Cyber-Physical Systems: Design Standards, Applications, Limitations, Challenges, and Future Perspectives

Rajkumar Palaniappan(✉)

Department of Mechatronics Engineering, College of Engineering, University of Technology Bahrain, Salmabad, Bahrain
r.palaniappan@utb.edu.bh

Abstract. A revolutionary technology that merges the real and virtual worlds is called a "cyber-physical system" (CPS). This article provides a comprehensive examination of CPS with an emphasis on its design principles, uses, constraints, difficulties, and potential. We examine the foundational ideas behind CPS design, talk about current design guidelines, and emphasize the value of these guidelines in guaranteeing safe and dependable operation. Additionally, we look at several fields where CPS is used and evaluate the restrictions and difficulties deployments of CPS encounter. Our discussion of probable future advancements and research trajectories in the area of cyber-physical systems concludes.

Keywords: CPS · Edge computing · AI · Machine learning · Automation · smart cities

1 Introduction

Cyber-Physical Systems (CPS) is a new paradigm that has emerged as a result of the convergence of computer science, information technology, and engineering in recent years. CPS is an innovative technology that combines the real and virtual worlds, enabling seamless communication between computer systems and real-world operations. Transportation, healthcare, manufacturing, and energy systems are just a few of the businesses and areas that this integration has the potential to alter [1].

The growing interdependence and connectivity of physical systems with computational and communication infrastructure led to the development of the CPS concept. Intelligent systems can now monitor, regulate, and optimize physical processes in real time because to advancements in sensor technology, communication and networking, and computational power. CPS bridges the gap between the physical and digital worlds through the use of data, algorithms, and networking, resulting in increased productivity, better decision-making, and new capabilities [2].

The ability of CPS to identify, assess, and react to changes in the physical world is what makes it unique. In order to get data from the physical environment, process it using

P. Pareek et al. (Eds.): IC4S 2024, LNICST 598, pp. 17–30, 2025.
https://doi.org/10.1007/978-3-031-77078-4_2

models and algorithms, and take the necessary steps to affect the physical processes, it depends on actuators, sensor networks, and computing devices. These systems can react rapidly to changing physical conditions and make sure that resources are used efficiently because they are made to function in real-time [3].

Experts from a variety of fields collaborate to design and create a CPS, including but not limited to data analytics, computer science, electrical engineering, mechanical engineering, and control systems. CPS design includes the design of hardware, software, communication protocols, security features, and human-machine interfaces. CPS design guidelines are crucial to ensuring these systems' dependability, safety, security, and interoperability [4].

The uses for CPS are numerous and varied. CPS can optimize the administration of urban infrastructure, such as transportation networks, electricity grids, and waste management systems, in smart cities. CPS can facilitate individualized care, efficient healthcare delivery, and remote patient monitoring in the healthcare industry. CPS also finds use in industrial automation, facilitating supply chain optimization, predictive maintenance, and sophisticated production techniques. Other areas where CPS is having a big impact include energy systems, smart homes, and driverless vehicles [5].

Despite the enormous potential of CPS, there are a number of issues and restrictions that must be resolved. Due to the complexity involved in integrating large-scale systems with heterogeneous components, CPS installations frequently have scalability problems. Safety and security considerations are of the utmost importance since CPS flaws or vulnerabilities could have devastating effects on physical systems and human life [6]. Due to the significant collecting and processing of personal data, privacy and ethical issues also surface. The design and operation of CPS are further complicated by resource limitations, such as those related to power and computing capacity.

Future prospects for CPS are positive. It is anticipated that cutting-edge technologies will significantly contribute to the development of CPS capabilities [7]. Examples include artificial intelligence, edge computing, blockchain, and quantum computing. CPS may be able to learn from and adapt to changing settings with the help of AI and machine learning algorithms, which will enhance system performance and decision-making [6]. By allowing for quicker response times and lowering network latency, edge computing can improve real-time processing capabilities. Blockchain technology's distributed consensus and tamper-proof data storage can improve the security and dependability of CPS. The use of quantum computing could help CPS by resolving challenging optimization and modeling issues [8].

In conclusion, cyber-physical systems are a revolutionary technology that fuses computing strength, connectedness, and intelligence with physical processes. CPS have the potential to change numerous sectors and domains because to their broad uses. To realize the full potential of CPS and direct its future course, it is essential to address the issues, ensure design standards, and take advantage of developing technologies [7].

