A Critical Analysis of Advanced Communication in Cyber-Physical Systems

[1]Vincenzo Anselmi
[1]Department of Computer Science, University of Salerno, Fisciano SA, Italy.
[1]anselmivin@unisa.it

Correspondence should be addressed to Vincenzo Anselmi : anselmivin@unisa.it

Article Info
Journal of Machine and Computing (http://anapub.co.ke/journals/jmc/jmc.html)
Doi: https://doi.org/10.53759/7669/jmc202202021
Received 22 March 2022; Revised form 28 May 2022; Accepted 24 July 2022.
Available online 05 October 2022.

Abstract – Cyber-Physical Systems (CPSs) are a new study area that has the potential to bring together the physical and digital worlds. Researchers in this study focus on the ways in which CPSs communicate with one other. Features and requirements for data transfer in CPSs, and also related unsolved issues, are covered in this paper. The IEEE 802.11 b/g protocols were used to construct a CPS solution for ambient sensing (humidity and temperature). Wireless Fidelity (Wi-Fi) sensors that can connect to a preexisting Wireless LAN and servers that provides access to data collected everywhere IEEE 802.11 b/g networks connectivity is available and from any Internet-connected device are required for this method.

Keywords – Cyber-Physical Systems (CPSs), Wireless Fidelity (Wi-Fi), Internet Protocol (IP), Internet of Things (IoT)

I. INTRODUCTION

Cyber-physical systems (CPSs) [1] are made up of linked components that work together to accomplish tasks by bridging the physical and digital worlds. A convergence of CPSs and the Internet of Things (IoT) has led to a rise in the complexity of activities, resulting in the need to design ubiquitous CPSs capable of delivering services on time. It is possible to create a network of real-time decentralized CPSs capable of managing physical object control and monitoring while also ensuring dependability across scales and levels of organization.

Innovations such as Service-Oriented Architecture (SOA) [2], interactive networks, and cloud technology have emerged in the evolution of CPSs after the combination of CPSs with IoT. A major advantage of service-oriented CPSs is that they need devices in CPSs to work together across physical and cyber scales. Real-time decentralized real-time CPSs which account for the substantial inter-dependencies between cyber and physical subsystems can only be realized via a combination of a service-oriented design and optimum resource usage. A distributed ubiquitous computing methodology based on agents that are aware of their context is indeed more appealing because it is possible to incorporate various attributes into agents and achieve distributed cloud computing with improved synchronisation and interconnectivity among independent and inhomogeneous agents. When it comes to CPSs, context-awareness is a must, since this new technology relies heavily on sensors, resources, adaptability, and augmentation. Because CPSs are dispersed and dynamic, it is only logical that partial measurability be a feature of CPSs. Probabilistic modeling strategies must be used in order to achieve acceptable model performance when ontologies are used as the semantical technologies.

Semantic annotations of low-level contextual data blend with knowledge base in a reasoning engine to produce the semantic capacities of this paradigm. Annotated information and lexical processing allow distributed application agents working in the internet to give decision assistance for actuation data. Despite their differences, all of the agents can communicate with one another and with the physical world. Therefore, the agents may expose, consume and even execute collaborative resources that are aimed at predetermined system objectives. Event recognition on this model leverages the inferential capacity of Markov Logic Networks (MLNs) [3] to minimize inferential and computing burdens by incorporating uncertainty into the modeling process. This strategy to modeling concurrent occurrences in CPSs is shown to be feasible in tests with a home automation as a CPS.

The annotation of high-level complicated services from low-level data is required to provide dynamic development of collaborative services for the execution of difficult tasks. This procedure ensures higher-quality CPSs and eliminates frequent design defects, allowing it to offer accurate actuation data for real-world devices. When dealing with a fire breakout in a CPS setting, we may create a task, such as extinguishing the flames, using low-level data. Although this particular activity necessitates complicated functionality, it may be broken down into simpler components that can be handled by specialized

resources because of the amount of abstraction required to do it. As a result, a specific framework is needed to figure out complicated capability from low-level circumstances in this process.

Fig. 1 illustrates the inherent actuation link between cyberspace and decentralized CPS settings, which is why this technique was developed. The physical ecosystem is categorized into use and context surroundings for clarity of portrayal. Systems may accomplish tasks in the use environment via processes conducted by semantic agents. The usage ecosystem purportedly provides defined goals that specify the actions of agents towards usable output since each agent's behavior best matches its environment. Context information derived from the context acquisition procedure is the foundation of this approach's semantic capabilities.

