Robotics Platforms for Internal Logistics: A Technical Architecture Proposal

Francisco Fraile [1,2] and Raul Poler [1]

[1] *Universitat Politècnica de València, Camino de Vera S/N, Valencia, 46022, Spain*
[2] *Escuela de Empresarios, Muelle de la Aduana S/N, Valencia, 46022, Spain*

Abstract

This paper presents a reference technical architecture model for robotic platforms specifically designed for internal logistics applications. The reference application is based in industry standards like ISA/IEC 62443 and the Industrial IoT Reference Architecture (IIRA).

Keywords

Autonomous mobile robots, internal logistics, reference architecture, fleet management systems

1. Introduction

Autonomous Guided Vehicles (AGVs) are a well-established solution to automate internal logistic operations [1]. AGVs have been designed to operate in large installations and consequently, they require large spaces dedicated to robot operations. Human safety is thus achieved through physical isolation: Humans and robots do not share the same space to avoid any risk of accidents that could cause harm to human operators. These requirements on the other hand make it difficult to introduce this technology in smaller logistic installations, as those typically found in medium or small sized companies, which do not have enough space available to deploy AGVs, or that need instead a collaborative solution that would allow for a scaled, progressive automation of logistic tasks. As a response, Autonomous Mobile Robots (AMRs) represent a versatile alternative. Unlike AGVs, AMRs are able to navigate freely in a space shared with humans, taking a more collaborative approach to internal logistics automation.

In this sense, robotic platforms for internal logistics facilitate the deployment, planning, management, and supervision of fleets of AMRs in large, medium-sized, or small enterprises, to perform logistics tasks in industrial environments. Primarily, these platforms rely on the following technologies to support internal logistic operations and management:

- **Autonomous vehicles and collaborative robots for logistics applications**: The robotic platform will integrate with autonomous vehicles and collaborative robots designed to execute logistics tasks in industrial environments. The robots will be able to execute tasks in the internal logistics of companies, favoring the automation and efficiency of processes.
- **Supervision and monitoring in the edge/cloud**: The platform facilitates the deployment of a set of services that will connect the physical elements (robots) with the management and optimization logic, allowing decoupling the control aspects from the operations. These services are rooted in cloud technologies to provide the required elasticity to deploy on-premise or in- cloud depending on the specific user requirements.
- **Fleet management and optimization**: From a functional perspective, the main added value of the services provided by the platform is to facilitate robot fleet management and operations: Optimal planning and sequencing of operations, routing and monitoring of

Proceedings of the Workshop of I-ESA'22, March 23–24, 2022, Valencia, Spain
EMAIL: ffraile@cigip.upv.es (F. Fraile); rpoler@cigip.upv.es (R. Poler)
ORCID: 0000-0003-0852-8953 (F. Fraile); 0000-0003-4475-6371 (R. Poler)

operations through indicators. The algorithms and analytical techniques used are integrated into applications in a simple and efficient way using the Function as a Service (FaaS) cloud computing paradigm.

- **Blockchain and traceability in the supply chain**: LogiBlock will leverage Industrial IoT and blockchain technologies to provide the level of trust required by supply chain collaborators in operations traceability.

The efficient integration of these technologies, together with other information systems already present in factories, such as Enterprise Resource Planning (ERP), Manufacturing Execution Systems (MES), or Warehouse Management Systems (WMS) potentially enables a turn-key solution with the following features:

- **Plug-and-Play**: Communication services use standard communication interfaces and modules to automatically discover and integrate with hardware and software systems in the factory. The solution will scale transparently to the user as new vehicles and robots or modules are added to those already deployed. For instance, the FMS can automatically discover and on-board a new AMR, or dispatch a picking order to an integrated WMS.
- **Scalability and modularity**: The hardware required to enable robot navigation and management is affordable, has a small footprint, and can be deployed in a cost-efficient way. Services can be hosted on-premise or on-cloud, to simplify the connection and deployment of the platform to end users solution, making the solution modular and scalable. End-users will be able to easily add new modules to vehicles and robots to execute different logistic tasks or to adapt them to different environments.
- **Customizable**: The solution will provide programming interfaces (APIs) and software development kits (SDKs) to facilitate the integration of the service layer with other systems and applications, and the development of customizations or adaptations to different verticals.

