**Issues in Information Systems**
Volume 26, Issue 4, pp. 155-167, 2025

DOI: https://doi.org/10.48009/4_iis_2025_114

# Classification and challenges of cyber-physical systems projects

**Nader Mohamed,** Pennsylvania Western University, mohamed@pennwest.edu
**Jameela Al-Jaroodi,** Robert Morris University, aljaroodi@rmu.edu

## Abstract

Advanced technologies like Cyber-Physical Systems (CPS) are poised to provide valuable opportunities to support smart interactions between the physical world (machines, people and environments) and the cyber worlds. They provide smart capabilities to enhance the physical world. These include improving reliability, quality, safety, health, security, efficiency, operational costs, and maintenance of physical systems or environments. CPS are designed using distributed hardware, software, and network components embedded in physical systems or attached to humans. Many CPS applications are being developed, implemented, and deployed by several organizations for several purposes. However, the development of most of these applications is extremely difficult because this involves different components and has hard requirements. These hard requirements make managing cyber-physical system projects challenging and very difficult. Project managers need to understand the challenges of different CPS to be able to successfully plan, complete, and deliver their projects with less difficulty. As CPS applications can have a wide range of usage and properties, it is necessary to identify common grounds among different types of these applications. Therefore, in this paper we provide a classification for these projects based on the type of network they use. We identify five categories: Nanoscale CPS (NCPS), Body Area CPS (BCPS), Local Area CPS (LCPS), Mobile Ad Hoc CPS (MCPS), and Wide Area CPS (WCPS). This classification offers a better way for project managers to understand the common complexities and possible solution directions for each category.

**Keywords**: cyber-physical systems, CPS projects, senor networks, smart applications, project management

## Introduction

Achieving effective and efficient integration and improved interactions between the physical world and the cyber world is possible using Cyber-physical Systems (CPS). CPS is a promising technology that can deliver various smart capabilities to different physical/cyber applications in diverse domains. CPS can be used to add automation capabilities in manufacturing processes for enhanced productivity by helping improve the efficiency, accuracy, safety, and reliability of the physical system's operations. In healthcare applications it can provide useful real-time interactions for patients and healthcare professionals. CPS can also support and optimize the operations in commercial and residential buildings to improve energy efficiency and living/working conditions. In transportation systems it can help enhance safety and efficiency and optimize traffic flows. CPS utilize and connect different technologies, features, and ideas from networks, distributed systems, sensors, embedded systems, software, and hardware such as microcontrollers and sensors; in addition to other fields such as mechanical, biomedical, industrial, civil,

and electrical engineering to deliver value-added features to applications in the physical world (Hoenig et al., 2024)

CPSs add many smart features and improvements for physical systems and processes, yet the development of CPS systems requires the incorporation of various heterogeneous components that will cooperate in several ways and will have multiple functionalities is tremendously complex. CPS will link different hardware components such as sensors, actuators, and microcontrollers to physical systems and use distributed software and smart algorithms to control these systems. The distribution and heterogeneity of the devices and their links with the physical components increase the complexity of the design, development, deployment and operations of CPS and make the entire process more challenging. Because CPS applications are important and their development processes are complex, enormous research was invested to investigate the different issues. These include security, safety, scalability, reliability, performance, quality, and development methodologies (Al-Jaroodi and Mohamed, 2018; Mohamed et al., 2020). The rapid growth in attention to CPS in the academic/research communities and in industry highlights the significance of the field and its importance for applications in different domains.

Due to the advantages of CPS, many organizations have started to utilize such systems for different applications (Gunes et al., 2014; Shi, et al., 2011; Wu et al., 2011). However, managing CPS projects is extremely difficult. This is due to their heterogeneity, complexity, hard requirements, and uniqueness of each project. All these and other challenges make managing such projects extremely difficult. It is difficult to manage scope, schedule, cost, quality, resources, risks, and integration in these projects. There were limited research efforts investigating the project management issues of developing, implementing, and deploying CPS applications. Palma (Palma, 2016) investigated project management best practices for developing cyber-physical systems. Palma et al. (Palma et al., 2018) proposed a new approach CPS-PMBOK which is based on the Project Management Institute's PMBOK body of knowledge for managing CPS projects. The focus of the approach is on the integration, scope, stakeholder, and human resource knowledge areas. Ivo et al. (Ivo et al., 2023) investigated the conceptual analysis issues of cyber-physical systems projects. Luedeke et al. (Luedeke et al., 2018) presented an agile approach for cyber-physical products. Unlike other research, this paper focuses on identifying the challenges of different CPS projects.