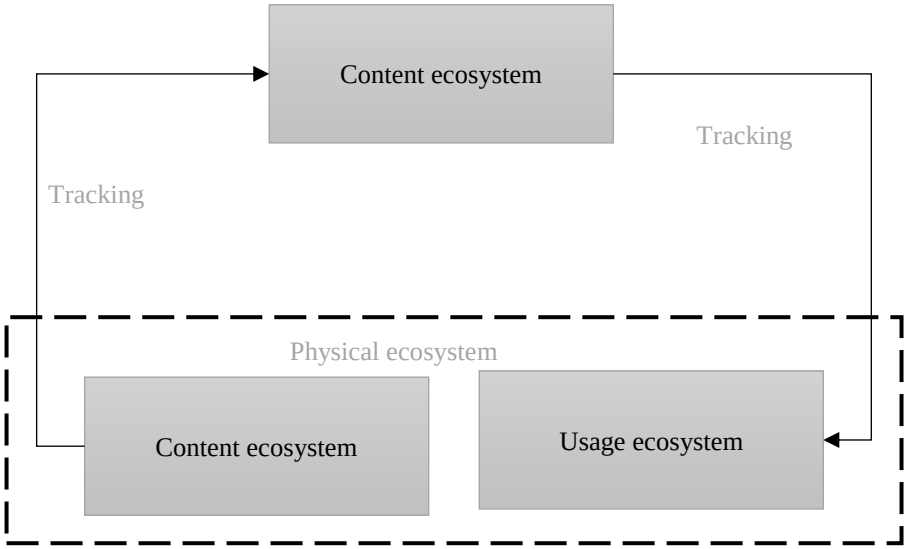

Fig 1. Interlinkage between decentralized CPS ecosystem and cyberspace

Embedded systems and complex software programs [4] form the third phase of controllers, which are connected together via wired and wireless connections. CPSs Products and services will come preloaded with these features, enabling real-time communication between a wide range of systems, whether they are physical or virtual. Consequently, Distributed Cyber-Physical Systems (DCPSs) [5] are required to be intelligent in order to be used in mission-critical operations, with a communication and computation core being able to monitor, synchronize, regulate, and integrate the many subsystems. They acquire physical data via underlying technologies and monitoring system, and then use actuators, organisation and control mechanisms, and applications to operate on that data. CPSs include smart grid systems, environmental control systems, SCADA structures, and distributed management structures for developing automated networks.

An advanced federative design for a virtual organization supported by interactive tools and built on top of an advanced manufacturing methodology for the configuration, development, and implementation of the assimilation of homogenous SCADA systems is another benefit of CPSs over traditional technologies of system design models. CPSs are the pinnacle of the monitoring, communications, and computation. As a consequence, this research focuses on communications as a key component of these networks. Underlying technologies and digitalization have led to a rise in the use of wireless connections in CPSs, which are less costly, less sophisticated, and lighter. When it comes to these networks, the Web is and will always be the main means of linking people and information. This is where Wireless Sensor Networks (WSNs) defined by Almesaeed and Al-Salem [6] come into play, extending the Web, which symbolizes the cyber domain, into the physical realm. Since IoT permits things and users to be interlinked at any moment over a particular route and application," CPSs are at the forefront of the IoT revolution.

The rest of the paper is organized as follows: Section II defines the aspect of communications between different Cyber Physical Security (CPSs) components. Section III evaluates the challenges facing the CPSs, which Section IV presents a solution enhancing the communications between CPSs components and limits the challenges facing the systems. Lastly, Section V concludes the paper and presents directions for future research.

II. COMMUNICATIONS BETWEEN CPS COMPONENTS

There are three major types of media used to transmit data and information: wireless signals, optical discs, wires/cables. There are several drawbacks to using cables to communicate between electronic devices, including as high costs and a lot of time and effort required for installation, installation, and management. Cyber-Physical Systems (CPS) are particularly vulnerable because they may traverse vast distances, including inaccessible locations, and function in hostile environments. As a consequence of the increased use of digital systems, a plethora of communication protocols across wires has emerged. However, in industrial contexts, fieldbus protocols predominate over Ethernet, which is component of the TCP/IP and UDP

stacks. Ethernet technologies are the most dominant protocol employed for office and home operations. Field devices, digital controller, and applications communicate with one another using various protocols such as OPC Unified Architecture (OPC UA), Profibus TCP/IP, CANopen, Interbus, Profinet, and others.

The obvious advantages that wireless technology provides are driving the current trend toward wider use in control and monitoring applications. The apparent advantages of wireless networks over wired ones include the freedom to modify network architecture, scalability, and lower maintenance costs. A price must be paid for these advantages, since wireless communication introduces several problems and challenges for researchers to work through. It is important to address concerns like data transfer dependability, actual data distribution, and energy efficiency from the beginning of the design process to the end of the deployment phase when designing and developing wireless actuators and sensors for such applications.

As depicted by Javaheri Javid [7], complexity is also beyond current breakthroughs in terms of schemas and configurations that can provide easy assimilation and integration of great numbers of modules, distributed numerical simulation and interconnected command for time-based and event-based computer technology, time delays, failures and reconfigurations, distributed decision support meant to pacify high degrees of validation, reliability and verification to guarantee Quality of Service. Since physical and cyber elements must be seamlessly integrated, multiple challenges must be overcome at different points in CPS systems. Because of the high number of devices interacting and sharing data through a variety of protocols and technologies (Wi-Fi, Bluetooth, ZigBee), the reliability of communication is becoming more important. Because of this, interoperability across various devices and systems becomes a challenge.

Because the sensors are occasionally placed in unexpected locations and must rely on self-organizing algorithms, they transmit data over short ranges straight to the ground station (single hop). As the system's size increases, communication protocols must be developed that allow for appropriate throughput and minimum delay. The security of CPSs is vital since they are commonly employed in mission-critical tasks. passive data interception and aggressive traffic injection are only two of the many threats to communication. Secure wireless technology relies heavily on message encryption, but deploying cryptographic methods in systems with storage, transmission, computation, and processing limits is challenging. An overview of the wireless systems being developed to solve these concerns may be found in the paragraphs that follow.

