e-ISSN: 2583 - 1941

An Evaluation of Cyber-Physical System (CPS) or Intelligent System in Which a Mechanism is Controlled or Monitored by Computer-Based Algorithms

Dr.M.Aruna Safali[1], Elangovan Muniyandy[2]

[1] IDET,JNTUK, India
[2] Professor and Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, India
*Corresponding Author Email: [1] arunasafali.m@mail.com

Abstract

This article is based on the CPS or cyber-physical system or intelligent system. The term "physical" is associated with natural and also human man-made systems that have been governed by the laws that are connected with physics while operating in continuity. CPS is described as the network of some embedded systems which establishes an interaction with both physical inputs as well as output. CPS faces the challenges of cyber and physical threats as these systems have been found to be of heterogeneous nature that has a reliance on both private and sensitive data. This study has focused on the CPS and CPS components as well. This is the integration of sensing, controlling, networking and computation into some physical objects as well as infrastructures that connect them through the help of the internet with each other. There are some CPS components that have been utilized for sensing different types of information where the CPS components can be classified into Sensing Components (SC) and also Controlling Components (CC). this study also shed light on the "Programmable Logic Controllers" (PLC) have been created for replacing hard-wired relays and have been assumed in the form of "industrial digital computers" controlling manufacturing processes including the performance of robotic performance. This study has also shed light on the improvements in unsupervised intrusion detection within CPS. Intrusion Detection Systems (IDSs) have been becoming certain building blocks for developing the CPS while detecting its potential threats and also triggering the modules to block and also mitigate those adverse impacts from cyber threats. Development via digital twin through CPS. The CPS paradigm has been involved with physical and software components that have been deeply intertwined with each other where each component has been operating on both spatial and temporal scales possessing multiple behavioural modalities and also interacting with each other.

Keywords

CPS systems, intelligent algorithms running, intelligent interfaces, open architecture system CPS, RFID- based position detection.

INTRODUCTION

The article is based on two distinct terms where cyber is associated with computation, control along with communication that have been assumed to be discrete and also logical. The term "physical" is associated with natural and also human man-made systems that have been governed by the laws that are connected with physics while operating in continuity. Therefore, the cyber-physical system (CPS) is described to be an essential mechanism that is either controlled and monitored through computer-based algorithms associated with the internet and users [1]. There is an involvement of engineered computing along with communicating systems that has been interfacing with the physical world. CPS has the power to enable the smart application and also services in a way to operate in the real-time. There is an integration between cyber and the physical worlds that takes place through exchanging the data and also sensitive information in the real-time manner.

The CPS is described as the network of some embedded systems which establishes an interaction with both physical input as well as output. There is a combination of interconnected systems within the CPS possessing the capability for monitoring IoT-related objects and also processes. CPS faces the challenges of cyber and physical threats as these systems have been found to be of heterogeneous nature that has a reliance towards both private and sensitive data. In case there is an intentional exposure of the systems then it can result in some catastrophic impacts that can pose difficulty for rousting the security measures [2]. The issues with exchanging data through CPS have been evaluated through the intentional and accidental exposure of the system in front of an unknown individual. CPS systems have been seen to be incorporated within some of the critical infrastructures such as "supply chain healthcare", "smart grid" and others that makes these systems to be attractive for attacking as per economical, espionage, criminal and others.

The study aims to discuss the mechanism within the CPS that is controlled through computer-based algorithms. However, on the other hand, there are different aspects associated with the security of CPS where there is a qualitative risk associated with the CPS system and device. The hackers have the ability to disclose the personal information with the help of creating an interception related with communication traffic through utilising tools of wireless hacking that leads to violation of confidentiality [3]. On the other hand, there are aspects of unauthorised access that is conducted through breaching of logical and physical networks to retrieve significant information that eventually leads towards privacy breaching.

LITERATURE REVIEW

CPS and CPS components

Cyber-physical systems or CPS is an intelligent system of modern computer systems and mechanisms that can be monitored and controlled by computer-based algorithms. In this context software and physical components are deeply interconnected and it is able to operate on different kinds of temporal and spatial scales. On the other hand, this also involves the transdisciplinary approach and also collaborated with mechatronics, cybernetic process, and design science. It can be said that CPS is deeply connected with the internet of things and is also able to share the fundamental architecture as well. In this context cyber-physical system presents higher coordination and combination between computational, and physical elements. Generally, cps is one kind of sensor-based communication element that can enable the autonomous system as well. It is also able to serve real-time data and help to gain desired outcomes as well.

CPS can be defined as the integration of sensing, controlling, networking and computation into some physical objects as well as infrastructures that connect them through the help of the internet with each other. [4] opined that CPS presents a "networked controlled systems" that possess some promising applications, which includes "ground-breaking transmission system" that is incorporated within the fleet of some cooperative and also autonomous vehicles, smart cities, sensing and control that have been based on "Internet-of-things" devices and others. There are some traditional control infrastructures that have been involved with CPS that can be found within the process control as well as power industries. There are some CPS components that have been utilised for sensing different types of information where the CPS components can be classified into Sensing Components (SC) and also Controlling Components (CC). SC is utilised for collecting as well as sensing of the vital information while CCis used for collecting and also monitoring the relevant information.

