Research Article

A Systems Theoretic Approach to Safety Analysis in Medical Cyber Physical Systems

Sonali Gupta

Asst. Professor, Department of CSE (Computer sc)

GEHU-Dehradun Campus

Abstract: The concept of a Cyber-Physical System (CPS) has been gaining traction as a promising new field of study in recent years. It integrates digital processing and data transfer with the real environment. Healthcare, aircraft, automobiles, chemicals, civil infrastructure, energy, manufacturing, transportation, and biological systems are just a few of the many applications of cyber-physical systems. Medical Safe, context-aware, and interconnected networks of medical equipment are what we call Medical Cyber-Physical Systems (MCPS). More and more hospitals are installing these systems in order to give their patients with round-the-clock, high-quality treatment. Systems theory is an umbrella term for the study of how various parts of a system interact to provide a unified whole. Bio-electronic systems (implantable medical devices) are a common kind of MCPS. Bionic ear and eye implants, deep brain stimulators for neurological disorders, and bionic arms for amputees are all examples of computer-based bio-electronic systems designed to replace impaired human body parts. There is a lot of work being done to boost the efficiency of bionic systems so that they can operate at near 100% efficiency, at cheap cost, and in smaller, safer packages. Avoiding risks to property and human life caused by uncontrolled interactions in implanted devices of CPS makes the design of bug-free and safe medical device software in MCPS both crucial and difficult.

Keywords: Cyber-Physical System (CPS), Medical Cyber-Physical Systems (MCPS), Deep Brain Stimulator, bio-electronic systems

Introduction

Recent advances in computing and software have altered the typical nature of accidents. Many mishaps using our modern methods are caused not by a single faulty part but by dangerous interactions between parts that all functioned well. Computers are increasingly being used in systems that must maintain a high level of dependability and safety. However, conventional methods of risk assessment minimise human error by focusing on the failure of individual parts [2, 3]. There have been attempts to update these conventional methods of hazard analysis to account for programme and cognitively complex human faults, but these efforts have shown inconsistent results. Current hazard analysis techniques, such as Fault Tree Analysis (FTA) and Failure Mode and Effect Analysis (FMEA), analyse component failures and readily miss dangerous requirements, despite the fact that the majority of software-related mishaps can be traced back to incomplete or incorrect programme requirements [4, 5]. These problems on Cyber-Physical Systems (CPS) need for new models of accident causation and hazard study approaches. Critical Physical Systems (CPS) combine computing, social networking, and physical processes in a way that prioritises safety. Transportation planning as well as safety, automobile engineering, industrial and process management, Integrating ideas from cybernetics, mechanical engineering, and process science, CPS employs multidisciplinary approaches [7, 8, 9].

Combined physical and computational systems (CPS) provide a more reliable combination and synchronisation of the two. Standardisation for Medical Cyber-Physical Systems is still in its infancy. In order to apply the best practises and standards from the medical field to healthcare Cyber-Physical Systems, much study is required.

Reasons for unsafe situations in key industrial sectors

Several mishaps using cyber-physical systems have occurred. Here are summaries of a few high-profile cases of software-related disaster in critical industries.

A) Biomedical Industry The Therac-25 is a computerised radiation treatment system that has been the subject of widely reported software-related incidents in CyberPhysical Systems. The Therac-25 was a cancer irradiation device that, by accelerating electrons to create high strength beams, could kill cancer cells while leaving healthy tissue unharmed. In 1982, one of the first of a new series of computer-controlled devices, the Therac-25, was released. The Therac-25's innovative safety features stem from its usage of the computer to replace the need for separate, hardwired electro-mechanical circuits, known as interlocks. The flaw was a race situation introduced during development due to a lack of data source security [10].