Wireless Network Protocols

The most typical wireless networking protocols in CPSs integrates Wireless Fidelity (Wi-Fi), WirelessHART, ISA100.11a, ZigBee (IEEE 802.15.4), Bluetooth (IEEE 802.15.1).

Bluetooth

For short-range, low-power and low-cost communication between mobile and fixed devices. Bluetooth is the de facto industry standard. 2010 debuted BLE (Bluetooth Smart) as an extension of the Bluetooth platform to include wireless sensor networks and wireless controllers. It is more feasible that the BLE network is utilized in the house for management and sensing in the future as this technology progresses. In order to transmit and receive data from and to distant places, these systems need the usage of BT Internet gateways. Because the protocol is so simple, it has security issues, which compromises the privacy of information sent between parties. As a result of denial of service and eavesdropping, unauthorized access and control of data may be gained.

ZigBee

Both star and peer-to-peer configurations are supported by IEEE 802.15.4, which has low power consumption and modest data transfer rates. Reduced-Function Devices (RFDs) and Full-Function Devices (FFDs) are two forms of devices, which may be distinguished. Due to its foundation in IEEE 802.15.4, ZigBee may be used in a range of measurement and management applications, such as building automation, that require wireless connectivity but cannot fulfill stringent latency and dependability standards. Despite this, ZigBee including the other 802.15.4-centric approaches are increasingly being employed in sensor network implementation due to their low power consumption. Gateways are required to send data from these devices to the Internet. Resource-constrained ZigBee node may face difficulties due to the use of the Advanced Encryption Standard (AES) protocol with counter function that needs substantial code and time overhead.

ISA100.11a

Using wireless sensors and communications in the industrial automation industry is particularly challenging since the update rates required range from 100 milliseconds down to one millisecond. The increasing need for wireless technology in industrial environments prompted the development of several standards, including ISA100.11a. For non-critical measurement and management applications, this IEEE 802.15.4-centric wireless technologies provides more secure and reliable operation. Among network components are a peripheral, backbone networks, gateways, system supervisors and security administrator. Even though the standard covers a wide range of automatic networks, it poses challenges and makes comprehensive device compatibility hard because of this.

WirelessHART

In order to provide reliable and secure communication, this standard was designed to be easy to set up, versatile to be installed, and rapid to obtain instrumentation data. The network is made up of a variety of components, including routers, switches, network and security administrators, mobile devices, and other types of adapters. To that aim, WirelessHART is centered on IEEE 802.15.4 as well as appropriate for mission-crucial systems due to its ability to guarantee low latency and high reliability from the beginning to the finish. As low-power systems, ISA100.11a as well as WirelessHART are compatible with long-lasting batteries. Employing AES- 128 encryption, they are likewise safe and secure, ensuring secrecy and giving a variety of degrees of protection.