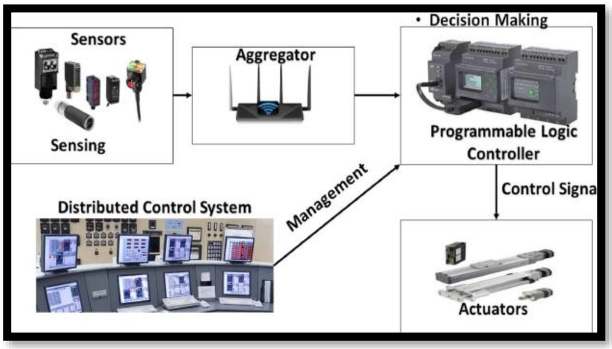


Figure 1: Components of CPS
(Source: [5])

SC is situated within the perception layer and contains sensors used for collecting data and simultaneously forward them towards aggregators followed by sending the data towards the actuators to ensure appropriate decision-making. The sensors have been utilized for recording the data from the real-world through the assistance of a correlation process named as "calibration" to evaluate the correctness within the collected data. It is important to sense the data as the data will be analyzed on the basis of those sensed data. Aggregators are seen to be situated within the transmission layer that processes received data obtained from sensors. Actuators are situated within the location layer to ensure visibility of the information towards the surrounding environment as per decision carried out by the aggregator. [5] argued that CC attains an increase in accuracy and protects the signal from certain malicious attacks.

"Programmable Logic Controllers" (PLC) have been created for replacing hard-wired relays and have been assumed in the form of "industrial digital computers" controlling manufacturing processes including the performance of robotic performance. [6] opined that "Distributed Control Systems" (DCS) are control systems allowing the distribution by the controllers throughout the CPS through utilising "central operator supervisory control". However, "Remote Terminal Units" (RTU) are assumed to be some electronic devices that have been controlled through a microprocessor named as "Master Terminal Unit" (MTU). RTU does not control the algorithms and hence does not support the control loop as compared with PLC.

Improvement of Unsupervised Intrusion Detection within CPS

Artificial Intelligence (AI)-based classifiers have relied on the algorithms of Machine-Learning (ML) that provide functionalities through which system architects may be able to integrate with CPS. [7] mentioned that CPS helps in designing the hardware and also software systems whose functionalities are dependent on computer-based sub-systems. Intrusion Detection Systems (IDSs) have been becoming certain building blocks for developing the CPS while detecting its potential threats and also trigger the modules to block and also mitigate those adverse impacts from cyber-threats. IDSs usually collects and evaluates the data from different networks and also systems that indicate the detection of both malicious and also unauthorized activities. IDS have been able to adopt AI mechanisms in the form of signature-based algorithms where the search is carried out based on the predefined patterns within the monitored data to detect the attack matching either one or more than one signatures. In this context, traditional NIds or network intrusion detection systems are able to rely on the specialized signature of expensive and previously seen attacks or difficulties for producing the traffic-labeled datasets.

These signature-based algorithms are computer-based algorithms defining a mechanism associated with attacks on CPS. [7] argued that signature-based approaches seem to be helpful for identifying the known threats while these approaches possess weakness while detecting certain slight variations within known attacks. This weakness can be assumed to be a major weakness because CPSs may be able to evolve during the operational life while at the same time, exposing the interfaces towards the multiple threats that have not been defined during the time of designing. The intrinsic aspect within the CPS eventually calls for mechanisms that have been dealing with certain unknown threats named as threats from anomaly detectors. The anomaly detectors have been dependent on the knowledge associated with threats whereas these detectors are involved in the characterization of the normal behavior within the system. This knowledge has been helpful in figuring out certain patterns within the data that do not match with expected behavior of the system therefore, these patterns are named as anomalies. On the other hand, the detection process of the attack on the network is one of the paramount tasks for the network operators on the internet. Malware, botnets, DDoS or distributed denial of service attacks, scanning activities of the network, buffer overflow attacks, viruses, and spreading worms are the basic examples of the different kinds of threats.

Anomaly-based IDS have been based on the fact that the attacks will be able to provide observable anomalies within the features that have been obtained from the respective system. [8] defined that unsupervised algorithms will be able to detect unknown threats without being dependent on labeling training data. Various “unsupervised algorithms” have been able to possess various rates in terms of missed and also wrong detections resulting in various detection capabilities. However, these algorithms have been generic and effective for detecting particular attacks on particular systems. as mentioned previously there are many kinds of threats, and these kinds of threats are daily able to compromise the normal and integrity operations of the network. In this case, principal challenges have the capability to auto-detect networking attacks. “Network intrusion detection system” or NIDS is the major warhorse of the security system of the networks. There are two different kinds of approaches such as misuse or signature-based detention and anomaly detection process.

A "cyber-physical system" (CPS) is a system that integrates computer-aided software with mechanical and electronic parts and is accessed through a data infrastructure, such as Internet-connected data centres. Cyber-physical systems are unprecedented in their complexity. The theoretical foundation of cyber-physical systems is the interconnection of embedded devices with one another across wired or wireless networks. The notion was sparked by the need for a fresh theoretical grounding in the analysis and design of massive, distributed, complex systems.