2 Design Standards for Cyber-Physical Systems

Cyber-physical systems (CPS) interoperability, dependability, safety, and security are significantly influenced by design standards. The design, development, and deployment of CPS across several domains are made easier by the guidelines, best practices, and

specifications provided by these standards. The following are some significant CPS design guidelines:

2.1 IEC 62443

The International Electrotechnical Commission (IEC) established this standard, which focuses on the safety of industrial automation and control systems, including CPS. It offers a thorough methodology for putting security controls in place, managing security risks, and creating a safe architecture in CPS installations [9].

2.2 ISO 26262

The functional safety of automotive systems, including CPS utilized in automobiles, is especially addressed by this standard produced by the International Organization for Standardization (ISO). To protect the safety of passengers, drivers, and pedestrians, it provides recommendations for hazard analysis, risk assessment, and the design of safety-critical systems [10].

2.3 IEC 61508

The functional safety of electrical, electronic, and programmable electronic safety-related systems is the emphasis of this international standard. It offers a methodical approach to designing and verifying safety-critical systems, such as CPS, in a variety of industries, including transportation, process control, and energy [11].

2.4 IEEE 1686

The Standard for IP-Based Smart Object Networking (IETF 6LoWPAN) standard offers instructions for creating communication protocols for CPS that are low-power, low-cost, and low-bandwidth. Its main objective is to make it possible for CPS networks and devices to interact with one another seamlessly [12].

2.5 NIST Cybersecurity Framework

This framework, created by the National Institute of Standards and Technology (NIST), offers a collection of rules, recommendations, and benchmarks for handling cybersecurity risks in CPS. In CPS deployments, it provides a risk-based method for identifying, guarding against, spotting, responding to, and recovering from cybersecurity breaches [13].

2.6 OPC UA (Unified Architecture)

A machine-to-machine communication protocol called OPC UA is popular in CPS and industrial automation. It gives different CPS components, such as sensors, actuators, and control systems, a standardized framework for data sharing, security, and interoperability [14].

2.7 OMAC (Organization for Machine Automation and Control)

OMAC produces a number of standards pertaining to the development and management of CPS and other industrial automation and control systems. These guidelines concentrate on issues including machine integration, interoperability, and performance enhancement in manufacturing settings [15].

2.8 IETF (Internet Engineering Task Force) Standards

The IETF creates standards and protocols for web-based networking and communication, which frequently apply to CPS. For effective and dependable communication between devices in CPS, protocols like MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol) are frequently employed [16].

It is significant to note that different industries and geographical areas may adopt and apply these standards in different ways. New standards and recommendations can also appear as CPS technology develops to handle new requirements and issues. For the design and operation of safe and dependable cyber-physical systems, it's essential to stay current with the latest standards and best practices.

3 Applications of Cyber-Physical Systems

Applications for Cyber-Physical Systems (CPS) are numerous and spread across many industries. Here are a few famous CPS application examples:

3.1 Smart Cities

By linking diverse infrastructure systems, including those for transportation, electricity, water management, and waste management, and public safety, CPS technology is utilized to create smart cities. In order to optimize resource allocation, improve traffic management, increase energy efficiency, and improve overall urban sustainability, CPS provides real-time monitoring, data analysis, and decision-making [16, 17].

3.2 Industrial Automation

Industrial automation, commonly referred to as Industry 4.0 or the Industrial Internet of Things (IIoT), is extremely important. CPS makes it possible to monitor, regulate, and optimize industrial processes in real-time by fusing physical equipment with intelligent software systems. It boosts efficiency in manufacturing, logistics, and supply chain management as well as worker safety, quality control, and predictive maintenance [14, 18].

3.3 Autonomous Vehicles

Autonomous car development depends heavily on CPS technology. To achieve self-driving capabilities, CPS enables the integration of sensors, control systems, communication networks, and artificial intelligence algorithms. In order to ensure safe and effective mobility, it enables cars to sense their environment, make decisions, and interact with other vehicles, infrastructure, and pedestrians [1, 7].

3.4 Healthcare Systems

By enabling remote patient monitoring, telemedicine, and intelligent healthcare systems, CPS is transforming healthcare. Wearable sensors, medical equipment, electronic health records, and communication networks are all integrated by CPS technology to provide real-time patient health monitoring, individualized care, and early disease identification. It improves patient outcomes, streamlines the delivery of healthcare, and lowers hospital stays [19, 20].

