Medical Cyber-Physica System: Technical And Forensic Approach

Syed Muhammad Saim[1]

Contents

Abstract: The integration of technology and the medical industry boosted an interest in the Medical Cyber-Physical Systems (MCPS). These systems are increasingly used in clinics and hospitals to provide patients with high-quality healthcare. The idea of MCPS faces various challenges that include inoperability, security, safety, privacy, and device certifiability, system availability. In the current work,

[1] syed-muhammad.saim@stud.hshl.de(2180551)

the architecture of Medical Cyber-Physical Systems (MCPS) and its security from unauthorized access is discussed. This article lays the foundation of future research and implementation concurrently.

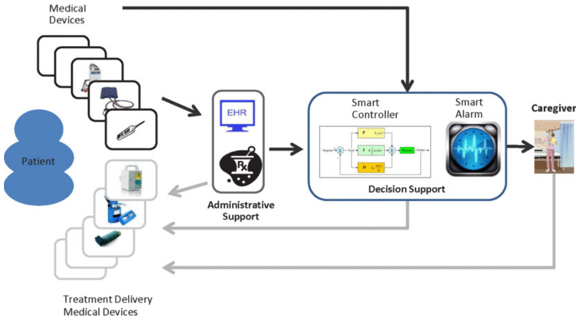
1 Motivation

Unification of computation, including physical processes and cyber world (i.e., computers) through computer networks is referred as Cyber physical systems (CPS). Involvement of embedded computers and networks is essential in monitoring and controlling the physical processes using feedback loops [Vo13]. Sensors are also required to acquire numerous data type so that the data can be transmitted to the cyber world, analyzed, and processed. The concept behind the CPS is to unify intelligence of routine objects/services to carry out critical tasks. The CPS idea has a notable role in various information technology (IT)-based social service frameworks [YFP06]. It can be applied to different areas of social services, especially in medical and healthcare devices [RR14]. In general, various countries encounter a set down in the medical care quality and considerable escalation in healthcare expenditures. This problem results due to the dreadful deficiency of healthcare personnel. Expertise of redesign advance gadgets for healthcare controlling and monitoring systems have ameliorated. In healthcare monitoring, ineffectiveness in handling enormous amount of data in real time comes across due to data transmission utilizing inexpensive sensors and various communication media has led to a prime concern for the prevailing platforms. As a result, an infrastructure and computing framework are needed to improve this field. This directs to Big data processing frameworks for Medical Cyber-Physical Systems (MCPS) which unify the cyber world aspects and the real world with dynamic, fully flexible systems for decision making and other healthcare applications [HAR14a] [HAR14b].

A groundbreaking breakthrough in communication and computers occurred during the modern era. The Internet has spread across many networks, having a significant impact on every area of life, particularly in the medical field. The CPS and MCPS systems have a far greater social and economic impact. Various expenditures are made around the world to improve this technology. Because medical data may be transmitted via the internet, the physical components of the systems in question face numerous issues, including security, reliability, and safety [Ta14]. These obstacles are unlike anything you'll find in a typical computing application. Physical components are inferior to conventional object-oriented software components in terms of quality. The next generation will rely on a wide range of resources with significant sensing capabilities that will be extended beyond physically connected computers to include multimodal data from biological, cognitive, and social networks [Ba13]. As a result, cyber-physical social systems (CPS) and net-centric societies (NCS) came into being with the help of standard modification that will include interdependent social networks (networks of individuals), smart devices, communication devices and mobile personal computing. As a result, cyber-physical social systems (CPSS) and net-centric societies (NCS) emerged as a result of standardization, which included interdependent social networks (individual networks), smart gadgets, communication devices, and mobile personal computer [Ra10] [Li11]. Technology advancement is considered a crucial function in developing infrastructures that result in the removal of healthcare problems by applying automated ubiquitous health monitoring systems.

To complicate matters further, a MCPS is plausibly to gather and manage enormous amounts of medical data [KSA16]. This will probably give boost to security and privacy concerns within the healthcare community. In addition to this, medical industry is a high target industry for malicious use of data according to 2015 IBM [To17]. As a result, the Federal Bureau od Investigation (FBI) foretells that healthcare systems and medical devices are progressively becoming targets for attackers in the future [CB18]. It is also emphasized in the same FBI press release that medical industry is still not designed to secure against basic cyber attacks. Therefore, it is also a dire need to consider the security and safety requirements of MCPS systems together with advanced components.

