Cybersecure Omnidirectional Autonomous Mobile Robot (OAMR) for Indoor Manipulation of Roll-to-Roll Flexible Printed Circuits (FPC)

Brijesh Patel, Shang-Chen Kuo, Chih-Chi Yuan, Chin-Hsing Kuo, Ming-Hau Tsai, Lung Chen Liang, Jen-Wei Yeh, Chung-Hsien Kuo, *Member, RST*, Chao-Lung Yang and Po Ting Lin*, *Member, RST*

Abstract— **In the current era of automation, there is a growing demand for Autonomous Mobile Robots (AMRs) specifically designed for indoor mobility, where space is often limited. Operating AMRs effectively within such confined environments, where object manipulation poses numerous challenges, is a significant undertaking. This paper introduces the design and development of an Omnidirectional Autonomous Mobile Robot (OAMR) tailored for the indoor manipulation of roll-to-roll flexible printed circuits (FPC) with a payload capacity of 20 Kg. This OAMR is equipped with Mecanum wheels and a two-degree-of-freedom arm, showcasing enhanced maneuverability, which is well-suited for navigating and manipulating objects in tight spaces. Structural analysis of the platform (Application layer) affirms its robustness, ensuring dependable performance in demanding industrial settings with a good safety factor. The control system consists of a controller that implements motion control and multi-sensor data processing. To navigate the OAMR in the indoor environment, LiDAR, along with visual sensors, are fused. Furthermore, the paper delves into the cybersecurity authentication of the OAMR, advocating for the adoption of a zero-trust framework, public key infrastructure (PKI), and digital certificate trust chain technology to safeguard network communication and identity authentication within smart factory environments.**

Index Terms*—*Autonomous Mobile Robot (AMR), Flexible Printed Circuit (FPC), Mobile Manipulation, Cybersecurity.

I. INTRODUCTION

In the current industrial revolution, the expectation for Autonomous Mobile Robots (AMR) has risen significantly for indoor applications [1]. Smart manufacturing requirements have created the space for application-based autonomous mobile robots [2, 3]. The work environment exerts a significant influence on the flexibility and safety of mobile robots [4]. Consequently, it is imperative for mobile robots to operate with a low turning radius and exhibit adaptable movement capabilities, especially when navigating indoor spaces. These characteristics are essential for ensuring optimal performance and safety in dynamic and confined work environments, where maneuverability and flexibility are paramount [5]. To achieve localization, navigation proficiency, and obstacle avoidance, AMRs rely on an extensive array of sensors, external reference points, and sophisticated algorithms [6, 7].

Different omnidirectional mobile robots have been developed in recent years consisting of various types of steerable wheels [8]. For a multi-directional approach, Mecanum wheels are more suitable for carrying heavy payloads with easy control capabilities [9].To deal with AMR localization, onboard sensors with sophisticated fusion algorithms have been integrated and extensively investigated [10, 11]. Obstacle avoidance is essential for autonomous mobile robots when considering a safe environment [12]. The mobile robots must confirm the presence of an obstacle as accurately as possible with the estimation of its position and must respond appropriately to that. The Lidar sensor was typically used to overcome this problem, which is directly related to the distance of objects and obstacles surrounding the robot; the data from this sensor are crucial and are used for detection [12, 13].

AMR is a cyber-physical system (CPS) comprising physical entities with perception, processing, and decision-making abilities [14]. These intelligent mobile robots are crucial in facilitating flexible and efficient material flow within intelligent manufacturing systems, especially in multi-station and multi-task applications [15, 16]. Achieving seamless data exchange among physical entities depends on unified interfaces and communication standards [11], which can be challenging due to the need for upgrades in traditional physical entities. Thus, AMRs should be designed for intelligent manufacturing systems. However, they are vulnerable to network security risks, including hacking and unauthorized access [17]. In smart factories, safeguarding AMR security is vital, using technologies like zero trust [18], public key infrastructure (PKI) [19], and digital certificate trust chain [20]. The framework in this study ensures robust identity authentication and secure communication by utilizing PKI technology and digital certificates.

Brijesh Patel is a Postdoctoral Researcher in Department of Mechanical Engineering at National Taiwan University of Science and Technology (NTUST-ME), Taipei, Taiwan. (e-mail: aero.brijesh@gmail.com)

Shang-Chen Kuo and Chih-Chi Yuan are MS students in NTUST-ME. (e-mails: janicedal0624@gmail.com and chihchiyuan2@gmail.com)

Chin-Hsing Kuo is a Senior Lecturer in School of Mechanical, Materials, Mechatronic and Biomedical Engineering, University of Wollongong (UOW), NSW, Australia. (e-mail: chkuo@uow.edu.au)

Ming-Hau Tsai is with Industrial Technology Research Institute (ITRI), Hsinchu, Taiwan. (e-mail: tinotsai@itri.org.tw)

Lung Chen Liang is with Career Technology Manufacturing Company, Limited, New Taipei City, Taiwan. (e-mail: david.liang@carrergroups.com)

Jen-Wei Yeh is with Taiwan Certification Authority Corporation (Taiwan-CA Inc.). (e-mail:jw.yeh@twca.com.tw)

Chung-Hsien Kuo is a Professor in Department of Mechanical Engineering at National Taiwan University (NTU), Taipei, Taiwan. (e-mail: chunghsien@ntu.edu.tw)

Chao-Lung Yang is a Professor in Department of Industrial Management, NTUST. (e-mail: clyang@mail.ntust.edu.tw)

Po Ting Lin is a Professor in NTUST-ME and Intelligent Manufacturing Innovation Center (IMIC) at NTUST. (Corresponding author. phone: +886-983-033-147; e-mail: potinglin@mail.ntust.edu.tw)

This paper focuses on designing and developing an Omni-Directional Autonomous Mobile Robot (OAMR) based on four Mecanum wheels. The design is divided into two layers: the autonomous vehicle layer, known as the chassis layer, and another layer for application and manipulation. The multi-layer mechanism includes a manipulation system based on linear actuators to handle Roll-to-Roll Flexible Printed Circuits (FPC). Consequently, an industrial-grade controller is used for motion control, and an industrial-grade PC for multisensory data processing. We fuse data from wheel encoders, a Kinect visual sensor, and Lidar for localizing the mobile robot to achieve autonomous navigation in unknown semi-structured indoor environments. Additionally, we propose a framework based on zero-trust architecture and PKI to enhance the security of network communication and identity authentication for the OAMR.

II. Multi-layer Mechanical System Design and Structural Analysis of Omnidirectional Autonomous Mobile Robot

This study presents a multi-layered autonomous vehicle design comprising a distinct chassis and application layer. The chassis layer forms the foundational framework, housing essential components such as circuits, batteries, and air compressors. These components collectively underpin the vehicle's autonomous operation and functionality.

In contrast, the application layer is tailored to enable the vehicle to manipulate objects weighing up to 20 kilograms. This layer is designed with a focus on two key attributes: removability and adaptability. This design feature allows for the detachment and replacement of the application layer, enhancing the vehicle's versatility for a wide array of applications. Whether the task involves object manipulation or other functions, the adaptable application layer ensures the autonomous vehicle's efficient and effective fulfillment of its intended purpose.

A. Chasis Layer

In the typically confined indoor environment of the manufacturing area, there arises a need for omnidirectional mobile robots capable of nimble navigation in small and tight spaces. Consequently, the design of the chassis layer should be able to accommodate and support all the components within itself.

The vehicle chassis is designed with dimensions measuring 900mm in length, 820mm in width, and 500mm in height, and it has a total weight of 164kg. A 3D view depicting the overall chassis structure is illustrated in Fig. 1. Constructed primarily from S45C carbon steel, the chassis incorporates square tubes that are 100mm in length and 50mm in width. These tubes offer dedicated space for housing vehicle circuitry, batteries, and an air compressor.