3.5 Energy Management

To maximize energy production, distribution, and consumption, smart grid systems use CPS. CPS makes it possible to integrate renewable energy sources, monitor energy infrastructure in real-time, and implement demand response systems. It improves grid dependability, energy efficiency, and allows for the efficient integration of dispersed energy resources [20].

3.6 Environmental Monitoring

CPS is used in environmental monitoring systems to track and manage weather, air quality, water quality, and natural resource availability. CPS allows real-time monitoring, early warning systems, and adaptive management techniques for environmental conservation and disaster management by integrating sensor networks, data analytics, and decision support systems [20].

3.7 Agriculture and Precision Farming

Precision farming uses CPS to enhance agricultural techniques. CPS offers real-time monitoring of soil conditions, crop health, and irrigation systems by integrating sensor networks, drones, autonomous vehicles, and data analytics. It makes it possible to apply fertilizers, herbicides, and water supplies precisely, improving crop yields, cutting expenses, and protecting the environment [20].

3.8 Smart Homes and Buildings

Smart houses and buildings use CPS technology to improve comfort, security, and energy efficiency. To optimize lighting, heating, ventilation, and air conditioning (HVAC) systems, CPS enables the integration of sensors, actuators, and intelligent control systems. Additionally, it makes smart home automation, energy management, and security systems possible for better living conditions and lower energy usage [19, 20].

These are but a few instances of the numerous uses for which cyber-physical systems are put to use. Various sectors and disciplines could be transformed by CPS technology, enhancing productivity, sustainability, and quality of life. As CPS develops, we may anticipate seeing its application in new fields as it addresses complicated problems and generates creative solutions.

4 Limitations of Cyber-Physical Systems

While Cyber-Physical Systems (CPS) provide many advantages, there are also some restrictions that must be taken into account. The following are some major drawbacks of CPS:

4.1 Complexity and Design Challenges

Sensors, actuators, communication networks, and control systems are just a few examples of the various components that are frequently integrated into CPS [21–23]. The complexity of CPS can be difficult to design and manage since it necessitates knowledge across many areas and careful consideration of system interactions, dependencies, and fault tolerance.

4.2 Scalability Issues

It can be challenging to scale up CPS to manage widespread deployments. Managing the communication, coordination, and data processing is harder when there are more devices, sensors, and actuators. It might be difficult to maintain performance, stability, and real-time responsiveness while ensuring scalability [20].

4.3 Dependence on Communication Networks

For data interchange and component coordination, CPS strongly rely on communication networks. The functionality of CPS may be impacted by any network infrastructure outages or breakdowns. It becomes essential to ensure dependable and strong network connectivity, especially for mission-critical applications like healthcare, transportation, or industrial control [21].

4.4 Safety and Security Risks

There are hazards to safety and security when physical processes and digital technologies are combined. System failures, illegal access, data breaches, and physical injury are just a few of the hazards that could result from CPS vulnerabilities. Strong cybersecurity safeguards, secure communication protocols, and adherence to industry best practices in system design and operation are all necessary to ensure the safety and security of CPS [23].

4.5 Legacy System Compatibility

It can be difficult to integrate CPS with legacy systems already in place. Integrating legacy systems seamlessly can be difficult and time-consuming since they may use various communication protocols, data formats, and operational needs. It can be expensive and complicated to retrofit current infrastructure to provide CPS capabilities [24].

4.6 Privacy and Ethical Concerns

Large volumes of personal data are frequently collected and processed by CPS, raising privacy issues. Important issues that must be addressed in CPS deployments include guaranteeing privacy protection, obtaining informed consent, and addressing ethical issues linked to data utilization, transparency, and accountability [24, 25].

4.7 Cost and Resource Constraints

The cost of hardware, software development, infrastructure updates, and maintenance can all be significant when implementing CPS. Particularly in contexts with tight resources, creating and running effective CPS systems can be difficult due to limited resources including electricity, bandwidth, and compute capability [21, 22].

4.8 Interoperability and Standardization

The seamless integration and broad acceptance of CPS across several areas may be hampered by the absence of defined protocols, interfaces, and interoperability frameworks. To make it easier to integrate CPS components from many vendors and to guarantee compatibility and scalability, interoperability must be ensured [22].

4.9 Regulatory and Legal Challenges

The creation of rules and regulatory frameworks frequently lags behind the quick growth of CPS technology. Dealing with legal and regulatory issues, such as responsibility, data ownership, and compliance standards, can be difficult and differ between different disciplines and geographical areas [20].