This study's main contribution is to increase knowledge of MCPS systems, their function in healthcare, and the incorporation of forensic-driven requirements into the design and development phases of MCPS. This study focused on improvements to the CP and MCPS systems. Also highlighted is the possibility of encountering a forensic-driven strategy. Finally, current research goals and obstacles in MCPS for future medical devices are discussed.



[De18]

2 Technical Aspect

MCPSs are medical device safety-critical, networked, intelligent systems. Traditional clinical scenarios can be thought of as closed-loop systems, with caregivers acting as controllers, medical devices acting as sensors and actuators, and patients acting as "plants."MCPSs change this perspective by introducing new computational entities that help the caregiver manipulate the "plant."The conceptual overview of MCPSs is shown in Figure 1. Monitoring devices, such as heart-rate and oxygen-level monitors and sensors, which provide information about the patient's physiologic state, and delivery devices, such as infusion pumps and ventilators, which actuate therapy capable of changing the patient's physiologic state, are the two large groups of devices used in MCPSs. In MCPSs, data generated by monitoring devices can be fed to decision support or administrative support entities, each of which serves a different, but complimentary, role.

Patient's health and treatment information is collected over time and is managed by administrative entities such as electronic health records (EHRs) and pharmacy stores. They have the potential to give tailored treatment based on a more comprehensive view of the patient's health because they have access to a lot of individualized data (e.g., by considering potential drug interactions or by taking into account the longitudinal evolution of a specific patient physiological parameter). They can help in this area by meeting the requirement for the patient's ongoing care. Many of today's health concerns, such as dealing with the aging population and the significant rise in the number of people with chronic illnesses like asthma and diabetes, require continuous data collection and administration.

For many medical emergencies, decision support entities can process the data collected and raise alarms. Alarms are required to tell clinicians when a patient's condition has deteriorated and what information is needed to treat them. However, it is now obvious that smart alarm systems must be developed that go beyond current threshold-based methods to deliver more precise, targeted alarms, as well as context information. After assessing the data, caregivers can use delivery devices to begin therapy, putting them in the control loop encircling the patient. Decision support entities can also use a smart controller to analyze data from monitoring devices, assess the patient's health, and automatically commence therapy (e.g., drug infusion) by sending commands to delivery devices, essentially closing the loop.

MCPS Challenges are a set of tasks that students must complete in order to graduate Developing various kinds of MCPS necessitates overcoming a number of significant obstacles.

- Software with high confidence is becoming increasingly crucial in medical equipment.
- Interoperability: It's critical to ensure that the resulting integrated medical devices are safe, effective, and secure, and that they can be certified as such in the future when medical equipment adds communication interfaces.
- Context awareness: Patient data communicated during device interoperability can help with not just a better understanding of a patient's overall health, but also the early detection of illnesses and the development of effective emergency alarms.
- Autonomy: By permitting therapeutic actuation based on the patient's present health state, the computational intelligence in MCPS can be used to strengthen the system's autonomy.
- Security and privacy: The medical information gathered and maintained by MCPSs is crucial. As a result, ensuring the security of MCPSs is essential.
- Certifiability: The intricate and life-or-death nature of MCPSs necessitates a low-cost method of demonstrating medical device software reliability. As a result, certifiability is a critical criterion for the long-term viability of MCPSs and a significant hurdle to overcome.

Increased regulatory pressure has been applied to firms in the healthcare business, requiring security incident response capabilities, including forensic investigations, as a result of growing security concerns with medical equipment. [Jo03]. As part of a company's security incident response capability, forensic investigations are usually employed to determine the six important questions that an incident raises: what, why, who, when, where, and how [FS07]. Security incident response is focused with restoring service and learning about the causes of a security breach, whereas digital forensics is focused with gathering and analyzing information that can be used in court. [FS07].Security incident handlers inside an organization frequently collect and analyze potential evidentiary data after a security event occurs. As a result, some people are concerned that businesses appear careless about data activity prior to an event. Therefore, data needed for an inquiry will either exist and be preserved by a system, or it will not exist, which can obstruct an effective inquiry. These worries spurred comments that businesses should be more proactive when it comes to digital forensics and structure environments to keep data needed for investigations safe. This technique or posture is referred to as "forensic readiness.". Previous studies on forensic readiness focused at policy and procedure implementation, system alignment with forensic aims, and personnel impact and training [BSJ10].