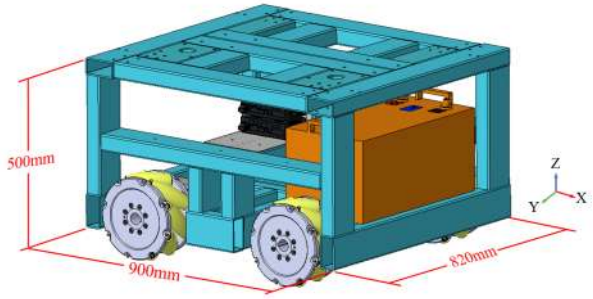


Fig. 1. 3D view of chassis design of OAMR

The chassis is equipped with four ten-inch Mecanum wheels to enhance mobility and maneuverability. These wheels are specially designed with a diameter of 245mm and are constructed from lightweight yet durable aluminum alloy material. Each Mecanum wheel weighs 15 kilograms, showcasing a remarkable load-bearing capacity of up to 1000 kilograms. This substantial weight-bearing capability contributes to the vehicle's versatility and ability to handle various tasks. The Mecanum wheel design and its placement in the chassis are shown in Fig. 2.

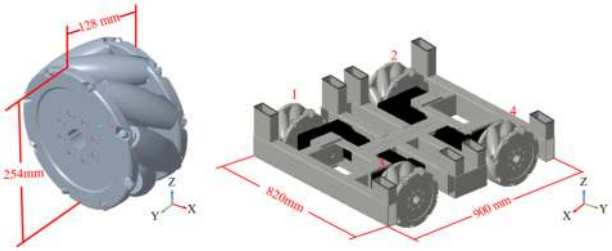


Fig. 2. Mecanum wheel design and its placement on the chassis

Mecanum wheels provide omnidirectional movement capabilities, encompassing three degrees of freedom shown in Fig. 3, granting the vehicle exceptional handling capabilities and unmatched flexibility, particularly when navigating tight or confined spaces. This dynamic mobility aspect empowers the autonomous vehicle to perform tasks efficiently. The brushless motor BLV series incorporates permanent magnets within the motor unit, allowing it to achieve a slim, high-output design. With a motor length of 104mm, it can deliver a maximum power output of 400W, generating an instantaneous maximum torque of 1.3Nm. The OAMR is powered by a lithium-ion battery (DC-52V/50Ah). The actual OAMR chassis image showing the components is illustrated in Fig. 4.

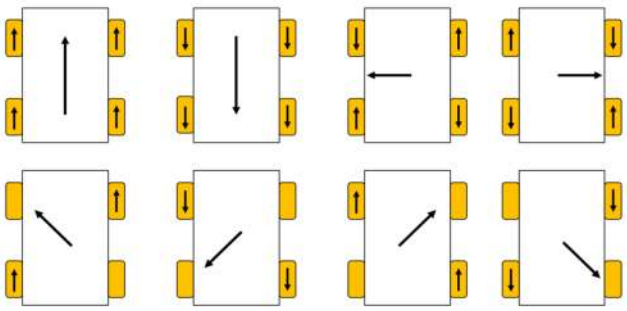
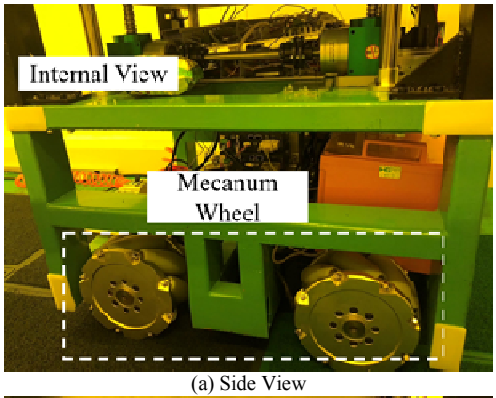
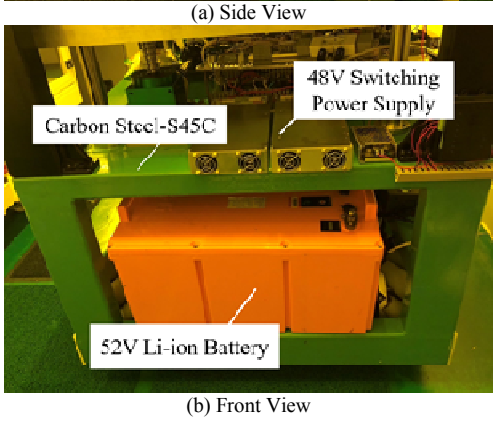


Fig. 3. Degree of freedom of vehicle



(a) Side View



(b) Front View

Fig. 4. OAMR chassis layer

B. Application Layer

The main purpose of the application layer is to manipulate FPC rolls weighing 10kg and feed them to the machine. The application layer for placing the hollow cylinder consists of a ball screw mechanism that extends/retracts along the Z-axis, a ball screw with a horizontal grip key for gripping objects, and a linear slide rail. Therefore, a comprehensive analysis of the selected motor's torque is carried out before constructing the prototype.

This design chooses a motor with a torque rating of 1.3Nm. This motor is synchronized with a C7 lead size 10mm ball screw, which serves as the primary driver for the mobile platform. A critical aspect of this configuration is the translation of one rotation into a linear movement of 10mm. The force F_a that propels the nut in a forward direction (N) is represented as F, the motor input torque (N-m) is denoted as T, the motor efficiency is represented by η, and the Ball Screw lead (mm) is denoted as R. The input motor can be calculated using Eq. (1):

$$T = \frac{F_a \cdot R \times 10^{-3}}{2\pi\eta} \tag{1}$$

After meticulous calculations, the torque requirements for the telescopic arms are determined to be 1.194 Nm. Additionally, for the motor responsible for vertically lifting the platform, which is equipped with an 8-to-1 gearbox, the torque is evaluated at 1.144 Nm. Both of these calculated torque values comfortably fall within the rated torque capacity of the selected servo motor. The overall dimensions of the application layer measure 900mm in length, 820mm in width, and 790mm in height, with a total weight of approximately 260kg, as shown in the assembly diagram in Fig. 5.

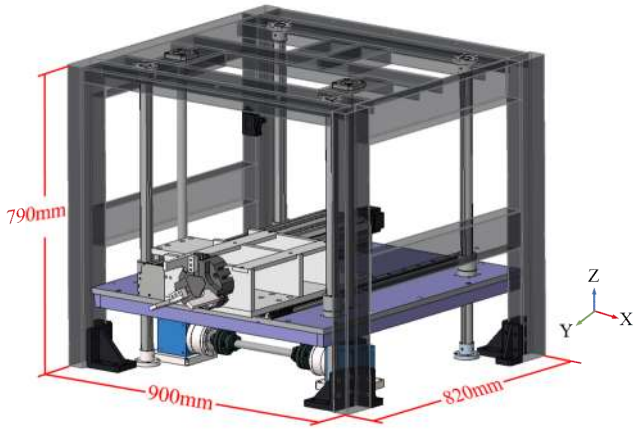


Fig. 5. 3D view of the application layer

The framework of the application layer is constructed using medium carbon steel S45C as the primary material. The central lifting platform, which measures 820mm in length, 750mm in width, and 15mm in thickness, is fabricated from a lighter aluminum alloy. To enhance the structural integrity of the lifting platform, we have added 35mm thick beams around all four sides. The 3D view of the lifting mechanism is illustrated in Fig. 6. The real-time application layer of OAMR, consisting of all the components, is shown in Fig. 7.