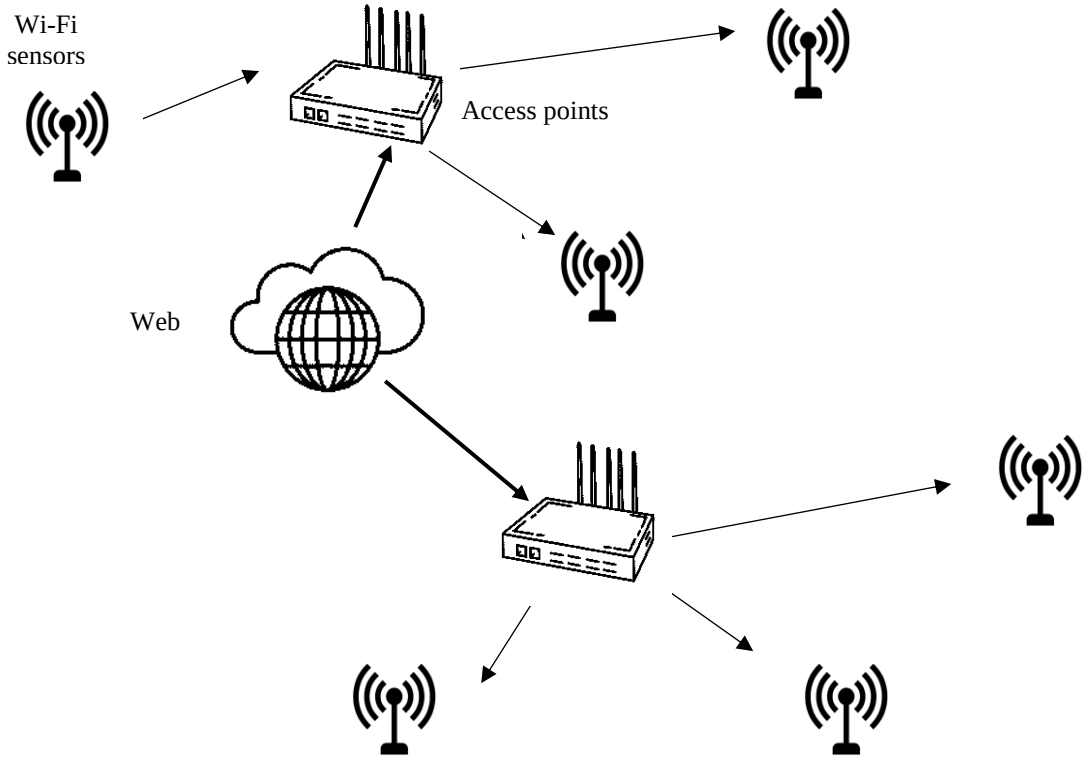

Fig 2. Network for access points

Wi-Fi

Although the signal strength and bandwidth of IEEE 802.15.4 are effective, the energy efficacy of IEEE 802.11 is lower. IEEE 802.11 is a set of wireless LAN protocols. For consumers, Wi-Fi enables them to link to the Internet or a company's network remotely by using IEEE 802.11 standards. In the past, wireless sensors were not considered because of their excessive energy usage. When it comes to wireless sensing technologies, nevertheless, low-power Wi-Fi gadgets such as RN131C/G from Rover Systems have made Wi-Fi much more enticing. Table 2 shows some of the other ways CPS may be put to use (see **Table 1**). These sensors take use of the current infrastructure, protocols compatibility, conventional Internet Protocol (IP) interoperability and ace of the wide range of network control devices and wide knowledge base. ZigBee (IEEE 802.15.4) networks, on the other hand, have been shown to have battery life equivalent to Wi-Fi networks.

Wi-Fi-enabled devices may employ the 802.11 standard's WEP, WPA2/AES-PSK and WPA/TKIP-PSK to protect anonymity of data, authenticity, and reliability. Sensors communicate automatically with the gateways or access points in the great preponderance of Wi-Fi-based wearable sensors (see **Fig. 2**). There is no need to install extra gateway to connect to a network in this case. It is unnecessary for applications to encapsulate data before it is sent over the Web if the detectors use network protocols such as UDP.

III. CHALLENGES

New innovative capabilities have emerged from the interconnectedness of networking, computational, physical, and human elements. A wide spectrum of basic scientific, architectural, organizational, and social difficulties is reflected in the underlying technological obstacles. As technology advances, it faces obstacles at every level of its lifecycle, from fundamental research through applied R&D and demonstrations to manufacture and deployment. To guarantee that CPS are dependable, safe, duplicatable, and secured, we must address the most crucial issues first.

Scientific and Technical Challenges

A novel systems study is needed to advance CPS, one that incorporates physical as well as computing features. To solve CPS's unique scientific and technological difficulties, a novel systems theory must be developed from the ground up.

Integrating complex, heterogeneous large-scale systems

Heterogeneous decentralized systems and networks in the future CPS will be many and must operate together efficiently to give the performance anticipated. Many obstacles stand in the way of this now. The absence of standard vocabulary, modeling technologies, and coherent interpretations for expressing cyber and physical interconnections across diverse systems is a critical challenge. Without the advantage of unifying concepts and protocols, it is very difficult to ensure the interoperability of distinct components built in various technical fields and industries. Interoperability and integration issues may be exacerbated by a lack of unambiguous control of the interaction between technologies (e.g., among software, hardware, and various equipment providers). Interoperable networks, in addition to adhering to standards, must guarantee that timely outputs, result agreements, resiliency, packet forwarding, and technological security procedures are handled smoothly inside and between subsystems. This covers data aggregation and sharing inside and between systems and their components.

Table 1. CPSs applications

Innovative Applications and Products	CPSs	Implication
Intelligent Production and Manufacturing		
Supply chain connections; and lean manufacturing	Smart controls; assembly and process automations; and robotics operating safely with people	Great reliability, agility, and efficiency; US-based high technological manufacturing; and improved international competitiveness
Mobility and Transportation		
Automated vehicles (space, water, air and surface); vehicle-to-infrastructure, and vehicle-to-vehicle communications	Next-generation air transportation management; interactive traffic management frameworks; smart and plug-in vehicles; and drive-by-wires intelligent vehicles	Great safety and conveniences of travels; accident and congestion control (the zero-fatality highway)
Energy		
Oil and gas production; renewable energy supplies; and electric frameworks	Intelligent oil and gas supply grids; plug-in motor charging models; and intelligent electric power grids	Enhanced energy effectiveness; great diversity, security and reliability of energy supply
Civil Infrastructures		
Dams and bridges; municipal wastewater treatment schemes	Early weaning frameworks; intelligent grids for wastewater; and active control frameworks and monitoring systems	Accident prevention and warning; assurance of water supply and quality; more reliable, secure and safe infrastructures
Medicare		
Medical tools; personal care tools; disease prevention and diagnosis tools	Wearable body domain systems; assistive medical systems; and implantable devices and wearable sensors	Timely illness prevention and diagnosis; cost-efficient Medicare; and enhanced results and quality of living
Structures and Buildings		
Appliances; net-zero energy structures; high-performance commercial and residential structures	Networked appliance frameworks; building autonomous systems; intelligent HVAC tools; and whole construction control	Controls of indoors quality of air; enhanced occupant safety and health; and enhanced building convenience, comfort and efficiency
Defence		
Intelligent, and autonomous underwater sensors; supply tools; weapon platforms; and soldier tools	Precision-centric weapons; wearable sensing/computing uniforms; smart vehicles; and logistics systems and supply chains	Decreased exposures for human fighters and great capacity for remote wars; and enhanced warfighter effectiveness, agility and security
Emergency Response		
Fire-fighting tools; communication tools; and first responder tools	Surveillance and detection systems; Resilient communication system; and Integrated emergency response frameworks	Rapid capacity to reply to natural disasters; and enhanced emergency responder agility, efficiency, safety and effectiveness

Interaction between Humans and Systems

Using current theories of machine and human behaviors is insufficient for building CPS when people and machines communicate intimately. Situational awareness—the human awareness of the systems and its surroundings, as well as alterations in variables crucial to decision-making—is one of the issues. Complex, parametric models, such as those deployed in air traffic management, power station management, command structure and management and emergency personnel, need this kind of monitoring and control. Humans and machines may interact in a variety of ways in these systems, resulting in a wide range of possible outcomes. Accidents resulting from human mistake have been linked to inadequate contextual perception and a lack of capacity to understand the human element in big, complex structures.