3 Forensic Frame Work

The forensic-by-design framework for MCPS consists of nine components. The components are presented as a black-box with the objective of designing a forensic-ready MCPS that can assist developers in the overall design and development process along with guiding investigators in the examination of security incidents.

3.1 Forensic Readiness Principles

The ability of an organization to optimize the acquisition of evidence data while minimizing the cost of an investigation is the emphasis of forensic preparedness. The following forensic preparedness activities, as proposed by Rowlingson, are incorporated into this framework:

- define the circumstances in which digital proof is required in the workplace
- Determine what sources are available and what kind of evidence might be useful.

According to Kocabas et al [KSA16], MCPS design has four layers (data acquisition, data concentration, cloud processing and action layers).Wearable sensors, medical applications, and devices in the data acquisition layer; cloudlets and gateway servers in the data concentration layer; public and private cloud environments in the cloud processing layer; and the outcomes of actions taken in the action layer are all examples of evidence sources within MCPS.

- Determine the amount of evidence that must be collected.
- Create a policy for storing and processing potential evidence in a secure manner. If evidence data from MCPS is to be used in an inquiry, it must be handled and kept properly [Ca11].
- Indicate when an escalation to a full formal investigation should be undertaken. Because of the MCPS's intricacy, it may be difficult to determine when a suspicious event has happened. When a suspicious event is discovered, however, an organization will need to employ an incident response taxonomy to 'grade' the severity or impact of the occurrence [Gr16].
- Train workers in incident awareness so that everyone participating in the digital evidence process understands their responsibilities and the legal sensitivity of evidence.

There are potential to improve security incident awareness and reporting methods within businesses, according to Grispos et al. [Gr17] and Christopher et al. [CD16].

3.2 Security Requirements

When stakeholders see a system's worth to an organization, they will attempt to safeguard it by establishing security requirements early in the development process [Ha08]. Failure to correctly implement these principles could result in the necessity for a forensic inquiry from a forensic-by-design standpoint. In the context of MCPS, however, investigative findings and information acquired from responding to security incidents could be leveraged to define stronger security standards. Different security needs will almost certainly be required by the many applications, devices, and systems that make up MCPS. Hence, a greater knowledge of the security requirements for this complex interconnected system will help to strengthen MCPS security activities.

3.3 Privacy Requirements

Sensors and devices in MCPS could potentially acquire extremely sensitive data. Some sensors in MCPS, for example, might operate as a "lab-on-a-chip,"detecting the presence of medical medications, recording temperatures, and collecting bio-markers [Bu12]. Stakeholders must address a unique set of privacy-preserving considerations while developing these sensors and devices. For example, forensic investigators investigating a security event involving a hostile actor could be privy to sensitive patient information collected by general use of MCPS. Because of privacy considerations, developing a forensic-driven MCPS will almost certainly include acknowledging that privacy needs may conflict with forensic tactics.

3.4 Medical Requirements

Within MCPS, it's critical to understand how a medical device interacts with its numerous medical surroundings. Medical requirements, for the sake of this discussion, are the requirements that must be met in order for an application, device, or system to have a medical purpose. These requirements drive the creation of a device's functionality, such as an infusion pump's ability to provide insulin to a patient. It's worth noting that a forensic-driven MCPS development strategy could clash with certain medical needs for MCPS components. Medical needs, for example, will almost certainly necessitate that a component deliver its medical capability in the case of an incident or breach. This, however, may be incompatible with the preservation and collection of evidence. Therefore, stakeholders must first determine the medical requirements for MCPS before conducting a trade-off analysis between medical requirements and forensic readiness-related criteria.