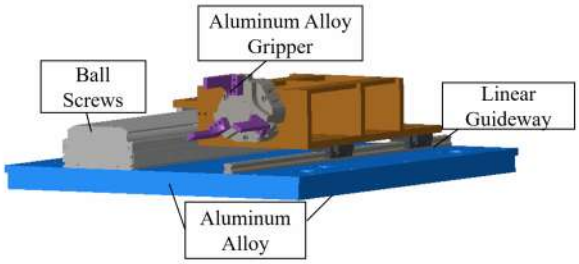
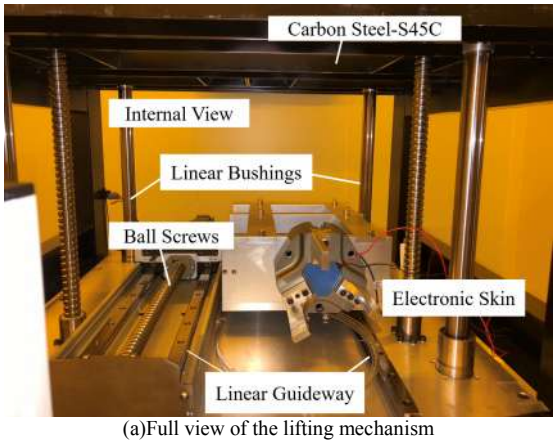
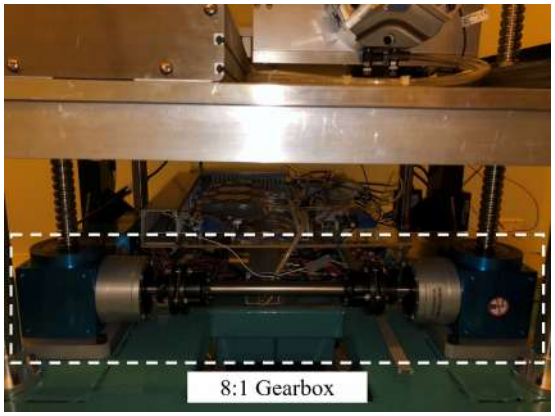


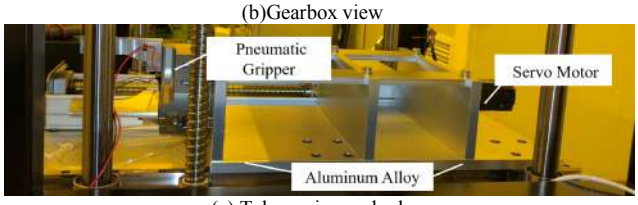
Fig. 6. 3D view of lifting platform with telescopic arm



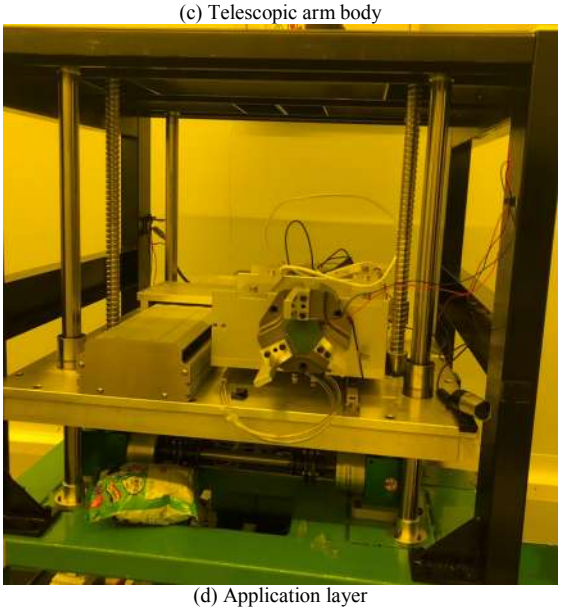
(a)Full view of the lifting mechanism



(b)Gearbox view



(c) Telescopic arm body



(d) Application layer

Fig. 7. OAMR Application layer

C. Finite Element Analysis of Working Platform

To assess the compliance of the machining and component designs of both the lifting platform and the telescopic arms with specified requirements, we conducted a comprehensive Finite Element Analysis (FEA) of the Structure of the main manipulation mechanism within the application layer. Our methodology included creating a 3D model using Creo Parametric, as illustrated in the diagram, and utilizing Ansys analysis software for a thorough structural assessment.

The FEA results provided valuable insights into various parameters, including maximum principal stresses, tensile force values, and overall deformation experienced by the application layer under applied pressure. Additionally, we applied the von Mises stress criterion to assess stress distribution across the structure and identify stress concentration areas. For constructing the lifting platform and the arms, we utilized aluminum alloys characterized by a stress-strain value of 469 MPa. The safety factor is crucial for ensuring the structural integrity of the components. This FEA analysis is illustrated in Figs. 8-13 critically evaluates the application layer's structural performance and safety margins. Overall, FEA analysis results are presented in Table I and Table II.