To offer a better way for project managers to identify and understand the challenges of CPS projects, we classify CPS projects into different categories. Our research methodology of this work is based on investigating different CPS applications and categorizing them into different groups based on their challenges. Although each of these applications has its own complexities, we classified these applications into different categories to simplify the process of identifying common complexities and issues in each category such that solution directions to the issues imposed on the applications in each category can be identified. We classify CPS applications into five categories based on the network used for the CPS applications. We determined that some of the challenges and capabilities are highly affected by the type of network being used and thus the categories were aligned with these network types. The categories are Nanoscale CPS (NCPS), Body Area CPS (BCPS), Local Area CPS (LCPS), Mobile Ad Hoc CPS (MCPS), and Wide Area CPS (WCPS). This classification offers a better way for project managers to understand the common complexities and challenges and possible solution directions for each category. The proposed classification can help project managers to easily identify the challenges and requirements of CPS projects. None of the previous research efforts have been dedicated to this direction of classifying CPS applications. By providing this classification we aim to help understand the common issues of each category and attempt to offer some ways to adapt some of the already developed solutions in the network and distributed systems fields for CPS. We also provide some discussion about advanced emerging enabling technologies for CPS applications and their potential advantages.

In the following sections we first offer some background information about CPS. Then, we discuss our research methodology and our classification of the CPS applications. This classification can help project managers to identify the challenges of their CPS projects. Then, we discuss some results, requirements, and opportunities for CPS applications. Finally, we give our concluding remarks and future directions.

## Background

CPS are considered embedded systems designed with the idea of having direct and continuous interactions between a physical system and its software counterpart (Hoenig et al., 2024). They are being used at an increasing pace in different application areas within physical domains like energy, manufacturing, healthcare, infrastructures, transportation, aerospace, appliances and even entertainment. A big sector of CPS applications is designed to support intelligent and context-aware mission-critical applications (Al-Jaroodi and Mohamed, 2018). The monitoring and control capabilities and the added smart components are used to achieve the predefined goals of the application domain of the CPS. Unlike other types of embedded systems, CPS are multi-layered systems that include heterogeneous distributed components and processing capabilities. Microcontrollers, sensors and actuators are some examples of embedded devices integrated into CPS. These devices are connected via wired or wireless networks, and they are tightly coupled with their physical environment.

Because CPS are embedded in physical systems via intelligent mechanisms and processes, they enable effective and smart interactions between the physical and cyber elements. The control tasks are divided into three main tasks:

1. Monitoring the physical system using sensors attached to the physical elements.
2. Making decisions using smart cyber capabilities to control/manage the physical system to meet the predefined objectives.
3. Executing actions using actuators connected to the physical elements.

These three tasks are linked in a feedback loop known as the closed-loop control (see Figure 1). This allows the CPS to offer monitoring and control functions to meet the objectives. These tasks and the closed-loop control create the base unit of a basic CPS. Beyond this, various CPS will include the features needed by the specific application domain they serve. Therefore, the functions of CPS are more elaborate and have more complex requirements, thus posing more technical challenges.

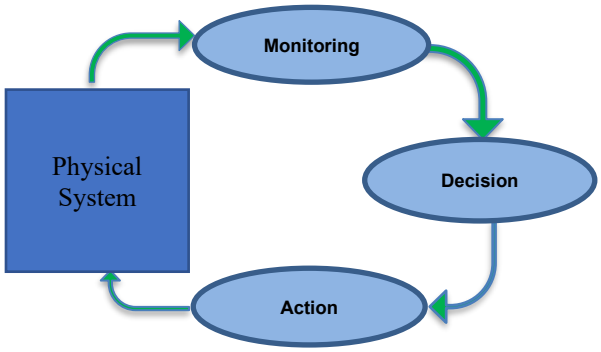


**Figure 1. Closed-loop control steps of CPS.**

In general, we can organize the components of CPS in five layers as illustrated in Figure 2.