B) Aerospace Industry On June 4th, 1996, just forty seconds after taking off from Kourou, French Guiana, an unmanned Ariane 5 rocket launched by the European Space Agency detonated. There was a $500 million loss due to the loss of the rocket and its payload. Following an investigation by a board of inquiry, it was determined that a software bug in the ship's inertial reference system was to blame for the explosion. The Breeze launcher's software flight-control system had a fault, as acknowledged by the European Space Agency. Because of this issue, the Breeze upper stage did not provide the necessary signal to turn off the second stage engine. An error prevented the rocket's second and third stages from separating, sending the satellite plummeting to Earth instead of into orbit. [12]

Safety in Cyber-Physical Systems (CPS)

Avoiding risks to people's health as a result of cyber-physical system interactions is what's meant by "safety" in this context. This interpretation is broad and may be applied to any CPS. Networking and Information Technology Research and Development (NITRD) programme study [20] confirms the safety-critical nature of CPS. CPS must be analysed and guaranteed for safety even before deployment, since hazards in CPS might have direct harmful implications on the physical environment. Complex dynamical systems (CPS) consist of numerous interconnected parts that behave as a whole. Faults in the computational hardware, software, communication channel, physical environment, and the interaction between components may all lead to undesirable aggregate consequences, and so constitute a potential source of safety breaches in the CPS. CPSs are made up of embedded computer units that have a close interaction with their physical surroundings to perform essential functions including monitoring health, gathering sensitive data, and ensuring continuous functioning.

When a system is safe, its users may rest easy knowing that it will not do any damage to the surrounding environment or infrastructure, even if anything goes wrong while it's in operation. In the academic literature, researchers have focused on various parts of a system and defined security in various technological environments. Cyber-physical systems (CPSs) are distinguished by the fact that its computational node communicates with the surrounding physical world. Therefore, with CPS, there are worries about how the computer will interact with the real world. In the past, accidents often resulted from faulty parts or unexpected breakdowns. Fortunately, modern approaches to safety engineering are excellent at preventing mishaps caused by faulty parts. These days, unanticipated interactions between parts are more likely to lead to catastrophic mishaps than individual parts failing. This is particularly true for parts of software that have a history of triggering mishaps when improperly executed. Human-computer interaction and operator jobs are evolving as a result of the proliferation of software. Operators are now tasked with a far higher level of decision making, including the identification of novel challenges and the creation of novel solutions, as opposed to just performing basic processes and learning simple rule-based activities.

Medical Cyber-Physical System (MCPS) architecture

Critical, linked, and smart medical device technologies are what make up a Medical Cyber-Physical System (MCPS). The systems interact with a collection of embedded devices, which they command and operate remotely using a predefined set of instructions. There is an immediate feedback loop between the real world and the virtual one. MCPS are often used in healthcare settings. Carer roles in conventional clinical settings may be modelled as controllers, medical equipment as sensors and actuators, and patients as plants in a closed-loop system. Figure 1 below provides a conceptual framework for understanding MCPS.