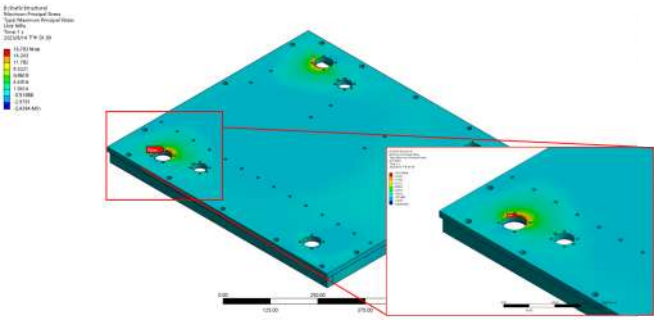


Fig. 8. FEA analysis of platform for maximum principal stress

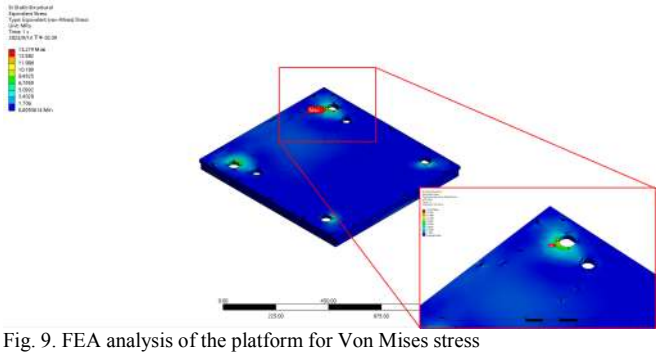


Fig. 9. FEA analysis of the platform for Von Mises stress

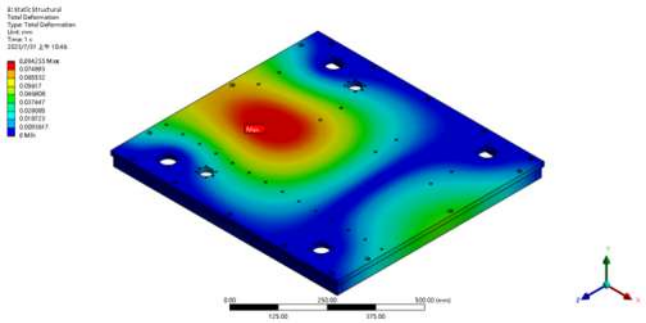


Fig. 10. FEA analysis of the platform for total deformation

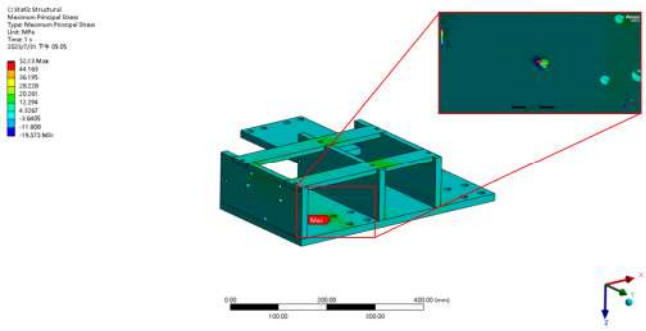


Fig. 11. FEA analysis of the telescopic arm body for maximum principal stress

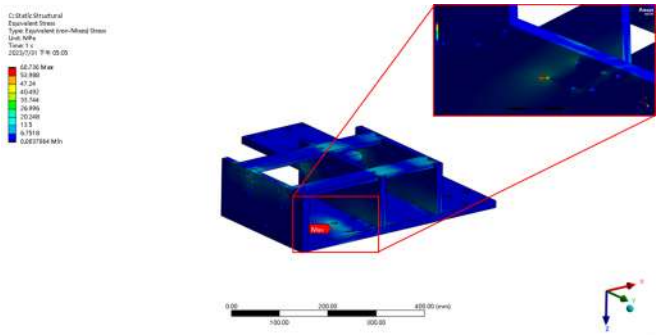


Fig. 12. FEA analysis of the telescopic arm body for Von Mises stress

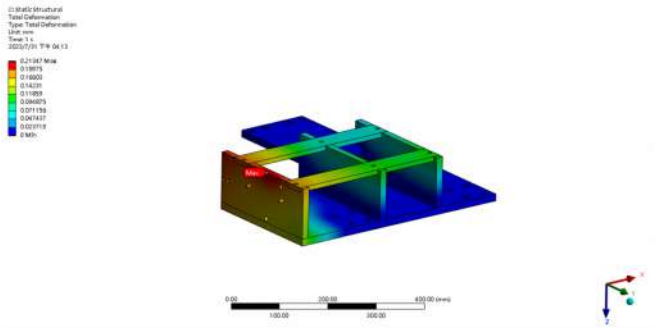


Fig. 13. FEA analysis of the telescopic arm body for total deformation

Table I
FEA RESULTS FOR PLATFORM OF APPLICATION LAYER

Property	Value
Von-Mises Stress（Mpa）	15.279
Max Principal Stress（Mpa）	16.703
Min Principal Stress（Mpa）	1.9905
Von-Mises safety factor	30.636
Max Principal Stress safety factor	82.079
Total Deformation（mm）	0.084255

Table II
FEA ANALYSIS RESULTS OF THE ARM BODY

Property	Value
Von-Mises Stress（Mpa）	60.736
Max Principal Stress（Mpa）	52.13
Min Princioal Stress（Mpa）	9.2603
Von-Mises safety factor	7.722
Max Principal Stress safety factor	8.997
Total Deformation（mm）	0.21347

Taking the analyzed stress values, we can ascertain the overall stress distribution using von Mises stress. The von Mises safety factors for the arms and the lifting platform are 7.722 and 30.636, respectively. Additionally, the safety factors for Maximum Principal Stress are 8.997 for the arms and 28.079 for the lifting platform. Importantly, all of these data points comfortably satisfy the safety thresholds.

III. Control Design and System Architecture

A. Control Hardware

In software, we categorize our system into four major components: Application, Chassis, Position, and human-machine interface (HMI), as described in Fig. 14. Both the Application and Chassis layers are connected to an Edge Gateway and communication with an industrial computer is facilitated through an Ethernet Switch. The Edge Gateway plays a critical role in the network architecture, serving as a key link between the internal corporate network and the external internet. It integrates several vital functions to enhance network performance, security, and availability. Primarily, the Edge Gateway provides robust network security protection through powerful security features such as firewalls, intrusion detection, and intrusion prevention systems, thwarting malicious attacks and data leaks.

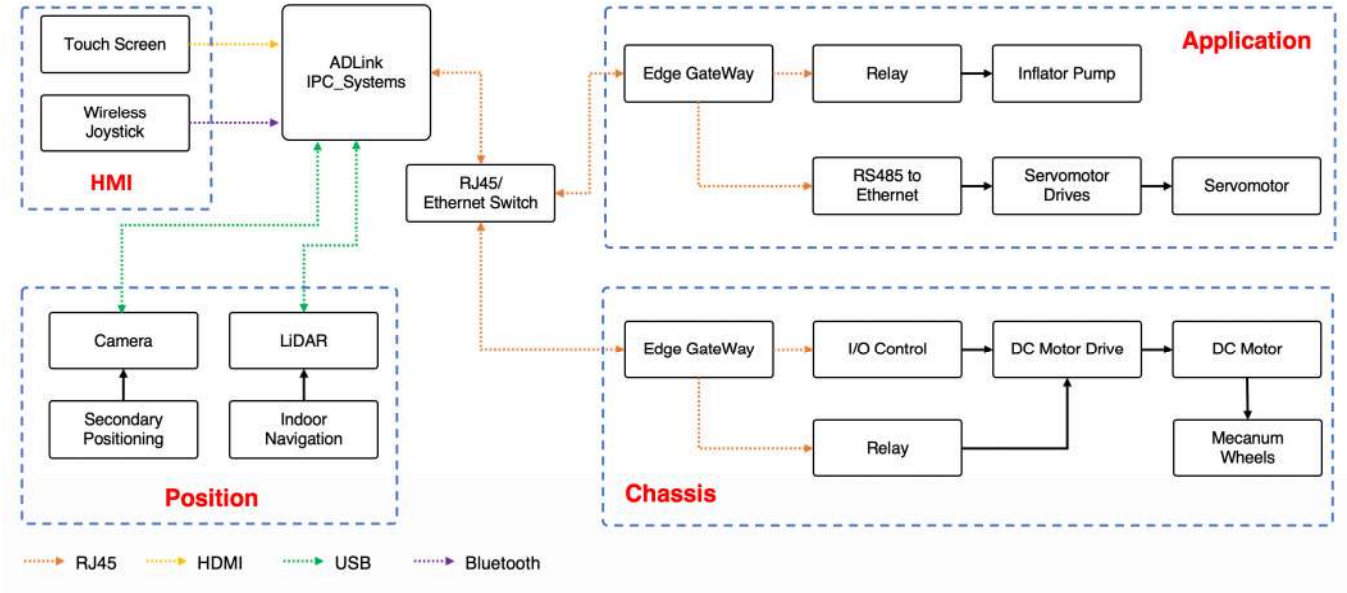


Fig. 14. OAMR control architecture

A. Software Architecture

The two-level control software architecture of the OAMR is designed according to the hardware structure. A complete control diagram for their data exchange is shown in Fig. 15. The Application layer is responsible for controlling gripper positioning and pick-and-place operations. A relay controls pick-and-place actions, while two servo motors regulate the gripper's positioning, as shown in Fig. 16. The JSDT1-6D4 servo drive offers CANopen and RS-485 communication interfaces, with communication protocols including ASCII and RTU as selectable options. To ensure consistency in communication protocols across the system, we utilize an RS485 to Ethernet converter, enabling us to control the servo motors via TCP commands.

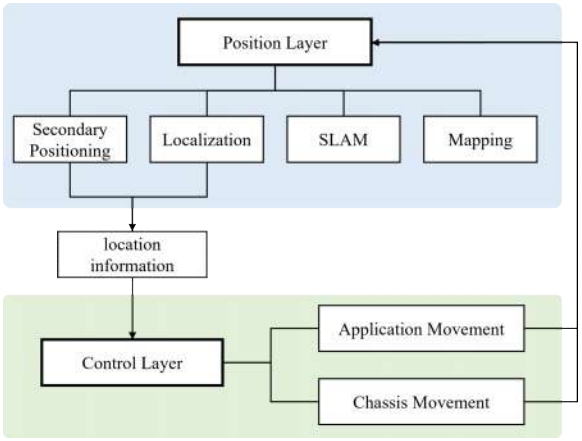


Fig. 15. Schematic diagram of the control software architecture of OAMR

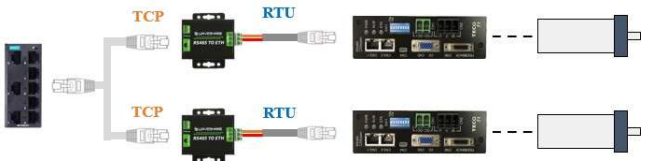


Fig. 16. Gripper positioning control architecture

The Chassis layer manages the movement control of the vehicle's main body. It employs an I/O controller and a relay to control four Mecanum wheels. The I/O controller adjusts the motor speeds while the relay reverses the motor direction. Mecanum wheels are configured as illustrated in Fig. 17. Mecanum wheels are a unique wheel configuration commonly used in robots and vehicles to provide exceptional maneuverability and flexibility. Each wheel has independent rotation capability consisting of four wheels situated at the vehicle's corners. This design enables Mecanum wheel vehicles to move in multiple directions, such as forward, backward, left, right, and diagonally, without requiring the entire vehicle body to rotate. The unique configuration of Mecanum wheels makes them highly valuable for precise direction control in narrow spaces, and they are widely applied in robots, automatic navigation systems, and certain specialized vehicles.