4.10 Human Factors

Human factors like acceptance, usability, and user experience must be considered by CPS. Making CPS systems that are user-friendly, intuitive, and sensitive to human needs and preferences can be challenging. User-centered design techniques, training programs, and human-machine interfaces are essential for the effective adoption and deployment of CPS [18].

Despite these shortcomings, ongoing research and development is being done to find ways to get around them and improve the capabilities, dependability, and usability of CPS. By getting beyond these limitations, CPS will be used more frequently and implemented into more fields.

5 Challenges in Cyber-Physical Systems

A number of issues need to be resolved in order for the deployment and operation of Cyber-Physical Systems (CPS) to be successful. These challenges include:

5.1 Interdisciplinary Collaboration

For the development of CPS, cooperation between experts from several domains is required, including computer science, engineering, control systems, and domain-specific knowledge. To properly bridge the gap between these many domains of knowledge and combine them into a functional system might be challenging [15].

5.2 System Complexity

Numerous heterogeneous components, including sensors, actuators, communication networks, and control systems, are frequently integrated in CPS. It can be quite difficult to manage the intricacy of many interrelated parts, ensure their compatibility, and keep the system stable [13].

5.3 Scalability

Large-scale CPS deployment can be challenging. It can be difficult to scale up CPS systems to manage more devices, sensors, and actuators while preserving performance, dependability, and real-time responsiveness [16].

5.4 Safety and Security

Because CPS deployments are integrated with physical processes, safety and security issues are raised. It is essential to guarantee the security of physical systems, connected networks, and data. Risks include system failures, unauthorized access, data breaches, and even bodily injury could result from vulnerabilities in CPS [14].

5.5 Real-Time Responsiveness

To successfully track, assess, and react to dynamic changes in the physical environment, CPS must function in real-time. It can be difficult to achieve low latency transmission, real-time data processing, and prompt decision-making, particularly in large-scale CPS implementations or when computational resources are few [20].

5.6 Privacy and Ethical Implications

Large volumes of personal data are routinely collected and processed as part of CPS. The adoption of CPS faces significant hurdles, including ensuring privacy protection, obtaining informed consent, and addressing ethical issues linked to data utilization, openness, and accountability [24].

5.7 Legacy System Integration

Integration of existing legacy systems, which may have different communication protocols, data formats, and operating needs, is a common task for CPS installations [21]. To ensure compatibility and a smooth transition, integrating CPS with legacy infrastructure can be challenging and requires careful preparation.

5.8 Standards and Regulations

It is difficult to create comprehensive, broadly agreed norms and regulations for CPS due to its dynamic nature [18]. The seamless integration and broad acceptance of CPS across several areas may be hampered by the lack of defined protocols, interfaces, and interoperability frameworks.

5.9 Cost and Resource Constraints

The cost of hardware, software development, infrastructure updates, and maintenance can all be significant when implementing CPS [17]. Designing and running CPS systems efficiently can also be difficult due to limited resources, such as electricity, bandwidth, and computational capability.

5.10 Training and Workforce Skills

A competent staff with knowledge in a variety of fields, such as software engineering, control systems, networking, and data analytics, is necessary for the design, development, and operation of CPS [26]. A challenge is ensuring the availability of a skilled staff and offering ongoing training to stay up with developing technologies.

A comprehensive strategy encompassing research, development, and cooperation between regulatory agencies, academia, and industry is needed to address these difficulties. To ensure the safe, secure, and effective application of CPS in many areas, it is necessary to build standardized frameworks, security and privacy safeguards, training programs, and standards.

6 Future Perspectives and Emerging Trends

6.1 Artificial Intelligence and Machine Learning in CPS

In the future of CPS, it's anticipated that the combination of artificial intelligence (AI) and machine learning (ML) techniques would be crucial [26, 27]. The intelligence and autonomy of CPS can be improved by AI and ML algorithms, allowing them to learn from data, make wise judgments, and adapt to changing situations. In CPS implementations, these technologies can boost system efficiency, enhance resource allocation, and enable predictive maintenance.

6.2 Edge Computing and Fog Computing

The real-time processing and low-latency requirements of CPS may be difficult for conventional cloud-based architectures to achieve [28]. Emerging paradigms like edge computing and fog computing move computation and data storage closer to the network's edge, enabling quicker response times and lowering reliance on centralized cloud infrastructure. These distributed computing models allow for real-time data processing, analytics, and decision-making at the edge devices themselves, making them ideal for CPS applications.