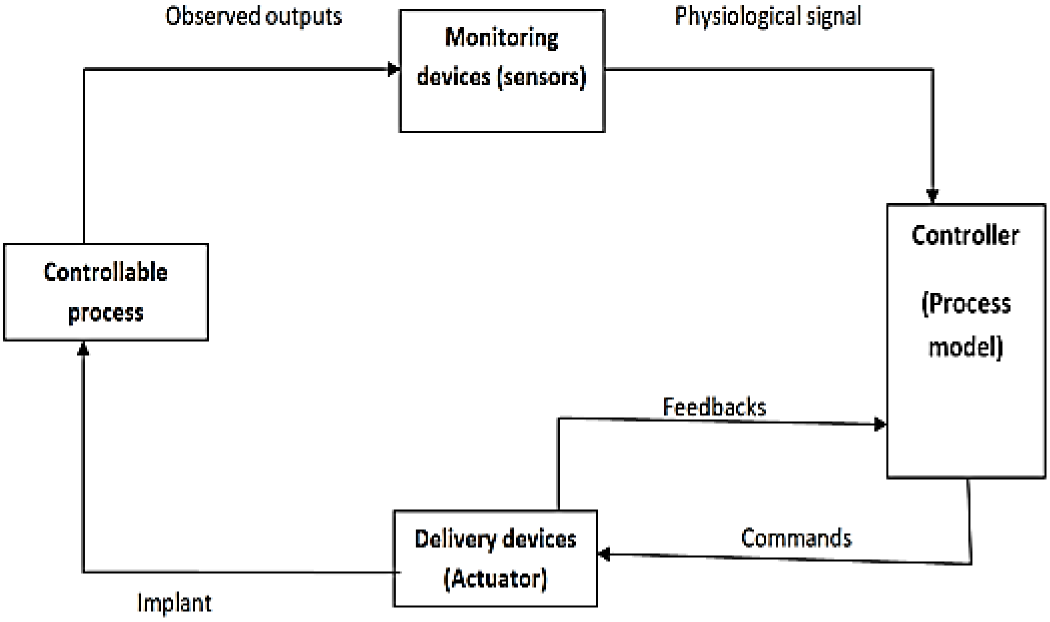


Figure 1: Medical Cyber-Physical System architecture

Sensors, bedside heart-rate and oxygen level monitors are examples of monitoring devices used in MCPS. These provide various types of clinic-relevant details about patients. Delivery devices, such as actuators, infusion pumps, and ventilators, are examples of treatment able to modify the patient's physiological state. MCPS's monitoring tools may feed data to either decision support or management aid agencies, each of which serves a distinct but complementary function. Individual health and therapeutic data is managed by administrative bodies like electronic health records and drugstores. Since they have access to the patient's unique data, they may potentially provide treatment that is more in line with the patient's actual state of health. In this way, they may contribute to meeting the need for the afflicted person's ongoing care. Many current medical challenges need constant data collection and management, including dealing with an ageing population and the rapid increase in the number of people suffering from catastrophic disorders such bronchial asthma and diabetes.

A systems-theoretic approach to safety analysis in Patient-Controlled Analgesia (PCA)–MCPS

The goal of patient-controlled analgesia (PCA) is to provide patients some measure of control over their pain by allowing them to administer their own doses of analgesic medication. System components include a patient-controlled analgesia (PCA) pump, a supervisor, and a pulse oximeter for continuous monitoring of blood oxygen saturation (SpO2) to gauge the effectiveness of the analgesic being administered. When the patient's SpO2 drops below a certain level, the supervisor is alerted and the PCA pump is shut off to avoid any additional potential harm. Patient care is still not adequately addressed by PCA-MCPS. Misuse of drugs or incorrect dosing may result in serious overdosing. However, the current PCA-MCPS cannot identify and avoid these types of human mistakes. It is possible that some individuals may have a very long delay before showing any respiratory symptoms to the medication administration. Therefore, the patient's respiratory status is not always indicative of the whole dose administered. Because of this, PCA- MCPS is unable to quickly turn off the PCA pump in the event of an overdose.

As a result, patients' lives may be at danger [13]. We offer a systems-theoretic method to safety analysis in PCA-MCPS [14] to address this critical issue. Figure 2 shows how the PCA-MCPS has been outfitted with sensors to identify human mistake and then respond preemptively to safeguard the patient.