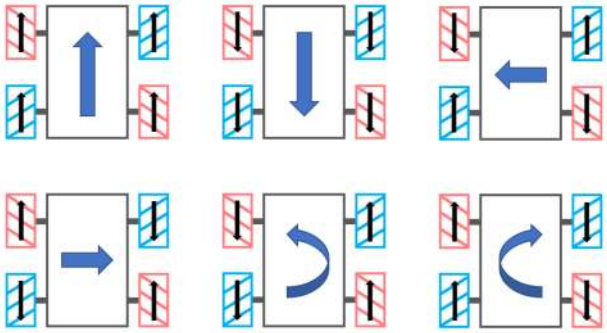


Fig. 17. Mecanum wheel steering

The Position layer handles the positioning control of the vehicle. In this layer, we install a LiDAR for indoor positioning and navigation. Our truck can autonomously navigate to designated positions by leveraging a previously established map. Upon reaching these positions, we activate a camera for precise secondary positioning. Finally, the HMI layer encompasses the external screen and joystick we employ for user interface and control.

B. Sensor Integration

In this advanced OAMR, an array of cutting-edge sensing technologies illustrated in Fig. 18 has been implemented to ensure the highest levels of accuracy in navigation and safety. Lidar takes center stage as an optical remote sensing technology, capable of detecting and mapping the three-dimensional structure of objects and environments by emitting laser pulses. The Inertial Measurement Unit (IMU) supplies crucial data pertaining to the vehicle's direction, speed, and posture, greatly enhancing navigation and positioning capabilities. Additionally, cameras play a pivotal role in providing secondary positioning for the gripper. Lastly, electronic skin, an emerging sensing technology, enables the OAMR to perceive object contact and pressure, enriching its awareness of its surrounding environment. Through the integration of these state-of-the-art sensor components, this advanced OAMR intelligently and safely navigates its environment.

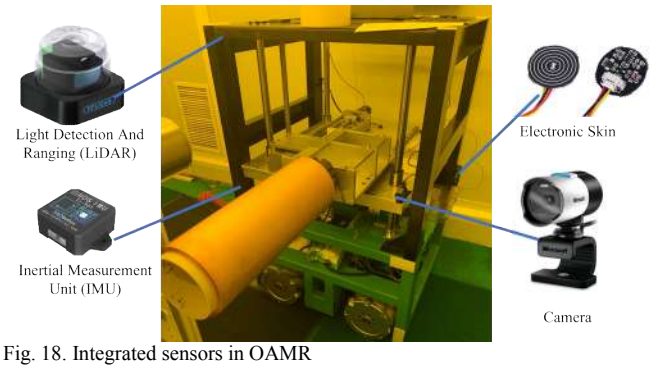


Fig. 18. Integrated sensors in OAMR

IV. Mobile Robot Localization

In this study, OAMR uses RViz (Robot Visualization), a vital tool within the ROS (Robot Operating System), which plays a pivotal role in robot research and development. Designed to assist researchers and engineers, RViz offers potent visualization capabilities for comprehending a robot's state,

sensor data, maps, path planning, and other critical information. It stands out with its capacity to visualize multi-sensor data in real-time, enabling users to monitor the environmental information perceived by the robot. RViz supports a wide array of sensors, including laser scanners, cameras, and inertial measurement units (IMUs), making it indispensable for verifying sensor data accuracy and assessing the robot's perception abilities. Additionally, RViz offers robust map display capabilities that simplify the loading and presentation of both static and dynamic maps. This empowers users to understand better the layout of the robot's surroundings and the positions of obstacles. Path planning visualization allows users to validate global path planning and local path tracking, ensuring the accuracy of the planned route and the safety of the robot's movement. The Lidar is placed on the top center of the OAMR, as illustrated in Fig. 19.

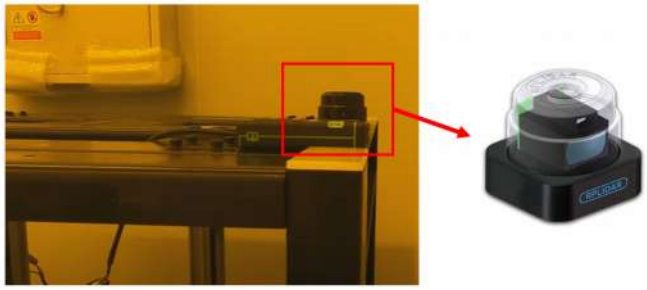


Fig. 19 LiDAR in OAMR for navigation

Simultaneous Localization and Mapping (SLAM) is a foundational technology integrated into our Omnidirectional Autonomous Mobile Robot (OAMR), allowing it to construct real-time maps of its environment while accurately determining its own position. Operating within the Robot Operating System (ROS) framework, SLAM plays a central role in empowering our OAMR with advanced mapping capabilities. Leveraging ROS's extensive suite of tools and libraries, including laser scanners, cameras, SLAM algorithms (such as GMapping or Cartographer), the TF (Transform Library) for reference frame management, environmental mapping, and the Navigation Stack for movement control, our OAMR follows a typical SLAM workflow. This process involves sensor data collection, SLAM algorithm-based estimation of the robot's pose, and the creation of comprehensive maps, as illustrated in Fig. 20. These maps are seamlessly integrated into the navigation system, enabling secure path planning and facilitating autonomous navigation. The adaptability and reliability of SLAM-based map construction in ROS make our OAMR suitable for indoor manipulation of cylindrical FPC.

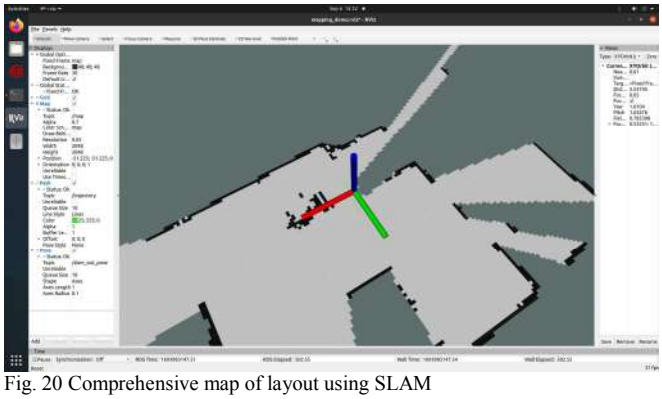


Fig. 20 Comprehensive map of layout using SLAM

V. Cybersecurity Authentication

Autonomous mobile robots (AMRs) enhance production efficiency and quality within intelligent factories. However, their susceptibility to security threats, including hacking attacks and unauthorized access, necessitates proactive measures. To address these concerns, our proposal introduces a streamlined framework grounded in the principles of zero trust, public key infrastructure (PKI), and digital certificate trust chains aimed at fortifying the security of AMRs in smart factory environments. This framework, bolstered by PKI technology and digital certificates, ensures robust identity authentication and secure communication, providing a robust defense against potential vulnerabilities.

A. About Cybersecurity Framework

Zero trust is an information security framework aimed at bolstering data and resource security. Key principles include granting minimal permissions (Least Privilege), rigorous identity authentication and authorization, multi-factor authentication for enhanced identity confirmation, resource segmentation to reduce attack surfaces, real-time monitoring with alert systems, strict access control for both internal and external entities, secure communication through encryption, and continuous updates and maintenance. These principles collectively establish a robust Zero Trust architecture illustrated in Fig. 21, safeguarding systems and data from unauthorized access and potential threats.