This paper presents a reference architecture of a robotic platform specifically designed for internal logistics applications using AMRs and meeting the requirements of small and medium-sized companies. The reference architecture is based on Robotic Operating System (ROS), an open-source, modular platform for robotic applications [2]. The next describes the proposed reference architecture, and section 3 describes the methodology used to develop usage, functional and technical specifications based on the proposed reference architecture.

2. Technical architecture

Figure 1 illustrates the reference architecture for robotic platforms proposed in this research paper. The reference architecture has been developed in the framework of the research project Logiblock, and is based in known industrial best practices, security standards, and relevant reference architectures like the Industrial Internet of Things Reference Architecture (IIRA) [3]. The main objective of Logiblock is the development of a trustworthy robotic platform designed to facilitate the introduction of AMRs in medium and small sized companies.

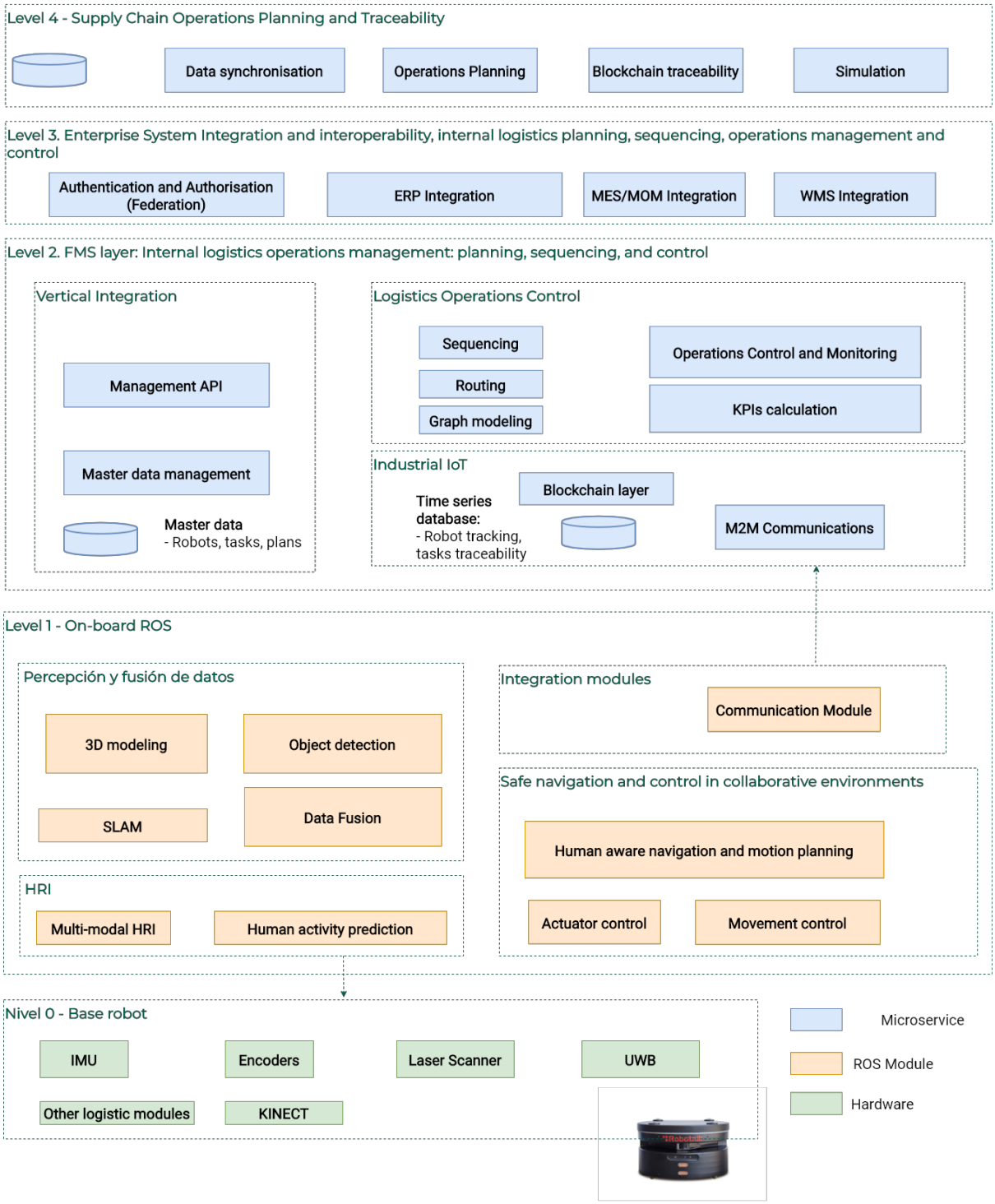

Figure 1: Reference Architecture Diagram

The definition of the reference architecture is based on industry standards and best practices for open robotics, and it follows the recommendations of the ISA/IEC 62443 standard on security in industrial control systems [4]. Specifically, IE 62443-3-3 "System Security Requirements and Security Levels" establishes a separation between different security levels or zones:

- **Level 0: Industrial level**. This level groups together the physical components of industrial systems, mainly actuators and sensors. In a robotic platform, this level groups the physical sensors and modules that enable navigation, such as Laser Imaging Detection and Ranging (LIDAR), Inertial Measurement Unit (UMI) or Ultra Wideband (UWB), as well as logistic modules like cameras, laser scanners or encoders to detect products, e.g. for product

inventory. At this stage it is important to consider that for robustness and efficiency, in practice, several indoor localization technologies are combined. UWB and IMU-UWB integration provides a good trade-off between cost, accuracy and deployment complexity [5]. The base hardware selected to implement the reference architecture comprises ROS compatible logistic robots like Robotnik`s RB-1 [6] (up to 30kg loading weight) and Theron logistic robots [7] (up to 200kg loading weight).

- **Level 1: Control.** This level contains the system-level control elements of the components at level 0. In a robotic platform, this level groups the Human-Robot-Interaction modules, the modules to model the environment, including humans, and the modules to control the robot: human navigation and motion planning, actuator control, and movement control. Modules for data fusion to enable the integration of different indoor positioning systems are also located at this level. From a technical point of view, the modules at this level are implemented as ROS modules, interconnected in a level-1 ROS network, deployed in a edge platform or on-board computer with GPU acceleration to achieve the required performance. This is particularly important for modules that rely on neural networks, like (Yolov4) object detection [10] and human activity prediction. The performance of these modules has been successfully tested using a NVIDIA Jetson module [11]. Communication with higher layers is implemented through ROS bridge modules (communication modules) that act as secure conduits to exchange information with level-2 components, using the Message Queue Telemetry Transport Protocol (MQTT) [8] or the OPC Unified Architecture (OPC UA) [9] protocol.
- **Level 2: Operation.** This level groups together the operation and supervision systems, such as operator terminals or consoles, monitoring applications to monitor and control the fleet, etc. In a robotic platform, this level groups the main functional blocks of the Fleet Management system, including functions to control and orchestrate the robotic fleet, calculate Key Performance Indicators (KPIs) for logistic operations monitoring, as well as functions to enable communication between level 1 and higher levels according to security specifications for Industrial Control Systems. From a technical point of view, these modules are microservices [12] deployed in a microservice orchestration platform like Kubernetes [13]. The Machine 2 Machine communication module provides an endpoint (e.g. MQTT broker) used to send control commands to and receive status feedback from the robotic fleet. The information is stored in a time series database microservice to enable robot tracking and tasks traceability. Moreover, the global navigation map used by the robots is processed to generate a network graph used to implement routing and task sequencing functions. To facilitate vertical integration, this level implements microservices to manage master data and expose management functions to level 3 services or external systems through a management Application Programming Interface (API).
- **Level 3: Enterprise.** This level groups together equipment and systems to provide support to the company's business processes, such as ERP. This level of the reference architecture groups functional blocks to implement Role Based Access Control to the FMS functions, including federation with external authentication and authorization services, as well as functional blocks to integrate with other enterprise systems, like the ERP, MES/MOM, or WMS integration. From a technical point of view, these functions are mapped to microservices. Communication with level 2 functional blocks is achieved through the management API, so that level 2 and level 3 services are decoupled to achieve inter-level isolation.
- **Level 4: Supply chain**. This level is introduced by the authors to extend the solution to the supply chain level, enabling collaboration among supply chain collaborators. This level groups advanced services to enable trustable supply chain traceability using blockchain technology, data services to enable the integration and synchronization of data distributed across different platforms, supply chain operations planning services, and simulation services to simulate internal logistic processes.