The prevalence of cyber-physical systems that can move around on their own has increased recently. In contrast to traditional embedded systems, full CPSs are more commonly conceived of as a network of elements that respond to and influence physical inputs and outputs. The concept is associated with AI-like systems, as those used to control and monitor sensor networks and robotics. As the link between computational and physical parts is improved by intelligent processes, the adaptability, autonomy, efficiency, functionality, dependability, safety, and usability of cyber-physical systems will increase significantly. Some of the areas that could benefit from this innovation include: intervention (e.g., collision avoidance), precision (e.g., robotic surgery and nano-technology manufacturing), operation in hazardous or inaccessible environments (e.g., search and rescue, fire fighting, and abyssal sea exploration), coordination (e.g., air traffic control and war), efficiency (e.g., zero-net-energy buildings), and improvement of human capabilities (eg, health monitoring).

Development of Digital Twin through CPS

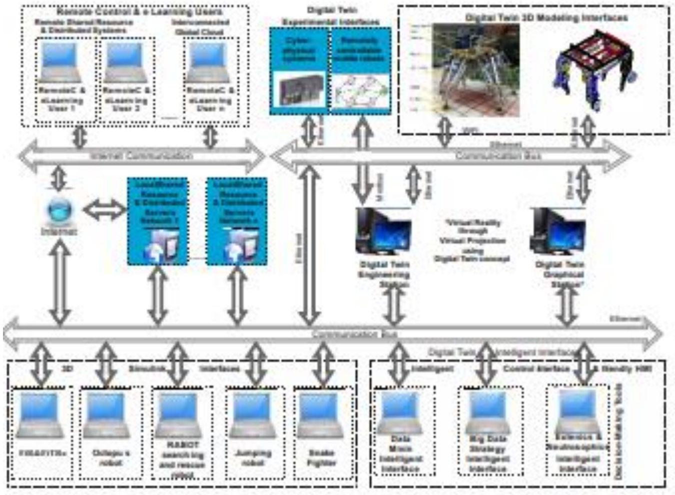

Remote Control & e-Learning Users
Remote Shared Resource & Distributed Systems
Interconnected Global Cloud
RemoteC & eLearning User 1
RemoteC & eLearning User 2
RemoteC & eLearning User n
Digital Twin Experimental Interfaces
Digital Twin 3D Modeling Interfaces
Internet Communication
Ethernet Communication Bus
Internet
Digital Twin Engineering Station
"Virtual Reality through Virtual Projection using Digital Twin concept
Digital Twin Graphical Station"
Ethernet
Communication Bus
3D Simulink Interfaces
Digital Twin Intelligent Interfaces
Intelligent Control Interface & friendly HMI
Octopus robot
RABOT searching and rescue robot
Jumping robot
Snake Fighter
Data Mining Intelligent Interface
Big Data Strategy Intelligent Interface
Intelligent Interface
Decision Making Tools

Figure 2: VIPRO Platform
(Source: [9])

An “open architecture system CPS” (CPS&OAH) along with “intelligent interfaces” (OAH) within the VIPRO platform involves “intelligent control interfaces” that is integrated within “CPS Engineering Station”. This CPS control robot vector by “virtual projection method” with the help of the concept of digital twin. An “intelligent control interfaces and genetic” algorithms have been utilized to integrate CPS within the “VIPRO- Platform” for developing digital twins. It is significant to understand that CPS itself is a significant mechanism therefore, the mechanism is required to be understood. [9] opined that VIPRO platform has been associated with the concept of digital twin where the “intelligent interface of position control” in relation with a flight formation is evaluated through “robotic system architecture”. The CPS paradigm has been involved with physical and software components that have been deeply intertwined with each other where each component has been operating on both spatial and temporal scales possessing multiple behavioural modalities and also interaction among each other.

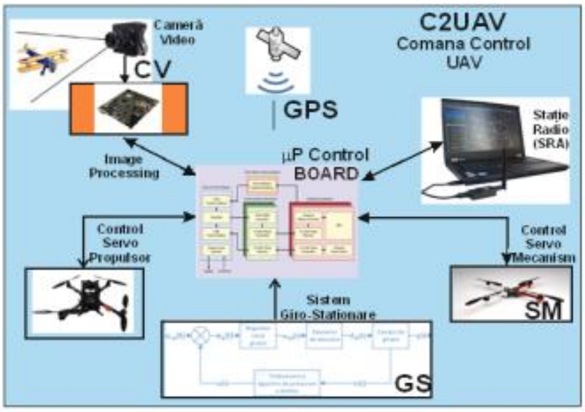


Figure 3: GCS
(Source: [9])

A virtual model synonymous with control systems has been created for the robot vector for monitoring and controlling the functions of the Ground control center (GCS). The robot vector consists of aerial robots that are quadcopter and flying robots whereas the model has been developed through computer-aided engineering and has been further integrated with IoT, Big Data Analytics and others. [9] argued that GCS aims to offer a stable behaviour for the robot vectors possessing maximum performance. “Multi-agent collaborative system” in association with “intelligent multi-agent optimisation and decision interfaces” have been implemented upon GCS for the application of the digital twin. The system is prepared from “3D robot vectors” that includes “aerial”, “aquatic” and others acting as the intelligent agents for commanding the center CTC2, which is considered to be a “mission management center” as CMM and also a “radio communication system” such as “SRA, SRB, SRC”. It has been further found that GCS have used algorithms on artificial intelligence for the purpose of decision-making and also optimisation. The purpose of multi-agent collaboration is to share messages, transmit those messages in real-time and others. “Network intrusion detection system” or NIDS is the major warhorse of the security system of the networks.