Dealing with Uncertainty.

This means that complex CPS must have the ability to adapt and function reliably in a wide range of conditions. As these systems grow more and more dependent on machine learning approaches, they will also begin to exhibit emergent and unforeseen behaviors. CPS development and design will have to include new methods for quantifying uncertainty due to ambiguity in the information or the result of a process. Uncertainty can only be described and quantified using the current tools now available. There are several factors that contribute to this, including as the dependability and precision of physical elements, the veracity of models that describe them and network connections. Uncertainty quantification is also a topic of discussion, as is the goal of achieving ideal outcomes in the face of physical uncertainties and estimates in the design process.

Measuring and Verifying System Performance

CPS innovation and investments are hampered by the difficulties of proving multiple functionalities, reliability, accuracy, confidentiality, and other criteria needs. When compared to the development time, current verification and validation (V&V) capacities for CPS are restricted and expensive. Both methodology and test beds and databases must be developed to provide a methodical process to the verification of complicated CPS, which is a huge problem. Designing and testing may be streamlined if the first step is more trustworthy. It is projected that future CPS, which will have huge sensor, actuator, and element systems integrated, would provide more severe issues in terms of assessment. Many parts of CPS, from design through testing, installation, and operations, need metrics for assessment. Complexity, flexibility, security, safety, confidentiality, resiliency, dependability, and manufacturability are some of the most critical domains where scientifically-based measurements are required. One of the biggest challenges is designing metrics that can be used to a broad range of systems. Another challenge is figuring out how to utilize analytics efficiently. This means that design strategies for fulfilling privacy goals must be devised if privacy metrics are specified. Designing privacy criteria and then testing a system to see whether it meets them is also a difficulty.

System Design

The development of CPS is hindered by the inability to develop systems-level. It is difficult to design technologies at the network level because of a lack of formalised high-fidelity simulations for large systems, as well as insufficient means of monitoring efficiency and weak scientific underpinnings (e.g., no "science of systems"). In the design process, compositionality and versatility are essential. The interconnections between code and systems design have a significant influence on CPS compositionality, which is typically constrained by insufficient system design.

For instance, the creation of a CPS may be considerably eased if system elements could be built and tested in seclusion, and the system-level qualities could be deduced from the attributes of its pieces. In both design and implementation, CPS designers strive for this modular and symphonic approach. Nevertheless, this is presently only viable in limited areas and with basic properties. Compositionality is difficult to achieve due to a lack of mathematics and system science underpinnings, codified metrics, assessment procedures, and ways for coping with cross-cutting features in the design process. Extending the mathematical methods for exploring design space is crucial to offering a systematic approach to designing modular complex structures.

Institutional, Societal, and Other Challenges

Trust, Security, and Privacy

In order to ensure that technologies are reliable, secured, and private, there are both technological and policy hurdles. Among the numerous reasons why CPS relies on cyber-security is that it safeguards national infrastructure, personal privacy, system reliability, and intellectual properties. Several previous foreign-based breaches on US computer networks, both governmental and commercial, demonstrate the existing Internet flaws and the reason for tackling global cyberspace security. Whereas cyber-security is a national concern, CPS security introduces a number of additional issues. Cyber and physical flaws may combine to create attacks that are radically unique, difficult to assess, and pose a significant threat to the physical integrity of key systems, for instance.

Secure CPS has a number of challenges include adopting a systematic method to CPS vulnerability analysis as well as constructing evolutionary and robust designs to deal with continuously emerging physical and cyber threats. In addition to security, protecting privacy and secrecy is essential. As an example, patients who rely on embedded biomedical devices are concerned about the potential exposure of personal and health information if such devices are connected to monitoring systems. It is necessary for businesses to safeguard their intellectual properties, as well as sensitive financial and

demographic data. As the systems that gather, handle, and interpret data quickly evolve and in certain circumstances need to function in a dispersed or almost open environment, ensuring the confidentiality and privacy and limiting the accessibility and usage of data are challenging.

Effective Models of Governance

We need new governance frameworks that are both local and global to ensure that CPS technologies that function both in the real and virtual world are governed by standards, standards, and supervision that are consistent across both. However, these new forms of governance have yet to be formally established. Monitoring and control may be provided via governance, which might help to decrease the liability that arises from unauthorized intrusions or other security flaws. Many institutions, from expert platforms to governmental decision-making bodies founded on treaties, are debating administration. While some advocate for more intergovernmental monitoring, others argue that the private industry can self-regulate by developing proper economic advantages, rules, and regulations, there is rising discussion around these concerns.

