cyber-physical system based framework for motor rehabilitation after stroke," in *Proceedings of the 1st International Conference on Wireless Technologies for Humanitarian Relief*. ACM, 2011, pp. 285–290.

[73] T. S. Dillon, H. Zhuge, C. Wu, J. Singh, and E. Chang, "Web-of-things framework for cyber–physical systems," *Concurrency and Computation: Practice and Experience*, vol. 23, no. 9, pp. 905–923, 2011.

[74] S. Lim, L. Chung, O. Han, and J.-H. Kim, "An interactive cyber-physical system (CPS) for people with disability and frail elderly people," in *Proceedings of the 5th international conference on ubiquitous information management and communication*. ACM, 2011, p. 113.

[75] Y. Tan, M. C. Vuran, and S. Goddard, "Spatio-temporal event model for cyber-physical systems," in *29th IEEE International Conference on Distributed Computing Systems Workshops*. IEEE, 2009, pp. 44–50.

[76] M. S. Hossain, "Cloud-supported cyber–physical localization framework for patients monitoring," *IEEE Systems Journal*, 2015.

[77] L. T. T. Phuong, N. T. Hieu, J. Wang, S. Lee, and Y.-K. Lee, "Energy efficiency based on quality of data for cyber physical systems," in *International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*. IEEE, 2011, pp. 232–241.

[78] Y. Zhang, M. Qiu, C.-W. Tsai, M. M. Hassan, and A. Alamri, "Health-CPS: Healthcare cyber-physical system assisted by cloud and big data," *IEEE Systems Journal*, pp. 1–8, 2015.

[79] J. He, Y. Geng, Y. Wan, S. Li, and K. Pahlavan, "A cyber physical test-bed for virtualization of rf access environment for body sensor network," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3826–3836, 2013.

[80] V. Gunes, S. Peter, and T. Givargis, "Modeling and mitigation of faults in cyber-physical systems with binary sensors," in *IEEE 16th International Conference on Computational Science and Engineering*. IEEE, 2013, pp. 515–522.

[81] M. Wolf, M. van der Schaar, H. Kim, and J. Xu, "Caring analytics for adults with special needs," *IEEE Design and Test*, vol. 32, no. 5, pp. 35–44, 2015.

[82] J. Jezewski, A. Pawlak, J. Wróbel, K. Horoba, and P. Penkala, "Towards a medical cyber-physical system for home telecare of high-risk pregnancy," *IFAC-PapersOnLine*, vol. 48, no. 4, pp. 466–473, 2015.

[83] C.-S. Shih, Y.-H. Wang, C.-M. Yang, and S.-H. Chao, "Elastic computation middleware for interactive wearable devices in cyber-physical systems," in *IEEE 3rd International Conference on Cyber-Physical Systems, Networks, and Applications*. IEEE, 2015, pp. 1–6.

[84] D. Fernandes, A. Ferreira, J. Mendes, and J. Cabral, "A wireless body sensor network based on dynamic power control and opportunistic packet scheduling mechanisms," in *IEEE International Conference on Industrial Technology*. IEEE, 2015, pp. 2160–2165.

[85] F. Xia, L. Wang, D. Zhang, D. He, and X. Kong, "An adaptive MAC protocol for real-time and reliable communications in medical cyber-physical systems," *Telecommunication Systems*, vol. 58, no. 2, pp. 125–138, 2015.

[86] A. Banerjee, K. Venkatasubramanian, and S. K. Gupta, "Challenges of implementing cyber-physical security solutions in body area networks," in *Proceedings of the Fourth International Conference on Body Area Networks*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009, p. 18.

[87] J. Hatcliff, A. King, I. Lee, A. Macdonald, A. Fernando, M. Robkin, E. Vasserman, S. Weininger, and J. M. Goldman, "Rationale and architecture principles for medical application platforms," in *IEEE/ACM Third International Conference on Cyber-Physical Systems*. IEEE, 2012, pp. 3–12.

[88] F. Xia, L. Ma, J. Dong, and Y. Sun, "Network QoS management in cyber-physical systems," in *International Conference on Embedded Software and Systems Symposia*. IEEE, 2008, pp. 302–307.

[89] T. Dillon, V. Potdar, J. Singh, and A. Talevski, "Cyber-physical systems: Providing quality of service (QoS) in a heterogeneous systems-of-systems environment," in *Proceedings of the 5th IEEE International Conference on Digital Ecosystems and Technologies Conference*. IEEE, 2011, pp. 330–335.

[90] J. Liu and L. Zhang, "QoS modeling for cyber-physical systems using aspect-oriented approach," in *Second International Conference on Networking and Distributed Computing*. IEEE, 2011, pp. 154–158.

[91] M. García-Valls and R. Baldoni, "Adaptive middleware design for CPS: Considerations on the OS, resource managers, and the network run-time," in *Proceedings of the 14th International Workshop on Adaptive and Reflective Middleware*. ACM, 2015, pp. 1–6.

[92] S.-Y. Lien, S.-M. Cheng, S.-Y. Shih, and K.-C. Chen, "Radio resource management for QoS guarantees in cyber-physical systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1752–1761, 2012.

[93] J. Huang, F. B. Bastani, I. Yen, W. Zhang *et al.*, "A framework for efficient service composition in cyber-physical systems," in *Fifth IEEE International Symposium on Service Oriented System Engineering*. IEEE, 2010, pp. 291–298.