- **Physical World Layer**: includes the physical system/components like buildings, aircraft, vehicles, or humans. It could also include intangible physical conditions such as temperature, sound levels, humidity, smells etc.
- **Observation and Action Layer**: this includes the sensors used to monitor the systems/components. This also includes the actuators used to initiate actions upon the systems/components in response to decisions received from the cyber part or to specific monitored conditions.
- **Network Layer**: the distributed components of CPS communicate using networks. The network may be wired, wireless, or both and vary in scale from nanoscale network to a global wide area network. The choice of network is sometimes determined by the CPS applications and their expected operational areas. The network layer will provide the needed mechanisms for the CPS to interact with the sensors and actuators as a system rather than individual components. Examples of the mechanisms are addressing, routing, and forwarding schemes to provide efficient communication and integration.
- **Control Cyber Layer**: this is a software component of the CPS that collects status information about the cyber system/components from the sensor and makes instantaneous decisions to meet given objectives. The decisions will issue action steps to the actuators. This layer may be centralized; thus, it runs on one microcontroller or computer works well for small-scale CPS applications. It is also possible to implement the layer as a distributed software hosted across multiple microcontrollers or computers. This works better for large-scale CPS applications to provide wider access and capabilities across the entire CPS. This approach is more complex, yet more reliable and allows for better scalability and support for real-time functions.
- **Smart Cyber Layer**: this is also a software component geared towards offering advanced features and smart systems capabilities. It is designed to create and manage a knowledgebase about the physical systems and the CPS operating on it. It is considered a sophisticated addition that helps bring smartness and optimization for the CPS. The knowledgebase is constructed and expanded over time using collected sensor data, decisions made, actuator actions and other factors contributing to the operations of the CPS. The information is organized and refined to become the supporting part of smart features like prediction models, optimizations and smart components. This layer may include advanced functions in data mining and machine learning.

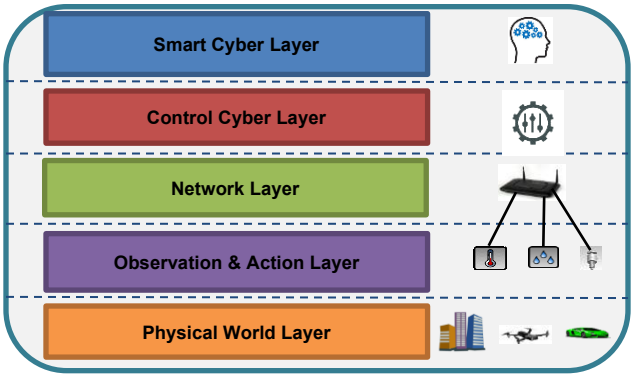


**Figure 2. CPS layers**.

## Methodology

One of the primary challenges in developing CPS applications is that each application has its own different set of requirements, and objectives. At the same time, they need skills from different fields like civil engineering, electrical engineering, mechanical engineering, medicine and healthcare among many others as each CPS could serve diverse domains (Al-Jaroodi and Mohamed, 2018). This makes CPS applications look like they are completely different from each other. Consequently, there are less efforts in developing tools, special development environments, and reusability modules for CPS applications compared to other more conventional systems. This leads to having to develop this type of application from scratch, which makes the development process more difficult, costly and time consuming. In addition, since such applications require many cyber and physical components, testing and validation efforts are usually hard to plan and carry out. Thus, the development process is associated with high risks as the produced system can have bugs or faults that are not discovered during testing. Fortunately, a closer look at CPS applications reveals that there are some similarities and common characteristics regardless of the application domain they target. Some characteristics and issues are common among all CPS applications, yet each will have a certain level of emphasis and importance in different applications. Some of these common issues are heterogeneity as CPSs are constructed using heterogeneous devices and systems for heterogeneous environment, and the need for real-time, security, context awareness supports. In addition, most CPS require using some services offered by other systems such as cloud and fog platforms, local servers or storage systems, and senor systems and networks.

These common issues may occur at different levels and importance when considering different types of CPS application domains. Different types of CPS applications will also have a distinct set of characteristics and issues that are only visible for those applications. To help simplify the process, we found it necessary to create some form of categorization that group CPS applications based on some commonalities within each group. We propose a classification for CPS that groups CPS applications based on specific criteria and identify the common characteristics and issues facing them in each category. This helps lead the way towards common solutions for these issues for all CPS applications or within a specific category rather than handling these issues repeatedly for every CPS application.

CPS can be considered as networked systems, so we opted to adopt the network classification to define the CPS categories. There are three reasons for adopting this type of classification. First, instead of inventing a completely new and unknown classification that is difficult to explain and justify, we mapped to a well-known classification. Networks are mainly classified as nanoscale networks, body-area networks, local-area networks, mobile ad hoc networks, and wide-area networks. Each of these networks has its own characteristics and issues. At the same time, there are many proposed solutions to solve and deal with these issues. We can easily map CPS applications to these network categories as they share similar categorization issues depending on their size and network use. Although there are other types of networks such as personal-area networks and metropolitan-area networks, we will not use them in our classification as these could easily fit within one or more of the five main categories. For example, a personal-area network can be part of a body-area network while metropolitan area networks can be part of wide-area networks. The second reason, although there are similarities across the different categories; the details, reasoning, and characteristics of these issues can be different from one category to another. For example, the security issues and solutions in body-area networks are different from the security issues and solutions in wide-area networks. However, all applications of body-area networks can have the same or very similar security concerns and similar solutions can be used to solve them. The third reason is that instead of completely inventing new solutions to solve CPS issues, mapping helps in some cases to adapt already developed and proven solutions in networks and distributed systems for CPS.