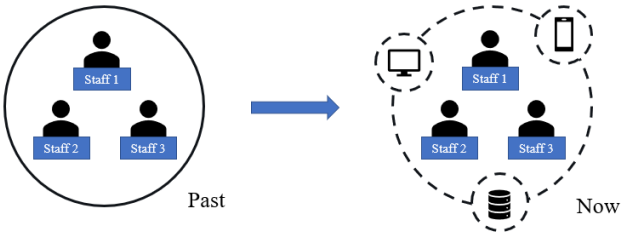


Fig. 21 Zero Trust architecture

Public Key Infrastructure (PKI) is a critical key management system that ensures the security of communication and digital data by utilizing public key encryption and digital signature technologies to securely establish and manage public-private key pairs, facilitating functions such as identity verification, digital signatures, encryption, and decryption. Within PKI, the Registration Authority (RA) plays a pivotal role in aiding users

with the certificate application and registration process. This process involves applying for digital certificates from a Certificate Authority (CA), including identity verification and submission of necessary evidence. The RA serves as an intermediary, assisting users in preparing the required information, verifying identities, and ensuring the accuracy and legitimacy of the provided data. Additionally, PKI employs the Validation Authority (VA) to verify the legality and validity of digital certificates, allowing users to use the CA's special key to authenticate certificates and verify their source and integrity. The overall PKI process is illustrated in Fig. 22.

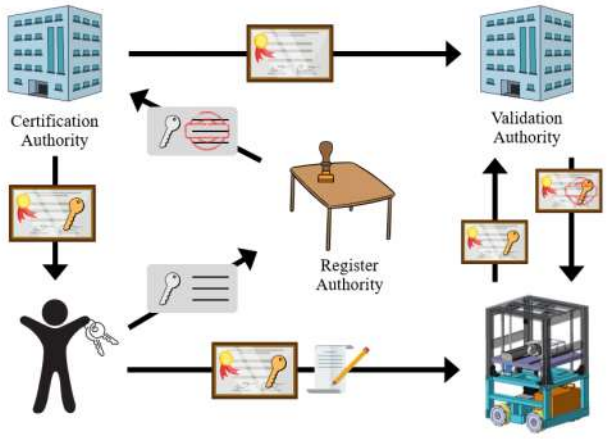


Fig. 22 Public Key Infrastructure

In Public Key Infrastructure (PKI), digital certificates serve as a means to verify the identity of digital entities. These certificates are organized into trust chains, which consist of a series of specialized certificates issued by trusted Certificate Authorities (CAs). Typically, this chain begins with a top-level certificate known as a Root Certificate, securely embedded within operating systems, browsers, or applications to ensure the reliability of CAs. The Root Certificate then issues lower-level certificates called Intermediate Certificates, which, in turn, can issue additional certificates. When verifying a digital certificate's authenticity, the recipient follows this trust chain, meticulously examining the signature of each certificate step by step. If all certificates bear the correct signatures and each certificate in the trust chain is trusted, the digital certificate is deemed valid and legitimate. The overall digital certificate chain is illustrated in Fig. 23.

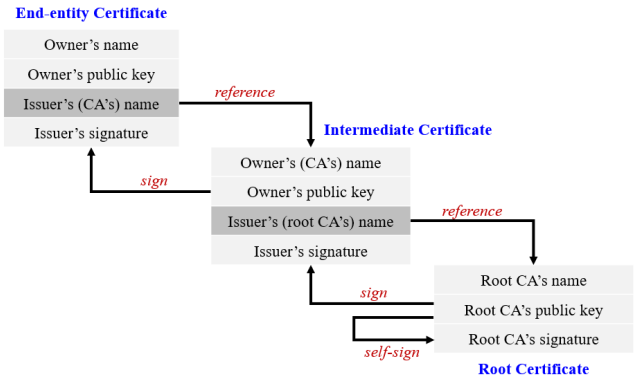


Fig. 23 Digital Certificate Trust Chains

B. Cybersecurity Architecture for OAMR

The systems cybersecurity architecture utilized in the OAMR system is illustrated in Fig. 24. Following the ISA-62443 standard, we implement the "Zone" and "Conduit" concepts to define security zones and communication channels within industrial automation and control systems. Our experimental system of cybersecurity architecture of OAMR comprises three main sections:

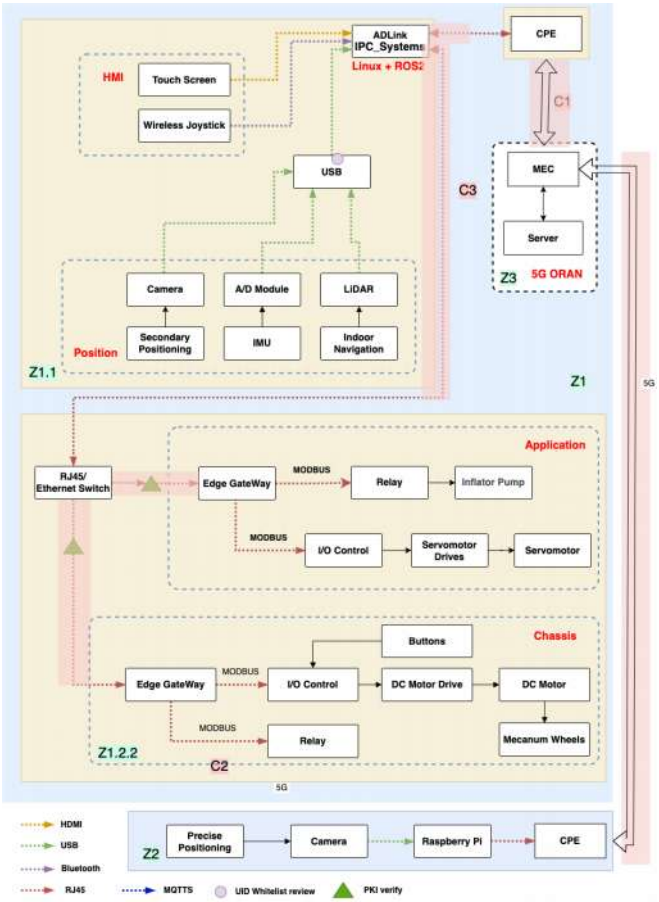


Fig. 24. Cybersecurity system Architecture of OAMR

1. **Autonomous Mobile Robots Segment**: This zone includes multiple devices and is further divided into two sub-zones, Z1.1 and Z1.2, each with distinct security levels and access control policies.

- **Z1.1**: This sub-zone includes the previously introduced HMI and Position components. Devices in this region communicate with industrial PCs via USB. In the Ubuntu operating system, each user is assigned a unique UID. Through USB UID whitelist settings, system administrators can effectively monitor USB device usage, reducing security threats and preventing data leaks and unauthorized duplication of sensitive documents. Only authorized users listed in the whitelist are granted access to these devices.
- **Z1.2**: The Application and Chassis components reside in this sub-zone. Devices in this area connect through RJ45 and Ethernet switches and undergo PKI authentication. PKI (Public Key Infrastructure) is a cryptographic framework for online security authentication, managing and verifying user identities, digital certificates, and their associated public and private keys.

PKI ensures secure online communication. Traditional perimeter defenses alone are insufficient in response to the growing complexity of information security challenges. Intruders within the network can move freely. Therefore, many organizations are adopting a zero-trust approach to enhance information security. Our strategy involves continuous verification, with the computer periodically checking with the Switch to validate the trustworthiness of connected devices. If deemed trustworthy, the device receives a digital badge, utilizing a decentralized digital identity verification and authorization system based on blockchain technology. In this digital badge trust chain, each participant possesses a unique identifier verified and authorized through blockchain technology.