3.5 Safety Requirements

Patient safety must be considered while designing and validating interconnected medical devices that could become part of MCPS [EGA05]. Incorporating forensic methodologies into the creation of MCPS could provide extra risks. This is due to the fact that many existing forensic methodologies and incident response processes are geared for investigations involving office-based systems and provide only rudimentary support for investigations involving safety-critical systems like MCPS [Jo03]. Traditional procedures, for example, suggest shutting down systems and preserving evidence stored in device memory. Nevertheless, shutting down a safety-critical application (such as a fusion pump or pacemaker) to collect potential evidence metadata may be impossible. Hence, when creating and developing the forensic strategy that will be integrated into the design of their MCPS, MCPS stakeholders must consider safety criteria, as well as additional options such as live forensic acquisition methodologies.

3.6 Software And Hardware Requirements

MCPS is likely to have a diverse set of applications, devices, and systems, all of which are powered by distinct hardware configurations and software from different suppliers. The interdependence of these numerous components within MCPS invariably complicates data protection and collecting. Potential evidentiary data could exist in many layers of MCPS design, as mentioned in Section III-B. As a result, knowing the various hardware and software needs that will arise from each layer aids in the identification, preservation, and collecting of data that may be useful in a forensic inquiry. A forensic investigator must identify potential evidence that can be recovered from a mobile device if it is employed as a gateway between a monitoring sensor and a cloud storage facility, for example. This ostensibly includes dealing with the difficulties of gathering evidence in a cloud computing setting.

4 Research directions and challenges in MCPS for future medical devices

Medical device systems are a prime example of cyber-physical systems, as they involve complicated and intimate interactions between treatment algorithms and the physical parts of the system, notably the patient. Since such systems are becoming increasingly interconnected and sophisticated, the main task is to secure and develop the security, safety, and dependability of the CPS medical device [Le11] [JPM11] [Ot06]. Researchers have recently been drawn to social networks/services, as well as big data analysis and applications [To16] [De17]. Recently, such fascinating technology has been used to support healthcare applications via cyber-physical systems. With the proliferation of Wireless Sensor Nettwroks (WSNs), Machine to Machine (M2M), Radio Frequency Identification (RFID), ubiquitous computing technology, network communication equipment, and a developing control model, CPSs can be considered a new pattern of Information of Things (IoT). Massive smart devices and wireless networks have the potential to improve CPS applications, allowing them to provide intelligent facilities based on data from the actual world. Therefore, one of the issues is supplying high-performance CPS systems as part of the IoT phase. Furthermore, concurrent models of computing that are significantly more predictable, deterministic, and intelligible will not be incorporated in the next generation of CPS systems. The researchers are motivated by a number of topics, including formal verification, simulation and emulation approaches, certification approaches, software engineering methods, software component technologies, and design patterns. The underlying computing abstractions must be rethought with incremental advancements to adequately appreciate the CPS impact. However, semantic models that capture the qualities of interest are required for effective software orchestration and physical processes. The following are some research difficulties that can be addressed:

- Engineering and science-based design and progress are supported by implementation technologies and platforms.;
- New ways to advancing end-to-end, development, and principled tools.

Additional areas to explore for MCPS medical systems and devices are:

- Medical information is synthesized, and medical systems progress towards CPS. This poses significant issues in terms of obtaining medical data, as various physicians may prescribe various treatment regimens for the same patient.;
- Innovative services, such as schedulers, are required in CPS-based healthcare systems to accommodate the reactive and synchronous systems.

CPS-supported developing health care has the potential to become a cost-effective laboratory/medical technology. Hence, device structural similarities will be extremely dynamic dependent on patient-specific medical concerns. This future will be built on a technological basis that enables for the creation of flexible embedded systems using control and networking technologies. At the same time, information technology must be able to handle effective therapy delivery, a wide range of device requirements, and stay highly adaptive to evolving user needs. As medical technology progresses to smaller scales due to molecular and cellular dynamics, new prospects for extremely integrated control and sensing are emerging. Moreover, additional research into Holistic cyber-physical systems in the healthcare domain should be conducted in order to develop the next generation of medical CPS devices. CPS, on the other hand, is regarded a development of M2M because it incorporates more interactive and cognitive activities into the IoT architecture. The linkages between M2M, CPSs, WSNs, and the IoT, on the other hand, are still a work in progress. M2M is a burgeoning sector that faces various critical hurdles, including: i) The rise of cloud computing will open up new possibilities for M2M applications. However, combining cloud computing with M2M systems will necessitate more research; ii) Integrating M2M components with other M2M components or bigger systems necessitates advanced system integration abilities.; and iii) Developing M2M systems using compound mesh networks is costly and time-consuming, and it necessitates substantial research. Other challenging directions in CPS design, such as network security, energy management, data management/transmission, distributed real-time control, system resource management, model-based design, and platforms/systems, have recently emerged. For upcoming CPS systems, the goal is to maximize QoS while lowering energy usage.Furthermore, when multiple devices coexist, communication consistency becomes a severe issue. Bluetooth, Zigbee, and WiFi, for example, all operate on the same ISM frequency band, resulting in likely interference. The current healthcare system has various design challenges in terms of sociality, including:

- cyber and physical security
- intelligent informing
- access control
- key management, encryption and secure protocols
- balance between availability and privacy
- detection of physical and cyber-attacks data mining
- social contexts verification.

There are various complexity types in the context of MCPSs:

- The relationships and amount of components are unchanged throughout time in static complexity

- dynamic complexity, in which the relationships and numbers of components vary throughout time
- co-evolving complexity
- evolving complexity and
- self-organizing complexity.

In the future, these complexities will have to be overcome. The CPS has a significant impact on human cognitive processes. The ability of people to recognize patterns and simplify them into models, for example, is unknown and not implemented on computers. Eventually, the medical Internet of Things (MIoT) to enable healthcare transformation, guarding interoperable clinical environments with authentication, and embedded, real-time, networked MCPS are all recent interesting domains of healthcare applications. Finally, multiple studies on various Medical CPS applications have been conducted, which can be regarded for future reading [BDM17].

5 Conclusion

The MCPS domain presents a unique set of issues not seen in any other CPS domain. The obstacles that MCPSs face are serious, but they also bring a wealth of research opportunities with direct application. Major problems in MCPS development were noted, and prospective research avenues that could assist solve some of these issues were explored.

6 Declaration of Originality

I hereby confirm that I have written the accompanying paper by myself, without contributions from any sources other than those cited in the text and acknowledgements. This applies also to all graphics, drawings, maps and images included in the paper. The paper was not examined before, nor has it been published.

Bibliography

[Ba13] Baronchelli, Andrea; Ferrer-i Cancho, Ramon; Pastor-Satorras, Romualdo; Chater, Nick; Christiansen, Morten H: Networks in cognitive science. Trends in cognitive sciences, 17(7):348–360, 2013.

[BDM17] Bernardeschi, Cinzia; Domenici, Andrea; Masci, Paolo: A PVS-simulink integrated environment for model-based analysis of cyber-physical systems. IEEE Transactions on Software Engineering, 44(6):512–533, 2017.

[BSJ10] Barske, David; Stander, Adrie; Jordaan, Jason: A digital forensic readiness framework for South African SME's. In: 2010 Information Security for South Africa. IEEE, pp. 1–6, 2010.

[Bu12] Burleson, Wayne; Clark, Shane S; Ransford, Benjamin; Fu, Kevin: Design challenges for secure implantable medical devices. In: DAC Design Automation Conference 2012. IEEE, pp. 12–17, 2012.

[Ca11] Casey, Eoghan: Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press, 2011.

[CB18] Coventry, Lynne; Branley, Dawn: Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas, 113:48–52, 2018.

[CD16] Choo, Kim-Kwang Raymond; Dehghantanha, Ali: Contemporary digital forensic investigations of cloud and mobile applications. Syngress, 2016.

[De17] Dey, Nilanjan; Ashour, Amira S; Chakraborty, Sayan; Banerjee, Sukanya; Gospodinova, Evgeniya; Gospodinov, Mitko; Hassanien, Aboul Ella: Watermarking in biomedical signal processing. In: Intelligent techniques in signal processing for multimedia security, pp. 345–369. Springer, 2017.

[De18] Dey, Nilanjan; Ashour, Amira S; Shi, Fuqian; Fong, Simon James; Tavares, João Manuel RS: Medical cyber-physical systems: A survey. Journal of medical systems, 42(4):1–13, 2018.

[EGA05] Emmet, Luke; Guerra, Sofia; Adelard, Drysdale Building: Application of a Commercial Assurance Case Tool to Support Software Certification Services. In: Proceedings of the 2005 Automated Software Engineering Workshop on Software Certificate Management (SoftCeMent'05), Association for Computing Machinery, New York. Citeseer, pp. 51–55, 2005.