Creation of CPS business models

Extreme inclusion in CPS is a revolutionary innovation that alters the current quo, generates new sectors, and destroys others. CPS-based restructuring of existing industries is a complicated and risky process that necessitates combining IT business strategies with those of engineering-based businesses. Fusion business concepts are still new and challenging to communicate. Economic and other statistics that may be utilized to support a feasibility study are not properly recorded for CPS, which contributes to the problem. There is a risk that new innovations and processes will not be adopted if there is no proven commercial model to guide investment. Examples of good CPS business structures today incorporate the aviation industry, which uses cyber-physical avionic technologies in current aircraft. Industry has created rigorous safety standards and certification procedures because they recognize the dangers and have addressed them. Business risk and responsibility rise as the size and complexity of CPSs expand". This risk may be mitigated by distributing the costs of creating precompetitive and infrastructural innovations that tap into innovations presented in **Table 2** below.

Table 2. Strategic Research and Development (R&D) opportunities for CPS

Domain	Opportunity
Workforce for progressive innovations within the CPSs	**Multi-disciplinary, dynamic training and learning** Establishing multi-disciplinary CPSs resources and degrees; Pursuing dynamic certifications and training in CPSs
Applied developments and deployments	**Reliable and efficient system interoperability and integration** Development of abstraction infrastructures for bridging physical and digital system elements; Building an inter-linked and interoperable developmental infrastructures; Creating global definitions for signifying extra-large heterogeneous frameworks
System engineering	**Enhanced quality assurance and performance of physical and computational systems** Efficiently characterization and qualifying reliability amidst an uncertainty; Developing science-centric metrics (such as dependability, reusability, flexibility, adaptability, resilience, safety, privacy, and security); and establish approaches for system-level validation, verification and evaluation of CPSs
Engineering and science foundations	**Effective, robust construction and design of infrastructures and systems** Developing systematic inter-personal and inter-process communications for actuators and sensors; Allowing natural, and seamless human CPSs communications; Managing the duty of time and harmonization in the infrastructure design; Creating domain-centric model for designs; and developing cost-effective model construction, analysis and design.

Understanding the value of CPS.

CPS will get the benefits of a well-developed infrastructures, which necessitates a huge investment up front. For such investments to take place, the value of CPS has to be better appreciated. CPS R&D is typically characterized in terms that are hypothetical or use jargon that is not easily understood. So, it might be difficult for companies and other stakeholders to comprehend and use the outcomes of CPS R&D. As a result, industrial adoption of developing technologies and better comprehension of CPS research's advantages and applications might be facilitated by less intellectual and more strategic methods of conveying CPS study, advantages, and dangers. In certain research, the benefit of CPS-related technologies has been effectively communicated, although this remains a barrier.

Multi-disciplinary Education and Collaboration

Engineering and science in CPS are multidisciplinary, needing knowledge of technology and mathematics as well as engineering and the whole range of physical sciences, including ethics and psychiatry. In order to work across disciplines effectively, specialists from a variety of backgrounds must be able to communicate effectively. It's fairly uncommon for CPS teaching and research in academia to be confined to either the physical and cyber realms, rather than a blend of both. Within

the current university system, which has traditionally been split into traditional professions (e.g., computer technology, architecture, biochemistry), there are significant hurdles in building multi-disciplinary CPS programmes. Similar issues have been faced by academia in the past, leading to the emergence of new, thriving sectors like bio-engineering.

Skilled Workforce

Knowledge and training are required for CPS, which are high technology systems that are difficult to design and execute. In order to meet their needs, they'll need additional employees with different backgrounds and specializations. It is a big issue in in of itself to develop and maintain a competent labor to support prospective CPS. Continuous training and education, as well as skilled instructors who keep up with the latest innovations, will be required in this fast-evolving sector of CPS technology. There are presently no rigorous instruments for workforce development in CPS, although they might be extremely useful in establishing and retaining a workforce of the future.

IV. CPS PROPOSED SOLUTION

This section presents CPS, a tool developed by the paper's authors and used in the study (Fig. 2). Multiple wireless sensor nodes make up the system, which communicates via UDP messages on the prevailing IEEE 802.11 b/g system. Temperatures and relative humidity are sent to the server platform over a pre-configured wireless connection via the cyber-physical system's sensors. Web pages maintained on the database server may be visited from any Internet-linked devices to see the data that has been gathered. Low-power operation is ensured by an RN131C/G remote Access module and a configurable microprocessor with an 8051 microprocessor at its heart. A 3V lithium battery energizes them and could probably last up to three years (a single data transfer and measurement cycle hourly). This strategy was adopted because of the ease of installation. Since the IEEE 802.11 architecture allows sensors to communicate device to the Network, Wi-Fi was chosen. It is possible to implement these sorts of wireless sensor nodes over wide areas when additional access nodes are added to the networks.

CPS Communications

An embedded technology and a complicated application software interconnected together via wireless and wired channels make up the third phase of control functions. In the future, all goods and services will have these features, which will enable for the real-time connectivity between a huge variety of channels in their surroundings, whether physical or virtual. To meet mission- and safety-critical requirements, CPSs must be smart distributed systems that contain both virtual and real elements and are operated by a computation and communications core. Embedded device and sensor technologies collect physical data, and controllers, management and operation systems and functions operate on the physical setting. Smart grid systems, environmental sensing, Supervisory Control and Data Acquisition (SCADA) solutions [8], distributed control mechanisms for smart building networks are some applications of CPSs. To further the notion of a "systems-of-system," CPSs have developed a unique "federative architecture" that allows the merging of diverse SCADA networks to be accomplished via the use of cooperative instrumentation and an advanced manufacturing methodology. Monitoring, communications, and calculation are all integrated into CPSs.