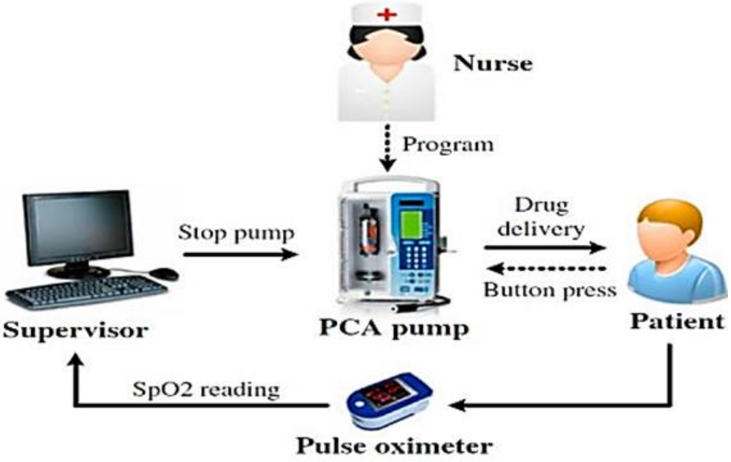
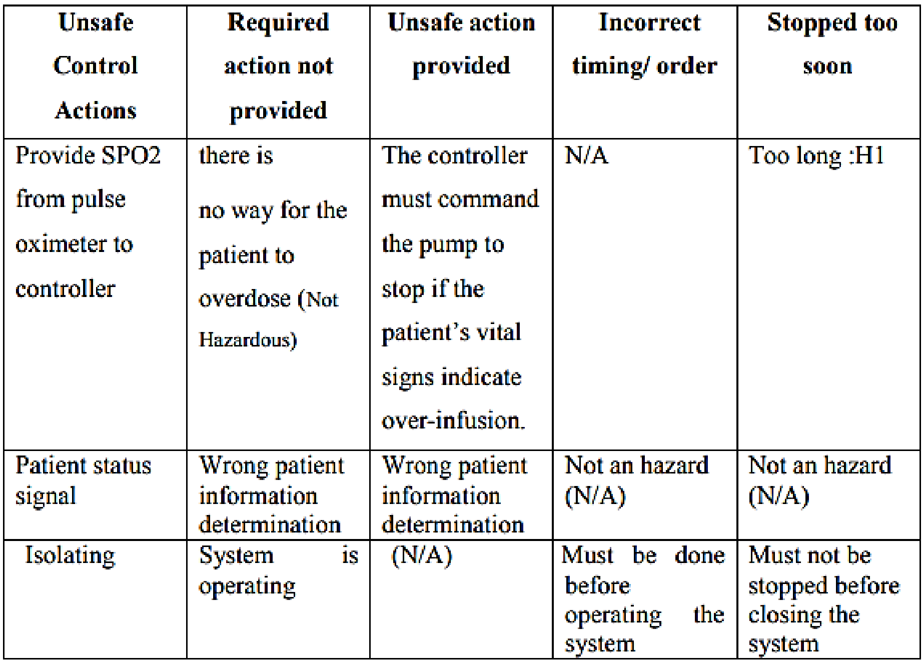


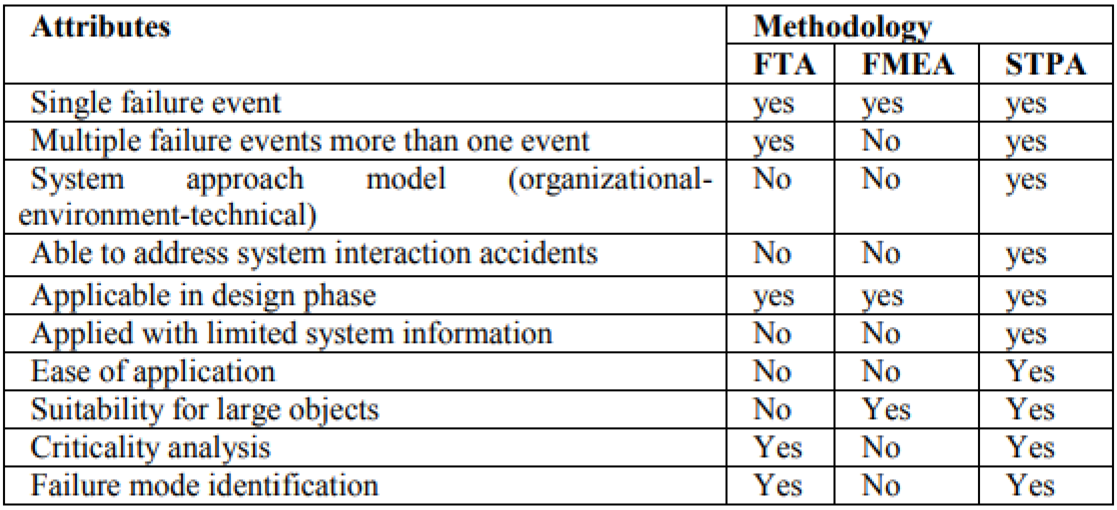
Figure 2: Closed-loop PCA-Medical Cyber-Physical System