## CPS Classification

Following in step with the network categories, we classify CPS applications into five categories: Nanoscale NCPS (Nanoscale Cyber-Physical Systems), BCPS (Body Area Cyber-Physical Systems), LCPS (Local Area Cyber-Physical Systems), MCPS (Mobile Ad Hoc Cyber-Physical Systems), and WCPS (Wide Area Cyber-Physical Systems). Each kind has certain well-known CPS applications and shared issues. As we classify the CPS by their geographic space coverage and network, we will notice that each kind will have its own issues due to its nature of operations and characteristics. Yet, with different levels of emphasis, all categories also share the common concerns and issues identified for all CPS.

**Nanoscale Cyber-Physical Systems (NCPS):**
NCPS systems are implemented and operated at the nanoscale level. They tie nano sensors, nanoactuators, and other nanocomponents utilizing nanonetworks. Nanorobotics, for example, are used to remove cancer cells, to deliver targeted drugs, and to control diabetes. The main issues here are:

- **Reliability and safety**: Most applications of nanoscale CPS are embedded in other systems, environments, or human bodies. As a result, their operations CPS must be reliable and safe. They should be designed to achieve their missions without negatively affecting the associated environment.
- **Accuracy**: Given the extremely miniature size of these systems and their operational targets, they must operate within very limited margins of errors to achieve their goals.
- **Limited resources**: Nanoscale CPS are very small with limited resources including limited power, processing and storage. Therefore, it is important to approach the solutions for their issues in a suitable small-scale approach.

**Body Area Cyber-Physical Systems (BCPS):**
This kind of CPS is utilized within a single mobile body such as a human or a moving machine. A mobile machine can be a manned vessel or vehicle or an unmanned autonomous vehicle. The components of BCPS are usually distributed within that body. All sensors, actuators, microcontrollers, communication devices, and other components are located within the same body and move with it. Examples of BCPS are wearable medical CPS, autonomous driving vehicles, automatic vehicular safety capable applications in traditional vehicles, and mobile robots such as UAV, UGV, USV, and AUV. Most BCPS consist of multiple devices coupled through mobile networks available within the body they operate on. The unique issues to this category are:

- **Energy efficiency**: BCPS are mobile and rely on batteries for their power and the general goal is to extend their life. This requires all solutions for this category to be designed with energy efficiency in mind. This includes monitoring, processing, controls, acting, and communication. Several energy-effect protocols developed for body-area networks can be utilized for some BCPS applications (Hughes et al., 2012; Zuhra et al., 2017).
- **Location awareness**: The mobility of the BCPS may impact their functions based on their location. For example, they should have stronger security mechanisms or sensing capability if they operate in certain locations. These adaptive capabilities can enhance energy efficiency BCPS. At the same time, as BCPS will interact with the physical world, knowing their location is important to enable useful interactions. For example, a mobile robot can achieve certain tasks if it is available in a certain location; otherwise, it will not be useful.

- **Safety**: BCPS mobility and frequent interaction with varying environments impose specific safety requirements as they operate. Safety includes safe operations, security, privacy, reliability, and fault tolerance features. Some of the security and privacy issues in this category are like those in body-area networks. Therefore, they can be solved by adapting the security and privacy solutions developed for body-area networks (Li et al., 2011).

**Local Area Cyber-Physical Systems (LCPS):**
This kind of CPS is located within a certain reduced geographic area such as within a single facility, building, multiple neighboring buildings, a segment of a street, or a traffic intersection. The elements of the LCPS are linked by a local area network (LAN). The network can be wired, wireless (WLAN), or a combination of both. Cases of the LCPS are greenhouse efficient control systems, smart buildings, hydro power plants, manufacturing monitoring and control systems, wind and hydro power plants, and energy efficiency systems in data centers. This category is considered less challenging compared to other categories as CPS applications are bounded within certain areas with better control for the whole environment. However, there are still typical CPS issues in this category such as real-time heterogeneity, reliability, context awareness, fault tolerance, security, and integration with other systems supports. Yet they exhibit less complexities due to their increased capabilities and available resources. These complexities, however, will increase if mobile nodes such as BCPS are included in the LCPS, thus introducing some BCPS specific issues into the LCPS. Other issues may arise when multiple LCPS are connected to achieving some collaborative set of goals, thus imposing a wider type of connection. These connections will create WCPS, which will lead to increased emphasis on certain issues like reliability, security, real-time support and connectivity with other systems.