Unsupervised Network Intrusion Detection System (UNIDS) has the capability to detect an attack on networks based on the training, signatures, and traffic-labeled instances based on the observation as well.

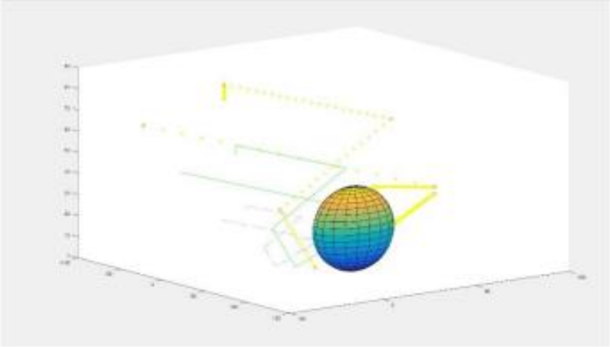


Figure 4: Search Space
(Source: [9])

There is an optimization issue witnessed within the GCS system especially in the “digital twin control functions” where it has been seen that the positioning of those quadcopters increases the wing-base connectivity therefore, this wing will be provided by the algorithm that notices the region-specific topology. [9] stated that the exposed issue will be considered to be trivial in case obstacles have been absent within the search space. The speed, path and also the obstacle have been pointed out in the above image that have been randomly generated whereas the solution has been proposed through “intelligent algorithms running”.

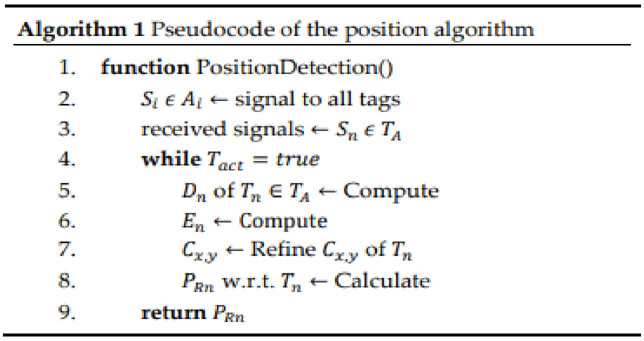
$$[max]\ F\big(tr(A), tr(B), tr(C)\big)$$

$$\begin{cases} v_B \leq v_{max}^{quad} \\ v_C \leq v_{max}^{quad} \\ Im\big(tr(B)\big) \cap Obst = \emptyset \\ Im\big(tr(C)\big) \cap Obst = \emptyset \end{cases}$$

Figure 5: Problem on optimization
(Source: [9])

As per the above equation, F is the measurement associated with wing-base connectivity whereas “tr(A), tr(B) and tr(C)” are aerian vectors while A is considered to be the base, B and C are some quadropters and others. [10] opined that there are some optimisation algorithms such as fmincon that are proprietary algorithm from Matlab trying to figure out the minimum from the constraint function while AG – genetic algorithms provides iterative improvement within a population while utilising operators however, these algorithms have been an essential aspect of “Matlab software package”.

METHODOLOGY



Algorithm 1 Pseudocode of the position algorithm

```
function PositionDetection()
    $S_i \in A_i$ ← signal to all tags
    received signals ← $S_n \in T_A$
    while $T_{act} = true$
        $D_n$ of $T_n \in T_A$ ← Compute
        $E_n$ ← Compute
        $C_{x,y}$ ← Refine $C_{x,y}$ of $T_n$
        $P_{Rn}$ w.r.t. $T_n$ ← Calculate
    return $P_{Rn}$
```

Figure 6: Algorithms for position detection
(Source: [11])

CPS systems have been incorporated in different production areas within the industries. In this aspect, there are different algorithms utilised for monitoring the physical devices, production lines and others. There are different algorithms that have been utilised for controlling the industrial devices, transfer vehicles and others. The global position of some logistic robots and also workloads have been determined while encoder-based methods have been utilised for locating the place of those mobile robots whereas encoder data may delve into providing error accumulation. “Tag based position detection” seems to be another essential method for locating those mobile robots within the operating environment. A “RFID- based position detection” has been recommended through the help of “RFID tags” and “reader” [11]. The tags have been placed in accordance with some predefined parameters on the floor in which a mobile robot will be able to make a certain movement process. The predefined parameters have been assumed as signals (S_i, S_n), while active task (T $_{act}$), distance Error (E_n), “between the tags” (T_n E T_A) and others.