An important consideration while designing the system's communication systems is limiting how much power the nodes use at all times. Due to the RF transceiver's high-power consumption, wireless wearable sensors should be operated at the lowest possible level. There are a number of wireless sensing applications in which sensor networks do not need to work constantly but rather alternate between periods of activity and times of sleep. The proposed CPS in **Fig 3** employs a one-way communication technique to further minimize the system's power usage. Battery-energized duty-cycled gadgets, which power on at a particular interval to activate the sensor, collect information, power WLAN module and sent datasets to servers have been created as a consequence. In order to configure the device, the operator needs link a serial port to the computer.

Wireless Node Components

To maximize energy efficiency, all of the wireless sensor network technologies were chosen. One of the most important components of the gadget is a PSoC 3 microprocessor, which has a sleep mode energy usage of 1 A on average. Another important part of the device is the Roving Networks RN131C [9], which supplies extremely little power during the sleep mode (i.e., 4 μA) and max of about 210 mA for a specific timeframe during transmissions. Once data has been gathered and is ready to be sent, this feature is engaged by default. By using serial instructions from its core microcontroller, the WLAN modules is programmed to join to a predetermined wireless system and either communicate data to a certain IP address or possibly broadcast datasets to all other network devices. Hardware engineering and more power sources that might be switched off culminate in a sleep state usage of 10 μA. The system's average energy usage in active mode allows for minimal energy usage and a long node life lifetime.

Protocol

UDP was chosen because of its speed and simplicity contrasted to TCP, including its ability to send data without maintaining a link with the server. In terms of power usage, these characteristics are beneficial, but packet losses might have a negative impact on reliability. Data from the preceding two measurement cycles is included in each message in order to alleviate this problem It is possible to use data from the next package to fill in a missing piece of information. When it comes to

environmental monitoring, this CPS is mostly concerned with power consumption rather that reponse time, determinism, and reliability. Due to this, additional approaches for data synchronization and recovery are not required, and low reliability level is acknowledged.

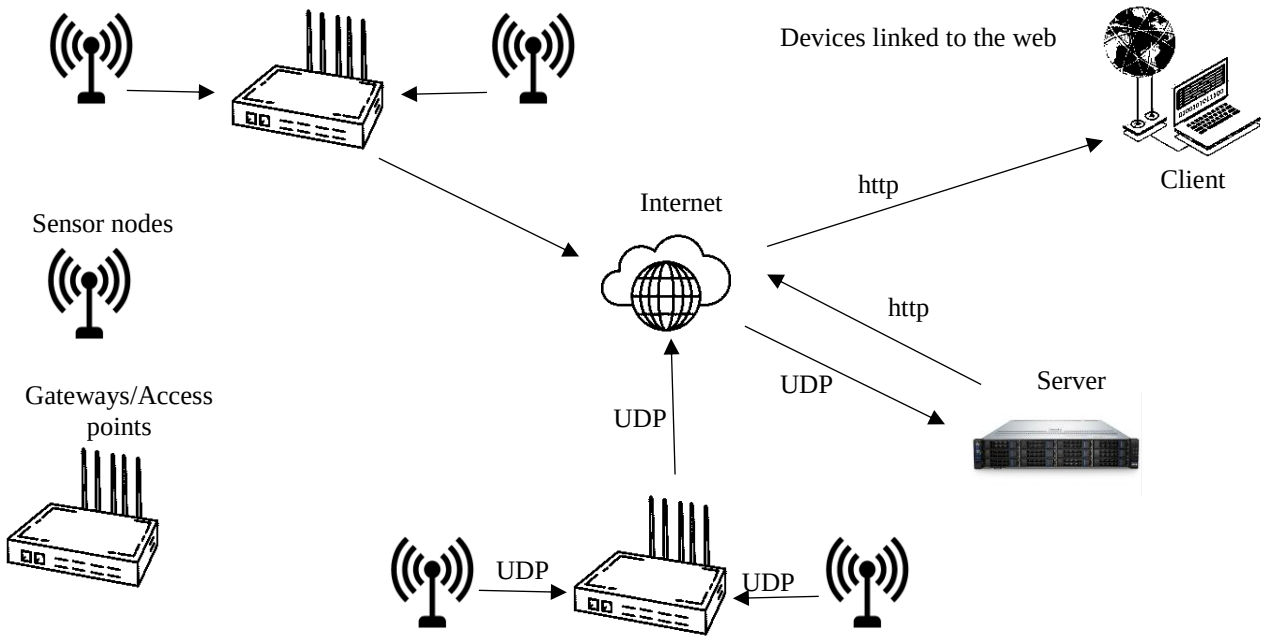

Fig 3. CPSs Infrastructure

When sensitive information is being sent, WPA2 encryption is used, but further protection is required. Although it is possible to include cryptographic algorithms, it is important to keep power consumption in mind when implementing them. The deployment of Wi-Fi advancements are direct communications to present wireless connections excludes the requirement for the gateway apart from the entry point when the servers are found in remote locations and might only be accessible through the web. Unlike ZigBee-based technologies, UDP does not need programs to encode data packets into Internet standards. Sensors used in this study transfer data to an already configured Network interface via the Internet via IEEE 802.11 b/g systems and Wi-Fi connections to preexisting entry points in the CPS.