2. **Human Posture Recognition Segment:** Our camera is linked to a Raspberry Pi, with an edge-located CPE device assisting in receiving 5G wireless signals. A built-in router converts these signals into wired or wireless local network signals, enabling rapid image transmission within a private network.

3. **5G ORAN Network**: The 5G ORAN (Open Radio Access Network) represents an open wireless access network grounded in Software Defined Networking (SDN) and Network Function Virtualization (NFV) technologies. This architecture ensures interoperability among infrastructure, cloud-native applications, and services via standardized interfaces and protocols. Unlike traditional wireless access networks, which often rely on proprietary, closed-off components provided by a single vendor, 5G ORAN disrupts this model. It offers an open framework that grants operators greater flexibility in selecting and integrating various hardware and software devices. This approach streamlines network construction and operation, leading to quicker, more cost-effective, and highly adaptable network deployment.

VI. Experiments and Discussion

A. OAMR Integration with Factory Environment

The integration of OAMR within a factory environment and its operation in manipulating cylindrical FPC boards and transporting them from the material area to the PCB machine is illustrated in Fig. 25.

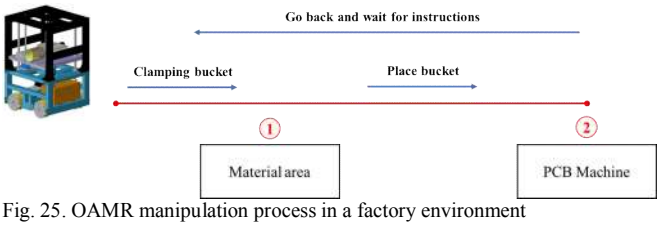


Fig. 25. OAMR manipulation process in a factory environment

Initially, our vehicle will proceed to the materials area to perform the loading operation. Upon successfully obtaining the materials, the vehicle will autonomously navigate to the vicinity of the machine, employing SLAM technology. As it approaches the AOI machine depicted in Fig. 26, we will employ a QR code positioned on the machine to refine the gripper's positioning through a secondary round of localization.

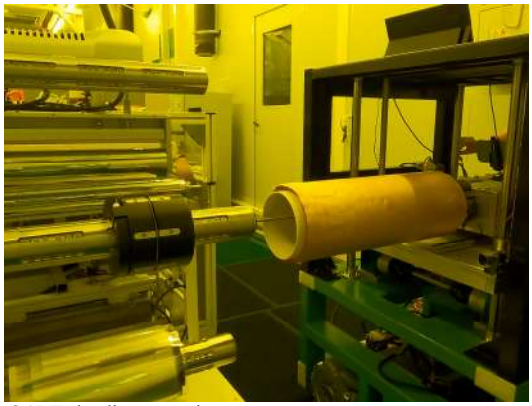


Fig. 26. OAMR loading operation

After completing the calibration process and ensuring the arm is in the precise location, as mentioned. If the arm is not precisely centered in the designated location, it will not proceed with the process, and a safety skin is in place to ensure complete safety. Only when the perfect center is achieved will the vehicle proceed to position the materials onto the PCB machine, as depicted in Fig. 27. Following the completion of the unloading process, the robot will then return to the materials area.

Fig. 27. OAMR unloading operation at AOI machine

The successful integration of OAMR technology into a factory environment for the efficient manipulation and transportation of cylindrical FPC is shown in this section. This process involves precise loading from the materials area, autonomous navigation using SLAM technology, and rigorous calibration to ensure safety and accuracy. Only when the arm is perfectly centered does the vehicle proceed to position the materials onto the PCB machine. This integration demonstrates OAMR's potential to enhance efficiency and safety in factories with precise material handling needs.

B. OAMR with Cybersecurity Authentication

In our experimental setup for cybersecurity authentication, we establish connectivity between two Raspberry Pi devices using an Ethernet switch, as illustrated in Fig. 28. Each Raspberry Pi undergoes a permissions validation procedure throughout this process, gaining control over the console only after successfully authenticating its credentials. In the chassis layer, we employ a combination of I/O and relay controls to effectively manage the movements of our vehicle. Simultaneously, within the application layer, our primary aim is to manipulate the servo motor, enabling the robotic arm to grasp

objects. To achieve this, given our motor's operation using RTU communication, we employ an RS485-to-Ethernet converter, enabling control via TCP. Leveraging relay control, we efficiently operate the jaws, allowing them to open and close as required.

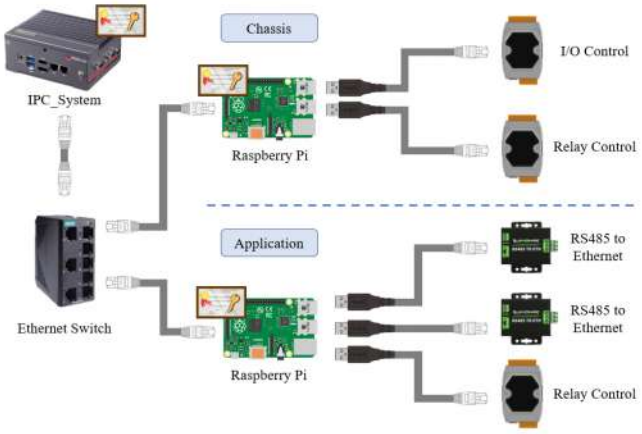


Fig. 28 Connection of chassis and application Layer for cybersecurity authentication

In the HMI (Human-Machine Interface) layer, as illustrated in Fig. 29, our setup includes a touchscreen interface connected via HDMI, while our keyboard and mouse peripherals are linked through USB. Moving to the positioning layer illustrated in Fig. 29, we integrate several key components, including a camera, an inertial measurement unit (IMU), and light detection and ranging (LiDAR) systems, all interconnected via USB interfaces. This configuration collectively enhances the system's functionality and sensory capabilities.

Fig. 29 HMI and Position Layer

In the Ubuntu system, connecting a device via USB requires a unique idVendor and idProduct. In Fig. 30 it is illustrated that the LiDAR is identified with an idVendor of 2717 and an idProduct of 5013.

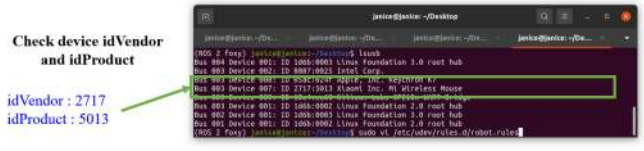


Fig. 30 Display of idVendor and idProduct

Afterward, this device is assigned appropriate permissions, with a permission level of 7 indicating read, write, and execute access. Additionally, symlinks are utilized to provide the flexibility of customizing the device's name. This allows us to easily locate the device by its customized name, as illustrated in Fig. 31.

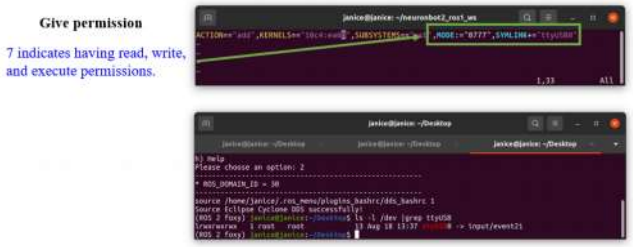


Fig. 31 Displaying the location of a device by its customized name

VII. Conclusion

The development of the Omnidirectional Autonomous Mobile Robot (OAMR) marks a significant advancement in meeting the increasing demand for indoor mobility solutions in today's era of automation, particularly within confined spaces where object manipulation presents considerable challenges. This paper develops an innovative solution tailored for indoor manipulation of cylindrical FPC with a payload capacity of 20 Kg. The OAMR utilizes Mecanum wheels for enhanced maneuverability and a two-degree-of-freedom arm for object manipulation. It enhances its maneuverability and makes it well-suited for indoor applications, having small space. The structural analysis ensures robustness for dependable performance in industrial settings underlined with an exemplary safety factor. Beyond physical capabilities, the integration of advanced sensor technologies and a comprehensive control system, including LiDAR and visual sensors, augments the OAMR's efficiency in navigating indoor spaces. Moreover, this paper emphasizes the paramount importance of cybersecurity in smart factory environments, advocating for a zero-trust framework, public key infrastructure (PKI), and digital certificate trust chain technology to safeguard network communication and identity authentication. Experimental integration of OAMR in a factory environment demonstrates its potential for efficient material handling, while cybersecurity measures enhance its security in smart factory settings. Overall, this research showcases the capabilities of OAMR in industrial applications and addresses critical cybersecurity concerns. Future research in this field can explore AI and machine learning integration for enhanced autonomous decision-making, lightweight yet robust construction materials for improved mobility, and advanced cybersecurity measures to adapt to evolving smart factory landscapes, promising further innovations in automation and robotics.