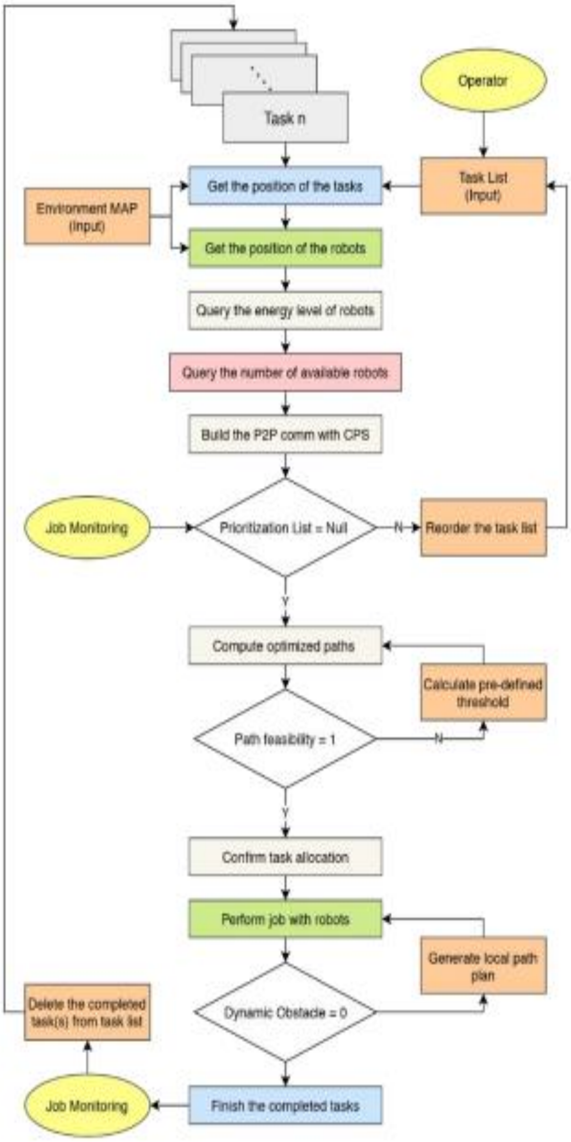
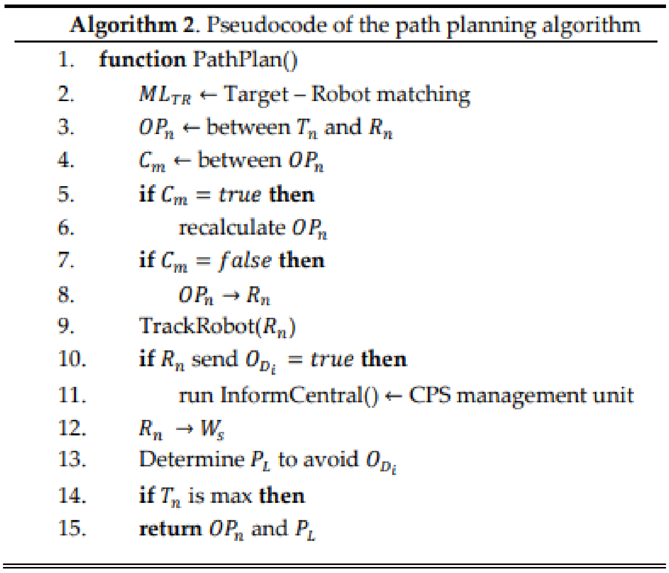

Task n
Operator
Get the position of the tasks
Task List
(Input)
Environment MAP
(Input)
Get the position of the robots
Query the energy level of robots
Query the number of available robots
Build the P2P comm with CPS
Job Monitoring
Prioritization List = Null
N
Reorder the task list
Y
Compute optimized paths
Calculate pre-defined threshold
Path feasibility = 1
N
Y
Confirm task allocation
Perform job with robots
Generate local path plan
Delete the completed task(s) from task list
Dynamic Obstacle = 0
Job Monitoring
Finish the completed tasks

Figure 7: “Adaptive operation model” of the robots within CPS
(Source: [11])

Multitasking is considered to be a challenging aspect for the robots within the “CPS configured environments”. The major parameters of multitasking have been defined where these parameters have been considered to be an environment map showcasing the static obstacles such as product lines, position of the available tasks, energy level of the robots, robot position and others [11]. The energy level of the robots has been questioned followed by determining the target and robot positions.

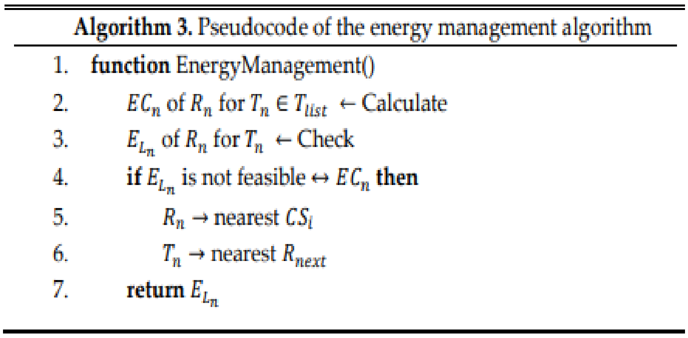


Algorithm 2. Pseudocode of the path planning algorithm

```
function PathPlan()
    $ML_{TR}$ ← Target – Robot matching
    $OP_n$ ← between $T_n$ and $R_n$
    $C_m$ ← between $OP_n$
    if $C_m = true$ then
        recalculate $OP_n$
    if $C_m = false$ then
        $OP_n \to R_n$
    TrackRobot($R_n$)
    if $R_n$ send $O_{D_i} = true$ then
        run InformCentral() ← CPS management unit
    $R_n \to W_s$
    Determine $P_L$ to avoid $O_{D_i}$
    if $T_n$ is max then
    return $OP_n$ and $P_L$
```

Figure 8: Algorithm for path planning
(Source: [11])

The approaches for path planning are “Dijkstra, A*, D*, APF, RRT, Probabilistic Roadmap” and others. For example, ML_{TR} parameter is the matching list of the task robot while OP_n is assumed to be the optimal path, CPS is considered to be central management unit, P_L is assumed to local path and others.