**Mobile Ad Hoc Cyber-Physical Systems (MCPS):**
This category of CPS generally has several BCPS, and other mobile devices or nodes linked in a mobile ad-hoc network via direct or multi-hop communication. There is typically no fixed structure that can be employed to offer communication and other required functions for the MCPS. The communication links and network topology among the nodes are usually self-organized and dynamic. In this category, each node can be a complete BCPS or a regular connected device. Examples of BCPS nodes are vehicles, robots, underwater vehicles, and unmanned autonomous vehicles (UAV). The applications of MCPS commonly include collaborative activities among the MCPS nodes. Application examples include collaborative UAVs and vehicular safety applications, and collaborative MRS. Many applications of this category are mission oriented. Examples of these missions are using collaborative UAVs for attacks or surveillance in war, using collaborative UAVs to fight fires, using collaborative USVs for oil spills cleanup in seas and rivers, and using collaborative MRS in search and rescue operations. There are many issues in this category mainly due to the nodes' mobility and the networks used for MCPS (Goyal et al., 2011):

- **Location awareness**: As MCPS nodes move, they need to be able to know their location to effectively provide location-based services depending on their location.
- **Communication among nodes**: Fast and efficient communication among nodes is needed by some applications. This requires maximizing routing and multicasting efficiencies. Unlike other categories, efficient communication in an ad hoc network is always challenging due to the lack of fixed structure and mobility.
- **Energy efficiency**: Most (if not all) nodes in MCPS are mobile and rely on batteries and most MCPS applications are mission oriented. Therefore, all solutions for the issues in this category should be designed with energy-efficiency in mind. This is important to extend the life of the nodes batteries to be able to complete the defined missions.

- **Resource management**: Effective resource management can help better achieve applications objectives. It helps allocate subtasks effectively and efficiently to the suitable components of the MCPS. It increases system performance by including energy-awareness and location-awareness features in task allocation. However, resource management for a mobile ad hoc network is exceptionally hard due to the dynamic and mobility of MCPS. Resource management involves several tasks such as resource discovery, resource allocation, and resource status monitoring. As nodes in MCPS are mobile then resource management will require frequent updates for all nodes, their available energy, and capabilities. Furthermore, recourse management can be more difficult with heterogeneous nodes, which is the norm in MCPS, compared to homogeneous nodes.
- **Security**: Most MCPS applications operate in open physical areas and unattended areas in some cases. Therefore, strong security measures are extremely important to avoid any type of unauthorized access or control to these nodes. In addition, security threats are stronger as these systems are mission-critical, and it is very important to ensure accurate deployment and uncompromised operations.
- **Fault tolerance**: Some MCPS applications are mission-criterial and must achieve their tasks within certain time frames. However, problems may occur in some nodes during the mission, which may slow them down or be completely non-operational. To continue the mission within the defined timeframe, fault tolerance solutions are needed to ensure continuity of operations. There are two possible solutions for fault-tolerance in MCPS. The first is by reallocating tasks to existing nodes to complete the mission or by having backup nodes available that can be used to replace faulty ones. In either case, an efficient fault detection model must be present to identify problems early and trigger the necessary corrections.
- **Distributed Processing**: There are some tasks that need distributed controls and/or have computationally intensive algorithms that could benefit from parallel/distributed processing. This requires utilizing multiple nodes to conduct the distributed processing and controls. However, this can be very difficult to achieve with MCPS due to the mobility of the nodes and lack of centralized controls.

**Wide Area Cyber-Physical Systems (WCPS):**

The applications elements of the WCPS are widely distributed over geographical areas. In addition, these components are connected fully or partially through open public networks like the Internet. Each WCPS application may consist of a few linked nodes of various devices and/or other kinds of CPS such as BCPS and LCPS. Each WCPS can be considered as a network of networks or as a system of systems. Application examples of WCPS are oil and gas pipeline monitoring smart grids, and smart water networks. WCPS applications have several issues in common, yet they could also be easily affected by the type of components making them up. For example, if a WCPS has some mobile nodes such as BCPS or MCPS, then issues from BCPS and MCPS will also be part of the issues of the WCPS. The main issues for WCPS are:

- **Scalability**: WCPS applications may be composed of a huge number of components that cover a wide geographical area, then the system needs to efficiently deal with the volume, location and connectivity of all these distributed components.
- **Efficient communication**: WCPS components need to communicate across wide areas, thus the communication system connecting them must be designed to efficiently handle long distance connections and high latencies among the components. At the same time, the communication system should also be able to handle high communication traffic volumes that may generated by the components.