Acknowledgment

The support from the National Science and Technology Council, Taiwan (grant number NSTC 112-2218-E-011-009) and Intelligent Manufacturing Innovation Center (IMIC), which is a Featured Areas Research Center in Higher Education Sprout

Project of Ministry of Education (MOE), Taiwan (since 2023) were appreciated.

REFERENCES

[1] A. Loganathan and N. S. Ahmad, "A systematic review on recent advances in autonomous mobile robot navigation," *Engineering Science and Technology, an International Journal,* vol. 40, p. 101343, 2023.
[2] V. Jaiganesh, J. D. Kumar, and J. Girijadevi, "Automated guided vehicle with robotic logistics system," *Procedia Engineering,* vol. 97, pp. 2011-2021, 2014.
[3] S. Bogh *et al.*, "Integration and assessment of multiple mobile manipulators in a real-world industrial production facility," in *ISR/Robotik 2014; 41st International Symposium on Robotics*, 2014: VDE, pp. 1-8.
[4] A. Baldassarri, M. Bertelli, and M. Carricato, "Design of a Reconfigurable Mobile Collaborative Manipulator for Industrial Applications," *Journal of Computational and Nonlinear Dynamics,* pp. 1-12, 2023.
[5] G. K. Kraetzschmar *et al.*, "Robocup@ work: competing for the factory of the future," in *RoboCup 2014: Robot World Cup XVIII 18*, 2015: Springer, pp. 171-182.
[6] I. Doroftei, V. Grosu, and V. Spinu, *Omnidirectional mobile robot-design and implementation*. INTECH Open Access Publisher London, UK, 2007.
[7] M. A. Niloy *et al.*, "Critical design and control issues of indoor autonomous mobile robots: A review," *IEEE Access,* vol. 9, pp. 35338-35370, 2021.
[8] M. Schneier, M. Schneier, and R. Bostelman, *Literature review of mobile robots for manufacturing*. US Department of Commerce, National Institute of Standards and Technology, 2015.
[9] K. Kanjanawanishkul, "Omnidirectional wheeled mobile robots: wheel types and practical applications," *International Journal of Advanced Mechatronic Systems,* vol. 6, no. 6, pp. 289-302, 2015.
[10] V. De Silva, J. Roche, and A. Kondoz, "Robust fusion of LiDAR and wide-angle camera data for autonomous mobile robots," *Sensors,* vol. 18, no. 8, p. 2730, 2018.
[11] M. J. Puerto, D. Sallé, J. L. Outón, H. Herrero, and Z. Lizuain, "Towards a flexible production system Environment Server implementation," in *International Conference on Computer as a Tool (EUROCON), 2015*, 2015: IEEE, pp. 1-6.
[12] L. Mochurad, Y. Hladun, and R. Tkachenko, "An Obstacle-Finding Approach for Autonomous Mobile Robots Using 2D LiDAR Data," *Big Data and Cognitive Computing,* vol. 7, no. 1, p. 43, 2023.
[13] T. Ji and L. Xie, "Vision-aided Localization and Navigation for Autonomous Vehicles," in *2022 IEEE 17th International Conference on Control & Automation (ICCA)*, 2022: IEEE, pp. 599-604.
[14] A. Haldorai, "A Review on Artificial Intelligence in Internet of Things and Cyber Physical Systems," *Journal of Computing and Natural Science,* vol. 3, no. 1, pp. 012-023, 2023.
[15] S. Wang, L. Jiang, J. Meng, Y. Xie, and H. Ding, "Training for smart manufacturing using a mobile robot-based production line," *Frontiers of Mechanical Engineering,* vol. 16, pp. 249-270, 2021.
[16] J.-H. Syue and S.-L. Chen, "A multi-layer network security system to enhance autonomous mobile carrier in smart manufacturing system," *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture,* p. 09544054221135930, 2023.
[17] A. Botta, S. Rotbei, S. Zinno, and G. Ventre, "Cyber Security of Robots: a Comprehensive Survey," *Intelligent Systems with Applications,* p. 200237, 2023.
[18] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," National Institute of Standards and Technology, 2020.
[19] U. Maurer, "Modelling a public-key infrastructure," in 4th European Symposium on Research in Computer Security Rome, Italy, September 25–27, 1996 1996: Springer, pp. 325-350.
[20] A. Agarwal and R. Shankar, "On-line trust building in e-enabled supply chain," *Supply Chain Management: An International Journal,* vol. 8, no. 4, pp. 324-334, 2003.

Brijesh Patel received a Ph.D. degree in Mechanical Engineering from MATS University, India. He is a post-doctoral researcher at the Department of Mechanical Engineering, National Taiwan University of Science and Technology (NTUST), Taiwan. His research interests are robotics and drones, industrial aerodynamics, and composite materials.

Shang-Chen Kuo is currently a M.S. student in the Department of Mechanical Engineering at National Taiwan University of Science and Technology (NTUST), Taipei, Taiwan, and expects to graduate in 2024.

Chih-Chi Yuan is currently a M.S. student in the Department of Mechanical Engineering at National Taiwan University of Science and Technology (NTUST), Taipei, Taiwan, and expects to graduate in 2024.

Chin-Hsing Kuo received a Ph.D. degree in Mechanical Engineering from Kings College, London, United Kingdom, in 2011. He is currently a Senior Lecturer in the School of Mechanical, Materials, Mechatronic and Biomedical Engineering, University of Wollongong (UOW), NSW, Australia. His research interests include machine design, static and dynamic balancing, magnetic mechanism systems, serial and parallel robots, continuum robotics, surgical robotics, rehabilitation robotics, etc.

Ming-Hau Tsai is with the Industrial Technology Research Institute (ITRI), Hsinchu, Taiwan.

Lung Chen Liang is with Career Technology Manufacturing Company, Limited, New Taipei City, Taiwan.

Jen-Wei Yeh is a Research Scientist / Product Manager at Taiwan Certification Authority Corporation (Taiwan-CA Inc.).

Chung-Hsien Kuo received a Ph.D. degree in Mechanical Engineering from the National Taiwan University, Taipei, Taiwan, in 1999. He is currently a Professor at the Department of Mechanical Engineering at National Taiwan University. His research interests include intelligent robots, autonomous systems, artificial intelligence, and sensor fusion applications.

Chao-Lung Yang received a Ph.D. degree in industrial engineering from Purdue University, USA, in 2009. He is currently a Professor at the Department of Industrial Management, National Taiwan University of Science and Technology. His research interests include data mining, machine learning, Big Data analytics, metaheuristic algorithms, and human action recognition.

Po Ting Lin received his M.S. and Ph.D. degrees in the Department of Mechanical and Aerospace Engineering at Rutgers University, New Brunswick, New Jersey, USA in 2007 and 2010, respectively. He's currently a Professor in the Department of Mechanical Engineering at National Taiwan University of Science and Technology (NTUST), Taipei, Taiwan. He's also the Director of the Global Development Engineering Program (GDEP) and the Director of International Advanced Technology Program (IATP) at NTUST. His research interests include design optimization with uncertainty, machine vision, industrial robotics, autonomous mobile robots, industry 4.0, cyber-physical systems, etc.