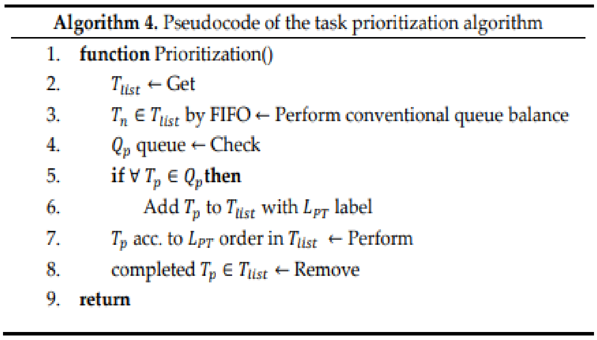


Algorithm 3. Pseudocode of the energy management algorithm

```
function EnergyManagement()
    $EC_n$ of $R_n$ for $T_n \in T_{list}$ ← Calculate
    $E_{L_n}$ of $R_n$ for $T_n$ ← Check
    if $E_{L_n}$ is not feasible ↔ $EC_n$ then
        $R_n$ → nearest $CS_i$
        $T_n$ → nearest $R_{next}$
    return $E_{L_n}$
```

Figure 9: Algorithm for energy management
(Source: [11])

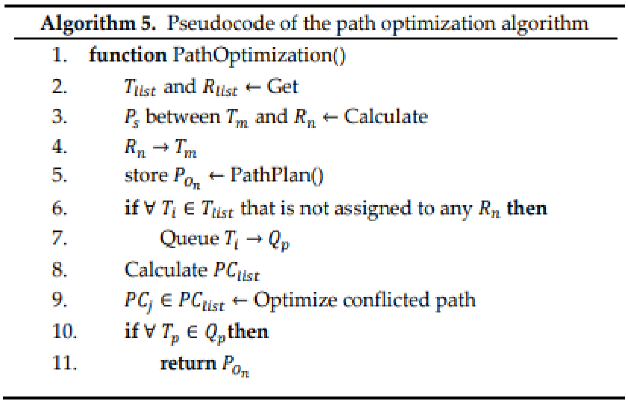
The battery needs to be researched when the charge of the battery will be down, which may delay the production, increase the expenses and decrease efficiency. Energy level of the robot EL_n, given time T_n, and the energy consumption of the task is EC_n.



```
Algorithm 4. Pseudocode of the task prioritization algorithm
function Prioritization()
    $T_{list}$ ← Get
    $T_n \in T_{list}$ by FIFO ← Perform conventional queue balance
    $Q_p$ queue ← Check
    if $\forall\, T_p \in Q_p$ then
        Add $T_p$ to $T_{list}$ with $L_{PT}$ label
    $T_p$ acc. to $L_{PT}$ order in $T_{list}$ ← Perform
    completed $T_p \in T_{list}$ ← Remove
return
```

Figure 10: Algorithm for task prioritisation
(Source: [11])

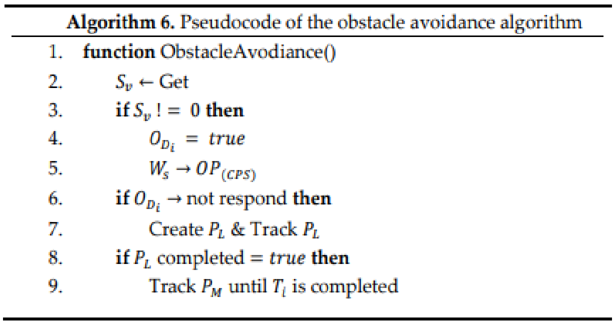
T_{list} is assumed to the task list however, Q_p is assumed to be prioritisation queue.



```
Algorithm 5. Pseudocode of the path optimization algorithm
function PathOptimization()
    $T_{list}$ and $R_{list}$ ← Get
    $P_s$ between $T_m$ and $R_n$ ← Calculate
    $R_n \rightarrow T_m$
    store $P_{O_n}$ ← PathPlan()
    if $\forall\, T_i \in T_{list}$ that is not assigned to any $R_n$ then
        Queue $T_i \rightarrow Q_p$
    Calculate $PC_{list}$
    $PC_j \in PC_{list}$ ← Optimize conflicted path
    if $\forall\, T_p \in Q_p$ then
        return $P_{O_n}$
```

Figure 11: Algorithm for path optimisation
(Source: [11])

T_i is the target whereas PC_{list} is the possible conflict, T_{list} and R_{list} are some available tasks.



```
Algorithm 6. Pseudocode of the obstacle avoidance algorithm
function ObstacleAvodiance()
    $S_v$ ← Get
    if $S_v$ ! = 0 then
        $O_{D_i}$ = $true$
        $W_s \rightarrow OP_{(CPS)}$
    if $O_{D_i}$ → not respond then
        Create $P_L$ & Track $P_L$
    if $P_L$ completed = $true$ then
        Track $P_M$ until $T_i$ is completed
```

Figure 12: Algorithm for obstacles avoidance
(Source: [11])

Two varieties of obstacles have been identified within the CPS operating environment such as static obstacles while the second obstacle is about the dynamic obstacles. In this respect, the obstacles have not been impacting the path trajectories where the robot needs to perform the assigned task. Conversely, dynamic obstacles have been detected through sensors (S_v). It is further seen that parameter OD_i have been presenting the i_{th} dynamic obstacle within that CPS environment.