- **Distributed processing**: Some WCPS applications may require utilizing multiple distributed processing units for some computational tasks. To accommodate for that the WCPS must be able to handle the distribution and control of such functions across widely distributed nodes, which can be very challenging.
- **Resource management**: A WCPS is a very large system with a very large number of heterogeneous resources that are also located across very large geographical areas. WCPS resources are widely distributed and dynamic in terms of operational availability. Resource management becomes critical for such systems to identify, keep track of, allocate and manage all the resources for WCPS applications.
- **Security**: Most WCPS applications will work across uncontrolled extended areas and may utilize public communication infrastructures like the Internet. Therefore, these applications have high security risks such as unauthorized access, malicious attacks to disrupt or fail operations, or attacks to steal or damage data. WCPS must include suitable and effective security and privacy measures to protect them.
- **Fault tolerance and real-time support**: Fault tolerance and real-time support rely on timely reception of, processing and responses to information across the applications components. Due to the high communication delays between some components in WCPS, fault tolerance and real-time support can be very complicated.

## Results and Discussion

Although CPS applications provide many benefits, there are also several issues involved in developing and operating such systems. One of these issues stems from the direct and intimate interaction between the cyber parts and the physical environments and systems including humans and critical components. As a result, any CPS application must exhibit strict security, reliability, and safety characteristics. Vulnerabilities to attacks, faults and safety problems may lead to undesired damage in the associated physical environments or systems (Banerjee et al., 2011). Another issue is the complexity of developing the cyber parts of such applications to satisfy the requirements. The cyber parts are developed as software that implements the data structures and algorithms needed to provide the necessary functionalities for the physical world. These include monitoring, analysis, decision making, control, applying actions, and building the knowledgebase for CPS applications. Some of these activities may be straightforward, while others may require complex algorithms and intensive computations for enhanced and smart results. The development complexity issues span across all the system development life cycle of CPS applications including the complexity of the requirements analysis, the design, the implementation, and the testing phases (Al-Jaroodi and Mohamed, 2018).

Another major aspect of complexity in CPS applications is the required network architecture. Although a lot of research is dedicated to studying the different aspects of CPS, there is very limited work highlighting the required network architecture as a significant contributor to the complexity of CPS applications. In this paper, we addressed this issue by classifying CPS applications in five categories based on the network architecture used. Through the classification we can identify the common issues involved in each category. This helps in using some available solutions from the network and middleware domains (Al-Jaroodi et al., 2018) to simplify the CPS applications development process. There are many protocols and methods developed for different types of networks. Many of which have been tested and optimized and ready for utilization in other domains. Furthermore, there are many middleware solutions developed for different types of networked environments and applications. These also offer well-designed and proven approaches ready for use. Both sets of solutions can be adapted and reused for developing CPS applications. Table 1 provides a summary of these categories, and their CPS applications and main issues involved.

**Table 1. The proposed CPS classification.**

| CPS Category | Applications | Issues |
|---|---|---|
| **Nanoscale CPS (NCPS)** | • Nanorobotics<br>• Nano medical devices | Mobility, energy efficiency, limited resources, reliability and dependability, real-time provision, interaction with other systems |
| **Body Area CPS (BCPS)** | • Medical and healthcare CPS<br>• Self-driving cars<br>• Safety applications for cars<br>• Autonomous drones<br>• CPS-based Games and Flight simulators | energy efficiency, mobility, location awareness, real-time provision heterogeneity, security and privacy, reliability, context awareness, interaction issues with other systems |
| **Local Area CPS (LCPS)** | • Smart facilities and buildings<br>• Production monitoring and control<br>• Greenhouse efficient management<br>• Wind and hydro power plants<br>• Energy efficient data centers | Heterogeneity, security, real-time provision, reliability, context awareness, smooth integration with other systems |
| **Mobile Ad Hoc CPS (MCPS)** | • Safety applications for collaborative cars<br>• Collaborative UAVs, UGVs, USVs and AUVs | Efficient communication, mobility, location awareness, distributed processing management, distributed resource management, heterogeneity, real-time provision, security, reliability, context awareness, smooth integration with other systems |
| **Wide Area CPS (WCPS)** | • Smart Grids<br>• Smart water networks<br>• Oil, gas, and water pipelines management | scalability, distributed processing management, efficient communication, distributed resource management, security, heterogeneity, reliability, context awareness, large-scale integration with other systems |