6.3 Blockchain Technology for CPS

Blockchain technology shows potential for boosting the security, trust, and transparency of CPS since it offers a decentralized and tamper-proof ledger [29]. CPS installations can guarantee safe and auditable data exchanges, decentralized access control, and consensus procedures by utilizing blockchain. Particularly in industries like supply chain management, healthcare, and smart grid systems, this technology offers the ability to address security and privacy issues in CPS.

6.4 Quantum Computing and CPS

With the potential to increase computing power and address challenging optimization and modeling issues, quantum computing is a young field [30]. Quantum computing in CPS can lead to more effective resource management, sophisticated optimization techniques, and improved physical process simulation. To fully utilize quantum computing for CPS applications, additional study and development are still required as it is still in its infancy.

6.5 Socio-economic Impacts of CPS

There will be major socio-economic effects to take into account as CPS spreads across a variety of fields. The widespread implementation of CPS may result in adjustments to economic models, labor needs, and job responsibilities [27]. To promote a balanced and inclusive deployment of these technologies, it is essential to comprehend and address the potential effects of CPS on social equity, employment, privacy, and ethics.

6.6 Human-Centric CPS Design

The importance of user experience and human connection increases as CPS become more prevalent. A major goal will be to create CPS systems that are user-friendly, intuitive, and responsive to human requirements and preferences [5]. The future of CPS will be greatly influenced by user-centered design methodologies, usability research, and human-machine interfaces.

6.7 Security and Privacy Enhancements

The security and privacy of these systems will continue to be a primary focus due to the growing integration of CPS into sensitive and vital infrastructure. Upgrading security mechanisms, putting in place strong encryption methods, upgrading authentication and access control, and resolving privacy issues with data collecting, storage, and sharing will be the main goals of future advancements [24].

6.8 Interoperability Standards and Ecosystems

The necessity of interoperability standards and ecosystems is essential as CPS installations cover numerous sectors and incorporate a variety of components. In order to facilitate smooth integration and collaboration between various CPS components and

systems, future developments will concentrate on providing standardized interfaces, communication protocols, and data formats [21].

In conclusion, CPS has a bright future as new technologies continue to shape the way these systems are designed. CPS capabilities will be advanced via the use of artificial intelligence, edge computing, blockchain, quantum computing, and human-centered design. In order to fully utilize CPS and ensure its widespread acceptance across multiple domains, it will be crucial to address security, privacy, interoperability, and socio-economic consequences.

7 Research Gap in Cyber-Physical Systems:

Even though Cyber-Physical Systems (CPS) have attracted a lot of interest and academic effort, there are still a number of gaps that demand more study. Several significant CPS research gaps include:

7.1 Security and Privacy

The difficulties with security and privacy in CPS continue to be a significant research gap. CPS are interconnected and entail the sharing of sensitive data, thus it is essential to have strong security measures in place and to preserve privacy. Future research should concentrate on creating sophisticated security protocols, authentication systems, and CPS-specific privacy-preserving methods. Further research is needed in the areas of examining the effects of adversarial attacks and creating resilient CPS systems.

7.2 Interoperability and Standardization

For smooth integration and cooperation, there must be interoperability across various CPS components and systems. Due to the diversity of CPS technology and standards, interoperability is still difficult to achieve. In order to provide uniform communication protocols, data exchange formats, and interoperability frameworks that facilitate smooth integration and information sharing across many CPS domains, more research is required.

7.3 Scalability and Resilience

Large-scale systems with a lot of interconnected devices and sensors are frequently used in CPS installations. There is a research need in ensuring scalability and resilience in such intricate CPS designs. Future research should concentrate on creating fault-tolerant systems, effective resource management strategies, and scalable CPS architectures to successfully manage system expansion, dynamic changes, and future disruptions.

7.4 Human-Centric CPS Design

Although CPS technology is developing quickly, human-centered design issues must be addressed. There is still a need for study on user requirements, human factors, and human-machine interaction in CPS contexts. In order to enhance user experience, usability, and acceptance of CPS solutions, future research should investigate user-centric design methodologies, user-friendly interfaces, and efficient training techniques.

7.5 Ethical and Legal Considerations

CPS's ethical and legal ramifications remain mostly unknown. It is vital to address ethical difficulties, data governance, liability concerns, and the regulatory framework around CPS installations as CPS systems spread and have a substantial impact on society. To create ethical standards, legal frameworks, and policy recommendations that assure the accountable and responsible use of CPS technology, more study is required.