Table 1: Unsafe Control Actions For PCA-MCPS



Unsafe Control Actions	**Required action not provided**	**Unsafe action provided**	**Incorrect timing/ order**	**Stopped too soon**
Provide SPO2 from pulse oximeter to controller	there is no way for the patient to overdose (Not Hazardous)	The controller must command the pump to stop if the patient's vital signs indicate over-infusion.	N/A	Too long :H1
Patient status signal	Wrong patient information determination	Wrong patient information determination	Not an hazard (N/A)	Not an hazard (N/A)
Isolating	System is operating	(N/A)	Must be done before operating the system	Must not be stopped before closing the system

Table 2: Hazard Analysis Methods Comparison Table



Attributes	Methodology		
	FTA	FMEA	STPA
Single failure event	yes	yes	yes
Multiple failure events more than one event	yes	No	yes
System approach model (organizational-environment-technical)	No	No	yes
Able to address system interaction accidents	No	No	yes
Applicable in design phase	yes	yes	yes
Applied with limited system information	No	No	yes
Ease of application	No	No	Yes
Suitability for large objects	No	Yes	Yes
Criticality analysis	Yes	No	Yes
Failure mode identification	Yes	No	Yes

Conclusion

The following substantial research issues are addressed in this paper: In the topic of medical cyber-physical system safety, researchers are primarily interested in discovering methods to reduce the chance of potentially hazardous system situations brought on by various parts of an MCPS and the consequences of failures in those elements. Improving MCPS system design and development is the major goal of this research. This includes reducing the likelihood of failures in critical areas such as control loops, component interfaces, and requirements. Specifically for the field of medicine's cyber-physical systems, we developed a Systems-theoretic functional approach to safety analysis to help fill in the gaps in our understanding of secure software development procedures. Systems engineering, software engineering, and safety engineering research aided in the creation of this technique. Our research aimed to answer two primary issues. Initially, attention was paid to expanding one's theoretical knowledge of the variables that go into safety studies. We then required to formally develop and practically implement the proposed systems-theoretic approach to safety analysis in medical cyber-physical systems.

References

1. C. Ericson, Hazard analysis techniques for system safety. Wiley-Inter science, 2005,
2. Dekker S., Ten questions about human error: a new view of human factors and system safety. Human factors in transportation 2005, Mahwah, N.J: Lawrence Erlbaum Associates Xix, pp. 230.
3. Dekker, S., The field guide to understanding human error 2006, Aldershot, England; Burlington, VT: Ashgate xv, pp. 236.
4. Lutz, R.R. Analyzing software requirements errors in safety-critical, embedded systems in IEEE International Conference on Software Requirements, 1992.
5. Leveson, N., SafeWare: system safety and computers. 1995, Reading, Mass.: Addison-Wesley, Xvii, pp. 680.
6. Khaitan et al., "Design Techniques and Applications of Cyber Physical Systems: A Survey", IEEE Systems Journal, 2014.
7. Hancu, O.; Maties, V.; Balan, R.; Stan, S. (2007), Mechatronic approach for design and control of a hydraulic 3-dof parallel robot, The 18th International DAAAM Symposium, "Intelligent 'Manufacturing & Automation: Focus on Creativity, Responsibility and Ethics of Engineers".