Data Formatting

Messages are typically encoded in a restricted amount of input data that is of a fixed length, which signifies pairs of hexadecimal numbers. First, every code indicates the function it performs, and then the value linked to it. In order for the server software to properly assess the data from each sensor, every message carries adequate information. This data is included in each message: the device's MAC address, reference number, temperature reading, signal strength reading, battery voltage reading, and relative humidity reading. Voltage of cells, which powers every item is integrated in every measurement, allowing the user to know when the battery requires replacement. Depending on the RSSI value, a wireless node might choose a different network for its connection to the entry point.

Server Application

Desktop computers or embedded devices may be used to run the server software. This keeps an eye on the UDP line and responds to any messages that come in. Tables and charts may be shown on a web page from the database that contains the processed data. There is a database for information storage, a web server that allows remote accessibility to Wi-Fi sensor data, and a UDP listening and message interpreter included in the server program's code base. Additionally, the server application contains modules for delivering SMS messages and e-mails when benchmark values defined in XML documents are reached.

Server-level implementation of OPC UA would allow the scalable proposed solution to integrate with industrial surveillance and management systems. CPSs are established with federative structures as a consequence of this development. There are several ways to describe federations, but the most common is to describe them as "virtual organizations" made up of cooperating units (individuals). In [10], the concept of federations was first put out. All organizations will have access to a Common Information Space (CIS) supervised by IS (Integrated Supervisors), which provide dependability, proactivity and functionality. The IS manager is obliged to facilitate time synchronization between the various CPS components, subscription/publication support and time stamping, including encompassing all the decision-making elements of every

institution within the CPS federation. IS correspondence is obliged to enhance data exchange between the institutions that are federated through an OPC UA protocol stacks. For a more complex evaluation and high dimension of accessibility and reliability for the federated institution, data from the proposed CPSs could be integrated with data from CPSs through client application.

V. CONCLUSION AND FUTURE RESEARCH

The present study focused on wireless networking in CPS systems and its characteristics and problems. We developed and presented a situational analysis CPS on environmental control to show the challenges we've had and the steps we've taken to overcome them. Anywhere IEEE 802.11 b/g broadband service exists, data may be collected using the system's Wi-Fi sensors and servers. Wi-Fi sensors collect environmental data, such as temperatures and relative humidity measurements, which may then be shown on any Internet-enabled computer or mobile device. Incorporating energy-harvesting elements to the sensors created, as well as techniques to boost data transmission dependability and security, is being considered as future work by the authors. The development of privacy-preserving technologies that fulfill user verification, adaptability, access rights limits, and other requirements will be an important topic of study in the future.

Data Availability

No data were used to support this study.

Conflicts of Interest

The author(s) declare(s) that they have no conflicts of interest

References

[1]. M. Khayatian et al., “Plan B - design methodology for cyber-Physical Systems robust to timing failures,” ACM trans. cyber-phys. syst., 2022.
[2]. S. Wang, Y. Gong, G. Chen, Q. Sun, and F. Yang, “Service vulnerability scanning based on service-oriented architecture in Web service environments,” J. Syst. Arch., vol. 59, no. 9, pp. 731–739, 2013.
[3]. W. Wang, W. Wei, J. Hu, J. Ye, and Q. Zheng, “Knowledge unit relation recognition based on Markov logic networks,” J. Netw., vol. 9, no. 9, 2014.
[4]. B. Kutukcu, S. Baidya, A. Raghunathan, and S. Dey, “Contention grading and adaptive model selection for machine vision in embedded systems,” ACM Trans. Embed. Comput. Syst., 2022.
[5]. M. Ma, J. Zhang, and P. Wang, “DePo: Dynamically offload expensive event processing to the edge of cyber-physical systems,” IEEE Trans. Parallel Distrib. Syst., vol. 33, no. 9, pp. 2120–2132, 2022.
[6]. R. Almesaeed and E. Al-Salem, “Sybil attack detection scheme based on channel profile and power regulations in wireless sensor networks,” Wirel. netw., vol. 28, no. 4, pp. 1361–1374, 2022.
[7]. M. A. Javaheri Javid, “Aesthetic evaluation of cellular automata configurations using spatial complexity and kolmogorov complexity,” in Artificial Intelligence in Music, Sound, Art and Design, Cham: Springer International Publishing, 2021, pp. 147–160.
[8]. M. Waghmare and A. Waghmare, "Supervisory Control and Data Acquisition System (Scada) In Construction Industries", Journal of Advances and Scholarly Researches in Allied Education, pp. 203-208, 2018. Doi: 10.29070/15/56815.
[9]. "Decision making net for an autonomous roving vehicle", Neural Networks, vol. 1, p. 333, 1988. doi 10.1016/0893-6080(88)90361-9.
[10]. T. Zefferer, D. Ziegler and A. Reiter, "A Federation of Federations: Secure Cloud Federations meet European Identity Federations", International Journal for Information Security Research, vol. 8, no. 1, pp. 774-784, 2018. doi: 10.20533/ijisr.2042.4639.2018.0089.