7.6 Data Analytics and Decision-Making

Large-scale data generation by CPS necessitates effective data analytics methods for quick decision-making. A research gap involves investigating CPS-specific machine learning methods, advanced data analytics algorithms, and decision support systems. Further research is needed to develop intelligent algorithms that can handle and evaluate CPS data streams in real-time, extract useful insights, and assist autonomous decision-making processes.

7.7 Socio-economic Impact

Policymakers and business stakeholders must comprehend the socioeconomic effects of CPS. Further study is needed to evaluate the economic gains, effects on the labor market, and societal effects of adopting and implementing CPS. It is possible to promote fair and inclusive adoption of CPS technology by examining the potential risks, inequities, and social ramifications of CPS deployment in various circumstances.

By filling in these research gaps, the field of CPS will advance, making it possible to design secure, effective, and human-centric CPS solutions while addressing the moral, legal, and social issues that come up during their implementation.

8 Conclusion

In summary, this research study has offered a thorough examination of Cyber-Physical Systems (CPS), a game-changing technology that connects the real and virtual worlds. The paper examines a number of CPS-related topics, such as design guidelines, applications, constraints, difficulties, and hopes for the future. The paper places a strong emphasis on the value of design criteria in guaranteeing the safe and dependable operation of CPS. The paper illustrates the crucial role foundational principles and current design standards play in enabling robust and reliable CPS deployments by exploring these concepts in depth. For researchers, practitioners, and policymakers involved in the creation and application of CPS, this understanding is essential. The essay also looks into the many different fields in which CPS is used. The CPS exhibits its potential to change a number of industries, boosting productivity, sustainability, and quality of life. These industries range from smart cities and industrial automation to healthcare systems and driverless vehicles. The research offers insightful information about the practical application of CPS technologies by examining various applications. The article also discusses the restrictions and difficulties that CPS deployments face. The study's main

issues are scalability, complexity, interoperability, safety, and security. Stakeholders must be aware of these difficulties in order to proactively address them and guarantee the effective application of CPS solutions. The study concludes by examining CPS's prospective developments and future research directions. Advancements in technologies like artificial intelligence, communication networks, and edge computing have the potential to improve CPS capabilities as it continues to develop. The study emphasizes the value of continual investigation and cooperation in order to overcome the problems found and realize the full potential of CPS. In conclusion, this research study advances understanding of CPS by in-depth analysis of its design principles, applications, constraints, difficulties, and opportunities. The study intends to inform and inspire new developments in the field of cyber-physical systems by providing light on these critical features, ultimately spurring innovation and societal change.

References

1. Hamdan, S., Almajali, S., Ayyash, M., Bany Salameh, H., Jararweh, Y.: An intelligent edge-enabled distributed multi-task learning architecture for large-scale IoT-based cyber–physical systems. Simul. Model. Pract. Theory **122**, 102685 (2023)
2. Napoleone, A., Negri, E., Macchi, M., Pozzetti, A.: How the technologies underlying cyber-physical systems support the reconfigurability capability in manufacturing: a literature review. Int. J. Prod. Res. **61**, 3122–3144 (2023)
3. Dalal, S., et al.: Optimized LightGBM model for security and privacy issues in cyber-physical systems. Trans. Emerg. Telecommun. Technol. **34**, e4771 (2023)
4. Alguliyev, R., Imamverdiyev, Y., Sukhostat, L.: Cyber-physical systems and their security issues. Comput. Ind. **100**, 212–223 (2018)
5. Wang, B., Zheng, P., Yin, Y., Shih, A., Wang, L.: Toward human-centric smart manufacturing: a human-cyber-physical systems (HCPS) perspective. J. Manuf. Syst. **63**, 471–490 (2022)
6. Jain, D.K., Neelakandan, S., Veeramani, T., Bhatia, S., Memon, F.H.: Design of fuzzy logic based energy management and traffic predictive model for cyber physical systems. Comput. Electr. Eng. **102**, 108135 (2022)
7. Lee, J., Kundu, P.: Integrated cyber-physical systems and industrial metaverse for remote manufacturing. Manuf. Lett. **34**, 12–15 (2022). https://doi.org/10.1016/j.mfglet.2022.08.012
8. Chen, L., Tang, S., Balasubramanian, V., Xia, J., Zhou, F., Fan, L.: Physical-layer security based mobile edge computing for emerging cyber physical systems. Comput. Commun. **194**, 180–188 (2022)
9. Shaaban, A.M., Chlup, S., El-Araby, N., Schmittner, C.: Towards optimized security attributes for IoT devices in smart agriculture based on the IEC 62443 security standard. Appl. Sci. **12** (2022)
10. Sini, J., Violante, M., Tronci, F.: A novel ISO 26262-compliant test bench to assess the diagnostic coverage of software hardening techniques against digital components random hardware failures. Electronics (Basel) **11** (2022)
11. Lyu, X., Ding, Y., Yang, S.-H.: Safety and security risk assessment in cyber-physical systems. IET Cyber-Phys. Syst. Theory Appl. **4**, 221–232 (2019)
12. Shaaban, A.M., Gruber, T., Schmittner, C.: Ontology-based security tool for critical cyber-physical systems. In: Proceedings of the 23rd International Systems and Software Product Line Conference – Volume B, pp. 207–210. Association for Computing Machinery, New York, NY, USA (2019)
13. Gordon, L.A., Loeb, M.P., Zhou, L.: Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. J Cybersecur. **6**, tyaa005 (2020)