8. Lee, E.A., Seshia, S.A.: Introduction to Embedded Systems - A Cyber-Physical Systems Approach, LeeSeshia.org, 2011.
9. Suh, S.C., Carbone, J.N., Eroglu, A.E.: Applied Cyber-Physical Systems, Springer 2014, Rad, Ciprian-Radu; Hancu, Olimpiu; Takacs, Ioana-Alexandra; Olteanu, Gheorghe (2015).
10. N.G. Leveson and C. S. Turner, an Investigation of the Therac-25 Accidents. IEEE Computer, pp. 18- 41, March 1987.
11. James Gleick. The New York Times Magazine 1st December 1996.
12. Leveson, N., Safe Ware: system safety and computers. 1995, Reading, Mass.: Addison-Wesley, xvii, pp. 680.
13. Hoffman, R.R. and L.G. Militello, Perspectives on Cognitive Task Analysis: Historical Origins and Modern Communities of Practice. 2012: Taylor & Francis.
14. Clarke, E.M., O. Grumberg, and D.A. Peled, Model Cheking. 1999: Mit Press.
15. Leveson, N., Engineering a safer world: systems thinking applied to safety Engineering systems. 2012, Cambridge, Mass.: MIT Press.
16. T. N. I. T. Research and D. Program, ―Different definition of cyber physical systems.‖, Available: http://www.nitrd.gov/about/blog/white_papers/ 16- Importance_of_Cyber-Physical_Systems.pdf.
17. Y. Bar-Yam, Dynamics of Complex Systems, ser. Studies in Nonlinearity. Westview Press, July 2003. Available: http://www.amazon.com/exec/ obidos/ISBN=0813341213/ newenglandcompleA.
18. D. Harel, ―Statecharts: A visual formalism for complex systems,‖ Sci. Comput. Program, vol. 8, pp. 231–274, June 1987. Available: http://dl.acm.org/citation.cfm?id=34884.34886.
19. Leveson, N., SafeWare: system safety and computers. 1995, Reading, Mass.: Addison-Wesley, xvii, pp. 680.
20. By Margaret V. Stringfellow, Nancy G. Leveson, Member IEEE, and Brandon D. Owens, Safety-Driven Design for Software-Intensive Aerospace and Automotive Systems, Vol. 0018-9219/$26.00 _2010 IEEE 98, No. 4, April 2010 Proceedings of the IEEE
21. Benzi, R., A. Sutera, and A. Vulpiani, The mechanism of stochastic resonance. Journal of Physics A: mathematical and general, 1999. 14(11): pp. L453
22. Anishchenko, V.S., M.A. Safonova, and L.O. Chua, Stochastic resonance in Chua‗s circuit driven by amplitude or frequency modulated signals, International Journal of Bifurcation and Chaos, 1994. 4(02): pp. 441-446
23. Wallace, R., D. Wallace, and H. Andrews, AIDS, tuberculosis, violent crime, and low birthweight in eight US metropolitan areas: public policy, stochastic resonance, and the regional diffusion of inner-city markers, Environment and Planning A, 1997. 29: pp: 525-555
24. T. Mukherjee, K. Venkatasubramanian, and S. K. S. Gupta, ―Performance modeling of critical event management for ubiquitous computing applications,‖ in MSWiM '06: Proceedings of the 9th ACM international symposium on Modeling analysis and simulation of wireless and mobile systems. New York, NY, USA: ACM, 2006, pp. 12–19.
25. K. Raja Kumar and P. Seetha Ramaiah, ―DSP and Microcontroller based Speech Processor for Auditory Prosthesis‖, Proceedings of the 14th International Conference on Advanced Computing and Communication, ADCOM-2006, Advanced Computing and Communications Society - Bangalore and National Institute of Technology, Surathkal, INDIA, Dec.20-23, 2006, pp. 518-522