[94] K. Wan, D. Hughes, K. L. Man, and T. Krilavičius, "Composition challenges and approaches for cyber physical systems," in *IEEE International Conference on Networked Embedded Systems for Enterprise Applications*. IEEE, 2010, pp. 1–7.

[95] D. Menasce, H. Gomaa, S. Malek, J. P. Sousa *et al.*, "SASSY: A framework for self-architecting service-oriented systems," *IEEE Software*, vol. 28, no. 6, pp. 78–85, 2011.

[96] W. Zhang and L. Zhang, "Designing and modeling cyber physical systems by a service-based approach," in *Software Engineering and Service Science (ICSESS), 2015 6th IEEE International Conference on*. IEEE, 2015, pp. 668–671.

[97] W. Zhu, G. Zhou, I.-L. Yen, and F. Bastani, "A PT-SOA model for CPS/IoT services," in *IEEE International Conference on Web Services*. IEEE, 2015, pp. 647–654.

[98] H. J. La and S. D. Kim, "A service-based approach to designing cyber physical systems," in *IEEE/ACIS 9th International Conference on Computer and Information Science*. IEEE, 2010, pp. 895–900.

[99] K. Mechitov and G. Agha, "Building portable middleware services for heterogeneous cyber-physical systems," in *Proceedings of the Third International Workshop on Software Engineering for Sensor Network Applications*. IEEE Press, 2012, pp. 31–36.

[100] S. O. Park, T. H. Do, Y.-S. Jeong, and S. J. Kim, "A dynamic control middleware for cyber physical systems on an IPv6-based global network," *International Journal of Communication Systems*, vol. 26, no. 6, pp. 690–704, 2013.

[101] K.-D. Kang and S. H. Son, "Real-time data services for cyber physical systems," in *28th International Conference on Distributed Computing Systems Workshops*. IEEE, 2008, pp. 483–488.

[102] F. Xia, A. Vinel, R. Gao, L. Wang, and T. Qiu, "Evaluating IEEE 802.15.4 for cyber-physical systems," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, pp. 1–14, 2011.

[103] H. Dubey, J. Yang, N. Constant, A. M. Amiri, Q. Yang, and K. Makodiya, "Fog data: Enhancing telehealth big data through fog computing," in *Proceedings of the ASE Big Data and Social Informatics 2015*. ACM, 2015, pp. 1–6.

[104] S. S. Craciunas, A. Haas, C. M. Kirsch, H. Payer, H. Röck, A. Rottmann, A. Sokolova, R. Trummer, J. Love, and R. Sengupta, "Information-acquisition-as-a-service for cyber-physical cloud computing," in *Proceedings of the 2nd USENIX conference on Hot topics in cloud computing*. USENIX Association, 2010, pp. 14–14.

[105] K.-C. Chen and S.-Y. Lien, "Machine-to-machine communications: Technologies and challenges," *Ad Hoc Networks*, vol. 18, pp. 3–23, 2014.

[106] Consulted on 2016-02-16. [Online]. Available: http://www.onem2m.org/

[107] Consulted on 2018-05-14. [Online]. Available: http://mdpnp.org/

[108] A. King, S. Procter, D. Andresen, J. Hatcliff, S. Warren, W. Spees, R. Jetley, P. Jones, and S. Weininger, "An open test bed for medical device integration and coordination," in *Proceedings of the 31st*

International Conference on Software Engineering - Companion Volume. IEEE, 2009, pp. 141–151.

[109] Consulted on 2018-05-14. [Online]. Available: http://mdpnp.mgh.harvard.edu/projects/openice/

[110] E. Sejdić, A. Millecamps, J. Teoli, M. Rothfuss, N. Franconi, S. Perera, A. Jones, J. Brach, and M. Mickle, "Assessing interactions among multiple physiological systems during walking outside a laboratory: An android based gait monitor," *Computer Methods and Programs in Biomedicine*, vol. 122, no. 3, pp. 450–461, 2015.

[111] B. Gyselinckx, C. Van Hoof, J. Ryckaert, R. F. Yazicioglu, P. Fiorini, and V. Leonov, "Human++: autonomous wireless sensors for body area networks," in *Proceedings of the IEEE 2005 Custom Integrated Circuits Conference*. IEEE, 2005, pp. 13–19.

[112] M. M. Montero-Odasso, Y. Sarquis-Adamson, M. Speechley, M. J. Borrie, V. C. Hachinski, J. Wells, P. M. Riccio, M. Schapira, E. Sejdic, R. M. Camicioli, R. Bartha, W. E. McIlroy, and S. Muir-Hunter, "Association of dual-task gait with incident dementia in mild cognitive impairment: Results from the gait and brain study." *JAMA neurology*, vol. 74, pp. 857–865, Jul. 2017.

[113] R. Wang, G. Blackburn, M. Desai, D. Phelan, L. Gillinov, P. Houghtaling, and M. Gillinov, "Accuracy of wrist-worn heart rate monitors," *Journal of the American Medical Association Cardiology*, vol. 2, pp. 104–106, Jan. 2017.

[114] A. Sushames, A. Edwards, F. Thompson, R. McDermott, and K. Gebel, "Validity and reliability of fitbit flex for step count, moderate to vigorous physical activity and activity energy expenditure." *PloS One*, vol. 11, no. 9, pp. 1–14, 2016.