14. Lin, H.-I., Hwang, Y.-C.: Integration of robot and IIoT over the OPC unified architecture. In: 2019 International Automatic Control Conference (CACS), pp. 1–6 (2019)
15. Zhao, R., et al.: Digital twin-driven cyber-physical system for autonomously controlling of micro punching system. IEEE Access **7**, 9459–9469 (2019)
16. Cath, C.: The technology we choose to create: Human rights advocacy in the Internet Engineering Task Force. Telecomm. Policy **45**, 102144 (2021)
17. Qi, Y., et al.: Cybersecurity knowledge graph enabled attack chain detection for cyber-physical systems. Comput. Electr. Eng. **108**, 108660 (2023)
18. El-Kady, A.H., Halim, S., El-Halwagi, M.M., Khan, F.: Analysis of safety and security challenges and opportunities related to cyber-physical systems. Process Saf. Environ. Prot. **173**, 384–413 (2023)
19. Priyadarshini, I., Sharma, R., Bhatt, D., Al-Numay, M.: Human activity recognition in cyber-physical systems using optimized machine learning techniques. Cluster Comput. **26**, 2199–2215 (2023)
20. Hamzah, M., et al.: Distributed control of cyber physical system on various domains: a critical review. Systems **11** (2023)
21. Yaacoub, J.-P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A., Malli, M.: Cyber-physical systems security: limitations, issues and future trends. Microprocess. Microsyst. **77**, 103201 (2020)
22. Pombo, I., Godino, L., Sánchez, J.A., Lizarralde, R.: Expectations and limitations of cyber-physical systems (CPS) for advanced manufacturing: a view from the grinding industry. Future Internet **12** (2020)
23. Darwish, A., Hassanien, A.E.: Cyber physical systems design, methodology, and integration: the current status and future outlook. J. Ambient. Intell. Humaniz. Comput. **9**, 1541–1556 (2018)
24. García-Valls, M., Calva-Urrego, C., de la Puente, J.A., Alonso, A.: Adjusting middleware knobs to assess scalability limits of distributed cyber-physical systems. Comput Stand Interfaces. **51**, 95–103 (2017)
25. Törngren, M., Grogan, P.T.: How to deal with the complexity of future cyber-physical systems? Designs (Basel) **2** (2018)
26. Latif, S.A., et al.: AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. Comput. Commun. **181**, 274–283 (2022)
27. Lv, Z., Chen, D., Lou, R., Alazab, A.: Artificial intelligence for securing industrial-based cyber–physical systems. Futur. Gener. Comput. Syst. **117**, 291–298 (2021)
28. Alwakeel, A.M.: An overview of fog computing and edge computing security and privacy issues. Sensors **21** (2021)
29. Verma, A., et al.: Blockchain for industry 5.0: vision, opportunities, key enablers, and future directions. IEEE Access **10**, 69160–69199 (2022)
30. Canagasabey, A., et al.: A comparison of Michelson and Mach-Zehnder interferometers for laser linewidth measurements. In: Proceedings of the International Quantum Electronics Conference and Conference on Lasers and Electro-Optics Pacific Rim 2011, p. C428. Optica Publishing Group, Sydney (2011)