CPS can provide different types of automation and control mechanisms for many applications in diverse domains. These mechanisms benefit these application domains in many ways. The benefits include enhancing safety, health, energy-efficiency, cost-effectiveness, productivity, quality, reliability, security, resource utilization, and sustainability. An important aspect of CPS is that they rely on detailed and continuous monitoring of the physical environment or systems. This leads to the collection of huge amounts of fine-grained data being collected over time. This data includes the characteristics, status, and operations of the CPS environments and systems. The data collected over time can be used to build and update CPS knowledgebase about the corresponding environments or systems. This collected knowledge will expand the knowledgebase over time leading to various benefits:

- **Enhancing the closed-loop control process**: The knowledgebase can be used to enhance monitoring, decision, and action tasks in the closed-loop control process to better achieve the main objectives of the CPS application. One example is enhancing the monitoring methods for more accurate results such as moving or fine tuning a sensor or set of sensors to gather better information. Another example is to change the decision task for faster controls. For instance, there are many control algorithms developed to achieve energy-efficiency in smart buildings (Dounis and Caraiscos, 2009). However, it is very difficult to know which one is best to use, since the suitability of these algorithms is based on the characteristics of smart buildings, their uses, and their occupants' behaviors. Over time the collected information will enrich the knowledgebase that can be better analyzed to select the most appropriate algorithms.
- **Improving maintenance processes**: Knowledge about an environment can help optimize the maintenance process for the corresponding system operating in it. Instead of conducting a routine and costly holistic maintenance based on a static time schedule, the collected knowledge about the system can propose the best maintenance times and activities. This can significantly reduce the

costs of maintenance. In addition, this same knowledge can be used to discover potential for failures as the data will provide fine grain analysis of the status and operations of the system's components and environment. For example, CPS in manufacturing can monitor and analyze the efficiency of the different processes over an assembly line and spot errors or discrepancies, which will trigger a request for inspection or maintenance. In addition, continuous monitoring and comparison of the products' quality can also trigger requests for maintenance if at a certain time, a consistent variation from the required measures is detected. This type of trigger becomes more accurate if historical data is available and the system can compare status with previous situations, which the knowledgebase can provide.

- **Finding unknown or hidden faults**: Some components of CPS can continue to operate even with the existence of faults due to the subtlety of these faults. Examples of these faults are sensors that provide wrong readings in some circumstances. For example, a pressure sensor that is off by a few percentage points may not be easily discovered. These faulty components can negatively impact the operations of the CPS. Thus, they will not be able to accurately accomplish their objectives. For example, unknown faulty temperature sensors (maybe by being off by a couple of degrees in their readings) in a smart building can impact on the controls of the HVAC system and reduce the energy-efficiency in the building. Another example is problematic sensors that should check a specific attribute of a product in a manufacturing process that deliver inaccurate results; thus, they will not help in achieving the required quality in the process. Building a comprehensive knowledgebase in these systems and using smart algorithms to analyze and compare information will help identify this type of problem early (Lee et al., 2015).
- **Informing and enhancing future CPS designs**: The collected information for many CPS applications in similar systems can be utilized to inform future CPS designs through identifying problem areas, highlighting success factors and providing detailed information on the operations of the current CPS being recorded in the knowledgebase. As a result, future CPS applications will be enhanced, and their operations will be further optimized. Using the knowledgebase, it will also be possible to identify limitations and weaknesses and better understand the human/user involvement with the system. The knowledgebase will also help determine the best practices in design, development and operations of new CPS applications.

## Conclusion

CPS offer unlimited opportunities to create and deploy increasingly useful applications integrating real world physical environments and systems with the cyber world. This integration creates a wealth of benefits allowing these applications to monitor, work with, manage, and improve the physical world. To have a better understanding of CPS applications, their potential and challenges, we started by investigating the different possible application domains. These applications span a huge spectrum from the medical field, power and energy, smart systems, and even data centers. We also took the opportunity to highlight the specific issues and challenges for these applications.

Armed with this knowledge, we then identified several commonalities across certain types of CPS applications. As a result, we classified these applications into five different categories. These were mapped from the categories imposed by the size of the system and the type of network used to connect its components (physical and cyber). Therefore, we have the Nanoscale CPS (NCPS), the body area CPS (BCPS), the local area CPS (LCPS), the mobile ad hoc CPS (MCPS) and the wide area CPS (WCPS). Many of the issues identified for each of these categories may find solutions by adopting approaches designed for their counterpart network type. However, as CPS span both the physical and cyber worlds as a complete operational unit, many of the challenges and issues are unique to these applications. The classification helps

create a systematic view of CPS applications and allow for a better understanding of these issues as they relate to a specific category. As a result, this creates a first step to develop suitable solutions addressing these issues with a specific category in mind, instead of having to deal with the generalities of the whole set of CPS applications.