the environment

FINDINGS AND DISCUSSION

Experimental results

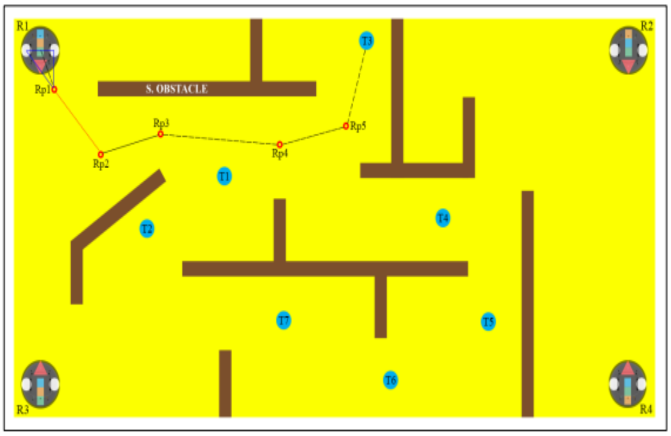


Figure 13: Operating Environment
(Source: [11])

There are around 4 robots in association with 4 7 tasks assumed as targets where static obstacles have been defined through brown color. Every robot has been assumed to be a dynamic obstacle in respect to other robots however, human beings have been considered to be some dynamic obstacles. The operating environment has been considered an “adaptive operation model” which has been defined in the above image where the simulation environment has been modeled through “MATLAB and Python programming”. “R1, R2” and others are assumed to be robots while “T1, T2” and others are some targets and “Rp1, Rp2” and others are some RFID tags [11]. RFID tags have been utilised for identifying the positions of the robots followed by the increase in the total number of “robots” and “targets”. The algorithm on multitask has been helpful for identifying the closest task and target.

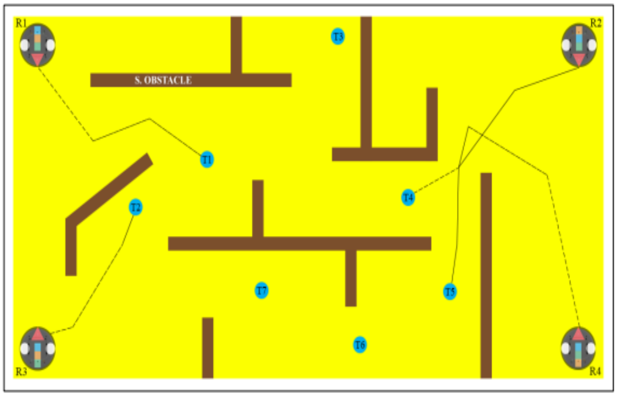


Figure 14: Path plans and multiple robots have been assigned with tasks
(Source: [11])

In case two robots have been found to be within a specific operating environment through following a particular path then that foremost task seems to have been prioritized. The algorithm is used for calculating the distance among the robots as well as targets. In case there is absence of targets then that distance will also be calculated [12]. The structure has been found to be helpful for determining the shortest paths among the allocated targets towards the robots.

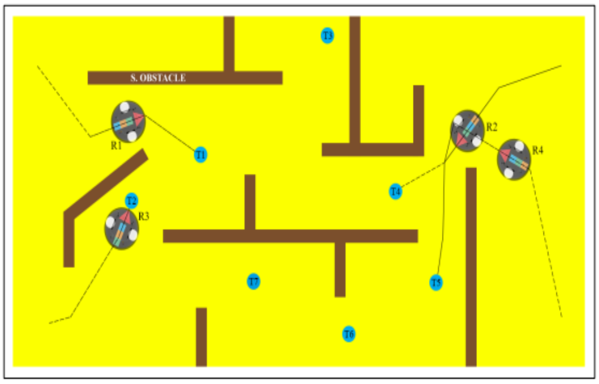
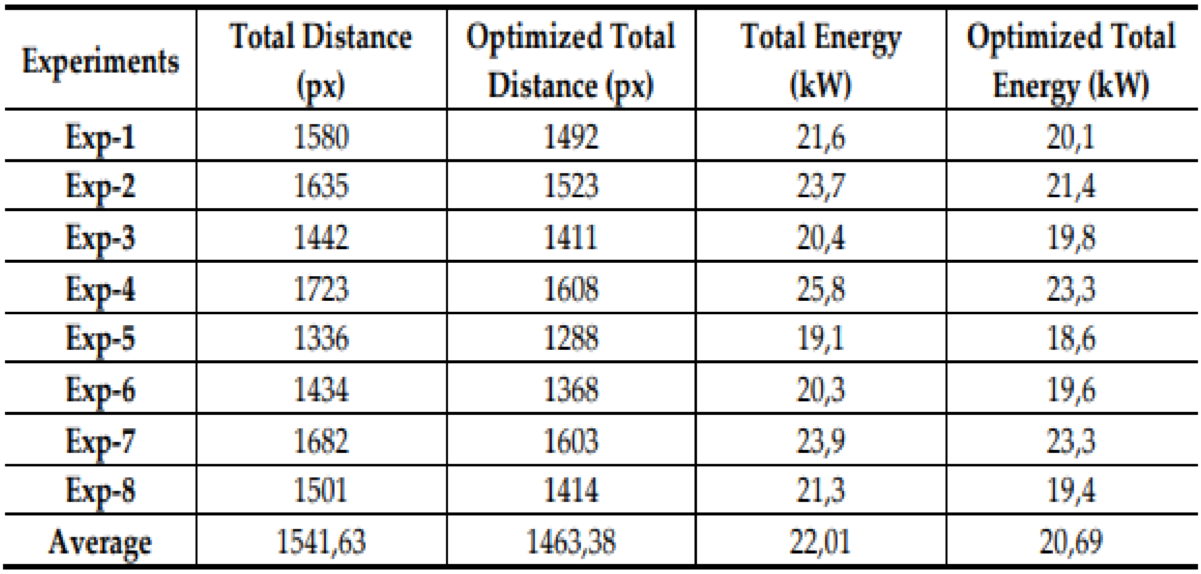