3. Discussion

The ISA/IEC 62443 standard establishes that any industrial control system compatible with this standard must conveniently define these levels, so that they can be located in independent sub-networks. To adequately protect the components at the physical level, level 0, which are those that can compromise the safety of operators, communications must always be made from the lower levels to the upper levels (communications are not allowed to be initiated in the opposite direction), and all communications between levels must use secure, properly protected conduits (security paths between two levels). This allows for the proper establishment of a Defense In Depth strategy, which is a defense strategy based on the establishment of different security controls to protect critical systems at lower levels [14].

From a business perspective, the system must be as user-friendly as possible, easy to deploy and therefore, its implementation in accordance with these standards must be simple, so as not to represent a potential threat, but rather an advantage in the factories. Furthermore, the system must allow the deployment of the different components in the edge/cloud continuum in a flexible way, allowing some of the system's features to be offered in Software as a Service models to favor collaboration in the supply chain. Thus, system components must be able to be deployed in a distributed manner across different hardware equipment to enable the deployment of defense strategies compatible with this standard. Based on these requirements, the proposed reference architecture has adopted a layered model that is compatible with this vision and which translates into the described levels.

4. Acknowledgements

This research has been funded by the Agència Valenciana de la Innovació, under the program Projectes Estratègics en Cooperació 2021 (UPV->INNEST/2021/226). Action co-financed by the European Union through the European Regional Development Fund (ERDF) Operational Programme for the Valencia Region 2014-2020.

5. References

[1] E.A. Oyekanlu, A.C. Smith, W. P. Thomas, G. Mulroy, D. Hitesh, M. Ramsey, ... D. Sun, A review of recent advances in automated guided vehicle technologies: Integration challenges and research areas for 5G-based smart manufacturing applications, IEEE Access 8 (2020) 202312-202353. doi: 10.1109/ACCESS.2020.3035729

[2] M. Quigley, K. Conley, B. Gerkey, J. Faust, T. Foote, J. Leibs,... A. Y. Ng, (2009, May). ROS: an open-source Robot Operating System, in: ICRA workshop on open source software, volume 3, IEEE, Kobe, 2009, p.5.

[3] S. W. Lin, B. Miller, J. Durand, R. Joshi, P. Didier, A. Chigani,... G. Bleakley, (2015). Industrial Internet Reference Architecture, 2015. URL: https://hub.iiconsortium.org/iira#:~:text=Industrial%20Internet%20Reference%20Architecture%20(IIRA)&text=The%20IIRA%20is%20a%20standards,guide%20technology%20and%20standard%20development.

[4] E. Kronfuss, Industrial Cyber Security Standard-IEC 62443 (No. IAEA-CN--267), 2018.

[5] H. Zhang, Z. Zhang, N. Gao, Y. Xiao, Z. Meng, Z. Li, Cost-effective wearable indoor localization and motion analysis via the integration of UWB and IMU, Sensors 20 (2020) 344. doi: 10.3390/s20020344.

[6] Robotnik RB-1, 2022. URL: https://robotnik.eu/products/mobile-robots/rb-1-base-en/

[7] Robotnik, RB-Theron Mobile Robot, 2022. URL: https://robotnik.eu/products/mobile-robots/rb-theron-en/

[8] OASIS, MQTT Version 5.0, 2019. URL: https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html

[9] OPC Foundation, Specifications, 2022. URL: https://opcfoundation.org/developer-tools/specifications-unified-architecture.

[10] A. Bochkovskiy, C. Y. Wang, H. Y. M. Liao, Yolov4: Optimal speed and accuracy of object detection, 2020. URL: https://arxiv.org/abs/2004.10934.

[11] S. Mittal, A survey on optimized implementation of deep learning models on the NVIDIA Jetson platform, Journal of Systems Architecture 97(2019) 428-442. doi: 10.1016/j.sysarc.2019.01.011.
[12] D. Jaramillo, D. V. Nguyen, Smart, R., Leveraging microservices architecture by using Docker technology, in: SoutheastCon 2016, IEEE, Norfolk, 2016, pp. 1-5. doi: 10.1109/SECON.2016.7506647.
[13] Kubernetes, What is Kubernetes, 2022. URL: https://kubernetes.io/docs/concepts/overview/what-is-kubernetes/.
[14] F. Fraile, T. Tagawa, R. Poler, A. Ortiz, Trustworthy industrial IoT gateways for interoperability platforms and ecosystems, IEEE Internet of Things Journal 5 (2018) 4506-4514. doi: 10.1109/JIOT.2018.2832041