[FS07] Freiling, Felix C; Schwittay, Bastian: A common process model for incident response and computer forensics. IMF 2007: IT-Incident Management & IT-Forensics, 2007.

[Gr16] Grispos, George: On the enhancement of data quality in security incident response investigations. PhD thesis, University of Glasgow, 2016.

[Gr17] Grispos, George; Glisson, William Bradley; Bourrie, David; Storer, Tim; Miller, Stacy: Security incident recognition and reporting (SIRR): an industrial perspective. arXiv preprint arXiv:1706.06818, 2017.

[Ha08] Haley, Charles; Laney, Robin; Moffett, Jonathan; Nuseibeh, Bashar: Security requirements engineering: A framework for representation and analysis. IEEE Transactions on Software Engineering, 34(1):133–153, 2008.

[HAR14a] Haque, Shah Ahsanul; Aziz, Syed Mahfuzul; Rahman, Mustafizur: Review of cyber-physical system in healthcare. international journal of distributed sensor networks, 10(4):217415, 2014.

[HAR14b] Haque, Shah Ahsanul; Aziz, Syed Mahfuzul; Rahman, Mustafizur: Review of cyber-physical system in healthcare. international journal of distributed sensor networks, 10(4):217415, 2014.

[Jo03] Johnson, CW: A handbook of incident and accident reporting. Cité dans la, p. 115, 2003.

[JPM11] Jiang, Zhihao; Pajic, Miroslav; Mangharam, Rahul: Cyber–physical modeling of implantable cardiac medical devices. Proceedings of the IEEE, 100(1):122–137, 2011.

[KSA16] Kocabas, Ovunc; Soyata, Tolga; Aktas, Mehmet K: Emerging security mechanisms for medical cyber physical systems. IEEE/ACM transactions on computational biology and bioinformatics, 13(3):401–416, 2016.

[Le11] Lee, Insup; Sokolsky, Oleg; Chen, Sanjian; Hatcliff, John; Jee, Eunkyoung; Kim, BaekGyu; King, Andrew; Mullen-Fortino, Margaret; Park, Soojin; Roederer, Alexander et al.: Challenges and research directions in medical cyber–physical systems. Proceedings of the IEEE, 100(1):75–90, 2011.

[Li11] Liu, Zhong; Yang, Dong-sheng; Wen, Ding; Zhang, Wei-ming; Mao, Wenji: Cyber-physical-social systems for command and control. IEEE Intelligent Systems, 26(4):92–96, 2011.

[Ot06] Otto, Chris; Milenkovic, Aleksandar; Sanders, Corey; Jovanov, Emil: System architecture of a wireless body area sensor network for ubiquitous health monitoring. Journal of mobile multimedia, 1(4):307–326, 2006.

[Ra10] Rajkumar, Ragunathan; Lee, Insup; Sha, Lui; Stankovic, John: Cyber-physical systems: the next computing revolution. In: Design automation conference. IEEE, pp. 731–736, 2010.

[RR14] Raghupathi, Wullianallur; Raghupathi, Viju: Big data analytics in healthcare: promise and potential. Health information science and systems, 2(1):1–10, 2014.

[Ta14] Tao, Li et al.: On coordination of cyber-physical systems. 2014.

[To16] Tong, Guangmo Amo; Li, Shasha; Wu, Weili; Du, Ding-Zhu: Effector detection in social networks. IEEE Transactions on Computational Social Systems, 3(4):151–163, 2016.

[To17] Torkura, Kennedy A; Sukmana, Muhammad IH; Cheng, Feng; Meinel, Christoph: Leveraging cloud native design patterns for security-as-a-service applications. In: 2017 IEEE International Conference on Smart Cloud (SmartCloud). IEEE, pp. 90–97, 2017.

[Vo13] Voit, Harald: An arbitrated networked control systems approach to cyber-physical systems. PhD thesis, Technische Universität München, 2013.

[YFP06] Yi, Mun Y; Fiedler, Kirk D; Park, Jae S: Understanding the role of individual innovativeness in the acceptance of IT-based innovations: Comparative analyses of models and measures. Decision Sciences, 37(3):393–426, 2006.