The next steps from here could include in depth investigation of each one of the categories to target specific challenges or project requirements. Several areas in resource management, mobility support, real-time constraints, and systems integration just to name a few require effective and efficient solutions finely tuned for the specific type of CPS applications. Another important aspect to address is providing a more suitable, more intuitive design and development approaches and environments for CPS applications. Frameworks, abstractions, and architectural models need to be created to support the analysis, design and implementation efforts. In addition, generalized approaches addressing specific issues for CPS applications can be designed and made available for reuse across varying CPS applications.

## References

Al-Jaroodi, J., & Mohamed, N. (2018). PsCPS: A distributed platform for cloud and fog integrated smart cyber-physical systems. *IEEE Access*, *6*, 41432-41449.

Al-Jaroodi, J., Mohamed, N., & Jawhar, I. (2018). A service-oriented middleware framework for manufacturing industry 4.0. *ACM SIGBED Review*, *15*(5), 29-36.

Banerjee, A., Venkatasubramanian, K. K., Mukherjee, T., & Gupta, S. K. S. (2011). Ensuring safety, security, and sustainability of mission-critical cyber–physical systems. *Proceedings of the IEEE*, *100*(1), 283-299.

Dounis, A. I., & Caraiscos, C. (2009). Advanced control systems engineering for energy and comfort management in a building environment—A review. *Renewable and Sustainable Energy Reviews*, *13*(6-7), 1246-1261.

Goyal, P., Parmar, V., & Rishi, R. (2011). Manet: vulnerabilities, challenges, attacks, application. *IJCEM International Journal of Computational Engineering & Management*, *11*(2011), 32-37.

Gunes, V., Peter, S., Givargis, T., & Vahid, F. (2014). A survey on concepts, applications, and challenges in cyber-physical systems. *KSII Transactions on Internet and Information Systems (TIIS)*, *8*(12), 4242-4268.

Hoenig, A., Roy, K., Acquaah, Y. T., Yi, S., & Desai, S. S. (2024). Explainable AI for cyber-physical systems: Issues and challenges. *IEEE access*, *12*, 73113-73140.

Hughes, L., Wang, X., & Chen, T. (2012). A review of protocol implementations and energy efficient cross-layer design for wireless body area networks. *Sensors*, *12*(11), 14730-14773.

Ivo, A. A., Ribeiro, S. G., Mattiello-Francisco, F., & Bondavalli, A. (2023). Toward conceptual analysis of cyber-physical systems projects focusing on the composition of legacy systems. *IEEE Access*, *11*, 58136-58158.

Lee, J., Bagheri, B., & Kao, H. A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing letters*, *3*, 18-23.

Li, M., Lou, W., & Ren, K. (2010). Data security and privacy in wireless body area networks. *IEEE Wireless communications*, *17*(1), 51-58.

Luedeke, T. F., Köhler, C., Conrad, J., Grashiller, M., Sailer, A., & Vielhaber, M. (2018). CPM/PDD in the context of design thinking and agile development of cyber-physical systems. *DS 91: Proceedings of NordDesign 2018, Linköping, Sweden, 14th-17th August 2018*.

Mohamed, N., Al-Jaroodi, J., & Jawhar, I. (2020). Cyber–physical systems forensics: Today and tomorrow. *Journal of Sensor and Actuator Networks*, *9*(3), 37.

Palma, F. E. D. S. P. (2016). Project management best practices for cyber-physical systems development (Doctoral dissertation, Universidade de SÃ£ o Paulo).

Palma, F. E., Fantinato, M., Rafferty, L., & Hung, P. C. (2018, September). Enhancing project management for cyber-physical systems development. In *2018 Federated Conference on Computer Science and Information Systems (FedCSIS)* (pp. 747-750). IEEE.

Shi, J., Wan, J., Yan, H., & Suo, H. (2011, November). A survey of cyber-physical systems. In *2011 international conference on wireless communications and signal processing (WCSP)* (pp. 1-6). IEEE.

Wu, F. J., Kao, Y. F., & Tseng, Y. C. (2011). From wireless sensor networks towards cyber physical systems. *Pervasive and Mobile computing*, *7*(4), 397-413.

Zuhra, F. T., Bakar, K. A., Ahmed, A., & Tunio, M. A. (2017). Routing protocols in wireless body sensor networks: A comprehensive survey. *Journal of Network and Computer Applications*, *99*, 73-97.