Figure 15: Process of obstacle avoidance
(Source: [11])

According to the above image, it can be seen that the "R2 and R4" robots have faced the obstacles while performing those assigned tasks while the R2 robot can be considered to be a "dynamic obstacle" in front of the R4 Robot within a situation. It is the R4 robot that has been waiting for that R2 robot to cross towards the T4 target. "Obstacle detection sensors" related with R4 have not delved into identifying the obstacles while the R4 robot has been seen to be maintaining the movement towards T5 target.



Experiments	Total Distance (px)	Optimized Total Distance (px)	Total Energy (kW)	Optimized Total Energy (kW)
Exp-1	1580	1492	21,6	20,1
Exp-2	1635	1523	23,7	21,4
Exp-3	1442	1411	20,4	19,8
Exp-4	1723	1608	25,8	23,3
Exp-5	1336	1288	19,1	18,6
Exp-6	1434	1368	20,3	19,6
Exp-7	1682	1603	23,9	23,3
Exp-8	1501	1414	21,3	19,4
Average	1541,63	1463,38	22,01	20,69

Table 1: Experimental results related with distance cost and energy
(Source: [11])

There are around 8 experiments where every experiment has been seen to be repeated around 5 times while average values related with those experiments have been subsequently calculated to figure out the results. The total distance followed by "optimized total distance", "total energy" and others have been evaluated.

REFERENCES

[1] *Interdisciplinary cyber physical systems (ICPS) Division: Department of Science &amp; Technology: Department of Science (no date) The in file Open in new window*. Available at: https://dst.gov.in/interdisciplinary-cyber-physical-systems-icps-division#:~:text=A%20Cyber%20Physical%20System%20(CPS,computational%20algorithms%20and%20physical%20components. (Accessed: January 2, 2023).

[2] J.P.A. Yaacoub, O. Salman, H.N. Noura, N. Kaaniche, A. Chehab and M. Malli. Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and microsystems*, *77*, p.103201, 2020

[3] F. Tao, Q. Qi, L. Wang and A.Y.C. Nee. Digital twins and cyber–physical systems toward smart manufacturing and industry 4.0: Correlation and comparison. *Engineering*, *5*(4), pp.653-661, 2019

[4] G.D. Putnik, L. Ferreira, N. Lopes and Z. Putnik. What is a Cyber-Physical System: Definitions and models spectrum. *Fme Transactions*, *47*(4), pp.663-674, 2019

[5] M.C. Chiu, C.D. Tsai and T.L. Li. An integrative machine learning method to improve fault detection and productivity performance in a cyber-physical system. *Journal of Computing and Information Science in Engineering*, *20*(2), p.021009, 2020

[6] D.G. Rosado, A. Santos-Olmo, L.E. Sánchez, M.A. Serrano, C. Blanco, H. Mouratidis and E., Fernandez-Medina. Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern. *Computers in Industry*, *142*, p.103715, 2022

[7] T. Zoppi, M. Gharib, M. Atif, and A., Bondavalli. Meta-Learning to Improve Unsupervised Intrusion Detection in Cyber-Physical Systems. *ACM Transactions on Cyber-Physical Systems (TCPS)*, *5*(4), pp.1-27, 2021

[8] M.C. Chiu, C.D. Tsai and T.L. Li. An integrative machine learning method to improve fault detection and productivity performance in a cyber-physical system. *Journal of Computing and Information Science in Engineering*, *20*(2), p.021009, 2020

[9] L. Vladareanu, V. Vladareanu, A.I. Gal, O.D. Melinte, M. Pandelea, M. Radulescu and A.C. Ciocîrlan. Digital Twin in 5G Digital era developed through cyber physical systems. *IFAC-PapersOnLine*, *53*(2), pp.10885-10890, 2020

[10] H. Ye, J. Liu, W. Wang, P. Li, T. Li, and J. Li. Secure and efficient outsourcing differential privacy data release scheme in cyber–physical system. *Future Generation Computer Systems*, *108*, pp.1314-1323, 2020

[11] E.DÖNMEZ, F.OKUMUŞ and Z, F. KOCAMA. ADAPTIVE OPERATION MODEL FOR INTERIOR SMART LOGISTICS IN CYBER PHYSICAL SYSTEMS. *Konya Mühendislik Bilimleri Dergisi*, *9*(4), pp.965-980.

[12] S. Tan, J.M. Guerrero, P. Xie, R. Han, and J.C. Vasquez. Brief survey on attack detection methods for cyber-physical systems. *IEEE Systems Journal*, *14*(4), pp.5329-5339, 2020